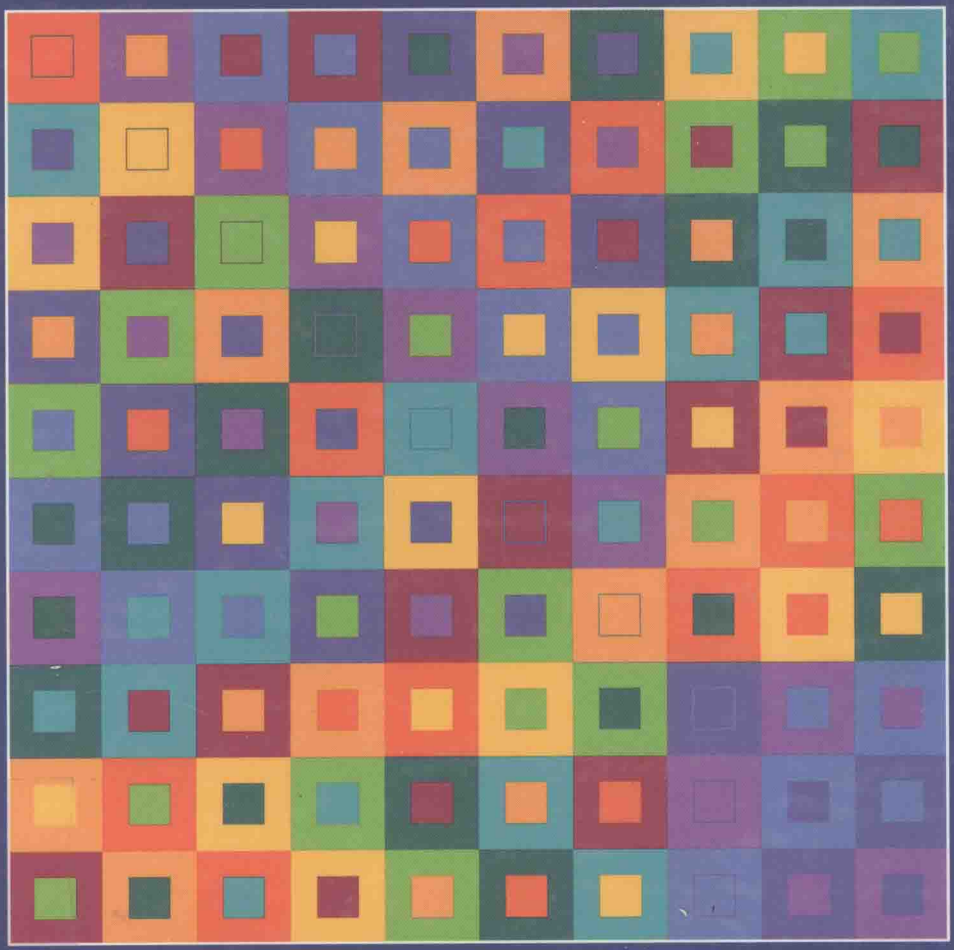
A FIRST COURSE IN ABSTRACT ALGEBRA



JOSEPH ROTMAN

A First Course in Abstract Algebra

Joseph J. Rotman

University of Illinois

at Urbana-Champaign

PRENTICE HALL, Upper Saddle River, New Jersey 07458

Library of Congress Cataloging-in-Publication Data

Rotman, Joseph J.
A first course in abstract algebra / Joseph J. Rotman.
p. cm.
Includes bibliographical references and index.
ISBN 0–13–311374–4
1. Algebra, Abstract. I. Title.
QA162.R67 1996
512' .02—dc20 95–31129
CIP

Acquisitions editor: George Lobell
Production editor: Carol Barbara/Elaine Wetterau
Cover design: Bruce Kenselaar
Manufacturing buyer: Alan Fischer

The original painting of 10×10 orthogonal Latin squares by Emi Kasai hangs in the office of the Mathematics Department of the University of Illinois at Urbana–Champaign

Simon & Schuster/A Viacom Company
Upper Saddle River, New Jersey 07458

Printed in the United States of America

10 9 8 7 6 5 4 3

ISBN 0–13–311374–4

PRENTICE-HALL INTERNATIONAL (UK) LIMITED, *LONDON*
PRENTICE-HALL OF AUSTRALIA PTY. LIMITED, *SYDNEY*
PRENTICE-HALL CANADA INC., *TORONTO*
PRENTICE-HALL HISPANOAMERICANA, S.A., *MEXICO*
PRENTICE-HALL OF INDIA PRIVATE LIMITED, *NEW DELHI*
PRENTICE-HALL OF JAPAN, INC., *TOKYO*
SIMON & SCHUSTER ASIA PTE, LTD., *SINGAPORE*
EDITORA PRENTICE-HALL DO BRASIL, LTDA., *RIO DE JANEIRO*

PREFACE

A First Course in Abstract Algebra introduces three related topics: number theory (division algorithm, greatest common divisors, unique factorization into primes, and congruences), group theory (permutations, Lagrange's theorem, homomorphisms, and quotient groups), and commutative ring theory (domains, fields, polynomial rings, homomorphisms, quotient rings, and finite fields). The final chapter combines the preceding chapters to solve some classical problems: angle trisection, squaring the circle, doubling the cube, construction of regular n-gons, and impossibility of generalizing the quadratic, cubic, and quartic formulas to polynomials of higher degree. Such results make it clear that mathematics is, indeed, one subject whose various areas do bear one on the other.

A complicating factor, permeating introductory courses, is that this may be one of the first times students are expected to read and write proofs. This book is my attempt to cover the required topics, to give models of proofs, and to make it all enjoyable.

There is enough material here for a two-semester course, even though many readers may be interested in only one semester's worth. All the "usual suspects" are assembled here, however, and I hope that instructors will be able to find those theorems and examples they believe to be appropriate for a first course. When teaching a one-semester course, one must skip parts of the text; however, it is often possible simply to state and use theorems whose proofs have been omitted. For example, if the discussion of generalized associativity is omitted, one can safely cite the laws of exponents; if the proof of Gauss's lemma is omitted, one can quote it and still derive irreducibility criteria for polynomials in $\mathbb{Q}[x]$. Here is one possible selection of topics for a one-semester (40–45 lecture) course.

Do all of Chapter 1 except Theorems 1.22 and 1.41 (for the moment, "Theorem" means Lemma, Theorem, or Corollary), Examples 1.1, 1.2, 1.3, and 1.5, and the section on calendars.

In Chapter 2, do not cover Theorems 2.19, 2.21, 2.21′, 2.29 through 2.40, 2.53 through 2.60, 2.65, 2.72, 2.73, 2.80, 2.81, 2.84, 2.85, and 2.86 (but note that the introduction of the dihedral groups has now been omitted), and do not assign Examples 2.5, 2.17, 2.18, 2.24, 2.34, 2.35, 2.36, and 2.39.

In Chapter 3, do not cover Theorems 3.37, 3.38, 3.39, 3.52 through 3.56, 3.67 through 3.72, Example 3.27, and the section on Latin squares. Skip Chapter 4.

I do not enjoy reading introductory chapters of books that consist wholly of "tools" needed for understanding subsequent material. By the Golden Rule, I do not inflict such greetings on my readers. Rather than beginning with a discussion of logic, sets, Boolean operations, functions, equivalence relations, and so forth, I introduce such tools as they are needed. For example, functions and bijections are introduced with permutation groups; equivalence relations are introduced in Chapter 3 to construct fraction fields of domains (I recognize that this late entry of equivalence relations and equivalence classes may annoy those who prefer introducing quotient groups with them; however, I feel that readers first meeting cosets and quotient groups do not need the extra baggage of an earlier discussion of equivalence classes). The first section of Chapter 1 does introduce an essential tool, induction, but induction also serves there as a vehicle to introduce more interesting topics such as primes and De Moivre's theorem.

Several results that are not usually included in a first course have been included just because they are interesting and accessible applications; they should not be presented in class because they are designed for curious readers only. In Chapter 1 on number theory, congruences are used to find on which day of the week a given date falls. In Chapter 2 on groups, the group of motions of the plane is used to describe symmetry of planar figures, the affine group is used to prove theorems of plane geometry, and a counting lemma is applied to solve some difficult combinatorial problems. In Chapter 3 on rings, we construct finite fields, and then we use them to construct complete sets of orthogonal Latin squares. The last chapter is both a dessert and an appetizer. After a short discussion of vector spaces and dimension (which reinforces the categorical viewpoint of objects and morphisms), we show how modern algebra solves several classical problems of geometry. After giving the quadratic, cubic, and quartic formulas, we present an analogy between symmetry groups of figures and Galois groups, and we prove the theorem of Abel and Ruffini that there is no generalization of the classical formulas to higher degree polynomials. This discussion can serve as an introduction to Galois Theory.

Since Birkhoff and Mac Lane created this course half a century ago, there has been mild controversy about the order of presentation: should the exposition of groups precede that of rings, or should rings be done first (Birkhoff and Mac Lane do rings first). There are arguments on both sides and, after being a rings first man for a long time, I have come to believe that it is more reasonable to do groups first. The definition of group is very simple, and permutation groups offer an immediate nontrivial example. Many elementary properties of rings are much simpler once one has studied groups. Indeed, the very definition of a ring is more

palatable once one has seen groups. As a second example, the quotient group construction can be used to construct quotient rings (since rings are additive abelian groups and ideals are normal subgroups), but the quotient ring construction cannot be used directly in constructing quotient groups. Thus, discussing groups first is more efficient than the alternative. Finally, whenever I have taught rings first, I have found an initial confusion in the class about the relation of general rings to the particular ring $\mathbb{Z}$ of integers. There is a need to develop some arithmetic properties of $\mathbb{Z}$, and bouncing back and forth between commutative rings and $\mathbb{Z}$ creates an unnecessary difficulty for many students. In particular, students become unsure about which properties of $\mathbb{Z}$ may be assumed and which need proof. The organization here avoids this problem by separating these two subjects by group theory.

Giving the etymology of mathematical terms is rarely done. Let me explain, with an analogy, why I have included derivations of many terms. There are many variations of standard poker games and, in my poker group, the dealer announces the game of his choice by naming it. Now some names are better than others. For example, "Little Red" is a game in which one's smallest red card is wild; this is a good name because it reminds the players of its distinctive feature. On the other hand, "Aggravation" is not such a good name, for though it is, indeed, suggestive, the name does not distinguish this particular game from several others. Most terms in mathematics have been well chosen; there are more red names than aggravating ones. An example of a good name is *even* permutation, for a permutation is even if it is a product of an even number of transpositions. Another example of a good term is the *parallelogram law* describing vector addition. But many good names, clear when they were chosen, are now obscure because their roots are either in another language or in another discipline. The term *mathematics* is obscure only because most of us do not know that it comes from the classical Greek word meaning "to learn." The term *corollary* is doubly obscure; it comes from the Latin word meaning "flower," but what do flowers have to do with theorems? A plausible explanation is that it was common, in ancient Rome, to give flowers as gifts, and so a corollary is a gift bequeathed by a theorem. The term *theorem* comes from the Greek word meaning "to watch" or "to contemplate" (*theatre* has the same root); it was used by Euclid with its present meaning. The term *lemma* comes from the Greek word meaning "taken" or "received;" it is a statement that is taken for granted (for it has already been proved) in the course of proving a theorem. On the other hand, I am not too fond of the mathematical terms *normal* and *regular* for, in themselves, they convey no specific meaning. Since the etymology of terms often removes unnecessary obscurity, it is worthwhile (and interesting!) to do so.

It is a pleasure to thank Dan Grayson, Heini Halberstam, David G. Poole, Ed Reingold, and John Wetzel for their suggestions. I also thank the Hebrew University of Jerusalem for the hospitality given me as I completed my manuscript. I thank the several reviewers who carefully read my manuscript and made valuable suggestions. They are Daniel D. Anderson, University of Iowa; Michael J. J. Barry, Allegheny College; Brad Shelton, University of Oregon; Warren M. Sinnott, Ohio State University; and Dalton Tarwater, Texas Tech University. And I thank George Lobell, who persuaded me to develop and improve my first manuscript into the present text.

Joseph J. Rotman

CONTENTS

1

NUMBER THEORY

INDUCTION

There are many styles of proof, and mathematical induction is one of them. We begin by saying what mathematical induction is not. In the natural sciences, *inductive reasoning* is the assertion that a phenomenon that has always occurred in the past will always occur. Thus, one says that the sun will rise tomorrow morning because, from the dawn of time, the sun has risen every morning. This is not a legitimate kind of proof in mathematics, for although a phenomenon may have been observed to occur many times, it need not always occur. Consider, for example, the polynomial

$$f(n) = n^2 - n + 41.$$

A ***prime number*** is a positive integer $p \geq 2$ that cannot be factored into smaller positive integers; i.e., there do not exist positive integers $a < p$ and $b < p$ with $p = ab$. An integer $a \geq 2$ that is not prime is called ***composite***. The first few primes are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, ...

Consider the assertion that $f(n)$ is always prime. Evaluating $f(n)$ for $n = 1, 2, 3, \ldots, 40$ gives the numbers

41, 43, 47, 53, 61, 71, 83, 97, 113, 131,

151, 173, 197, 223, 251, 281, 313, 347, 383, 421,

461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971,

1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601.

It is not too difficult to show that every one of these numbers is prime. Inductive reasoning predicts that all the numbers of the form $f(n)$ are prime. But the next number, $f(41) = 1681$, is not prime, for $f(41) = 41^2 - 41 + 41 = 41^2$, which is, obviously, composite. Thus, inductive reasoning is not appropriate for mathematical proofs.

Here is an even more spectacular example (which I first saw in an article by W. Sierpinski). Recall that ***perfect squares*** are numbers of the form n^2, where n is an integer; the first few perfect squares are 1, 4, 9, 16, 25, 36, ... For each $n \geq 1$, consider the statement

$$S(n): \ 991n^2 + 1 \text{ is not a perfect square.}$$

The nth statement, $S(n)$, is true for many n; in fact, the smallest number n for which $S(n)$ is false is

$$\begin{aligned} n &= 12{,}055{,}735{,}790{,}331{,}359{,}447{,}442{,}538{,}767 \\ &\approx 1.2 \times 10^{29}. \end{aligned}$$

(The original equation is an example of *Pell's equation*—an equation of the form $x^2 = dy^2 + 1$, where d is ***squarefree***; that is, it is not divisible by any square larger than 1—and there is a way of calculating all possible solutions of it.) The most generous estimate of the age of the earth is 10 billion (10,000,000,000) years, or 3.65×10^{12} days, a number insignificant when compared to 1.2×10^{29}. If, starting from the very first day after creation, one verified statement $S(n)$ on the nth day, then there would be today as much evidence of the general truth of these statements as there is that the sun will rise tomorrow morning!

We have seen what (mathematical) induction is not; let us now discuss what induction is. Suppose one has determined that statements $S(n)$ are true for many values of n, and then guesses that all the $S(n)$ are true. Induction is a technique of proving that *all* the statements $S(n)$ are, indeed, true. For example, the reader may check that $2^n > n$ for many values of n, but is this inequality true for every value of n? We will soon prove, using induction, that this is so.

Our discussion is based on the following property of positive integers (usually called the *well ordering principle*).

Least Integer Axiom. There is a smallest integer in every nonempty collection C of positive integers.

Saying that C is *nonempty* merely means that there is at least one integer in the collection C. Although this axiom cannot be proved (it arises in analyzing what integers are), it is certainly plausible. Consider the following procedure. Check whether 1 belongs to C; if it does, then it is the smallest integer in C. Otherwise, check whether 2 belongs to C; if it does, then 2 is the smallest integer; if not, check 3. Continue this procedure until one bumps into C; this will occur eventually, for C is nonempty.

We remark that the least integer axiom holds for nonempty collections C of nonnegative integers as well. If C contains 0, then 0 is the smallest integer in

C; otherwise, C is actually a nonempty collection of positive integers, and the original least integer axiom now applies to C.

We begin by recasting the least integer axiom.

Theorem 1.1 (Least Criminal). *Let $S(1), S(2), S(3), \ldots, S(n), \ldots$ be statements, one for each $n \geq 1$. If some of these statements are false, then there is a first false statement.*

Proof. Let C be the collection of all those positive integers n for which $S(n)$ is false; by hypothesis, C is nonempty. The least integer axiom provides a smallest integer m in C, and $S(m)$ is the first false statement. •

This seemingly innocuous theorem is useful.

Theorem 1.2. *Every integer $n \geq 2$ is either a prime or a product of primes.*

Proof. Were this not so, there would be "criminals," that is, integers $n \geq 2$ neither prime nor products of primes; a least criminal m is the smallest such integer. Since m is not a prime, it is composite; there is thus a factorization $m = ab$ with $2 \leq a < m$ and $2 \leq b < m$. Since m is the least criminal, both a and b are "honest," i.e., each is either prime or a product of primes. Therefore, m is a product of primes, which is a contradiction. •

Theorem 1.3. *If $m \geq 2$ is a positive integer that is not divisible by any prime p with $p \leq \sqrt{m}$, then m is a prime.*

Proof.[1] If m is not prime, then $m = ab$, where $a < m$ and $b < m$ are positive integers. If $a > \sqrt{m}$ and $b > \sqrt{m}$, then $m = ab > \sqrt{m}\sqrt{m} = m$, a contradiction. Therefore, we may assume that $a \leq \sqrt{m}$. By Theorem 1.2, a is either a prime or a product of primes, and any (prime) divisor of a is also a divisor of m. Thus, if m is not prime, then it has a "small" prime divisor p; i.e., $p \leq \sqrt{m}$. The contrapositive says that if m has no small prime divisor, then m is prime. •

One can use Theorem 1.3 to see that the numbers $f(n) = n^2 - n + 41$, for $1 \leq n \leq 40$, are all prime. For example, consider $1447 = 38^2 - 38 + 41$. To check whether 1447 is prime, it suffices to check if 1447 is divisible by some prime p with $p \leq \sqrt{1447} \approx 38.04$; if 1447 is not divisible by some one of 2, 3, 5, ..., 37, then it is prime. There are 12 such primes, and one can now check that none of them is a divisor of 1447.

[1] The ***contrapositive*** of an implication "P implies Q" is the implication "not Q implies not P." For example, the contrapositive of "If a series Σa_n converges, then $\lim_{n\to\infty} a_n = 0$" is "If $\lim_{n\to\infty} a_n \neq 0$, then Σa_n diverges." If an implication is true, then so is its contrapositive; conversely, if the contrapositive is true, then so is the original implication. The strategy of this proof is to prove the contrapositive of the original implication. Although a statement and its contrapositive are logically equivalent, it is sometimes more convenient to prove the contrapositive. Proving the contrapositive is also called an ***indirect proof***, or a ***proof by contradiction***.

Mathematical induction is a version of least criminal that is more convenient to use. The key idea is just this. Imagine a stairway going up to the sky. If its first step is white and if the next step above a white step is also white, then all the steps of the stairway are white. (One can trace this idea back to Levi ben Gershon in 1321. There is an explicit description of induction, cited by Pascal, written by Francesco Maurolico in 1557.) For example, the statement "$2^n > n$ for all $n \geq 1$" can be regarded as an infinite sequence of statements (the stairway to the sky):

$$2^1 > 1;\ 2^2 > 2;\ 2^3 > 3;\ 2^4 > 4;\ 2^5 > 5;\ \ldots.$$

Certainly, $2^1 = 2 > 1$. Multiplying both sides by 2, we have $2^2 > 2 \times 1 = 2$; multiplying again gives $2^3 > 2 \times 2 > 3$; $2^4 > 2 \times 3 > 4$; ...; if $2^{100} > 100$, then $2^{101} = 2 \times 2^{100} > 2 \times 100 > 101$. There is nothing magic about the exponent 100; once we have reached any stair, we can climb up to the next one. This argument will be formalized in Theorem 1.5.

Theorem 1.4 (Mathematical Induction). *Given statements $S(n)$, one for each $n \geq 1$, suppose that*

(i) $S(1)$ *is true, and*
(ii) *if $S(n)$ is true, then $S(n + 1)$ is true.*

Then $S(n)$ is true for all $n \geq 1$.

Proof. We must show that the collection C of all those positive integers k for which the statement $S(k)$ is false is empty.

If, on the contrary, C is nonempty, then there is a least criminal $S(m)$. Since $S(1)$ is true, by (i), we must have $m \geq 2$. This implies that $m - 1 \geq 1$, and so there is a statement $S(m - 1)$ [there is no statement $S(0)$]. As $S(m)$ is the least criminal, $S(m - 1)$ must be honest; that is, $S(m - 1)$ is true. But (ii) says that $S(m) = S([m - 1] + 1)$ is true, and this is a contradiction. We conclude that C is empty and hence that all the statements are true. •

Let us now illustrate how to use (mathematical) induction.

Theorem 1.5. *$2^n > n$ for all $n \geq 1$.*

Proof. The nth statement $S(n)$ is

$$S(n):\ 2^n > n.$$

There are two steps required for induction.

Base step. The initial statement

$$S(1):\ 2^1 > 1$$

is true, for $2^1 = 2 > 1$.

Inductive step. If $S(n)$ were true, then $S(n + 1)$ would also be true; that is, using the ***inductive hypothesis*** $S(n)$, we must prove

$$S(n+1):\ 2^{n+1} > n+1.$$

If $2^n > n$ were true, then multiplying both sides of its inequality by 2 would give the valid inequality:

$$2^{n+1} = 2 \times 2^n > 2n.$$

Now $2n = n + n \geq n + 1$ (because $n \geq 1$), and hence $2^{n+1} > 2n \geq n + 1$, as desired. Having verified both the base step and the inductive step, we conclude that $2^n > n$ for all $n \geq 1$. •

Induction is plausible in the same sense that the least integer axiom is plausible. Suppose that $S(1)$, $S(2)$, $S(3)$, ... are statements with $S(n+1)$ true whenever $S(n)$ is true. If, in addition, $S(1)$ is true, then $S(2)$ is true; the truth of $S(2)$ now gives the truth of $S(3)$; the truth of $S(3)$ now gives the truth of $S(4)$; and so forth. Induction replaces the phrase *and so forth* by the inductive step; this guarantees, for every n, that there is no obstruction in the passage from any statement $S(n)$ to the next one $S(n+1)$.

Here are two comments before we give more illustrations of induction. First, one must verify both the base step and the inductive step; verification of only one of them is inadequate. For example, consider the statements $S(n)$: $n^2 = n$. The base step is true, but one cannot prove the inductive step (of course, these statements are mostly false). Another example is given by the statements $S(n)$: $n = n + 1$. It is easy to see that the inductive step is true: if $n = n + 1$, then adding 1 to both sides gives $n + 1 = (n + 1) + 1 = n + 2$, which is the next statement $S(n + 1)$. But the base step is false (of course, all these statements are false).

Second, when first seeing induction, many people suspect that the inductive step is circular reasoning: one is using $S(n)$, and this is what one wants to prove! A closer analysis shows that this is not at all what is happening. The inductive step, by itself, does not prove that $S(n + 1)$ is true. Rather, it says that *if* $S(n)$ were true, *then* one could prove that $S(n + 1)$ would also be true. In other words, the inductive step proves that the *implication* "If $S(n)$ is true, then $S(n + 1)$ is true" is correct. The truth of this implication is not the same thing as the truth of its conclusion. For example, consider the two statements: "Your grade on every exam is 100%" and "Your grade in the course is A." The implication "If all your exams are perfect, then you will get the highest grade for the course" is true. Unfortunately, this does not say that it is inevitable that your grade in the course will be A. Our discussion above gives a mathematical example: the implication "If $n = n + 1$, then $n + 1 = n + 2$" is correct, but the conclusion "$n + 1 = n + 2$" is false.

Theorem 1.6. $1 + 2 + \cdots + n = \frac{1}{2}n(n+1)$ *for every* $n \geq 1$.

Proof. The proof is by induction.

Base step. If $n = 1$, then the left side is 1 and the right side is $\frac{1}{2}1(1 + 1) = 1$, as desired.

Inductive step. It is always a good idea to write the $(n+1)$st statement $S(n+1)$ (so one can see what has to be proved). We must show that

$$1 + 2 + \cdots + n + (n+1) = \tfrac{1}{2}(n+1)(n+2).$$

By the inductive hypothesis, i.e., using $S(n)$, the left side is

$$[1 + 2 + \cdots + n] + (n+1) = \tfrac{1}{2}n(n+1) + (n+1),$$

and high school algebra shows that $\frac{1}{2}n(n+1) + (n+1) = \frac{1}{2}(n+1)(n+2)$. By induction,[2] the formula holds for all $n \geq 1$. •

There is a story told about the young Gauss. One of his teachers asked the students to add up all the numbers from 1 to 100, thereby hoping to get some time for other tasks. But Gauss quickly volunteered that the answer was 5050. Here is what he did (without induction). Let s denote the sum of all the numbers from 1 to 100: $s = 1 + 2 + \cdots + 99 + 100$. Of course, $s = 100 + 99 + \cdots + 2 + 1$. Arrange these nicely:

$$s = 1 + 2 + \cdots + 99 + 100$$
$$s = 100 + 99 + \cdots + 2 + 1,$$

add:

$$2s = 101 + 101 + \cdots + 101 + 101 \text{ (100 times)},$$

and solve: $s = \frac{1}{2}(100 \times 101) = 5050$. The same argument works for any number n in place of 100. Not only does this give a new proof of Theorem 1.6, it also shows how the formula could have been discovered.

Theorem 1.7. *Assuming the product rule for derivatives,* $D(fg) = (Df)g + f(Dg)$,

$$D(x^n) = nx^{n-1} \text{ for all } n \geq 1.$$

Proof. We proceed by induction.

Base step. If $n = 1$, then we ask whether $D(x) = x^0 = 1$. Now

$$D(f(x)) = \lim_{h\to 0}(1/h)[f(x+h) - f(x)].$$

When $f(x) = x$, therefore, $D(x) = \lim_{h\to 0}(1/h)[x + h - x] = \lim_{h\to 0} h/h = 1$.

Inductive step. We must prove that $D(x^{n+1}) = (n+1)x^n$, and we are allowed to use $D(x^n) = nx^{n-1}$. Since $x^{n+1} = x^n x$, the product rule gives

$$\begin{aligned} D(x^{n+1}) &= D(x^n x) = D(x^n)\,x + x^n D(x) \\ &= x(nx^{n-1}) + x^n 1 = (n+1)\,x^n. \end{aligned}$$

We conclude that $D(x^n) = nx^{n-1}$ is true for all $n \geq 1$. •

[2] *Induction*, having a Latin root meaning "to lead," came to mean "prevailing upon to do something" or "influencing." This is an apt name here, for the nth statement influences the $(n+1)$st one.

The base step of an induction may be an integer other than 1. For example, consider the statements

$$S(n):\ 2^n > n^2.$$

This is not true for small values of n: if $n = 2$ or 4, then there is equality, not inequality; if $n = 3$, the left side, 8, is smaller than the right side, 9. However, $S(5)$ is true, for $32 > 25$.

Theorem 1.8. *$2^n > n^2$ is true for all $n \geq 5$.*

Proof. We have just checked the base step $S(5)$. In proving

$$S(n+1):\ 2^{n+1} > (n+1)^2,$$

we are allowed to assume that $n \geq 5$ (actually, we will need only $n \geq 3$) as well as the inductive hypothesis. Multiply both sides of $2^n > n^2$ by 2 to get

$$2^{n+1} = 2 \times 2^n > 2n^2 = n^2 + n^2 = n^2 + nn.$$

Since $n \geq 5$, we have $n \geq 3$, and so

$$nn \geq 3n = 2n + n \geq 2n + 1.$$

Therefore,

$$2^{n+1} > n^2 + nn \geq n^2 + 2n + 1 = (n+1)^2. \quad \bullet$$

We have seen that the base step of an induction can begin at $n = 1$ or $n = 5$. Indeed, the base step of an induction can begin at any integer k; of course, the conclusion is that the statements are true for all $n \geq k$. Assuming that there is a statement $S(0)$, one may also start an induction with base step $n = 0$.

EXERCISES

1.1. Find a formula for $1 + 3 + 5 + \cdots + (2n - 1)$, and use mathematical induction to prove that your formula is correct.

Remark. Inductive reasoning is used in mathematics to help guess what might be true. Once a guess has been made, it must still be proved, perhaps using mathematical induction, perhaps by some other method.

1.2. For any $n \geq 0$ and any $r \neq 1$, prove that

$$1 + r + r^2 + r^3 + \cdots + r^n = (1 - r^{n+1})/(1 - r).$$

1.3. Show, for all $n \geq 1$, that 10^n leaves remainder 1 after dividing by 9. (*Hint*: This may be rephrased to say that there is an integer q_n with $10^n = 9q_n + 1$.)

1.4. Prove that $1^2 + 2^2 + \cdots + n^2 = n(n+1)(2n+1)/6$.

1.5. Prove that $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + \cdots + n)^2$.

1.6. Prove that $1^4 + 2^4 + \cdots + n^4 = n^5/5 + n^4/2 + n^3/3 - n/30$.

1.7. (i) Prove that $2^n > n^3$ for all $n \geq 10$.
(ii) Prove that $2^n > n^4$ for all $n \geq 17$.

1.8. Let $g_1(x), \ldots, g_n(x)$ be differentiable functions, and let $f(x)$ be their product: $f(x) = g_1(x) \cdots g_n(x)$. Prove that

$$Df(x) = \sum_{i=1}^{n} g_1(x) \cdots g_{i-1}(x) Dg_i(x) g_{i+1}(x) \cdots g_n(x).$$

1.9. Prove that $(1 + x)^n \geq 1 + nx$ if $1 + x > 0$.

1.10. Let T be a set of positive integers such that
(i) 1 is in T;
(ii) if all the *predecessors* of an integer n (i.e., all positive integers k with $k < n$) are in T, then n is in T.
Prove that T consists of all the positive integers.

1.11. ***(Second form of induction)***. Let $S(n)$ be a family of statements, one for each $n \geq 1$. Prove that if
(i) $S(1)$ is true, and
(ii) if $S(k)$ is true for all $k < n$, then $S(n)$ is true,
then $S(n)$ is true for all $n \geq 1$.

1.12. Use the second form of induction to give a new proof of Theorem 1.2: Every integer $n \geq 2$ is either a prime or a product of primes. (*Hint*: The base step is $n = 2$.)

BINOMIAL COEFFICIENTS

What is the pattern of the coefficients in the formulas for the powers $(1 + x)^n$ of the binomial $1 + x$? The first few such formulas are:

$$(1 + x)^1 = 1 + 1x$$
$$(1 + x)^2 = 1 + 2x + 1x^2$$
$$(1 + x)^3 = 1 + 3x + 3x^2 + 1x^3$$
$$(1 + x)^4 = 1 + 4x + 6x^2 + 4x^3 + 1x^4.$$

Figure 1.1, called ***Pascal's triangle*** [after B. Pascal (1623–1662)], displays the first few coefficients.

1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1

Figure 1.1

Figure 1.2, a picture from China in the year 1303, shows that the pattern of coefficients had been recognized long before Pascal.

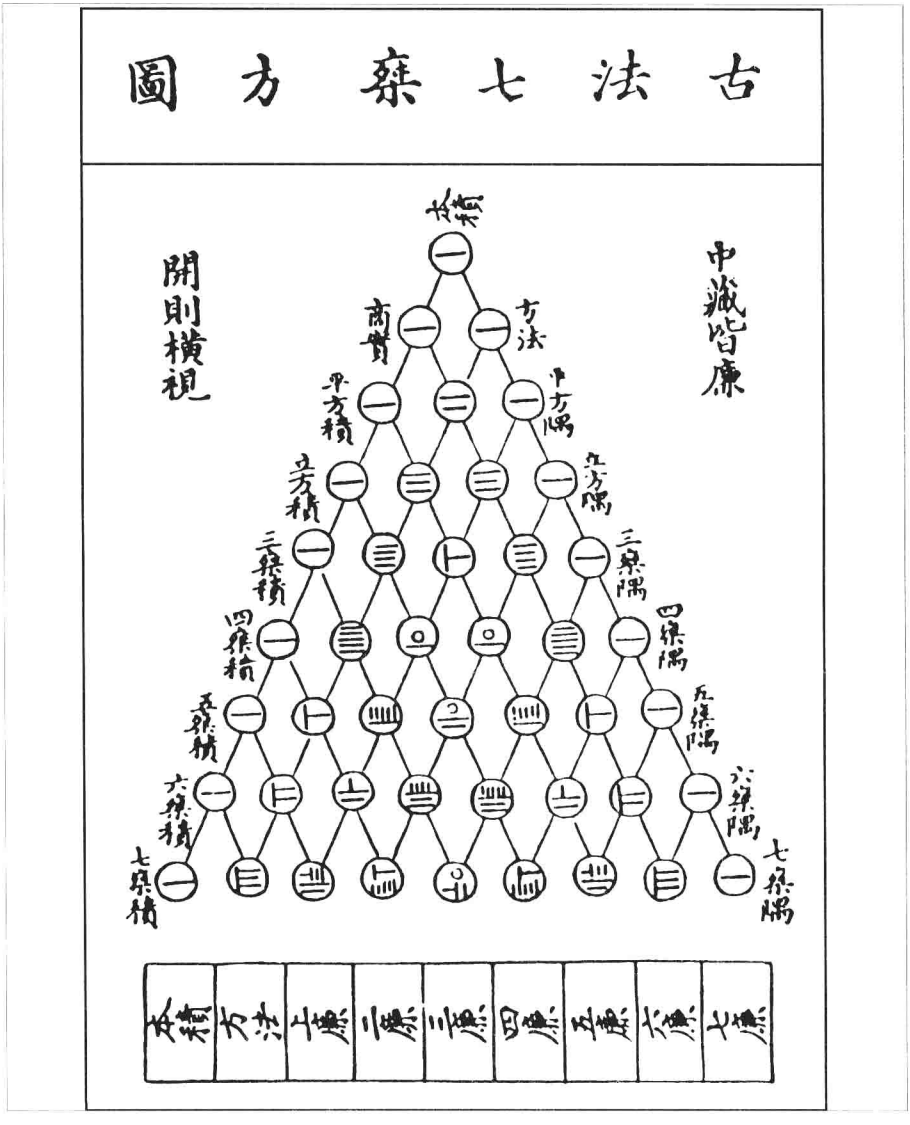


Figure 1.2