

<https://selldocx.com/products/solution-manual-contemporary-abstract-algebra-9e-gallian-293>
Complete Solutions Manual to Accompany

Contemporary Abstract Algebra

NINTH EDITION

Joseph Gallian

University of Minnesota Duluth

Prepared by

Joseph Gallian

University of Minnesota Duluth



CENGAGE
Learning

Australia • Brazil • Mexico • Singapore • United Kingdom • United States



© 2017 Cengage Learning

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, Web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher except as may be permitted by the license terms below.

For product information and technology assistance, contact us at **Cengage Learning Customer & Sales Support, 1-800-354-9706**.

For permission to use material from this text or product, submit all requests online at www.cengage.com/permissions. Further permissions questions can be emailed to permissionrequest@cengage.com.

ISBN-13: 978-13056579-84

ISBN-10: 0-130565798-5

Cengage Learning

200 First Stamford Place, 4th Floor
Stamford, CT 06902
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: www.cengage.com/global.

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

To learn more about Cengage Learning Solutions, visit www.cengage.com.

Purchase any of our products at your local college store or at our preferred online store www.cengagebrain.com.

READ IMPORTANT LICENSE INFORMATION

Dear Professor or Other Supplement Recipient:

Cengage Learning has provided you with this product (the "Supplement") for your review and, to the extent that you adopt the associated textbook for use in connection with your course (the "Course"), you and your students who purchase the textbook may use the Supplement as described below. Cengage Learning has established these use limitations in response to concerns raised by authors, professors, and other users regarding the pedagogical problems stemming from unlimited distribution of Supplements.

Cengage Learning hereby grants you a nontransferable license to use the Supplement in connection with the Course, subject to the following conditions. The Supplement is for your personal, noncommercial use only and may not be reproduced, posted electronically or distributed, except that portions of the Supplement may be provided to your students IN PRINT FORM ONLY in connection with your instruction of the Course, so long as such students are advised that they may not copy or distribute any portion of the Supplement to any third party. You may not sell, license, auction, or otherwise redistribute the Supplement in any form. We ask that you take reasonable steps to protect the Supplement from unauthorized use, reproduction, or distribution. Your use of the Supplement indicates your acceptance of the conditions set forth in this Agreement. If you do not accept these conditions, you must return the Supplement unused within 30 days of receipt.

All rights (including without limitation, copyrights, patents, and trade secrets) in the Supplement are and will remain the sole and exclusive property of Cengage Learning and/or its licensors. The Supplement is furnished by Cengage Learning on an "as is" basis without any warranties, express or implied. This Agreement will be governed by and construed pursuant to the laws of the State of New York, without regard to such State's conflict of law rules.

Thank you for your assistance in helping to safeguard the integrity of the content contained in this Supplement. We trust you find the Supplement a useful teaching tool.

**CONTEMPORARY ABSTRACT ALGEBRA 9TH EDITION
INSTRUCTOR SOLUTION MANUAL**

CONTENTS

Integers and Equivalence Relations

0 Preliminaries	1
-----------------	---

Groups

1 Introduction to Groups	7
2 Groups	9
3 Finite Groups; Subgroups	13
4 Cyclic Groups	20
5 Permutation Groups	27
6 Isomorphisms	34
7 Cosets and Lagrange's Theorem	40
8 External Direct Products	46
9 Normal Subgroups and Factor Groups	53
10 Group Homomorphisms	59
11 Fundamental Theorem of Finite Abelian Groups	65
12 Introduction to Rings	69
13 Integral Domains	74
14 Ideals and Factor Rings	80
15 Ring Homomorphisms	87
16 Polynomial Rings	94
17 Factorization of Polynomials	100
18 Divisibility in Integral Domains	105

Fields

19	Vector Spaces	110
20	Extension Fields	114
21	Algebraic Extensions	118
22	Finite Fields	123
23	Geometric Constructions	127

Special Topics

24	Sylow Theorems	129
25	Finite Simple Groups	135
26	Generators and Relations	140
27	Symmetry Groups	144
28	Frieze Groups and Crystallographic Groups	146
29	Symmetry and Counting	148
30	Cayley Digraphs of Groups	151
31	Introduction to Algebraic Coding Theory	154
32	An Introduction to Galois Theory	158
33	Cyclotomic Extensions	161

CHAPTER 0

Preliminaries

1. $\{1, 2, 3, 4\}; \{1, 3, 5, 7\}; \{1, 5, 7, 11\}; \{1, 3, 7, 9, 11, 13, 17, 19\};$
 $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$
2. **a.** 2; 10 **b.** 4; 40 **c.** 4; 120; **d.** 1; 1050 **e.** $pq^2; p^2q^3$
3. 12, 2, 2, 10, 1, 0, 4, 5.
4. $s = -3, t = 2; s = 8, t = -5$
5. By using 0 as an exponent if necessary, we may write $a = p_1^{m_1} \cdots p_k^{m_k}$ and $b = p_1^{n_1} \cdots p_k^{n_k}$, where the p 's are distinct primes and the m 's and n 's are nonnegative. Then $\text{lcm}(a, b) = p_1^{s_1} \cdots p_k^{s_k}$, where $s_i = \max(m_i, n_i)$ and $\text{gcd}(a, b) = p_1^{t_1} \cdots p_k^{t_k}$, where $t_i = \min(m_i, n_i)$. Then $\text{lcm}(a, b) \cdot \text{gcd}(a, b) = p_1^{m_1+n_1} \cdots p_k^{m_k+n_k} = ab$.
6. The first part follows from the Fundamental Theorem of Arithmetic; for the second part, take $a = 4, b = 6, c = 12$.
7. Write $a = nq_1 + r_1$ and $b = nq_2 + r_2$, where $0 \leq r_1, r_2 < n$. We may assume that $r_1 \geq r_2$. Then $a - b = n(q_1 - q_2) + (r_1 - r_2)$, where $r_1 - r_2 \geq 0$. If $a \bmod n = b \bmod n$, then $r_1 = r_2$ and n divides $a - b$. If n divides $a - b$, then by the uniqueness of the remainder, we then have $r_1 - r_2 = 0$. Thus, $r_1 = r_2$ and therefore $a \bmod n = b \bmod n$.
8. Write $as + bt = d$. Then $a's + b't = (a/d)s + (b/d)t = 1$.
9. By Exercise 7, to prove that $(a + b) \bmod n = (a' + b') \bmod n$ and $(ab) \bmod n = (a'b') \bmod n$ it suffices to show that n divides $(a + b) - (a' + b')$ and $ab - a'b'$. Since n divides both $a - a'$ and n divides $b - b'$, it divides their difference. Because $a = a' \bmod n$ and $b = b' \bmod n$ there are integers s and t such that $a = a' + ns$ and $b = b' + nt$. Thus $ab = (a' + ns)(b' + nt) = a'b' + nsb' + a'nt + nsnt$. Thus, $ab - a'b'$ is divisible by n .
10. Write $d = au + bv$. Since t divides both a and b , it divides d . Write $s = mq + r$ where $0 \leq r < m$. Then $r = s - mq$ is a common multiple of both a and b so $r = 0$.
11. Suppose that there is an integer n such that $ab \bmod n = 1$. Then there is an integer q such that $ab - nq = 1$. Since d divides both a and n , d also divides 1. So, $d = 1$. On the other hand, if $d = 1$, then by the corollary of Theorem 0.2, there are integers s and t such that $as + nt = 1$. Thus, modulo n , $as = 1$.

12. $7(5n + 3) - 5(7n + 4) = 1$
13. By the GCD Theorem there are integers s and t such that $ms + nt = 1$.
Then $m(sr) + n(tr) = r$.
14. It suffices to show that $(p^2 + q^2 + r^2) \bmod 3 = 0$. Notice that for any integer a not divisible by 3, $a \bmod 3$ is 1 or 2 and therefore $a^2 \bmod 3 = 1$. So, $(p^2 + q^2 + r^2) \bmod 3 = p^2 \bmod 3 + q^2 \bmod 3 + r^2 \bmod 3 = 3 \bmod 3 = 0$.
15. Let p be a prime greater than 3. By the Division Algorithm, we can write p in the form $6n + r$, where r satisfies $0 \leq r < 6$. Now observe that $6n, 6n + 2, 6n + 3$, and $6n + 4$ are not prime.
16. By properties of modular arithmetic we have
 $(7^{1000}) \bmod 6 = (7 \bmod 6)^{1000} = 1^{1000} = 1$. Similarly,
 $(6^{1001}) \bmod 7 = (6 \bmod 7)^{1001} = -1^{1001} \bmod 7 = -1 = 6 \bmod 7$.
17. Since st divides $a - b$, both s and t divide $a - b$. The converse is true when $\gcd(s, t) = 1$.
18. Observe that $8^{402} \bmod 5 = 3^{402} \bmod 5$ and $3^4 \bmod 5 = 1$. Thus, $8^{402} \bmod 5 = (3^4)^{100} 3^2 \bmod 5 = 4$.
19. If $\gcd(a, bc) = 1$, then there is no prime that divides both a and bc . By Euclid's Lemma and unique factorization, this means that there is no prime that divides both a and b or both a and c . Conversely, if no prime divides both a and b or both a and c , then by Euclid's Lemma, no prime divides both a and bc .
20. If one of the primes did divide $k = p_1 p_2 \cdots p_n + 1$, it would also divide 1.
21. Suppose that there are only a finite number of primes $p_1, p_2, \dots, p_n$. Then, by Exercise 20, $p_1 p_2 \cdots p_n + 1$ is not divisible by any prime. This means that $p_1 p_2 \cdots p_n + 1$, which is larger than any of $p_1, p_2, \dots, p_n$, is itself prime. This contradicts the assumption that $p_1, p_2, \dots, p_n$ is the list of all primes.
22. $\frac{-7}{58} + \frac{3}{58}i$
23. $\frac{-5+2i}{4-5i} = \frac{-5+2i}{4-5i} \frac{4+5i}{4+5i} = \frac{-30}{41} + \frac{-17}{41}i$
24. Let $z_1 = a + bi$ and $z_2 = c + di$. Then $z_1 z_2 = (ac - bd) + (ad + bc)i$; $|z_1| = \sqrt{a^2 + b^2}$, $|z_2| = \sqrt{c^2 + d^2}$, $|z_1 z_2| = \sqrt{a^2 c^2 + b^2 d^2 + a^2 d^2 + b^2 c^2} = |z_1| |z_2|$.
25. $x \text{ NAND } y$ is 1 if and only if both inputs are 0; $x \text{ XNOR } y$ is 1 if and only if both inputs are the same.
26. If $x = 1$, the output is y , else it is z .

27. Let S be a set with $n + 1$ elements and pick some a in S . By induction, S has 2^n subsets that do not contain a . But there is one-to-one correspondence between the subsets of S that do not contain a and those that do. So, there are $2 \cdot 2^n = 2^{n+1}$ subsets in all.
28. Use induction and note that

$$2^{n+1}3^{2n+2} - 1 = 18(2^n3^{2n}) - 1 = 18(2^n3^{3n} - 1) + 17.$$
29. Consider $n = 200! + 2$. Then 2 divides n , 3 divides $n + 1$, 4 divides $n + 2, \dots$, and 202 divides $n + 200$.
30. Use induction on n .
31. Say $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, where the p 's and the q 's are primes. By the Generalized Euclid's Lemma, p_1 divides some q_i , say q_1 (we may relabel the q 's if necessary). Then $p_1 = q_1$ and $p_2 \cdots p_r = q_2 \cdots q_s$. Repeating this argument at each step we obtain $p_2 = q_2, \dots, p_r = q_r$ and $r = s$.
32. 47. Mimic Example 12.
33. Suppose that S is a set that contains a and whenever $n \geq a$ belongs to S , then $n + 1 \in S$. We must prove that S contains all integers greater than or equal to a . Let T be the set of all integers greater than a that are not in S and suppose that T is not empty. Let b be the smallest integer in T (if T has no negative integers, b exists because of the Well Ordering Principle; if T has negative integers, it can have only a finite number of them so that there is a smallest one). Then $b - 1 \in S$, and therefore $b = (b - 1) + 1 \in S$. This contradicts our assumption that b is not in S .
34. By the Second Principle of Mathematical Induction,

$$f_n = f_{n-1} + f_{n-2} < 2^{n-1} + 2^{n-2} = 2^{n-2}(2 + 1) < 2^n.$$
35. For $n = 1$, observe that $1^3 + 2^3 + 3^3 = 36$. Assume that

$$n^3 + (n + 1)^3 + (n + 2)^3 = 9m \text{ for some integer } m.$$
We must prove that $(n + 1)^3 + (n + 2)^3 + (n + 3)^3$ is a multiple of 9. Using the induction hypothesis we have that

$$(n + 1)^3 + (n + 2)^3 + (n + 3)^3 = 9m - n^3 + (n + 3)^3 = 9m - n^3 + n^3 + 3 \cdot n^2 \cdot 3 + 3 \cdot n \cdot 9 + 3^3 = 9m + 9n^2 + 27n + 27 = 9(m + n^2 + 3n + 3).$$
36. You must verify the cases $n = 1$ and $n = 2$. This situation arises in cases where the arguments that the statement is true for n implies that it is true for $n + 2$ is different when n is even and when n is odd.
37. The statement is true for any divisor of $8^3 - 4 = 508$.
38. One need only verify the equation for $n = 0, 1, 2, 3, 4, 5$. Alternatively, observe that $n^3 - n = n(n - 1)(n + 1)$.
39. Since $3736 \bmod 24 = 16$, it would be 6 p.m.

40. 5

41. Observe that the number with the decimal representation $a_9a_8 \dots a_1a_0$ is $a_910^9 + a_810^8 + \dots + a_110 + a_0$. From Exercise 9 and the fact that $a_i10^i \bmod 9 = a_i \bmod 9$ we deduce that the check digit is $(a_9 + a_8 + \dots + a_1 + a_0) \bmod 9$. So, substituting 0 for 9 or vice versa for any a_i does not change the value of $(a_9 + a_8 + \dots + a_1 + a_0) \bmod 9$.

42. No

43. For the case in which the check digit is not involved, the argument given Exercise 41 applies to transposition errors. Denote the money order number by $a_9a_8 \dots a_1a_0c$ where c is the check digit. For a transposition involving the check digit $c = (a_9 + a_8 + \dots + a_0) \bmod 9$ to go undetected, we must have $a_0 = (a_9 + a_8 + \dots + a_1 + c) \bmod 9$. Substituting for c yields $2(a_9 + a_8 + \dots + a_0) \bmod 9 = a_0$. Then cancelling the a_0 , multiplying by sides by 5, and reducing module 9, we have $10(a_9 + a_8 + \dots + a_1) = a_9 + a_8 + \dots + a_1 = 0$. It follows that $c = a_9 + a_8 + \dots + a_1 + a_0 = a_0$. In this case the transposition does not yield an error.

44. 4

45. Say the number is $a_8a_7 \dots a_1a_0 = a_810^8 + a_710^7 + \dots + a_110 + a_0$. Then the error is undetected if and only if $(a_i10^i - a'_i10^i) \bmod 7 = 0$. Multiplying both sides by 5^i and noting that $50 \bmod 7 = 1$, we obtain $(a_i - a'_i) \bmod 7 = 0$.

46. All except those involving a and b with $|a - b| = 7$.

47. 4

48. Observe that for any integer k between 0 and 8, $k \div 9 = .kkk\dots$

50. 7

51. Say that the weight for a is i . Then an error is undetected if modulo 11, $ai + b(i - 1) + c(i - 2) = bi + c(i - 1) + a(i - 2)$. This reduces to the cases where $(2a - b - c) \bmod 11 = 0$.

52. Say the valid number is $a_1a_2 \dots a_{10}$ and a_i and a_{i+1} were transposed. Then, modulo 11, $10a_1 + 9a_2 + \dots + a_{10} = 0$ and $10a_1 + \dots + (11 - i)a_{i+1} + (11 - (i + 1))a_i + \dots + a_{10} = 5$. Thus, $5 = 5 - 0 = (10a_1 + \dots + (11 - i)a_{i+1} + (11 - (i + 1))a_i + a_{10}) - (10a_1 + 9a_2 + \dots + a_{10})$. It follows that $(a_{i+1} - a_i) \bmod 11 = 5$. Now look for adjacent digits x and y in the invalid number so that $(x - y) \bmod 11 = 5$. Since the only pair is 39, the correct number is 0-669-09325-4.

53. Since $10a_1 + 9a_2 + \cdots + a_{10} = 0 \pmod{11}$ if and only if
 $0 = (-10a_1 - 9a_2 - \cdots - 10a_{10}) \pmod{11} = (a_1 + 2a_2 + \cdots + 10a_{10}) \pmod{11}$,
the check digit would be the same.
54. 7344586061
55. First note that the sum of the digits modulo 11 is 2. So, some digit is 2 too large. Say the error is in position i . Then
 $10 = (4, 3, 0, 2, 5, 1, 1, 5, 6, 8) \cdot (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \pmod{11} = 2i$. Thus,
the digit in position 5 to 2 too large. So, the correct number is 4302311568.
56. An error in an even numbered position changes the value of the sum by an even amount. However,
 $(9 \cdot 1 + 8 \cdot 4 + 7 \cdot 9 + 6 \cdot 1 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 2 + 2 \cdot 6 + 7) \pmod{10} = 5$.
57. 2. Since β is one-to-one, $\beta(\alpha(a_1)) = \beta(\alpha(a_2))$ implies that $\alpha(a_1) = \alpha(a_2)$
and since α is one-to-one, $a_1 = a_2$.
3. Let $c \in C$. There is a b in B such that $\beta(b) = c$ and an a in A such that
 $\alpha(a) = b$. Thus, $(\beta\alpha)(a) = \beta(\alpha(a)) = \beta(b) = c$.
4. Since α is one-to-one and onto we may define $\alpha^{-1}(x) = y$ if and only if
 $\alpha(y) = x$. Then $\alpha^{-1}(\alpha(a)) = a$ and $\alpha(\alpha^{-1}(b)) = b$.
58. $a - a = 0$; if $a - b$ is an integer k then $b - a$ is the integer $-k$; if $a - b$ is
the integer n and $b - c$ is the integer m , then $a - c = (a - b) + (b - c)$ is
the integer $n + m$. The set of equivalence classes is
 $\{[k] \mid 0 \leq k < 1, \ k \text{ is real}\}$. The equivalence classes can be represented by
the real numbers in the interval $[0, 1)$. For any real number a , $[a] = \{a + k \mid$
where k ranges over all integers $\}$.
59. No. $(1, 0) \in R$ and $(0, -1) \in R$ but $(1, -1) \notin R$.
60. Obviously, $a + a = 2a$ is even and $a + b$ is even implies $b + a$ is even. If
 $a + b$ and $b + c$ are even, then $a + c = (a + b) + (b + c) - 2b$ is also even. The
equivalence classes are the set of even integers and the set of odd integers.
61. a belongs to the same subset as a . If a and b belong to the subset A and b
and c belong to the subset B , then $A = B$, since the distinct subsets of P
are disjoint. So, a and c belong to A .
62. Suppose that n is odd prime greater than 3 and $n + 2$ and $n + 4$ are also
prime. Then $n \pmod{3} = 1$ or $n \pmod{3} = 2$. If $n \pmod{3} = 1$ then
 $n + 2 \pmod{3} = 0$ and so is not prime. If $n \pmod{3} = 2$ then $n + 4 \pmod{3} = 0$
and so is not prime.

63. The last digit of 3^{100} is the value of $3^{100} \bmod 10$. Observe that $3^{100} \bmod 10$ is the same as $((3^4 \bmod 10)^{25} \bmod 10$ and $3^4 \bmod 10 = 1$. Similarly, the last digit of 2^{100} is the value of $2^{100} \bmod 10$. Observe that $2^5 \bmod 10 = 2$ so that $2^{100} \bmod 10$ is the same as $(2^5 \bmod 10)^{20} \bmod 10 = 2^{20} \bmod 10 = (2^5)^4 \bmod 10 = 2^4 \bmod 10 = 6$.
64. Suppose that there are integers a, b, c , and d with $\gcd(a, b) = 1$ and $\gcd(c, d) = 1$ such that $a^2/b^2 - c^2/d^2 = 1002$. Then $a^2d^2 - c^2b^2 = 1002b^2d^2$. If both b and d are odd, then modulo 4, $b^2 = d^2 = 1$ and $a^2/b^2 - c^2/d^2 = 1002$ reduces to $a^2 - c^2 = 2$. This case is handled in Example 7. If 2^i ($i > 0$) divides b , then a is odd and $a^2d^2 - c^2b^2 = 1002b^2d^2$ implies that 2^i divides d also. It follows that if 2^n is the highest power of 2 that divides one of b or d , then 2^n is the highest power of 2 that divides the other. So dividing both sides of $a^2d^2 - c^2b^2 = 1002b^2d^2$ by 2^n we get an equation of the same form where both b and d are odd. Taking both sides modulo 4 and recalling that for odd x , $x^2 \bmod 4 = 1$ we have that $a^2d^2 - c^2b^2 = 1002b^2d^2$ reduces to $a^2 - c^2 = 2$, which was done in Example 7.
65. Apply γ^{-1} to both sides of $\alpha\gamma = \beta\gamma$.

CHAPTER 1

Introduction to Groups

1. Three rotations: 0° , 120° , 240° , and three reflections across lines from vertices to midpoints of opposite sides.
2. Let $R = R_{120}$, $R^2 = R_{240}$, F a reflection across a vertical axis, $F' = RF$ and $F'' = R^2F$

	R_0	R	R^2	F	F'	F''
R_0	R_0	R	R^2	F	F'	F''
R	R	R^2	R_0	F'	F''	F
R^2	R^2	R_0	R	F''	F	F'
F	F	F''	F'	R_0	R^2	R
F'	F'	F	F''	R	R_0	R^2
F''	F''	F'	F	R^2	R	R_0

3. **a.** V **b.** R_{270} **c.** R_0 **d.** $R_0, R_{180}, H, V, D, D'$ **e.** none
4. Five rotations: 0° , 72° , 144° , 216° , 288° , and five reflections across lines from vertices to midpoints of opposite sides.
5. D_n has n rotations of the form $k(360^\circ/n)$, where $k = 0, \dots, n-1$. In addition, D_n has n reflections. When n is odd, the axes of reflection are the lines from the vertices to the midpoints of the opposite sides. When n is even, half of the axes of reflection are obtained by joining opposite vertices; the other half, by joining midpoints of opposite sides.
6. A nonidentity rotation leaves only one point fixed – the center of rotation. A reflection leaves the axis of reflection fixed. A reflection followed by a different reflection would leave only one point fixed (the intersection of the two axes of reflection) so it must be a rotation.
7. A rotation followed by a rotation either fixes every point (and so is the identity) or fixes only the center of rotation. However, a reflection fixes a line.
8. In either case, the set of points fixed is some axis of reflection.
9. Observe that $1 \cdot 1 = 1$; $1(-1) = -1$; $(-1)1 = -1$; $(-1)(-1) = 1$. These relationships also hold when 1 is replaced by a “rotation” and -1 is replaced by a “reflection.”
10. reflection.

11. Thinking geometrically and observing that even powers of elements of a dihedral group do not change orientation we note that each of a, b and c appears an even number of times in the expression. So, there is no change in orientation. Thus, the expression is a rotation. Alternatively, as in Exercise 9, we associate each of a, b and c with 1 if they are rotations and -1 if they are reflections and we observe that in the product $a^2b^4ac^5a^3c$ the terms involving a represents six 1s or six -1 s, the term b^4 represents four 1s or four -1 s, and the terms involving c represents six 1s or six -1 s. Thus the product of all the 1s and -1 s is 1. So the expression is a rotation.
12. H, I, O, X. Rotations of $0^\circ, 180^\circ$, horizontal reflection, and vertical reflection.
13. In D_4 , $HD = DV$ but $H \neq V$.
14. D_n is not commutative.
15. R_0, R_{180}, H, V
16. Rotations of 0° and 180° ; Rotations of 0° and 180° and reflections about the diagonals.
17. R_0, R_{180}, H, V
18. Let the distance from a point on one H to the corresponding point on an adjacent H be one unit. Then translations of any number of units to the right or left are symmetries; reflection across the horizontal axis through the middle of the H 's is a symmetry; reflection across any vertical axis midway between two H 's or bisecting any H is a symmetry. All other symmetries are compositions of finitely many of those already described. The group is non-Abelian.
19. In each case the group is D_6 .
20. D_{28}
21. First observe that $X^2 \neq R_0$. Since R_0 and R_{180} are the only elements in D_4 that are squares we have $X^2 = R_{180}$. Solving $X^2Y = R_{90}$ for Y gives $Y = R_{270}$.
22. $X^2 = F$ has no solutions; the only solution to $X^3 = F$ is F .
23. 180° rotational symmetry.
24. Z_4, D_5, D_4, Z_2
 D_4, Z_3, D_3, D_{16}
 D_7, D_4, D_5, Z_{10}
25. Their only symmetry is the identity.

CHAPTER 2

Groups

1. **c, d**
2. **c, d**
3. none
4. **a, c**
5. $7; 13; n-1; \frac{1}{3-2i} = \frac{1}{3-2i} \frac{3+2i}{3+2i} = \frac{3}{13} + \frac{2}{13}i$
6. **a.** $-31-i$ **b.** 5 **c.** $\frac{1}{12} \begin{bmatrix} 2 & -3 \\ -8 & 6 \end{bmatrix}$ **d.** $\begin{bmatrix} 2 & 4 \\ 4 & 6 \end{bmatrix}$.
7. The set does not contain the identity; closure fails.
8. 1, 3, 7, 9, 11, 13, 17, 19.
9. Under multiplication modulo 4, 2 does not have an inverse. Under multiplication modulo 5, $\{1, 2, 3, 4\}$ is closed, 1 is the identity, 1 and 4 are their own inverses, and 2 and 3 are inverses of each other. Modulo multiplication is associative.
10. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$.
11. a^{11}, a^6, a^4, a^1
12. 5, 4, 8
13. (a) $2a + 3b$; (b) $-2a + 2(-b + c)$; (c) $-3(a + 2b) + 2c = 0$
14. $(ab)^3 = ababab$ and $(ab^{-2}c)^{-2} = ((ab^{-2}c)^{-1})^2 = (c^{-1}b^2a^{-1})^2 = c^{-1}b^2a^{-1}c^{-1}b^2a^{-1}$.
15. Observe that $a^5 = e$ implies that $a^{-2} = a^3$ and $b^7 = e$ implies that $b^{14} = e$ and therefore $b^{-11} = b^3$. Thus, $a^{-2}b^{-11} = a^3b^3$. Moreover, $(a^2b^4)^{-2} = ((a^2b^4)^{-1})^2 = (b^{-4}a^{-2})^2 = (b^3a^3)^2$.
16. The identity is 25.
17. Since the inverse of an element in G is in G , $H \subseteq G$. Let g belong to G . Then g^{-1} belongs to G and therefore $(g^{-1})^{-1} = g$ belong to G . So, $G \subseteq H$.
18. $K = \{R_0, R_{180}\}$; $L = \{R_0, R_{180}, H, V, D, D'\}$.

19. The set is closed because $\det(AB) = (\det A)(\det B)$. Matrix multiplication is associative. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity.
- Since $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ its determinant is $ad - bc = 1$.
20. $1^2 = (n-1)^2 = 1$.
21. Using closure and trial and error, we discover that $9 \cdot 74 = 29$ and 29 is not on the list.
22. Consider $xyx = xyx$.
23. For $n \geq 0$, we use induction. The case that $n = 0$ is trivial. Then note that $(ab)^{n+1} = (ab)^n ab = a^n b^n ab = a^{n+1} b^{n+1}$. For $n < 0$, note that $e = (ab)^0 = (ab)^n (ab)^{-n} = (ab)^n a^{-n} b^{-n}$ so that $a^n b^n = (ab)^n$. In a non-Abelian group $(ab)^n$ need not equal $a^n b^n$.
24. The “inverse” of putting on your socks and then putting on your shoes is taking off your shoes then taking off your socks. Use D_4 for the examples. (An appropriate name for the property $(abc)^{-1} = c^{-1}b^{-1}a^{-1}$ is “Socks-Shoes-Boots Property.”)
25. Suppose that G is Abelian. Then by Exercise 24, $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$. If $(ab)^{-1} = a^{-1}b^{-1}$ then by Exercise 24 $e = aba^{-1}b^{-1}$. Multiplying both sides on the right by ba yields $ba = ab$.
26. By definition, $a^{-1}(a^{-1})^{-1} = e$. Now multiply on the left by a .
27. The case where $n = 0$ is trivial. For $n > 0$, note that $(a^{-1}ba)^n = (a^{-1}ba)(a^{-1}ba) \cdots (a^{-1}ba)$ (n terms). So, cancelling the consecutive a and a^{-1} terms gives $a^{-1}b^n a$. For $n < 0$, note that $e = (a^{-1}ba)^n (a^{-1}ba)^{-n} = (a^{-1}ba)^n (a^{-1}b^{-n}a)$ and solve for $(a^{-1}ba)^n$.
28. $(a_1 a_2 \cdots a_n)(a_n^{-1} a_{n-1}^{-1} \cdots a_2^{-1} a_1^{-1}) = e$
29. By closure we have $\{1, 3, 5, 9, 13, 15, 19, 23, 25, 27, 39, 45\}$.
30. Z_{105} ; Z_{44} and D_{22} .
31. Suppose x appears in a row labeled with a twice. Say $x = ab$ and $x = ac$. Then cancellation gives $b = c$. But we use distinct elements to label the columns.
- 32.
- | | 1 | 5 | 7 | 11 |
|----|----|----|----|----|
| 1 | 1 | 5 | 7 | 11 |
| 5 | 5 | 1 | 11 | 7 |
| 7 | 7 | 11 | 1 | 5 |
| 11 | 11 | 7 | 5 | 1 |

33. Proceed as follows. By definition of the identity, we may complete the first row and column. Then complete row 3 and column 5 by using Exercise 31. In row 2 only c and d remain to be used. We cannot use d in position 3 in row 2 because there would then be two d 's in column 3. This observation allows us to complete row 2. Then rows 3 and 4 may be completed by inserting the unused two elements. Finally, we complete the bottom row by inserting the unused column elements.
34. $(ab)^2 = a^2b^2 \Leftrightarrow abab = aabb \Leftrightarrow ba = ab$.
 $(ab)^{-2} = b^{-2}a^{-2} \Leftrightarrow b^{-1}a^{-1}b^{-1}a^{-1} = b^{-1}b^{-1}a^{-1}a^{-1} \Leftrightarrow a^{-1}b^{-1} = b^{-1}a^{-1} \Leftrightarrow ba = ab$.
35. $axb = c$ implies that $x = a^{-1}(axb)b^{-1} = a^{-1}cb^{-1}$; $a^{-1}xa = c$ implies that $x = a(a^{-1}xa)a^{-1} = aca^{-1}$.
36. Observe that $xabx^{-1} = ba$ is equivalent to $xab = bax$ and this is true for $x = b$.
37. Since e is one solution it suffices to show that nonidentity solutions come in distinct pairs. To this end note that if $x^3 = e$ and $x \neq e$, then $(x^{-1})^3 = e$ and $x \neq x^{-1}$. So if we can find one nonidentity solution we can find a second one. Now suppose that a and a^{-1} are nonidentity elements that satisfy $x^3 = e$ and b is a nonidentity element such that $b \neq a$ and $b \neq a^{-1}$ and $b^3 = e$. Then, as before, $(b^{-1})^3 = e$ and $b \neq b^{-1}$. Moreover, $b^{-1} \neq a$ and $b^{-1} \neq a^{-1}$. Thus, finding a third nonidentity solution gives a fourth one. Continuing in this fashion we see that we always have an even number of nonidentity solutions to the equation $x^3 = e$.
 To prove the second statement note that if $x^2 \neq e$, then $x^{-1} \neq x$ and $(x^{-1})^2 \neq e$. So, arguing as in the preceding case we see that solutions to $x^2 \neq e$ come in distinct pairs.
38. In D_4 , $HR_{90}V = DR_{90}H$ but $HV \neq DH$.
39. Observe that $aa^{-1}b = ba^{-1}a$. Cancelling the middle term a^{-1} on both sides we obtain $ab = ba$.
40. $X = VR_{270}D'H$.
41. If $F_1F_2 = R_0$ then $F_1F_2 = F_1F_1$ and by cancellation $F_1 = F_2$.
42. Observe that $F_1F_2 = F_2F_1$ implies that $(F_1F_2)(F_1F_2) = R_0$. Since F_1 and F_2 are distinct and F_1F_2 is a rotation it must be R_{180} .
43. Since FR^k is a reflection we have $(FR^k)(FR^k) = R_0$. Multiplying on the left by F gives $R^kFR^k = F$.
44. Since FR^k is a reflection we have $(FR^k)(FR^k) = R_0$. Multiplying on the right by R^{-k} gives $FR^kF = R^{-k}$. If D_n were Abelian, then $FR_{360^\circ/n}F = R_{360^\circ/n}$. But $(R_{360^\circ/n})^{-1} = R_{360^\circ(n-1)/n} \neq R_{360^\circ/n}$ when $n \geq 3$.

45. **a.** R^3 **b.** R **c.** R^5F
46. Closure and associativity follow from the definition of multiplication; $a = b = c = 0$ gives the identity; we may find inverses by solving the equations $a + a' = 0$, $b' + ac' + b = 0$, $c' + c = 0$ for a', b', c' .
47. Since $a^2 = b^2 = (ab)^2 = e$, we have $aabb = abab$. Now cancel on left and right.
48. If a satisfies $x^5 = e$ and $a \neq e$, then so does a^2, a^3, a^4 . Now, using cancellation we have that a^2, a^3, a^4 are not the identity and are distinct from each other and distinct from a . If these are all of the nonidentity solutions of $x^5 = e$ we are done. If b is another solution that is not a power of a , then by the same argument b, b^2, b^3 and b^4 are four distinct nonidentity solutions. We must further show that b^2, b^3 and b^4 are distinct from a, a^2, a^3, a^4 . If $b^2 = a^i$ for some i , then cubing both sides we have $b = b^6 = a^{3i}$, which is a contradiction. A similar argument applies to b^3 and b^4 . Continuing in this fashion we have that the number of nonidentity solutions to $x^5 = e$ is a multiple of 4. In the general case, the number of solutions is a multiple of 4 or is infinite.
49. The matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is in $\text{GL}(2, Z_2)$ if and only if $ad \neq bc$. This happens when a and d are 1 and at least 1 of b and c is 0 and when b and c are 1 and at least 1 of a and d is 0. So, the elements are
- $$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$
- $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ and $\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ do not commute.
50. If n is not prime, we can write $n = ab$, where $1 < a < n$ and $1 < b < n$. Then a and b belong to the set $\{1, 2, \dots, n-1\}$ but $0 = ab \bmod n$ does not.
51. Let a be any element in G and write $x = ea$. Then $a^{-1}x = a^{-1}(ea) = (a^{-1}e)a = a^{-1}a = e$. Then solving for x we obtain $x = ae = a$.
52. Suppose that $ab = e$ and let b' be the element in G with the property that $bb' = e$. Then observe that $ba = (ba)e = ba(bb') = b(ab)b' = beb' = (be)b' = bb' = e$.

CHAPTER 3

Finite Groups; Subgroups

1. $|Z_{12}| = 12$; $|U(10)| = 4$; $|U(12)| = 4$; $|U(20)| = 8$; $|D_4| = 8$.
 In Z_{12} , $|0| = 1$; $|1| = |5| = |7| = |11| = 12$; $|2| = |10| = 6$; $|3| = |9| = 4$; $|4| = |8| = 3$; $|6| = 2$.
 In $U(10)$, $|1| = 1$; $|3| = |7| = 4$; $|9| = 2$.
 In $U(20)$, $|1| = 1$; $|3| = |7| = |13| = |17| = 4$; $|9| = |11| = |19| = 2$.
 In D_4 , $|R_0| = 1$; $|R_{90}| = |R_{270}| = 4$; $|R_{180}| = |H| = |V| = |D| = |D'| = 2$.
 In each case, notice that the order of the element divides the order of the group.
2. In Q , $\langle 1/2 \rangle = \{n(1/2) \mid n \in Z\} = \{0, \pm 1/2, \pm 1, \pm 3/2, \dots\}$. In Q^* ,
 $\langle 1/2 \rangle = \{(1/2)^n \mid n \in Z\} = \{1, 1/2, 1/4, 1/8, \dots; 2, 4, 8, \dots\}$.
3. In Q , $|0| = 1$. All other elements have infinite order since
 $x + x + \dots + x = 0$ only when $x = 0$.
4. Suppose $|a| = n$ and $|a^{-1}| = k$. Then $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. So
 $k \leq n$. Now reverse the roles of a and a^{-1} to obtain $n \leq k$. The infinite
 case follows from the finite case.
5. In Z_{30} , $2 + 28 = 0$ and $8 + 22 = 0$. So, 2 and 28 are inverses of each other
 and 8 and 22 are inverses of each other. In $U(15)$, $2 \cdot 8 = 1$ and $7 \cdot 13 = 1$.
 So, 2 and 8 are inverses of each other and 7 and 13 are inverses of each
 other.
6. **a.** $|6| = 2, |2| = 6, |8| = 3$; **b.** $|3| = 4, |8| = 5, |11| = 12$;
c. $|5| = 12, |4| = 3, |9| = 4$. In each case $|a + b|$ divides $\text{lcm}(|a|, |b|)$.
7. $(a^4c^{-2}b^4)^{-1} = b^{-4}c^2a^{-4} = b^3c^2a^2$.
8. If a subgroup of D_3 contains R_{240} and F it also contains
 $R_0, R_{240}^2 = R_{120}, R_{240}F$, and $R_{120}F$, which is all six elements of D_3 . If F
 and F' are distinct reflections in a subgroup of D_3 , then $FF' = R_{240}$ is
 also in the subgroup. Thus the subgroup must be D_3 .
9. If a subgroup of D_4 contains R_{270} and a reflection F , then it also contains
 the six other elements $R_0, (R_{270})^2 = R_{180}, (R_{270})^3 = R_{90}, R_{270}F, R_{180}F$
 and $R_{90}F$. If a subgroup of D_4 contains H and D , then it also contains
 $HD = R_{90}$ and $DH = R_{270}$. But this implies that the subgroup contains
 every element of D_4 . If it contains H and V then it contains $HV = R_{180}$
 and R_0 .