

INSTRUCTOR'S
SOLUTIONS MANUAL

JOHN B. FRALEIGH AND NEAL BRAND

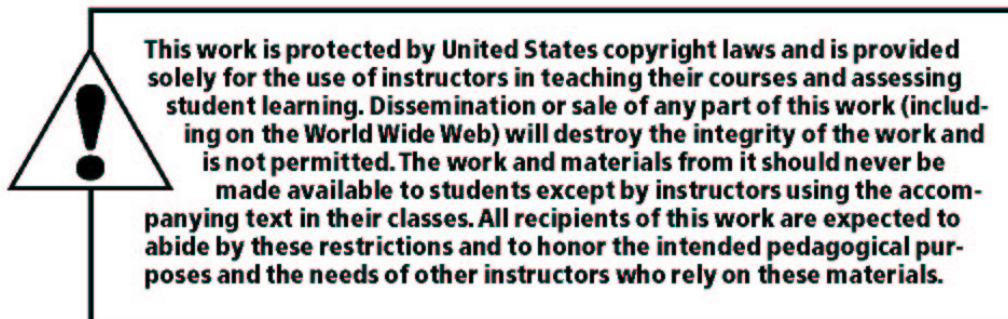
A FIRST COURSE IN
ABSTRACT ALGEBRA

EIGHTH EDITION

John B. Fraleigh
University of Rhode Island

Neal Brand
University of North Texas





The author and publisher of this book have used their best efforts in preparing this book. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness. The author and publisher make no warranty of any kind, expressed or implied, with regard to these programs or the documentation contained in this book. The author and publisher shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of these programs.

Reproduced by Pearson from electronic files supplied by the author.

Copyright © 2021, 2003 by Pearson Education, Inc. 221 River Street, Hoboken, NJ 07030. All rights reserved.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. Printed in the United States of America.



ISBN-13: 978-0-32-139037-0

ISBN-10: 0-321-39037-7

Preface for Seventh Edition

This manual contains solutions to all exercises in the text, except those odd-numbered exercises for which fairly lengthy complete solutions are given in the answers at the back of the text. Then reference is simply given to the text answers to save typing.

I prepared these solutions myself. While I tried to be accurate, there are sure to be the inevitable mistakes and typos. An author reading proof tends to see what he or she wants to see. However, the instructor should find this manual adequate for the purpose for which it is intended.

Morgan, Vermont
July, 2002

J.B.F

Preface for Eighth Edition

In keeping with the seventh edition, this manual contains solutions to all exercises in the text except for some of the odd-numbered exercises whose solutions are in the back of the text book. I made few changes to solutions to exercises that were in the seventh edition. However, solutions to new exercises do not always include as much detail as would be found in the seventh edition. My thinking is that instructors teaching the class would use the solution manual to see the idea behind a solution and they would easily fill in the routine details.

As in the seventh edition, I tried to be accurate. However, there are sure to be some errors. I hope instructors find the manual helpful.

Denton, Texas
March, 2020

N.B.

CONTENTS

0. Sets and Relations	01
-----------------------	----

I. Groups and Subgroups

1. Binary Operations	05
2. Groups	08
3. Abelian Examples	14
4. Nonabelian Examples	19
5. Subgroups	22
6. Cyclic Groups	27
7. Generators and Cayley Digraphs	32

II. Structure of Groups

8. Groups of Permutations	34
9. Finitely Generated Abelian Groups	40
10. Cosets and the Theorem of Lagrange	45
11. Plane Isometries	50

III. Homomorphisms and Factor Groups

12. Factor Groups	53
13. Factor Group Computations and Simple Groups	58
14. Group Action on a Set	65
15. Applications of G-Sets to Counting	70

VI. Advanced Group Theory

16. Isomorphism Theorems	73
17. Sylow Theorems	75
18. Series of Groups	80
19. Free Abelian Groups	85
20. Free Groups	88
21. Group Presentations	91

V. Rings and Fields

- 22. Rings and Fields 95
- 23. Integral Domains 102
- 24. Fermat's and Euler's Theorems 106
- 25. RSA Encryption 109

VI. Constructing Rings and Fields

- 26. The Field of Quotients of an Integral Domain 110
- 27. Rings of Polynomials 112
- 28. Factorization of Polynomials over a Field 116
- 29. Algebraic Coding Theory 123
- 30. Homomorphisms and Factor Rings 125
- 31. Prime and Maximal Ideals 131
- 32. Noncommutative Examples 137

VII. Commutative Algebra

- 33. Vector Spaces 140
- 34. Unique Factorization Domains 145
- 35. Euclidean Domains 149
- 36. Number Theory 154
- 37. Algebraic Geometry 160
- 38. Gröbner Bases for Ideals 163

VIII. Extension Fields

- 39. Introduction to Extension Fields 168
- 40. Algebraic Extensions 174
- 41. Geometric Constructions 179
- 42. Finite Fields 182

IX. Galois Theory

- 43. Automorphisms of Fields 185
- 44. Splitting Fields 191
- 45. Separable Extensions 195
- 46. Galois Theory 199

47. Illustrations of Galois Theory	203
48. Cyclotomic Extensions	211
49. Insolvability of the Quintic	214
APPENDIX: Matrix Algebra	216

0. Sets and Relations

1. $\{\sqrt{3}, -\sqrt{3}\}$
2. $\{2, -3\}$.
3. $\{1, -1, 2, -2, 3, -3, 4, -4, 5, -5, 6, -6, 10, -10, 12, -12, 15, -15, 20, -20, 30, -30, 60, -60\}$
4. $\{2, 3, 4, 5, 6, 7, 8\}$
5. It is not a well-defined set. (Some may argue that no element of $\mathbb{Z}^+$ is large, because every element exceeds only a finite number of other elements but is exceeded by an infinite number of other elements. Such people might claim the answer should be $\emptyset$.)
6. $\emptyset$
7. The set is $\emptyset$ because $3^3 = 27$ and $4^3 = 64$.
8. $\{r \in \mathbb{Q} \mid r = \frac{a}{2^n} \text{ for some } a \in \mathbb{Z}^+ \text{ and some integer } n \geq 0\}$.
9. It is not a well-defined set.
10. The set containing all numbers that are (positive, negative, or zero) integer multiples of 1, $1/2$, or $1/3$.
11. $\{(a, 1), (a, 2), (a, c), (b, 1), (b, 2), (b, c), (c, 1), (c, 2), (c, c)\}$
12. a. This is a function which is both one-to-one and onto B.
 b. This is not a subset of $A \times B$, and therefore not a function.
 c. It is not a function because there are two pairs with first member 1.
 d. This is a function which is neither one-to-one (6 appears twice in the second coordinate) nor onto B (4 is not in the second coordinate).
 e. It is a function. It is not one-to-one because there are two pairs with second member 6. It is not onto B because there is no pair with second member 2.
 f. This is not a function mapping A into B since 3 is not in the first coordinate of any ordered pair.
13. Draw the line through P and x , and let y be its point of intersection with the line segment CD .
14. a. $\phi: [0, 1] \rightarrow [0, 2]$ where $\phi(x) = 2x$
 b. $\phi: [1, 3] \rightarrow [5, 25]$ where $\phi(x) = 2x + 3$
 c. $\phi: [a, b] \rightarrow [c, d]$ where $\phi(x) = c + \frac{d-c}{b-a}(x-a)$
15. Let $\phi: S \rightarrow \mathbb{R}$ be defined by $\phi(x) = \tan(\pi(x - \frac{1}{2}))$.
16. a. $\emptyset$; cardinality 1
 b. $\emptyset, \{a\}$; cardinality 2
 c. $\emptyset, \{a\}, \{b\}, \{a, b\}$; cardinality 4
 d. $\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$; cardinality 8

17. Conjecture: $|P(A)| = 2^s = 2^{|A|}$.

Proof The number of subsets of a set A depends only on the cardinality of A , not on what the elements of A actually are. Suppose $B = \{1, 2, 3, \dots, s-1\}$ and $A = \{1, 2, 3, \dots, s\}$. Then A has all the elements of B plus the one additional element s . All subsets of B are also subsets of A ; these are precisely the subsets of A that do not contain s , so the number of subsets of A not containing s is $|P(B)|$. Any other subset of A must contain s , and removal of the s would produce a subset of B . Thus the number of subsets of A containing s is also $|P(B)|$. Because every subset of A either contains s or does not contain s (but not both), we see that the number of subsets of A is $2|P(B)|$.

We have shown that if A has one more element than B , then $|P(A)| = 2|P(B)|$. Now $|P(\emptyset)| = 1$, so if $|A| = s$, then $|P(A)| = 2^s$.

18. We define a one-to-one map ϕ of B^A onto $P(A)$. Let $f \in B^A$, and let $\phi(f) = \{x \in A \mid f(x) = 1\}$. Suppose $\phi(f) = \phi(g)$. Then $f(x) = 1$ if and only if $g(x) = 1$. Because the only possible values for $f(x)$ and $g(x)$ are 0 and 1, we see that $f(x) = 0$ if and only if $g(x) = 0$. Consequently $f(x) = g(x)$ for all $x \in A$ so $f = g$ and ϕ is one to one. To show that ϕ is onto $P(A)$, let $S \subseteq A$, and let $h : A \rightarrow \{0, 1\}$ be defined by $h(x) = 1$ if $x \in S$ and $h(x) = 0$ otherwise. Clearly $\phi(h) = S$, showing that ϕ is indeed onto $P(A)$.

19. Picking up from the hint, let $Z = \{x \in A \mid x \notin \phi(x)\}$. We claim that for any $a \in A$, $\phi(a) \neq Z$. Either $a \in \phi(a)$, in which case $a \notin Z$, or $a \notin \phi(a)$, in which case $a \in Z$. Thus Z and $\phi(a)$ are certainly different subsets of A ; one of them contains a and the other one does not.

Based on what we just showed, we feel that the power set of A has cardinality greater than $|A|$. Proceeding naively, we can start with the infinite set $\mathbb{Z}$, form its power set, then form the power set of that, and continue this process indefinitely. If there were only a finite number of infinite cardinal numbers, this process would have to terminate after a fixed finite number of steps. Since it doesn't, it appears that there must be an infinite number of different infinite cardinal numbers.

The set of everything is not logically acceptable, because the set of all subsets of the set of everything would be larger than the set of everything, which is a fallacy.

20. a. The set containing precisely the two elements of A and the three (different) elements of B is $C = \{1, 2, 3, 4, 5\}$ which has 5 elements.

i) Let $A = \{-2, -1, 0\}$ and $B = \{1, 2, 3, \dots\} = \mathbb{Z}^+$. Then $|A| = 3$ and $|B| = \aleph_0$, and A and B have no elements in common. The set C containing all elements in either A or B is $C = \{-2, -1, 0, 1, 2, 3, \dots\}$. The map $\phi : C \rightarrow B$ defined by $\phi(x) = x + 3$ is one to one and onto B , so $|C| = |B| = \aleph_0$. Thus we consider $3 + \aleph_0 = \aleph_0$.

ii) Let $A = \{1, 2, 3, \dots\}$ and $B = \{1/2, 3/2, 5/2, \dots\}$. Then $|A| = |B| = \aleph_0$ and A and B have no elements in common. The set C containing all elements in either A or B is $C = \{1/2, 1, 3/2, 2, 5/2, 3, \dots\}$. The map $\phi : C \rightarrow A$ defined by $\phi(x) = 2x$ is one to one and onto A , so $|C| = |A| = \aleph_0$. Thus we consider $\aleph_0 + \aleph_0 = \aleph_0$.

b. We leave the plotting of the points in $A \times B$ to you. Figure 0.15 in the text, where there are $\aleph_0$ rows each having $\aleph_0$ entries, illustrates that we would consider that $\aleph_0 \cdot \aleph_0 = \aleph_0$.