

Complete Solutions Manual to Accompany

Contemporary Abstract Algebra

NINTH EDITION

Joseph Gallian

University of Minnesota Duluth

Prepared by

Joseph Gallian

University of Minnesota Duluth



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

- $\{1, 2, 3, 4\}$; $\{1, 3, 5, 7\}$; $\{1, 5, 7, 11\}$; $\{1, 3, 7, 9, 11, 13, 17, 19\}$;
 $\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$
- a.** 2; 10 **b.** 4; 40 **c.** 4; 120; **d.** 1; 1050 **e.** pq^2 ; p^2q^3
- 12, 2, 2, 10, 1, 0, 4, 5.
- $s = -3$, $t = 2$; $s = 8$, $t = -5$
- 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 $\text{lcm}(a, b) \cdot \text{gcd}(a, b) = p_1^{m_1+n_1} \cdots p_k^{m_k+n_k} = ab$.
- The first part follows from the Fundamental Theorem of Arithmetic; for the second part, take $a = 4$, $b = 6$, $c = 12$.
- 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 $a \bmod n = b \bmod n$.
- Write $as + bt = d$. Then $a's + b't = (a/d)s + (b/d)t = 1$.
- 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 .
- 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 $r = 0$.
- 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 , $as = 1$.

CHAPTER 8

External Direct Products

1. Closure and associativity in the product follows from the closure and associativity in each component. The identity in the product is the n -tuple with the identity in each component. The inverse of (g_1, g_2, \dots, g_n) is $(g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$.
2. In general, $(1, 1, \dots, 1)$ is an element of largest order in $Z_{n_1} \oplus Z_{n_2} \oplus \dots \oplus Z_{n_t}$. To see this note that because the order of the 1 in each component is the order of the group in that component, $|(1, 1, \dots, 1)| = \text{lcm}(n_1, n_2, \dots, n_t)$ and the order of every element in the product must divide $\text{lcm}(n_1, n_2, \dots, n_t)$.
3. The mapping $\phi(g) = (g, e_H)$ is an isomorphism from G to $G \oplus \{e_H\}$. To verify that ϕ is one-to-one, we note that $\phi(g) = \phi(g')$ implies $(g, e_H) = (g', e_H)$ which means that $g = g'$. The element $(g, e_H) \in G \oplus \{e_H\}$ is the image of g . Finally, $\phi((g, e_H)(g', e_H)) = \phi((gg', e_H e_H)) = \phi((gg', e_H)) = gg' = \phi((g, e_H))\phi((g', e_H))$. A similar argument shows that $\phi(h) = (e_G, h)$ is an isomorphism from H onto $\{e_G\} \oplus H$.
4. $(g, h)(g', h') = (g', h')(g, h)$ for all g, g', h, h' if and only if $gg' = g'g$ and $hh' = h'h$, that is, if and only if G and H are Abelian. A corresponding statement holds for the external direct product of any number of groups.
5. If $Z \oplus Z = \langle\langle a, b \rangle\rangle$ then neither a nor b is 0. But then $(1, 0) \notin \langle\langle a, b \rangle\rangle$. $Z \oplus G$ is not cycle when $|G| > 1$.
6. $Z_8 \oplus Z_2$ contains elements of order 8, while $Z_4 \oplus Z_4$ does not.
7. Define a mapping from $G_1 \oplus G_2$ to $G_2 \oplus G_1$ by $\phi(g_1, g_2) = (g_2, g_1)$. To verify that ϕ is one-to-one, we note that $\phi((g_1, g_2)) = \phi((g'_1, g'_2))$ implies $(g_2, g_1) = (g'_2, g'_1)$. From this we obtain that $g_1 = g'_1$ and $g_2 = g'_2$. The element (g_2, g_1) is the image on (g_1, g_2) so ϕ is onto. Finally, $\phi((g_1, g_2)(g'_1, g'_2)) = \phi((g_1g'_1, g_2g'_2)) = (g_2g'_2, g_1g'_1) = (g_2, g_1)(g'_2, g'_1) = \phi((g_1, g_2))\phi((g'_1, g'_2))$. In general, the external direct product of any number of groups is isomorphic to the external direct product of any rearrangement of those groups.
8. No, $Z_3 \oplus Z_9$ does not have an element of order 27. See also Theorem 8.2.
9. In $Z_6 \oplus Z_2$, $|\langle\langle (1, 0) \rangle\rangle| = 6$ and $|\langle\langle (1, 1) \rangle\rangle| = 6$.

26. Consider $\langle 2, x \rangle = \{2f(x) + xg(x) \mid f(x), g(x) \in Z[x]\}$.
27. We start with $(x - 1/2)(x + 1/3)$ and clear fractions to obtain $(6x - 3)(6x + 2)$ as one possible solution.
28. If a had multiplicity greater than 1, then we could write $f(x) = (x - a)^2g(x)$. Now use the product rule to calculate $f'(x)$.
29. The proof given for Theorem 16.2 with $g(x) = x - a$ is valid over any commutative ring with unity. Moreover, the proofs for Corollaries 1 and 2 of Theorem 16.2 are also valid over any commutative ring with unity.
30. Notice that the proof of the division algorithm holds for integral domains when $g(x)$ has the form $x - a$. Likewise the proofs of the Factor Theorem and Corollary 3 of Theorem 16.2 hold.
31. Observe that $f(x) \in I$ if and only if $f(1) = 0$. Then if f and g belong to I and h belongs to $F[x]$, we have $(f - g)(1) = f(1) - g(1) = 0 - 0$ and $(hf)(1) = h(1)f(1) = h(1) \cdot 0 = 0$. So, I is an ideal. By Theorem 16.5, $I = \langle x - 1 \rangle$.
32. Use the Factor Theorem.
33. This follows directly from Corollary 2 of Theorem 15.5 and Exercise 11 in this chapter.
34. Consider the ideal $\langle x^3 - x \rangle$.
35. For any a in $U(p)$, $a^{p-1} = 1$, so every member of $U(p)$ is a zero of $x^{p-1} - 1$. From the Factor Theorem (Corollary 2 of Theorem 16.2) we obtain that $g(x) = (x - 1)(x - 2) \cdots (x - (p - 1))$ is a factor of $x^{p-1} - 1$. Since both $g(x)$ and $x^{p-1} - 1$ have lead coefficient 1, the same degree, and their difference has $p - 1$ zeros, their difference must be 0 (for otherwise their difference would be a polynomial of degree less than $p - 1$ that had $p - 1$ zeros).
36. By Theorem 16.5 the only possibility for $g(x)$ is $\pm(x - 1)$. By Theorem 15.3 $Z[x]/\text{Ker } \phi$ is isomorphic Z . The only possibilities for $g(x)$ are $a(x - 1)$ where a is any nonzero rational number. $Q[x]/\text{Ker } \phi$ is isomorphic Q . x in Z . But then $g(x) = f(x) - a$ has infinitely many zeros. This contradicts Corollary 3 of Theorem 16.2.
37. $\mathbf{C}(x)$ (field of quotients of $\mathbf{C}[x]$). Since p does not divide $(p - 1)$ we know that p divides $(p - 2)! - 1$. Thus, $(p - 2)! \bmod p = 1$.
38. When n is prime, use Exercise 37. When n is composite and greater than 4, $(n - 1)! \bmod n = 0$.
39. By Exercise 38, $(p - 1)! \bmod p = p - 1$. So, p divides $(p - 1)! - (p - 1) = (p - 1)((p - 2)! - 1)$.

CHAPTER 28

Frieze Groups and Crystallographic Groups

1. The mapping $\phi(x^m y^n) = (m, n)$ is an isomorphism. Onto is by observation. If $\phi(x^m y^n) = \phi(x^i y^j)$, then $(m, n) = (i, j)$ and therefore, $m = i$ and $n = j$. Also, $\phi((x^m y^n)(x^i y^j)) = \phi(x^{m+i} y^{n+j}) = (m+i, n+j) = (m, n)(i, j) = \phi(x^m y^n)\phi(x^i y^j)$.
2. 4
3. Using Figure 28.9 we obtain $x^2 y z x z = x y$.
4. $x^{-4} y$
5. Use Figure 28.9.
6. Use Figure 28.8.
7. $x^2 y z x z = x^2 y x^{-1} = x^2 x^{-1} y = x y$
 $x^{-3} z x z y = x^{-3} x^{-1} y = x^{-4} y$
8. It suffices to show $y^{-1} x y = x^i$ and $z^{-1} x z = x^j$ for some i and j .
9. A subgroup of index 2 is normal.
11. **a.** V, **b.** I, **c.** II, **d.** VI, **e.** VII, and **f.** III.
12. **a.** V **b.** III **c.** VII **d.** IV **e.** V
13. cmm
14. Reading down the columns starting on the left we have:
 $pgg, pmm, p2, p1, cmm, pmg, pg, pm, p3, p4, p4m, p4g, cm, p6,$
 $p3m1, p31m, p6m.$
15. **a.** $p4m$, **b.** $p3$, **c.** $p31m$, and **d.** $p6m$
16. The top row

$$\alpha^{-3}\beta^2, \alpha^{-2}\beta^2, \alpha^{-1}\beta^2, \beta^2, \alpha\beta^2.$$

The bottom row is

$$\alpha^{-2}\beta^{-1}, \alpha^{-1}\beta^{-1}, \beta^{-1}, \alpha\beta^{-1}, \alpha^2\beta^{-1}, \alpha^3\beta^{-1}.$$