AMS / MAA | CLASSROOM RESOURCE MATERIALS VOL 7

A PRIMER of Abstract Mathematics

ROBERT B. ASH

MAA PRESS

An Imprint of the AMERICAN MATHEMATICAL SOCIETY

A Primer of Abstract Mathematics

Library of Congress Catalog Card Number 98-85593

ISBN 0-88385-708-1

Printed in the United States of America

Current Printing (last digit):
10 9 8 7 6 5 4 3 2 1

10.1090/clrm/007

A Primer of Abstract Mathematics

Robert B. Ash

Published by

THE MATHEMATICAL ASSOCIATION OF AMERICA

CLASSROOM RESOURCE MATERIALS

Classroom Resource Materials is intended to provide supplementary classroom material for students—laboratory exercises, projects, historical information, textbooks with unusual approaches for presenting mathematical ideas, career information, etc.

101 Careers in Mathematics, edited by Andrew Sterrett
Calculus Mysteries and Thrillers, R. Grant Woods
Combinatorics: A Problem Oriented Approach, Daniel A. Marcus
Elementary Mathematical Models, Dan Kalman
Interdisciplinary Lively Application Projects, edited by Chris Arney
Laboratory Experiences in Group Theory, Ellen Maycock Parker
Learn from the Masters, Frank Swetz, John Fauvel, Otto Bekken, Bengt Johansson, and Victor Katz
Mathematical Modeling for the Environment, Charles Hadlock
A Primer of Abstract Mathematics, Robert B. Ash
Proofs Without Words, Roger B. Nelsen
A Radical Approach to Real Analysis, David M. Bressoud
She Does Math!, edited by Marla Parker

MAA Service Center
P. O. Box 91112
Washington, DC 20090-1112
1-800-331-1622 fax: 1-301-206-9789

Preface

The purpose of this book is to prepare you to cope with abstract mathematics. The intended audience consists of: prospective math majors; those taking or intending to take a first course in abstract algebra who feel the need to strengthen their background; and graduate students (and possibly some undergraduates) in applied fields who need some experience in dealing with abstract mathematical ideas. If you have studied calculus, you have had some practice working with common functions and doing computations. If you have taken further courses with an applied flavor, such as differential equations and matrix algebra, you have probably begun to appreciate mathematical structure and reasoning. If you have taken a course in discrete mathematics, you may have some experience in writing proofs. How much of this is sufficient background for the present text? I don't know; it will depend on the individual student. My suggestion would be that if you have taken some math courses, enjoyed them and done well, give it a try.

Upon completing the book, you should be ready to handle a first course in abstract algebra. (It is also useful to prepare for a first course in abstract analysis, and one possible source is *Real Variables With Basic Metric Space Topology* by Robert B. Ash, IEEE Press, 1993. This basic analysis text covers the course itself as well as the preparation.)

In studying any area of mathematics, there are, in my view, three essential factors, in order of importance:

1. Learning to think intuitively about the subject;
2. Expressing ideas clearly and cogently using ordinary English;
3. Writing formal proofs.

Abstract language is used by mathematicians for precision and economy in statements and proofs, so it is certainly involved in item 3 above. But abstraction can interfere with the learning process, at all levels, so for best results in items 1 and 2, we should use abstract language sparingly. We are pulled in opposite directions and must compromise. I will try to be as informal as I can, but at some point we must confront the beast (i.e., an abstract theorem and its proof). I think you'll find that if you understand the intuition behind a mathematical statement or argument, you will have a much easier time finding your way through it.

I've attempted to come up with a selection of topics that will help make you very comfortable when you begin to study abstract algebra. Here is a summary:

1. Logic and Foundations. Basic logic and standard methods of proof; sets, functions and relations, especially partial orderings and equivalence relations.

2. Counting. Finite sets and standard methods of counting (permutations and combinations); countable and uncountable sets; proof that the rational numbers are countable but the real numbers are uncountable.

3. Elementary Number Theory. Some basic properties of the integers, including the Euclidean algorithm, congruence modulo m, simple diophantine equations, the Euler φ function, and the Möbius Inversion Formula.

4. Some Highly Informal Set Theory. Cardinal numbers and their arithmetic; well-ordering and its applications, including Zorn's Lemma.

5. Linear Algebra. Finite-dimensional vector spaces, along with linear transformations and their representation by matrices.

6. Theory of Linear Operators. Jordan Canonical Form; minimal and characteristic polynomials; adjoints; normal operators.

A single chapter on a subject such as number theory does not replace a full course, and if you find a particular subject interesting, I would urge you to pursue the area further. The more mathematics you study, the more skillful you will become at it.

Another purpose of the book is to provide one possible model for how to write mathematics for an audience with limited experience in formalism and abstraction. I try to keep proofs short and as informal as possible, and to use concrete examples which illustrate all the features of the general case. When a formal development would take too long (notably in set theory), I try to replace the sequence of abstract definitions and theorems by a consistent thought process. This makes it possible to give an intuitive development of some major results. In the last chapter on linear operators, you are given a powerful engine, the Jordan Canonical Form. The proof of existence is difficult and should probably be skipped on first reading. But using the Jordan form right from the start simplifies the development considerably, and this should contribute to your understanding of linear algebra.

Each section has a moderate number of exercises, with solutions given at the end of the book. Doing most of them will help you master the material, without (I hope) consuming too much time.

The book may be used as a text for a course in learning how to think mathematically. The duration of the course (one semester, one quarter, two quarters) will depend on the background of the students. Chapter 3, Chapter 4, and Chapters 5–6 are almost independent. (Before studying Chapter 5, it is probably useful to look at the description of various algebraic structures at the beginning of Section 3.3 and the definition of a vector space at the end of Section 4.2.) A shorter course can be constructed by choosing one or two of these options after covering Chapters 1 and 2.

We are doing theoretical, abstract mathematics, and students in applied fields may wonder where the applications are. But a computer scientist needs to know some elementary number theory in order to understand public key cryptography. An electrical engineer might want to study basic set theory in order to cope with abstract algebra and thereby learn about error-correcting codes. A statistician needs to know some theoretical linear algebra (projections, diagonalization of symmetric matrices, quadratic forms) in order to work with the multivariate normal distribution. There is potentially a large audience for abstract mathematics, and to reach this audience it is not necessary for us to teach detailed physical and engineering applications. The physics and engineering departments are quite capable of doing this. It is certainly useful to suggest possible applications, and as an illustration, I have included an appendix giving a typical application of linear algebra. But it is essential that we write in an accessible and congenial style, and give informal or heuristic arguments when appropriate.

Some acknowledgments: I got the idea of doing an intuitive development of set theory after seeing an informal discussion of the Maximum Principle in *Topology, A First Course* by James R. Munkres, Prentice-Hall 1975. I thank Ed Merkes for many helpful suggestions to improve the exposition, Ken Ross and Andy Sterrett for their encouragement and advice, and my wife Carol Ash for many insights on the teaching of combinatorics and linear algebra.

A typical reader of this text is likely to be motivated by a need to deal with formal mathematics in his or her professional career. But I hope that in addition there will be some readers who will simply take pleasure in a mathematical journey toward a high level of sophistication. There are many who would enjoy this trip, just as there are many who might enjoy listening to a symphony with a clear melodic line.

Robert B. Ash

Contents

Appendix

An Application Of Linear Algebra

Virtually every branch of science uses linear algebra. Here is an application that is of interest in many fields. A *finite Markov chain* is a system with *states* $s_1, \dots, s_r$ and *transition probabilities* p_{ij}, $i, j = 1, \dots, r$. Starting in an initial state at time $t = 0$, the system moves from one state to another at subsequent times $t = 1, 2, \dots$. If the system is in state i at a given time, the probability that it will move to state j at the next transition is p_{ij}. (We allow $j = i$, so that p_{ii} can be greater than zero.)

The matrix A with entries p_{ij} is called the *transition matrix* of the chain. It is an example of a *stochastic matrix*: the entries are nonnegative and the sum across each row is 1.

If we start in state i at $t = 0$, what is the probability $p_{ij}^{(2)}$ that we will be in state j after *two* transitions? One way this can happen is to move to state k at $t = 1$ and then move from state k to state j at time $t = 2$. The probability that this will occur is $p_{ik}p_{kj}$. But k can be any integer from 1 to r, and we must add all of the corresponding probabilities. The result is

$$p_{ij}^{(2)} = \sum_{k=1}^{r} p_{ik}p_{kj},$$

which is the ij entry of the matrix A^2.

Thus the entries of A^2 are the two-step transition probabilities. Similarly, we can consider three-step transition probabilities $p_{ij}^{(3)}$. If we start in s_i at $t = 0$, one way of arriving at s_j at $t = 3$ is to be in s_k at $t = 2$ and move from s_k to s_j at $t = 3$. This event has probability $p_{ik}^{(2)}p_{kj}$, and consequently

$$p_{ij}^{(3)} = \sum_{k=1}^{r} p_{ik}^{(2)}p_{kj},$$

the ij entry of $A^2A = A^3$.

An induction argument shows that if $p_{ij}^{(n)}$ is the probability, starting in s_i, of being in s_j n steps later, then $p_{ij}^{(n)}$ is the ij entry of A^n. Thus to compute n-step transition probabilities, we must calculate the nth power of the transition matrix A. This is quite a tedious chore for large n. But if A is diagonalizable (in particular, if A has distinct eigenvalues), and the eigenvalues and eigenvectors of A are found, then all powers of A can be computed efficiently, as follows.

Let P be a nonsingular matrix such that $P^{-1}AP = D$, a diagonal matrix whose main diagonal entries are the eigenvalues λ_i $(i = 1, \dots, r)$ of A. Then $A = PDP^{-1}$, and if we begin to compute the powers of A, a pattern emerges quickly:

$$A^2 = AA = PDP^{-1}PDP^{-1} = PD^2P^{-1},$$
$$A^3 = A^2A = PD^2P^{-1}PDP^{-1} = PD^3P^{-1},$$

and by induction,

$$A^n = PD^nP^{-1}.$$

But since D is diagonal, so is D^n, and the main diagonal entries of D^n are λ_i^n, $i = 1, \dots, r$. Once the eigenvalues and eigenvectors have been found, the matrix P can be taken to have eigenvectors as columns. The computation of A^n has been reduced to finding the nth powers of the λ_i, followed by a matrix inversion and two matrix multiplications, one of which is easy (because D^n is diagonal).

Solutions to Problems

Section 1.1

1.

A	B	$A \vee B$	$\neg(A \vee B)$	$\neg A$	$\neg B$	$(\neg A) \wedge (\neg B)$
T	T	T	F	F	F	F
T	F	T	F	F	T	F
F	T	T	F	T	F	F
F	F	F	T	T	T	T

2. To prove the first law, note that the left side is true iff $A_1 \wedge \cdots \wedge A_n$ is false, which happens iff at least one A_i is false, i.e., at least one $(\neg A_i)$ is true, equivalently, the right side is true. For the second law, note that the left side is true iff $A_1 \vee \cdots \vee A_n$ is false, which happens iff all A_i are false, i.e., all $(\neg A_i)$ are true, equivalently, the right side is true.

3.

A	B	$A \Rightarrow B$	$\neg A$	$(\neg A) \vee B$
T	T	T	F	T
T	F	F	F	F
F	T	T	T	T
F	F	T	T	T

4.

A	$\neg A$	$A \vee (\neg A)$	$A \wedge (\neg A)$
T	F	T	F
F	T	T	F

5. The left side is true iff A and (either B or C) are true. The right side is true iff either (A and B) or (A and C) is true, in other words, A is true in conjunction with either B or C. Thus the two sides have the same truth table. (If you are not comfortable with this reasoning, construct the complete truth tables for $A \wedge (B \vee C)$ and $(A \wedge B) \vee (A \wedge C)$, and verify that they are identical.)

6. The left side is true iff either A or (B and C) is true. The right side is true iff both (A or B) and (A or C) are true. This will happen if A is true, but if A is false, both B and C must be true (a proof by cases; see Section 1.3). Thus the right side is true iff either A or (B and C) is true. As in Problem 5, this can be verified by a truth table.

7. Going from Problem 5 to Problem 6 gives a concrete example with the essential features of the general case, so let's do it this way rather than use messy formal notation. Having established the result of Problem 5, take the negation of both sides, using the DeMorgan Laws. We get

$$\begin{aligned}\neg\big[A\wedge(B\vee C)\big] &\Leftrightarrow \neg\big[(A\wedge B)\vee(A\wedge C)\big]\\ \big[(\neg A)\vee\neg(B\vee C)\big] &\Leftrightarrow \Big(\big[\neg(A\wedge B)\big]\wedge\big[\neg(A\wedge C)\big]\Big)\\ \Big[(\neg A)\vee\big((\neg B)\wedge(\neg C)\big)\Big] &\Leftrightarrow \Big(\big[(\neg A)\vee(\neg B)\big]\wedge\big[(\neg A)\vee(\neg C)\big]\Big).\end{aligned}$$

This is the result of Problem 6, except that each proposition A, B, C is replaced by its negation. But A, B, and C are *arbitrary* propositions, which is a key point; as A ranges over all possible propositions, so does $\neg A$. (A similar but perhaps more familiar statement is that if x ranges over all real numbers, so does $-x$; if you want $-x$ to equal y, take $x = -y$). Thus the result of Problem 6 holds in general. Notice also that if a tautology T appears in the original statement, taking the negation changes it to F, and similarly a contradiction F is changed to T.

Section 1.2

1. $\forall x\,\exists N\ (N > x)$

2. $\exists x\,\forall N\ (N \le x)$, which says that there is a real number x that is at least as big as every integer (false!).

Section 1.3

1. True for $n = 1$, since $1(2)/2 = 1$. If true for n, then

$$\begin{aligned}1+2+\cdots+n &= n(n+1)/2 \qquad \text{by the induction hypothesis}\\ n+1 &= n+1 \qquad \text{(an identity), so}\\ 1+2+\cdots+n+1) &= \big[n(n+1)/2\big]+(n+1) = (n+1)\big[(n/2)+1)\big]\\ &= (n+1)(n+2)/2.\end{aligned}$$

Thus the statement is true for $n{+}1$, and therefore the result holds for all n, by mathematical induction.

2. True for $n = 1$, since $2^{2(1)} - 1 = 4 - 1 = 3$. If $2^{2n} - 1$ is divisible by 3, consider

$$2^{2(n+1)} - 1 = 2^{(2n+2)} - 1 = (4)2^{2n} - 1 = (3)2^{2n} + (2^{2n} - 1).$$

By the induction hypothesis, $2^{2n} - 1$ is divisible by 3, and it follows that $2^{2(n+1)} - 1$ is the sum of two numbers divisible by 3, and consequently is divisible by 3. The induction argument is therefore complete.

3. True for $n = 1$, since $11^1 - 4^1 = 7$. If $11^n - 4^n$ is divisible by 7, then

$$11^{n+1} - 4^{n+1} = 11(11^n) - 4(4^n) = 11(11^n - 4^n) + (11 - 4)4^n,$$

which (using the induction hypothesis) is the sum of two numbers divisible by 7. The result follows.

4. True for $n = 1$, since $1^2 = 1(2)(3)/6$. If true for n, then by the induction hypothesis,

$$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= (n+1)\left(\frac{2n^2+n}{6} + n + 1\right) && \text{by factoring} \\ &= \frac{(n+1)(2n^2+7n+6)}{6} && \text{by algebra} \\ &= \frac{(n+1)(n+2)(2n+3)}{6} && \text{by more algebra.} \end{aligned}$$

Since $2n + 3 = 2(n + 1) + 1$, the induction step is proved.

5. The assertion is true for a postage of $n = 35$ cents, since we can pay with seven 5-cent stamps. If the result holds for a postage of n cents ($n \geq 35$), consider a postage of $n + 1$. In case 1, a postage of n can be paid with all 5's, and it takes at least seven of them since $n \geq 35$. If we replace seven 5's by four 9's, we have paid for $n + 1$ using only 5's and 9's. In case 2, postage n is paid using at least one 9. To pay for n+1 in this case, replace the 9 by two 5's, and again we have paid for $n + 1$ using only 5's and 9's. This completes the induction step.

Section 1.4

1. We have $x \in (\bigcap_i A_i)^c$ iff $x \notin \bigcap_i A_i$ iff it is not the case that x belongs to A_i for all i iff for at least one i, $x \notin A_i$ iff $x \in \bigcup_i (A_i^c)$.

2. We have $x \in A \cup (\bigcap_i B_i)$ iff $x \in A$ or $x \in B_i$ for all i iff for all i, $x \in A$ or $x \in B_i$ iff for all i, ($x \in A$ or $x \in B_i$) iff $x \in \bigcap_i (A \cup B_i)$.

3. We must show that A has no members. But if $x \in A$ then by hypothesis, x belongs to the empty set, which is impossible.

4. If $i \neq j$, then $B_i \cap B_j \subseteq A_i \cap A_j = \varphi$. By Problem 3, $B_i \cap B_j = \varphi$.

5. No. For example, let $A = \{1,2,3,4\}$, $B = \{1,2\}$, $C = \{1,4\}$. Then $A \cup B = A \cup C = A$, but $B \neq C$.

6. No. For example, let $A = \{1,2,3,4\}$, $B = \{1,2,5\}$. Then $A \cup (B \setminus A) = \{1,2,3,4\} \cup \{5\} \neq B$.

7. $A \cup (B \setminus A) = A \cup B$. For if $x \in A \cup (B \setminus A)$, then x belongs to A or x belongs to B but not A, so that $x \in A \cup B$. Conversely, if $x \in A \cup B$, then it is convenient to do a proof by cases:

Case 1. $x \in A$; then certainly $x \in A \cup (B \setminus A)$.
Case 2. $x \notin A$; then, since $x \in A \cup B$, we must have $x \in B$, so that $x \in B \setminus A$.

(A Venn diagram may be useful in visualizing the result.)

8. The Distributive Law provides a concrete example with all the features of the general case. In the original Distributive Law $A \cap (\bigcup_i B_i) = \bigcup_i (A \cap B_i)$, take the complement of both sides and use the DeMorgan Laws to obtain $A^c \cup (\bigcap_i B_i^c) = \bigcap_i (A^c \cup B_i^c)$. Since the sets A and B_i are arbitrary, we may replace A^c by A and B_i^c by B_i to obtain the second Distributive Law of Problem 2. Notice that if Ω appears in the original identity, taking the complement changes Ω to $\varnothing$. Similarly, $\varnothing$ is replaced by Ω.

9. $A \subseteq B$ iff $(x \in A \Rightarrow x \in B)$ iff $\big((x \in A) \Leftrightarrow (x \in A \text{ and } x \in B)\big)$ iff $\big((x \in B) \Leftrightarrow (x \in A \text{ or } x \in B)\big)$, and the result follows.

Section 1.5

1. If $x^3 = y^3$, we may take cube roots to conclude that $x = y$, so f is injective. Any real number y has a real cube root $x = y^{1/3}$, so f is surjective.

2. f is neither injective nor surjective, by an analysis similiar to that in the text for $f(x) = x^2$.

3. $h(x) = g\big(f(x)\big)$, where $f(x) = x^2 + 1$ and $g(y) = y^{10}$.

4. If A consists of a single point then f is injective, and if B consists of a single point (necessarily c), then f is surjective. These are the only circumstances.

5. If $A = \{a_1, \ldots, a_m\}$, then B has at least m distinct points $f(a_1), \ldots, f(a_m)$, so $m \leq n$.

6. If $B = \{b_1, \ldots, b_n\}$ then for each i there is a point $a_i \in A$ such that $f(a_i) = b_i$. The elements a_i are distinct, for otherwise the function f would map the same point to two different images in B, which is impossible. Thus A has at least n distinct points, so that $m \geq n$.

7. In view of (1.5.5(a)), we need only prove that $f^{-1}\big[f(C)\big]$ is a subset of C. If $x \in f^{-1}\big[f(C)\big]$, then $f(x) \in f(C)$, so that $f(x) = f(y)$ for some $y \in C$. Since f is injective we have $x = y$, and therefore $x \in C$.

8. In view of (1.5.5(b)), we need only prove that D is a subset of $f\big[f^{-1}(D)\big]$. If $y \in D$, then since f is surjective we have $y = f(x)$ for some $x \in A$. But then $f(x) = y \in D$, so $y = f(x)$ with $x \in f^{-1}(D)$; that is, $y \in f\big[f^{-1}(D)\big]$.

9. In view of (1.5.5(d)), we need only prove that the intersection of the $f(A_i)$ is a subset of $f(\bigcap_i A_i)$. If $y \in \bigcap_i f(A_i)$, then for each i we have $y = f(x_i)$ for some $x_i \in A_i$. Since f is injective, all the x_i are equal (to x, say); hence $y = f(x)$ with $x \in \bigcap_i A_i$, and the result follows.

Section 1.6

1. R is reflexive (W and W certainly begin with the same letter), symmetric (if W and V begin with the same letter, so do V and W) and transitive (if W and V begin with the same letter, and V and U begin with the same letter, then W and U begin with the same letter). If W begins with a, the equivalence class of W consists of all words beginning with a. Thus there are 26 equivalence classes, one for each possible letter.

2. If aRb, then bRa by symmetry, so $a = b$ by antisymmetry. Conversely, if $a = b$, then aRb by reflexivity. Thus aRb if and only if $a = b$.

3. The argument of Problem 2 uses reflexivity, which is no longer assumed.

4. Let $A = \{1, 2, 3\}$ and let R consist of the ordered pairs $(1, 1)$ and $(2, 2)$. Then R is symmetric and antisymmetric, but $(3, 3) \notin R$, so that R is not equality.

5. If R is relation that is reflexive, symmetric and antisymmetric, then R is the equality relation. The argument of Problem 2 goes through in this case.

6. No. If a and b are maximal and R is total, then aRb or bRa. If, say, aRb, then since a is maximal we have $a = b$.

7. The inclusion relation is reflexive ($A \subseteq A$), antisymmetric (if $A \subseteq B$ and $B \subseteq A$ then $A = B$), and transitive (if $A \subseteq B$ and $B \subseteq C$ then $A \subseteq C$). The relation is not total (unless W has at most one element). For example, if $A = \{1, 2, 3\}$ and $B = \{2, 3, 4\}$ then A is not a subset of B and B is not a subset of A.

8. (a) If $x \in A_j$, then certainly $x \in A_i$ for at least one i, so $A_j \subseteq B$.

(b) We must show that if each $A_i \subseteq C$, then $\bigcup_i A_i \subseteq C$. But this follows directly from the definition of union.

9. (a) If $x \in B$, then x belongs to every A_i, so $B \subseteq A_i$ for all i.

(b) We must show that if $C \subseteq A_i$ for every i, then $C \subseteq \bigcap_i A_i$. But this follows directly from the definition of intersection.

Section 2.1

1. A bijective function from A to A corresponds to a permutation of A, and by (2.1.2), the total number of permutations is $n!$

2. We have n choices for $f(a)$, where a ranges over the k elements of A. The total number of functions is $(n)(n)\cdots(n) = n^k$.

3. Once an element $f(a) \in B$ is chosen, it cannot be used again. Therefore the number of injective functions is

$$(n)(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}.$$

4. By Problem 2, the number of functions from A to $\{0,1\}$ is 2^n.

5. Suppose that 1 and 4 go to R_1, 5 to R_2, and 2 and 3 to R_3. This corresponds to the sequence $R_1R_3R_3R_1R_2$. In general, we are counting generalized permutations of R_1, R_2, and R_3 in which R_1 occurs twice, R_2 once and R_3 twice. The result is $\frac{5!}{2!1!2!} = 30$.

6. By the formula for generalized permutations, the number of assignments is

$$\frac{n!}{k_1!\cdots k_r!}.$$

7. The assignment of Problem 5 yields the partition $\{1,4\}$, $\{5\}$, $\{2,3\}$. But the assignment in which 1 and 4 go to R_3, 5 to R_2, and 2 and 3 to R_1, yields the same partition, since we get the same collection of disjoint subsets whose union is $\{1,2,3,4,5\}$. Because there are two rooms of the same size, the computation of Problem 5 overcounts by a factor of 2, and the correct answer is $30/2 = 15$.

8. Suppose we have two subsets S_1 and S_2 of size 5, four subsets T_1, T_2, T_3, and T_4 of size 3, and one subset U_1 of size 2. This can be converted into a room assignment by permuting S_1 and S_2, and then permuting T_1, T_2, T_3, and T_4. (There is only one permutation of the single symbol U_1.) For example, $S_2S_1T_3T_4T_2T_1$ corresponds to sending the people in S_2 to room R_1, the people in S_1 to R_2, the people in T_3 to R_3, T_4 to R_4, T_2 to R_5, and T_1 to R_6. Thus the number of partitions times $2!4!1!$ is the number of room assignments, so the correction factor is $2!4!1!$.

9. By the same reasoning as in Problem 8, we obtain

$$\frac{n!}{k_1!\cdots k_r!t_1!\cdots t_m!}.$$

10. We are counting the number of nonnegative integer solutions of $x_1 + x_2 + x_3 + x_4 + x_5 = 10$, which is

$$\binom{10+5-1}{10}.$$

Section 2.2

1. $(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k}$, and the result follows.

2. $(-1+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k}$, and the result follows.

3. By Problem 4 of Section 2.1, there are 2^n subsets of a set A with n elements. But by (2.1.4), there are $\binom{n}{k}$ k-element subsets of A. Sum from $k = 0$ to n to obtain the desired identity.

4. The desired identity is

$$\frac{n!}{k!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!}.$$

Multiply by $k!(n-k)!$ to obtain $n! = k(n-1)! + (n-k)(n-1)! = n(n-1)!$, which is valid. The steps of this argument may be reversed to establish the original identity.

5. There are $\binom{n}{k}$ k-element subsets of $\{1, 2, \ldots, n\}$. Consider any fixed element of $\{1, 2, \ldots, n\}$, say n. If S is a k-element subset, there are two possibilities:

Case 1. $n \in S$. Then there are $k - 1$ other elements of S, to be chosen from the integers $1, 2, \ldots, n-1$. The number of such subsets is $\binom{n-1}{k-1}$.

Case 2. $n \notin S$. Then S is a k-element subset of $\{1, 2, \ldots, n-1\}$, and the number of such subsets is $\binom{n-1}{k}$.

Now any k-element subset falls into one of the two cases (but not both), and therefore the total number of k-element subsets is the sum of the number of subsets in case 1 plus the number in case 2. The result follows.

6. The sum of all the coefficients in the multinomial expansion of $(a_1 + \cdots + a_r)^n$ may be obtained by setting all $a_i = 1$ (cf. Problem 1). The sum of the coefficients is therefore r^n. When $r = 3$ and $n = 4$, we get $3^4 = 81$, as expected.

Section 2.3

1. We must place i in position i, and the remaining $n-1$ integers $1, 2, \ldots, i-1, i+1, \ldots, n$ can be permuted arbitrarily. Thus $N(A_i)$ is the number of permutations of a set with $n-1$ members, which is $(n-1)!$

2. We must place $i_1, \ldots, i_k$ in their natural positions, and we can then permute the remaining $n-k$ integers arbitrarily. There are $(n-k)!$ ways of doing this.

3. The number $d(n)$ of derangements is the total number of permutations minus the number of permutations in which at least one integer stands in its natural position. Thus $d(n) = n! - N(A_1 \cup \cdots \cup A_n)$, and we compute $N(A_1 \cup \cdots \cup A_n)$ with the aid of PIE_n. There are $\binom{n}{i}$ terms involving intersections of i of the sets A_j. Terms involving an even number of intersections appear with a minus sign, and by Problem 2, each term is $(n-i)!$ in absolute value. Therefore

$$d(n) = n! - \sum_{i=1}^{n}(-1)^{i-1}\binom{n}{i}(n-i)! = \sum_{i=0}^{n}(-1)^{i}\binom{n}{i}(n-i)!.$$

The alternative expression for $d(n)$ follows from the identity

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}.$$

4. By Problem 3,

$$\left|d(n) - \frac{n!}{e}\right| = n!\left|\sum_{i=n+1}^{\infty}\frac{(-1)^i}{i!}\right|.$$

Now an alternating series whose terms decrease in magnitude must be less than the first term in absolute value, so

$$\left|d(n) - \frac{n!}{e}\right| < \frac{n!}{(n+1)!} = \frac{1}{n+1} \leq \frac{1}{2},$$

and the result follows.

5. $N(A_i)$ is the number of functions from a set with k elements to a set with $n-1$ elements (one of the original n elements, namely i, is excluded). By Problem 2 of Section 2.1, $N(A_i) = (n-1)^k$.

6. We are counting the number of functions from a set with k elements to a set with $n-r$ elements (r of the original n elements are excluded). The result is $(n-r)^k$.

7. The number $S(k,n)$ of surjective functions is the total number of functions minus the number of functions f such that some integer $i \in \{1, \ldots, n\}$ is missing from the image of f. Thus $S(k,n) = n^k - N(A_1 \cup \cdots \cup A_n)$, and we compute $N(A_1 \cup \cdots \cup A_n)$ with the aid of PIE_n. There are $\binom{n}{i}$ terms involving intersections of i of the sets. Terms involving an even number of intersections appear with a minus sign, and by Problem 6, each term is $(n-i)^k$ in absolute value. Therefore

$$\begin{aligned} S(k,n) &= n^k - \sum_{i=1}^{n}(-1)^{i-1}\binom{n}{i}(n-i)^k \\ &= \sum_{i=0}^{n}(-1)^i\binom{n}{i}(n-i)^k. \end{aligned}$$

8. A partition of $\{1,\ldots,8\}$ into four disjoint nonempty subsets gives rise to $4! = 24$ surjective functions; there are 4 possible choices for $f(1)$ $(= f(2))$, and then 3 possible choices for $f(3)$ $(= f(4) = f(5))$, and so on. For example, we might choose $f(1) = f(2) = 3$, $f(3) = f(4) = f(5) = 1$, $f(6) = 4$, $f(7) = f(8) = 2$. The correct statement is that the number of surjective functions from $\{1,\ldots,8\}$ to $\{1,2,3,4\}$ is $4!$ times the number of partitions of $\{1,\ldots,8\}$ into four disjoint nonempty subsets.

9. $S(k,n) = n!P(k,n)$. The reasoning is the same as in the concrete example of Problem 8.

10. $S(k,n) = 3^4 - \binom{3}{1}2^4 + \binom{3}{2}1^4 - \binom{3}{3}0^4 = 81 - 48 + 3 - 0 = 36$

$$P(k,n) = \frac{S(k,n)}{n!} = \frac{36}{3!} = 6.$$

The partitions are

$$\begin{gathered} \{1,2\},\{3\},\{4\} \\ \{1,3\},\{2\},\{4\} \\ \{1,4\},\{2\},\{3\} \\ \{2,3\},\{1\},\{4\} \\ \{2,4\},\{1\},\{3\} \\ \{3,4\},\{1\},\{2\}. \end{gathered}$$

Section 2.4

1. There is no way to guarantee that the number r selected is rational.

2. We give a proof by mathematical induction. The $n = 2$ case follows from the diagonal scheme that we used to count the rationals. If $A_1 = \{a_1, a_2, \ldots\}$ and $A_2 = \{b_1, b_2, \ldots\}$, we simply replace the rational number i/j by the ordered pair (a_i, b_j). If we have proved that the Cartesian product of $n-1$ countable sets is countable, then the result for n sets follows because an ordered n-tuple $(x_1, x_2, \ldots, x_n)$ can be regarded as an ordered pair $\big((x_1, \ldots, x_{n-1}), x_n\big)$. The result then follows from the induction hypothesis and the $n = 2$ case.

3. Let

$$x = \frac{r_1 + r_2}{2};$$

then $r_1 < x < r_2$, so x must occur after r_1 but before r_2 on the list. This is a contradiction, since we are given that r_1 is followed immediately by r_2. Alternatively, simply observe that there is no smallest positive rational, so the list cannot even get started.

4. Let a_1 be any element of A, and set $f(1) = a_1$. Since A is infinite, it must contain an element $a_2 \neq a_1$; set $f(2) = a_2$. Since A is infinite, it must contain an element a_3 with $a_3 \neq a_1$ and $a_3 \neq a_2$; set $f(3) = a_3$. We continue in this fashion, performing an inductive procedure (compare the proof of (1.6.5)). At step n we have distinct points $a_1, \ldots, a_n$, with $f(i) = a_i$, $1 \leq i \leq n$. If we define $f : Z^+ \to A$ by $f(n) = a_n$, $n = 1, 2, \ldots$, then f is a one-to-one mapping of Z^+ into A.

Section 3.1

1. By (i), d divides both a and b, so by (ii), d divides e. A symmetrical argument shows that e divides d. Thus $|d| \leq |e|$ and $|e| \leq |d|$, so $|d| = |e|$.

2. If e is any positive integer that divides both a and b, then e divides d by definition of d, so $e \leq |d|$, and the result follows.

3.

i	q_i	s_i	t_i	r_i
-1		1	0	770
0		0	1	84
1	9	1	-9	14

$\gcd(770, 84) = 14$, and $1(770) - 9(84) = 14$.

4.

i	q_i	s_i	t_i	r_i
-1		1	0	232
0		0	1	14
1	16	1	-16	8
2	1	-1	17	6
3	1	2	-33	2

$\gcd(232, 14) = 2$, and $2(232) - 33(14) = 464 - 462 = 2$.

5. Not unique. If $sa + tb = d$, then $(s + kb)a + (t - ka)b = sa + tb = d$, so there are infinitely many solutions.

Section 3.2

1. $10561485 = (3)(5)(11^3)(23)^2$

2. N can be written as a product of primes, in particular, N has at least one prime factor p, which must be one of the p_i. But then p divides N and p divides $p_1 p_2 \dots p_k$; hence p divides 1, a contradiction.

3. If $N = t(n+1)! + 1$, then $N + r - 1 = t(n+1)! + r$, which is divisible by r for $r = 2, 3, \dots, n+1$, which implies that $N + r - 1$ is composite. Thus $N + 1, \dots, N + n$ are all composite.

4. If c is any composite number between 1 and n, then c must have a prime factor $p \le \sqrt{n}$ (otherwise $c = ab$ where both a and b exceed $\sqrt{n}$, so $c > n$, a contradiction). Thus c will be removed from the list.

5. If p^e appears in the prime factorization of a, then by the Unique Factorization Theorem, p^{ke} must appear in the prime factorization of a^k. Thus all exponents in the prime factorization of a^k (and similarly b^k) are multiples of k, and therefore all exponents in the prime factorization of n are multiples of k. It follows that $\sqrt[k]{n}$ is an integer, contradicting the hypothesis.

6. (a) The least common multiple is $m = p_1^{g_1} \dots p_k^{g_k}$ where $g_i = \max(e_i, f_i)$. The argument is exactly the same as in Theorem 3.2.6, with all inequalities reversed and divisors replaced by multiples.

(b) In view of part (a) and (3.2.6), we must show that

$$p^e p^f = p^{\min(e,f)} p^{\max(e,f)}$$

or equivalently, $e + f = \min(e, f) + \max(e, f)$. But this is always true (the sum of two numbers is the smaller plus the larger).

7. If t is any positive integer that is a multiple of both a and b, then by definition of m, we have $m|t$, so $|m| \le t$, and the result follows.

8. $\gcd(a, b) = (2^2)(5)(13)$, $\operatorname{lcm}(a, b) = (2^3)(5^2)(7)(13^2)$.

Section 3.3

1. $3(0) = 0$, $3(1) = 3$, $3(2) = 1$ (note $6 \equiv 1 \bmod 5$), $3(3) = 4$, $3(4) = 2$. Since $3(2) = 1$ in $\mathbb{Z}_5$, the multiplicative inverse of 3 is 2.

2. $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$.

3. $F[X]$ is a commutative ring because polynomials can be added, subtracted and multiplied and the result will still be a polynomial. (Formally, axioms (A1)–(A5) and (M1)–(M5) must be checked.) In fact $F[X]$ is an integral domain. To see this, suppose $f(X)g(X) = (a_nX^n + \cdots + a_0)(b_mX^m + \cdots + b_0) = 0$. If neither $f(X)$ nor $g(X)$ is 0, then we have nonzero leading coefficients a_n and b_m whose product is 0, contradicting the fact that F is a field. $F[X]$ is not a field because $f(X)/g(X)$ is in general not a polynomial (for example, let $f(X) = X + 2$ and $g(X) = X + 1$).

4. We obtain the field $F(X)$ of *rational functions* $f(X)/g(X)$, where $f(X)$ and $g(X)$ are polynomials with coefficients in F, and $g(X) \neq 0$. Since the sum, difference, product or quotient (with nonzero denominator) of rational functions is also a rational function, $F(X)$ is a field.

Section 3.4

1. As in (3.4.2), we find that $4(37)-7(21) = 1$, and it follows that -7 is a multiplicative inverse of 21 mod 37. We are free to replace -7 by the canonical representative $-7+37 = 30$.

2. As in (3.4.2), we find that $3(127) - 38(10) = 1$, so -38 is a multiplicative inverse of 10 mod 127, and we can replace -38 by $-38 + 127 = 89$. If $10x \equiv 7 \bmod 127$, then $x \equiv (10)^{-1}(7) \equiv 89(7) \equiv 115 \equiv -12 \bmod 127$.

3. We have $1 \equiv 1 \bmod 9,\ \ 10 \equiv 1 \bmod 9,\ \ 10^2 = 10(10) \equiv 1(1) = 1 \bmod 9, \ldots,$ $10^{n-1} \equiv 1 \bmod 9$, so $N \equiv a_1 + a_2 + \cdots + a_n \bmod 9$.

4. We have $1 \equiv 1 \bmod 11$, $10 \equiv -1 \bmod 11$, $10^2 \equiv (-1)^2 = 1 \bmod 11$, $10^3 \equiv (-1)^3 = -1 \bmod 11, \ldots, 10^{n-1} \equiv (-1)^{n-1} \bmod 11$. Thus $N \equiv a_1 - a_2 + a_3 - a_4 + \cdots \bmod 11$.

5. We have

$$\begin{aligned} N &= (a_1 + a_2 10^1 + \cdots + a_r 10^{r-1}) + (a_{r+1}10^r + \cdots + a_n 10^{n-1}) \\ &= A + B, \end{aligned}$$

and since $M = 2^r$ and 2 divides 10, M divides B. Thus M divides N if and only if M divides A, as asserted.

6. Let p be a prime factor of N. Then p cannot be any of the p_i, for if p_i were to divide N, the equation $N = 4p_1 \cdots p_k - 1$ implies that p_i divides 1, which is impossible. Since $p_1, \ldots, p_k$ constitute all the primes $\equiv 3 \bmod 4$, p must be congruent to $1 \bmod 4$. (If $p \equiv 0 \bmod 4$, then 4 divides p, which is impossible because p is prime. If $p \equiv 2 \bmod 4$, then p is even, so that $p = 2$. This cannot happen because N is an odd number.) Since the product of numbers congruent to $1 \bmod 4$ is also congruent to $1 \bmod 4$, we have $N \equiv 1 \bmod 4$, a contradiction.

Section 3.5

1. The Euclidean algorithm gives $18(1) + 12(-1) = 6$, so $18(5) + 12(-5) = 30$. Thus $x = 5$ is a solution of $18x \equiv 30 \bmod 12$, or equivalently $3x \equiv 5 \bmod 2$. Thus the general solution is $x = 5 + 2u$, $y = -5 - 3u$. There are 6 distinct solutions $\bmod 12$, corresponding to $u = 0, 1, 2, 3, 4, 5$.

2. The Euclidean algorithm gives $11(-1) + 6(2) = 1$, so $x = -1$ is a solution of $11x \equiv 1 \bmod 6$, and we may replace -1 by 5 since $-1 \equiv 5 \bmod 6$. The general solution is $x = 5 + 6u$, $y = -9 - 11u$, which is unique $\bmod 6$.

3. The given equation is equivalent to $6x + 9y = 3$, and from the Euclidean algorithm we have $6(-1) + 9(1) = 3$, with $\gcd(6, 9) = 3$. Thus $6x \equiv 3 \bmod 9$ is equivalent to $2x \equiv 1 \bmod 3$, and $x = -1$, which can be replaced by $x = 2$, is a solution. The general solution is $x = 2 + 3u$, $y = -1 - 2u$. There are 3 distinct solutions of $6x \equiv 3 \bmod 9$, namely, $x = 2$, $x = 5$, and $x = 8$.

4. We have $m = 4(5)(9) = 180$, $y_1 = 180/4 = 45$, $y_2 = 180/5 = 36$, $y_3 = 180/9 = 20$. Since $45 \equiv 1 \bmod 4$, $36 \equiv 1 \bmod 5$, and $20 \equiv 2 \bmod 9$, we may take $z_1 = 1$, $z_2 = 1$, and $z_3 = 5$. Thus one solution is given by $x_0 = 2(45)(1) + 1(36)(1) + 6(20)(5) = 726 \equiv 6 \bmod 180$. The general solution is $x = 6 + 180u$, $u \in \mathbb{Z}$; the solution is unique $\bmod 180$.

5. If

$$\sum_{i=1}^{k} b_i y_i z_i \equiv 0 \bmod m$$

(hence $\bmod m_j$ for all j), then by (12) we have $b_j \equiv 0 \bmod m_j$ for all $j = 1, \dots, k$. Now suppose that $(b_1, \dots, b_k)$ and $(c_1, \dots, c_k)$ both map to x_0. Since in (13), x_0 is a linear combination of the b_i, it follows that $(b_1 - c_1, \dots, b_k - c_k)$ will map to $x_0 - x_0 = 0$. But then $b_i - c_i \equiv 0 \bmod m_i$, proving that the mapping is injective. Since $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ and $\mathbb{Z}_m$ each have m elements, the mapping is surjective by (1.5.2).

Section 3.6

1. (a) $600 = 2^3(3)(5^2)$, $\varphi(600) = 600(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 160$
(b) $841 = 29^2$, $\varphi(841) = 29^2 - 29 = 812$
(c) $6174 = 2(3^2)(7^3)$, $\varphi(6174) = 6174(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7}) = 1764$

2. The residues are 5, 1, 2, 7, 8, 4, a permutation of 1, 2, 4, 5, 7, 8.

3. Let $p_1, \dots, p_r$ be the primes occurring in the factorization of m, and let $q_1, \dots, q_s$ be the primes occurring in the factorization of n. Since m and n are relatively prime,

$p_i \neq q_j$ for all i, j. Thus

$$\varphi(mn) = mn\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{q_1}\right)\cdots\left(1-\frac{1}{q_s}\right) = \varphi(m)\varphi(n).$$

4. Let $n = 4$, $r = 2$. Then $\binom{n}{r} = 6$, which is not divisible by 4.

5. If p does not divide a, then by Fermat's Theorem, the inverse of a mod p is a^{p-2}. But for large p, the computation becomes very laborious.

6. Let $N = 2^{(p_1-1)\cdots(p_k-1)} = n+1$. Since $p_1 > 2$, p_1 cannot divide 2 and therefore Fermat's Theorem implies that $2^{p_1-1} \equiv 1 \bmod p_1$. Successively raising both sides of this congruence to the powers $p_2-1, \ldots, p_k-1$, we find that $N \equiv 1 \bmod p_1$. Since $p_2 > 2$, p_2 cannot divide 2^{p_1-1}, and Fermat's Theorem gives $2^{(p_1-1)(p_2-1)} \equiv 1 \bmod p_2$. As above, we conclude that $N \equiv 1 \bmod p_2$. Continuing in this fashion, we have $N \equiv 1 \bmod p_i$, $i = 1, 2, \ldots, k$. In other words, $n = N-1$ is divisible by each p_i, and since the p_i are distinct primes, the product $p_1 \cdots p_k$ divides n (see (3.4.5 (f)).

Section 3.7

1. This follows because 17305893 is divisible by $9 = 3^2$.

2. If m is the product of r distinct primes and n is the product of s distinct primes, then since m and n are relatively prime, mn is the product of $r+s$ distinct primes. Thus $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$. If m or n has a repeated prime factor, so does mn, and $\mu(mn) = \mu(m)\mu(n) = 0$.

3. A divisor d of n is of the form $d = p_1^{r_1}\ldots p_k^{r_k}$, $0 \le r_i \le e_i$. Since f is multiplicative, $f(d) = f(p_1^{r_1})\ldots f(p_k^{r_k})$. Thus the terms in the expansion of

$$\left(1+f(p_1)+\cdots+f(p_1^{e_1})\right)\ldots\left(1+f(p_k)+\cdots+f(p_k^{e_k})\right)$$

correspond to the $f(d)$, $d|n$, and the result follows.

4. This follows from Problem 3, since $f(n) = n^r$ is multiplicative.

5. By definition, n is perfect if and only if the sum of all its positive divisors is $n+n = 2n$. Since $\sum_{d|n} d = S_1(n)$, the result follows.

6. $S_1(2^{n-1}) = 1+2+2^2+\cdots+2^{n-1} = 2^n-1$, and since 2^n-1 is prime,

$$S_1(2^n-1) = 1+(2^n-1) = 2^n.$$

Thus $S_1(x) = (2^n-1)(2^n) = 2x$.

7. (a) By Problem 5, $S_1(x) = 2x$, and by Problem 4, $S_1(x) = S_1(2^h)S_1(q)$. But as in Problem 6, $S_1(2^h) = 2^{h+1} - 1$, and the result follows.

(b) $\dfrac{S_1(q)}{q} = \dfrac{2^{h+1}}{2^{h+1}-1} > 1.$

(c) By (b), $2^{h+1}q = (2^{h+1}-1)S_1(q) = (2^{h+1}-1)(q+r)$, so $0 = -q+(2^{h+1}-1)r$, as asserted.

(d) If $r > 1$, then r is a divisor of q and $1 < r < q$. Thus $S_1(q) \geq q+r+1 > q+r$, contradicting (c).

(e) By (c) and (d), $S_1(q) = q + 1$, so the only positive divisors of q are q and 1. It follows that q must be prime.

Section 4.1

1. $\{1, 2, 4, 12\}$ and $\{1, 2, 6, 12\}$

2. If you visualize the ordered pair (a, b) as determined by a vertical line (column) at $x = a$ and a horizontal line (row) at $y = b$ in an x-y plane, then to compare two pairs, we first look at columns, and if the columns are equal, we then look at rows. It should be clear intuitively that we have a total ordering, and the formal details are straightforward. Let C be a nonempty subset of $A \times B$. Among all first coordinates a of ordered pairs $(a, b) \in C$, there is a smallest element a_0, and among all second coordinates b of ordered pairs $(a_0, b) \in C$, there is a smallest element b_0. If $(a, b) \in C$, then

Case 1: $a_0 < a$. Then $(a_0, b_0) < (a, b)$.
Case 2: $a_0 = a$. Then $(a_0, b) = (a, b) \in C$, so $(a_0, b_0) \leq (a_0, b) = (a, b)$.

Thus (a_0, b_0) is the smallest element of C.

3. No, the ordering is not even total, assuming that A and B each have at least two elements. For if $a_1 < a_2$ and $b_1 < b_2$, then (a_1, b_2) and (a_2, b_1) cannot be compared.

Section 4.2

1. Assuming Zorn's Lemma, let B be a chain of the partially ordered set A. The collection $\mathcal{C}$ of all chains containing B is nonempty (since B is a chain containing B) and is partially ordered by inclusion. (See Section 1.6, Problem 7.) Every chain of $\mathcal{C}$ has an upper bound in $\mathcal{C}$, namely the union of all the chains of A that comprise the chain of $\mathcal{C}$. By Zorn's Lemma, there is a maximal element, in other words, a maximal chain containing B.

2. If $r_1v_1 + \cdots + r_nv_n = 0$ but not all $r_i = 0$, say $r_1 \neq 0$. Then

$$v_1 = -r_1^{-1}r_2v_2 - r_1^{-1}r_3v_3 - \cdots - r_1^{-1}r_nv_n,$$

so that v_1 can be expressed as a linear combination of $v_2, \dots, v_n$. Conversely, if one of the v_i can be expressed as a linear combination of the others, move all v_i to the same side of the equation to conclude that a nontrivial linear combination of the v_i is 0.

3. The argument is virtually identical to that of Problem 2.

4. Suppose that the chain consists of the linearly independent sets L_i, $i \in I$. Then each L_i is contained in the union of all the L_i, so $\bigcup_{i\in I} L_i$ is an upper bound of the chain in $\mathcal{C}$, provided we can show that it is a linearly independent set. But if $r_1v_1 + \cdots + r_nv_n = 0$ with the $v_j \in \bigcup_{i\in I} L_i$, then for some index k we have all $v_j \in L_k$, because the L_i form a chain. (For example, if $v_1 \in L_1$, $v_2 \in L_7$, and $L_1 \subseteq L_7$, then both v_1 and v_2 belong to L_7.) Since L_k is linearly independent, all r_i must be 0.

5. By Zorn's Lemma, $\mathcal{C}$ has a maximal element, that is, V has a maximal linearly independent set.

Section 4.3

1. If $c \in C$, there is an element $b \in B$ such that $g(b) = c$, and an element $a \in A$ such that $f(a) = b$. But then $g(f(a)) = c$, proving $g \in f$ surjective.

2. There are many possibilities. For example, let $f(x) = x^2$ on the reals. Then f is not injective, but if we restrict f to the nonnegative reals, the resulting function is injective.

3. If $B \leq_s A$, then there is an injective map g from B into A. The inverse of this function maps $g(B)$ onto B. If we define $f(x) = g(x)$ for $x \in g(B)$, and define $f(x)$ to be an arbitrary element of B for $x \in A \setminus g(B)$, then $f : A \to B$ is surjective. Conversely, if f maps A onto B, then for each $y \in B$ there is an element $x \in A$ such that $f(x) = y$. Choose one such x (Axiom of Choice!) and call it $g(y)$. If $x = g(y_1) = g(y_2)$, then by definition of g, x is mapped by f to both y_1 and y_2, and since f is a function, we must conclude that $y_1 = y_2$. Thus g is an injective map of B into A, so $B \leq_s A$.

4. If B is countably infinite, then there is a bijection between B and $\mathbb{N}$, and if B is finite, there is an injective map from B to $\mathbb{N}$. Thus B is countable if and only if $B \leq_s \mathbb{N}$, and the result follows from Problem 3.

5. Let $A = \{a_1, \dots, a_m\}$ and $B = \{b_1, \dots, b_n\}$. If $m = n$, then $a_i \to b_i$, $1 \leq i \leq n$, defines a bijection between A and B, so $|A| = |B|$. If $m < n$, then $a_i \to b_i$, $1 \leq i \leq m$, defines an injective map from A to B, so $|A| \leq |B|$. Since $m < n$, any function from B to A must map at least two b_i's to the same element of A, so there can be no bijection between A and B. Therefore $|A| < |B|$, and the result follows.

Section 4.4

In Problems 1, 2, and 3, $|A| = \alpha$, $|B| = \beta$, $|C| = \gamma$.

1. A^{B+C} is the set of functions from the disjoint union of B and C to A, and this set of functions is in one-to-one correspondence with the set of pairs of functions (f,g) where $f : B \to A$ and $g : C \to A$. (If $h : B+C \to A$, take f and g to be the restrictions of h to B and C, respectively.) Thus $|A^{B+C}| = |A^B|\,|A^C|$.

2. $(A \times B)^C$ is the set of functions $f : C \to A \times B$, and f corresponds to a pair (g,h) with $g : C \to A$ and $h : C \to B$. Explicitly, if $f(c) = (a,b)$ then $g(c) = a$ and $h(c) = b$. Thus $(A \times B)^C$ has the same cardinality as $A^C B^C$.

3. If $f : B \times C \to A$, define $f_c : B \to A$ as $f_c(b) = f(b,c)$. Then f determines a mapping $c \to f_c$ from C to A^B. Conversely, given the mapping $c \to f_c$, we can recapture f by $f(b,c) = f_c(b)$. This establishes a one-to-one correspondence between $A^{B\times C}$ and $(A^B)^C$.

4. If B is any infinite set, then B has a countably infinite subset C, as we found in the proof of (4.4.3(b)). Thus $\aleph_0 = |C| \le |B|$.

5. A real number may be specified by selecting an interval $[n, n+1)$ and then choosing a point in that interval. If α is the cardinality of the set of reals between 0 and 1, then each interval $[n, n+1)$ has cardinality α, so $c = \aleph_0\alpha$. But $\aleph_0 < \alpha$ (see Section 2.4), and consequently $c = \alpha$ by (4.4.3(b)).

6. An element of A can be identified with a finite subset of the positive integers. For example, 01001 has 1's in positions 2 and 5, and therefore corresponds to $\{2,5\}$. But we know that there are only countably many finite subsets of the positive integers (see (2.4.3) and the discussion preceding it, or (4.4.4)).

7. By Problems 5 and 6, $2^{\aleph_0} = c + \aleph_0$, and since $\aleph_0 < c$, we have $c + \aleph_0 = c$ by (4.4.3(a)).

8. By (4.3.7), $2^{\aleph_0} > \aleph_0$, and since $\aleph_1$ is the smallest cardinal greater than $\aleph_0$, we must have $\aleph_1 \le 2^{\aleph_0}$.

Section 5.1

1. The ij element of $A(B+C)$ is $\sum_k a_{ik}(b_{kj} + c_{kj}) = \sum_k a_{ik}b_{kj} + \sum_k a_{ik}c_{kj}$, which is the ij element of AB plus the ij element of AC. The second distributive law is proved similarly. The key point is that the distributive laws hold for real numbers, in fact for any field.

2. The ij element of $A(BC)$ is

$$\sum_k a_{ik} \sum_r b_{kr} c_{rj} = \sum_r \left(\sum_k a_{ik} b_{kr} \right) c_{rj} = \sum_r (AB)_{ir} C_{rj},$$

which is the ij element of $(AB)C$. The key points are that multiplication is associative in any field, and the order of summation of a finite double series can always be reversed.

3. No. For example, let

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

4. If we apply the row operations represented by $E_1, \dots, E_k$ to A in that order, the result is the product $E_k E_{k-1} \cdots E_1 A$, which is I_n by hypothesis. But if the row operations are applied to I_n, we get $E_k E_{k-1} \cdots E_1 I_n = E_k E_{k-1} \cdots E_1 = B$. Therefore $BA = I_n$.

5. Multiply $BA = I_n$ on the right by A^{-1} to obtain $B = A^{-1}$.

6. A is an elementary row matrix obtained from I_2 by adding 3 times row 2 to row 1. Thus A^2 is obtained from A by adding 3 times row 2 to row 1; the result is

$$\begin{bmatrix} 1 & 6 \\ 0 & 1 \end{bmatrix}.$$

Continuing in this fashion, we have

$$A^k = \begin{bmatrix} 1 & 3k \\ 0 & 1 \end{bmatrix};$$

in particular,

$$A^{74} = \begin{bmatrix} 1 & 222 \\ 0 & 1 \end{bmatrix}.$$

7. If A is $m \times n$, then A^t is $n \times m$, so that AA^t exists and is $m \times m$. Since $(AA^t)^t = (A^t)^t A^t = AA^t$, it follows that AA^t is symmetric.

8. No. As in the text we have $a_{ii} = -a_{ii}$ so $a_{ii} + a_{ii} = 0$. In a field of "characteristic 2", in other words a field in which $1 + 1 = 0$, it does not follow that $a_{ii} = 0$. We have already met one such field, namely $\mathbb{Z}_2$, the field of integers modulo 2.

9. We have $A = \frac{1}{2}(A + A^t) + \frac{1}{2}(A - A^t) =$ symmetric $+$ skew-symmetric.

10. Direct computation shows that A^2 has 1's in the 1-3 and 2-4 positions, and 0's elsewhere; A^3 has a 1 in the 1-4 position, and 0's elsewhere; A^4 has all zero entries.

Section 5.2

1. Apply the elementary row operations $R_2 \leftarrow R_2 - 2R_1$, $R_2 \leftarrow -\frac{1}{5}R_2$, $R_1 \leftarrow R_1 - 3R_2$, $R_3 \leftarrow R_3 - R_2$, $R_3 \leftarrow -R_3$ to I_3 to get

$$A^{-1} = \begin{bmatrix} -1/5 & 3/5 & 0 \\ 2/5 & -1/5 & 0 \\ 2/5 & -1/5 & -1 \end{bmatrix}.$$

2. In Problem 1, the second operation multiplies the determinant by $-\frac{1}{5}$, and the fifth operation multiplies the determinant by -1; the other operations leave the determinant unchanged. Thus $\det A = \frac{1}{1/5} = 5$. Checking by Laplace Expansion down column 3, we have $(-1)(1-6) = 5$.

3. If rows i and j are identical, add -1 times row i to row j to produce a row of zeros, and therefore a zero determinant.

4. If $R_i = a_1 R_{i_1} + \cdots + a_k R_{i_k}$, successively add $-a_1$ times row $i_1, \ldots, -a_k$ times row i_k to row i to produce a row of zeros, and therefore a zero determinant.

5. If a sequence of elementary row operations reduces A to echelon form Q, then the analogous sequence of elementary column operations will reduce A^t to Q^t. (If $BA = Q$, then $A^t B^t = Q^t$). If $Q = I$, then $Q^t = I$, and if Q has a row of zeros, then Q^t has a column of zeros. Thus the computational procedure for finding the determinant of A^t produces exactly the same set of numbers as the procedure for finding the determinant of A. Therefore $\det A^t = \det A$.

Section 5.3

1. If S is a basis then S spans, so each $x \in V$ has an expression of the desired form. If x has two distinct representations then $u_1, \ldots, u_n$ are linearly dependent, a contradiction. Conversely, if each x is a linear combination of the u_i, then S spans V. If $a_1 u_1 + \cdots + a_n u_n = 0$, then since 0 has the unique representation $0u_1 + \cdots + 0u_n$, we have $a_1 = \cdots = a_n = 0$.

2. Lining up u, v, and w as columns, we have

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Since the echelon form of A is I_3 (equivalently, A is invertible; equivalently, $\det A \neq 0$), the equations $au + bv + cw = 0$ have the unique solution $a = b = c = 0$. Therefore u, v, and w are three linearly independent vectors in $\mathbb{R}^3$, hence a basis.

3. With A as in Problem 2, we must solve the equations

$$A\begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 2 \\ 3 \\ 4 \end{bmatrix}$$

for a, b, and c. The result is $a = 2$, $b = 3$, $c = 1$.

4. Assume that one of the bases, say T, is finite. The proof of (5.3.2) applies verbatim, and shows that $|S| \leq |T|$. But then S is also finite.

5. If $j \in I$ but j does not belong to the union of the $I(x)$, then for any $x \in S$, x depends on the y_i, $i \in I(x)$, but i is never equal to j. Thus the vectors in S can be expressed in terms of $T \setminus \{y_j\}$, a contradiction since T is a basis, hence a minimal spanning set.

6. An element of $\cup\{I(x) : x \in S\}$ is determined by selecting a vector $x \in S$ and then choosing an index in $I(x)$. Since $I(x)$ is finite, we have $|I(x)| \leq \aleph_0$. By Problem 5, we have $|I| = |\cup \{I(x) : x \in S\}|$, so $|I| \leq |S|\aleph_0$, and the result follows.

Section 5.4

1. (a) The first quadrant $\{(x, y) : x \geq 0 \text{ and } y \geq 0\}$.
(b) The union of the first quadrant and the third quadrant $\{(x, y) : x \leq 0 \text{ and } y \leq 0\}$.

2. The fourth component of a vector in S is twice the first component minus the second component. This property is maintained under addition and scalar multiplication, so S is a subspace.

3. Let $a = 1$, $b = c = 0$ to get $u = (1, 0, 0, 2)$; let $a = 0$, $b = 1$, $c = 0$ to get $v = (0, 1, 0, -1)$; let $a = b = 0$, $c = 1$ to get $w = (0, 0, 1, 0)$. Our choices of a, b, and c guarantee that u, v, w are linearly independent. If $p = (a, b, c, 2a - b)$ is any vector in S, then $p = au + bv + cw$. Thus u, v, and w span and therefore form a basis.

4. If $a(u + v) + b(v + w) + c(w + u) = 0$, then by linear independence of u, v, w we have $a + c = 0$, $a + b = 0$, and $b + c = 0$. These equations have a unique solution $a = b = c = 0$, so $u + v$, $v + w$, and $w + u$ are three linearly independent vectors in a three-dimensional subspace. Thus $u + v$, $v + w$, and $w + u$ are a basis.

5. Line up the vectors as columns to obtain

$$\begin{bmatrix} 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 4 \\ 2 & 3 & 1 & 8 \end{bmatrix}.$$

Elementary row operations yield the echelon form

$$\begin{bmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 5 \end{bmatrix}.$$

If C_i is column i, then C_1, C_2, and C_3 are linearly independent, and it follows that u, v, and w are a basis. Since $C_4 = 3C_1 - C_2 + 5C_3$, we have $(1, 4, 8) = 3u - v + 5w$.

6. (a) K will be a subspace, typically a line or a plane through the origin. Then C will be a translated subspace, in other words, a line or a plane not necessarily through the origin.

(b) Suppose $u+K = v+K$. Then $u = u+0 \in u+K = v+K$, so $u-v \in K = N(A)$. But then $A(u-v) = 0$, hence $Au = Av$. Note also that if $u-v \in K$, then $u+K = v+K$, for if $w \in u + K$, then $w = u + p$, $p \in K$, and also $u = v + q$, $q \in K$. Thus $w = u + p = v + (p + q) \in v + K$, so $u + K \subseteq v + K$; the reverse inclusion is proved by a symmetrical argument. This observation will be useful in Problem 7.

7. (a) If $u_1+K = u_2+K$ and $v_1+K = v_2+K$, then u_1-u_2 and v_1-v_2 belong to K, so $(u_1-u_2)+(v_1-v_2) = (u_1+v_1)-(u_2+v_2) \in K$. Therefore $(u_1+v_1)+K = (u_2+v_2)+K$. Similarly $au_1 - au_2 = a(u_1 - u_2) \in K$, so $au_1 + K = au_2 + K$.

(b) $\pi\big(a(u + K) + b(v + K)\big) = \pi(au + bv + K) = A(au + bv) = aAu + bAv$
$= a\pi(u + K) + b\pi(v + K)$.

(c) If $\pi(u + K) = \pi(v + K)$, then $Au = Av$, so $A(u - v) = 0$, and therefore $u - v \in K$. But then $u + K = v + K$, proving that π is injective. Since $\pi(u + K) = Au$, which ranges over all of $R(A)$ as u ranges over F^n, π is surjective.

Section 5.5

1. If $u = Tx$ and $v = Ty$, then $u + v = Tx + Ty = T(x + y)$, so $T^{-1}(u + v) = x + y = T^{-1}u + T^{-1}v$. Also, $cu = cTx = T(cx)$, so $T^{-1}(cu) = cx = cT^{-1}u$, proving that T^{-1} is linear. If the matrix B represents T^{-1} then since $T^{-1} \circ T$ is the identity transformation, represented by the identity matrix I, we have $BA = I$, so $B = A^{-1}$.

2. New coordinates $= P^{-1}$(old coordinates), so

$$P^{-1} = \begin{bmatrix} 4 & -6 \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad P = \begin{bmatrix} 1/4 & 3/2 \\ 0 & 1 \end{bmatrix}.$$

Therefore

$$u = \begin{bmatrix} 1/4 \\ 0 \end{bmatrix} = \frac{1}{4}e_1 \quad \text{and} \quad v = \begin{bmatrix} 3/2 \\ 1 \end{bmatrix} = \frac{3}{2}e_1 + e_2.$$

3. $T(1,0)$ has length 1 and angle θ, so $T(1,0) = (\cos\theta, \sin\theta)$. $T(0,1)$ has length 1 and angle $\frac{\pi}{2} + \theta$, so $T(0,1) = (\cos(\frac{\pi}{2} + \theta), \sin(\frac{\pi}{2} + \theta)) = (-\sin\theta, \cos\theta)$. The matrix of T with respect to the standard basis is

$$A = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

4. $T(u) = u$ and $T(v) = -v$, so $B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. The basis-changing matrix is $P = \begin{bmatrix} 1 & -a \\ a & 1 \end{bmatrix}$. Then

$$P^{-1} = \frac{1}{1+a^2}\begin{bmatrix} 1 & a \\ -a & 1 \end{bmatrix} \quad \text{and} \quad B = P^{-1}AP.$$

Thus

$$A = PBP^{-1} = \frac{1}{1+a^2}\begin{bmatrix} 1-a^2 & 2a \\ 2a & a^2-1 \end{bmatrix}.$$

5. If T is a linear transformation represented by the matrix A with respect to a given basis, the mapping $x \to Tx$ corresponds to the matrix calculation $c \to Ac$. The image of T corresponds to $R(A)$, the range of A. If the basis is changed, the same linear transformation T is represented by a matrix B similar to A, and now the image of T corresponds to $R(B)$. Therefore $R(A)$ and $R(B)$ have the same dimension, that is, $\operatorname{rank} A = \operatorname{rank} B$.

6. If $B = P^{-1}AP$, then $B^t = P^tA^t(P^{-1})^t = P^tA^t(P^t)^{-1} = Q^{-1}A^tQ$, where $Q = (P^t)^{-1}$.

7. Both results follow from (5.5.5): $\dim(\ker T) + \dim(\operatorname{im} T) = \dim V$.

(a) If $\ker T = \{0\}$, then $\dim(\operatorname{im} T) = \dim V > \dim W$, which is impossible since $\operatorname{im} T \subseteq W$. Thus $\ker T$ contains a nonzero vector, so T is not injective.

(b) If $\operatorname{im} T = W$, then $\dim(\ker T) = \dim V - \dim W < 0$, a contradiction. Thus the image of T must be a proper subset of W, so that T is not surjective.

Section 5.6

1.
$$\begin{aligned}
\|x+y\|^2 &= \|x\|^2 + \|y\|^2 + 2\operatorname{Re}\langle x, y\rangle;\\
\|x-y\|^2 &= \|x\|^2 + \|y\|^2 - 2\operatorname{Re}\langle x, y\rangle;\\
\|x+iy\|^2 &= \|x\|^2 + \|y\|^2 + 2\operatorname{Re}\langle x, iy\rangle;\\
\|x-iy\|^2 &= \|x\|^2 + \|y\|^2 - 2\operatorname{Re}\langle x, iy\rangle.
\end{aligned}$$

But $\operatorname{Re}\langle x, iy\rangle = \operatorname{Re}[-i\langle x, y\rangle] = \operatorname{Im}\langle x, y\rangle$, and the result follows.

2. This follows from the last equation in the proof of (5.6.7), with $a_i = \langle x, x_i\rangle$.

3. If $z \in S$ and $x, y \in S^\perp$, a, $b \in C$, then $\langle ax + by, z\rangle = a\langle x, z\rangle + b\langle y, z\rangle = 0$. Thus $S^\perp$ is closed under linear combination and is therefore a subspace.

4. By the Projection Theorem (5.6.9), p is the unique vector in S such that $x-p$ is orthogonal to each x_i. Since the components of x_i will appear in row i of A^t, we have $A^t(x-p)=0$, or $A^tx=A^tp$. But $p=a_1x_1+\cdots+a_kx_k=a_1$ (column 1 of A) $+\cdots+a_k$ (column k of A) $=Aq$, as can be visualized by walking across a row of A and down the column vector q. Thus $A^tx=A^tAq$. If the scalars are allowed to be complex, the normal equations become $A^*x=A^*Aq$, where A^* is the conjugate transpose of A; that is, A^* is formed by taking the complex conjugate of each element of A, and then transposing. (The condition that $x-p$ is orthogonal to each x_i can be expressed as $A^*(x-p)=0$; the remainder of the analysis is the same.)

5. We have $E=\|Y-AX\|^2$, and as the components of X range over all real numbers, the vectors AX range over the space spanned by the columns of A. Thus we are projecting Y on the space spanned by the columns of A. The result follows from Problem 4.

6. The vector Y is the same as in Problem 5, but now we have

$$E=\sum_{i=1}^{m}|y_i-ax_i^2-bx_i-c|^2 \quad \text{and} \quad X=\begin{bmatrix} a \\ b \\ c \end{bmatrix}.$$

The matrix A now has three columns. The components of the first column are $x_1^2,\dots,x_m^2$, the components of the second column are $x_1,\dots,x_m$, and the components of the third column are $1,\dots,1$.

7. Equality holds if and only if x and y are linearly dependent. For if there is equality, then by the proof of (5.6.2), $x+ay=0$ for some a. (If $y=0$, then equality holds, and x and y are linearly dependent as well, so this case causes no difficulty.) Conversely, if x and y are linearly dependent, then one is a multiple of the other, say $x=cy$. Then

$$|\langle x,y\rangle|=|\langle cy,y\rangle|=|c|\,\|y\|^2=\big(|c|\|y\|\big)\|y\|=\|x\|\,\|y\|.$$

Section 5.7

1. If A and B are unitary, then $(AB)(AB)^*=ABB^*A^*=AIA^*=AA^*=I$, proving that AB is unitary. The sum need not be unitary; for example, take $B=-A$.

2. If $Tx=\lambda x$, then $T^2x=T(Tx)=T(\lambda x)=\lambda(Tx)=\lambda(\lambda x)=\lambda^2x$. Apply T successively to get the result.

3. $\det(A-\lambda I)=(2-\lambda)^2(1-\lambda)$, so the eigenvalues are $\lambda=2$ (2-fold) and $\lambda=1$. When $\lambda=2$, the equations

$$(A-\lambda I)\begin{bmatrix} x \\ y \\ z \end{bmatrix}=0$$

become $y = 0$, $z = 0$, x arbitrary. The eigenspace is only one-dimensional, spanned by $(1, 0, 0)$. When $\lambda = 1$, the equations are $x + y = 0$, $y = 0$, z arbitrary, so the eigenspace is spanned by $(0, 0, 1)$. There are only two linearly independent eigenvectors in a three-dimensional space, so A cannot be diagonalized.

4. A is invertible if and only if $\det A = \det(A - 0I) \neq 0$, in other words, 0 is not an eigenvalue of A.

5. $(2, 4)$ and $(-7, y)$ are orthogonal by (5.7.7), so $-14 + 4y = 0$, $y = 7/2$.

6. We have $A = UDU^*$, so $A^* = U^{**}D^*U^* = UDU^* = A$.

7. If A is similar to the matrix $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$, then by (5.7.2), $\det A = \det D = \lambda_1 \dots \lambda_n$.

8. $A^2 = PDP^{-1}PDP^{-1} = PD^2P^{-1}$, and by iteration, $A^k = PD^kP^{-1}$. But D^k is a diagonal matrix with entries $\lambda_1^k, \dots, \lambda_n^k$, so A^k is relatively easy to compute.

9. $q = 3(x^2 + \frac{2}{3}xy + \frac{1}{9}y^2) - y^2 - \frac{1}{3}y^2 = 3(x + \frac{1}{3}y)^2 - \frac{4}{3}y^2 = 3X^2 - \frac{4}{3}Y^2$ where $X = x + \frac{1}{3}y$, $Y = y$. Thus

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} 1 & 1/3 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix},$$

and by (5.5.6),

$$P^{-1} = \begin{bmatrix} 1 & 1/3 \\ 0 & 1 \end{bmatrix}.$$

Invert P^{-1} to get

$$P = \begin{bmatrix} 1 & -1/3 \\ 0 & 1 \end{bmatrix}.$$

The new basis vectors are $(1, 0)$ and $(-1/3, 1)$.

10. $$\begin{aligned} q &= 3(x^2 + (2y + 6z)x + (y + 3z)^2) - 6y^2 + z^2 - 3(y + 3z)^2 \\ &= 3(x + y + 3z)^2 - 9y^2 - 18yz - 26z^2; \end{aligned}$$

then proceed to reduce $-9y^2 - 18yz - 26z^2$ as in Problem 9.

11. $\|Ux\|^2 = \langle Ux, Ux\rangle = (Ux)^*Ux = x^*U^*Ux = x^*x = \langle x, x\rangle = \|x\|^2$.

12. Let x be an eigenvector for λ. Then $Ux = \lambda x$, and by Problem 11, $\|Ux\| = \|x\|$, so $\|x\| = \|\lambda x\| = |\lambda|\,\|x\|$. Therefore $|\lambda| = 1$.

Section 6.1

1. The largest Jordan block has order 3, and in fact there are 2 blocks of order 3. Since $\operatorname{rank}(J - \lambda I) = 2$ (# of blocks of order 3) $+ 1$ (# of blocks of order 2), there are $7 - 4 = 3$ blocks of order 2. The # of blocks of order 1 is

$$14 - 3 \text{ (\# of blocks of order 3)} - 2 \text{ (\# of blocks of order 2)} = 14 - 6 - 6 = 2.$$

2. The largest Jordan block must have order 3, and there must be only 1 block of this order. Therefore the conditions are

$$\operatorname{rank}(J - \lambda I)^3 = 0, \qquad \operatorname{rank}(J - \lambda I)^2 = 1$$

3. In this case, the rank of $J - \lambda I$ must be 0, in other words, $J - \lambda I$ must be the zero matrix.

4. Look at the 18 by 18 matrix J at the beginning of the section. The determinant of J is 3^{18}, and since $\det(J - \lambda I) = (3 - \lambda)^{18}$, the multiplicity of the eigenvalue 3 is 18. This argument works in the general case, and the result now follows from the fact that the Jordan canonical form is a direct sum of matrices $J(\lambda)$, λ ranging over all eigenvalues of A.

Section 6.2

1. J is already in Jordan canonical form, and its characteristic polynomial is $c(x) = (x - \lambda)^r$. Thus J has only one eigenvalue λ, of multiplicity r. In this case, there is only one Jordan block, of order r. By (6.2.4), the minimal polynomial of J is $m(x) = (x - \lambda)^r$.

2. By (6.2.6), $c(x) = (x - \lambda_1) \cdots (x - \lambda_n)$. By (5.7.4), A is diagonalizable, so by (6.2.4) and (6.2.5), $m(x)$ coincides with $c(x)$. The Jordan canonical form is $\operatorname{diag}(\lambda_1, \dots, \lambda_n)$.

3. Case 1: $m(x) = c(x)$. Then corresponding to λ_1 there is one Jordan block of order 2, and corresponding to λ_2 there is one Jordan block of order 1. The Jordan canonical form is

$$\begin{bmatrix} \lambda_1 & 1 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{bmatrix}.$$

Case 2: $m(x) = (x - \lambda_1)(x - \lambda_2)$. Then corresponding to λ_1 there are two blocks of order 1, and corresponding to λ_2 there is one block of order 1. The Jordan canonical form is

$$\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{bmatrix}.$$

4. Case 1: $m(x) = c(x)$. Then there is only one Jordan block, of order 3, and the Jordan canonical form is

$$\begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{bmatrix}.$$

Case 2: $m(x) = (x - \lambda)^2$. There is one block of order 2 and one block of order 1, and the Jordan canonical form is

$$\begin{bmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix}.$$

Case 3: $m(x) = x - \lambda$. There are three blocks of order 1, and the Jordan canonical form is

$$\begin{bmatrix} \lambda & 0 & 0 \\ 0 & \lambda & 0 \\ 0 & 0 & \lambda \end{bmatrix}.$$

5. Let A be a 4 by 4 matrix with characteristic polynomial $c(x) = (x - \lambda)^4$ and minimal polynomial $m(x) = (x - \lambda)^2$. Then the largest block is of order 2, giving rise to a submatrix

$$\begin{bmatrix} \lambda & 1 \\ 0 & \lambda \end{bmatrix}.$$

There can be another Jordan block of order 2, or two blocks of order 1, so the Jordan form is not determined by simply giving $c(x)$ and $m(x)$.

6. Suppose that $c(x) = \sum_{i=0}^{n} a_i x^i$; then $\sum_{i=0}^{n} a_i A^i = 0$ by Cayley-Hamilton (take A^0 to be I). If A is known to be invertible, we can multiply both sides of the equation by A^{-1} to get $a_0 A^{-1} + \sum_{i=1}^{n} a_i A^{i-1} = 0$, so that A^{-1} can be expressed in terms of powers of A. Notice that if $a_0 = 0$, then x is a factor of $c(x)$, so that 0 is an eigenvalue of A. But then A can't be invertible (see Section 5.7, Problem 4).

Section 6.3

1. $$\begin{aligned}\langle x, (T+S)^* y\rangle &= \langle (T+S)x, y\rangle = \langle Tx + Sx, y\rangle = \langle Tx, y\rangle + \langle Sx, y\rangle \\ &= \langle x, T^* y\rangle + \langle x, S^* y\rangle = \langle x, T^* y + S^* y\rangle,\end{aligned}$$

so $(T+S)^* y = T^* y + S^* y$, that is, $(T+S)^* = T^* + S^*$.

2. $$\begin{aligned}\langle x, (cT)^* y\rangle &= \langle (cT)x, y\rangle = \langle cTx, y\rangle = c\langle Tx, y\rangle = c\langle x, T^* y\rangle \\ &= \langle x, \overline{c} T^* y\rangle, \text{ so } (cT)^* = \overline{c} T^*.\end{aligned}$$

3. $\langle x, (TS)^* y\rangle = \langle TSx, y\rangle = \langle Sx, T^* y\rangle = \langle x, S^* T^* y\rangle$, so $(TS)^* = S^* T^*$.

4. $\langle Tx, y\rangle = \langle x, T^* y\rangle = \overline{\langle T^* y, x\rangle} = \overline{\langle y, T^{**} x\rangle} = \langle T^{**} x, y\rangle$, so $T^{**} = T$.

5. $\langle x, I^*y\rangle = \langle Ix, y\rangle = \langle x, y\rangle$, so $I^* = I$.

6. $Tx = 0$ iff $\langle Tx, y\rangle = 0$ for all y iff $\langle x, T^*y\rangle = 0$ for all y.

7. By Problem 6, the kernel of T^* and the image of T^{**} are orthogonal complements. But by Problem 4, $T^{**} = T$ and the result follows.

Section 6.4

1. A has distinct eigenvalues $\lambda = 1$ and $\lambda = 2$, so A is diagonalizable. But $AA^* \neq A^*A$, so A is not unitarily diagonalizable.

2. Take $g = \sum_{i=0}^{n} b_i f_i$.

3. Since the T_i are projection operators, this is immediate from (6.3.7).

4. We have $T^2 = (\lambda_1 T_1 + \cdots + \lambda_k T_k)(\lambda_1 T_1 + \cdots + \lambda_k T_k) = \lambda_1^2 T_1 + \cdots + \lambda_k^2 T_k$, and similarly $T^m = \sum_{i=1}^{k} \lambda_i^m T_i$ for all m. Thus

$$\begin{aligned} &a_0 I + a_1 T + \cdots + a_n T^n \\ &\qquad = (a_0 + a_1\lambda_1 + \cdots + a_n\lambda_1^n)T_1 + \cdots + (a_0 + a_1\lambda_k + \cdots + a_n\lambda_k^n)T_k, \end{aligned}$$

and the result follows.

5. If $T^* = g(T)$, then $TT^* = Tg(T) = g(T)T = T^*T$, so T is normal. If T is normal, write $T = \lambda_1 T_1 + \cdots + \lambda_k T_k$ as in (6.4.5). By (6.3.5), $T^* = \overline{\lambda_1}T_1^* + \cdots + \overline{\lambda_k}T_k^* = \overline{\lambda_1}T_1 + \cdots + \overline{\lambda_k}T_k$ by Problem 3. By Problem 2, there is a polynomial g such that $g(\lambda_i) = \overline{\lambda_i}$, $i = 1, \dots, k$. Thus $T^* = g(\lambda_1)T_1 + \cdots + g(\lambda_k)T_k = g(T)$ by Problem 4.

6. If T is unitary, then T is normal by (6.4.1), and the eigenvalues of T have magnitude 1 by Section 5.7, Problem 12. Conversely, assume T normal with $|\lambda| = 1$ for all eigenvalues λ. Then by (6.4.5) and (6.3.5),

$$\begin{aligned} TT^* &= (\lambda_1 T_1 + \cdots + \lambda_k T_k)(\overline{\lambda}_1 T_1^* + \cdots + \overline{\lambda}_k T_k^*) \\ &= (\lambda_1 T_1 + \cdots + \lambda_k T_k)(\overline{\lambda}_1 T_1 + \cdots + \overline{\lambda}_k T_k) \quad \text{by Problem 3} \\ &= |\lambda_1|^2 T_1 + \cdots + |\lambda_k|^2 T_k = T_1 + \cdots + T_k = I \quad \text{by (6.4.5),} \end{aligned}$$

proving T unitary.

7. If T is self-adjoint then all eigenvalues of T are real by (5.7.7). Conversely, assume that all eigenvalues of T are real. Then $T = \lambda_1 T_1 + \cdots + \lambda_k T_k$ and

$$\begin{aligned} T^* &= \overline{\lambda_1}T_1^* + \cdots + \overline{\lambda_k}T_k^* \quad \text{by (6.3.5)} \\ &= \overline{\lambda_1}T_1 + \cdots + \overline{\lambda_k}T_k \quad \text{by Problem 3} \\ &= \lambda_1 T_1 + \cdots + +\lambda_k T_k \quad \text{since the } \lambda_i \text{ are real.} \end{aligned}$$

Thus $T^* = T$, so that T is self-adjoint.

8. For each $i = 1, \dots, k$, let f_i be a polynomial such that

$$f_i(\lambda_j) = \delta_{ij} = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$$

(see Problem 2). By Problem 4,

$$\begin{aligned} f_i(T) &= f_i(\lambda_1)T_1 + \cdots + f_i(\lambda_k)T_k \\ &= \delta_{i1}T_1 + \cdots + \delta_{ik}T_k = T_i. \end{aligned}$$

9. By (6.3.5) and Problems 3 and 4, $f(T)^*$ is a linear combination of the T_i, and therefore by Problem 8, $f(T)^*$ is a polynomial in T. By Problem 5, $f(T)$ is normal. The second statement follows from the representation

$$f(T) = f(\lambda_1)T_1 + \cdots + f(\lambda_k)T_k$$

(see Problem 4).

10. To find the eigenvalues, we must solve

$$\begin{bmatrix} \cos\psi - \lambda & -\sin\psi \\ \sin\psi & \cos\psi - \lambda \end{bmatrix} = 0,$$

i.e., $\lambda^2 - 2\lambda\cos\psi + 1 = 0$. The eigenvalues are $\cos\psi \pm i\sin\psi$. When $\lambda = \cos\psi + i\sin\psi$, the equations $Ax = \lambda x$, with $x = (u, v)^t$, reduce to $(-i\sin\psi)u - (sin\psi)v = 0$, or $u = iv$. Thus $(i, 1)$ is an eigenvector. When $\lambda = \cos\psi - i\sin\psi$, we get $(i\sin\psi)u - (\sin\psi)v = 0$, so that $v = iu$. Thus $(1, i)$ is an eigenvector. An orthonormal basis of eigenvectors is given by $(i/\sqrt{2}, 1/\sqrt{2})$ and $(1/\sqrt{2}, i/\sqrt{2})$.

Section 6.5

1. Near the end of the proof we said ... let λ be any eigenvalue of A. We need the complex numbers to guarantee that A has at least one eigenvalue (see Example 6.4.2). If A is n by n, the eigenvalues are the roots of $\det(A - \lambda I)$, which is a polynomial of degree n in λ. The key point is that every polynomial of degree at least 1 with coefficients in the field of complex numbers has at least one root. A field in which this property holds is said to be *algebraically closed.* It can be shown that the Jordan canonical form exists over any algebraically closed field.

2. (a) $S(Tx) = STx = TSx = T(\lambda x) = \lambda(Tx)$.

(b) If $x \in W$, then $Sx = \lambda x$ for some λ, so by (a), $S(Tx) = \lambda(Tx)$, hence $Tx \in W$.

(c) If $m_T(x)$ is the minimal polynomial of T, then $m_T(T) = 0$, in particular, $m_T(T)$ is 0 on W. Thus the minimal polynomial $q(x)$ of T_W divides $m_T(x)$ by (6.2.2). But by (6.2.5), $m_T(x)$ is a product of distinct linear factors, hence so is $q(x)$. Again by (6.2.5), T_W is diagonalizable. If T is unitarily diagonalizable and therefore normal, then

$TT^* = T^*T$; in particular, this holds on W, so that T_W is also normal and therefore unitarily diagonalizable.

(d) Since S is diagonalizable, there is a basis of eigenvectors of S. By (c), T is diagonalizable on each eigenspace W of S, so we may choose a basis for W whose members are eigenvectors of both T and S. If we do this for each eigenspace of S, we have simultaneously diagonalized the operators.

(e) Proceed exactly as in (d), with "diagonalizable" replaced by "unitarily diagonalizable" and "basis" by "orthonormal basis".

(f) There is a basis whose members are eigenvectors of both T and S. With respect to this basis, both T and S are represented by diagonal matrices, which always commute. Therefore $TS = ST$.

List of Symbols

Symbol	Meaning	First Appearance
iff	if and only if	4
$\vee$	or	4
$\wedge$	and	4
$\neg$	not	4
$\Rightarrow$	implies	4
$\Leftrightarrow$	equivalence	4
$\exists$	there exists	6
$\forall$	for all	6
$\in$	set membership	11
$\cup$	union	11
$\cap$	intersection	11
c	complement	11
$\subseteq$	subset	13
$\subset$	proper subset	13
$\varnothing$	empty set	13
$\setminus$	difference between sets	13
$\circ$	composition	14
f^{-1}	preimage under f	16
(a, b)	ordered pair	18
$A \times B$	cartesian product	19
$\equiv$	congruence	19, 52
$\binom{n}{k}$	combinations of k objects out of n	26
$\mathbb{Z}$	integers	40
$\mathbb{Z}^+$	positive integers	40
$\mathbb{Q}$	rationals	40
$\mathbb{R}$	reals	40
gcd	greatest common divisor	45
lcm	least common multiple	51
$\mathbb{Z}_m$	integers modulo m	54
μ	Möbius function	64
$\mathbb{N}$	natural numbers	69
$\leq_s$	equal or smaller size	74
$=_s$	same size	74
$\|A\|$	cardinal number of A	77
$\aleph_0$	cardinal number of a countably infinite set	77

Index

AMS / MAA | CLASSROOM RESOURCE MATERIALS

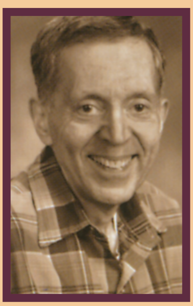
A Primer of Abstract Mathematics

Robert B. Ash

A Primer of Abstract Mathematics prepares the reader to cope with abstract mathematics, specifically abstract algebra. It can serve as a text for prospective mathematics majors, as well as for those students taking or preparing to take a first course in abstract algebra, or those in applied fields who need experience in dealing with abstract mathematical ideas.

Learning any area of abstract mathematics involves writing formal proofs, but it is equally important to think intuitively about the subject and to express ideas clearly and cogently. The author aids intuition by keeping proofs short and as informal as possible, using concrete examples which illustrate all features of the general case, and by giving heuristic arguments when a formal development would take too long. The text can serve as a model on how to write mathematics for an audience with limited experience in formalism and abstraction.

Ash introduces several expository innovations in *A Primer of Abstract Mathematics*. He presents an entirely informal development of set theory that gives students the basic results that they will need in algebra. The chapter which presents the theory of linear operators introduces the Jordan Canonical Form right at the beginning, with a proof of existence at the end of the chapter.



Robert Ash received his PhD in Electrical Engineering from Columbia University. Although he began his career as an electrical engineer, he learned mathematics on his own, and eventually became a mathematician. He taught mathematics at the University of Illinois at Urbana-Champaign and is currently Professor Emeritus. He is the author of several books including: *Information Theory*, *Real Analysis and Probability*, *The Calculus Tutoring Book* (with Carol Ash), *Basic Probability Theory*, *Topics in Stochastic Processes* (with Melvin F. Gardner), *Introduction to Discrete Mathematics* (with Robert J. McEliece and Carol Ash), and *Real Variables with Basic Metric Space Topology*.

www.ams.org