Complete Solutions Manual

Abstract Algebra
An Introduction

THIRD EDITION

Thomas W. Hungerford
St. Louis University

Prepared by

Roger Lipsett

BROOKS/COLE
CENGAGE Learning

Australia • Brazil • Japan • Korea • Mexico • Singapore • Spain • United Kingdom • United States

BROOKS/COLE
CENGAGE Learning

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

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

ISBN-13: 978-1-133-61123-3
ISBN-10: 1-133-61123-0

Brooks/Cole
20 Channel Center Street
Boston, MA 02210
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 Brooks/Cole, visit **www.cengage.com/brookscole**

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

READ IMPORTANT LICENSE INFORMATION

Dear Professor or Other Supplement Recipient:

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

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

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

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

Printed in the United States of America
1 2 3 4 5 6 7 17 16 15 14 13

CONTENTS

Chapter 1

Arithmetic in $\mathbb{Z}$ Revisited

1.1 The Division Algorithm

1. (a) $q = 4$, $r = 1$. (b) $q = 0$, $r = 0$. (c) $q = -5$, $r = 3$.

2. (a) $q = -9$, $r = 3$. (b) $q = 15$, $r = 17$. (c) $q = 117$, $r = 11$.

3. (a) $q = 6$, $r = 19$. (b) $q = -9$, $r = 54$. (c) $q = 62720$, $r = 92$.

4. (a) $q = 15021$, $r = 132$. (b) $q = -14940$, $r = 335$. (c) $q = 39763$, $r = 3997$.

5. Suppose $a = bq + r$, with $0 \le r < b$. Multiplying this equation through by c gives $ac = (bc)q + rc$. Further, since $0 \le r < b$, it follows that $0 \le rc < bc$. Thus this equation expresses ac as a multiple of bc plus a remainder between 0 and $bc - 1$. Since by Theorem 1.1 this representation is unique, it must be that q is the quotient and rc the remainder on dividing ac by bc.

6. When q is divided by c, the quotient is k, so that $q = ck$. Thus $a = bq + r = b(ck) + r = (bc)k + r$. Further, since $0 \le r < b$, it follows (since $c \ge 1$) than $0 \le r < bc$. Thus $a = (bc)k + r$ is the unique representation with $0 \le r < bc$, so that the quotient is indeed k.

7. Answered in the text.

8. Any integer n can be divided by 4 with remainder r equal to 0, 1, 2 or 3. Then either $n = 4k$, $4k + 1$, $4k + 2$ or $4k + 3$, where k is the quotient. If $n = 4k$ or $4k + 2$ then n is even. Therefore if n is odd then $n = 4k + 1$ or $4k + 3$.

9. We know that every integer a is of the form $3q$, $3q + 1$ or $3q + 2$ for some q. In the last case $a^3 = (3q + 2)^3 = 27q^3 + 54q^2 + 36q + 8 = 9k + 8$ where $k = 3q^3 + 6q^2 + 4q$. Other cases are similar.

10. Suppose $a = nq + r$ where $0 \le r < n$ and $c = nq' + r'$ where $0 < r' < n$. If $r = r'$ then $a - c =$ n$(q - q')$ and $k = q - q'$ is an integer. Conversely, given $a - c = nk$ we can substitute to find: $(r - r') = n(k - q + q')$. Suppose $r \ge r'$ (the other case is similar). The given inequalities imply that $0 \le (r - r') < n$ and it follows that $0 \le (k - q + q') < 1$ and we conclude that $k - q + q' = 0$. Therefore $r - r' = 0$, so that $r = r'$ as claimed.

11. Given integers a and c with $c \neq 0$. Apply Theorem 1.1 with $b = |c|$ to get $a = |c| \cdot q_0 + r$ where $0 \leq r < |c|$. Let $q = q_0$ if $c > 0$ and $q = -q_0$ if $c < 0$. Then $a = cq + r$ as claimed. The uniqueness is proved as in Theorem 1.1.

1.2 Divisibility

1. (a) 8.
   (b) 6.
   (c) 1.
   (d) 11.
   (e) 9.
   (f) 17.
   (g) 592.
   (h) 6.

2. If $b \mid a$ then $a = bx$ for some integer x. Then $a = (-b)(-x)$ so that $(-b) \mid a$. The converse follows similarly.

3. Answered in the text.

4. (a) Given $b = ax$ and $c = ay$ for some integers x, y, we find $b + c = ax + ay = a(x + y)$. Since $x + y$ is an integer, conclude that $a \mid (b + c)$.
   (b) Given x and y as above we find $br + ct = (ax)r + (ay)t = a(xr + yt)$ using the associative and distributive laws. Since $xr + yt$ is an integer we conclude that $a \mid (br + ct)$.

5. Since $a \mid b$, we have $b = ak$ for some integer k, and $a \neq 0$. Since $b \mid a$, we have $a = bl$ for some integer l, and $b \neq 0$. Thus $a = bl = (ak)l = a(kl)$. Since $a \neq 0$, divide through by a to get $1 = kl$. But this means that $k = \pm 1$ and $l = \pm 1$, so that $a = \pm\, b$.

6. Given $b = ax$ and $d = cy$ for some integers x, y, we have $bd = (ax)(cy) = (ac)(xy)$. Then $ac \mid bd$ because xy is an integer.

7. Clearly $(a, 0)$ is at most $|a|$ since no integer larger than $|a|$ divides a. But also $|a| \mid a$, and $|a| \mid 0$ since any nonzero integer divides 0. Hence $|a|$ is the gcd of a and 0.

8. If $d = (n, n + 1)$ then $d \mid n$ and $d \mid (n + 1)$. Since $(n + 1) - n = 1$ we conclude that $d \mid 1$. (Apply Exercise 4(b).) This implies $d = 1$, since $d > 0$.

9. No, ab need not divide c. For one example, note that $4 \mid 12$ and $6 \mid 12$, but $4 \cdot 6 = 24$ does not divide 12.

10. Since $a \mid a$ and $a \mid 0$ we have $a \mid (a, 0)$. If $(a, 0) = 1$ then $a \mid 1$ forcing $a = \pm 1$.

11. (a) 1 or 2 (b) 1, 2, 3 or 6. Generally if $d = (n, n + c)$ then $d \mid n$ and $d \mid (n + c)$. Since c is a linear combination of n and n+c, conclude that $d \mid c$.

12. (a) False. (ab, a) is always at least a since $a \mid ab$ and $a \mid a$.
    (b) False. For example, $(2, 3) = 1$ and $(2, 9) = 1$, but $(3, 9) = 3$.
    (c) False. For example, let $a = 2$, $b = 3$, and $c = 9$. Then $(2, 3) = 1 = (2, 9)$, but $(2 \cdot 3, 9) = 3$.

13. (a) Suppose $c \mid a$ and $c \mid b$. Write $a = ck$ and $b = cl$. Then $a = bq + r$ can be rewritten $ck = (cl)q + r$, so that $r = ck - clq = c(k - lq)$. Thus $c \mid r$ as well, so that c is a common divisor of b and r.

    (b) Suppose $c \mid b$ and $c \mid r$. Write $b = ck$ and $r = cl$, and substitute into $a = bq + r$ to get $a = ckq + cl = c(kq + l)$. Thus $c \mid a$, so that c is a common divisor of a and b.

    (c) Since (a, b) is a common divisor of a and b, it is also a common divisor of b and r, by part (a). If (a, b) is not the greatest common divisor (b, r) of b and r, then $(a, b) > (b, r)$. Now, consider (b, r). By part (b), this is also a common divisor of (a, b), but it is less than (a, b). This is a contradiction. Thus $(a, b) = (b, r)$.

14. By Theorem 1.3, the smallest positive integer in the set S of all linear combinations of a and b is exactly $(a,\ b)$.

    (a) $(6,\ 15) = 3$ (b) $(12,\ 17)$=1.

15. (a) This is a calculation.

    (b) At the first step, for example, by Exercise 13 we have $(a, b) = (524, 148) = (148, 80) = (b, r)$. The same applies at each of the remaining steps. So at the final step, we have $(8, 4) = (4, 0)$; putting this string of equalities together gives

    $$(524, 148) = (148, 80) = (80, 68) = (68, 12) = (12, 8) = (8, 4) = (4, 0).$$

    But by Example 4, $(4, 0) = 4$, so that $(524, 148) = 4$.

    (c) $1003 = 56 \cdot 17 + 51$, $56 = 51 \cdot 1 + 5$, $51 = 5 \cdot 10 + 1$, $5 = 1 \cdot 5 + 0$. Thus $(1003, 56) = (1, 0) = 1$.

    (d) $322 = 148 \cdot 2 + 26$, $148 = 26 \cdot 5 + 18$, $26 = 18 \cdot 1 + 8$, $18 = 8 \cdot 2 + 2$, $8 = 2 \cdot 4 + 0$, so that $(322, 148) = (2, 0) = 2$.

    (e) $5858 = 1436 \cdot 4 + 114$, $1436 = 114 \cdot 12 + 68$, $114 = 68 \cdot 1 + 46$, $68 = 46 \cdot 1 + 22$, $46 = 22 \cdot 2 + 2$, $22 = 2 \cdot 11 + 0$, so that $(5858, 1436) = (2, 0) = 2$.

    (f) $68 = 148 - (524 - 148 \cdot 3) = -524 + 148 \cdot 4$.

    (g) $12 = 80 - 68 \cdot 1 = (524 - 148 \cdot 3) - (-524 + 148 \cdot 4) \cdot 1 = 524 \cdot 2 - 148 \cdot 7$.

    (h) $8 = 68 - 12 \cdot 5 = (-524 + 148 \cdot 4) - (524 \cdot 2 - 148 \cdot 7) \cdot 5 = -524 \cdot 11 + 148 \cdot 39$.

    (i) $4 = 12 - 8 = (524 \cdot 2 - 148 \cdot 7) - (-524 \cdot 11 + 148 \cdot 39) = 524 \cdot 13 - 148 \cdot 46$.

    (j) Working the computation backwards gives $1 = 1003 \cdot 11 - 56 \cdot 197$.

16. Let $a = da_1$ and $b = db_1$. Then a_1 and b_1 are integers and we are to prove: $(a_1,\ b_1) = 1$. By Theorem 1.3 there exist integers u, v such that $au +\ bv = d$. Substituting and cancelling we find that $a_1u +\ b_1v = 1$. Therefore any common divisor of a_1 and b_1 must also divide this linear combination, so it divides 1. Hence $(a_1,\ b_1) = 1$.

17. Since $b \mid c$, we know that $c = bt$ for some integer t. Thus $a \mid c$ means that $a \mid bt$. But then Theorem 1.4 tells us, since $(a, b) = 1$, that $a \mid t$. Multiplying both sides by b gives $ab \mid bt = c$.

18. Let $d = (a,\ b)$ so there exist integers $x,\ y$ with $ax +\ by = d$. Note that $cd \mid (ca,\ cb)$ since cd divides ca and cb. Also $cd = cax +\ cby$ so that $(ca,\ cb) \mid cd$. Since these quantities are positive we get $cd = (ca,\ cd)$.

19. Let $d = (a,\ b)$. Since $b +\ c = aw$ for some integer w, we know c is a linear combination of a and b so that $d \mid c$. But then $d \mid (b, c\ ) = 1$ forcing $d = 1$. Similarly $(a, c\ ) = 1$.

20. Let $d = (a, b)$ and $e = (a, b + at)$. Since $b + at$ is a linear combination of a and b, $d \mid (b + at)$ so that $d \mid e$. Similarly since $b = a(-t) + (b + at)$ is a linear combination of a and $b + at$ we know $e \mid b$ so that $e \mid d$. Therefore $d = e$.

21. Answered in the text.

22. Let $d = (a, b, c)$. Claim: $(a, d) = 1$. [Proof: (a, d) divides d so it also divides c. Then $(a, d) \mid (a, c) = 1$ so that $(a, d)= 1$.] Similarly $(b, d)= 1$. But $d \mid ab$ and $(a, d) = 1$ so that Theorem 1.5 implies that $d \mid$ b. Therefore $d = (b. d) = 1$.

23. Define the powers b^n recursively as follows: $b^1 = b$ and for every $n \geq 1$, $b^{n+1} = b \cdot b^n$. By hypothesis $(a, b^1) = 1$. Given $k \geq 1$, assume that $(a, b^k) = 1$. Then $(a, b^{k+1}) = (a, b \cdot b^k) = 1$ by Exercise 24. This proves that $(a, b^n) = 1$ for every $n \geq 1$.

24. Let $d = (a, b)$. If $ax + by = c$ for some integers x, y then c is *a* linear combination of a and b so that $d \mid c$. Conversely suppose c is given with $d \mid$ c, say $c = dw$ for an integer w. By Theorem 1.3 there exist integers u, v with $d = au + bv$. Then $c = dw = auw + bvw$ and we use $x = uw$ and $y = vw$ to solve the equation.

25. (a) Given $au + bv = 1$ suppose $d = (a, b)$. Then $d \mid a$ and $d \mid b$ so that d divides the linear combination $au + bv = 1$. Therefore $d = 1$.
    (b) There are many examples. For instance if $a = b = d = u = v = 1$ then $(a, b) = (1, 1)= 1$ while $d = au + bv = 1 + 1 = 2$.

26. Let $d = (a, b)$ and express $a = da_1$ and $b = db_1$ for integers a_1, b_1. By Exercise 16, $(a_1, b_1) = 1$. Since $a \mid c$ we have $c = au = da_1u$ for some integer u. Similarly $c = bv = db_1v$ for some integer v. Then $a_1u = c/d = b_1V$ and Theorem 1.5 implies that $a_1 \mid v$ so that $v = a_1w$ for some integer w. Then $c = da_1b_1w$ so that $cd = d^2a_1b_1w = abw$ and $ab \mid cd$.

27. Answered in the text.

28. Suppose the integer consists of the digits $a_na_{n-1}\ldots a_1a_0$. Then the number is equal to

$$\sum_{k=0}^{n} a_k 10^k = \sum_{k=0}^{n} a_k(10^k - 1) + \sum_{k=0}^{n} a_k.$$

Now, the first term consists of terms with factors of the form $10^k - 1$, all of which are of the form $999\ldots99$, which are divisible by 3, so that the first term is always divisible by 3. Thus $\sum_{k=0}^{n} a_k 10^k$ is divisible by 3 if and only if the second term $\sum_{k=0}^{n} a_k$ is divisible by 3. But this is the sum of the digits.

29. This is almost identical to Exercise 28. Suppose the integer consists of the digits $a_na_{n-1}\ldots a_1a_0$. Then the number is equal to

$$\sum_{k=0}^{n} a_k 10^k = \sum_{k=0}^{n} a_k(10^k - 1) + \sum_{k=0}^{n} a_k.$$

Now, the first term consists of terms with factors of the form $10^k - 1$, all of which are of the form $999\ldots99$, which are divisible by 9, so that the first term is always divisible by 9. Thus $\sum_{k=0}^{n} a_k 10^k$ is divisible by 9 if and only if the second term $\sum_{k=0}^{n} a_k$ is divisible by 9. But this is the sum of the digits.

30. Let $S = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n : x_1\ x_2, ..., x \text{ are integers}\}$. As in the proof of Theorem 1.3, S does contain some positive elements (for if $a_i \neq 0$ then $a_i^2 \in S$ is positive). By the Well Ordering Axiom this set S contains a smallest positive element, which we call t. Suppose $t = a_1u_1 + a_2u_2 + \cdots + a_nu_n$ for some integers u_i.
Claim. $t = d$. The first step is to show that $t \mid a_1$. By the division algorithm there exist integers q and r such that $a_1 = tq + r$ with $0 \leq r < t$. Then $r = a_1 - tq = a_1(1 - u_1q) + a_2(-u_2q) + \cdots + a_n(-u_nq)$ is an element of S. Since $r < t$ (the smallest positive element of S), we know r is not positive. Since $r \geq 0$ the only possibility is $r = 0$. Therefore $a_1 = tq$ and $t \mid a_1$. Similarly we have $t \mid a_j$ for each j, and t is *a* common divisor of $a_1, a_2, \cdots, a_n$. Then $t \leq d$ by definition.

On the other hand d divides each a_i so d divides every integer linear combination of $a_1, a_2, \cdots, a_n$. In particular, $d \mid t$. Since $t > 0$ this implies that $d \leq t$ and therefore $d = t$.

31. (a) $[6, 10] = 30$; $[4, 5, 6, 10] = 60$; $[20, 42] = 420$, and $[2, 3, 14, 36, 42] = 252$.

(b) Suppose $a_i \mid t$ for $i = 1, 2, \ldots, k$, and let $m = [a_1, a_2, \ldots, a_k]$. Then we can write $t = mq + r$ with $0 \leq r < m$. For each i, $a_i \mid t$ by assumption, and $a_i \mid m$ since m is a common multiple of the a_i. Thus $a_i \mid (t - mq) = r$. Since $a_i \mid r$ for each i, we see that r is a common multiple of the a_i. But m is the smallest positive integer that is a common multiple of the a_i; since $0 \leq r < m$, the only possibility is that $r = 0$ so that $t = mq$. Thus any common multiple of the a_i is a multiple of the least common multiple.

32. First suppose that $t = [a, b]$. Then by definition of the least common multiple, t is a multiple of both a and b, so that $t \mid a$ and $t \mid b$. If $a \mid c$ and $b \mid c$, then c is also a common multiple of a and b, so by Exercise 31, it is a multiple of t so that $t \mid c$.

Conversely, suppose that t satisfies the conditions (i) and (ii). Then since $a \mid t$ and $b \mid t$, we see that t is a common multiple of a and b. Choose any other common multiple c, so that $a \mid c$ and $b \mid c$. Then by condition (ii), we have $t \mid c$, so that $t \leq c$. It follows that t is the least common multiple of a and b.

33. Let $d = (a, b)$, and write $a = da_1$ and $b = db_1$. Write $m = \frac{ab}{d} = \frac{da_1db_1}{d} = da_1b_1$. Since a and b are both positive, so is m, and since $m = da_1b_1 = (da_1)b_1 = ab_1$ and $m = da_1b_1 = (db_1)a_1 = ba_1$, we see that m is a common multiple of a and b. Suppose now that k is a positive integer with $a \mid k$ and $b \mid k$. Then $k = au = bv$, so that $k = da_1u = db_1v$. Thus $\frac{k}{d} = a_1u = b_1v$. By Exercise 16, $(a_1, b_1) = 1$, so that $a_1 \mid v$, say $v = a_1w$. Then $k = db_1v = db_1a_1w = mw$, so that $m \mid k$. Thus $m \leq k$. It follows that m is the least common multiple. But by construction, $m = \frac{ab}{(a,b)} = \frac{ab}{d}$.

34. (a) Let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, it follows that $d \mid (a + b)$ and $d \mid (a - b)$, so that d is a common divisor of $a + b$ and $a - b$. Hence it is a divisor of the greatest common divisor, so that $d = (a, b) \mid (a + b, a - b)$.

(b) We already know that $(a, b) \mid (a+b, a-b)$. Now suppose that $d = (a+b, a-b)$. Then $a+b = dt$ and $a - b = du$, so that $2a = d(t + u)$. Since a is even and b is odd, d must be odd. Since $d \mid 2a$, it follows that $d \mid a$. Similarly, $2b = d(t - u)$, so by the same argument, $d \mid b$. Thus d is a common divisor of a and b, so that $d \mid (a, b)$. Thus $(a, b) = (a + b, a - b)$.

(c) Suppose that $d = (a + b, a - b)$. Then $a + b = dt$ and $a - b = du$, so that $2a = d(t + u)$. Since a and b are both odd, $a + b$ and $a - b$ are both even, so that d is even. Thus $a = \frac{d}{2}(t + u)$, so that $\frac{d}{2} \mid a$. Similarly, $\frac{d}{2} \mid b$, so that $\frac{d}{2} = \frac{(a+b,a-b)}{2} \mid (a, b) \mid (a + b, a - b)$. Thus $(a, b) = \frac{(a+b,a-b)}{2}$ or $(a, b) = (a + b, a - b)$. But since (a, b) is odd and $(a + b, a - b)$ is even, we must have $\frac{(a+b,a-b)}{2} = (a, b)$, or $2(a, b) = (a + b, a - b)$.

1.3 Primes and Unique Factorization

1. (a) $2^4 \cdot 3^2 \cdot 5 \cdot 7$.

   (b) $-5 \cdot 7 \cdot 67$.

   (c) $2 \cdot 5 \cdot 4567$.

   (d) $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17$.

2. (a) Since $2^5 - 1 = 31$, and $\sqrt{31} < 6$, we need only check divisibility by the primes 2, 3, and 5. Since none of those divides 31, it is prime.

   (b) Since $2^7 - 1 = 127$, and $\sqrt{127} < 12$, we need only check divisibility by the primes 2, 3, 5, 7, and 11. Since none of those divides 127, it is prime.

   (c) $2^{11} - 1 = 2047 = 23 \cdot 89$.

3. They are all prime.

4. The pairs are $\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$, $\{29, 31\}$, $\{41, 43\}$, $\{59, 61\}$, $\{71, 73\}$, $\{101, 103\}$, $\{107, 109\}$, $\{137, 139\}$, $\{149, 151\}$, $\{179, 181\}$, $\{191, 193\}$, $\{197, 199\}$.

5. (a) Answered in the text. These divisors can be listed as $2^j \cdot 3^k$ for $0 \le j \le s$ and $0 \le k \le t$.

   (b) The number of divisors equals $(r + 1)(s + 1)(t + 1)$.

6. The possible remainders on dividing a number by 10 are $0, 1, 2, \ldots, 9$. If the remainder on dividing p by 10 is $0, 2, 4, 6$, or 8, then p is even; since $p > 2$, p is divisible by 2 in addition to 1 and itself and cannot be prime. If the remainder is 5, then since $p > 5$, p is divisible by 5 in addition to 1 and itself and cannot be prime. That leaves as possible remainders only $1, 3, 7$, and 9.

7. Since $p \mid (a + bc)$ and $p \mid a$, we have $a = pk$ and $a + bc = pl$, so that $pk + bc = pl$ and thus $bc = p(l - k)$. Thus $p \mid bc$. By Theorem 1.5, either $p \mid b$ or $p \mid c$ (or both).

8. (a) As polynomials,
$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

   (b) Since $2^{2n} \cdot 3^n - 1 = (2^2 \cdot 3)^n - 1 = 12^n - 1$, by part (a), $12^n - 1$ is divisible by $12 - 1 = 11$.

9. If p is a prime and $p = rs$ then by the definition r, s must lie in $\{1, -1, p, -p\}$. Then either $r = \pm 1$ or $r = \pm p$ and $s = p/r = \pm 1$, Conversely if p is not a prime then it has a divisor r not in $\{1, -1, p, -p\}$. Then $p = rs$ for some integer s. If s equals ± 1 or $\pm p$ then $r = p/s$ would equal $\pm p$ or $+1$, contrary to assumption. This r, s provides an example where the given statement fails.

10. Assume first that $p > 0$. If p is a prime then (a, p) is a positive divisor of p, so that $(a, p) = 1$ or p. If $(a, p) = p$ then $p \mid a$. Conversely if p is not a prime it has a divisor d other than ± 1 and $\pm p$. We may change signs to assume $d > 0$. Then $(p, d) = d \neq 1$. Also $p \nmid d$ since otherwise $p \mid d$ and $d = p$ implies $d = p$. Then $a = d$ provides an example where the required statement fails. Finally if $p < 0$ apply the argument above to $-p$.

11. Since $p \mid a - b$ and $p \mid c - d$, also $p \mid (a - b) + (c - d) = (a + c) - (b + d)$. Thus p is a divisor of $(a + c) - (b + d)$; the fact that p is prime means that it is a prime divisor.

12. Since $n > 1$ Theorem 1.10 implies that n equals a product of primes. We can pull out minus signs to see that $\mathrm{n} = p_1\ p_2\ \ldots\ p_{\mathrm{r}}$ where each p_{i} is a positive prime. Re-ordering these primes if necessary, to assume $p_1 \leq p_2 \leq \ldots \leq p_{\mathrm{r}}$. For the uniqueness, suppose there is another factorization $n = q_1\, q_2 \ldots q_{\mathrm{s}}$ for some positive primes $\mathrm{q_i}$ with $q_1 \leq q_2 \ldots \leq q_{\mathrm{s}}$. By theorem 1.11 we know that $r = s$ and the p_{i}'s are just a re-arrangement of the q_{i}s. Then p_1 is the smallest of the p_{i}'s, so it also equals the smallest of the q_{i}'s and therefore $p_1 = q_1$. We can argue similarly that $p_2 = q_2, \ldots, p_{\mathrm{r}} = q_{\mathrm{r}}$. (This last step should really be done by a formal proof invoking the Well Ordering Axiom.)

13. By Theorem 1.8, the Fundamental Theorem of Arithmetic, every integer except 0 and ±1 can be written as a product of primes, and the representation is unique up to order and the signs of the primes. Since in our case $n > 1$ is positive and we wish to use positive primes, the representation is unique up to order. So write $n = q_1\, q_2 \ldots q_s$ where each $q_i > 0$ is prime. Let $p_1, p_2, \ldots, p_r$ be the distinct primes in the list. Collect together all the occurrences of each p_i, giving r_i copies of p_i, i.e. $p_i^{r_i}$.

14. Suppose $d \mid p$ so that $p = dt$ for some integer t. The hypothesis then implies that $p \mid d$ or $p \mid t$. If $p \mid d$ then (applying Exercise 1.2.5) $d = \pm p$. Similarly if $p \mid t$ then, since we know that $t \mid p$, we get $t = +p$, and therefore $d = \pm 1$.

15. Apply Corollary 1.9 in the case $a_1 = a_2 = \cdots = a_n$ to see that if $p \mid a^n$ then $p \mid a$. Then $a = pu$ for some integer u, so that $a^n = p^n u^n$ and $p^n \mid a^n$.

16. Generally, $p \mid a$ and $p \mid b$ if and only if $p \mid (a,\, b)$, as in Corollary 1.4. Then the Exercise is equivalent to: $(a,\, b) = 1$ if and only if there is no prime p such that $p \mid (a,\, b)$. This follows using Theorem 1.10.

17. First suppose u, v are integers with $(u,\, v) = 1$. Claim. $(u^2,\, v^2) = 1$. For suppose p is a prime such that $p \mid u^2$ and $p \mid v^2$. Then $p \mid u$ and $p \mid v$ (using Theorem 1.8), contrary to the hypothesis $(u,\, v) = 1$. Then no such prime exists and the Claim follows by Exercise 8.
Given $(a,\, b) = p$ write $a = pa_1$ and $b = pb_1$. Then $(a_1,\, b_1) = 1$ by Exercise 1.2.16. Then $(a^2,\, b^2) = (p^2 a_1{}^2,\, p^2 b_1{}^2) = p^2(a_1{}^2,\, b_1{}^2)$, using Exercise 1.2.18. By the Claim we conclude that $(a^2,\, b^2) = p^2$.

18. The choices $p = 2$, $a = b = 0$, $c = d = 1$ provide a counterexample to (a) and (b).
(c) Since $p \mid (a^2 + b^2) - a{\cdot}\mathrm{a} = b^2$, conclude that $p \mid b$ by Theorem 1.8.

19. If $r_i \leq s_i$ for every i, then

$$b = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k} = p_1^{r_1} p_1^{s_1 - r_1} p_2^{r_2} p_2^{s_2 - r_2} \ldots p_k^{r_k} p_k^{s_k - r_k} = (p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}) \cdot \left(p_1^{s_1 - r_1} p_2^{s_2 - r_2} \ldots p_k^{s_2 - r_k}\right)$$
$$= a \cdot \left(p_1^{s_1 - r_1} p_2^{s_2 - r_2} \ldots p_k^{s_2 - r_k}\right).$$

Since each $s_i - r_i \geq 0$, the second factor above is an integer, so that $a \mid b$.

Now suppose $a \mid b$, and consider $p_i^{r_i}$. Since this is composed of factors only of p_i, it must divide $p_i^{s_i}$, since $p_i \nmid p_j$ for $i \neq j$. Thus $p_i^{r_i} \mid p_i^{s_i}$. Clearly this holds if $r_i \leq s_i$, and also clearly it does not hold if $r_i > s_i$, since then $p_i^{r_i} > p_i^{s_i}$.

20. (a) The positive divisors of a are the numbers $d = p_1{}^{m1} p_2{}^{m2} \cdots p_k{}^{mk}$ where the exponents m_j satisfy $0 \leq m_j \leq r_j$ for each $j = 1, 2,,.., k$. This follows from unique factorization. If d also divides b we have $0 \leq m_i \leq s_i$ for each $i = 1, 2,... k$. Since $n_j = \min\{r_j, s_j\}$ we see that the positive common divisors of a and b are exactly those numbers $d = p_1{}^{m1} p_2{}^{m2} \cdots p_k{}^{mk}$ where $0 \leq m_j \leq n_j$ for each $j = 1, 2,..., k$. Then (a, b) is the largest among these common divisors, so it equals $p_1{}^{n1} p_2{}^{n2} \cdots p_k{}^{nk}$.
    (b) For $[a, b]$ a similar argument can be given, or we can apply Exercise 1.2.31, noting that $\max\{r, s\} = r + s - \min\{r, s\}$ for any positive numbers r, s.

21. Answered in the text.

22. If every r_i is even it is easy to see that n is a perfect square. Conversely suppose n is a square. First consider the special case $n = p^r$ is a power of a prime. If $p^r = m^2$ is a square, consider the prime factorization of m. By the uniqueness (Theorem 1.11), p is the only prime that can occur, so m $= p^s$ for some s, and $p^r = m^2 = p^{2s}$. Then $r = 2s'$ is even. Now for the general case, suppose $n = m^2$ is a perfect square. If some r_i is odd, express $n = p_i{}^{ri} \cdot k$ where k is the product of the other primes involved in n.

    Then $p_i{}^{ri}$ and k are relatively prime and Exercise 13 implies that $p_i{}^{ri}$ is a perfect square. By the special case, r_i. is even.

23. Suppose $a = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ and $b = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$ where the p_i are distinct positive primes and $r_i \geq 0$, $s_i \geq 0$. Then $a^2 = p_1^{2r_1} p_2^{2r_2} \ldots p_k^{2r_k}$ and $b^2 = p_1^{2s_1} p_2^{2s_2} \ldots p_k^{2s_k}$. Then using Exercise 19 (twice), we have $a \mid b$ if and only if $r_i \leq s_i$ for each i if and only if $2r_i \leq 2s_i$ for each i if and only if $a^2 \mid b^2$.

24. This is almost identical to the previous exercise. If $n > 0$ is an integer, suppose $a = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$ and $b = p_1^{s_1} p_2^{s_2} \ldots p_k^{s_k}$ where the p_i are distinct positive primes and $r_i \geq 0$, $s_i \geq 0$. Then $a^n = p_1^{nr_1} p_2^{nr_2} \ldots p_k^{nr_k}$ and $b^2 = p_1^{ns_1} p_2^{ns_2} \ldots p_k^{ns_k}$. Then using Exercise 19 (twice), we have $a \mid b$ if and only if $r_i \leq s_i$ for each i if and only if $nr_i \leq ns_i$ for each i if and only if $a^n \mid b^n$.

25. The binomial coefficient $\binom{p}{k}$ is

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p \cdot (p-1) \cdots (p-k+1)}{k(k-1) \cdots 1}.$$

    Now, the numerator is clearly divisible by p. The denominator, however, consists of a product of integers all of which are less than p. Since p is prime, none of those integers (except 1) divide p, so the product cannot have a factor of p (to make this more precise, you may wish to write the denominator as a product of primes and note that p cannot appear in the list).

26. Claim: Each $A_k = (n + 1)! + k$ is composite, for $k = 2, 3,. .. , n + 1$. Proof. Since $k \leq n + 1$ we have $k \mid (n + 1)!$ and therefore $k \mid A_k$. Then A_k is composite since $I < k < A_k$.

27. By the division algorithm $p = 6k + r$ where $0 \leq r < 6$. Since $p > 3$ is prime it is not divisible by 2 or 3, and we must have $r = 1$ or 5. If $p = 6k + 1$ then $p^2 = 36k^2 + 12k + 1$ and $p^2 + 2 = 36k^2 + 12k + 3$ is a multiple of 3. Similarly if $p = 6k + 5$ then $p^2 + 2 = 36k^2 + 60k + 27$ is a multiple of 3. So in each case, $p^2 + 2$ is composite.

28. The sums in question are: $1 + 2 + 4 + \cdots + 2^n$. When $n = 7$ the sum is $255 = 3{\cdot}5{\cdot}17$ and when $n = 8$ the sum is $511 = 7{\cdot}73$. Therefore the assertion is false. The interested reader can verify that this sum equals $2^{n+1} - 1$. These numbers are related to the "Mersenne primes".

29. This assertion follows immediately from the Fundamental Theorem 1.11.

30. (a) If $a^2 = 2b^2$ for positive integers a, b, compare the prime factorizations on both sides. The power of 2 occurring in the factorization of a^2 must be even (since it is a square). The power of 2 occurring in $2b^2$ must be odd. By the uniqueness of factorizations (The Fundamental Theorem) these powers of 2 must be equal, a contradiction.
(b) If $\sqrt{2}$ is rational it can be expressed as a fraction $\frac{\mathrm{a}}{\mathrm{b}}$ for some positive integers a, b. Clearing denominators and squaring leads to: $a^2 = 2b^2$, and part (a) applies.

31. The argument in Exercise 20 applies. More generally see Exercise 27 below.

32. Suppose all the primes can be put in a finite list $p_1, p_2, \cdots, p_k$ and consider $N = p_1\, p_2 \ldots p_k + 1$. None of these p_i can divide N (since 1 can be expressed as a linear combination of p_i and N). But $N > 1$ so N must have some prime factor p. (Theorem 1.10). This p is a prime number not equal to any of the primes in our list, contrary to hypothesis.

33. Suppose n is composite, and write $n = rs$ where $1 < r, s < n$. Then, as you can see by multiplying it out,

$$2^n - 1 = (2^r - 1)\left(2^{s(r-1)} + 2^{s(r-2)} + 2^{s(r-3)} + \cdots + 2^s + 1\right).$$

Since $r > 1$, it follows that $2^r > 1$. Since $s > 1$, we see that $2^s + 1 > 1$, so that the second factor must also be greater than 1. So $2^n - 1$ has been written as the product of two integers greater than one, so it cannot be prime.

34. Proof: Since $n > 2$ we know that $n! - 1 > 1$ so it has some prime factor p. If $p \leq n$ then $p \mid n!$, contrary to the fact that $p \mid n!$. Therefore $n < p < n!$.

35. We sketch the proof (b). Suppose $a > 0$ (What if $a < 0$?), $r^n = a$ and $r = u/v$ where u, v are integers and $v > 0$. Then $u^n = av^u$. If p is a prime let k be the exponent of p occurring in a (that is: $p^k \mid a$ and $p^{k+1} \nmid a$). The exponents of p occurring in u^n and in v^n must be multiples of n, so unique factorization implies k is a multiple of n. Putting all the primes together we conclude that $a = b^n$ for some integer b.

36. If p is a prime > 3 then $2 \nmid p$ and $3 \nmid p$, so by Exercise 1.2.34 we know $24 \mid p^2 - 1$. Similarly $24 \mid (q^2 - 1)$ so that $p^2 - q^2 = (p^2 - 1) - (q^2 - 1)$ is a multiple of 24.

Chapter 2

Congruence in $\mathbb{Z}$ and Modular Arithmetic

2.1 Congruence and Congruence Classes

1. (a) $2^{5-1} = 2^4 = 16 \equiv 1 \pmod 5$. (b) $4^{7-1} = 4^6 = 4096 \equiv 1 \pmod 7$.
   (c) $3^{11-1} = 3^{10} = 59049 \equiv 1 \pmod{11}$.

2. (a) Use Theorems 2.1 and 2.2: $6k + 5 \equiv 6.1 + 5 \equiv 11 \equiv 3 \pmod 4$.
   (b) $2r + 3s \equiv 2.3 + 3.(-7) \equiv -15 \equiv 5 \pmod{10}$.

3. (a) Computing the checksum gives

$$\begin{aligned}10\cdot 3 + 9\cdot 5 + 8\cdot 4 + 7\cdot 0 + 6\cdot 9 + 5\cdot 0 + 4\cdot 5 + 3\cdot 1 + 2\cdot 8 + 1\cdot 9 \\ = 30 + 45 + 32 + 54 + 20 + 3 + 16 + 9 = 209.\end{aligned}$$

   Since $209 = 11\cdot 19$, we see that $209 \equiv 0 \pmod{11}$, so that this could be a valid ISBN number.

   (b) Computing the checksum gives

$$\begin{aligned}10\cdot 0 + 9\cdot 0 + 8\cdot 3 + 7\cdot 1 + 6\cdot 1 + 5\cdot 0 + 4\cdot 5 + 3\cdot 5 + 2\cdot 9 + 1\cdot 5 \\ = 24 + 7 + 6 + 20 + 15 + 18 + 5 = 95.\end{aligned}$$

   Since $95 = 11\cdot 8 + 7$, we see that $95 \equiv 7 \pmod{11}$, so that this could not be a valid ISBN number.

   (c) Computing the checksum gives

$$\begin{aligned}10\cdot 0 + 9\cdot 3 + 8\cdot 8 + 7\cdot 5 + 6\cdot 4 + 5\cdot 9 + 4\cdot 5 + 3\cdot 9 + 2\cdot 6 + 1\cdot 10 \\ = 27 + 64 + 35 + 24 + 45 + 20 + 27 + 12 + 10 = 264.\end{aligned}$$

   Since $264 = 11\cdot 24$, we see that $264 \equiv 0 \pmod{11}$, so that this could be a valid ISBN number.

4. (a) Computing the checksum gives

$$3 \cdot 0 + 3 + 3 \cdot 7 + 0 + 3 \cdot 0 + 0 + 3 \cdot 3 + 5 + 3 \cdot 6 + 6 + 3 \cdot 9 + 1 = 90.$$

Since $90 = 10 \cdot 9$, we have $90 \equiv 0 \pmod{10}$, so that this was scanned correctly.

(b) Computing the checksum gives

$$3 \cdot 8 + 3 + 3 \cdot 3 + 7 + 3 \cdot 3 + 2 + 3 \cdot 0 + 0 + 3 \cdot 0 + 6 + 3 \cdot 2 + 5 = 71.$$

Since $71 = 10 \cdot 7 + 1$, we have $71 \equiv 1 \pmod{10}$, so that this was not scanned correctly.

(c) Computing the checksum gives

$$3 \cdot 0 + 4 + 3 \cdot 0 + 2 + 3 \cdot 9 + 3 + 3 \cdot 6 + 7 + 3 \cdot 3 + 0 + 3 \cdot 3 + 4 = 83.$$

Since $83 = 10 \cdot 8 + 3$, we have $83 \equiv 3 \pmod{10}$, so that this was not scanned correctly.

5. Since $5 \equiv 1 \pmod 4$, it follows from Theorem 2.2 that $5^2 \equiv 1^2 \pmod 4$, so that (applying Theorem 2.2 again) $5^3 \equiv 1^3 \pmod 4$. Continuing, we get $5^{1000} \equiv 1^{1000} \equiv 1 \pmod 4$. Since $5^{1000} \equiv 1 \pmod 4$, Theorem 2.3 tells us that $\left[5^{1000}\right] = [1]$ in $\mathbb{Z}_4$.

6. Given $n \mid (a - b)$ so that $a - b = nq$ for some integer q. Since $k \mid n$ it follows that $k \mid (a - b)$ and therefore $a \equiv b \pmod k$.

7. By Corollary 2.5, $a \equiv 0, 1, 2$ or $3 \pmod 4$. Theorem 2.2 implies $a^2 \equiv 0, 1 \pmod 4$. Therefore a^2 cannot be congruent to either 2 or 3 (mod 4).

8. By the division algorithm, any integer n is expressible as $n = 4q + r$ where $r \in \{0, 1, 2, 3\}$, and $n \equiv r \pmod 4$. If r is 0 or 2 then n is even. Therefore if n is odd then $n \equiv 1$ or $3 \pmod 4$.

9. (a) $(n - a)^2 \equiv n^2 - 2na + a^2 \equiv a^2 \pmod n$ since $n \equiv 0 \pmod n$.
(b) $(2n - a)^2 \equiv 4n^2 - 4na + a^2 \equiv a^2 \pmod{4n}$ since $4n \equiv 0 \pmod{4n}$.

10. Suppose the base ten digits of a are $(c_n c_{n-1} \ldots c_1 c_0)$. (Compare Exercise 1.2.32). Then $a = c_n 10^n + c_{n-1} 10^{n-1} + \ldots c_1 10 + c_0 \equiv c_0 \pmod{10}$, since $10^k \equiv 0 \pmod{10}$ for every $k \geq 1$.

11. Since there are infinitely many primes (Exercise 1.3.25) there exists a prime $p > |a - b|$. By hypothesis, $p \mid (a - b)$ so the only possibility is $a - b = 0$ and $a = b$.

12. If $p \equiv 0, 2$ or $4 \pmod 6$, then p is divisible by 2. If $p \equiv 0$ or $3 \pmod 6$ then p is divisible by 3. Since p is a prime > 3 these cases cannot occur, so that $p \equiv 1$ or $5 \pmod 6$. By Theorem 2.3 this says that $[p] = [1]$ or $[5]$ in $\mathbb{Z}_6$.

13. Suppose r, r' are the remainders for a and b, respectively. Theorem 2.3 and Corollary 2.5 imply: $a \equiv b \pmod n$ if and only if $[a] = [b]$ if and only if $[r] = [r']$. Then $r = r'$ as in the proof of Corollary 2.5(2).

14. (a) Here is one example: $a = b = 2$ and $n = 4$.
(b) The assertion is: if $n \mid ab$ then either $n \mid a$ or $n \mid b$. This is true when n is prime by Theorem 1.8.

15. Since $(a, n) = 1$ there exist integers u, v such that $au + nv = 1$, by Theorem 1.3. Therefore $au \equiv au + nv \equiv 1 \pmod{n}$, and we can choose $b = u$.

16. Given that $a \equiv 1 \pmod{n}$, we have $a = nq + 1$ for some integer q. Then (a, n) must divide $a - nq = 1$, so $(a, n) = 1$. One example to see that the converse is false is to use $a = 2$ and $n = 3$. Then $(a, n) = 1$ but $[a] \neq [1]$.

17. Since $10 \equiv -1 \pmod{11}$, Theorem 2.2 (repeated) shows that $10^n \equiv (-l)^n \pmod{11}$.

18. By Exercise 23 we have $125698 \equiv 31 \equiv 4 \pmod{9}$, $23797 \equiv 28 \equiv 1 \pmod{9}$ and $2891235306 \equiv 39 \equiv 12 \equiv 3 \pmod{9}$. Since $4{\cdot}1 \not\equiv 3 \pmod{9}$ the conclusion follows.

19. Proof: If $[a] = [b]$ then $a \equiv b \pmod{n}$ so that $a = b + nk$ for some integer k. Then $(a, n) = (b, n)$ using Lemma 1.7.

20. (a) One counterexample occurs when $a = 0$, $b = 2$ and $n = 4$.
(b) Given $a^2 \equiv b^2 \pmod{n}$, we have $n \mid (a^2 - b^2) = (a + b)(a - b)$. Since n is prime, use Theorem 1.8 to conclude that either $n \mid (a + b)$ or $n \mid (a - b)$.Therefore, either $a \equiv b \pmod{n}$ or $a \equiv -b \pmod{n}$.

21. (a) Since $10 \equiv 1 \pmod{9}$, Theorem 2.2 (repeated) shows that $10^n \equiv 1 \pmod{9}$.
(b) (Compare Exercise 1.2.32). Express integer a in base ten notation: $a = c_n 10^n + \ldots + c_1 10 + c_0$. Then $a \equiv c_n + c_{n-t} + \ldots c_1 + c_0 \pmod{9}$, since $10^k \equiv 1 \pmod{9}$.

22. (a) Here is one example: $a = 2$, $b = 0$, $c = 2$, $n = 4$.
(b) We have $n \mid ab - ac = a(b - c)$. Since $(a, n) = l$ Theorem 1.5 implies that $n \mid (b - c)$ and therefore $b \equiv c \pmod{n}$.

2.2 Modular Arithmetic

1. (a) Answered in the text.

(b)

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

−	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(c) Answered in the text.

(d)

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

However, the notation must be changed to correspond to the new notation. See the tables in Example 2 to see what it must look like.

2. To solve $x^2 \oplus x = [0]$ in $\mathbb{Z}_4$, substitute each of $[0], [1], [2]$, and $[3]$ in the equation to see if it is a solution:

x	$x^2 \oplus x$	Is $x^2 \oplus x = [0]$?
$[0]$	$[0] \otimes [0] \oplus [0] = [0] + [0] = [0]$	Yes; solution.
$[1]$	$[1] \otimes [1] \oplus [1] = [1] + [1] = [2]$	No.
$[2]$	$[2] \otimes [2] \oplus [2] = [0] + [2] = [2]$	No.
$[3]$	$[3] \otimes [3] \oplus [3] = [1] \oplus [3] = [0]$	Yes; solution.

3. $x = 1$, 3, 5 or 7 in $\mathbb{Z}_0$. However, the notation should be changed to use, for example, [3] instead of 3.

4. $x = 1$, 2, 3 or 4 in $\mathbb{Z}_5$. However, the notation should be changed to use, for example, [3] instead of 3.

5. $x = 1$, 2, 4, 5 in $\mathbb{Z}_6$. However, the notation should be changed to use, for example, [3] instead of 3.

6. To solve $x^2 \oplus [8] \otimes x = [0]$ in $\mathbb{Z}_9$, substitute each of $[0], [1], [2], \dots, [8]$ in the equation to see if it is a solution:

x	$x^2 \oplus [8] \otimes x$	Is $x^2 \oplus [8] \otimes x = [0]$?
$[0]$	$[0] \otimes [0] \oplus [8] \otimes [0] = [0] + [0] = [0]$	Yes; solution.
$[1]$	$[1] \otimes [1] \oplus [8] \otimes [1] = [1] + [8] = [0]$	Yes; solution.
$[2]$	$[2] \otimes [2] \oplus [8] \otimes [2] = [4] + [7] = [2]$	No.
$[3]$	$[3] \otimes [3] \oplus [8] \otimes [3] = [0] \oplus [6] = [6]$	No.
$[4]$	$[4] \otimes [4] \oplus [8] \otimes [4] = [7] \oplus [5] = [3]$	No.
$[5]$	$[5] \otimes [5] \oplus [8] \otimes [5] = [7] \oplus [4] = [2]$	No.
$[6]$	$[6] \otimes [6] \oplus [8] \otimes [6] = [0] \oplus [3] = [3]$	No.
$[7]$	$[7] \otimes [7] \oplus [8] \otimes [7] = [4] \oplus [2] = [6]$	No.
$[8]$	$[8] \otimes [8] \oplus [8] \otimes [8] = [1] \oplus [1] = [2]$	No.

The solutions are $x = [0]$ and $x = [1]$.

7. To solve $x^3 \oplus x^2 \oplus x \oplus [1] = [0]$ in $\mathbb{Z}_8$, substitute each of $[0], [1], [2], \dots, [7]$ in the equation to see if it is a solution:

x	$x^3 \oplus x^2 \oplus x \oplus [1]$	Is $x^3 \oplus x^2 \oplus x \oplus [1] = [0]$?
$[0]$	$[1]$	No.
$[1]$	$[4]$	No.
$[2]$	$[7]$	No.
$[3]$	$[0]$	No.
$[4]$	$[5]$	No.
$[5]$	$[4]$	No.
$[6]$	$[3]$	No.
$[7]$	$[0]$	Yes; solution.

The only solution is $x = [7]$.

8. To solve $x^3 + x^2 = [2]$ in $\mathbb{Z}_{10}$, substitute each of $[0], [1], \dots, [9]$ in the equation to see if it is a

solution:

x	$x^3 \oplus x^2$	Is $x^3 \oplus x^2 = [2]$?
[0]	[0]	No.
[1]	[2]	Yes; solution.
[2]	[2]	Yes; solution..
[3]	[6]	No.
[4]	[0]	No.
[5]	[0]	No.
[6]	[2]	Yes; solution.
[7]	[2]	Yes; solution.
[8]	[6]	No.
[9]	[0]	No.

The solutions are $x = [1], [2], [6]$, and $[7]$.

9. (a) $a = 3$ or 5. (b) $a = 2$ or 3. (c) No such element exists in $\mathbb{Z}_6$.

However, the notation should be changed to use, for example, [3] instead of 3.

10. Part 3: $[a] \oplus [b] = [a + b] = [b + a] = [b] \oplus [a]$ since $a + b = b + a$ in $\mathbb{Z}$.

Part 7: $[a] \odot ([b] \odot [c]) = [a] \odot [be] = [a(bc)] = [(ab)c] = [ab] \odot [c] = ([a] \odot [b]) \odot [c]$.

Part 8: $[a] \odot ([b] \oplus [c]) = [a] \odot [b + c] = [a(b + c)] = [ab + ac] = [ab] \oplus [ac] = ([a] \odot [b]) \oplus ([a \odot [c])$.

Part 9: $[a] \odot [b] = [ab] = [ba] = [b] \odot [a]$.

11. Every value of x satisfies these equations.

12. See Exercise 2.1.14.

13. See Exercise 2.1.22.

14. (a) $x = 0$ or 4 in $\mathbb{Z}_5$. (b) $x = 0, 2, 3$ or 5 in $\mathbb{Z}_6$.

However, the notation should be changed to use, for example, [3] instead of 3.

15. (a) $(a + b)^5 = a^5 + b^5$ in $\mathbb{Z}_5$. (b) $(a + b)^3 = a^3 + b^3$ in $\mathbb{Z}_3$.

(c) $(a + b)^2 = a^2 + b^2$ in $\mathbb{Z}_2$.

(d) One is led to conjecture that $(a + b)^7 = a^7 + b^7$ in $\mathbb{Z}_7$.

To investigate the general result for any prime exponent, use the Binomial Theorem and Exercise 1.4.13.

However, the notation should be changed to use, for example, $[a]$ instead of a.

16. (a) $a = 1, 2, 3$ or 4 in $\mathbb{Z}_5$. (b) $a = 1$ or 3 in $\mathbb{Z}_4$.

(c) $a = 1$ or 2 in $\mathbb{Z}_3$ (d) a = l or 5 in $\mathbb{Z}_6$.

However, the notation should be changed to use, for example, [3] instead of 3.

2.3 The Structure of $\mathbb{Z}_p$ (p Prime) and $\mathbb{Z}_n$

1. (a) 1, 2, 3, 4, 5, 6 (b) 1, 3, 5, 7

(c) 1, 2, 4, 5, 7, 8 (d) 1, 3, 7, 9

2. (a) Since 7 is prime, part (3) of Theorem 2.8 says that there are no zero divisors in $\mathbb{Z}_7$.

(b) The zero divisors are 2, 4, and 6, since $2 \cdot 4 = 0$ and $6 \cdot 4 = 0$. Further computations will show that the other elements of $\mathbb{Z}_8$ are not zero divisors.

(c) The zero divisors are 3 and 6, since $3 \cdot 6 = 0$. Further computations will show that the other elements of $\mathbb{Z}_9$ are not zero divisors.

(d) The zero divisors are $2, 4, 5, 6$, and 8, since $2 \cdot 5 = 4 \cdot 5 = 6 \cdot 5 = 8 \cdot 5 = 0$. Further computations will show that the other elements of $\mathbb{Z}_{10}$ are not zero divisors.

3. In $\mathbb{Z}_n$, it appears that every nonzero element is either a unit or a zero divisor.

4. (a) 1 solution in $\mathbb{Z}_7$ (b) 2 solutions in $\mathbb{Z}_8$

(c) 0 solutions in $\mathbb{Z}_9$ (d) 2 solutions in $\mathbb{Z}_{|0}$.

5. We first show that $ab \neq 0$. If $ab = 0$, then since a is a unit, then $a^{-1}ab = 0$, so that $b = 0$. But b is a zero divisor, so that $b \neq 0$ and thus $ab \neq 0$. Now, since b is a zero divisor, choose $c \neq 0$ such that $bc = 0$; then $(ab)c = a(bc) = 0$ shows that ab is also a zero divisor.

6. Since n is composite, write $n = ab$ where $1 < a, b < n$. Then in $\mathbb{Z}_n$, $[a] \neq 0$ and $[b] \neq 0$, since both a and b are less than n, but $[a][b] = [ab] = [n] = 0$, so that a and b are zero divisors.

7. If $ab = 0$ in $\mathbb{Z}_p$ then $ab \equiv 0 \pmod{p}$ so that $p \mid ab$. By Theorem 1.8 we conclude that $p \mid a$ or $p \mid b$. Then $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. Equivalently, $a = 0$ or $b = 0$ in $\mathbb{Z}_p$.

8. (a) For instance choose a even and b odd. (b) Yes.

9. (a) Suppose a is a unit. Choose b such that $ab = 0$. Then since a is a unit, we have $a^{-1}ab = a^{-1}0 = 0$, so that $b = 0$. Thus a is not a zero divisor, since any such b must be zero.

(b) This statement is the contrapositive of part (a), so is also true.

10. No element can be both a unit and a zero divisor, by Exercise 9. Choose $x \neq 0 \in \mathbb{Z}_n$, and consider the set of products $\{x \cdot 1, x \cdot 2, \ldots, x \cdot (n-1)\}$. This set has $n-1$ elements. If x is not a zero divisor, then 0 is not one of those elements. So there are two possibilities: either no element is duplicated in that list, or there is a duplicate. If there is no duplicate, then since there are $n-1$ elements and $n-1$ possible values, one of the elements must be 1; that is, for some $a \in \mathbb{Z}_n$, we have $x \cdot a = 1$. Thus x is a unit. If there is a duplicate, say $x \cdot a = x \cdot b$, then $x \cdot (a-b) = 0$, so that x is a zero divisor, which contradicts our original assumption. This shows that if x is not a zero divisor, then it is a unit.

11. Since a is a unit, the equation $ax = b$ has the solution $a^{-1}b$, since $aa^{-1}b = b$. Now, suppose that $ax = b$ and also $ay = b$. Then $a(x-y) = 0$. Since a is not a zero divisor, and $a \neq 0$ since it is a unit, it follows that $x - y = 0$ so that $x = y$. Hence the solution is unique.

12. If $x = [r]$ is a solution then $[ar] = [b]$ so that $ar \equiv b \pmod{n}$ and ar $- b = kn$ for some integer k. Then $d \mid a$ and $d \mid n$ implies $d \mid (\mathrm{ar} - kn) = b$.

13. Since d divides each of a, b and n there are integers a_1, n_1, b_1. with $a = da_1$, $b = db_1$. and $n = dn_1$. By Theorem 1.3 there are integers u, v with $au + nv = d$ so that $au \equiv d \pmod{n}$. Therefore $a(ub_1) \equiv b_1 d = b \pmod{n}$ so that $x = [ub_1]$ is one solution. Since $an_1 = a_1 dn_1 = a_1 n \equiv 0 \pmod{n}$ we see that $x = [ub_1 + n_1 t]$ is a solution for every integer t.

14. (a) If $[ub_1 + sn_1]$ and $[ub_1 + tn_1]$ are equal in $\mathbb{Z}_n$ for some $0 \leq s < t < d$, then $n \mid (\mathrm{t}n_1 - \mathrm{s}n_1) = (t-s)n_1$ so that $d \mid (t-s)$ contrary to $0 < (t-s) < d$.
    (b) If $x = [r]$ is a solution then $[ar] = [b] = [a \cdot ub_1]$ so that $n \mid a(r - ub_1)$ so that $a(r - ub_1) = nw$ for some integer w. Cancel d to obtain $a_1(r - ub_1) = n_1 w$. Since $(a_1, n_1) = 1$, (Why?) Theorem 1.5 implies $n_1 \mid (r - ub_1)$ so that $r = ub_1 + tn_1$ for some t. Then $x = [r] = [ub_1 + tn_1]$. Divide t by d to get $t = dq + k$ where $0 \leq k < d$. Then $x = [ub_1 + (dq + k)n_1] = [ub_1 + kn_1]$ because $[dn_1] = [n] = [0]$.

15. (a) $15x = 9$ in Z_{18} if and only if $15x \equiv 9 \pmod{18}$ if and only if $5x \equiv 3 \pmod{6}$ if and only if $x \equiv 3 \pmod{6}$ if and only if $x \equiv 3, 9, 15 \pmod{18}$ if and only if $x = [3], [9], [15]$ in Z_{18}.
    (b) $x = 3, 16, 29, 42$ or 55 in Z_{65}.

16. By Exercise 10, every nonzero element of $\mathbb{Z}_n$ is a unit or a zero divisor, but not both. So the statement we are trying to prove is equivalent to the following statement: If $a \neq 0$ and b are elements of $\mathbb{Z}_n$ and $ax = b$ has no solutions in $\mathbb{Z}_n$, prove that a is not a unit. The contrapositive of this statement, which is equivalent to the statement itself, is: If $a \neq 0$ and b are elements of $\mathbb{Z}_n$ and a is a unit, then $ax = b$ has at least one solution in $\mathbb{Z}_n$. But Exercise 11 proves this statement.

17. Suppose that a and b are units. Then $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1$, so that ab is a unit.

18. See the Hint when $0 < 1$. Otherwise, if $0 \not< 1$, then since $0 = 1$, we must have $1 < 0$ since we have fully ordered $\mathbb{Z}_n$. Adding 1 to both sides repeatedly, using rule (ii), gives $n-1 < n-2 < \cdots < 1 < 0$, so that, by rule (i), $n - 1 < 0$. Now add 1 to both sides to get $0 < 1$, which is a contradiction.

Chapter 3

Rings

3.1 Definition and Examples of Rings

1. (a) closure for addition. (b) axiom 5 (additive inverses)

2. The closure axioms are quickly seen from the tables (only the symbols 0, e, b, c appear). Commutativity of an operation appears as a symmetry of the table: the products xy and yx will appear in the table in positions which are symmetric relative to the "main diagonal". The system is commutative if these symmetrically placed entries are equal. Equivalently, the entries of the k^{th} row and the k^{th} column of the table are identical. In this example both operations are commutative. Also 0 is the zero element since the row for 0 is (0, e, b, c) which is identical with the top (index) row. Similarly we read from the other table that e is the multiplicative identity element. Axiom 4 (additive inverses) follows since 0 occurs in each row of the addition table. Since we are assuming the other axioms, R is a commutative ring.

3. As in Exercise 2 we can read quickly from the tables that the operations are closed and commutative. Also 0 is the zero element, and e is the multiplicative identity. Additive inverses exist since there is a 0 in every row of the addition table. Finally, multiplicative inverses exist for the non-zero elements e, a, b since e occurs in every row (and column) indexed by those entries. Since we are assuming the other axioms, F is a field.

4. Use the matrices from the end of Example 6:

$$\begin{pmatrix}4&6\\2&3\end{pmatrix}\begin{pmatrix}-3&-9\\2&6\end{pmatrix}=\begin{pmatrix}4(-3)+6\cdot 2&4(-9)+6\cdot 6\\2(-3)+3\cdot 2&2(-9)+3\cdot 6\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$$
$$\begin{pmatrix}-3&-9\\2&6\end{pmatrix}\begin{pmatrix}4&6\\2&3\end{pmatrix}=\begin{pmatrix}-3\cdot 4-9\cdot 2&-3\cdot 6-9\cdot 3\\2\cdot 4+6\cdot 2&2\cdot 6+6\cdot 3\end{pmatrix}=\begin{pmatrix}-30&-45\\20&30\end{pmatrix}$$

5. (a) This is a subring without identity; all products in this ring are zero.

   (b) This is a subring with the identity $\begin{pmatrix}1&0\\0&1\end{pmatrix}$.

   (c) This is not a subring. For example,

$$\begin{pmatrix}1&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}=\begin{pmatrix}2&1\\1&1\end{pmatrix},$$

   which is not of the required form.

(d) This is a subring without identity.

(e) This is a subring with the identity $\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$.

(f) This is a subring with the identity $\begin{pmatrix}1 & 0\\0 & 0\end{pmatrix}$.

6. (a) Check the axioms. Since the sum and product of two multiples of 3 is again a multiple of 3 the closure axioms (1 and 6) hold. Since 0 is a multiple of 3, R has an additive identity element (Axiom 4), If a is a multiple of 3 then the solution of $a + x = 0$ (namely $-a$) is also a multiple of 3, and so Axiom 5 holds. The other axioms (associativity, commutativity, distributivity) hold for all integers and therefore are true in R.
   (b) The same proof works with k everywhere in place of 3.

7. Axiom 1 is satisfied since $a\sqrt{2} + b\sqrt{2} = (a+b)\sqrt{2}$, so if a and b are integers, then $(a+b)\sqrt{2} \in K$. Axiom 2 is satisfied since

$$\begin{aligned}a\sqrt{2} + (b\sqrt{2} + c\sqrt{2}) = a\sqrt{2} + (b+c)\sqrt{2} = (a+b+c)\sqrt{2} &= (a+b)\sqrt{2} + c\sqrt{2}\\ &= (a\sqrt{2} + b\sqrt{2}) + c\sqrt{2}.\end{aligned}$$

Axiom 3 is satisfied since $a\sqrt{2} + b\sqrt{2} = (a+b)\sqrt{2} = (b+a)\sqrt{2} = b\sqrt{2} + a\sqrt{2}$. The additive identity is $0 = 0\sqrt{2}$, so Axiom 4 is satisfied. Given $a\sqrt{2} \in K$, the element $(-a)\sqrt{2}$ is also in K, and $a\sqrt{2} + (-a)\sqrt{2} = (a-a)\sqrt{2} = 0\sqrt{2}$, so Axiom 5 is also satisfied.

However, K is not a ring, since if $a\sqrt{2}, b\sqrt{2} \in K$, then $(a\sqrt{2})(b\sqrt{2}) = 2ab$ is not in K since it is not an integer multiple of $\sqrt{2}$.

8. No, it is not closed under addition.

9. (a) $R^* = \{(0, 0), (1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\}$.
   (b) Check the properties in Theorem 3.2. If $r, r' \in R$ then $(r, r) + (r', r') = (r + r', r + r')$ and $(r, r)\cdot(r, r') = (rr', rr')$. Therefore R^* is closed under addition and multiplication. The zero element $(0, 0)$ is in R^* and additive inverses exist: The solution to $(r, r) + x = (0, 0)$ is $x = -(r, r) = (-r, -r)$ which does lie in R^*.

10. No, it is not a subring. For example, $(3, -3) \in S$ and $(4, -4) \in S$, but $(3, -3)\cdot(4, -4) = (12, 12) \notin S$ since $12 + 12 \neq 0$.

11. (a) **Axiom 1.** $\begin{pmatrix}a & a\\b & b\end{pmatrix} + \begin{pmatrix}c & c\\d & d\end{pmatrix} = \begin{pmatrix}a+c & a+c\\b+d & b+d\end{pmatrix} \in S$.

Axiom 2. This is similar to part (a); it follows since addition of reals is associative.

Axiom 3. This is similar to the previous parts:

$$\begin{pmatrix}a & a\\b & b\end{pmatrix} + \begin{pmatrix}c & c\\d & d\end{pmatrix} = \begin{pmatrix}a+c & a+c\\b+d & b+d\end{pmatrix} = \begin{pmatrix}c & c\\d & d\end{pmatrix} + \begin{pmatrix}a & a\\b & b\end{pmatrix}$$

Axiom 4. $\begin{pmatrix}0 & 0\\0 & 0\end{pmatrix} \in S$, and it is obviously an additive identity.

Axiom 5. The inverse of $\begin{pmatrix}a & a\\b & b\end{pmatrix}$ is $\begin{pmatrix}-a & -a\\-b & -b\end{pmatrix}$.

Axiom 6. $\begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} c & c \\ d & d \end{pmatrix} = \begin{pmatrix} ac+ad & ac+ad \\ bc+bd & bc+bd \end{pmatrix} \in S.$

Axiom 7.

$$\begin{aligned}
\begin{pmatrix} a & a \\ b & b \end{pmatrix}\left(\begin{pmatrix} c & c \\ d & d \end{pmatrix}\begin{pmatrix} e & e \\ f & f \end{pmatrix}\right) &= \begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} ce+cf & ce+cf \\ de+df & de+df \end{pmatrix} \\
&= \begin{pmatrix} a(ce+cf)+a(de+df) & a(ce+cf)+a(de+df) \\ b(ce+cf)+b(de+df) & b(ce+cf)+b(de+df) \end{pmatrix} \\
&= \begin{pmatrix} ace+acf+ade+adf & ace+acf+ade+adf \\ bce+bcf+bde+bdf & bce+bcf+bde+bdf \end{pmatrix} \\
\left(\begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} c & c \\ d & d \end{pmatrix}\right)\begin{pmatrix} e & e \\ f & f \end{pmatrix} &= \begin{pmatrix} ac+ad & ac+ad \\ bc+bd & bc+bd \end{pmatrix}\begin{pmatrix} e & e \\ f & f \end{pmatrix} \\
&= \begin{pmatrix} (ac+ad)e+(ac+ad)f & (ac+ad)e+(ac+ad)f \\ (bc+bd)e+(bc+bd)f & (bc+bd)e+(bc+bd)f \end{pmatrix} \\
&= \begin{pmatrix} ace+acf+ade+adf & ace+acf+ade+adf \\ bce+bcf+bde+bdf & bce+bcf+bde+bdf \end{pmatrix}.
\end{aligned}$$

Axiom 8.

$$\begin{aligned}
\begin{pmatrix} a & a \\ b & b \end{pmatrix}\left(\begin{pmatrix} c & c \\ d & d \end{pmatrix}+\begin{pmatrix} e & e \\ f & f \end{pmatrix}\right) &= \begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} c+e & c+e \\ d+f & d+f \end{pmatrix} \\
&= \begin{pmatrix} a(c+e)+a(d+f) & a(c+e)+a(d+f) \\ b(c+e)+b(d+f) & b(c+e)+b(d+f) \end{pmatrix} \\
&= \begin{pmatrix} ac+ae+ad+af & ac+ae+ad+af \\ bc+be+bd+bf & bc+be+bd+bf \end{pmatrix} \\
\begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} c & c \\ d & d \end{pmatrix}+\begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} e & e \\ f & f \end{pmatrix} &= \begin{pmatrix} ac+ad & ac+ad \\ bc+bd & bc+bd \end{pmatrix}+\begin{pmatrix} ae+af & ae+af \\ be+bf & be+bf \end{pmatrix} \\
&= \begin{pmatrix} ac+ae+ad+af & ac+ae+ad+af \\ bc+be+bd+bf & bc+be+bd+bf \end{pmatrix}
\end{aligned}$$

Since S satisfies all 8 axioms, it is a ring.

(b) Note that $J \in S$, and that

$$\begin{pmatrix} a & a \\ b & b \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a\cdot 1+b\cdot 0 & a\cdot 1+b\cdot 0 \\ b\cdot 1+a\cdot 0 & b\cdot 1+a\cdot 0 \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix}.$$

Thus J is a right identity.

(c) We have

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 2 & 2 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1\cdot 2+1\cdot 1 & 1\cdot 2+1\cdot 1 \\ 0\cdot 2+0\cdot 1 & 0\cdot 2+0\cdot 1 \end{pmatrix} = \begin{pmatrix} 3 & 3 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}.$$

12. $\mathbb{Z}$ [i] is closed under addition and multiplication. For example $(a + bi)\cdot(c + di) = (ac - bd) + (ad + bc)i$. The zero element and additive inverses exist in $\mathbb{Z}[i]$, (compare Exercise 9).

13. Since $(a + b\sqrt{2}\,) + (c + d\sqrt{2}\,) = (a + c) + (b + d)\sqrt{2}$ and $(a + b\sqrt{2}\,)\cdot(c + d\sqrt{2}\,) = (ac + 2bd) + (ad + bc)\sqrt{2}$ we see that $\mathbb{Z}[\sqrt{2}\,]$ is closed under addition and multiplication. The zero element $0 = 0 + 0\sqrt{2}$ is in the set and additive inverses exist: $-(a + b\sqrt{2}) = (-a) + (-b)\sqrt{2}$. Apply Theorem 3.2.

14. Yes S is a subring (without identity). For instance to prove closure for addition suppose $f, g \in S$. Then $(f + g)(2) = f(2) + g(2) = 0 + 0 = 0$ so that $f + g \in S$.

15. (a) Answered in the text.

(b)

+	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(0,0)	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(1, 1)	(1, 1)	(0, 0)	(0, 1)	(1, 0)
(1, 0)	(1, 0)	(0, 1)	(0, 0)	(1, 1)
(0, 1)	(0, 1)	(1, 0)	(1, l)	(0, 0)

−	(0, 0)	(1.1)	(1, 0)	(0, 1)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(1.1)	(0, 0)	(1, 1)	(1, 0)	(0, 1)
(1, 0)	(0, 0)	(1, 0)	(1, 0)	(0, 0)
(0, 1)	(0, 0)	(0, 1)	(0, 0)	(0, 1)

(c)

+	(0, 0)	(1, 1)	(2, 2)	(0, 1)	(1, 2)	(2, 0)	(1, 0)	(2, 1)	(0, 2)
(0, 0)	(0, 0)	(1, 1)	(2, 2)	(0, 1)	(1, 2)	(2, 0)	(1, 0)	(2, 1)	(0, 2)
(1, 1)	(1, 1)	(2, 2)	(0, 0)	(1, 2)	(2, 0)	(0, 1)	(2, 1)	(0, 2)	(1, 0)
(2, 2)	(2, 2)	(0, 0)	(1, 1)	(2, 0)	(0, 1)	(1, 2)	(0, 2)	(1, 0)	(2, 1)
(0, 1)	(0, 1)	(1, 2)	(2, 0)	(0, 2)	(1, 0)	(2, 1)	(1, 1)	(2, 2)	(0, 0)
(1, 2)	(1, 2)	(2, 0)	(0, 1)	(1, 0)	(2, 1)	(0, 2)	(2, 2)	(0, 0)	(1, 1)
(2, 0)	(2, 0)	(0, 1)	(1, 2)	(2, 1)	(0, 2)	(1, 0)	(0, 0)	(1, 1)	(2, 2)
(1, 0)	(1, 0)	(2, 1)	(0, 2)	(1, 1)	(2, 2)	(0, 0)	(2, 0)	(0, 1)	(1, 2)
(2, 1)	(2, 1)	(0, 2)	(1, 0)	(2, 2)	(0, 0)	(1, 1)	(0, 1)	(1, 2)	(2, 0)
(0, 2)	(0, 2)	(1, 0)	(2, 1)	(0, 0)	(1, 1)	(2, 2)	(1, 2)	(2, 0)	(0, 1)

−	(0, 0)	(1, 1)	(2, 2)	(0, 1)	(1, 2)	(2, 0)	(1, 0)	(2, 1)	(0, 2)
(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)	(0, 0)
(1, 1)	(0, 0)	(1, 1)	(2, 2)	(0, 1)	(1, 2)	(2, 0)	(1, 0)	(2, 1)	(0, 2)
(2, 2)	(0, 0)	(2, 2)	(1, 1)	(0, 2)	(2, 1)	(1, 0)	(2, 0)	(1, 2)	(0, 1)
(0, t)	(0, 0)	(0, 1)	(0, 2)	(0, 1)	(0, 2)	(0, 0)	(0, 0)	(0, 1)	(0, 2)
(1, 2)	(0, 0)	(1, 2)	(2, 1)	(0, 2)	(1, 1)	(2, 0)	(1, 0)	(2, 2)	(0, 1)
(2, 0)	(0, 0)	(2, 0)	(1, 0)	(0, 0)	(2, 0)	(1, 0)	(2, 0)	(1, 0)	(0, 0)
(1, 0)	(0, 0)	(1, 0)	(2, 0)	(0, 0)	(1, 0)	(2, 0)	(1, 0)	(2, 0)	(0, 0)
(2, 1)	(0, 0)	(2, 1)	(1, 2)	(0, 1)	(2, 2)	(1, 0)	(2, 0)	(1, 1)	(0, 2)
(0, 2)	(0, 0)	(0, 2)	(0, 1)	(0, 2)	(0, 1)	(0, 0)	(0, 0)	(0, 2)	(0, 1)

16. (a) For example,

$$\begin{pmatrix} 1 & 2 \\ -1 & -2 \end{pmatrix}, \begin{pmatrix} -3 & 5 \\ 5 & -3 \end{pmatrix}, \begin{pmatrix} 0 & 4 \\ 0 & -4 \end{pmatrix}.$$

(b) Suppose $B, C \in S$. Then since $M(\mathbb{R})$ is a ring, multiplication distributes over addition, so that $A(B + C) = AB + AC = 0 + 0 = 0$ since $B, C \in S$. Thus $B + C \in S$. Also, $A(BC) = (AB)C = 0 \cdot C = 0$, so that $BC \in S$. Certainly $0 \in S$. Finally, if $B \in S$, then $A(-B) = -AB = 0$, so that $-B \in S$ and thus condition (iv) for subrings is satisfied as well. Thus S is a subring of $M(\mathbb{R})$.

17. The axioms involving addition only (1, 2, 3, 4) certainly remain true in the new system. The remaining axioms are trivial: Closure: $ab = 0$ is always in $\mathbb{Z}$. Associativity: $a(bc) = 0 = (ab)c$. Distributivity: $a(b + c) = 0$ and $ab + ac = 0 + 0 = 0$. Also multiplication is commutative: $ab = 0 = ba$.

18. This is not a ring since the distributive law fails: $a(b + c) = 1$ while $ab + ac = 1 + 1 = 2$.

19. Answered in the text.

20. $R = 3{\cdot}\mathbb{Z}_{18}$ is of all the multiples of 3, that is, $R = \{\, k : k \ = 3\text{r}$ for some $r \in \mathbb{Z}_{\text{lg}}\}$. This observation makes it easy to check closure of the operations, the existence of a zero and of additive inverses. Therefore R is a subring (compare Exercise 21). If $3k$ is an identity element in R, then $(3k){\cdot}(3n) \equiv (3n) \pmod{18}$ for every n. Choosing $n = 2$ this implies $0 \equiv 6 \pmod{18}$, which is false. No identity exists in R.

21. $S = 2{\cdot}\mathbb{Z}_{10}$ is the set of all multiples of 2. Then S is a subring as in Exercise 16. Noting that $6.2 = 2$, $6.4 = 4$, $6.6 = 6$ and $6.8 = 8$, we see that 6 acts as an identity element in S.

22. Closure properties are clear. $a \oplus (b \oplus c) = a \oplus (b + c - \text{l}) = a + (b + c - \text{l}) - 1 = a + b + c - 2$. Checking that $(a \oplus b) \oplus c = a + b + c - 2$, we see addition is associative. Commutativity: $a \oplus b = a + b - 1 = b + a - 1 = b \oplus a$. Note that 1 is the "zero element" here: $1 \oplus a = \text{l} + a - \text{l} = a$. The "negative" of a is $2 - a$, because $a \oplus (2 - a) = a + (2 - a) - 1 = 1$, which is the "zero". For multiplication, $a \odot (b \odot c) = a \odot (b + c - bc) = a + (b + c - bc) - a(b + c - bc) = a + b + c - bc - ab - ac + abc$. Check that $(a \odot b) \odot c$ equals the same thing. Also $a \odot b = a + b - ab = b + a - ba = b \odot a$. For the distributive laws we need only check one side: $a \odot (b \odot c) = a \odot (b + c - \text{l}) = a + (b + c - \text{l}) - a(b + c - \text{l}) = (a + b - ab) + (a + c - ac) - 1 = (a \odot b) \oplus (a \odot c)$. Finally to prove it is an integral domain suppose $a \odot b = 1$, the "zero element". Then $a + b - ab = \text{l}$ so that $(\text{l} - a)(\text{l} - b) = 0$ in $\mathbb{Z}$. Therefore either $a = \text{l}$ or $b = \text{l}$. That is, either a or b must equal "zero".

23. Answered in the text.

24. The axioms for addition have been proved in Exercise 18. The multiplication is clearly closed in $\mathbb{Z}$, Commutativity of $\odot$ is easy. For associativity, $a \odot (b \odot c) = a(b \odot c) - (a + (b \odot c)) + 2 = a(bc - (b + c) + 2) - (a + (bc - (b + c) + 2) + 2 = abc - ab - ac - bc + a + b + c$. Check that $(a \odot b) \odot c$ equals the same thing. For distributivity: $a \odot (b \odot c) = a \odot (b + c - \text{l}) = a(b + c - \text{l}) - (a + (b + c - \text{l})) + 2 = ab + ac - 2a - b - c + 3 = (ab - a - b + 2) + (ac - a - c + 2) - 1 = (a \odot b) \oplus (a \odot c)$. Finally to prove it is an integral domain suppose $a \odot b = \text{l}$. Then $ab - (a + b) + 2 = \text{l}$ and $(a - \text{l})(b - 1) = 0$ in $\mathbb{Z}$ forcing $a = 1$ or $b = 1$.

25. Closure properties are clear. $a \oplus (b \oplus c) = a \oplus (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2$. Check that $(a \oplus b) \oplus c = a + b + c + 2$ to show that addition is associative. Commutativity: $a \oplus \mathrm{b} = a + b + 1 = b + a + \mathrm{l} = \mathrm{b} \oplus a$. Note that –1 is the "zero element" here: $(-1) \oplus a = -\mathrm{l} + a + \mathrm{l} = a$. The “negative” of a is $-2 - a$, because $a \oplus (-2 - a) = a + (-2 - a) + 1 = -1$, which is the “zero”. For multiplication: $a \odot (b \odot c) = a \odot (b\mathrm{c} + \mathrm{b} + c) = a(b\mathrm{c} + b + c) + a + (b\mathrm{c} + b + c) = ab\mathrm{c} + ab + ac + b\mathrm{c} + a + b + c$. Check that $(a \odot b) \odot c$ equals the same thing. Also $a \odot b = ab + a + b = ba + b + a = b \odot a$. Distributivity: $a \odot (b \odot c) = a \odot (b + c + \mathrm{l}) = a(b + c + 1) + a + (b + c + \mathrm{l}) = (ab + a + b) + (ac + a + c) + 1 = (a \odot b) \oplus (a \odot c)$. Finally to prove it is an integral domain suppose a $\odot\ b = -1$, the “zero element”. Then ab + a + $b = -\mathrm{l}$ so that $(\mathrm{l} + a)(\mathrm{l} + b) = 0$ in $\mathbb{Q}$. Therefore either $a = -\mathrm{l}$ or $b = -\mathrm{l}$. That is, either a or b must equal “zero”.

26. Yes. Closure is clear and so is the commutativity and associativity of $\oplus$. The zero element is 1 and the additive inverse of a is $\frac{1}{\mathrm{a}}$. Note that $a \odot b = a^{\mathrm{logb}} = \exp(\log(a) - \log(b))$, where $\exp(x) = e^{bx}$. From this the associativity and commutativity of $\odot$ are easily seen. Also $a \odot (b \odot c) = \exp(\log(a) - \log(b \oplus c)) = \exp(\log(a) - (\log(b) + \log(c))) = \exp(\log(a) - 1\mathrm{og}(b))\ {'}\exp(\log(a) - \log(c)) = (a \odot b) \oplus (a \odot c)$. Therefore L is a commutative ring. The identity element is e (the b*a*se of the log). To prove L is a field we start with $a \neq e$ in L and show that there exists b with $a \odot b = \mathrm{e}$. Equivalently we need $\log(a) - \log(b) = 1$ so that $b = \exp(\frac{1}{\log(\mathrm{b})})$ which does exist in L.

27. If $\frac{a}{p}, \frac{b}{q} \in S$, with p, q odd, then

$$\frac{a}{p} + \frac{b}{q} = \frac{aq + bp}{pq} \in S \text{ since } pq \text{ is odd}$$
$$\frac{a}{q} \cdot \frac{b}{q} = \frac{ab}{pq} \in S \text{ since } pq \text{ is odd.}$$

Thus S satisfies conditions (i) and (ii) for being a subring. Clearly $0 = \frac{0}{1} \in S$, satisfying (iii). Finally, if $\frac{a}{p} \in S$, then $\frac{-a}{p} \in S$, so that $\frac{a}{p} + x = 0$ has a solution. Thus S is a subring.

However, S is not a field, since for example the inverse of $\frac{2}{3}$ in $\mathbb{Q}$ is $\frac{3}{2}$, which cannot be written with an odd denominator (and an integral numerator). Thus $\frac{2}{3}$ does not have a multiplicative inverse in S.

28. Let r/p^i and s/p^i be typical elements of R. Then $r/p^i + s/p^j = (rp^i + sp^i)/p^{i+j}$ and $(r/p^i)(s/p^j) = (rs)/p^{i+j}$ both lie in R, so that R is closed under the operations. Since $\mathbb{Z} \subseteq R$ we know that $0, 1 \in R$ and R has additive inverses (if $x \in R$ then $-x = (-\mathrm{l})x \in R$).

29. $st = s(s + s) = ss + ss = t + t = s$. Similarly we have $ts = s$. Finally $tt = (s + s)t = st + st = s + s = t$.

30. There are several ways to produce the answers. For instance, $xy = x(x + x) = xx + xx = y + y = w$, Similarly $yx = w$. Then $zx = (x + y)x = xx + yx = y + w = y$ and similarly $xz = y$. Finally $yz = y(x + y) = yx + yy = w + w = w$.

31. (a) Let S be the set of scalar matrices, and write A_k for the scalar matrix $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. Then short computations show that $A_k + A_k = A_{2k} \in S$ and $A_k \cdot A_k = A_{k^2} \in S$. Clearly $0 \in S$. Finally, $A_k + A_{-k} = 0$, so that $A_k + x = 0$ has a solution. Thus S satisfies all four conditions for being a subring of $M(\mathbb{R})$, so it is a subring.

(b) If $A \in M(\mathbb{R})$ is an arbitrary matrix, we have

$$A_k A = \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}, \qquad AA_k = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} = \begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}.$$

(c) Suppose $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is such a matrix. Since $KA = AK$ for every $A \in M(\mathbb{R})$, we have for instance with $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$:

$$KA = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix}, \text{ while } AK = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

Since these two must be equal, we get $b = c = 0$, so that $K = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}$. Now choose $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$:

$$KA = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}, \text{ while } AK = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} = \begin{pmatrix} 0 & d \\ 0 & 0 \end{pmatrix}.$$

Since these two must be equal, we must have $a = d$, so that K is a scalar matrix.

32. If $a, b \in Z(R)$, then for all $r \in R$ we have $(a+b)r = ar+br = ra+rb = r(a+b)$, so that $a+b \in Z(R)$. Similarly, for all $r \in R$ we have $(ab)r = a(br) = a(rb) = (ar)b = (ra)b = r(ab)$, so that $ab \in Z(R)$. Clearly $0 \in Z(R)$ since $0r = r0 = 0$ for all $r \in R$. Finally, if $a \in Z(R)$, then also $-a \in Z(R)$, where $-a$ is a solution to $a + x = 0_R$, since $a + (-a) = 0$ implies that $(a + (-a))r = ar + (-a)r = 0$ and also that $r(a + (-a)) = ra + r(-a) = 0$. Thus $ar + (-a)r = ra + r(-a)$. But $ar = ra$, so that $ar + (-a)r = ar + r(-a)$. Let x be such that $ar + x = 0_R$; then $ar + (-a)r + x = (-a)r$ and $ar + r(-a) + x = r(-a)$, so that $(-a)r = r(-a)$ and $-a \in Z(R)$. Thus $Z(R)$ is a subring of R.

33. Since R and S are closed under addition and multiplication, Theorem 3.1 shows that $R \times S$ is also closed under addition and multiplication. Each of the commutative, associative and distributive laws for $R \times S$ follows from the corresponding law for R and S. For example, $(r, s)\ ((r', s')\ .\ (r'', s'')) = (r, s) \cdot (r'\mathrm{r}'', s's'') = (r(r'r''), s(s's'') = ((rr')r'', (ss')s'') = (rr', ss')\ (r'', s'') = ((r, s).(r', s'))-(r'', s'')$. We omit the verification of the other laws. The zero element is $(0_R\ 0_S)$ and the additive inverse is given by $-\ (r, s) = (-r, -s)$. If R and S each have an identity, it is easy to verify that $(1_R\ \mathrm{l}_S)$ is an identity for $R \times S$.

34. Generally if R is a ring with identity then $M(R)$ is also a ring with identity. The proof involves some direct calculations with the definitions of matrix addition and multiplication. We omit most of the details, but here is part of a proof for associativity of multiplication: Let
$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ and
$C = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$ in $M(R)$. Then $AB = \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$ and the upper left entry of
$(AB)C$ is $(a_{11}b_{I1} + a_{12}b_{21})c_{11} + (a_{11}b_{12}+a_{12}b_{22})c_{21}$. Similarly $BC = \begin{pmatrix} b_{11}c_{11} + b_{12}c_{21} & b_{11}c_{12} + b_{12}c_{22} \\ b_{21}c_{11} + b_{22}c_{21} & b_{21}c_{12} + b_{22}c_{22} \end{pmatrix}$

and the upper left entry of $A(BC)$ is $a_{11}(b_{11}c_{11} + b_{12}c_{21}) + a_{12}(b_{21}c_{11} + b_{22}c_{21})$. These entries are equal, and three similar calculations show that $(AB)C = A(BC)$.

Furthermore $M(R)$ is noncommutative since for example the matrices $\mathrm{U} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\mathrm{V} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ do not commute: $\mathrm{UV} \neq \mathrm{VU}$. To complete the problem we apply this information to the ring $\mathbb{R} = \mathbb{Z}_2$ and note that there are 16 elements in the ring $\mathrm{M}(\mathbb{Z}_2)$.

35. Answered in the text. The example shows that both assertions are false.

36. To show that f and g lie in T check the continuity. Since the functions 0, $x - 2$ and $2 - x$ are clearly continuous, the question is whether f and g are continuous at $x = 2$, The one-sided limits at $x = 2$ are :

$$\lim_{x \to 2^-} \mathrm{f(x)} = \lim_{x \to 2^-} 0 = 0 \qquad \text{and} \qquad \lim_{x \to 2^+} \mathrm{f(x)} = \lim_{x \to 2^+} (\mathrm{x}-2) = 0.$$

Since they are equal, the function f is continuous at 2. Similarly g is continuous. If $x \leq 2$ then $(fg)(x) = f(x).g(x) = 0\ (2 - x) = 0$. If $2 < x$ then $(fg)(x) = f(x)\ g(x) = (x - 2).0 = 0$. Therefore $fg = 0$ in the ring T. Since $f \neq 0$ and $g \neq 0$ we conclude that T is not an integral domain.

37. (a) If $A, B \in M(R)$, then the entries of $A + B$ and of AB are sums and products of the entries of A and B; since those are elements of R, so are their sums and products. Thus $A + B$ and $AB \in M(R)$, satisfying Axioms 1 and 6. Since addition in $M(R)$ is component by component, and addition in R is commutative and associative, the same holds for $M(R)$, so that Axioms 2 and 3 are satisfied. $\mathbf{0} \in M(R)$ is the matrix all of whose entries are 0, satisfying Axiom 4. For axiom 5, the inverse of a matrix $A \in M(R)$ is the matrix $-A$ each of whose entries is the additive inverse in R of the corresponding entry of A. For axioms 7 and 8, let

$$a = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \quad b = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, \quad c = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}.$$

Then

$$\begin{aligned}
a(bc) &= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \left(\begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \right) = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} b_1c_1 + b_2c_3 & b_1c_2 + b_2c_4 \\ b_3c_1 + b_4c_3 & b_3c_2 + b_4c_4 \end{pmatrix} \\
&= \begin{pmatrix} a_1(b_1c_1 + b_2c_3) + a_2(b_3c_1 + b_4c_3) & a_1(b_1c_2 + b_2c_4) + a_2(b_3c_2 + b_4c_4) \\ a_3(b_1c_1 + b_2c_3) + a_4(b_3c_1 + b_4c_3) & a_3(b_1c_2 + b_2c_4) + a_4(b_3c_2 + b_4c_4) \end{pmatrix} \\
&= \begin{pmatrix} a_1b_1c_1 + a_1b_2c_3 + a_2b_3c_1 + a_2b_4c_1 & a_1b_1c_2 + a_1b_2c_4 + a_2b_3c_2 + a_2b_4c_4 \\ a_3b_1c_1 + a_3b_2c_3 + a_4b_3c_1 + a_4b_4c_3 & a_3b_1c_2 + a_3b_2c_4 + a_4b_3c_2 + a_4b_4c_4 \end{pmatrix} \\
(ab)c &= \left(\begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \right) \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} = \begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \\
&= \begin{pmatrix} (a_1b_1 + a_2b_3)c_1 + (a_1b_2 + a_2b_4)c_3 & (a_1b_1 + a_2b_3)c_2 + (a_1b_2 + a_2b_4)c_4 \\ (a_3b_1 + a_4b_3)c_1 + (a_3b_2 + a_4b_4)c_3 & (a_3b_1 + a_4b_3)c_2 + (a_3b_2 + a_4b_4)c_4 \end{pmatrix} \\
&= \begin{pmatrix} a_1b_1c_1 + a_1b_2c_3 + a_2b_3c_1 + a_2b_4c_3 & a_1b_1c_1 + a_1b_2c_4 + a_2b_3c_2 + a_2b_4c_4 \\ a_3b_1c_1 + a_3b_2c_3 + a_4b_3c_1 + a_4b_4c_3 & a_3b_1c_2 + a_3b_2c_4 + a_4b_3c_2 + a_4b_4c_4 \end{pmatrix}
\end{aligned}$$

The computation for Axiom 8 is similar but simpler. Thus $M(R)$ is a ring.

(b) If e is the identity in R, then $I = \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix}$ is the identity in $M(R)$, since if $A \in M(R)$, we have

$$IA = \begin{pmatrix} e & 0 \\ 0 & e \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} e \cdot a + 0 \cdot c & e \cdot b + 0 \cdot d \\ 0 \cdot a + e \cdot c & 0 \cdot b + e \cdot d \end{pmatrix} = A,$$

and similarly for AI.

38. Suppose $r, s \in A_R$. Then $a(r+s) = ar + as = 0 + 0 = 0$, so that $r + s \in A_R$. Also $a(rs) = (ar)s = 0s = 0$, so that $rs \in A_R$. Clearly $0 \in A_R$. Finally, if $r \in A_R$, then $-r \in A_R$, where $-r$ is a solution to $r + x = 0_R$. This is true since $r + (-r) = 0$, so that $a(r + (-r)) = ar + a(-r) = 0$. But $ar = 0$, so that $0 + a(-r) = a(-r) = 0$. Hence A_R is a subring of R.

39. Since $(r + s\sqrt{2})(u + v\sqrt{2}) = (ru + 2sv) + (ru + su)\sqrt{2}$, the set $\mathbb{Q}(\sqrt{2}\,)$ is closed under multiplication. Closure under addition is easier to check. Since $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}\,)$ we have 0 and 1 there. Additive inverses are easy to check. To show that $\mathbb{Q}(\sqrt{2}\,)$ is a subfield we need to show that if $0 \neq r + s\sqrt{2}$ in $\mathbb{Q}(\sqrt{2}\,)$, then $(r + s\sqrt{2}\,)^{-1}$ also lies in $\mathbb{Q}(\sqrt{2}\,)$. To see this, "rationalize the denominator" to express $(r + s\sqrt{2}\,)^{-1} = \dfrac{r - s\sqrt{2}}{(r + s\sqrt{2})(r - s\sqrt{2}\,)} = \dfrac{r}{\delta} - \dfrac{r}{\delta}\sqrt{2}$ where $\delta = r^2 - 2\delta^2$.

40. Repeat the answer for Exercise 31, changing 2 to d in all the appropriate places.

41. (a) Let $A = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \in S$. Then

$$\begin{aligned}
A \begin{pmatrix} 0.5 & 0.5 \\ 0.5 & 0.5 \end{pmatrix} &= \begin{pmatrix} a(0.5) + a(0.5) & a(0.5) + a(0.5) \\ b(0.5) + b(0.5) & b(0.5) + b(0.5) \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix} = A \\
A \begin{pmatrix} 0.7 & 0.7 \\ 0.3 & 0.3 \end{pmatrix} &= \begin{pmatrix} a(0.7) + a(0.3) & a(0.7) + a(0.3) \\ b(0.7) + b(0.3) & b(0.7) + b(0.3) \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix} = A \\
A \begin{pmatrix} 2 & 2 \\ -1 & -1 \end{pmatrix} &= \begin{pmatrix} a(2) + a(-1) & a(2) + a(-1) \\ b(2) + b(-1) & b(2) + b(-1) \end{pmatrix} = \begin{pmatrix} a & a \\ b & b \end{pmatrix} = A.
\end{aligned}$$

(b) Suppose $B = \begin{pmatrix} x & x \\ y & y \end{pmatrix} \in S$. Then

$$AB = \begin{pmatrix} a & a \\ b & b \end{pmatrix} \begin{pmatrix} x & x \\ y & y \end{pmatrix} = \begin{pmatrix} ax+ay & ax+ay \\ bx+by & bx+by \end{pmatrix} = \begin{pmatrix} a(x+y) & a(x+y) \\ b(x+y) & b(x+y) \end{pmatrix}$$

Clearly $AB = A$ if and only if $x + y = 1$.

(c) Suppose B is as in the previous part, with $x + y = 1$. Then

$$BA = \begin{pmatrix} x & x \\ y & y \end{pmatrix} \begin{pmatrix} a & a \\ b & b \end{pmatrix} = \begin{pmatrix} xa+xb & xa+xb \\ ya+yb & ya+yb \end{pmatrix}$$

If $BA = A$, then $xa + xb = x(a + b) = a$ and $ya + yb = y(a + b) = b$, so that we must have

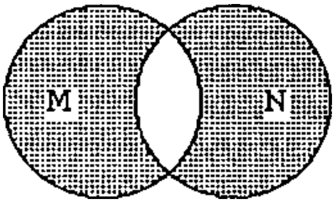
$$x + y = \frac{a}{a+b} + \frac{b}{a+b} = 1.$$

42. (a) Suppose $bv = 1_R$. Then if $bb = b$ we find $1_R = bv = (bb)v = b(bv) = bl_R = b$.
(b) Suppose $au = 1_R$. Then $ua \cdot ua = u(au)a = u1_Ra = ua$ and part (a) applies with $b = ua$. Therefore $ua= l_R$, as claimed.

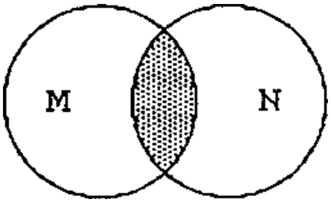
43. (a) Verifying these formulas is a routine calculation with 2 × 2 matrices.
(b) Showing closure under addition is easy. For multiplication: $(a + bi + cj + dk)$-$(a' + b'i + c'j + d'k) = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac\text{v} - bd' + ca' + db')j + (ad' + be' - cb' + da')k$. Since all the coefficients are real this answer lies in H. The commutative, associative and distributive laws are inherited from M(₵). Since the zero matrix and the identity matrix are in H, and H is closed under "negatives" we see that H is a subring. It is non-commutative since, for example, $ij \neq ji$.
(c) By explicit calculation we get $(a + bi + cj + dk)(a - bi - cj - dk) = (a^2 + b^2 + c + d)$. If $\alpha = (a + bi + cj + dk) \neq 0$ then $\Delta = (a^2 + b^2 + c^2 + d^2) \neq 0$ in R and $a^{-1} = \Delta^{-1}(a - bi - cj - dk)$ does lie in H.

(d) Setting $\alpha = bi + cj + dk$ we see from (c) that $\alpha^2 = -\alpha(-\alpha) = -(b^2 + \text{c}^2 + d^2)$. Then any choice of b, c, d € R with $b^2 + c^2 + d^2 = 1$ provides a quaternion α with $\alpha^2 = -1$.

44. (a) The sets M and N are indicated as disks in the pictures. (Such pictures are called "Venn diagrams".) The shaded parts indicate the sets $M + N$ and MN.

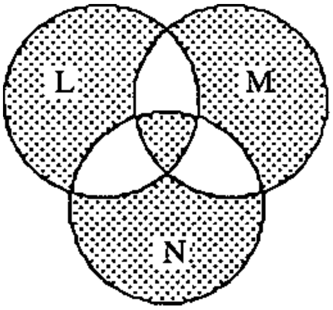


$M + N$

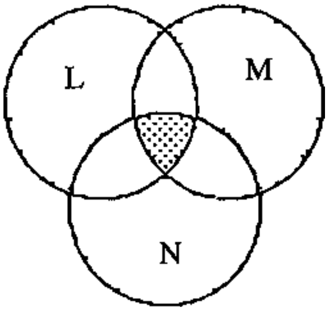


MN

The axioms can be "proved by picture" here. For instance the commutativity is clear. The associativity follows after considering the following pictures.

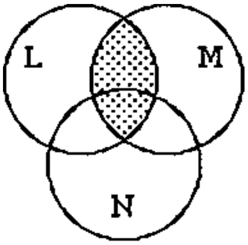


$L + M + N$

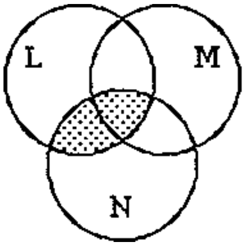


LMN

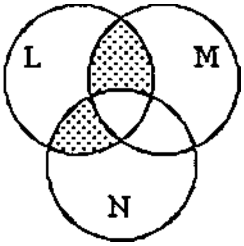
The distributive law is illustrated by drawing $LM + LN$ and comparing it to the picture for $L(M + N)$.



LM



LN



***L*(*M* + *N*)**

The zero element is the empty set Ø, since $M + \emptyset = (M\ ) \cup (\emptyset) = M$. The identity element is S since $SM = S \cap M = M$.

(b) $M^2 = M \cap M = M$ and $M + M = \emptyset \cup \emptyset\ = \emptyset$.

45. The axioms involving addition alone have already been verified. The closure of multiplication is clear from the formula. The associative, commutative and distributive laws can be checked by direct multiplication (compare Exercise 35). For example, $(a, b) \cdot ((a', b') + (a'', b'')) = (a, b) - (a' + a'', b' + b'') = (a(a' + a'') - b(b' + b''), a(b' + b'') + b(a' + a''))$ and $(a, b) - (a', b'') + (a, b) -(a'', b'') = (aa' - bb', ab' + ba') + (aa'' - bb'', ab'' + ba'') = (aa' - bb' + aa'' - bb'', ab' + ba' + ab'' + ba'')$. These quantities are equal, so the distributive law is verified. The element (1, 0) is the identity element. Therefore these operations make $\mathbb{R} \times \mathbb{R}$ into a commutative ring with identity. Note that $(a, b) \cdot (a, -b) = (a^2 + b^2, 0)$. If $(a, b) \neq (0, 0)$ then $a^2 + b^2 \neq 0$ and $(a/(a^2 + b^2), -b/(a^2 + b^2))$ is the inverse of (a, b). Hence this ring is a field.

46. Let r, s be any positive integers and let T be the subset of all multiples of r in the ring $\mathbb{Z}_{rs}$. Since $ar \equiv br \pmod{rs}$ if and only if $a \equiv b \pmod{s}$, we see that $T = \{0, r, 2r, 3r, \ldots, (s-1)r\}$ is the given subset. The closure of the operations in T and the existence of additive inverses is easy to check. For instance, if ar and br are typical elements of T then $ar + br = (a+b)r$ is also in T. Hence T is a subring.

    T has an identity element e if and only if $e = xr$ for some x and $(xr)(yr) \equiv (yr) \pmod{rs}$ for every y. This is equivalent to requiring $xr^2 \equiv r \pmod{rs}$, which becomes: $xr \equiv 1 \pmod{s}$. By Corollary 2.10, such an x exists whenever $(r, s) = 1$. Therefore, the subring T has an identity element e if and only if $(r, s) = 1$. In that case, there exist integers x, k satisfying $xr - ks = 1$ and $e = xr = ks + 1$.

3.2 Basic Properties of Rings

1. (a) $a^2 - ab + ba - b^2$
   (b) $a^3 + a^2b + aba + ba^2 + ab^2 + bab + b^2a + b^3$
   (c) $a^2 - b^2$ and $a^3 + 3\,a^2b + 3\,ab^2 + b^3$

2.

$$A^{-1} = \begin{pmatrix} \frac{5}{3\cdot5-2\cdot7} & -\frac{2}{3\cdot5-2\cdot7} \\ -\frac{7}{3\cdot5-2\cdot7} & \frac{3}{3\cdot5-2\cdot7} \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ 7 & 3 \end{pmatrix}$$

$$B^{-1} = \begin{pmatrix} \frac{5}{4\cdot5-3\cdot(-2)} & -\frac{3}{4\cdot5-3\cdot(-2)} \\ -\frac{-2}{4\cdot5-3\cdot(-2)} & \frac{4}{4\cdot5-3\cdot(-2)} \end{pmatrix} = \begin{pmatrix} \frac{5}{26} & -\frac{3}{26} \\ \frac{1}{13} & \frac{2}{13} \end{pmatrix}$$

$$C^{-1} = \begin{pmatrix} \frac{6}{(1/3)\cdot6-0\cdot5} & -\frac{0}{(1/3)\cdot6-0\cdot5} \\ -\frac{5}{(1/3)\cdot6-0\cdot5} & \frac{1/3}{(1/3)\cdot6-0\cdot5} \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ -\frac{5}{2} & \frac{1}{6} \end{pmatrix}$$

3. (a) For example, $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

   (b) Since $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16 \equiv 4$, $5^2 = 25 \equiv 1$, $6^2 = 36 \equiv 0$, $7^2 = 48 \equiv 1$, $8^2 = 64 \equiv 4$, $9^2 = 81 \equiv 9$, $10^2 = 100 \equiv 4$, and $11^2 = 121 \equiv 1$, the idempotents are 0, 1, 4, and 9.

4. Of course $C = 0$ would work for all three matrices. But nonzero matrices are (for example):

$$\begin{pmatrix} 6 & 9 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} -3 & -3 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 5 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 5 & -10 \\ -2 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$$\begin{pmatrix} \frac{1}{2} & \frac{1}{4} \\ 3 & \frac{3}{2} \end{pmatrix} \begin{pmatrix} -3 & -3 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

5. (a) Suppose that 0_R is a zero element of R, and let w also be a zero element. Then $0_R + x = 0_R$ has the solutions 0_R, since 0_R is a zero element, and also w, since w is a zero element. Since the solution to that equation is unique, we must have $w = 0_R$, so that the zero element is unique.

(b) Suppose that 1_R is an identity of R, and let e also be an identity element. Since 1_R is an identity element, we have $1_R e = e$. Since e is an identity element, we have $1_R e = 1_R$. Thus $1_R = 1_R e = e$, so that $e = 1_R$ and the identity is unique.

(c) No, it cannot. Suppose that b and c are inverses to a. Then since $ab = 1 = ac$, we get $ab = ac$; multiply both sides on the left by b to get $(ba)b = (ba)c$. But b is an inverse, so that $ba = 1$ and thus $b = c$.

6. (a) The product AC has entries each of which is a sum of terms; each of those terms is the product of an entry of A and an entry of C, say ac. The product $A(kC)$ has the same combination of products of entries, obviously, but each entry of kC is k times the corresponding element of C. Thus the product ac in AC becomes $akc = k(ac)$ in the product $A(kC)$. Since an entry of AC is a sum of terms like that, it is k times the corresponding sum of terms in AC. But $AC = 0$, so that each such sum of terms is zero, so k times it is zero, and $A(kC) = 0$.

(b) For example (other answers are possible)

$$\begin{pmatrix} -1 & -1 \\ 2 & 2 \end{pmatrix}, \quad \begin{pmatrix} -3 & -3 \\ 6 & 6 \end{pmatrix}, \quad \begin{pmatrix} 2 & 2 \\ -4 & -4 \end{pmatrix}.$$

7. To prove S is a subring we should know that if $m, n \in \mathbb{Z}$ then $m1_R - n1_R = (m - n)\, 1_R$ and $(m1_R)(n1_R) = (mn)1_R$. These are special cases of formulas proved in Exercise 21.

8. T is nonempty since it contains 0_R. Suppose $x, y \in T$. Then $x = rb$ and $y = sb$ for some $r, s \in R$. Compute $x - y = rb - sb = (r - s)b$ lies in T and $xy = x(sb) = (xs)b$ lies in T. Apply Theorem 3.6.

9. By Theorem 3.6, we need only show it is closed under subtraction and multiplication, since it is clearly nonempty:

$$\begin{pmatrix} a & 4b \\ b & a \end{pmatrix} - \begin{pmatrix} c & 4d \\ d & c \end{pmatrix} = \begin{pmatrix} a-c & 4(b-d) \\ b-d & a-c \end{pmatrix}, \begin{pmatrix} a & 4b \\ b & a \end{pmatrix}\begin{pmatrix} c & 4d \\ d & c \end{pmatrix} = \begin{pmatrix} ac+4bd & 4ad+4bc \\ bc+ad & 4bd+ac \end{pmatrix}$$
$$= \begin{pmatrix} ac+4bd & 4(ad+bc) \\ ad+bc & ac+4bd \end{pmatrix},$$

and both of those matrices are of the required form. Thus S is a subring.

10. (a) $\overline{R} = \{(0,0),\ (1,0),\ (2,0)\}$ and $\overline{S} = \{(0,0),\ (0,1),\ (0,2),\ (0,3),\ (0,4)\}$.

(b) $\overline{R}$ is closed under subtraction since $(r_1, 0_S) - (r_2, 0_S) = (r_1 - r_2, 0_S - 0_S) = (r_1 - r_2, 0_S) \in \overline{R}$. It is closed under multiplication since $(r_1, 0_S)(r_2, 0_S) = (r_1 r_2, 0_S 0_S) = (r_1 r_2, 0_s) \in \overline{R}$. Thus $\overline{R}$ is a subring of $R \times S$.

(c) $\overline{S}$ is closed under subtraction since $(0_R, s_1) - (0_R, s_2) = (0_R - 0_R, s_1 - s_2) = (0_R, s_1 - s_2) \in \overline{S}$. It is closed under multiplication since $(0_R, s_1)(0_R, s_2) = (0_R 0_R, s_1 s_2) = (0_R, s_1 s_2) \in \overline{S}$. Thus $\overline{S}$ is a subring of $R \times S$.

11. To show it is closed under subtraction, suppose $r, s \in S$. Then $m(r-s) = mr - ms = 0_R - 0_R = 0_R$, so that $r - s \in S$. To show it is closed under multiplication, $m(rs) = (mr)s = 0_R s = 0_R$, so that $rs \in S$. Thus S is a subring of R.

12. (a) To see that it has a solution, add $-a$ to both sides to get $-a + a + x = -a + b$, so that $0_R + x = -a + b$ and thus $x = -a + b$ is a solution (check: $a + (-a + b) = (a + (-a)) + b = 0_R + b = b$). To see that the solution is unique, suppose that $a + x = b = a + y$. Then by Theorem 3.4, $x = y$, so that the solution is unique.

(b) To see that it has a solution, multiply both sides on the left by a^{-1}. This gives $a^{-1}(ax) = a^{-1}b$, or $(a^{-1}a)x = 1_Rx = x = a^{-1}b$. To see that the solution is unique, suppose $ax = b = ay$. Then $ax = ay$; multiplying both sides of the equation by a^{-1} on the left gives $a^{-1}(ax) = a^{-1}(ay)$, so that $(a^{-1}a)x = 1_Rx = x = (a^{-1}a)y = 1_Ry = y$. Thus $x = y$ and the solution is unique.

13. (a) Yes. Use Theorem 3.6. $S \cap T$ is nonempty since 0_R lies in every subring. If $a, b \in S \cap T$ then $a, b \in S$ and $a, b \in T$. Therefore $a - b$ and ab lie in both S and T, since they are subrings. Putting them back together, conclude that $a - b$ and ab lie in $S \cap T$.
(b) Not necessarily. For example $2\mathbb{Z}$ and $3\mathbb{Z}$ are subrings of $\mathbb{Z}$ but their union is not closed under addition.

14. Suppose e is an idempotent. Then $e^2 = e$ so that $e^2 - e = e(e-1) = 0$. But R is an integral domain, so either $e = 0$ or $e - 1 = 0$; that is, either $e = 0_R$ or $e = 1_R$.

15. (*a*) We know that a^{-1} and b^{-1} exist in R. Then $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a(l_R)a^{-1} = aa^{-1} = 1_R$. Similarly we have $(b^{-1}\ a^{-1}\ )ab = 1_R$. Therefore ab is a unit with inverse equal to $b^{-1}\ a^{-1}$.
(*b*) In the ring of quaternions, we know that $i{\cdot}(-i) = (-i){\cdot}i = -i^2 = 1$, so that $i^{-1} = -i$. Similarly $j^{-1} = -j$ and $k^{-1} = -k$. Then $(ij)^{-1} = k^{-1} = -k$ while $i^{-1}\ j^{-1} = (-i)(-j) = ij = k$.

16. False. 0_R is not in the set of units of R (*u*nless R is the zero ring $\{0_R\}$).

17. Suppose that a is a unit and that $ab = 0$. Multiplying on the left by a^{-1} gives $a^{-1}ab = a^{-1}0 = 0$. But $a^{-1}ab = b$, so we get $b = 0$. Thus if $ab = 0$, then $b = 0$, so that a is not a zero divisor.

18. We are given $au = 1_R = va$. Thus

$$v = v1_R = v(au) = (va)u = 1_Ru = u.$$

19. $(r\ \ s) \in R \times S$ is a unit if and only if r is a unit in R and s is a unit in S.

20. If $0_R \neq r \in R$ and $0_R \neq s \in S$, then $(r, 0_s\ )$ and $(0_R, s)$ are nonzero elements of $R \times S$ having product $(r, 0_s){\cdot}(0_R, s) = (0_R, 0_s) = 0_{R \times S.}$

21. (a) Since $ab = ac$, we have $ab - ac = a(b - c) = 0$. But a is not a zero divisor, and $a \neq 0$. It follows that $b - c = 0$, so that $b = c$.
(b) Since $ba = ca$, we have $ba - ca = (b - c)a = 0$. But a is not a zero divisor, and $a \neq 0$. It follows that $b - c = 0$, so that $b = c$.

22. (*a*) A proof "by contradiction": Suppose a and b are not zero divisors and suppose $x \in R$ and $(ab)x = 0_R$. Then $a(bx) = 0_R$ implies $bx = 0_R$ since otherwise a is a zero divisor. But $bx = 0_R$ implies $x = 0_R$, since b is not a zero divisor. The implication $(ab)x = 0 => x = 0$ shows that ab is not a zero divisor.
(*b*) Suppose a is a zero divisor, so that $ac = 0_R$ for some $c \pm 0_R$. Then $(ab)c = b(ac) = b0_R = 0_R$, so that ab is a zero divisor. When b is a zero divisor a similar proof works.

23. (a) (i) For a positive integer m we defined $ma = \mathrm{a} + \mathrm{a} + \ldots + a$, where there are m summands. If m, n are positive integers then $(m + n)a = (a + \ldots + a) + (a + \ldots + a)$, equalling m summands followed by n summands. Altogether there are $m + n$ summands which add to $(m + n)a$. (Compare Exercise 17a.) If $m = 0$ then $0a = 0_R$. Therefore $(0 + n)a = na = 0 + na = 0a + na = (0 + n)a$, and the formula works in this case too. The case $n = 0$ is similar.

(ii) Suppose $m > 0$. Then $m(a + b) = (a + b) + (a + b) + \ldots + (a + b)$ with m summands. Then there are m "a" terms and m "b" terms. Re-arranging (*u*sing the commutative and associative laws), we may First add up the m a's, then the m b's. Hence the quantity equals $ma + mb$. If $m = 0$ we easily find $0(a + b) = 0_R = 0_R + 0_R = 0a + 0b$.

(iii) Suppose $m > 0$. Then $m(ab) = ab + ab + \ldots + ab$ with m terms. By distributivity this equals $(a + a + \ldots + a)b = (ma)b$. Similarly using the other distributive law, $a(b + b + \ldots + b) = a(mb)$. If $m = 0$ the equation is easier to verify.

(iv) Suppose m, $n > 0$. Then $(ma)(nb) = (a + a + \ldots + a)(nb)$ with m summands. By distributivity this equals $a(nb) + a(nb) + \ldots + a(nb)$, and by (iii) it equals $n(ab) + n(ab) + \ldots + n(ab)$. Since there are m summands, this quantity equals $mn(ab)$. (*N*ote: For this last step we should really verify first that $(mn)x = m(nx)$ for every $x \in R$.) If $m = 0$ or $n = 0$ a short separate argument is needed to show that each side of the equation equals 0_R.

(b) To handle negative cases, recall the definition. If $n > 0$ then $(-n)a = (-a) + (-a) + \ldots + (-a)$ with n summands. That is: $(-n)a = n(-a)$. Claim, $(-n)a = -(na)$. Proof. For by Theorem 3.5(4) we have $-(2a) = -(a + a) = (-a) + (-a) = (-2)a$. Extending this to larger sums proves the Claim.

(i) Claim. If m, $n \geq 0$ then $(m - n)a = ma - na$. Proof. In the case $m - n \geq 0$ we apply part (a) to see: $(m - n)a + na = (m - n + n)a = ma$. Subtracting na we are done. If $m - n \leq 0$, use the definition and the case just done to see: $(m - n)a = -(n - m)a = -(\mathrm{n}a - ma) = ma - na$.

Claim. If m, $n \geq 0$ then $(-m + n)a = (-m)a + na$. The proof is similar.

Claim. If m, $n \geq 0$ then $(-m - n)a = (-m)a + (-n)a$.

Proof, $(-m - n)a = (-(m + n))a = -((m + n)a) = -(\mathrm{m}a + na) = -(ma) + -(na) = (-m)a + (-n)a$. These Claims combine to prove the assertion for all integers.

(ii) if $m > 0$ then $(-m)(a + b) = -(m(a + b)) = -(\mathrm{m}a + mb) = -(ma) + -<mb) = (-m)a + (-m)b$.

(iii) and (iv) are proved similarly.

24. (a) For a positive integer m we have, by definition, $a^m = a \cdot a \cdot a \cdots a$ with m factors. Then $a^m a^n = (a \cdot a \cdots a)(a \cdot a \cdots a)$ equals m factors followed by n factors, yielding a total of $m + n$ factors. Then it equals a^{m+n}. If R has identity and $a \neq 0$ then we have defined $a^0 = 1$. In this case the formulas also work when m or n equals 0.

(b) $(a^m)^n = (a^m) \cdot (a^m) \cdots (a^m)$ with n factors. Expanding each factor a^m as a product of m a's, we see that there is a total of mn factors of a. Hence it equals a^{mn}.

(c) If $ab = ba$ then $a^n b^n = (ab)^n$ for every positive integer n. This can be proved in the same way, listing all the factors and rearranging.

25. (a) Consider the subring $S = \mathbb{Z} \times 0$ of the ring $\mathbb{Z} \times \mathbb{Z}$. Then S has identity $1_S = (1, 0)$, but $1_R = (1, 1)$.

(b) By Exercise 14, the only idempotents in R are 0_R and 1_R, so these are the only solutions to $x^2 = x$ in R. But 1_S satisfies this equation, since multiplication in S is the same as that in R, so that $1_S = 0_R = 0_S$ or $1_S = 1_R$. Since R and S are integral domains, $1_S \neq 0_S$, so that we must have $1_S = 1_R$

26. If $a \in S$ then $a + 0_s = a$ since 0_s is the zero for S. But since S is a subring of R we may add $-a$ to both sides (viewed in R now) to conclude that $0_S = 0_R$.

27. No. For example in the polynomial ring $\mathbb{R}[x]$ the subset $S = \mathbb{Z}x = \{nx \mid n \in \mathbb{Z}\}$ is not closed under multiplication.

28. We use 1 for 1_R and 0 for 0_R to simplify the table. Since a and b are units and $a, b \neq 1$, we know $ab \neq 0, a, b$. Therefore $ab = 1$ and the following table is easy to complete.

	0	**1**	**a**	**b**
0	**0**	**0**	**0**	**0**
1	**0**	**1**	**a**	**b**
a	**0**	**a**	**b**	**1**
b	**0**	**b**	**1**	**a**

29. Assume $1_R \neq 0_R$. If R is an integral domain then we prove cancellation: Suppose $a \neq 0_R$ and $ab = ac$. Then $a(b - c) = ab - ac = 0_R$ and therefore $b - c = 0_R$ (since R is an integral domain. Then $b = c$ and cancellation holds. Conversely, to show: If $ab = 0_R$ then $a = 0_R$ or $b = 0_R$. Proof. Suppose $a \neq 0_R$ (otherwise we are immediately done). Then $ab = 0_R = a0_R$ and cancellation implies $b = 0_R$.

30. Given a unit $u \in T$. For any $x \in R$ we have $xu \in T$ (compare Exercise 6). Then for any $r \in R$: $r = (ru^{-1})u \in T$. Therefore $R = T$.

31. (a) Answered in the text. Consequently we have $a = -a$ for every a.
(b) $a + b = (a + b)^2 = a^2 + ab + ba + b^2$ Cancelling $a = a^2$ and $b = b^2$ we conclude that $0_R = ab + ba$.

Then by part (a), $ab = -ba = ba$.

32. (*a*) It is easy to check that the rules for addition all hold in $R \times \mathbb{Z}$. The system is closed under multiplication, since $rs + ms + nr \in R$ and $mn \in \mathbb{Z}$. Associativity: $(r, m).((s, n)(t, k)) = (r, m).(st + nt + ks, nk) = (r(st + nt + ks) + m(st + nt + ks) + (nk)r, m(nk))$. On the other hand $((r, m)\cdot(s, n))\cdot(t, k) = (rs + ms + nr, mn)\cdot(t, k) = ((rs + ms + nr)t + (mn)t + k(rs + ms + nr), (mn)k)$. These quantities are seen to be equal, using the rules derived in Exercise 21.
Distributivitv. $(r, m)\cdot((s, n) + (t, k)) = (r, m)\cdot(s + t, n + k) = (r(s + t) + m(s + t) + (n + k)r, m(n + k))$. On the other hand $(r, m)\cdot(s, n) + (r, m)\cdot(t, k) = (rs + ms + nr, mn) + (rt + mt + kr, mk) = (rs + rt + ms + mt + nr + kr, mn + mk)$. These quantities are equal.

The other distributive law is similar. Hence T is a ring. The element $(0, 1)$ is seen to be an identity element for T.

(*b*) R^* is closed under the two operations. For example, $(r, 0) - (s, 0) = (rs + 0s + 0r, 0 - 0) = (rs, 0)$. Also die zero element $(0, 0)$ is in R^* and R^* is closed under negatives. Hence R^* is a subring.

33. Given $ab\cdot x = x\cdot ab = 1_R$ and $ay = ya = 1_R$. Then $xa\cdot b = 1$ so xa should equal b^{-1} . To prove b is invertible we check that $b\cdot xa = 1_R$. First note that $y = y\cdot abx = ya\cdot bx = bx$. Then $b\cdot xa = bx\cdot a = ya = 1_R$, as hoped.

34. (a) Since $M(F)$ has an identity, namely $\begin{pmatrix} 1_F & 0 \\ 0 & 1_F \end{pmatrix}$, Exercise 17 shows that any unit (i.e., invertible element) in $M(F)$ is not a zero divisor, and thus that any zero divisor is not invertible. By Example 8, if $ad - bc \neq 0_F$, then A is invertible. For the reverse, note that by Example 10, if $ad - bc = 0_f$, then A is a zero divisor, and thus is not invertible. Thus A is invertible if and only if $ad - bc \neq 0_F$.

(b) Example 10 shows that $ad-bc = 0_F$ implies that A is a zero divisor. By part (a), if $ad-bc \neq 0_F$ then A is invertible, so by Exercise 17 it is not a zero divisor.

35. (a) By Example 7, the inverse of a matrix in $M(\mathbb{R})$ with integer entries is a matrix of rational numbers all of which have denominator $ad - bc$. Thus if $ad - bc = \pm 1$, the entries are actually integers, so that the matrix is invertible in $M(\mathbb{Z})$.

(b) If the inverse of A is an integer, then all of $\frac{a}{ad-bc}$, $\frac{b}{ad-bc}$, $\frac{c}{ad-bc}$, and $\frac{d}{ad-bc}$ are integers. Thus also

$$\frac{a}{ad-bc} \cdot \frac{d}{ad-bc} - \frac{b}{ad-bc} \cdot \frac{c}{ad-bc} = \frac{ad-bc}{(ad-bc)^2} = \frac{1}{ad-bc}$$

is an integer. Thus $ad - bc = \pm 1$. By Exercise 34(b), we know that A is a zero divisor if and only if $ad - bc = 0$. Thus if $ad - bc \neq 0, 1$, or -1, A can be neither a unit nor a zero divisor.

36. Claim that

$$A^{-1} = \begin{pmatrix} d(ad-bc)^{-1} & -b(ad-bc)^{-1} \\ -c(ad-bc)^{-1} & a(ad-bc)^{-1} \end{pmatrix}.$$

To see this, multiply the two together:

$$\begin{aligned} AA^{-1} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d(ad-bc)^{-1} & -b(ad-bc)^{-1} \\ -c(ad-bc)^{-1} & a(ad-bc)^{-1} \end{pmatrix} \\ &= \begin{pmatrix} ad(ad-bc)^{-1} - bc(ad-bc)^{-1} & -ab(ad-bc)^{-1} + ab(ad-bc)^{-1} \\ cd(ad-bc)^{-1} - dc(ad-bc)^{-1} & -bc(ad-bc)^{-1} + ad(ad-bc)^{-1} \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{aligned}$$

Similarly $A^{-1}A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

37. If $ab = 1_R$, multiplying both sides by a on the right yields $aba = a$. Since a is not a zero divisor, Exercise 21(a) shows that $ba = 1_R$. Conversely, if $ba = 1_R$, multiplying both sides by a on the left yields $aba = a$. Since a is not a zero divisor, Exercise 21(b) shows that $ab = 1_R$.

38. If ab is a unit, say with inverse c, then $(ab)c = a(bc) = 1_R$, so that a is a unit. But then b is a unit, since $abc = 1_R$ implies, multiplying both sides by a^{-1} on the left, that $bc = a^{-1}$. Then multiply both sides by a on the right to get $bca = 1_R$, so that $b(ca) = 1_R$ and b is a unit.

39. Suppose a is not a zero divisor. Then in order to show that a is a unit, we must show that the equation $ax = 1_R$ has a solution in R. Since R is finite, let $a_1, a_2, \ldots, a_r$ be the distinct elements of R. Consider the elements $aa_1, aa_2, \ldots, aa_r$. Those elements are all distinct, for if $aa_i = aa_j$ and a is not a zero divisor, Exercise 21(a) shows that $a_i = a_j$ so that $i = j$. But there are r elements, and they are distinct elements of R, which has r elements, so that one of them must be 1_R; say $aa_k = 1_R$. Then a is a unit, since a_k is its inverse.

40. If there exists $x \neq 0_R$ with $x^2 = 0_R$ then x is a nonzero nilpotent element. Conversely if a is a nonzero nilpotent element choose the minimal positive integer n for which $a^n = 0$. Certainly $n > 1$, and if $n = 2$ we are done. Suppose $n \geq 3$ and set $x = a^{n-1}$. Then $x \neq 0$ (by the minimality of n) and $x^2 = a^{2(n-1)} = a^n a^{n-2} = 0_R$.

41. (a) $\mathbb{Z}$ has characteristic zero since there is no positive integer n with $n \cdot l_{\mathbb{Z}} = n = 0$. Suppose that $k > 0$ and $k \cdot l_R = 0_R$ in $R = \mathbb{Z}_{\text{n}}$. Equivalently, $k \equiv 0 \pmod{n}$, which means $n \mid k$. The smallest positive k satisfying this condition is certainly n, so the characteristic of $\mathbb{Z}_{\text{n}}$ is n.
(b) Let $R = \mathbb{Z}_4 \times \mathbb{Z}_6$ so that $1_R = (1, 1)$. Then for $k > 0$ we have $k.1_R = 0_R$ if and only if $k = 0$ (mod 4) and $k \equiv 0$ (mod 6). Equivalently, $4 \mid k$ and $6 \mid k$, so that k is a common multiple of 4 and 6. The characteristic of R is the smallest such k which is the least common multiple $[4, 6] = 12$.

42. Since R is finite there must exist integers $r < s$ with $rl_R = sl_R$. Use the formulas in Exercise 21 to find $(s - r)l_R = 0_R$. Since $s - r$ is a positive integer, R has finite characteristic.

43. (a) $na = n(1_R a) = (n1_R)a = 0_R a = 0_R$ using formulas from Exercise 21.
(b) Suppose $n = n_1 n_2$ where $n_1, n_2 > 1$. Then $0_R = nl_R = (n_1 n_2)1_R = (n_1 l_R)(n_2, 1_R)$ using Exercise 21. Since R is an integral domain, $n_1 l_R = 0_R$ or $n_2 l_R = 0_R$. In either case this contradicts the minimality of n

44. (a) Suppose $a^m = 0_R$ and $b^n = 0_R$ for some $m, n > 0$. Then $(a + b)^{m+n-1}$ equals a sum of terms of the type $C\, a^r \cdot b^s$ where $C > 0$ is a binomial coefficient, and $r, s > 0$ with $r + s = m + n - 1$. Then either $r \geq m$ or $s \geq n$ (for otherwise $r \leq m - 1$ and $s \leq n - 1$ so that $r + s \leq m + n - 2$ which is false). Therefore either $a^r = 0_R$ or $b^s = 0_R$. Therefore each term of this sum equals 0_R. Hence $a + b$ is nilpotent.
(b) If $a, b \in N$ we have just seen that $a + b \in N$. Also $ab \in N$ because, for the exponents m, n above, let $k = \max\{a, b\}$. Then $a^k = 0_R$ and $b^k = 0_R$ so that $(ab)^k = 0_R$. Certainly $0_R \in N$ and if $a \in N$ then also $-a \in N$. Therefore N is a subring.

45. This tricky problem has a number of different solutions. Here is one that seems fairly efficient, using a sequence of steps:

(1) If $c^2 = 0$ then $c = 0$.
Proof. $c = c^3 = c^2 c = 0c = 0$.
(2) $yx = x^2 yx$ and $xy = xyx^2$ for every $x, y \in R$.
Proof. $(yx - x^2\, yx)^2 = yxyx - yxx^2\, yx - x^2\, yxyx + x^2\, yxx^2\, yx$
$= yxyx - yxyx - x^2 yxyx + x^2 yxyx = 0$. Now apply part (1).
The second equation is proved similarly.
(3) $a^2 b = ba^2$ for every $a, b \in R$.
Proof. Use $x = a^2$ and $y = b$ in (2) to conclude that $ba^2 = (a^2)^2 ba^2 = a^2 ba^2$ and $a^2 b = a^2 b(a^2)^2 = a^2 ba^2$.
(4) $xy = yx$ for every $x, y \in R$.
Proof, $xy = (xy)^3 = xy(xy)^2 = x(xy)^2 y$ since squares commute with every element by (3). This quantity equals $x(xyxy)y = x^2\,(yx)y^2 = y^2\,(yx)x^2 = y^3 x^3 = yx$. Here we used (3) again to switch around the x^2 and y^2.

46. A nonzero commutative ring R with identity that has no zero divisors except for 0_R is an integral domain. By Theorem 3.11 a finite integral domain is a field. The difficulty here is to prove that R has an identity element.

Let $0 \neq a \in R$ and consider the "left multiplication" map λ_a: $R \rightarrow R$ defined by $\lambda_a(x) = ax$. This map λ_a is injective (If $\lambda_a(x) = \lambda(y)$ then $ax = ay$ so that $a(x - y) = 0$. Since a is not a zero divisor, $x - y = 0$ so that $x = y$.) Since R is finite λ_a is also surjective (This is essentially the argument in Theorem 3.11.)

Therefore every $r \in R$ can be expressed as $r = ax$ for some $x \in R$. Similarly consider the "right multiplication" map p_a defined by $p_a(y) = ya$. By the same argument we find that every $r \in R$ can be expressed as $r = ya$ for some $y \in R$.

Applying this to $r = a$ we see that there exist $e, f \in R$ such that $a = ae$ and $a = fa$. For any $r \in R$, express $r = ax = ya$ as above. Then $re = yae = ya = r$ and $fr = fax = ax = r$. Applying these equations to $r = e$ and $r = f$ we obtain $e = fe = f$. Therefore $re = r = er$ for every r , and e is the identity element for R.

3.3 Isomorphisms and Homomorphisms

1. If we denote by $[a]_6$, $[a]_2$, and $[a]_3$, the congruence classes of a modulo 2, 3, and 6 respectively, then by inspection, the bijection f is the function $f([a]_6) = ([a]_2, [a]_3)$. But then

$$\begin{aligned}
f([a]_6 + [b]_6) &= f([a+b]_6) && \text{(Addition in } \mathbb{Z}_6\text{)}\\
&= ([a+b]_2, [a+b]_3) && \text{(Definition of } f\text{)}\\
&= ([a]_2 + [b]_2, [a]_3 + [b]_3) && \text{(Addition in } \mathbb{Z}_2,\ \mathbb{Z}_3\text{)}\\
&= ([a]_2, [a]_3) + ([b]_2, [b]_3) && \text{(Addition in } \mathbb{Z}_2 \times \mathbb{Z}_3\text{)}\\
&= f([a]_6) + f([b]_6) && \text{(Definition of } f\text{)}\\
f([a]_6[b]_6] &= f([ab]_6) && \text{(Multiplication in } \mathbb{Z}_6\text{)}\\
&= ([ab]_2, [ab]_3) && \text{(Definition of } f\text{)}\\
&= ([a]_2[b]_2, [a]_2[b]_3) && \text{(Multiplication in } \mathbb{Z}_2,\ \mathbb{Z}_3\text{)}\\
&= ([a]_2, [a]_3) \cdot ([b]_2, [b]_3) && \text{(Multiplication in } \mathbb{Z}_2 \times \mathbb{Z}_3\text{)}\\
&= f([a]_6)f([b]_6) && \text{(Definition of } f\text{)}
\end{aligned}$$

Thus f is a homomorphism; since it is a bijection, it is an isomorphism.

2. $\mathbb{Z}_2 \times \mathbb{Z}_2$ has 4 elements ([0], [0]), ([l],[l]), ([1], [0]), ([0], [1]). To shorten notations we refer to these elements as 00, 11, 10 and 01. The addition and multiplication tables for this ring are:

+	00	11	10	01
00	00	11	10	01
11	11	00	01	10
10	10	01	00	11
01	01	10	11	00

	00	11	10	0)
00	00	00	00	00
11	00	11	10	01
10	00	10	10	00
01	00	01	00	01

Compare these tables with those in Exercise 3.1.2, conclude that the correspondence 00 → 0, 11 → e, 10 → b, 01 → c is an isomorphism of rings.

3. f is bijective as shown in the answers in the text. Homomorphism conditions: $f(a + b) = (a + b, a + b) = (a, a) + (b, b) = f(a) + f(b)$. Similarly, $f(ab) = (ab, ab) = (a, a)(b, b) = f(a)f(b)$.

4. Let f: $\mathbb{Z}_5 \rightarrow S$ be the bijection listed. Then $f(\bar{1}) = 2$ and $f(\bar{1} \cdot \bar{1}) = f(\bar{1}) = 2$ while $f(\bar{1})f(\bar{1}) = 2 - 2 = 4$. Then f is not a homomorphism.

5. Let $f(a) = \begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$. Letting S be the set of all such matrices we see that f: $\mathbb{R} \rightarrow S$ is a bijective mapping. The definitions of matrix addition and multiplication are used to show that $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

6. The map f: $R \rightarrow \overline{\mathrm{R}}$ is injective (if $f(a) = f(b)$ then $(a, 0_s) = (b, 0_s)$ and therefore $a = b$). It is also subjective (a typical element of $\overline{\mathrm{R}}$ is $(a, 0_{\mathrm{S}}) = f(a)$), Homomorphism properties: $f(a + b) = (a + b, 0_{\mathrm{S}}) = (a, 0_{\mathrm{S}}) + (b, 0_{\mathrm{S}}) = f(a) + f(b)$. Multiplication works similarly.

7. Define $g : R \rightarrow D$, where D is the set of all real matrices of the type $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$. by setting $g(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ It easily follows that e is an isomorphism.

8. As seen in the answers in the text, f is injective. To prove f is subjective let $a + b\sqrt{2}$ be a typical element of $\mathbb{Q}(\sqrt{2})$. Then $a + b\sqrt{2} = f(a - b\sqrt{2})$. (Compare Exercise 15.) The homomorphism property for addition is easy to check. For multiplication we have: $f((a + b\sqrt{2})(c + d\sqrt{2})) = f((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} = (a - b\sqrt{2})(c - d\sqrt{2}) = f(a + b\sqrt{2})f(c + d\sqrt{2})$. Therefore f is an isomorphism.

9. $f(1) = 1$ since identity elements must match. <u>Claim</u>. $f(n) = n$ for every $n > 0$. <u>Proof</u>. If not, the Well-Ordering Axiom implies that there exists a smallest positive integer m with $f(m) \neq m$. Then $f(m - 1) = m - 1$ by the minimality, so that $f(m) = f(m - 1 + 1) = f(m - 1) + f(l) = m - 1 + 1 = m$, contradiction.

   Certainly $f(0) = 0$ and for $n > 0$ we have $f(-n) = -f(n) = -n$ by Theorem 3.12. Therefore f is the identity map.

10. To show that $f(1_R)$ is an idempotent, we must show that $f(1_R)^2 = f(1_R)$. But since f is a homomorphism, $f(1_R)^2 = f(1_R) \cdot f(1_R) = f(1_R \cdot 1_R) = f(1_R)$.

11. (a) For one thing, f is not defined on all of $\mathbb{R}$, since square roots of negative numbers are not real. For another, $f(a + b) = \sqrt{a + b} \neq \sqrt{a} + \sqrt{b} = f(a) + f(b)$.

    (b) This is not a homomorphism since $f(xy) = 3xy$ while $f(x)f(y) = 3x \cdot 3y = 9xy$.

    (c) This is not a homomorphism since $f(xy) = 2^{xy}$ while $f(x)f(y) = 2^x \cdot 2^y = 2^{x+y}$. (Additionally, $f(x + y) \neq f(x) + f(y)$).

    (d) This is not a homomorphism since

$$f\left(\frac{a}{b} + \frac{c}{d}\right) = f\left(\frac{ad + bc}{bd}\right) = \frac{bd}{ad + bc}, \qquad \text{while}$$

$$f\left(\frac{a}{b}\right) + f\left(\frac{c}{d}\right) = \frac{b}{a} + \frac{d}{c} = \frac{ad + bc}{ac}.$$

12. (a) Not a homomorphism. Consider $f(-1)f(-1)$.
    (b) Homomorphism. In fact f is the identity map since $[-1] = [1]$ in $\mathbb{Z}_2$.
    (c) Not a homomorphism.
    (d) Not a homomorphism. Consider h(1).
    (e) Homomorphism. The hardest part here is to verify that f is well defined. (That is, show that $[x]_4$ is independent of the choice of x representing the class $[x]_{12}$).

13. (a) Choose $r \in R$. Then $f((r, 0_S)) = r$. Thus f is surjective.
    (b) Choose $s \in S$. Then $g((0_R, s)) = s$. Thus g is surjective.
    (c) Since S is nonzero, it contains some element $a \neq 0_S$. Then for any $r \in R$, we have $f((r, 0_S)) = r = f((r, a))$. Since $a \neq 0_S$, it follows that f is not injective. Similarly, since R is nonzero, it contains some element $b \neq 0_R$. Then for any $s \in S$, we have $g((0_R, s)) = s = g((b, s))$. Since $b \neq 0_R$, it follows that g is not injective.

14. It suffices to show that K is closed under subtraction and multiplication. Suppose that $a, b \in K$. Then since f is a homomorphism,

$$f(a-b) = f(a) - f(b) = [0] - [0] = [0], \text{ so that } a-b \in K$$
$$f(ab) = f(a)f(b) = [0][0] = [0], \text{ so that } ab \in K.$$

Thus K is a subring of $\mathbb{Z}$ (it is the subring consisting of all multiples of 6).

15. No. For example define f: $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ by $f(x, y) = x$. Then the element (1, 0) is a zero divisor in $\mathbb{Z} \times \mathbb{Z}$ but $f(1,0)=1$ is not a zero divisor in $\mathbb{Z}$

16. T is non-commutative (since $rs \neq$ sr) while R and F are commutative. Therefore T cannot be isomorphic to R or F. Also R and F cannot be isomorphic since F possesses 3 units while R has only 2 units.

17. Note that $f^2 = 1$, the identity map on ₵. (Because $f(a + bi) = f(a - bi) = a + bi$.) Then f is invertible ($f^1 = f$), so it is objective, using Theorem B.1 of Appendix B.

18. We check the values $f([0]_5) = [0]_{10}$, $f([l]_5) = [6]_{10}$, $f([2]_5) = [12]_{10} = [2]_{10}$, $f([3]_5) = [18]_{10} = [8]10$ and $f([4]_5) = [24]_{10} = [4]_{10}$. These match the values in the Example. Homomorphism properties: $f([x]_5 + [y]_5) = f([x + y]_5) = [6(x + y)]_{10} = [6x]_{10} + [6y]_{10} = f([x]_5) + f([y]_5)$. The products work similarly.

19. Define f: $\mathbb{Z}_7 \to \mathbb{Z}_{28}$ by $f([x]_7) = [8x]_{28}$. As in Exercise 16, this f is a homomorphism. The image set is $f(\mathbb{Z}_7) = \{[0]_{28}, [8]_{28}, [16]_{28}, [24]_{28}, [4]_{28}, [I2]_{28}, (20]_{28}\} = S$, the given subset. Check that S is a subring. View f as a surjection f: $\mathbb{Z} \to S$. Since these two rings have the same (finite) number of elements, f must be a objection. (See Exercises 31 and 32 of Appendix B.)

20. f is a bijection since the map $g : \mathbb{Z} \to E$ given by $g(x) = 2x$ is the inverse. Homomorphism properties: $f(x + y) = (x + y)/2 = x/2 + y/2 = f(x) + f(y)$. $f(x{*}y) = (x{*}y)/2 = (xy/2)/2 = (x/2)(y/2) = f(x)f(y)$.

21. Define f: $\mathbb{Z}^* \to \mathbb{Z}$ by $f(x) = 1 - x$. Then f is a bijection since the map $g : \mathbb{Z} \to \mathbb{Z}^*$ with $g(y) = 1 - y$ is its inverse. Homomorphism:
$f(a \oplus b) = 1 - (a \oplus b) = 1 - (a + b - 1) = (1 - a) + (1 - b) = f(a) + f(b)$.
$f(a \odot b) = 1 - (a \odot b) = 1 - (a + b - ab) = (1 - a)(1 - b) = f(a)f(b)$.

22. Define f: $Z \to \mathbb{Z}$ by $f(x) = x - 1$. Then f is a bijection since the map g: $\mathbb{Z} \to Z$ with $g(y) = y + 1$ is its inverse. Homomorphism:
$f(a \oplus b) = (a \oplus b) - 1 = (a + b - 1) -1 = (a - 1) + (b - 1) = f(a) + f(b)$.
$f(a \odot b) = (a \odot b) -1 = (ab - (a + b) + 2) - 1 = (a - l)\ (b - 1) = f(a)f(b)$.

23. Define f: $R \times E \to ₵$ by $f(a, b) = a + bi$. This f is a bijection since the inverse map is defined ($use\ g(a + bi) = (a, b)$). The homomorphism property for addition is easy to check. For multiplication, $f((a, b)\cdot(c, d)) = f(ac - bd, ad + bc) = (ac - bd) + (ad + bc)i = (a + bi)(c + di) = f(a, b)f(c, d)$.

24. (a) Since addition in this new ring is the same as in the usual ring $\mathbb{R} \times \mathbb{R}$, Axioms 1-5 in the definition of a ring are still satisfied. For Axiom 6, if (a, b) and $(c, d) \in \mathbb{R} \times \mathbb{R}$, then clearly $(ac, bc) \in \mathbb{R} \times \mathbb{R}$. To see that multiplication is associative,

$$\begin{aligned}((a,b)(c,d))(e,f) &= (ac,bc)(e,f) = (ace,bce), \quad \text{and}\\ (a,b)((c,d)(e,f)) &= (a,b)(ce,de) = (ace,bce).\end{aligned}$$

Finally, for the distributive laws, we have

$$\begin{aligned}(a,b)((c,d)+(e,f)) &= (a,b)(c+e,d+f) = (a(c+e),b(c+e)) = (ac+ae,bc+be)\\ &= (ac,bc)+(ae,be) = (a,b)(c,d)+(a,b)(e,f)\\ ((a,b)+(c,d))(e,f) &= (a+c,b+d)(e,f) = ((a+c)e,(b+d)e) = (ae+ce,be+de)\\ &= (ae,be)+(ce,de) = (a,b)(e,f)+(c,d)(e,f).\end{aligned}$$

Thus this new multiplication makes $\mathbb{R} \times \mathbb{R}$ into a ring.

(b) Write S for $\mathbb{R} \times \mathbb{R}$ with the multiplication in part (a), and define

$$f : S \to M(\mathbb{R}) : (a,b) \mapsto \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}.$$

We must show that f is a bijective homomorphism. f is obviously injective, since $f((a,b)) = f((c,d))$ means that $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} = \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix}$, so that $a = c$ and $b = d$ and thus $(a,b) = (c,d)$. It is also obviously surjective, for the matrix $\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \in M(\mathbb{R})$ is the image under f of (a,b), so that any matrix in $M(\mathbb{R})$ is in the image of f. To see that f is a homomorphism,

$$\begin{aligned}f((a,b))+f((c,d)) &= \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} + \begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} a+c & 0 \\ b+d & 0 \end{pmatrix}\\ &= f((a+c,b+d)) = f((a,b)+(c,d))\\ f((a,b))f((c,d)) &= \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix}\begin{pmatrix} c & 0 \\ d & 0 \end{pmatrix} = \begin{pmatrix} ac & 0 \\ bc & 0 \end{pmatrix} = f((ac,bc)) = f((a,b)(c,d)).\end{aligned}$$

Thus f is a bijective homomorphism, so is an isomorphism.

25. Certainly f is subjective since for any $a \in \mathbb{Z}$ we have $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$. Also, f is not injective since $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ have the since image Homomorphism properties: $f(\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} + \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}) =$
$f\begin{pmatrix} a+a' & 0 \\ b+b' & c+c' \end{pmatrix} = a + a' = f\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} + f\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}$. $f(\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} + \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}) =$
$f\begin{pmatrix} aa' & 0 \\ ba' + cb' & cc' \end{pmatrix} = aa' = f\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} f\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix}$

26. g: $R \to \mathrm{M}(R)$ is injective since if $g(r) = g(s)$ then $\begin{pmatrix} 0 & 0 \\ -r & r \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ -s & s \end{pmatrix}$, forcing $r = s$. It is not subjective since, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is not in the image of g.

27. Answered in the text. For(b), see Exercise 27 of Appendix B.

28. Let A be a ring without identity, (a) Consider the zero map $z : \mathbb{Z} \to A$. This does not contradict Theorem 3.12 since f is not surjective.
(b) consider the zero map z. $A \to \mathbb{Z}$.

29. By definition of "inverse", $f(g(x)) = x$ for every $x \in S$. Then $f(g(x + y)) = x + y = f(g(x)) + f(g(y)) = f(g(x) + g(y))$ since f is a homomorphism. Since f in injective this equality implies $g(x + y) = g(x) + g(y)$. A similar argument works for products.

30. Suppose r, $s \in K$, so that $f(r) = 0_R$ and $f(s) = 0_R$. Then $f(r - s) = f(r) - f(s) = 0_R$ and $r - s \in K$. Also $f(rs) = f(r)f(s)\ 0_R$ and $rs \in K$. This proves K is a subring.

31. Suppose $r.s \in P$ so that $f(r)$, $f(s) \in T$. Then $f(r - s) = f(r) - f(s) \in T$ and $f(rs) = f(r)f(s) \in T$ since T is a subring. Therefore $r - s$ and $rs \in P$ showing that P is a subring.

32. First check that mis function makes sense. If $[x]_m = [y]_m$ then show that $[nx]_{mn} = [ny]_{mn}$. That is, if $x \equiv y \pmod m$ then $nx \equiv ny \pmod{mn}$. This is easy to see, and hence f is a well-defined function. Conversely, if $[nx]_{mn} = [ny]_{mn}$ then $nx \equiv ny \pmod{mn}$. It follows that $x \equiv y \pmod m$ (why?) and therefore $[x]_m = [y]_m$. Hence f is injective. Since the number of elements in the domain is m and the number of elements in the range is mn, we see that this f cannot be objective if $n > 1$.

It is routine to check the homomorphism properties.

33. (a) If $c \in R$ define $x_c : R \to R$ to be the constant function $x(x) = C$ Then $x_c \in T$ and $\theta(x_c) = x_c(5) = c$. Therefore θ is subjective, Homomorphism: If f, $g \in T$ then $f + g$ and fg are defined "pointwise": $(f + g((x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$. Therefore $\theta(f + g) = (f + g)(5) = f(5) + g(5) = \theta(f) + \theta(g)$ and $\theta(fg) = (fg)(5) = f(5)g(5) = \theta(f)\theta(g)$. This θ is not an isomorphism. For instance $f(x) = x - 5$ is nonzero in T but $\theta(f) = 0$.
(b) Yes.

34. (*a*) preserved. Suppose $ab = 0_R$ and b $\neq 0_R$. Then $f(a)f(b) = f(ab) = f(0_R) = 0_s$ and $f(b) \neq \mathrm{O}_s$. Therefore $f(a)$ is a zero divisor.

(b) preserved. If $a^2 = a$ then $f(a)^2 = f(a^2) = f(a)$ and $f(a)$ is idempotent.

(c) preserved. Suppose $s,\ t \in\ S$ with $st = 0_S$. By subjectivity there exist $a,\ b \in R$ with $f(a) = s$ and $f(b) = t$. Then $f(ab) = f(a)f(b) = st = 0s$ and injectivity implies that $ab = 0$. since R is an integral domain, either $a = 0_R$ or $b = 0_R$, and therefore eimer $s = f(a) = 0_\mathrm{S}$ or $t = f(b) = 0_\mathrm{S}$. Then S is an integral domain.

35. (a) (c) (e) are answered in the text, (b) $R \times R \times R \times R$ is commutative but M(E) is not.

(d) Any isomorphism f: $R \to \mathbb{Q}$ has $f(2) = 2$ (why?). The equation $x^2 = 2$ has no solution in $\mathbb{Q}$ but it does have solutions in E.

(f) Every element $x \in \mathbb{Z}_4 \times \mathbb{Z}_4$ satisfies $x + x + x + x = 0$, but the element $1 \in \mathbb{Z}_{16}$ does not satisfy such an equation.

36. (a) If $n > 0$, then $f(nr) = f(r + r + \dots + r) = f(r) + f(r) + \dots + f(r) = nf(r)$. Certainly $f(0r) = f(0_R) = 0_s = 0f(r)$. Finally $n > 0$ then $f((-n)r) = f(-nr) = -f(nr) = -(nf(r)) = (-n)f(r)$.

(b) Suppose f: $R \to S$ is an isomorphism. If $n > 0$ and $nl_R = 0_R$ then $nl_\mathrm{s} = nf(1_R) = f(n\mathrm{l}_R) = f(0_R) = 0_\mathrm{S}$. Similarly $nl_\mathrm{s} = 0_s$ implies that $nl_R = 0_R$. Therefore the characteristics are equal.

37. (a) Since e is an idempotent, that means by definition that $e^2 = e$. Then if $a \in R$, we have $e^2a = ea$, or $e(ea) = ea$. Since e is not a zero divisor, Exercise 21(a) in Section 3.2 says that we can cancel the e to get $ea = a$. Similarly, multiplying by a on the left and using the same procedure gives $ae = a$. Since this holds for any $a \in R$, it follows that e is the identity in R.

(b) Since $f(1_S)^2 = f(1_S)f(1_s) = f(1_S1_S) = f(1_S)$, we see that $f(1_S)$ is an idempotent of T. Also, $f(1_S) \neq 0_T$, since if it did, then for any $s \in S$, we would have $f(s) = f(1_Ss) = f(1_S)f(s) = 0_Tf(s) = 0_T$ in contradiction to the assumption that f is a nonzero homomorphism. Finally, since T has no zero divisors, it follows that $f(1_S)$ satisfies the hypotheses of part (a), so that $f(1_S)$ is the identity element of T.

38. (a) Chose any $x \in F$; we must show that $f(x) = 0_R$. Since F is a field and $c \in F$ is nonzero, it is invertible. But then

$$f(x) = f(xcc^{-1}) = f(x)f(c)f(c^{-1}) = f(x)0_Rf(c^{-1}) = 0_R,$$

so that f is the zero homomorphism.

(b) Suppose that $f : F \to R$ is not the zero homomorphism, and suppose that $f(a) = f(b)$. Then $0_R = f(a) - f(b) = f(a - b)$, so that $f(a - b) = 0_R$. If $a \neq b$, then $a - b$ is invertible, so that $f(1_F) = f((a - b)(a - b)^{-1}) = f(a - b)f((a - b)^{-1}) = 0_Rf((a - b)^{-1}) = 0_R$ and then, by the argument in Exercise 37(b), f is the zero homomorphism. This is a contradiction, so that $a = b$ and f is injective.

39. Define f: $R \to R^*$ by $f(r) = (r, 0)$. This f is easily seen to be bijective, and is a homomorphism since $(r, 0) + (s, 0) = (r + s, 0)$ and $(r, 0) - (s, 0) = (rs, 0)$.

40. Suppose there is an isomorphism f: $m\mathbb{Z} \to n\mathbb{Z}$. Let $f(m) = nz$ for some $z \in \mathbb{Z}$, By Exercise 34(a) we have $f(km) = kf(m) = knz$ for every $k \in \mathbb{Z}$. Since f is surjective, there exists $u \in \mathbb{Z}$ with $n = f(um) = unz$. Therefore $1 = uz$ so that $u = z = \pm 1$. Apply the formula to $k = m$ to get $mnz = f(mm) = f(m)f(m) = n^2 z^2$, Cancel nz, to conclude $m = nz = \pm n$. But then $m = n$ since m, n are positive, contrary to the hypothesis.

41. (a) If $[a]_{mn} = [b]_{mn}$ then $a \equiv b$ (mod mn), so that $mn \mid (a - b)$. Then certainly $n \mid (a - b)$, so that $a \equiv b$ (mod n) and $[a]_n = [b]_n$. Similarly $[a]_m= [b]$.

(b) It is not hard to check that f is a homomorphism. To show f is injective suppose $f([a]_{mn})$ $= f([b]_{mn}) =$ Then $[a]_m = [b]_m$ and $[a]_n = [b]_n$, so that a $\equiv b$ (mod m) and $a \equiv b$ (mod n). Therefore $m \mid (a - b)$ and $n \mid (a - b)$. Since $(m, n) = 1$ we have $mn \mid (a - b)$ (using Exercise 1.2.17), Therefore $a \equiv b$ (mod mn) and $[a]_{mn} = [b]_{mn}$.

Since f: $\mathbb{Z}_{\mathrm{m}} \times \mathbb{Z}_{\mathrm{n}} \to \mathbb{Z}_{\mathrm{mn}}$ is injective and both rings have exactly mn elements, conclude that f is also subjective. (See Exercise 32 of Appendix B.)

42. The characteristic of $\mathbb{Z}_{\mathrm{mn}}$ is mn. (See Exercise 3.2.31.) The characteristic of $R = \mathbb{Z}_{\mathrm{m}} \times \mathbb{Z}_{\mathrm{n}}$ is the the least common multiple $[m, n]$. Proof. The characteristic is the smallest $k > 0$ where $k - l_R = 0_R$. That is: $[k]_m = [0]_m$ and $[k]_n = [0]_n$, or equivalently $m \mid k$ and $n \mid k$. The smallest such k is exactly the least common multiple $[m, n] = mn/(m, n)$ (as in Exercise 1.2.31).

If $(m, n) > 1$ then $\mathbb{Z}_{\mathrm{mn}}$ and $\mathbb{Z}_{\mathrm{m}} \times \mathbb{Z}_{\mathrm{n}}$ have unequal characteristics. By Exercise 34 these rings cannot be isomorphic.

Chapter 4

Arithmetic in $F[x]$

4.1 Polynomial Arithmetic and the Division Algorithm

1. (a) $3x^4 + x^3 + 2x^2 + 2$ (b) $x^3 + 1$
(c) $x^5 - \mathrm{I}$ (d) $2x^5 + x^4 + 6x^2 + 3x + 2$

2. Let S be that set. Every $a_0 \in \mathbb{Z}$ lies in S since we may choose $n = 0$, and $\pi \in S$ by choosing $n = 1$, $a_0 = 0$ and $a_1 = 1$. By the associative, commutative and distributive laws it is easy (but tedious) to show that the set S is closed under subtraction and multiplication. Therefore S is a subring $\mathbb{R}$.

3. (a) Answered in the text.
(b) 1, 2;
x, $x + 1$, $x + 2$, $2x$, $2x + l$, $2x + 2$;
x^2, $x^2 + l$, $x^2 + 2$, $x^2 + x$, $x^2 + x + l$, $x^2 + x + 2$, $x^2 + 2x$, $x^2 + 2x + l$, $x^2 + 2x + 2$,
$2x^2$, $2x^2 + 1$, $2x^2 + 2$, $2x^2 + x$, $2x^2 + x + 1$, $2x^2 + x + 2$, $2x^2 + 2x$, $2x^2 + 2x + 1$, $2x^2 + 2x + 2$.

4. (a) $f(x) = x + 1$ and $g(x) = -x$ (b) $f(x) = x + 1$ and $g(x) = 1$.

5. (a) Answered in the text. (b) $q(x) = \dfrac{1}{2}x^2 - \dfrac{1}{4}$, $r(x) = -7x + \dfrac{5}{4}$.
(c) Answered in the text. (d) $q(x) = 6x^2 + 3x + 5$, $r(x) = 5x + 2$.

6. (a) Subring. $f(x)$ has constant term zero if and only if $f(x) = xg(x)$ for some polynomial $g(x)$. Using this observation, the closure under subtraction and product is easy to check.
(b) Not generally a subring. The closure properties fail.
(c) Not generally a subring since it is not closed under multiplication.
(d) Subring. If only even powers of x occur in $f(x)$ and $g(x)$ then only even powers can occur in $f(x) - g(x)$ and in $f(x)g(x)$.
(e) Not a subring. For instance, x is in the set but $x \cdot x = x^2$ is not.

7. In the definition of multiplication the coefficient of x^k equals $a_0b_k + a_1b_{k-1} + \cdots + a_k\, b_n$. This formula is valid for every k provided we interpret the coefficient a_1 to be 0 for $i > n$ and $b_j = 0$ for $j > m$.

Interchanging the letters "a" and "b" in this formula, and using the commutative law in R, produces the same term. Therefore the multiplication is commutative.

8. If $f(x) = a_0 + a_1x + \cdots + a_nx^n$ in $\mathbb{R}[x]$ and $c \in \mathbb{R}$, then from the definition: $c{\cdot}f(x) = ca_0 + ca_1x + \cdots + ca_nx^n$ and $f(x)\text{-}c = a_0c + a_1cx + \cdots : a_ncx^n$. Therefore, 1_{R} acts as the identity element in $\mathbb{R}[x]$.

9. Yes. If $c \neq 0$ and $cd = 0$ for some $d \neq 0$ in $\mathbb{R}$ then these conditions still hold in $\mathbb{R}[x]$.

10. If x is a unit there is some $f(x) \in R[x]$ with $x \cdot f(x) = 1_R$. By Theorem 4.2 we have $0 = \deg 1_R = \deg[x \cdot f(x)] = \deg x + \deg f(x) = 1 + \deg f(x) \geq 1$. This contradiction shows that no such $f(x)$ can exist.

11. Since
$$(1 + 3x)(1 + 6x) = 1 + 3x + 6x + 18x^2 = 1 + 9x + 18x^2 = 1$$
in $\mathbb{Z}_9[x]$, we see that $1 + 3x$ is a unit. If $\mathbb{Z}_9$ were an integral domain, Corollary 4.5 says that all units are constants. However, $\mathbb{Z}_9$ is not an integral domain since for example 3 is a zero divisor.

12. (We must assume $f(x) + g(x) \neq 0_R$ to have its degree defined here.) Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + \cdots + b_mx^m$, where $a_n \neq 0$ and $b_m \neq 0$. Then $\deg f(x) = n$ and $\deg g(x) = m$. Suppose $n < m$.

    From the definition of addition, $f(x) + g(x) = (a_0 + b_0) + \cdots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \cdots + b_mx^m$. Since $b_m \neq 0$ we conclude that $\deg[f(x) + g(x)] = m = \max\{n, m\}$. Similarly if $n > m$ the highest degree term equals a_nx^n, and the degree is $n = \max\{n, m\}$. Finally if $n = m$ then $f(x) + g(x) = (a_0 + b_0) + \cdots + (a_n + b_n)x^n$. Therefore the degree is at most n, and it is less when $a_n + b_n = 0$.

    Summarizing, we have $\deg[f(x) + g(x)] \leq \max\{\deg f(x), \deg g(x)\}$, with equality holding whenever $\deg f(x) \neq \deg g(x)$.

13. Given $(a_0 + a_1x + \cdots + a_nx^n){\cdot}g(x) = 0$ for some $g(x) \neq 0_R$ in $R[x]$. Write $g(x) = b_0 + \cdots + b_mx^m$ for some $b_i \in R$ where $b_m \neq 0_R$. Multiplying this out we get $a_0b_0 + \cdots + a_nb_mx^{\prime\prime+m} = 0_R$. In particular, $a_nb_m = 0_R$ and $b_m \neq 0_{\mathrm{R}}$. Therefore a_n is a zero divisor in R.

14. (a) In the proof of Theorem 4.4 F can be any commutative ring, except for one place where inverses are used: to get the existence of b_m^{-1} where b_m is the leading coefficient of the divisor $g(x)$. If $\mathbb{R}$ is a commutative ring, then the division algorithm works in $R[x]$ provided that the divisor $g(x)$ has leading coefficient which is a unit in R,

    (b) Examples are easy to find. For instance consider the constant polynomials $f(x) = 1$ and $g(x) = 2$. If the division algorithm holds in $\mathbb{Z}[x]$ there must be $q(x)$, $r(x) \in [x]$ with $1 = 2{\cdot}q(x) + r(x)$ and either $r(x) = 0$ or $\deg r(x) < \deg 2$. Since $\deg 2 = 0$ the second condition is impossible, so that $r(x) = 0$ and $1 = 2{\cdot}q(x)$. This is impossible for $q(x) \in \mathbb{Z}[x]$.

15. (a) As the hint suggests, multiply by $1_R - ax + a^2x^2$:
$$(1_R + ax)(1_R - ax + a^2x^2) = 1_R - ax + a^2x^2 + ax - a^2x^2 - a^3x^3 = 1_R - a^3x^3 = 1_R$$
since $a^3 = 0_R$.

(b) Multiply it by $1_R - ax + a^2x^2 - a^3x^3$:

$$\begin{aligned}(1_R + ax)(1_R - ax + a^2x^2 - a^3x^3) &= 1_R - ax + a^2x^2 - a^3x^3 + ax - a^2x^2 + a^3x^3 - a^4x^4 \\ &= 1 - a^4x^4 = 1\end{aligned}$$

since $a^4 = 0_R$.

16. Suppose the inverse of $1_R + ax$ is $b_0 + b_1x + b_2x^2 + \cdots + b_kx^k$. Then

$$\begin{aligned}1 &= (1_R + ax)(b_0 + b_1x + b_2x^2 + \cdots + b_kx^k) \\ &= b_0 + (ab_0 + b_1)x + (ab_1 + b_2)x^2 + \cdots + (ab_{k-1} + b_k)x^k + ab_kx^{k+1}.\end{aligned}$$

Comparing coefficients of powers of x on both sides of this equation, we see first that $b_0 = 1_R$. Since the coefficient of x on the left is zero, we must have $ab_0 + b_1 = a + b_1 = 0_R$, so that $b_1 = -a$. Then $ab_1 + b_2 = -a^2 + b_2 = 0$, so that $b_2 = a^2$. Continuing, we get $b_j = (-1)^j a^j$ for $1 \le j \le k$. Now look at the final term, ab_kx^{k+1}. This term must be zero. Since $b_k = (-1)^k a^k$, the term is $(-1)^k a^{k+1} x^{k+1} = 0_R$. Since $x^{k+1} \neq 0$, and it is not a zero divisor, we must have $a^{k+1} = 0_R$.

17. Answered in the text.

18. Let $f(x) = a_0 + a_1x + \ldots + a_nx^n$ and $g(x) = b_0 + b_1x + \ldots + b_mx^m$. Then $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + \ldots$. Therefore $\varphi(f(x) + g(x)) = a_0 + b_0 = \varphi(f(x)) + \varphi(g(x))$. Similarly $f(x)\cdot g(x) = (a_0b_0) + (a_0b_1 + a_1b_0)x + \ldots$, so that $\varphi(f(x)g(x)) = a_0b_0 = \varphi f(x))\ \varphi(g(x))$. Also φ is surjective since every $r \in \mathbb{R}$ is the constant term of some polynomial. (Just use the constant polynomial r !)

19. The map φ is surjective since every element of $\mathbb{Z}_n$ is of the form $[k]$ for some $k \in \mathbb{Z}$. Let $f(x)$ and $g(x)$ be as in Exercise 16, where $a_i, b_j \in \mathbb{Z}$. Then $\varphi(f(x) + g(x)) = \varphi((a_0 + b_0) + (a_1 + b_1)x + \ldots) = [a_0 + b_0] + [a_1 + b_1]x + \ldots = [a_0] + [b_0] + ([a_1]) + [b_1])x + \ldots = ([a_0] + [a_1]x + \ldots) + ([b_0]) + [b_1]x + \ldots) = \varphi(f(x)) + \varphi(g(x))$. Similarly $\varphi(f(x)\cdot g(x)) = \varphi(a_0b_0) + (a_0b_1 + a_1b_0)x + \ldots) = [a_0b_0] + [a_0b_1 + a_1b_0]x + \ldots = ([a_0][b_0]) + ([a_0][b_1] + [a_1][b_0])x + \ldots = ([a_0] + [a_1]x + \ldots)\cdot([b_0] + [b_1]x + \ldots) = \varphi(f(x))\cdot\varphi(g(x))$.

20. D is not a homomorphism, since $D(f\cdot g) = f\cdot D(g) + D(f)\cdot g$ by the product rule. Examples where this quantity does not equal $D(f)\cdot D(g)$ arc easy to find.

21. (a) Let $f(x)$ and $g(x)$ be given as in Exercise 16. Recall the convention that $a_i = 0_R$ for every $i > n$ and $b_j = 0_R$ for every $j > m$. Let Σ denote a summation over all indices $k = 0, 1, 2, \ldots$ These sums are really finite since after some point all the terms equal zero. For products: $\overline{h}(f(x)\cdot g(x)) = \overline{h}(\Sigma(a_0b_{\mathrm{k}} + a_1b_{k-1} + \ldots + a_kb_0)x^k) = \Sigma h(a_0b_k + a_1b_{k-1} + \ldots + \underline{a_k}b_0)x^k = \Sigma(h(a_0)h(b_k) + h(a_1)h(b_{k-1}) + \ldots + h(a_k)h(b_0))x^k = (\Sigma h(a_k)x^k)\cdot(\Sigma h(b_k)x^k) = \overline{h}(f(x))\cdot\ \overline{h}(g(x))$. The easier argument for sums is omitted.

(b) Suppose $\overline{h}$ is injective, and $h(a) = h(b)$ for some $a, b \in R$. Viewing $a, b \in R[x]$ we have $\overline{h}(a) = h(a) = h(b) = \overline{h}(b)$, so that $a = b$ in $R[x]$ and hence $a = b$ in R. Suppose h is injective. For $f(x)$ and $g(x)$ as above suppose that $\overline{h}(f(x)) = \overline{h}(g(x))$. Then $h(a_k) = h(b_k)$ for every k. Since h is injective this implies $a_k = b_k$ for every k and therefore $f(x) = g(x)$.

(c) Suppose $\overline{h}$ is surjective and $c \in S$. Then there exists some $f(x) = \Sigma a_k x_k \in R[x]$ with $c = \overline{h}(f(x)) = h(a_0) + h(a_1)x + h(\mathrm{a}_2)x^2 + \ldots$. The constant terms must coincide and we have $c = h(a_0)$. Therefore h is surjective.

Suppose h is surjective and $g(x) = \Sigma c_k x^k$ is given in $S[x]$, Then for every index k there exists $a \in R$ with $h(a_k) = c_k$. Define $f(x) = \Sigma a_k x^k$ in $R[x]$. Then $h(f(x)) = \Sigma h(a_k)x^{\mathrm{k}} = \Sigma c_k x_k = g(x)$. Therefore $\overline{h}$ is surjective.

(d) If $h : R \to S$ is an isomorphism, the function $\overline{h} : R[x] \to S[x]$ defined above is an isomorphism, using parts (a), (b) and (c).

22. For any $f(x) = \Sigma a_m x^m$ in $\mathbb{R}[x]$, define $\varphi(f(x)) = \Sigma a_m k(x)^m$. This map $\varphi : R[x] \to R[x]$ is well defined since there are only finitely many of the a_m which are not zero. By definition $\varphi(r) = r$ for every $r \in R$.

Homomorphism for products: Let $f(x) = \Sigma a_i x^i$ and $g(x) = \Sigma b_j x^j$. Then $\varphi(f(x)g(x)) = \varphi(\Sigma(a_0 b_m + a_1 b_{m-1} + \ldots + a_m b_0)x^m) = \Sigma(a_0 b_m + a_1 b_{m-1} + \ldots + a_m b_0)k(x)^m = (\Sigma a_i k(x)^i)(\Sigma b_j k(x)^{\mathrm{j}} = \varphi(f(x))\varphi(g(x))$. The easier proof for sums is omitted.

Suppose $\psi : R[x] \to R[x]$ is another such homomorphism. Then $\psi(a_0 + \ldots + a_{\mathrm{n}}x^n) = \psi(a_0) + \psi(a_1)\psi(x) + \psi(a^2)\psi(x)^2 + \ldots + \psi(a_n)\psi(x)^n = a_0 + a_1 k(x) + \ldots + a_n k(x)^n = \varphi(a_0 + \ldots + a_n x^n)$. Therefore φ is the unique homomorphism satisfying the given property.

Remark. If S is any ring containing R as a subring and $s \in S$ is given, men there exists a unique homomorphism $\varphi : R[x] \to S$ satisfying: $\varphi(r) = r$ for every $r \in R$ and $\psi(x) = s$. (Compare Exercise 24 of Section 4.4 below.)

4.2 Divisibility in $F[x]$

1. Answered in the text.

2. Since $a(x) \cdot 0_F = 0_F$ we have $a(x) \mid 0_F$ for every polynomial $a(x)$. Then $a(x)$ is a common divisor of $f(x)$ and 0_F if and only if $a(x) \mid f(x)$. Certainly $a(x) = f(x)$ provides a common divisor of maximal degree. Since it must be monic, the gcd = gcd = $c^{-1}f(x)$.

3. If $d(x)$ be the gcd of $x + a$ and $x + b$. Since $d(x) \mid (x + a)$ we have deg $d(x) \leq$ deg $(x + a) = 1$. Suppose the degree is 1, so that $d(x) = x + c$ for some $c \in F$, (since $d(x)$ is monic). The condition $d(x) \mid (x + a)$ then implies $c = a$ while $d(x) \mid (x + b)$ implies $c = b$. Since $a \neq b$ this is impossible. Therefore deg $d(x) = 0$ and $d(x) = 1$.

4. (a) Given $u(x), v(x) \in F[x]$ where $g(x) = f(x)u(x)$ and $f(x) = g(x)\,v(x)$. Therefore $g(x) = g(x)u(x)v(x)$ and $f(x) = f(x)u(x)v(x)$. If either $f(x) \neq 0$ or $g(x) \neq 0$, cancel to conclude $u(x)v(x) = l_F$, so that $v(x)$ is a unit in $F[x]$. By Exercise 4.1.12, $v(x) = c$ is a non-zero constant and $f(x) = cg(x)$. Finally if $f(x) = g(x) = 0_F$ the conclusion is trivial.

   (b) Given $f(x) = cg(x)$ where $0_F \neq c \in F$. If $g(x) = x^n + a_{n-1}x^{n-1} + \ldots$ then $f(x) = cx^n + ca_{n-1}x^{n-1} + \ldots$. Since $f(x)$ is also monic, $c = 1$.

5. (a) $x - 1$

   (b) $x^2 + x + 2$

   (c) $x^2 - 1$

   (d) $x + 6$

   (e) $x - i$

   (f) 1

   (g) $x^2 + \frac{3}{14}x - \frac{1}{7}$.

6. In each problem let $f(x)$, $g(x)$ be the given polynomials.
   (a) $x - 1 = f(x)\cdot(x + 1) + g(x)\cdot(-x^2 + 2)$
   (b) $x^2 + x + 2 = f(x)\cdot(\dfrac{1}{4}x + \dfrac{1}{2}) + g(x)\cdot(-\dfrac{1}{4}x^2 - \dfrac{1}{4}x + \dfrac{3}{4})$
   (c) $x^2 - 1 = f(x)\cdot(0) + g(x)\cdot(1)$
   (d) $x + 6 = f(x)\cdot(3x + 4) + g(x)\cdot(3x^2 + 4x + 2)$
   (e) $x + i = f(x)\cdot(\dfrac{1}{3}) + g(x)\cdot(-\dfrac{1}{3}x + \dfrac{1}{3}i)$
   (f) $1 = f(x)\cdot(1) + g(x)\cdot(x^2 + x)$

7. By hypothesis $f(x) \mid x$ and $f(x) \mid (x + 1)$. Therefore $f(x)$ must divide $(x + l) - x = 1$. Therefore $f(x)$ is a unit so it is a constant polynomial.

8. By Theorem 4.5 there exist $u(x)$, $v(x) \in F[x]$ such that $d(x) = f(x)u(x) + g(x)v(x)$. Since $h(x) \mid f(x)$ and $h(x) \mid g(x)$ it follows that $h(x) \mid d(x)$. Say $d(x) = h(x)w(x)$ for some $w(x)$. Since $d(x)$ is a common divisor of $f(x)$ and $g(x)$ the definition of $h(x)$ implies deg $d(x) \leq$ deg $h(x)$. Conclude that deg $h(x) =$ deg $d(x)$ and therefore deg $w(x) = 0$. Then and $w(x) = r$ is a nonzero constant and $h(x) = r^{-1}d(x)$.

9. $f(x)$ must be a unit (a nonzero constant). For if $f(x)$ and 0_F are relatively prime then 1 is the gcd of $f(x)$ and 0_F (and therefore $f(x) \neq 0_F$ since the gcd of 0_F with itself is undefined). But this gcd equals $cf(x)$ for some non-zero constant c as in Exercise 2. Then $cf(x) = 1_F$ and $f(x)$ is a nonzero constant.

10. Since $x^3 - 3abx + a^3 + b^3 = (x + a + b)\cdot(x^2 - (a + b)x + (a^2 - ab + b^2))$ we see that the gcd is $x + a + b$.

11. We claim that $t(x)$ is the gcd of $f(x)$ and $g(x)$. First let us show that $t(x) \mid f(x)$. By the division algorithm there exist $q(x)$ and $r(x)$ with $f(x) = t(x)q(x) + r(x)$ and either $r(x) = 0$ or deg $r(x) <$ deg $t(x)$. If the latter case holds then $r(x) = f(x) - t(x)q(x) = f(x) - (f(x)u(x) + g(x)v(x))q(x) = f(x)\cdot(1 - u(x)q(x)) + g(x)\cdot(v(x)q(x))$ lies in S. But $r(x)$ has degree less than deg $t(x)$, contrary to the choice of $t(x)$. Therefore this case cannot hold, forcing $r(x) = 0$ so that $f(x) = t(x)q(x)$ and $t(x) \mid f(x)$ as claimed. Similarly we have $t(x) \mid g(x)$, and $t(x)$ is a common divisor.

    Finally if $c(x) \mid f(x)$ and $c(x) \mid g(x)$ then $c(x)$ divides every linear combination of $f(x)$ and $g(x)$, so in particular it divides $t(x) = f(x)u(x) + g(x)v(x)$. Therefore deg $c(x) \leq$ deg $t(x)$, and hence $t(x)$ is the gcd.

12. Let $d(x)$ be the gcd. Then certainly (i) holds. For (ii) suppose $c(x) \mid f(x)$ and $c(x) \mid g(x)$. Then $c(x)$ divides any linear combination of $f(x)$ and $g(x)$. By Theorem 4.4 we know that $d(x)$ is such a linear combination: $d(x) = f(x)u(x) + g(x)v(x)$ for some $u(x)$ and $v(x)$. Therefore $c(x)$ divides $d(x)$

    Suppose $d(x)$ satisfied (i) and (ii). Then it is easy to check that $d(x)$ satisfies the conditions (i) and (ii) of the definition of gcd, for if $c(x) \mid d(x)$ then deg $c(x) \leq$ deg $d(x)$. Therefore $d(x)$ is the gcd.

13. Since $f(x)$ and $g(x)$ are relatively prime their gcd is 1 and Theorem 4.5 implies that there exist $u(x)$, $v(x)$ such that $1 = f(x)u(x) + g(x)v(x)$. Therefore $h(x) = f(x)\cdot(u(x)h(x)) + (g(x)h(x))\cdot v(x)$ which is a linear combination of $f(x)$ and $g(x)h(x)$. Since $f(x)$ divides both of these terms, $f(x)$ must divide their linear combination $h(x)$.

14. (Compare Exercise 1.2.17) Suppose $h(x) = g(x)w(x)$ for some $w(x)$. Then $f(x) \mid g(x)w(x)$ and $f(x)$, $g(x)$ are relatively prime. Theorem 4.7 implies $f(x) \mid w(x)$, say $w(x) = f(x)q(x)$ for some $q(x)$. Therefore $h(x) = g(x)\cdot(f(x)q(x))$ and $f(x)g(x) \mid h(x)$.

15. Let $d(x)$ be the gcd of $h(x)$ and $g(x)$. Then $h(x) \mid f(x)$ implies $d(x) \mid f(x)$. Since the gcd of $f(x)$ and $g(x)$ is 1_F we must have $d(x) \mid 1_F$. Then d(x) is a unit, hence a nonzero constant. Since $d(x)$ is monic we see $d(x) = 1_F$.

16. Let $d(x)$ be the gcd of $f(x)h(x)$ and $g(x)$, and let $e(x)$ be the gcd of $h(x)$ and $g(x)$. Since $e(x)$ 1 $h(x)$ we also have $e(x) \mid f(x)h(x)$, so mat $e(x)$ is a common divisor of $f(x)h(x)$ and $g(x)$, and by Corollary 4.5 $e(x) \mid d(x)$.

    On the other hand $d(x) \mid g(x)$ so by Exercise 15 $d(x)$ and $f(x)$ are relatively prime. Since $d(x) \mid f(x)h(x)$ we deduce from Theorem 4.7 that $d(x) \mid h(x)$. Therefore $d(x)$ is a common divisor of $h(x)$ and $g(x)$ and Corollary 4.6 implies that $d(x) \mid e(x)$. Exercise 4(b) then implies that $e(x) = d(x)$.

4.3 Irreducibles and Unique Factorization

1. (a) Answered in the text. (b) $x^5 + 2x^2 + 2$
   (c) Answered in the text.

2. Let $f(x) = a_nx^n + a_{n-1}\,x^{n-1} + \ldots + a_0$ where a$_n \neq 0$. Then $g(x) =$ $a_n^{-1}f(x) = x^n + a_n^{-1}a_{n-1}x^{n-1} + . \; . \; . + a_n^{-1}a_0$ is a monic associate of $f(x)$. If $h(x)$ is another monic associate of $f(x)$ then $g(x) = c\cdot h(x)$ for some nonzero $c \in F$. Since $g(x)$ and $h(x)$ have leading coefficients equal to l_F we see that $c = l_F$ and $g(x) = h(x)$.

3. (a) Answered in the text.
   (b) $x + 3$, $2x + 6$, $3x + 2$, $4x + 5$, $5x + 1$, $6x + 4$

4. Let $f(x) = a_nx^n + \ldots + a_0$ where $a_n \neq 0$. (This is valid since we assume $f(x) \neq 0$.) The associates of $f(x)$ are exactly the polynomials $c\cdot f(x) = ca_nx^n + \ldots + ca_0$ for the $p - 1$ different values of c which are the nonzero elements of $\mathbb{Z}_p$. These are all different since $cf(x) = c'f(x)$ implies $c = c'$.

5. If $f(x)$ and $g(x)$ are associates then $f(x) = c\cdot g(x)$ for some unit c. This equation implies $g(x) \mid f(x)$ and the equation $g(x) = c^{-1}\cdot f(x)$ implies that $g(x) \mid f(x)$. The converse appears in Exercise 4(a) of Section 4.2.

6. If $x^2 + 1 = (ax + b)(cx + d)$ then $ac = 1$, $ad + bc = 0$ and $bd = 1$. But then $(ad)^2 = ad{\cdot}ad = (-bc)\ ad = -(ac)(bd) = -1$. However every square in $\mathbb{R}$ is positive and -1 is negative, a contradiction. Therefore no such factorization can exist in $\mathbb{R}[x]$, so it certainly cannot exist in $\mathbb{Q}[x]$.

7. ($\Rightarrow$) Answered in the text. ($\Leftarrow$) If every associate of $f(x)$ is irreducible then certainly $f(x)$ is irreducible since it is one of its associates.

8. Suppose $f(x) = g(x)h(x)$ where the polynomials $g(x)$, $h(x)$ have degrees smaller than deg $f(x)$. Then $g(x) \mid f(x)$, $g(x)$ is not an associate of $f(x)$ (since associates have the same degrees), and $g(x)$ is not a unit (for if deg $g(x) = 0$ and deg $h(x) =$ deg $f(x)$).

9. (a) Answered in the text. (b) $x^3 + x + 1$, $x^3 + x^2 + 1$
(c) Answered in the text.

10. (a) Irreducible in $\mathbb{Q}[x]$ but not in $\mathbb{R}[x]$, because $x^2 - 3 = (x - \sqrt{3}\,)(x + \sqrt{3}\,)$ and $\sqrt{3}$ is in $\mathbb{R}$ but not in $\mathbb{Q}$
(b) Reducible: $x^2 + x - 2 = (x - 1)(x + 2)$ in $\mathbb{Z}_3[x]$ and in $\mathbb{Z}_7[x]$.

11. If $x^3 - 3$ factors non-trivially in $\mathbb{Z}_7[x]$ then it equals $r(x)s(x)$ where deg $r(x)$, deg $s(x)$ are 1 or 2 and add up to 3. Then one of the factors has degree 1. The monic associate of that factor is still a factor of $x^3 - 3$ (see Exercise 5). Therefore $(x - \mathrm{a})$ is a factor of $x^3 - 3$ for some $a \in \mathbb{Z}_7$. Claim, $a^3 = 3$ in $\mathbb{Z}_7$. Proof. Suppose $x^3 - 3 = (x - a){\cdot}(x^2 + bx + c)$. By multiplying out the terms and equating like coefficients we obtain: $a = b$, $c = ab$ and $ac = 3$. Then $a^3 = aab = ac = 3$.

Finally, by computing a^3 for each of the 7 elements of $\mathbb{Z}_7$ we find that that 3 never arises. Then no such a can exist and the factorization is impossible.

12. $x^4 - 4 = (x^2 - 2)(x^2 + 2)$ in $\mathbb{Q}[x]$.
It factors as $(x - \sqrt{2}\,)(x + \sqrt{2}\,)(x^2 + 2)$ in $\mathbb{R}[x]$.
It factors as $(x - \sqrt{2}\,)(x + \sqrt{2}\,)(x + \sqrt{-2}\,)(x - \sqrt{-2}\,)$ in $\mathbb{C}[x]$.

The linear factors are clearly irreducible. If $x + 2$ factors in $\mathbb{R}[x]$ it would be a product of two factors of degree 1, which we may assume are monic (as in Exercise 11). But then the unique factorization in $\mathbb{C}[x]$ implies that the factors must be $x \pm \sqrt{-2}$ which do not lie in $\mathbb{R}[x]$.

Since $x^2 + 2$ is irreducible in $\mathbb{R}[x]$ it certainly is irreducible in $\mathbb{Q}[x]$. The polynomial $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, for otherwise the monic factors $x \pm \sqrt{2}$ would lie in $\mathbb{Q}[x]$, but $\sqrt{2}$ is not in $\mathbb{Q}$.

13. (a) $(3x + 1)(6x + 1) = 1$ in $\mathbb{Z}_9[x]$.
(b) First of all examine all the products $(3x + r)(3x + s)$ and $(3x + r)(6x + s)$. Every polynomial of the form $ax + b$ in $\mathbb{Z}_9[x]$ arises this way, except for the constant polynomials 3 and 6. If $g(x) \in \mathbb{Z}_9[x]$ then $g(x) = a(x)b(x)$ where $a(x) = (3x + 1)g(x)$ and $b(x) = 6x{+}1$. This factorization fulfills the condition provided $a(x)$ has positive degree. This fails only when $a(x)$ is a constant. Work (mod 3) to show that $a(x) = g(x)$ (mod 3) is a constant so there is an expression $g(x) = c_0 + 3x \cdot\cdot g_1(x)$ in $\mathbb{Z}_9[x]$. Then $a(x) = (3x + 1)(c_0 + 3x{\cdot}g_1(x)) = c_0 + 3x(c_0 + g_1(x))$ is a constant, so that $3(c_0 + g_1(x)) = 0$. But then $g(x) = c_0 + x{\cdot}(3g_1(x)) = c_0 + x{\cdot}(-3c_0)$ has degree ≤ 1. Therefore if deg $g(x) > 1$ then the original factorization does not fail. All the cases where deg $g(x) \le 1$ were handled earlier.

Those constant polynomials 3 and 6 cannot be factored that way. For instance suppose $3 = a(x) \cdot b(x)$ in $\mathbb{Z}_9[x]$. Then $a(x) \cdot b(x) = 0 \pmod 3$. Switch the factors if necessary to assume $a(x) = 0 \pmod 3$. Then $a(x) = 3a_1(x)$ in $\mathbb{Z}_9[x]$ and $3a_1(x) \cdot b(x) = 3$. This implies that $a_1(x) \cdot b(x) = 1 \pmod 3$ so both terms must be constants (mod 3). Express $a_1(x) = c_0 + 3c_1x + 3c_2x^2 + \ldots$ in $\mathbb{Z}_9[x]$. Then $a(x) = 3a_1(x) = 3c_0$ does not have positive degree in $\mathbb{Z}_9[x]$.

14. $x^2 + x = x(x + 1) = (x + 4)(x + 3)$.

15. Answered in the text. Compare Exercise 1.3.11.

16. ($\Rightarrow$) If $p(x)$ is irreducible let $d(x)$ be the gcd of $p(x)$ and $g(x)$. Then $d(x) \mid p(x)$ so that either $d(x)$ is a nonzero constant, and hence $d(x) = 1$ since it is monic, or $d(x)$ is an associate of $p(x)$. Since $d(x) \mid g(x)$, the latter condition implies that $p(x) \mid g(x)$. (See Exercise 5.)
($\Leftarrow$) If $p(x)$ is reducible then there exists a factor $a(x) \mid p(x)$ where $0 < \deg a(x) < \deg p(x)$. Then $p(x)$ does not divide $a(x)$ and is not relatively prime to $a(x)$. Then the stated condition fails.

17. The only gap is in the proof of (1) $\Rightarrow$ (2). Suppose $p(x)$ is irreducible and $p(x) \mid b(x)\ c(x)$. If $p(x) \nmid b(x)$ then Exercise 16 implies that $p(x)$ and $b(x)$ are relatively prime. Theorem 4.7 then implies that $p(x) \mid c(x)$.

18. (1) $\Rightarrow$ (3). Suppose $p(x)$ is irreducible and $p(x) = r(x)s(x)$. Then $r(x)$ and $s(x)$ are divisors of $p(x)$ and the irreducibility implies that they are either nonzero constants or associates of $p(x)$. If $r(x)$ is not a nonzero constant then $r(x) = cp(x)$ for some nonzero $c \in F$. Then $p(x) = cp(x)s(x)$ so that $1_F = cs(x)$. Then $s(x)$ is a unit in $F[x]$, so it is a nonzero constant.
(3) $\Rightarrow$ (1). Suppose $r(x)$ is a divisor of $p(x)$. Then $p(x) = r(x)s(x)$ for some $s(x)$. By hypothesis, $r(x)$ or $s(x)$ is a nonzero constant. If $r(x)$ is not a nonzero constant then we must have $s(x) = c$ is a nonzero constant. But then $p(x) = cr(x)$ and $r(x) = c^{-1}p(x)$ is an associate of $p(x)$.

19. Use induction on n. The case $n = 1$ is vacuous and the case $n = 2$ is done in Theorem 4.11. Suppose $n \geq 3$ and $p(x) \mid a_1(x)a_2(x) \ldots a_n(x)$. Applying Theorem 4.11 we see that either $p(x) \mid a_1(x)$ or $p(x) \mid a_2(x) \ldots a_n(x)$. In the latter case the induction hypothesis implies that $p(x)$ divides one of the $a_i(x)$ for some $j = 2, 3, \ldots, n$.

20. From the definition of "irreducible" we know that $p(x)$ cannot divide $q(x)$. Then Exercise 16 implies that $p(x)$ and q(x) are relatively prime.

21. (a) As seen in the answers in the text, if $f(x)$ is a monic reducible quadratic then $f(x) = (x - a)(x - b)$ for some $a, b \in \mathbb{Z}p$. There are p of these of the type $(x - a)^2$ and there are $p(p - 1)/2$ of them having $a \neq b$ (the number of ways of choosing 2 things from a set of p things). Therefore there are $p + p(p - 1)/2 = (p^2 + p)/2$ of them.
(b) The monic quadratic polynomials in $\mathbb{Z}_p\,[x]$ are $x^2 + rx + s$ for any $r, s \in \mathbb{Z}_p$. Therefore there are exactly p^2 of them. Then using part (a), the number of irreducible quadratics is $p^2 - (p^2 + \text{p})/2 = (p^2 - \text{p})/2$.

22. These polynomials can be factored one by one. For a more unified approach recall Exercise 2.2.9.
(a) Note that $a^3 = a$ for each of the 3 elements of $\mathbb{Z}_3$. Therefore $(x + a)^3 = x^3 + a^3 = x^3 + a$.
(b) Note that $a = a$ for each of the 5 elements of $\mathbb{Z}_5$. Therefore $(x + a)^5 = x^5 + a^5 = x^5 + a$.

23. (a) If $x^2 + 2$ is reducible it must be a product of two linear factors. As in Exercise 11 we can adjust the leading coefficients to assume these factors are monic. Then $x^3 + 2 = (x - a)(x- b)$ for some a, $b \in \mathbb{Z}_5$.

Multiplying this out and equating coefficients shows that $a + b = 0$ and $ab = 2$. Therefore $a^2 = a(-b) = -2 = 3$ in $\mathbb{Z}_5$. Computing $0^2, 1^2, \ldots, 4^2$ in $\mathbb{Z}_5$ we see that 3 never occurs. Then no such factorization can occur.

(b) $x^4 - 4 = (x^2 + 2)(x^2 + 3)$. The same argument as in (a) shows that $x^2 +3$ is also irreducible in $\mathbb{Z}\ [x]$.

24. Let $S = \{\ f(x) \in F[x] : f(x)$ is nonconstant and $f(x)$ is not expressible as a product of irreducibles in $f[x]\ \}$. Assume S is not empty and try to derive a contradiction. Then the set $S_0 = \{\ \deg f(x) : f(x) \in S\ \}$ is a non-empty subset of non-negative integers so (by the Well Ordering Axiom) it has a minimal element d. Let $g(x) \in S$ be an element having this minimal degree: $\deg g(x) = d$. Since no irreducible polynomial lies in S (by definition) we see that $g(x)$ must be reducible. Therefore $g(x) = a(x)b(x)$ for some $a(x)$ and $b(x)$, nonconstant polynomials of degree $< d$. By the minimal choice of d it follows that $a(x)$ and $b(x)$ are not in S so they are expressible as products of irreducibles. But then their product $g(x)$ is also expressible as a product of irreducibles, contrary to hypothesis. This contradiction shows that S must be empty.

The uniqueness proof is partly done in the text. To complete the argument we note that $p_2(x)(c_1p_3(x) \ldots p_r(x)) = q_2(x)q_3(x) \ldots q_s(x)$. Then $p_2(x) \mid q_2(x)q_3(x)\cdots q_s(x)$ and Corollary 4.12 implies that $p_2(x)$ divides one of the $q_i(x)$; as above, assume $p_2(x) \mid q_2(x)$. Hence $p_2(x) = c_2q_2(x)$ for some nonzero $c_2 \in F$, and $q_2(x)(c_1c_2p_3(x) \ldots p_r(x)) = p_2(x)(c_1p_3(x) \ldots p_r(x)) = q_2(x)q_3(x)\cdots q_s(x)$. Cancel $q_2(x)$ to get $p_3(x)(c,c_2p_4(x) \ldots p_r(x)) = q_3(x) \ldots q_s(x)$. Continue in this manner, repeatedly using Corollary 4.12 and eliminating one irreducible on each side at every step. If $r > s$ then after s steps all the q's will be eliminated and $p_{s+1}(x) \ldots p_r(x) = c$ for some $c \in F$. Comparing degrees yields a contradiction. By a similar argument, $s > r$ is also impossible. Therefore $r = s$, and after r steps the elimination process ends with $p_1\ (x) = c_1q_1(x)$, $p_2(x) = c_2q_2(x), \ldots, p_r(x) = c_rq_r(x)$ for some nonzero $c_j \in F$.

25. By Theorem 4.13 $f(x) = q_1(x)q_2(x) \ldots q_r(x)$ for some irreducible $q_i(x)$. Let $q_i(x) = c_ip_i(x)$ where $p_j\cdot\ (x)$ is monic irreducible (see Exercises 2 and 7). Then $f(x) = cp_1(x)p_2(x) \ldots p_r\ (x)$ where $c = c_1c_2 \ldots c_r$.

Now suppose that $f(x) = dg_1(x)g_2(x)\cdots g_s(x)$ where $d \in F$ and $g_i(x)$ is monic irreducible. Since all the polynomials $p_i(x)$ and $g_i(x)$ are monic, we have $c = d$ by comparing the leading coefficients. Therefore $p_1(x)p_2(x) \ldots p_r(x) = g_1(x)g_2(x)\cdot\cdot\cdot g_s(x)$, and Theorem 4.10 implies that after relabeling the $g_i(x)$'s we have $r = s$ and $p_i(x)$ is an associate of $g_i(x)$ for each i. Since these are monic it follows that $p_{i\cdot}(x) = g_i(x)$ for each i.

26. Suppose $f(x) = ax^2 + bx + c$ is irreducible in $\mathbb{C}[x]$. The quadratic formula implies that $f(x)$ has a root in $\mathbb{C}$, so it factors into linear factors. To justify the quadratic formula, we must know that every element of $\mathbb{C}$ has a square root in $\mathbb{C}$. One proof is to use the polar form for elements of $\mathbb{C}$. Here is another method, using only properties of the real numbers: Proof. If a, $b \in \mathbb{R}$, solve $(x + yi)^2 = a + bi$ for real x, y by multiplying it out, eliminating y and using the quadratic formula. A solution exists since every nonnegative element in $\mathbb{R}$ has a square root in $\mathbb{R}$.

4.4 Polynomial Functions, Roots, and Reducibility

1. (a) Answered in the text. (b) $x^n - x$ is one example.

2. (a) 2 (b) 170802 (c) -5 (d) 4

3. (a) $f(-2) = -24 \neq 0$ in $\mathbb{R}$, so $x + 2$ is not a factor.
 (b) $f(\frac{1}{2}) = 0$ in $\mathbb{Q}$ so $x - \frac{1}{2}$ is a factor.
 (c) $f(3) = 0$ in $\mathbb{Z}_5$ so $x + 2$ is a factor.
 (d) $f(3) = 0$ in $\mathbb{Z}_7$ so $x - 3$ is a factor.

4. (a) k $= -2$ (b) $k = 2$

5. Let $f(x) = a_n x^n + \ldots + a_2 x^2 + a_1 x + a_0$. Then by Theorem 4.15 $x - 1_F$ is a factor of $f(x)$ if and only if $f(1_F) = 0_F$. Since $f(1_F) = a_n + \ldots + a_1 + a_0$ the claim follows.

6. (a) and (b) are direct calculations. For instance $3^4 = 81 \equiv 1 \pmod{5}$ so that $3^5 \equiv 3 \pmod{5}$.
 (c) Conjecture that $a^p = a \pmod{p}$ for every integer a.

7. As in Exercise 6, verify directly that $a^7 = a \pmod{7}$ for each $a = 0, 1, 2, 3, 4, 5$ and 6. By the argument used to prove Corollary 4.16, the polynomial $f(x) = x(x-1)(x-2)(x-3)(x-4)(x-5)(x-6)$ must divide $x^7 - x$. Since they have the same degree, the quotient has degree 0, so it is a nonzero constant. Since both polynomials are monic, compare leading coefficients to see that they are equal.

8. (a) $\sqrt{7} \in \mathbb{R}$ so it is reducible.
 (d) No root in $\mathbb{Q}$ so irreducible by Corollary 4.18.
 (c) $\sqrt{7} \in$ ₵ so it is reducible.
 (d) Irreducible since none of the 5 elements is a root.
 (e) 4 is a root so it is reducible.
 (f) 1 is a root so it is reducible.

9. Answered in the text for $\mathbb{Z}_3[x]$.
 For $\mathbb{Z}_5[x]$: $x^2 + 2$, $x^2 + 3$, $x^2 + x + 1$, $x^2 + x + 2$, $x^2 + 2x + 3$, $x^2 + 2x + 4$, $x^2 + 3x + 3$, $x^2 + 3x + 4$, $x^2 + 4x + 1$, $x^2 + 4x + 2$ (There are 10 listed, as predicted in Exercise 4.3.21(b).)

10. $x^2 + 1$ is reducible in $\mathbb{Z}_p[x]$ when it has a root in $\mathbb{Z}_p$, that is, when -1 is a square in $\mathbb{Z}_p$. For example, if p is expressible as $p = a^2 + 1$ in $\mathbb{Z}$, then $[a]$ is a root of $x^2 + 1$. For example, $p = 17$ and $p = 37$.

11. The polynomial $f(x)$ given has $f(2) = 39$ in $\mathbb{Z}$, In order for $f(2) = 0$ in $\mathbb{Z}_p$ we need p 139. Therefore $p = 3$ or 13.

12. If $f(x) = c_0x^n + c_1x^{n-1} + . . . + c_{n-1}x + c_n$ define $f^*(x) = c_nx^n + c_{n-1}.x^{n-1} + . . . + c_1x + c_0$. Calculate that $x^nf(x^{-1}) = f^*(x)$ and $x^nf^*(x^{-1}) = f(x)$. Therefore if $a \neq 0$ then a is a root of $f(x) \Leftrightarrow 0 = f(a) = \mathrm{a}^nf^*(a^{-1}) \Leftrightarrow f^*(a^{-1}) = 0 \Leftrightarrow a^{-1}$ is a root of $f^*(x)$.

13. (a) Answered in the text,
    (b) No. The polynomials x and x^2 have the same roots. Similarly the polynomials 1 and $x^2 + 1$ have the same roots in $\mathbb{R}$.

14. (a) The Factor Theorem applied twice implies that $(x - r)(x - s)$ divides $ax^2 + bx + c$. Since these have the same degree, the quotient must be a nonzero constant. Comparison of leading coefficients shows that the quotient is a. Therefore $ax + bx + c = a(x - r)(x - s)$. Multiplying this out and equating like coefficients yields the claim.
    (b) The same argument implies that $ax^3 + bx^2 + cx + d = a(x - r)(x - s)(x - t) = a(x^3 - (r + s + t)x^2 + (rs + rt + st)x + rst)$. Equating like coefficients completes the proof.

15. $x^2 + 1$ is reducible in $\mathbb{Z}_p[x]$ if and only if there is a root, or equivalently, there exists $a \in \mathbb{Z}$ with $a^2 \equiv -1 \pmod{p}$. This is the same saying: there exists $a \in 2$ with $a(p - a) \equiv 1 \pmod{p}$. Let $b = p - a$.

16. Let $h(x) = f(x) - g(x)$. By hypothesis this polynomial has $n + 1$ roots $c_0 . . . c_n$. If $h(x) \neq 0$ then deg $h(x) \leq \max\{\deg f(x), \deg g(x)\} \leq n$ contrary to Corollary 4.16. Therefore $h(x)$ must be the zero polynomial and $f(x) = g(x)$.

17. $x^2 + 5x = x(x + 5) = (x + 2)(x + 3)$ has roots 0, 1, 4, 3 in $\mathbb{Z}_6$. This does not contradict Corollary 4.13 since $\mathbb{Z}_6$ is not a field.

18. Let $f(x) = c_nx^n + c_{n-1}x^{n-1} + . . . + c_1x + c_0$. Since $c_i \in \mathbb{Q}$ we know that $\varphi(c_i) = c_i$. Then $f(r) = 0$ implies that $0 = \varphi(f(r)) = \varphi(c_nr^n + + . . . + c_1r + c_0) = c_n\varphi(r)^n + . . . + c_1\varphi(r)\ c_0 = f(\varphi(r))$. Then $\varphi(r)$ is also a root of $f(x)$.

19. (a) Partly answered in the text. We have $f(x) = (x - a)^kg(x)$ where $g(a) \neq 0$. Then $f'(x) = k(x - a)^{k-1}g(x) + (x - a)^kg'(x)$. If $k \geq 2$ then a is a root of both $f'(x)$ and $f'(x)$. Conversely suppose a is a root of both $f(x)$ and $f'(x)$. If $k = 1$ then $f'(x) = g(x) + (x - a)g'(x)$ and $f'(a) = g(a) \neq 0$.
    b) If $f(x)$ has a multiple root $a \in R$ then part (a) implies that a is a root of $f(x)$ and $f'(x)$. Then $x - a$ divides both $f(x)$ and $f'(x)$ so they are not relatively prime.

20. The proofs of the Remainder and Factor Theorems involve dividing by the monic polynomial $x - a$ and analyzing the remainder. By Exercise 4.1.14, division by monic polynomials is valid in $R[x]$, whenever R is a commutative ring with identity. The proofs of the Remainder and Factor Theorems go through unchanged.

21. The proof of Corollary 4.16 contains only onestep where properties of the coefficient ring F are used. This step is the statement that if $0_F = f(c) = (c - a)g(c)$ and $c - a \neq 0$ then $g(c) = 0_F$. This statement is valid in an integral domain R, since there are no zero divisors. (Corollary 4.16 does fail when zero divisors exist, as in Exercise 17.)

22. The same proof works, substituting Exercise 21 for Corollary 4.16.

23. These statements go back to the definitions of polynomial addition and multiplication and work equally well in $R\,[x]$ for any commutative ring R instead of a field F.
   Let $g(x) = \Sigma\, a_n x^n$, where the sigma denotes a sum over $n = 0, 1, 2, \ldots$ and all the coefficients equal 0_F after some point, so the sum is a finite one. Similarly let $h(x) = \Sigma\, b_n x^n$.
   (a) $f(x) = g(x) + h(x) = \Sigma(a_n + b_n)x^n$ by definition. By definition of "evaluation at r" we have $f(r) = \Sigma(a_n + b_n)r^n$. The axioms of the ring F then imply that $f(r) = (\Sigma a_n r^n) + (\Sigma\, b_n r^n) = g(r) + h(r)$.
   (b) $f(x) = g(x)h(x) = \Sigma\, (a_0 b_n + a_1 b_{n\text{-}1} + \ldots + a_n b_0)x^n$ by definition. Therefore $f(r) = \Sigma\, (a_0 b_n + a_1 b_{n\text{-}1} + \ldots + a_n b_0)r^n$ and the axioms of the ring F imply that $f(r) = (\Sigma\, a_i r^i)(\Sigma\, b_j r^j) = g(r)\cdot h(r)$.
   These facts are often used when evaluations at $x = r$ are made. For example in the proof of the Remainder Theorem 4.14 the polynomial $f(x) = (x - a)q(x) + r(x)$ is evaluated at $x = a$ to yield $f(a) = r(a)$. This evaluation uses the properties above. Also compare Exercise 4.1.20.

24. By Exercise 23, φ_a is a homomorphism. It is certainly surjective since for any $c \in F$ we view $c \in F[x]$ and find $\varphi_a(c) = c$. (See Exercise 31 for an application.)

25. (a) As Exercise 4.1.2, check that $\mathbb{Q}\,[\pi]$ is a subring of $\mathbb{R}$ containing $\mathbb{Q}$ and π.
   (b) The proof in Exercises 23, 24 proves a more general result:
   Lemma. Suppose $\mathbb{R}$ and S are commutative rings with $R \subseteq S$, and $a \in S$ is given. Define a map $\varphi_a : \mathbb{R}[x] \to S$ by $\varphi(f(\mathrm{x})) = f(a)$. Then φ_a is a homomorphism of rings and $\varphi_a(c) = c$ for every $c \in R$. In our case consider the homomorphism $\varphi_\pi : \mathbb{Q}\,[x] \to \mathbb{R}$. Its image is the set of all $f(\pi)$ where $f(x) \in \mathbb{Q}\,[x]$. That is, its image is $\mathbb{Q}\,[\pi]$ and we obtain a surjective ring homomorphism $\varphi_\pi : \mathbb{Q}\,[x] \to Q\,[\pi]$. To prove it is injective, suppose $\varphi_\pi(f(x)) = \varphi_\pi(g(x))$ for some f, $g \in \mathbb{Q}\,[x]$, Consider $h(x) = f(x) - g(x)$ and note that $\varphi_\pi(h(x)) = \varphi_\pi(f(x) - g(x)) = \varphi_\pi(f(x)) - \varphi_\pi(g(x)) = 0$. Then $h(\pi) = 0$ and the assumed nontrivial fact then implies that $h(x) = 0$. Therefore $f(x) = g(x)$ proving that φ_π is injective.

26. (a) It is a subring for the same reasons as in Exercise 25 or Exercise 4.1.2. In this case the ring is much smaller since any power $(\sqrt{2})^m$ can be expressed as r or $s\sqrt{2}$ for suitable integers r, s. Then the general element of $\mathbb{Q}[\sqrt{2}\,]$ is of the type $r_0 + r_1\sqrt{2}$ where r_0, $r_1 \in \mathbb{Q}$.
   (b) The function θ is the evaluation map $\varphi_{\sqrt{2}}$ as described in Exercise 25, so it is a ring homomorphism. Clearly it is surjective, but it is not injective because $\theta(x^2 - 2) = 0$.

27. Suppose f, $g \in T$. Then there exist polynomials $f_0(x)$, $g_0(x) \in F[x]$ such that $f(r) = f_0(r)$ for every $r \in F$. Exercise 23 shows that $f + g$ is the function associated to the polynomial $f_0(x) + g_0(x)$, and fg is the function associated to the polynomial $f_0(x)\cdot g_0(x)$. Therefore $f + g$, $fg \in T$.

   It is routine to verify the axioms to show T is a ring. The constant zero function is 0_T, and the constant 1 function is 1_T. The commutative, associative and distributive axioms are checked by evaluating at a fixed $r \in F$ and using the corresponding axiom of F.

28. (a) A function $\theta : \mathbb{Z}_3 \to \mathbb{Z}_3$ is determined by the values $\theta([0])$, $\theta([1])$, $\theta([2])$. Each of these values has three possibilities, so there are exactly 27 functions altogether. Then the ring T has at most 27 elements. By evaluating, check that $(x + 1)\cdot(x^2 + 2x) = 0_T$ but the factors are nonzero.
b) (T is finite but $\mathbb{Z}_3[x]$ is infinite, so they cannot be isomorphic.

29. If f is a nonzero polynomial of degree zero, then it is a nonzero constant, so it has no roots in F and thus satisfies the conclusion of the corollary. Now suppose that the corollary holds for all functions with degree less than n, where $n > 0$ is some integer, and let $f(x)$ be a nonzero polynomial of degree n. If f has no roots in F, then the corollary obviously holds, so assume that f has a root in F, say $a \in F$. Then by the Factor Theorem,

$$f(x) = (x - a)g(x):$$

Comparing degrees, we see that $n = \deg f(x) = \deg(x - a) + \deg g(x) = 1 + \deg g(x)$, so that $\deg g(x) = n - 1$. By the inductive hypothesis, g(x) has at most $n - 1$ roots in F. But the roots of F consist of a plus the roots of $g(x)$, so that $f(x)$ has at most n roots in F.

30. Define $\varphi : F[x] \to T$ as in the Hint. First check that φ is a homomorphism: $\varphi(f(x) + g(x))$ is the function $F \to F$ sending r to $(f + g)(r). = f(r) + g(r)$. This coincides with $\varphi(f(x)) + \varphi(g(x))$. Similarly $\varphi(f(x)g(x))$ coincides with $\varphi(f(x))\cdot\varphi(g(x))$. By definition, the ring T is the image of φ, so φ is surjective. Finally, φ is injective by Corollary 4.19.

31. If $f(x)$ is reducible then $f(x) = a(x)b(x)$ where $a(x)$, $b(x)$ are not units (i.e. they have degrees > 0). Then $\varphi(f(x)) = \varphi(a(x))\cdot\varphi(b(x))$. Since φ is an isomorphism, φ carries units to units and non-units to non-units. Therefore the factors $\varphi(a(x))$ and $\varphi(b(x))$ cannot be units, and $\varphi(f(x))$ is reducible. Conversely if $\varphi(f(x))$ is reducible then applying the part just done to the isomorphism φ^{-1} we see that $f(x)$ is reducible.

32. (a) Use the Lemma stated in Exercise 25 in the case $\mathbb{R} = F$ and $S = F[x]$ with $a = x + 1_F$. The corresponding map is a homomorphism Fixing F. Similarly defining $\psi : F[x] \to F[x]$ by setting $\psi(f(x)) = f(x - 1_F)$ we see that ψ is the inverse of φ. Therefore φ is bijective, so it is an isomorphism. (b) $f(x)$ is irreducible if and only if $\varphi(f(x)) = f(x + 1_F)$ is irreducible, using Exercise 30.

4.5 Irreducibility in $\mathbb{Q}[x]$

1. (a) Answered in the text. (b) $xx(x^3 + 4x^2 + x + 1)$
(c) Answered in the text. (d) $(x + 1)(2x - 3)(x^2 - 2x + 2)$
(e) Answered in the text. (f) $(3x + 1)(2x - 7)(x^2 - 2x - 1)$
2. $x^2 - p$ is irreducible in $\mathbb{Q}[x]$ by the Eisenstein Criterion. Therefore the factor $(x - \sqrt{p}\,)$ cannot be in $\mathbb{Q}[x]$. Hence $\sqrt{p}$ is not rational. (Alternatively we could use the Rational Root Test here. See Exercise 3.)

3. If $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ where each a_i is an integer, and if r/s is a rational root (in lowest terms) then the Rational Root Test implies that $s \mid 1$. Therefore $s = \pm 1$ and $r/s = \pm r$ is an integer.

4. (a) First check that 1 and –1 are not roots. Then the Rational Root Test implies mere are no rational roots, hence no degree 1 factors. If it factors in $\mathbb{Q}[x]$ it must be the product of two irreducible quadratics. As in the example we would then get integers a, b, c, d satisfying $a + c = 2$, $ac + b + d = 0$, $bc + ad = 1$ and $bd = 1$. Therefore $c = -a$ and $b = d = +1$. Eliminating c and d from the third equation yields: $b(2 - a) + ab = 1$ which leads to the adsurdity $2b = 1$. Therefore no factorization is possible.
   (b) Suppose it is reducible. As in (a), ± 1 are not roots so it must factor as a product of two quadratics. This implies there are integers a, b, c, d satisfying $a + c = 0$, $ac + b + d = -2$, $bc + ad = 8$ and $bd = 1$. Then $c = -a$ and $b = d = \pm 1$ so that $8 = b(-a) + ab$, leading to the contradiction $8 = 0$. Therefore no factorization is possible.

5. (a) Let $p – 2$. (b) Let $p = 5$. (c) Let $p = 2$ or 3.

6. Let $k = 3m$ for any integer m not divisible by 3. Then Eisenstein applies with $p = 3$.

7. (a) Answered in the text. (b) Reducing (mod 2) the polynomial becomes $x^4 + x + 1$. This has no root in $\mathbb{Z}_2$ so there is no degree 1 factor. If it factors in $\mathbb{Z}_2[x]$ it must be a product of two irreducible quadratics. But the only irreducible quadratic in $x^2 + x + 1$. Since $(x^2 + x + 1)^2 = x^4 + x^2 + 1$, the given polynomial is irreducible in $\mathbb{Z}_2[x]$.

8. $f(x) = 2x^2 + 3x + 1$ is reducible in $\mathbb{Q}[x]$ since it equals $(2x + 1)(x + 1)$. However $\overline{f}(x) = x + 1$ in $\mathbb{Z}_2[x]$ and this is certainly irreducible. It does not contradict the Theorem since p divides the leading coefficient here.

9. $f(x) = x^2 + 60$ is irreducible in $\mathbb{Q}[x]$ since it has no real root. It reduces (mod n) for $n = 2$, 3, 4, 5 because $\overline{f}(x) = x \cdot x$ in $\mathbb{Z}_n[x]$. For $n = 7$ we have $\overline{f}(x) = x^2 + 4$ in $\mathbb{Z}_7[x]$ which is irreducible since it has no root in $\mathbb{Z}_r$.

10. Given a monic $f(x) \in \mathbb{Z}[x]$ and a factorization $f(x) = g(x)h(x)$ for some $g(x)$, $h(x) \in \mathbb{Z}[x]$ where deg $g(x) = m$ and deg $h(x) = n$. Suppose $g(x) = a_m x^m + \ldots + a_0$ and $h(x) = b_n x^n + \ldots + b_0$. Then $f(x) = {}_m a\, {}_n b\, x^{m+n} + \ldots + a_0 b_0$. Since $f(x)$ is monic we have ${}_m a\, {}_n b = 1$ so that $a_m = b_n = \pm 1$. If $a_m = b_n = 1$ then $g(x)$ and $h(x)$ are monic. Otherwise $a_m = b_n = -1$ and $f(x) = (-g(x))(-h(x))$ is a factorization of the required type.

11. Since $91 = 7{\cdot}13$, apply Eisenstein with $p = 7$ to deduce that $30x^n – 91$ is irreducible in $\mathbb{Q}[x]$. Since $n > 1$ this polynomial has no linear factors, hence no rational roots (see Corollary 4.17).

12. If $f(x)$ is reducible then $f(x) = g(x)h(x)$ forsome $g(x)$, $h(x) \in F[x]$ of degree ≥ 1. We can "evaluate" this equation at any particular value of x: $f(a) = g(a)h(a)$. (Compare Exercise 4.4.31.) Using $a = x + c$ in the ring $F[x]$ we have $f(x + c) = g(x + c)h(x + c)$ in $F[x]$. Therefore $f(x + c)$ is reducible in $F[x]$.

13. $f(x + 1) = (x + 1)^4 + 4(x + 1) + 1 = x^4 + 4x^3 + 6x^2 + 8x + 6$. Eisenstein with $p = 2$ shows that $f(x + 1)$ is irreducible and therefore $f(x)$ is also irreducible in $\mathbb{Q}[x]$.

14. Since $f(x) = (x^5 - 1)/(x - 1)$ we find: $f(x + 1) = ((x + 1)^5 - 1)/x = x^4 + 5x^3 + 10x^2 + 10x + 5$. Eisenstein with $p = 5$ shows that $f(x + 1)$ is irreducible in $\mathbb{Q}[x]$. By Exercise 12 $f(x)$ is also irreducible.

15. Let $f^*(x) = x^n f(x^{-1}) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ as in Exercise 4.4.12. Suppose $f(x) = g(x)h(x)$ is a non-trivial factorization in $F[x]$. Then deg $g(x) = d$ and deg $h(x) = n - d$ where $0 < d < n$. Note that $g^*(x) = x^d g(x^{-1})$ and $h^*(x) = x^{n-d}h(x^{-1})$ arise from $g(x)$ and $h(x)$ respectively by reversing the coefficients. Furthermore $f^*(x) = x^n f(x^{-1}) = x^d g(x^{-1})x^{n-d}h(x^{-1}) = g^*(x)h^*(x)$ in $\mathbb{Z}[x]$. Finally knowing $a_0 \neq 0$, the constant terms of $g(x)$ and $h(x)$ are also non-zero. Therefore deg $f(x) = n$, deg $g(x) = d$ and deg $h(x) = n - d$ and the factorization of $f^*(x)$ is also non-trivial.

    Now for the particular situation in the problem, apply Eisenstein's Criterion to deduce that $f^*(x)$ is irreducible in $\mathbb{Q}[x]$. Since $a_0 \neq 0$, the discussion above shows that $f(x)$ must also be irreducible in $\mathbb{Q}[x]$.

16. One example is $f(x) = x^2 + 1$.

17. Following the answer in the text we see that there are n choices for each coefficient a_0, a_1, . . ., a_{k-1} and there are $n - 1$ choices for a_k (since we require $a_k \neq 0$ to have degree k. Altogether there are $n^k(n - 1)$ possibilities.

18. (a) Irreducible. By the Rational Root Test the only possible rational roots are 1 and –1. Since these are not roots there arc no factors of degree 1. As in the examples, if the polynomial factors in $\mathbb{Q}[x]$ it must be the product of two monic quadratics in $\mathbb{Z}[x]$, say $x^4 - x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$. Then $a + c = 0$, $ac + b + d = -1$, $ad + bc = 0$ and $bd = 1$. Then $c = -a$ and $b = d = \pm 1$, so the second equation becomes $-a^2 + 2b = -1$. Then $a^2 = 2b + 1 = -1$ or 3 (since $b = \pm 1$). This is impossible for an integer a.
    (b) Irreducible. One way to see this is to apply Theorem 4.24, recalling from Exercise 7(b) that $x^4 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.
    (c) Irreducible. One proof uses Theorem 4,24, by showing that $\overline{f}(x)$ in $\mathbb{Z}_3[x]$ is irreducible. Express $\overline{f}(x) = x^5 + x^4 + 2x^3 + 2x + 2$ in $\mathbb{Z}_3[x]$. Evaluation at $x = 0, 1, 2$ shows that there is no root in $\mathbb{Z}_3$ and hence there is no linear factor. If it is reducible it must be a product of two monic irreducibles of degrees 2 and 3. The only monic irreducibles of degree 2 are: $x^2 + 1$, $x^2 + x + 2$ and $x^2 + 2x + 2$ (see Exercise 4.4.9). Dividing each into $\overline{f}(x)$ shows that none is a factor. Hence $\overline{f}(x)$ is irreducible.
    (d) Irreducible. As in (c) check that $\overline{f}(x) = x^5 + 2x^2 + x + 1$ has no root in $\mathbb{Z}_3$, and that the 3 monic irreducibles of degree 2 are not factors. Hence $\overline{f}(x)$ is irreducible in $\mathbb{Z}_3[x]$ and Theorem 4.24 applies.

19. (a) $x^5+2x^4-6x^2-16x-8=(x+2)(x-2)(x^3+2x^2+4x+2)$. Since x^3+2x^2+4x+2 has no rational roots (the only possibilities are 0, ±1, and ±2), it is irreducible over $\mathbb{Q}$.

    (b) $x^7-2x^6-6x^4-15x^2-33x-9=(x+1)(x-3)(x^5+3x^3+9x+3)$. Since x^5+3x^3+9x+3 has no rational roots (the only possibilities are 0, ±1, and ±3), it is irreducible over $\mathbb{Q}$.

20. From Exercise 4.1.17, the map $\varphi\ :\mathbb{Z}[x]\to\mathbb{Z}_n[x]$ where $\varphi\,(f(x))=\overline{f}(x)$ is a surjective homomorphism. Then if $f(x)=g(x)h(x)$ in $\mathbb{Z}[x]$ then applying φ shows that $\overline{f}(x)=\overline{g}(x)$ $\overline{h}(x)\,(x)$ in $\mathbb{Z}_n[x]$.

21. As in the Hint, use the Binomial Theorem (Appendix E) to show that $f(x+1)=((x+1)^p$ $-1)/x=\sum\binom{p}{k}x^{p-1-k}=x^{p-1}+px^{p-2}+\frac{p(p-1)}{2}x^{p-3}+\ldots+p$. By Exercise 1.4.13, $p\mid\begin{pmatrix}p\\k\end{pmatrix}$ for k $=1,\ .\ .\ .\ p-1$, and the constant term is p, which is not divisible by p^2. Eisenstein's Criterion then implies that $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. By Exercise 12, $f(x)$ is also irreducible in $\mathbb{Q}[x]$.

4.6 Irreducibility in $\mathbb{R}[x]$ and $\mathbb{C}[x]$

1. (a) Answered in the text. (b) $1+i,\quad 1-i\quad \sqrt{3}\,,\ -\sqrt{3}$

   (c) Answered in the text.

2. (a) $x^3-8x^2+22x-20$ (b) $x^4-2x^3+6x^2-8x+8$ (c) $x^3-x^2+11x-51$

3. (a) Answered in the text.

   (b) $(x+1)(x^2–x+1)$ in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$; $(x+1)(\,x-\frac{1+\sqrt{3}\cdot i}{2}\,)(\,x-\frac{1-\sqrt{3}\cdot i}{2}\,)$ in $\mathbb{C}[x]$.

   (c) $(x-1)(x^2-5)$ in $\mathbb{Q}[x]$ and $\mathbb{R}[x]$; $(x-1)(x-\sqrt{5}\,)(x+\sqrt{5}\,)$ in $\mathbb{C}[x]$.

4. $(x+i)(x+1-i)$.

5. By Lemma 4.28 the nonreal roots of $f(x)$ occur in pairs, so there is an even number of them. By hypothesis there is no repetition among the roots, so there must be an odd number of real roots.

6. If $x\in\mathbb{C}$ is a root of $f(x)$ then $ax^2+bx^2+c=0$. Since $a\neq 0$ we have $x^2+(b/a)x=-c/a$. Adding $(b/2a)^2$ to both sides we obtain: $(x+b/(2a))^2=b^2/(4a^2)-c/a=(b^2-4ac)/(4a^2)$. Take the square root of both sides to get: $x+b/(2a)=\pm\sqrt{b^2-4ac/}(2a)$. The claim follows.

7. If it factors in $\mathbb{R}[x]$ it is the product of two linear factors so that the two roots $r_1,\ r_2\in\mathbb{C}$ must be real. From the quadratic formula (Exercise 6), $a(r_1-r_2)=\sqrt{b^2-4ac}$. Since this quantity is real, the number under the square root sign must be non-negative: $b^2-4ac\geq 0$. This contradicts the hypothesis, so the polynomial must be irreducible in $\mathbb{R}[x]$.

8. No. In fact if $a + bi$ is a root of that polynomial $f(x) = x^3 - 3x^2 + 2ix + i - 1$ it turns out that $a - bi$ is not a root of $f(x)$. For suppose that $a - bi$ is a root of $f(x)$. Applying the "bar" as in the proof of Lemma 4.28, we find that $a + bi$ is also a root of $\overline{f}(x) = x^3 - 3x^2 - 2ix - i - 1$. But then $a + bi$ is a root of $f(x) - \overline{f}(x) - 4ix + 2i$ forcing $a + bi = -1/2$. Check that $-1/2$ is not a root of $f(x)$ to see that such $a + bi$ cannot exist.

Chapter 5

Congruence in $F[x]$ and Congruence-Class Arithmetic

5.1 Congruence in $F[x]$ and Congruence Classes

1. (a) $f(x) - g(x) = x^5 - 2x^4 + 4x^3 + x + 1 - (3x^4 + 2x^3 - 5x^2 - 9) = x^5 - 5x^4 + 2x^3 + 5x^2 + x + 10$. Using polynomial long division gives $x^5 - 5x^4 + 2x^3 + 5x^2 + x + 10 = (x^2+1)(x^3 - 5x^2 + x + 10)$ with no remainder, so that $f(x) \equiv g(x) \pmod{p(x)}$.

   (b) $f(x) - g(x) = x^4 + x^2 + x + 1 - (x^4 + x^3 + x^2 + 1) = -x^3 + x = x^3 + x$. Using polynomial long division gives $x^3 + x = (x^2 + x)(x + 1)$ with zero remainder (since the product is $x^3 + 2x^2 + x = x^3 + x$ in $\mathbb{Z}_2$), Thus $f(x) \equiv g(x) \pmod{p(x)}$.

   (c) $f(x) - g(x) = (3x^5 + 4x^4 + 5x^3 - 6x^2 + 5x - 7) - (2x^5 + 6x^4 + x^3 + 2x^2 + 2x - 5) = x^5 - 2x^4 + 4x^3 - 8x^2 + 3x - 2$. Using polynomial long division gives $x^5 - 2x^4 + 4x^3 - 8x^2 + 3x - 2 = (x^3 - x^2 + x - 1)(x^2 - x + 2) - 4x^2$. Since the remainder is nonzero, $f(x) \not\equiv g(x) \pmod{p(x)}$.

2. Given $p(x) = c$ for some nonzero $c \in F$. For any $f(x) \in F[x]$ we have $c \mid f(x)$ (since $f(x) = c(c^{-1} f(x)))$. Therefore $f(x) \equiv 0 \pmod{c}$.

3. There are 8 classes. 0, 1; x, $x + 1$; x^2, $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$.

4. By Corollary 5.5 the classes are uniquely represented by the elements $ax^2 + bx + c$ for a, b, $c \in \mathbb{Z}_3$. There are 3 independent choices for a, b, c here, yielding 27 possibilities.

5. As above the classes are uniquely represented by the elements $ax + b$ for a, $b \in \mathbb{Q}$. There are an infinite number of different choices.

6. By Corollary 5.5 the classes are uniquely represented by the elements c, for $c \in F$. In fact, by the Remainder Theorem, for any $f(x) \in F[x]$ we have $f(x) \equiv f(a) \pmod{x - a}$.

7. $f(x) \equiv g(x) \pmod{x}$ if and only if $f(x) - g(x)$ is divisible by x. This happens if and only if $f(x) - g(x)$ has a zero constant term. So $f(x) \equiv g(x) \pmod{x}$ whenever the constant terms in f and g are the same, so that there is one congruence class for each possible constant, i.e., one congruence class per element of F.

8. Proof: Given $p(x)$ divides $f(x)k(x) - g(x)k(x) = (f(x) - g(x))k(x)$ and $p(x)$, $k(x)$ are relatively prime. By Theorem 4.7 conclude that $p(x)$ divides $f(x) - g(x)$ and therefore $f(x) \equiv g(x) \pmod{p(x)}$.

9. Answered in the text.

10. Proof. Given $p(x) \mid f(x)g(x)$. By Theorem 4.11 either $p(x) \mid f(x)$ or $p(x) \mid g(x)$. Therefore, $f(x) \equiv 0_F \pmod{p(x)}$ or $g(x) \equiv 0_F \pmod{p(x)}$.

11. Given a factorization $p(x) = f(x)g(x)$ where $f(x)$, $g(x)$ are polynomials of degrees ≥ 1. By comparing degrees we see that $p(x) \nmid f(x)$ and $p(x) \nmid g(x)$. Therefore $f(x) \not\equiv 0_F \pmod{p(x)}$, $g(x) \not\equiv 0_F \pmod{p(x)}$ and $f(x)g(x) \equiv 0_F \pmod{p(x)}$.

12. Since the gcd is 1 Theorem 4.5 implies that there exist $u(x)$, $v(x) \in F[x]$ with $f(x)u(x) + p(x)v(x) = 1_F$. Then $f(x)u(x) \equiv 1_F \pmod{p(x)}$.

13. $f(x) \equiv g(x) \pmod{x}$ if and only if $x \mid (f(x) - g(x))$. By the Factor Theorem 4.15 this is equivalent to $f(0) = g(0)$. This condition holds when the graphs have the same y-intercept.

5.2 Congruence-Class Arithmetic

1. Answered in the text.

2.

$+$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[1]$	$[1]$	$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$
$[2]$	$[2]$	10]	$[1]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$
$[x]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$
$[x+1]$	$[x+1]$	$[x+2]$	$[x]$	$[2x+1]$	$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$
$[x+2]$	$[x+2]$	$[x]$	$[x+1]$	$[2x+2]$	$[2x]$	$[2x+1]$	$[2]$	$[0]$	$[1]$
$[2x]$	$[2x]$	$[2x+1]$	$[2x+2]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+1]$
$[2x+1]$	$[2x+1]$	$[2x+2]$	$[2x]$	$[1]$	$[2]$	$[0]$	$[x+1]$	$[x+2]$	$[x]$
$[2x+2]$	$[2x+2]$	$[2x]$	$[2x+1]$	$[2]$	$[0]$	$[1]$	$[x+2]$	$[x]$	$[x+1]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[x]$	$[x+1]$	$[x+2]$	$[2x]$	$[2x+1]$	$[2x+2]$
$[2]$	$[0]$	$[2]$	$[1]$	$[2x]$	$[2x+2]$	$[2x+1]$	$[x]$	$[x+2]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[2x]$	$[2]$	$[x+2]$	$[2x+2]$	$[1]$	$[x+1]$	$[2x+1]$
$[x+1]$	$[0]$	$[x+1]$	$[2x+2]$	$[x+2]$	$[2x]$	$[1]$	$[2x+1]$	$[2]$	$[x]$
$[x+2]$	$[0]$	$[x+2]$	$[2x+1]$	$[2x+2]$	$[1]$	$[x]$	$[x+1]$	$[2x]$	$[2]$
$[2x]$	$[0]$	$[2x]$	$[x]$	$[1]$	$[2x+1]$	$[x+1]$	$[2]$	$[2x+2]$	$[x+2]$
$[2x+1]$	$[0]$	$[2x+1]$	$[x+2]$	$[x+1]$	$[2]$	$[2x]$	$[2x+2]$	$[x]$	$[1]$
$[2x+2]$	$[0]$	$[2x+2]$	$[x+1]$	$[2x+1]$	$[x]$	$[2]$	$[x+2]$	$[1]$	$[2x]$

3. Answered in the text.

4. This 25 element ring is too big for us to give the complete tables here. It is not a field since there are zero divisors. For example $[x{+}2]\cdot[x{+}3] = [0]$.

5. $[ax + b] + [cx + d] = [(a + c)x + (b + d)]$

   $[ax + b]\cdot[cx + d] = [(ad + bc)x + (-c + bd)]$

The rules for addition in these exercises are all the same.

6. $[ax + b]\cdot[cx + d] = [(ad + bc)x + (2ac + bd)]$

7. $[ax + b]\cdot[cx + d] = [(ad + bc)x + (3ac + bd)]$

8. $[ax + b]\cdot[cx + d] = [(ad + bc)x + bd]$

9. If $[ax + b] \neq [0]$ then a, b are not both 0 so that $\boldsymbol{\delta} = a^2 + b^2 > 0$. Following the Hint let $c = -a/\boldsymbol{\delta}$ and $d = b/\boldsymbol{\delta}$. Then $[ax + b]\cdot[cx + d] = [(ad + bc)x + (-ac + bd] = [0x + (a^2 + b^2)/\boldsymbol{\delta}] = [1]$.

10. Since $[a] + [b] = [a + b]$ and $[ab] = [a]\cdot[b]$ the subset F^* is closed under addition and multiplication. Also $[0]$ acts as the zero element and $[1]$ acts as the identity element. All the other properties are automatic. (For instance, $[a] + [-a] = [a - a] = [0]$ so that $-[a] = [-a]$.)

11. $[x] \neq [0]$ but $[x]\cdot[x] = [0]$, so $[x]$ is a zero divisor.

12. Given $f - g = pu$ and $h - k = pv$ for some $u, v \in F[x]$. Then $(f + h) - (g + k) = p(u - v)$ and therefore $[f + h] = [g + k]$. Similarly, $fh - gk = (g + pu)\cdot(k + pv) - g\cdot k = p(uk + gv + puv)$. Conclude that $[fh] = [gk]$.

13. The proof that $F[x]/(p(x))$ is a commutative ring with identity is almost identical to the proof of Theorem 2.7. The only difference is a change of notation: write $F[x]$ for $\mathbb{Z}$, $p(x)$ for n, $F[x]/(p(x))$ for $\mathbb{Z}$, and write $a(x)$ for a and $b(x)$ for b, *etc.* For example to prove associativitiy for addition (property 2), use the definition of addition of classes: $[a] \oplus ([b] \oplus [c]) = [a] \oplus [b + c] = [a + (b + c)] = [(a + b) + c] = [a + b] \oplus [c] = ([a] \oplus [b]) \oplus [c]$. The remaining details are omitted.

14. (a) Note that if $f(x) \in \mathbb{Q}[x]$, then on dividing $f(x)$ by x^2-2 we get $f(x) = (x^2-2)g(x)+r(x)$, and $\deg r(x) < \deg(x^2 - 2) = 2$, so that $f(x) \equiv r(x) = ax+b$ for $a, b \in \mathbb{Q}$. Thus any polynomial is congruent to a linear function in $\mathbb{Q}[x]/(x^2 - 2)$. To show that $[f(x)]$ is a unit in $\mathbb{Q}[x]/(x^2 - 2)$ it suffices to show that $f(x)$ is relatively prime to $x^2 - 2$. But $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$, so that indeed $f(x) = 2x - 3$ is relatively prime to $x^2 - 2$ (see Exercise 16 in Section 4.3). Thus by Theorem 5.9, $[f(x)]$ is a unit in $\mathbb{Q}[x]/(x^2 - 2)$. Thus there are $u(x), v(x) \in \mathbb{Q}[x]$ such that $[f(x)][u(x)] = [1] = [1] - [p(x)][v(x)]$, so that $[f(x)][u(x)] + [p(x)][v(x)] = [1]$. Per the above comment, we may assume that $u(x) = ax + b$ and $v(x) = cx + d$. Then we want to solve $(2x - 3)(ax + b) + (x^2 - 2)(cx + d) = 1$ in $\mathbb{Q}[x]$. Expanding gives $cx^3 + (2a + d)x^2 + (-3a + 2b - 2c)x - (3b + 2d) = 1$. Then $c = 2a + d = -3a + 2b - 2c = 0$ and $-3b - 2d = 1$. Solving gives $a = -2$, $b = -3$, and $d = 4$, so that the inverse is $ax + b = -2x - 3$. Indeed $(2x - 3)(-2x - 3) = -4x^2 + 9 = -4(x^2 - 2) + 1$.

(b) Note that $[x^2+x+1]=[x]$, since $x^2+x+1-x=x^2+1$ is divisible by x^2+1. To show that $[x]$ is a unit in $\mathbb{Z}_3[x]/(x^2+1)$ it suffices to show that x is relatively prime to x^2+1 in $\mathbb{Z}_3[x]$. But x^2+1 is irreducible in $\mathbb{Z}_3[x]$ since it has no roots, so that indeed x is relatively prime to x^2+1 (see Exercise 16 in Section 4.3). Thus by Theorem 5.9, $[x]$ is a unit in $\mathbb{Z}_3[x]/(x^2+1)$. Thus there are $u(x), v(x) \in \mathbb{Z}_3[x]$ such that $[x][u(x)]=[1]=[1]-[p(x)][v(x)]$, so that $[x][u(x)]+[p(x)][v(x)]=[1]$. Per the above comment, we may assume that $u(x)=ax+b$ and $v(x)=cx+d$. Then we want to solve $(x)(ax+b)+(x^2+1)(cx+d)=1$ in $\mathbb{Z}_3[x]$. Expanding gives $cx^3+(a+d)x^2+(b+c)x+(b+d)=1$, so that $a=-1$, $b=c=0$, and $d=1$. Thus the inverse is $-x$, and indeed

$$[(x^2+x+1)(-x)]=[-x^3-x^2-x]=[-x(x^2+1)]-[x^2]=-[x^2]=[1].$$

15. Use a new variable T to avoid confusion with x. The polynomial T^2+T has roots 0, 1 and the polynomial T^2+T+1 has roots $[x]$, $[x+1]$. Therefore $T^4+T=(T^2+T)(T^2+T+1)$ has all four roots.

16. By Corollary 5.5 a typical element of this ring $K=\mathbb{Q}[x]/(x^2-2)$ is $[ax+\mathrm{b}]$ where $a, b \in \mathbb{Q}$. Since x^2-2 is irreducible, $ax+b$ and x^2-2 are relatively prime whenever a, b are not both zero. Then by Theorem 5.9, every nonzero element $[ax+b]$ is a unit in K. This shows that K is a field.

5.3 The Structure of $F[x]/(p(x))$ When $p(x)$ is Irreducible

1. (a) Evaluation at $x=0,1,2$ shows that x^3+2x^2+x+1 has no root in $\mathbb{Z}_3$. By Corollary 4.18, that polynomial is irreducible and Theorem 5.10 implies the ring is a field.
   (b) Not a field by Theorem 5.10 since the polynomial is reducible. In fact $2x^3-4x^2+2x+1=2(x+2)(x+3)^2$.
   (c) Not a field since $x^4+x^2+1=(x^2+x+1)^2$.

2. (a) Verifying that $\mathbb{Q}(\sqrt{2})$ is a subring of $\mathbb{R}$ has essentially been done in Exercise 3.1.9. To show it is a subfield we must see that any nonzero element $r+s\sqrt{2}$ has an inverse in $\mathbb{Q}(\sqrt{2})$. Rationalizing the denominator shows that $(r+s\sqrt{2})^{-1}=(r/\delta)-(s/\delta)\sqrt{2}$ where $\delta=r^2-2s^2$. (Note that $\delta\neq 0$ since $\sqrt{2}$ is irrational.) These coefficients are in $\mathbb{Q}$ so the inverse lies in $\mathbb{Q}(\sqrt{2})$.
   (b) By Corollary 5.5 every element of the ring $A=\mathbb{Q}[x]/(x^2-2)$ can be uniquely expressed as $[rx+s]$ for some $r, s\in\mathbb{Q}$. Then the map $\varphi: A\to\mathbb{Q}(\sqrt{2})$ given by $\varphi([r+sx])=r+s\sqrt{2}$ is a well defined bijection. Also $\varphi(r)=[r]$ for $r\in\mathbb{Q}$ and $\varphi([x])=\sqrt{2}$. Finally the calculation in Exercise 5.2.6 implies that this φ is a homomorphism.

3. By Theorem 5.7 we know that $F^* = \{[a] : a \in F\}$ is a subring of $F[x]/(x - a)$ which is isomorphic to F. In fact the map $\varphi : F \to F^*$ defined by $\varphi(a) = [a]$ is an isomorphism. Corollary 5.5 implies that every element of $F[x]/(x - a)$ already lies in F^*. Therefore $(\varphi : F \to F[x]/(x - a)$ is an isomorphism.

4. Restate the problem in terms of congruences: If $f(x)g(x) \equiv 0_F \pmod{p(x)}$ then either $f(x) \equiv 0_F \pmod{p(x)}$ or $g(x) \equiv 0_p \pmod{p(x)}$. This is the content of Exercise 5.1.10.

5. (a) For subtraction: $(a + b\sqrt{3}) - (c + d\sqrt{3}) = (a - c) + (b - d)\sqrt{3}$. For multiplication: $(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (ad + bc)\sqrt{3}$. Therefore $\mathbb{Q}(\sqrt{3})$ is a subring of $\mathbb{R}$. If $a + b\sqrt{3} \neq 0$ then $\delta = a^2 - 3b^2 \neq 0$ in $\mathbb{Q}$ (for if $a^2 = 3b^2$ for positive $a, b \in \mathbb{Q}$ then $\sqrt{3} = a/b$ would be rational). Since $(a + b\sqrt{3})(a - b\sqrt{3}) = \delta$ it follows that $(a + b\sqrt{3})^{-1} = (a/\delta) - (b/\delta)\sqrt{3} \in \mathbb{Q}(\sqrt{3})$. Hence it is a field.

   (b) As in Exercise 2(b) the map $\varphi : (\mathbb{Q}[x]/(x^2 - 3) \to \mathbb{Q}(\sqrt{3})$ given by $\varphi([r + sx]) = r + s\sqrt{3}$ is a well defined bijection, with $\varphi(r) = [r]$ for $r \in \mathbb{Q}$ and $\varphi([x]) = \sqrt{3}$. The proof that φ is a homomorphism reduces to verifying that $[a + bx]\cdot[c + dx] = [(ac + 3bd) + (ad + bc)x]$ in $\mathbb{Q}[x]/(x^2 - 3)$.

6. The assertion follows since $F[x]/(p(x))$ is a field (Theorem 5.9). Set $[g(x)] = [f(x)]^{-1}[h(x)]$.

7. By Corollary 5.11 there is an extension field K_1 of F which contains some root c_1 of $f(x)$. Then the Factor Theorem implies that $f(x) = (x - c_1)f_1(x)$ for some $f_1(x) \in K_1[x]$ of degree $n - 1$. If $n > 1$ repeat the process to find an extension K_2 of K_1 containing some root c_2 of $f_1(x)$. Then $f(x) = (x - c_1)(x - c_2)f_2(x)$ for some $f_2(x) \in K_2[x]$ of degree $n - 2$. Continue the process, finding extensions $K_2 \subseteq K_3 \subseteq \dots \subseteq K_n$ where $f(x) = (x - c_1)(x - c_2) \subseteq \dots (x - c_n)f_n(x)$ where $\deg f_n(x) = 0$. But then $f_n(x) = c_0$ is a nonzero constant. Let $E = K_n$ to get the result.

8. By Theorem 5.10 we know that $K = F[x]/(p(x))$ is a field containing F and that there exists $\alpha \in K$ which is a root of $p(x)$. The Factor Theorem implies that $p(x) = (x - \alpha)q(x)$ for some $q(x) \in K[x]$. Compare degrees to find $\deg q(x) = 1$. Factoring out the leading coefficient $\beta \in K$ of $q(x)$ we get $q(x) = \beta(x - \gamma)$ for some $\gamma \in K$. Then $p(x) = \beta(x - \alpha)(x - \gamma)$ and both roots α, γ lie in K.

9. (a) By Corollary 4.18, $x^3 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$, since neither 0 nor 1 is a root. By Theorem 5.10 the ring $K = \mathbb{Z}_2[x]/(x^3 + x + 1)$ is a field.

   (b) As in Theorem 5.11 we know that $\alpha = [x] \in K$ is a root of $x^3 + x + 1$. That is $\alpha^3 = \alpha + 1$. (Recall that $-1 = 1$ in K.) Dividing by $(x + \alpha)$ we find that $x^3 + x + 1 = (x + \alpha)(x^2 + \alpha x + (\alpha^2 + 1))$. This quadratic quotient can be factored (by inspection) in K to yield $x^3 + x + 1 = (x + \alpha)(x + \alpha^2)(x + \alpha^2 + \alpha)$.

   Therefore the three roots α, α^2 and $\alpha^2 + \alpha$ all lie in K.

10. By Exercises 2 and 5, if these fields were isomorphic there would be an isomorphism φ : $\mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$. Since $\varphi(1) = 1$ we find that $\alpha(n) = n$ for every positive integer n (since $n = 1 + 1 + . . . + 1$). (In fact, $\varphi(r) = r$ for every $r \in \mathbb{Q}$.) Suppose $\varphi(\sqrt{2}) = a + b\sqrt{3}$ for some a, $b \in \mathbb{Q}$. Then $2 = \varphi(2) = \varphi(\sqrt{2})^2 = (a + b\sqrt{3})^2 = (a^2 - 3b^2) + (2ab)\sqrt{3}$. Therefore $a^2 - 3b^2 = 2$ and $2ab = 0$, so either $a = 0$ or $b = 0$. If $a = 0$ then $b = -2/3$, which is impossible for $b \in \mathbb{Q}$. If $b = 0$ then $a^2 = 2$, also impossible in $\mathbb{Q}$. Therefore no such isomorphism can exist.

11. If u were a root in K then $3u^2 +1 = 0$. Since $6 = 0$ in K, multiplying by 2 shows: $2 = 2(3u^2 + 1) = 0$ in K, contrary to the hypothesis that $\mathbb{Z}_6$ is a subring. Consequently there is no commutative ring containing $\mathbb{Z}_6$ and containing a root of $3x^2 + 1$. This shows that Corollary 5.12 requires the hypothesis that F is a field.

12. If u were a root in K then $2u^3 + 4u^2 + 8u + 3 = 0$. Since $16 = 0$ in K we obtain $8 = 24 = 8(2u^3 + 4u^2 + 8u + 3) = 0$ in K contradicting the hypothesis that $\mathbb{Z}_{16}$ is a subring.

13. Let $K = \mathbb{Z}_2[x]/(x^4 + x + 1)$ with $\alpha = [x] \in K$. Then $\alpha^4 = \alpha + 1$. It is useful to compute a table of the powers of α:

$\alpha^4 = \alpha + 1$	$\alpha^5 = \alpha^2 + \alpha$	$\alpha^6 = \alpha^3 + \alpha^2$	$\alpha^7 = \alpha^3 + \alpha + 1$
$\alpha^8 = \alpha^2 + 1$	$\alpha^9 = \alpha^3 + \alpha$	$\alpha^{10} = \alpha^2 + \alpha + 1$	$\alpha^{11} = \alpha^3 + \alpha^2 + \alpha$
$\alpha^{12} = \alpha^3 + \alpha^2 + \alpha + 1$	$\alpha^{13} = \alpha^3 + \alpha + 1$	$\alpha^{14} = \alpha^3 + 1$	$\alpha^{15} = 1$

It is enough to consider irreducible polynomials. The irreducibles of degree 1 are x, $x + 1$ and these have roots already in $\mathbb{Z}_2$. The only irreducible of degree 2 is $x^2 + x + 1$. It turns out that $\beta = \alpha^2 + \alpha$ is a root, as we verify directly: $\beta^2 + \beta + 1 = (\alpha^2 + \alpha)^2 + (\alpha^2 + \alpha) + 1 = \alpha^4 + \alpha + 1 = 0$.

The irreducibles of degree 4 are $x^4 + x + 1$, $x^4 + x^3 + 1$ and $x^4 + x^3 + x^2 + x + 1$. The first polynomial has α itself as a root, by construction.

Let $\delta = \alpha^{14} = \alpha^3 + 1$. Then δ is a root of $x^4 + x^3 + 1$, because: $\delta^4 + \delta^3 + 1 = \alpha^{56} + \alpha^{42} + 1 = \alpha^{11} + \alpha^{12} + 1 = (\alpha^3 + \alpha^2 + \alpha) + (\alpha^3 + \alpha^2 + \alpha + 1) + 1 = 0$.

Let $\gamma = \alpha^3$. Then γ is a root of $x^4 + x^3 + x^2 + x + 1$ as we verify similarly: $\gamma^4 + \gamma^3 + \gamma^2 + \gamma + 1 = \alpha^{12} + \alpha^9 + \alpha^6 + \alpha^3 + 1 = (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha) + (\alpha^3 + \alpha^2) + (\alpha^3) + 1 = 0$.
In fact each of the 16 elements of K is a root of one of these polynomials of degree 1, 2 or 4.

Chapter 6

Ideals and Quotient Rings

6.1 Ideals and Congruence

1. The subset K is certainly closed under subtraction and multiplication, so it is a subring. However K is not an ideal since it does not "absorb" products. For instance $1 \in K$ and $x \in \mathbb{Z}[x]$ but $x \cdot 1 = x$ is not in K.

2. If $f(x) \in \mathbb{Z}[x]$ then $f(x)$ lies in I if and only if $f(0)$ is even. If $f(x)$, $g(x) \in I$ then $(f - g)(0) = f(0) - g(0)$ is the sum of two even numbers, so it is even. Therefore $f(x) - g(x) \in I$. If $f(x) \in I$ and $r(x) \in \mathbb{Z}[x]$ then $(r \cdot f)(0) = r(0)f(0)$ is even since $f(0)$ is even. Therefore $r(x)f(x) \in I$. By Theorem 6.1 I is an ideal.

3. (a) $(k, 0) - (j, 0) = (k - j, 0) \in I$ and $(r, s) \cdot (k, 0) = (rk, 0) \in I$ for every $k, j, r, s \in \mathbb{Z}$. Therefore I is an ideal.
   (b) For example $(1, 1) \in T$ and $(1, 0) \in \mathbb{Z} \times \mathbb{Z}$ but $(1, 1)\cdot(1, 0) = (1, 0) \notin T$.

4. No. For example $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ so the set J does not absorb products.

5. It is easy to check that K is closed under subtraction, and since $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bw \\ 0 & 0 \end{pmatrix}$, K absorbs products from the right. In particular K is closed under multiplication (this is the case $z = w = 0$), and therefore K is a subring. However K does not absorb all products from the left. For example, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

6. (a) The set of nonunits, $J = \{0, 2, 4, 6\} = (2)$ is a principal ideal in $\mathbb{Z}_8$.
   (b) $J = \{0, 3, 6\} = (3)$ is a principal ideal in $\mathbb{Z}_9$.

7. (a) The proof of Theorem 6.2 did not use the hypothesis that R possesses an identity element.

   (b) No, c need not be in I. As in the Hint, let $I = \{2k \mid k \in E\}$ where E is the ring of even integers. Then every element $x \in I$ is a multiple of 4 in $\mathbb{Z}$ because $x = 2k$ and k is even. In particular, $2 \notin I$.

   (c) Let $c = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ in $M(\mathbb{R})$. Then $I = \{rc \mid r \in \mathrm{M}(\mathbb{R})\}$ consists of all matrices of the form $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & 0 \\ c & 0 \end{pmatrix}$. This is the example given before Theorem 6.1. This I is not an ideal, but it is a left ideal.

8. First note that $I \times J$ is nonempty since it contains $(0_R, 0_S)$. As in Theorem 6.1, suppose (a, b) and (a', b') are in $I \times J$. Then $(a, b) - (a', b') = (a - \mathrm{a}', b - b')$ lies in $I \times J$, since I and J are ideals. Similarly if $(a, b) \in I \times J$ and $(r, s) \in R \times S$ then $(r, s)\cdot(a, b) = (ra, sb)$ and $(a, b)\cdot(r, s) = (ar, bs)$ both lie in $R \times S$.

9. (a) Answered in the text.
   (b) Suppose $u \in I$ where u is a unit. Then $u^{-1} \in R$ and $1_R = u^{-1}u \in I$. By part (a) $I = R$.

10. If $I \neq (0_F)$ there exists $a \in I$ with $\mathrm{a} \neq 0_F$. Since F is a field this element a must be a unit. By Exercise 13, $I = F$.

11. (a) Answered in the text.
    (b) $(0) = \{0\}$; $(1) = (2) = (4) = (5) = (7) = (8) = \mathbb{Z}_9$; $(3) = (6) = \{0, 3, 6\}$.
    (c) Answered in the text.

12. The list of candidates is the ideals generated by $(0,0)$, $(1,0)$, $(0,1)$, $(1,1)$, $(0,2)$, and $(1,2)$. Clearly $(0,0)$ is the zero ideal, consisting of $(0,0)$ alone. Now, $((1,0)) = \{(1,0),(0,0)\}$, and $((0,1)) = \{(0,1),(0,2),(0,0)\} = ((0,2))$. The ideal $((1,1))$ is equal to $\mathbb{Z}_2 \times \mathbb{Z}_3$, since $(1,1)(a,b) = (a,b) \in ((1,1))$ since $((1,1))$ is an ideal. Finally, $((1,2)) = \mathbb{Z}_2 \times \mathbb{Z}_3$ as well, since $(1,2)(1,2) = (1,1)$ and $((1,1)) = \mathbb{Z}_2 \times \mathbb{Z}_3$. Thus the distinct principal ideals are

$$\{(0,0)\}, \qquad \{(0,0),\ (1,0)\}, \qquad \{(0,0),\ (0,1),\ (0,2)\}, \quad \text{and} \quad \mathbb{Z}_2 \times \mathbb{Z}_3.$$

13. No. For example, let $R = \mathbb{Z}$ and let $a = -2$ and $b = 2$. Then $(-2) = (2)$, but $-2 \neq 2$.

14. As in Theorem 6.1, suppose a, $b \in I$ and $r \in R$. To show: $a + b$ and ra lie in I. (The condition on ar is automatic by commutativity.) By hypothesis there exists expressions $a = s_1c_1 + \cdots\ s_nc_n$ and $b = t_1c_1 + \ldots\ t_nc_n$ for some $s_1, \ldots, s_n$ and $t_1, \ldots\ t_n \in R$. By the usual associative, commutative and distributive laws, deduce that $a + b = (s_1 + t_1)c_1 + \cdots + (s_n + t_n)c_n$ and that $ra = (r\mathrm{s}_1)c_1 + \cdots + (r\mathrm{s}_n)cn$. Since every $s_j + t_j$ and rs_j lie in R, conclude that $a + b \in I$ and $ra \in I$.

15. Let J be the ideal in $\mathbb{Z}[x]$ generated by 2 and x. If $g(x) \in J$ then $g(x) = r(x)\cdot 2 + s(x)\cdot x$ for some $r(x)$, $\mathrm{s}(x) \in \mathbb{Z}[x]$. Since $g(0) = r(0)\cdot 2 + 0$ is an even integer, conclude that $g(x)$ lies in the ideal I. Conversely suppose $h(x) \in I$, so that $h(x) = a_0 + a_1x + a_2x^2 + \cdots$ has even constant term. That is $a_0 = 2b$ for some $b \in \mathbb{Z}$ and $h(x) = b\cdot 2 + (a_1 + a_2x + a_3x^2 + \cdots)\cdot x$ lies in J. Hence $I = J$.

16. (a) (2) = (–2). (b) Let R be a commutative ring. As mentioned after Theorem 6.3, let $(c_1, c_2,..., c_n)$ denote the ideal generated by $c_1, \ldots, c_n$ in R.

Lemma. If J is an ideal of R and $c_1, \ldots, c_n \in J$ then $(c_1, \ldots, c_n) \subseteq J$.

Proof. If $a \in (c_1, \ldots, c_n)$ then $a = r_1c_1 + \cdots + r_nc_n$. By the definition of ideals, each $r_ic_i \in J$ and the sum a lies in J. QED

In $\mathbb{Z}$ we know that 4, 6 $\in$ (2) so that (4, 6) $\subseteq$ (2). Also, $2 = (-1)\cdot 4 + 1\cdot 6 \in (4, 6)$ so that (2) $\subseteq$ (4, 6).

This prove the equality.

(c) Since 6, 9, 15 are multiples of 3 we know that 6, 9, 15 $\in$ (3) so that (6, 9, 15) $\subseteq$ (3), by the Lemma above. Similarly, $3 = (-1)\cdot 6 + 1\cdot 9 + 0\cdot 15 \in (6, 9, 15)$ so that (3) $\subseteq$ (6, 9, 15). This proves the equality. Compare Exercise 19.

17. (a) If $a, b \in I \cap J$ then $a, b \in I$, so that $a - b \in I$. Similarly $a, b \in J$ so that $a - b \in J$. Therefore $a - b \in I \cap J$.

If $a \in I \cap J$ and $r \in R$ then $a \in I$ so that $ra, ar \in I$ and $a \in J$ so that $ra, ar \in J$. Therefore $ra, ar \in I \cap J$. Finally $0_R \in I \cap J$ so this set is not empty.

(b) Let J be the intersection of the family of ideals I_k. If $a, b \in J$ then $a, b \in I_k$ and $a - b \in I_k$, for every ideal in the family. Then $a - b \in J$, since J is the intersection. Similarly let $a \in J$ and $r \in R$. Then $a \in I_k$ so that $ra, ar \in I_k$ for every ideal in the family. Then $ra, ar \in J$ since J is the intersection. Also J is not empty since $0_R \in I_k$.

18. Let $I = (2)$ and $J = (3)$. Then $I \cup J = \{n \in \mathbb{Z} \mid \text{either } 2 \mid n \text{ or } 3 \mid n\}$. This set is not closed under addition: $2, 3 \in I \cup J$ but $5 \notin I \cup J$.

19. If $a, b \in I \cap S$ then $a - b \in I$ since it is an ideal and a $- b \in S$ since it is a subring. Therefore $a - b \in I \cap S$. If $a \in I \cap S$ and $s \in S$ men sa and as lie in I since I is an ideal in R and they lie in S since S is closed under multiplication. Hence $sa, as \in I \cap S$. Since $0_R \in I \cap S$ we know it is nonempty. Therefore $I \cap S$ is an ideal in S.

20. If $a, a' \in I$ and $b, b' \in J$ then $(a + b) - (a' + b') = (a - a') + (b - b')$ lies in K. Similarly if $a \in I$, $b \in J$ and $r \in R$ then $r(a + b) = ra + rb$ and $(a + b)r = ar + br$ lie in K. Since $0_R \in J$ conclude that $I = I + 0_R \subseteq K$ and similarly $J \subseteq K$. In particular K is nonempty and therefore K is an ideal. (It is the smallest ideal containing both I and J.)

21. Since $d \mid a$ and $d \mid b$ we have $a, b \in (d)$ so that $(a) + (b) = (a, b) \subseteq (d)$. (See the Lemma in Exercise 12 above.) Conversely by Theorem 1.3 there exist $u, v \in \mathbb{Z}$ such that $d = au + bv$. This says that $d \in (a, b)$ so that $(d) \subseteq (a, b)$ and equality follows.

22. The set K is not necessarily an ideal. There should be a counterexample when R is a commutative ring with 1. If $I = (c)$ is principal then $K = \{(rc)b \mid r \in R \text{ and } c \in J)$ does turn out to be an ideal. For a counterexample we need I, J to be non-principal. Let $I = J = (2, x)$ in $R = \mathbb{Z}[x]$. Then K contains $4 = 2\cdot 2$ and $x^2 = x\cdot x$ but $4 + x^2$ is not in K (it is irreducible in $\mathbb{Z}[x]$).

23. (a) $I = (3)$ is a principal ideal. The cosets are $I = \{0, 3\}$, $1 + I = \{1, 4\}$ and $2 + I = \{2, 5\}$.

(b) $I = (3)$ is a principal ideal. The cosets are $I = \{0, 3, 6, 9, 12\}$, $1 + I = \{1, 4, 7, 10, 13\}$ and $2 + I = \{2, 5, 8, 11, 14\}$.

24. If $R = \mathbb{Z}_6$ the nonunits are $\{0, 2, 3, 4\}$, which is not closed under addition.

25. Certainly $0_R \in I$ so I is not empty. If $r, s \in I$ then for every $t \in J$ we have $rt = st = 0_R$. Therefore $(r - s)t = rt - st = 0_R$ and hence $r - s \in I$. Suppose $r \in I$ and $x \in R$. Then $(xr)t = x(rt) = x{\cdot}0_R = 0_R$ so that $xr \in I$. Also $(rx)t = r(xt) = 0_R$ since $xt \in J$. Therefore $rx \in I$ as well, and I is an ideal.

26. Certainly $0_R \in K$ so K is not empty. If $a, b \in K$ and $r \in R$ then $ra, rb \in I$. Hence $r(a - b) = ra - rb \in I$, and $a - b \in K$. Also if $x \in R$ then $r(xa) = (rx)a \in I$ and $r(ax) = (ra)x \in Ix \subseteq I$. Therefore $xa, ax \in K$ and K is an ideal.

27. Following the answers in the text, we suppose $r \in R$ and $a \in K$. Then $f(a) = 0_S$ by hypothesis so that $f(ra) = f(r)f(a) = f(r){\cdot}0_S = 0_S$. Therefore $ra \in K$ and K is an ideal.

28. Since polynomials add term-by-term, if $f(x), g(x) \in I[x]$ then $f(x) - g(x) \in I[\mathrm{x}]$. If $r(x) = \sum a_j x^j \in R[x]$ and $f(x) \in \sum m_j x^j \in I[x]$ then the coefficient of x^n in $r(x)f(x)$ equals $a_0 m_n + a_1 m_{n-1} + \cdots + a_n m_0$. This lies in I since each $m_i \in I$. Therefore $r(x)f(x) \in I[x]$. Hence $I[x]$ is an ideal.

29. Answered in the text.

30. By Exercise 3.2.36 the set N of nilpotent elements of R is a subring. If $n \in N$ and $r \in R$ then $n^k = 0_R$ for some positive integer k. Therefore $(rn)^k = r^k n^k = 0_R$ and $rn \in N$. Hence N is an ideal.

31. ($\Rightarrow$) Answered in the text.
($\Leftarrow$) Suppose $a = bu$ where u is a unit. For any $r \in R$ we have $ra = (ru)b \in (b)$. Therefore (a) $\subseteq$ (b). Since $b = au^{-1}$ the same argument provides the reverse inclusion.

32. (a) $f(x) \in J$ if and only if $f(0)$ is a multiple of 3 in $\mathbb{Z}$, or equivalently: $f(0) \in (3)$. If $f(x), g(x) \in J$ then $(f - g)(0) = f(0) - g(0) \in (3)$ and hence $f(x) - g(x) \in J$. Also if $f(x) \in J$ and $r(x) \in \mathbb{Z}[x]$ then $(r \cdot f)(0) = r(0)f(0) \in (3)$ as well so that $r(x)f(x) \in J$. Hence J is an ideal.
(b) Suppose $J = (h(x))$ is principal. Then $3 \in J$ implies that $3 = h(x)q(x)$ for some $q(x) \in \mathbb{Z}[x]$. Then deg $h(x) = 0$ so that $h(x) = c$ is a nonzero constant. Also $x \in J$ so that $x = c{\cdot}r(x)$ for some $r(x) \in \mathbb{Z}[x]$. Comparing the leading coefficients shows that $c = \pm 1$. But then $1 = \pm\, c \in J$ so that $J = \mathbb{Z}[x]$ by Exercise 13. This contradiction shows that J is not principal.

33. If $r, s \in R$ and $n, m \in \mathbb{Z}$ then $(ra + na) - (sa + ma) = (r - s)\mathrm{a} + (n - m)a$ lies in A. If $x, r \in R$ and $n \in \mathbb{Z}$ then $x\ (ra + na) = (xr + nx)a \in A$. Also $a = 0_R{\cdot}a + 1{\cdot}a$ lies in A. Hence A is an ideal containing a.
If J is an ideal with $a \in J$ then J absorbs products, so $ra \in J$ for every $r \in$ R. If $n \in \mathbb{Z}$ and $n > 0$ then $na = a + a + \cdots + a \in J$ since J is closed under addition. Also $(-n)a = -(na) = 0_R - na \in J$ since J is closed under subtraction. Therefore $A \subseteq J$.

34. Certainly $M \subset J$ and $M \neq J$. If $m, m' \in M$ and $r, r' \in R$ then $(m + ra) - (m' + r'a) = (m - m') + (r - r')a \in J$. If $m \in M$, $r, x \in R$ then $x(m + ra) = xm + xra \in J$. Therefore J is an ideal.

35. If $I \neq (3)$ there exists $b \in I$ with $b \notin (3)$. Then $3 \nmid$ b and since 3 is prime, $(b, 3) = 1$. Then there exist $x, y \in \mathbb{Z}$ with $1 = 3x + by \in I$. By Exercise 13 we conclude $I = \mathbb{Z}$.

36. By definition IJ is closed under addition (a finite sum plus a finite sum is another finite sum). If $a \in I$ and $b \in J$ then $-(ab) = (-a)b$ lies in IJ. Therefore IJ is closed under taking negatives, so it is closed under subtraction. If $a \in I$, $b \in J$ and $r \in R$ then $r(ab) = (ra)b$ and $(ab)r = a(br)$ both lie in IJ. Therefore (using the distributive law) IJ absorbs products. Clearly $0_R \in IJ$ so it is not empty. Hence it is an ideal.

37. Suppose $a \neq 0_R$. Then the ideal (a) contains $a = I_R \cdot a$, so that $(a) \neq (0_R)$. Therefore $(a) = R$ so that $1_R \in (a)$. This means that $1_R = ra$ for some $r \in R$ and therefore a is a unit. Since every nonzero element is a unit, R is a field.

38. Suppose $a \in J$ and $x \in R$. Then $a^n \in I$ for some positive integer n, and $(xa)^n = x^n a^n \in I$ since I is an ideal. Hence $xa \in J$. Now suppose $a, b \in J$ so that $a^m, b^n \in I$ for some positive integers m, n. Then (as in Exercise 3.2.36) $(a + b)^{m+n-1}$ equals a sum of terms of the type $C \cdot a^r \cdot b^s$ where $C > 0$ is a binomial coefficient, and $r, s \geq 0$ with $r + s = m + n - 1$. Then either $r \geq m$ or $s \geq n$ (for otherwise $r \leq m - 1$ and $s \leq n - 1$ so that $r + s \leq m + n - 2$ which is false). Therefore either $a^r \in I$ or $b^s \in I$, so that each term of this sum lies in I. Therefore $a + b \in J$. This proves that J is an ideal.

39. (a) $c = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ has no inverse in $M(\mathbb{R})$. (There is no matrix a with $ac = 1$, as seen in Exercise 9.)

(b) Suppose $J \neq (0)$ is an ideal. Consider the special matrices $E_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $E_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $E_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ and $E_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Note that $E_{12} = E_{11}E_{12}$, $E_{21} = E_{21}E_{11}$, and $E_{22} = E_{21}E_{11}E_{12}$.

Then if $E_{11} \in J$, all these special matrices lie in J and hence every matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = aE_{11} + bE_{12} + cE_{21} + dE_{22}$ lies in J. In that case, $J = M(\mathbb{R})$.

Suppose $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in J$ is a nonzero element. Note that

$$aE_{11} = E_{11}ME_{11} \qquad bE_{11} = E_{11}ME_{21}$$
$$cE_{11} = E_{12}ME_{11} \qquad dE_{11} = E_{12}ME_{21}$$

Since at least one of a, b, c, d must be nonzero, one of these equations implies that E_{11} lies in the ideal J. The preceding paragraph then applies.

40. If $I \neq (0)$ then these exist positive elements in I (if $r \in I$ men $-r \in I$). By the Well Ordering Axiom there is a smallest positive element $c \in 1$. Then certainly $(c) \subseteq I$. If $a \in I$, the division algorithm implies that $a = cq + r$ for some $q, r \in \mathbb{Z}$ where $0 \leq r < c$. Then $r = a - cq \in I$ and the minimality of c implies that r cannot be positive. Therefore $r = 0$ and $a = cq \in (c)$. Therefore $I \subseteq (c)$ and we do have $I = (c)$.

41. (a) Suppose a/s, $b/t \in S$ where s, t are odd. Then $a/s - b/t = (at - bs)/st$ and $(a/s)(b/t) = (ab)/(st)$ have odd denominators so they also let in S. Therefore S is a subring.
    (b) Suppose a/s, $b/t \in I$ where a, b are even and s, t are odd. Since $at - bs$ is even and st is odd we see that $a/s - b/t \in I$. For any c/u in S we see that ac is even and su is odd so that $(a/s)(c/u) \in I$. Hence I is an ideal in S.
    (c) Let $a/s \in S$. If a is even then $a/s \in I$. Otherwise a is odd so that $a - s$ is even and $(a/s) - 1 = (a - s)/s \in I$. Then $a/s \in 1 + I$.

42. (a) Suppose a/s, $b/t \in T$ where s, t are not divisible by p. Then $a/s - b/t = (at - bs)/st$ and $(a/s)(b/t) = (ab)/(st)$ have denominator st which is not divisible by p (by Theorem 1.8). Then these quantities lie in T so that T is a subring.
    (b) Suppose a/s, $b/t \in I$ where a, b are multiples of p and s, t are not divisible by p. Since $at - bs$ is a multiple of p and st is not, we see that $a/s - b/t \in I$. For any c/u in T we see that ac is a multiple of p and su is not, so that $(a/s)(c/u) \in I$. Hence I is an ideal in T.
    (c) Let $a/s \in T$. Since s and p are relatively prime there exists $x \in \mathbb{Z}$ with $0 \le x < p$ satisfying $sx \equiv a \pmod{p}$. Then $(a/s) - x = (a - sx)/s \in I$, and $a/s \in x + I$ for this value of x. Therefore the only cosets are $I, 1 + I, 2 + I, \cdots, (p - 1) + I$.

    Finally to show those cosets are distinct suppose two of them coincide; $n + I = m + I$ for some $0 \le n < m < p$. Then $k = m - n$ lies in I and $0 < k < p$. This implies that $k = a/s$ where $p \mid a$ and $p \nmid s$. But then $a = ks$ and Theorem 1.8 implies $p \nmid k$. This contradiction shows that there are p cosets.

43. (a) If $f(x) = xg(x)$ for some $g(x) \in \mathbb{Z}[x]$ then $f(0) = 0$ so that $f(x) \in J$. Conversely, if $f(x) \in J$ then $f(0) = 0$ and the Factor Theorem 4.15 implies that $x \mid f(x)$ so that $f(x) \in (x)$.
    (b) Answered in the text.

44. (*a*) $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix} = \begin{pmatrix} a - a' & b - b' \\ 0 & a - a' \end{pmatrix}$ so T is closed under subtraction, $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ 0 & a' \end{pmatrix} = \begin{pmatrix} aa' & ab' + ba' \\ 0 & aa' \end{pmatrix}$ so T is closed under multiplication and it also follows that T is commutative. Therefore T is a subring.

    (b) It is easy to see I is closed under subtraction. Also $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \cdot \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ax \\ 0 & 0 \end{pmatrix}$ so that I is an ideal. Note that the product of any two elements of I equals 0_T.

    (c) For any a, $b \in \mathbb{R}$ we easily see that $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \equiv \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ (mod I). Therefore each coset of I equals $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + I$ for some $a \in \mathbb{R}$.

45. (a) $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} - \begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} a-a' & b-b' \\ 0 & c-c' \end{pmatrix}$ and $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bc' \\ 0 & cc' \end{pmatrix}$ so that S is a subring.

(b) I is closed under addition and we see that $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & ax \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = \begin{pmatrix} 0 & xc \\ 0 & 0 \end{pmatrix}$. Therefore I is an ideal in S.

(c) Certainly $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \equiv \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$ (mod I), so that any coset of I equals $\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} + I$ for some pair $(a, c) \in \mathbb{R} \times \mathbb{R}$. To show these cosets are all distinct it suffices to note that if $\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \in I$ then $(a, c) = (0, 0)$. This statement is clear from the definition of I.

46. Suppose $I \neq (0)$. Then there exist nonzero elements in I and the Well Ordering *Ax*iom implies that there exists some $p(x) \in I$ of smallest degree. Certainly $(p(x)) \subseteq I$. Conversely suppose $f(x) \in I$. The division algorithm implies that $f(x) = p(x)q(x) + r(x)$ for some $q(x)$, $r(x) \in F[x]$ where either $r(x) = 0_F$ or deg $r(x) <$ deg $p(x)$. Since $f(x)$, $p(x) \in I$ we know $r(x) \in I$. If $r(x) \neq 0_F$ this contradicts the minimality of deg $p(x)$. Therefore $r(x) = 0_F$ and $f(x) \in (p(x))$. Hence $I \subseteq (p(x))$. Consequently, $I = (p(x))$ is principal.

47. ($\Rightarrow$) Let u be the identity element of S. The ideal (u) in $\mathbb{Z}_n$ equals $\{0, u, 2u, 3u, \cdots, (n-1)u\}$. Since S is closed under addition all these elements lie in S. Conversely if $s \in S$ we have $s = us \in (u)$. Hence $S \subseteq (u)$ so that $S = (u)$. The condition $u^2 = u$ is clear since u is the identity element.

($\Leftarrow$) If $S = (u)$ is an ideal then certainly S is a subring. Every $s \in S$ can be written $s = ru$ for some $r \in \mathbb{Z}_n$. Then $su = (ru)u = ru^2 = ru = s$ so that u acts as the identity element of S.

6.2 Quotient Rings and Homomorphisms

1. Here $\theta(f(x)) = f(0)$ so θ is an "evaluation homomorphism" as considered in Exercise 4.4.24.

2. If $\varphi : F \to R$ is a surjective homomorphism then the kernel is an ideal of F. By Exercise 6.1.14 this ideal is either (0) or F. If it is F then φ carries every element to 0_R so that $R = \{0_R\}$ is the zero ring.
Otherwise the kernel is (0) and φ is injective, by Theorem 6.11. Hence φ is an isomorphism.

3. Answered in the text.

4. (a) If $[a]_{12} = [b]_{12}$ then $a = b + 12k$ for some integer k. Therefore $[a]_4 = [b]_4$. Also $f([a]_{12} + [b]_{12}) = f([a+b]_{12}) = [a+b]_4 = [a]_4 + [b]_4 = f([a]_{12}) + f([b]_{12})$. Products work similarly. For any $n \in \mathbb{Z}$, $[n]_4 = f([n]_{12})$ so f is a surjective homomorphism.
(b) The kernel equals $([4]_{12}) = \{[0]_{12}, [4]_{12}, [8]_{12}\}$.

5. Answered in the text. $\mathbb{Z}_6$ is not an integral domain.

6. $\ker\varphi$ is the set of elements $f(x) \in \mathbb{R}[x]$ such that $f(2) = 0$, i.e., polynomials with 2 as a root. By Theorem 4.16, this means that $x - 2$ is a factor of $f(x)$. Thus $\ker\varphi$ is the set of polynomials that are multiples of $x - 2$; that is, $\ker\varphi = (x - 2)$, the ideal generated by $x - 2$.

7. The identity map $\tau\colon R \to R$ has kernel (0_R). The First Isomorphism Theorem implies that $R/(0_R) \cong R$.

8. First check that $\pi((r, s) + (r', s')) = \pi(r + r', s + s') = r + r' = \pi(r, s) + \pi(r', s')$ and similarly for products, so π is a homomorphism. It is surjective since $r = \pi(r, 0_S)$. The kernel K equals $\{(0_R, s) \mid s \in S\}$. The map $\rho : K \to S$ defined by $\rho(0_R, s) = s$ shows that $K \cong S$.

9. (a) For subtraction: $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} - \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} a-a' & 0 \\ b-b' & c-c' \end{pmatrix}$. For multiplication: $\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}\begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ba'+cb' & cc' \end{pmatrix}$. Therefore R is a subring of $\mathrm{M}(\mathbb{Z})$ and R contains the identity matrix.

   (b) The map f is surjective since for every $a \in \mathbb{Z}$: $f\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} = a$. The homomorphism properties are easy to check by glancing at the formulas for subtraction and multiplication in part (a).

   (c) The kernel equals $\left\{\begin{pmatrix} 0 & 0 \\ b & c \end{pmatrix} : b, c \in \mathbb{Z}\right\}$.

10. (a) If $s, t \in f(I)$ then $s = f(a)$ and $t = f(b)$ for some $a, b \in I$. Then $s + t = f(a) + f(b) = f(a + b) \in f(I)$. For any $u \in S$ there exists $r \in R$ with $u = f(r)$, using the surjectivity. Then $us = f(r)f(a) = f(ar) \in f(I)$. Similarly su lies in $f(I)$. Therefore $f(I)$ is an ideal.

    (b) There are many examples. The inclusion map $\varphi\colon \mathbb{R} \to \mathbb{C}$ is a homomorphism of fields. The field $\mathbb{R}$ is an ideal in itself, but $\varphi(\mathbb{R}) = \mathbb{R}$ is not an ideal in $\mathbb{C}$.

11. (a) To see that f is a homomorphism, note that

$$\begin{aligned} f((a+b\sqrt{2}) + (c+d\sqrt{2})) &= f((a+c) + (b+d)\sqrt{2}) = (a+c) - (b+d)\sqrt{2} \\ &= (a-b\sqrt{2}) + (c-d\sqrt{2}) = f(a+b\sqrt{2}) + f(c+d\sqrt{2}) \\ f((a+b\sqrt{2})(c+d\sqrt{2})) &= f((ac+2bd) + (ad+bc)\sqrt{2}) = (ac+2bd) - (ad+bc)\sqrt{2} \\ &= (a-b\sqrt{2})(c-d\sqrt{2}) = f(a+b\sqrt{2})f(c+d\sqrt{2}). \end{aligned}$$

    f is clearly surjective since an arbitrary element $c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is $f(c - d\sqrt{2})$.

    (b) Suppose $f(a + b\sqrt{2}) = 0$. Then $a - b\sqrt{2} = 0$ and thus $a = b\sqrt{2}$ for $a, b \in \mathbb{Z}$. Since $\sqrt{2}$ is irrational, this is impossible unless $a = b = 0$ (otherwise $\frac{a}{b} = \sqrt{2}$). Thus $a + b\sqrt{2} = 0$, so that $\ker f = \{0\}$. By Theorem 6.11, f is injective. Since it is also a surjective homomorphism, it follows that f is an isomorphism.

12. For any a, $b \in R$ we have $(a + I)(b + I) - (b + I)(a + I) = ab + I - ba + I = (ab - ba) + I = I$ Therefore $(a + I)(b + I) = (b + I)(a + I)$.

13. $a + I$ has a square root in R/I if and only if there exists $b \in R$ where $a + I = (b + I)^2 = b^2 + I$. This occurs if and only if $a - b^2 \in I$.

14. If $a \in R$ then $a + I$ is a solution of $x^2 = x$ in R/I if and only if $a + I = (a + I)^2 = a^2 + I$. This occurs if and only if $a - a^2 \in I$.

15. R/I has an identity if and only if there exists $e \in R$ such that $(e + I)(a + I) = a + I$ for every $a \in R$. This equation is equivalent to: $ea + I = a + I$, which is the same as requiring: $ea - a \in I$.

16. R/I is a commutative ring with identity and it is not the zero ring, since $I \neq R$. Then R/I is an integral domain if and only if: whenever $(a + I)(b + I) = I$ then either $a + I = I$ or $b + I = I$. This is equivalent to saying: whenever $ab \in I$ then either $a \in I$ or $b \in I$.

17. (a) $f(a + b) = ((a + b) + I, (a + b) + J) = ((a + I) + (b + I), (a + J) + (b + J)) = (a + I, a + J) + (b + I, b + J) = f(a) + f(b)$. Similarly $f(ab) = f(a)f(b)$.
    (b) No, f is not necessarily surjective. For example $f : \mathbb{Z} \to \mathbb{Z}/(2) \times \mathbb{Z}/(4)$ is not surjective. In fact $(a + (2), b + (4))$ lies in the image of f if and only if $a \equiv b$ (mod 2). (Why?)

18. Let S be a homomorphic image of R, say $f : R \to S$ is a surjective homomorphism. Then the First Isomorphism Theorem implies that $S \equiv R/K$ where K is the kernel of f. Theorem 6.9 implies that S is a commutative ring with identity. Now let M be an ideal of S and define $I = f^{-1}(M) = \{r \in R : f(r) \in M\}$. **Lemma**. I is an ideal of R containing K and $f(I) = M$.

    Proof. If a, $b \in$ I then $f(a)$, $f(b) \in M$ so that $f(a + b) = f(a) + f(b)$ e M. Also if re R then $f(ra) = f(r)f(a) \in M$. Hence I is an ideal. Since $0_S \in M$ it follows that $K \subseteq I$. It is clear that $f(I) \subseteq M$.

    Conversely if m $\in M$ there exists $r \in R$ with $f(r) =$ m, since f is surjective. But then re I by definition and $m \in f(I)$.

    Now let us assume every ideal of R is principal. For any ideal M of S as above we have $M = f(I)$ where I is an ideal of R. By hypothesis, $I = (r)$ for some $r \in R$.

    Claim. $M = (f(r))$ is principal.

    Proof. If $m \in M$ then $m = f(w)$ for some $w \in I$. Then $w = rt$ for some $t \in R$, so that $m = f(rt) = f(r)f(t) \in (f(r))$. Conversely if m $\in (f(r))$ then $m = sf(r)$ for some s $\in$ S. Since f is surjective we have $s = f(t)$ for some t $\in$ R and m $= f(t)f(r) = f(tr) \in f(I) = M$.

19. For any a, $b \in R$ we have $(a + K) - (b + K) = (a - b) + K \in I/K$ and for any $r \in R$ we have $(r + K)(a + K) = ra + K \in I/K$ and $(a + K)(r + K) = ar + K \in I/K$. Therefore I/K is an ideal.

20. To show $\overline{f}$ is well defined suppose $r + I = r' + I$. To Show. $f(r) = f(r')$.
    Proof. Given $r - r' \in I$ we have $f(r) - f(r') = f(r - \mathrm{r'}) = 0_S$ since I is contained in the kernel. Then $f(r) = f(r')$.

    If r $r' \in R$ then $\overline{f}((r + I) + (r' + I)) = \overline{f}(r + r' + I) = f(r + r') = f(r) + f(r') = \overline{f}(r + I) + \overline{f}(r' + I)$. Similarly, $\overline{f}((r + I)\cdot(r' + I)) = f(rr' + I) = f(rr') = f(r)f(r') = \overline{f}(r + 1)\overline{f}(r' + I)$. Hence $\overline{f}$ is a homomorphism.

21. Let $\varphi : \mathbb{Z} \to \mathbb{Z}_5$ be the natural projection defined by $\varphi(k) = [k]_5$. The kernel of φ is (5) which contains the ideal (20). By Exercise 22 there is an induced homomorphism $\overline{\varphi} : \mathbb{Z}_{20} \to \mathbb{Z}_5$. Here $\overline{\varphi}$ $([k]_{20}) = [k]_5$ and we see that the kernel of $\overline{\varphi}$ is exactly (5) in $\mathbb{Z}_{20}$. The First Isomorphism Theorem then implies that $\mathbb{Z}_{20}/(5) \cong \mathbb{Z}_5$.

22. This was done in the solution to Exercise 20.

23. (a) If m, $n \in \mathbb{Z}$ we need to know that $(m + n)1_R = m1_R + n1_R$ and $(mn)1_R = (m_R)(n_R)$. These follow from results of Exercise 3.2.21.
    (b) The kernel of f is an ideal J of $\mathbb{Z}$. If $J = (0)$ then for every $n > 0$ we have $n1_R = f(n) \neq 0_R$. Therefore the characteristic of R is zero, and the assertion is true. Suppose $J \neq (0)$. Then by Exercise 6.1.38, $J = (n)$ is a principal ideal generated by the smallest positive element $n \in J$. That is, n is the smallest positive integer with $n1_R = 0_R$. Then n is the characteristic of R (as in Exercise 3.2.31).

24. The idempotents are 0, 1, $x^2 + 1$ and $-x^2$.

25. Answered in the text.

26. A direct proof is easily given, since we know there are only two cosets, and the quotient ring is a commutative ring with identity. Comparing the tables shows that this ring of two elements is isomorphic to $\mathbb{Z}_2$. For a more "abstract" proof see Exercise 29.

27. Define $\varphi : S \to \mathbb{Z}_p$ by $\varphi(r/\mathrm{s}) = [r]_p[s]_p^{-1}$. Suppose r/s is not in lowest terms, so that $r = dr_1$ and $s = ds_1$ where $d = (r, s)$ is the god. Since $[r]_p[s]_p^{-1} = [r_1]_p[s_1]_p^{-1}$ we conclude that $\varphi(r/s) = [r]_p[s]_p^{-1}$ even if r/s is not in lowest terms (provided $p \nmid s$ of course).

    If r/s and $r'/s' \in S$ then $\varphi(r/\mathrm{s} + r'/s') = \varphi((rs' + sr')/ss') = [rs' + sr']_p[ss']_p^{-1} = [rs']_p[ss']_p^{-1} + [sr']_p\,[ss']_p^{-1} = \varphi(r/s) + \varphi(r'/s')$. Similarly, $\varphi((r/s)(r'/s')) = \varphi(rr'/ss') = [rr']_p[ss']_p^{-1} = ([r]_p[s]_p^{-1})([r']_p[s']_p^{-1}) = \varphi(r/s)\ \varphi(r'/s')$. Therefore φ is a homomorphism. It is surjective since $\varphi\ (r) = [r]_p$ for any $r \in \mathbb{Z}$. Check that the kernel equals the ideal I. The First Isomorphism Theorem implies $S/I \cong \mathbb{Z}_p$.

28. Define φ: $\mathrm{T} \to \mathbb{R}$ by $\varphi\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} = a.$ From the formulas in Exercise 6.1.42 it follows that φ is a homomorphism. It is certainly surjective and the kernel is seen to be the ideal I of that Exercise. The First Isomorphism implies that $T/I \cong \mathbb{R}$.

29. Define $\psi\!: T \to \mathbb{R} \times \mathbb{R}$ by $\psi\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} = (a, c).$ From the formulas in Exercise 6.1.43 it follows that ψ is a homomorphism. It is surjective with kernel $= I$. The First Isomorphism Theorem implies that $T/I \cong \mathbb{R} \times \mathbb{R}$.

30. Define $f : I \to (I + J)/J$ as in the Hint. It is a homomorphism since it is the restriction of the projection homomorphism $\pi : R \to R/J$. Every element of $(I + J)/J$ equals some coset $i + j + J$ for $i \in I$ and $j \in J$. But this coset equals $i + J = f(i)$, so that f is surjective. If $a \in I \cap J$ then $f(a) = a + J = J$ so that a is in the kernel. Conversely, if $a \in I$ lies in the kernel then $f(a) = a + J = J$, so that $a \in J$. Therefore $a \in I \cap J$. The First Isomorphism Theorem implies that $I/(I \cap J) \equiv (I + J)/J$.

31. Let π: $R \to R/I$ be the projection homomorphism, which is surjective with kernel I. Since $K \subseteq I$ Exercise 22 implies that there is an induced homomorphism $f = \bar{\pi}$: $R/K \to R/I$ where $f(r + K) = r + I$. It is surjective since π is surjective. If $a \in I$ then $f(a + K) = a + I = I$ so that $a + K$ is in the kernel. Conversely, if $r + K$ is in the kernel of f then $r + I = f(r + K) = I$ and $r \in I$. Then the kernel $= \{a + K : a \in I\} = I/K$. The First Isomorphism Theorem implies that $(R/K)/(I/K) = R/I$.

32. (a) Suppose M is an ideal in R/K. Let $\pi : R \to R/K$ be the projection homomorphism. Then $I = \pi^{1}(M) = \{r \in R \mid \pi(r) \in M\}$ is an ideal of R containing K, and furthermore, $\pi(I) = M$. This was all proved in the answer to Exercise 20. Note mat $\pi(I) = \{a + K \mid a \in I\} = I/K$.

    (b) Let $I(S)$ denote the set of all ideals in the ring S. Let $I_K(R)$ be the set of all ideals of R which contain K. Define α: $I(S) \to I_K(R)$ by $\alpha(M) = f^{-1}(\mathrm{M}) = \{r \in R \mid f(r) \in M\}$. (By Exercise 24, this map a is wetl-defined.) Define $\beta : I_K(R) \to I(S)$ by $\beta(I) = f(I)$. (By Exercise 11 this β is well-defined.) As proved in Exercise 20 we also know that $\beta(\alpha(M)) = M$. Claim. $\alpha(\beta(I)) = I$.

    Proof. $\alpha(\beta(I)) = \{r \in R \mid f(r) \in f(I)\}$. This set certainly contains I. Conversely if $f(r) \in f(I)$ then $f(r) = f(a)$ for some $a \in I$. Then $f(r - a) = 0_S$ so that $r - a \in K \subseteq I$, and $r \in a + I = I$.

    Therefore α and β are inverses of each other, so they are bijections.

6.3 The Structure of R/I when I is Prime or Maximal

1. Answered in the text.

2. If P is a prime ideal then Theorem 6.14 implies that R/P is a finite integral domain. By Theorem 3.11 it is a field, hence P is maximal by Theorem 6.15.

3. (a) First note that p is prime if and only if –p is prime, and that $(p) = (–\mathrm{p})$. Therefore we may assume $p > 0$. If $p = 1$ then p is not prime and $\mathbb{Z}/(p) = (0)$ is not a field. Suppose $p > 1$. Theorem 2.8 implies that p is a prime if and only if $\mathbb{Z}_P$ is a field. Then, p is a prime number if and only if (p) is a maximal ideal, using Theorem 6.15.

    (b) If $p(x) = 0$ is the zero polynomial then it is not irreducible and (0_F) is not maximal. If $p(x) = c$ is a non-zero constant then it is not irreducible and $(p(x)) = F[x]$ is not a maximal ideal. Suppose deg $p(x) \geq 1$. By Theorem 5.10, $p(x)$ is irreducible if and only if $F[x]/(p(x))$ is a field. By Theorem 6.15 this is equivalent to saying $(p(x))$ is a maximal ideal.

4. R is an integral domain if and only if: if $ab = 0_R$ is R then either $a = 0_R$ or $b = 0_R$. By the definition of "prime ideal" this says exactly that (0_R) is prime.

5. For $\mathbb{Z}_6$ the maximal ideals are (2) and (3).
   For $\mathbb{Z}_{12}$ the maximal ideals are: $(2) = \{0, 2, 4, 6, 8, 10\}$ and $(3) = \{0, 3, 6, 9\}$.

6. (a) The ideals of $\mathbb{Z}_8$ are all principal (see Exercise 6.2.20) so they are (0), $(I) = \mathbb{Z}_8$, $(2) = \{0, 2, 4, 6\}$ and $(4) = \{0, 4\}$. The only maximal ideal is (2). Similarly the ideals of $\mathbb{Z}_9$ are (0), $(1) = \mathbb{Z}_9$ and $(3) = \{0,3,6\}$. The only maximal ideal is (3).

    (b) The ideals (2) and (5) are maximal in $\mathbb{Z}_{10}$ and (3) and (5) are maximal in $\mathbb{Z}_{15}$.

7. Answered in the text.

8. As the hint suggests, let $I = (2)$ and $J = (3)$ as ideals of $\mathbb{Z}$. Then I consists of all multiples of 2 and J of all multiples of 3, so elements of $I \cap J$ are multiples of both 2 and 3, so are multiples of 6. Thus $I \cap J = (6)$. This is not a prime ideal, since for example $2 \cdot 3 \in I \cap J$ but neither 2 nor 3 is in $I \cap J$ since neither is a multiple of 6.

9. Answered in the text.

10. Define $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_P$ by $\varphi\ (f(x)) = [f(0)]_p$. This map is the composition of the evaluation homomorphism $\mathbb{Z}[x] \to \mathbb{Z}$ considered in Exercise 4.1.16 (or Exercise 4.4.24) and the natural homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}_p$. Therefore φ is a surjective homomorphism. The First Isomorphism Theorem implies that $\mathbb{Z}[x]/K \cong \mathbb{Z}_p$ where K is the kernel of φ. This K is a maximal ideal by Theorem 6.15. Finally, a polynomial $f(x)$ lies in K if and only if $[f(0)]_p = [0]_p$, if and only if $f(0)$ is divisible by p. Since $f(0)$ is the constant term of $f(x)$, $J = K$.

11. The map $\psi : \mathbb{Z}[x] \to \mathbb{Z}$ defined by $\psi(f(x)) = \mathrm{f}(1)$ is a surjective homomorphism by Exercise 4.4.24. A polynomial $f(x)$ is in the kernel if and only if $f(1) = 0$. As remarked in Exercise 4.4.20 the Factor Theorem remains valid over any commutative ring with identity. Therefore $f(1) = 0$ if and only if $(x - 1) \mid f(x)$. Then the kernel equals the ideal $(x - 1)$. The First Isomorphism Theorem says that $\mathbb{Z}[x]/(x - 1) \cong \mathbb{Z}$. By Theorems 6.14 and 6.15, $(x - 1)$ is prime but not maximal.

12. Define $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_p$ by $\varphi\ (m,\ n) = [m]_p$. It is easy to verify that φ is a surjective homomorphism. The kernel of φ consists of all $(m,\ n)$ with $p \mid m$. Therefore M is this kernel. The First Isomorphism Theorem implies that $(\mathbb{Z} \times \mathbb{Z})/\mathrm{M} \cong \mathbb{Z}_p$ and Theorem 6.15 implies that M is maximal.

13. Define $f : R \times R \to R/I \times R/I : (a, b) \mapsto (a + I, b + I)$. Then f is a homomorphism of rings since

$$\begin{aligned} f((a,b)+(c,d)) &= f((a+c,b+d)) = (a+c+I,b+d+I) = (a+I,b+I)+(c+I,d+I) \\ &= f((a,b))+f((c,d)) \\ f((a,b)(c,d)) &= f((ac,bd)) = (ac+i,bd+i) = (a+I,b+I)(c+I,d+I) = f((a,b))f((c,d)). \end{aligned}$$

(The next-to-last equality in the previous line holds since $(a+I)(c+I) = ac+aI+cI+II = ac+I$ since I is an ideal). Thus f is a ring homomorphism. It is clearly surjective, since given $(a+I, b+I)$ a general element of $R/I \times R/I$, we have $(a+I, b+I) = f((a, b))$, so it is in the image of f. (Note that many choices are possible for a and b given an element of $R/I \times R/I$). It remains to determine $\ker f$. Suppose $f((a, b)) = 0$. Then $f((a, b)) = (a+I, b+I) = (0+I, 0+I)$, so that $a+I = 0+I$ and thus $a \in I$, and also $b+I = 0+I$ so that $b \in I$. So $\ker f$ consists of those (a, b) with $a, b \in I$; that is, $\ker f = I \times I$. Since f is a surjective homomorphism, we have $(R \times R)/(I \times I) \cong R/I \times R/I$ by Theorem 6.13.

14. No. In fact if I, J are ideals of R consider the map α: $R \times R \to (R/I) \times (R/J)$ given by $\alpha(a,\ b) = (a + I,\ b + J)$. Check that this is a surjective homomorphism with kernel $I \times J$. The First Isomorphism Theorem then implies that $(R \times R)/(I \times J) \cong (R/I) \times (R/J)$. In particular, $(R \times R)/(P \times P) \cong (R/P) \times (R/P)$. This ring is not an integral domain and therefore $P \times P$ is not prime.

15. (a) The axioms involving addition alone are certainly satisfied. For multiplication we have:
Associative. $a(bc) = 0 = (ab)c$ for every a, b, c.
Commutative. $ab = 0 = ba$ for every a, b.
Distributive. $a(b + c) = 0 = 0 + 0 = ab + ab$.
(b) Answered in the text. Corollary 6.16 requires R to have an identity element.

16. Suppose there is an ideal $J \neq M$ with $M \subseteq J \subseteq E$. Choose $n \in J$ with $n \notin M$. Since M contains every multiple of 4 in $\mathbb{Z}$ we have $n = 4k + 2$ for some integer k. Since $4k \in M$, $2 = n - 4k \in J$. Then every multiple of 2 lies in J and $J = E$. Therefore M is maximal.

Claim. E/M has no identity element. Proof. For any $x, y \in E$, xy is a multiple of 4 so that $xy \in M$. Therefore, $(x + M)(y + M) = M$ and every product in E/M equals zero. An identity element e in E/M would have to be zero, since $e = ee = 0$. In that case $E/M = (0)$ and $E = M$. Since $E \neq M$, no identity can exist.

Theorem 6.15 requires R to have an identity element.

17. Answered in the text

18. Suppose P has the given property. To prove P is prime suppose $a, b \in R$ and $ab \in P$.
Claim. The ideals $A = P + (a)$ and $B = P + (b)$ have the property that $AB \subseteq P$. Proof. Typical elements of A and B are $p_1 + ax$ and $p_2 + by$ for $p_1, p_2 \in P$ and $x, y \in R$. Then $(p_1 + ax)(p_2 + by) = p_1p_2 + p_1by + axp_2 + abxy$. Each term here lies in P, so the whole product lies in P. Since these products generate AB we conclude $AB \subseteq P$.
Therefore either $A \subseteq P$ so that $a \in P$, or $B \subseteq P$ so that $b \in P$.

Conversely suppose P is prime and A, B are ideals with $AB \subseteq P$. If the assertion is false then: $A \not\subseteq P$ and $B \not\subseteq P$. Then there exist $a \in A$ and $b \in B$ with $a, b \notin P$. But $ab \in AB \subseteq P$ and since P is prime either $a \in P$ or $b \in P$. This contradiction shows that the assertion must be true.

19. Claim. If R is a commutative ring with identity then the set of nonunits in R equals the union of all the maximal ideals of R.
Proof. If $a \in R$ is a nonunit then the ideal (a) is not the whole ring. The assumed property implies that (a) is contained in some maximal ideal, so a lies in that union. Conversely, if u is a unit in R then u cannot lie in any maximal ideal. (An ideal J contains a unit only when $J = R$. See Exercise 6.1.13.) Therefore u is not in that union.
In the case R contains a unique maximal ideal M this claim says that the set of nonunits equals M.
Conversely suppose the set of nonunits forms an ideal J. The Claim implies that $M \subseteq J$ for every maximal ideal M of R. Since $J \# R$ (since J does not contain any units) the maximality of M implies that $M =$ J for every maximal ideal. Therefore there is a unique maximal ideal M.

20. The projection map $\pi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $\pi(m, n) = m$ is a surjective homomorphism with kernel $K = (0) \times \mathbb{Z}$. By the First Isomorphism Theorem we have $(\mathbb{Z} \times \mathbb{Z})/K \cong \mathbb{Z}$. Then Theorem 6.14 and 6.15 imply that K is prime but not maximal.

21. (a) Verifying R is a subring is easy to do: just examine the formulas for sum and product of complex numbers. The set M is exactly the principal ideal (3). Suppose $r + si \notin M$ so that either $3 \nmid r$ or $3 \nmid s$.

Claim. $3 \nmid (r^2 + s^2)$. Proof. Otherwise $r^2 + s^2 = 0 \pmod 3$. Plug in all the possibilities for r, s (mod 3) to see that $r \equiv s \equiv 0 \pmod 3$. Then $3 \mid r$ and $3 \mid s$, contrary to hypothesis.

Now suppose J is an ideal larger that M. Choose some $r + si \in J$ where $r + si \notin M$. Then $r^2 + s^2 = (r + si)(r - si) \in J$ and we know $3 \in J$. By the Claim, 3 and $r^2 + s^2$ are relatively prime integers, so there is a linear combination of them equal to 1. Then $1 \in J$ so that $J = R$. Therefore M is maximal.

(b) By part (a) and Theorem 6.15, R/M is a field. Working with congruence mod M check that any $a + bi \in R$ can be reduced to some $a' + b'i$ where $0 \le a' < 3$ and $0 \le b' < 3$. There are 9 of these representative elements. Check that these are non-congruent, so that R/M has exactly 9 elements.

22. The set J here is the principal ideal (5). Since $(2 + i)(2 - i) \in J$ but $2 + i$ and $2 - i \notin J$. J is not a prime ideal.

23. We want an explicit isomorphism $R/(5) \cong \mathbb{Z}_5 \times \mathbb{Z}_5$. One way to do this is to argue that $R \cong \mathbb{Z}[x]/(x^2 + 1)$ so that we ought to have $R/(5) \cong \mathbb{Z}_5[x]/(x^2 + 1)$. Since $x^2 + 1 = (x - 2)(x + 2)$ in $\mathbb{Z}_5[x]$ we get induced homomorphisms to $\mathbb{Z}_5[x]/(x - 2)$ and to $\mathbb{Z}_5[x]/(x + 2)$. These rings are isomorphic to $\mathbb{Z}_5$ by "evaluation" at 2 and at -2. Gluing all these steps together, motivates the following definition.

Let $\varphi : R \to \mathbb{Z}_5 \times \mathbb{Z}_5$ be given by $\varphi(a + bi) = ([a + 2b]_5, [a - 2b]_5)$. It is straightforward (but somewhat long) to check that this φ is a surjective homomorphism, and to calculate that the kernel is exactly the ideal (5). The First Isomorphism Theorem implies finally that $\mathrm{R}/(5) \cong \mathbb{Z}_5 \times \mathbb{Z}_5$.

The tedious calculation in the preceding paragraph can be avoided if the steps in the first paragraph can be made precise. This can all be done with a little more work, using various versions of the Isomorphism Theorems.

24. As in Exercise 22 define $\psi : R \to \mathbb{Z}_5$ by $\psi(a + bi) = [a - 2b]_5$. The work done there already implies that ψ is a surjective homomorphism. If $a + bi$ is in the kernel then $[a - 2b]_5 = [0]_5$ so that $a = 2b + 5q$ for some $\mathrm{q} \in \mathbb{Z}$. Therefore $a + bi = (2 + i)b + 5q = (2 + i)\cdot(b + (2 - i)q)$ lies in the ideal $(2 + i)$. Consequently the kernel is $(2 + i)$ and the First Isomorphism Theorem can be applied.

25. The set M here is exactly the principal ideal (5). Suppose J is an ideal larger than M and choose some $r + s\sqrt{2} \in J$ but not in M. Then either $5 \nmid r$ or $5 \nmid s$. We know that $5 \in M \subseteq J$ and also that $r^2 - 2s^2 = (r + s\sqrt{2})(r - s\sqrt{2}) \in J$.

Claim. $r^2 - 2s^2$ and 5 are relatively prime.

Proof. If not then we have $r^2 = 2s^2 \pmod 5$. If one of r, s is congruent to zero they both are. Therefore we must have $r, s \not\equiv 0 \pmod 5$. Then $(r/s)^2 \equiv 2 \pmod 5$, but checking $0^2, 1^2, \ldots, 4^2$ we see that 2 does not occur. This contradiction proves the Claim.

From the Claim conclude that 1 is an integer linear combination of $r^2 - 2s^2$ and 5 so that $1 \in J$ forcing $J = (1) = T$. Therefore M is a maximal ideal.

Chapter 7

Groups

7.1 Definition and Examples of Groups

1. Answered in the text.

2. (a) Since 1 is the multiplicative identity, it is its own inverse. Since $2 \cdot 2 = 4 \equiv 1 \pmod 3$, we see that $2^{-1} = 2$.

   (b) Since 1 is the multiplicative identity, it is its own inverse. Further, $2 \cdot 3 = 3 \cdot 2 = 6 \equiv 1 \pmod 5$, so that 2 and 3 are multiplicative inverses. Finally, $4 \cdot 4 = 16 \equiv 1 \pmod 5$, so that 4 is its own inverse.

   (c) Since 1 is the multiplicative identity, it is its own inverse. Further, $2 \cdot 4 = 4 \cdot 2 = 8 \equiv 1 \pmod 7$, so that 2 and 4 are multiplicative inverses. Next, $3 \cdot 5 = 5 \cdot 3 = 15 \equiv 1 \pmod 7$, so that 3 and 5 are multiplicative inverses. Finally, $6 \cdot 6 = 36 \equiv 1 \pmod 7$, so that 6 is its own inverse.

3. (a) 18 (b) 8 (c) 24 (d) 120 (e) 6

4. (a) No, it is not. Although G is closed under the operation as a subset of $\mathbb{Z}_{10}$, there is no multiplicative identity.

   (b) No, it is not. G is not closed under the operation, since for example $2 - 2 = 0 \notin G \subset \mathbb{Z}_{10}$.

   (c) No, it is not. G is not closed under the operation, since the sum of two odd integers is even.

   (d) Yes, it is. G is closed since $2^x * 2^y = 2^x 2^y = 2^{x+y} \in G$ since the sum of two rationals is rational. Next, 2^0 is the identity, since $2^0 * 2^x = 2^0 2^x = 2^{0+x} = 2^0$, and the inverse of an element $2^x \in G$ is 2^{-x} (which is again a rational power of 2), since $2^x * 2^{-x} = 2^{x+(-x)} = 2^0$, which is the identity.

5. (a) The determinant of this matrix is $2 \cdot 1 - 0 \cdot 2 = 2$, and $2^{-1} = 2$ in $\mathbb{Z}_3$. Also, in $\mathbb{Z}_3$, we have $-2 = 1$ since $1 + 2 = 0$. Then by Example 8 in Section 3.2, the inverse is

$$\begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 \cdot 2^{-1} & 0 \cdot 2^{-1} \\ -2 \cdot 2^{-1} & 2 \cdot 2^{-1} \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ -2 \cdot 2 & 2 \cdot 2 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}$$

   Thus the matrix is its own inverse.

(b) The determinant of this matrix is $1 \cdot 4 - 2 \cdot 3 = 4 - 6 = -2 \equiv 3 \pmod 5$, and $3^{-1} = 2$ in $\mathbb{Z}_5$. Then by Example 8 in Section 3.2, the inverse is

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 4 \cdot 3^{-1} & -2 \cdot 3^{-1} \\ -3 \cdot 3^{-1} & 1 \cdot 3^{-1} \end{pmatrix} = \begin{pmatrix} 4 \cdot 2 & -2 \cdot 2 \\ -3 \cdot 2 & 1 \cdot 2 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 4 & 2 \end{pmatrix}$$

(c) The determinant of this matrix is $3 \cdot 6 - 5 \cdot 4 = 18 - 20 = -2 \equiv 5 \pmod 7$, and $5^{-1} = 3$ in $\mathbb{Z}_7$. Then by Example 8 in Section 3.2, the inverse is

$$\begin{pmatrix} 3 & 5 \\ 4 & 6 \end{pmatrix}^{-1} = \begin{pmatrix} 6 \cdot 5^{-1} & -5 \cdot 5^{-1} \\ -4 \cdot 5^{-1} & 3 \cdot 5^{-1} \end{pmatrix} = \begin{pmatrix} 6 \cdot 3 & 2 \cdot 3 \\ 3 \cdot 3 & 3 \cdot 3 \end{pmatrix} = \begin{pmatrix} 4 & 6 \\ 2 & 2 \end{pmatrix}$$

6. Using the hint, note that $\mathbb{Z}_2$ as an additive group satisfies $a+a=0$ for each element. Then consider $\mathbb{Z}_2 \times \mathbb{Z}_2$, and compute (for a, b arbitrary elements of $\mathbb{Z}_2$)

$$(a,b) * (a,b) = (a+a, b+b) = (0,0),$$

which is the identity element of $\mathbb{Z}_2 \times \mathbb{Z}_2$. Thus every element of the product group is its own inverse, as desired.

7. (a) There are sixteen possible 2×2 matrices each of whose elements is 0 or 1. Of these, the matrices that have zero or only one 1 have determinant zero, so they are not in $GL(2, \mathbb{Z}_2)$. There are five of these. There are also four matrices that have a row or column of zeros and a row or column of ones; these also have determinant zero. That leaves seven matrices. The matrix $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ also has determinant zero, leaving six matrices, which together form $GL(2, \mathbb{Z}_2)$:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

(b) For example, in $GL(2, \mathbb{R})$,

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad \text{but} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}.$$

In $GL(2, \mathbb{Z}_2)$, use the same two matrices. The two products, when interpreted as elements of $\mathbb{Z}_2$, are the unequal matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

8. $U_4 = \{1, 3\}$. $U_6 = \{1, 5\}$. $U_{10} = \{1.3,7,9\}$. $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. $U_{30} = \{1, 7, 11, 13, 17, 19, 23, 29\}$.

9. Answered in the text.

10. There is a direct computational proof that this set is closed under multiplication, contains inverses of its elements and is abelian. Another proof is provided by letting $C = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,\ b\ \in \mathbb{R} \mid \right\}$ and noting that the map φ: ₵ $\to$ C defined by $\varphi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ is an isomorphism. (See the second Example in Section 3.3). Then $G =$ φ(₵*) is an abelian group.

11. The operation table for $\mathbb{Z}_2 \times G$:

	$(0,\ 1)$	$(0,-1)$	$(0,\ i)$	$(0,\ -i)$	$(1,\ 1)$	$(1,-1)$	$(1,\ i)$	$(1,\ -i)$
$(1,\ 1)$	$(0,\ 1)$	$(0,-1)$	$(0,\ i)$	$(0,\ -i)$	$(1,\ 1)$	$(1,-1)$	$(1,\ i)$	$(1,\ -i)$
$(0,-1)$	$(0,-1)$	$(0,\ 1)$	$(0,-i)$	$(0,\ i)$	$(1,-1)$	$(1,\ 1)$	$(1,\ -i)$	$(1,\ i)$
$(0,\ i)$	$(0,\ i)$	$(0,-i)$	$(0,-1)$	$(0,\ 1)$	$(1,\ i)$	$(1,\ -i)$	$(1,-1)$	$(1,\ 1)$
$(0,\ -i)$	$(0,\ -i)$	$(0,\ i)$	$(0,\ 1)$	$(0,-1)$	$(1,\ -i)$	$(1,\ i)$	$(1,\ 1)$	$(0,-1)$
$(1,\ 1)$	$(1,\ 1)$	$(1,-1)$	$(1,\ i)$	$(1,\ -i)$	$(0,\ 1)$	$(0,-1)$	$(0,\ i)$	$(0,\ -i)$
$(1,-1)$	$(1,\ -1)$	$(1,\ 1)$	$(1,\ -i)$	$(1,\ i)$	$(0,-1)$	$(0,\ 1)$	$(0,\ -i)$	$(0,\ i)$
$(1,\ i)$	$(1,\ i)$	$(1,\ -i)$	$(0,-1)$	$(1,\ 1)$	$(0,\ i)$	$(0,\ -i)$	$(0,-1)$	$(0,\ 1)$
$(1,\ -i)$	$(1,\ -i)$	$(1,\ i)$	$(1,\ 1)$	$(1,-1)$	$(0,\ -i)$	$(0,\ i)$	$(0,\ 1)$	$(0,-1)$

12. Since a composition of bijective functions is bijective, $A(T)$ is closed under the operation. (See Exercise 27 of Appendix B.) The composition of functions is always associative. The identity element is the identity map ι_T. Finally if $f \in A(T)$ then there is an inverse function g satisfying $f \circ g = \iota_T$ and $g \circ f = \iota_T$ (See Theorem B.l in Appendix B.) Therefore $A(T)$ is a group.

13. Note that if G is nonabelian, and H is any group, then $G \times H$ is nonabelian. To see this, choose two elements in G with $a * b \neq b * a$. Then in $G \times H$, we have

$$(a, 1_H) * (b, 1_H) = (a * b, 1_H) \neq (b * a, 1_H) = (b, 1_H) * (a, 1_h).$$

Since for example D_3 is a nonabelian group of order 6, we see that $D_3 \times \mathbb{Z}_4$ is a nonabelian group of order $3 \times 4 = 12$, and similarly $D_3 \times \mathbb{Z}_{10}$ and $D_3 \times \mathbb{Z}_{16}$ are nonabelian of orders 30 and 48. Finally, D_4 is nonabelian of order 8, so that $D_4 \times \mathbb{Z}_2$ is nonabelian of order 16.

14. The corner 1 can go to any one of the 4 corners under a rigid motion. Once the position of corner 1 is fixed there are two possibilities: orientation face up or face down. These choices completely determine the rigid motion. Therefore there are $4 \cdot 2 = 8$ rigid motions of the square. There are 8 rotations listed, so they must include all the rigid motions.

15. (a) This group can be viewed as a subgroup of D_4, the symmetry group of the square. The rectangle does not allow a 90° rotation or a reflection through a diagonal, so we are left with 4 elements: $\{r_0,\ r_2,\ h,\ v\}$.
(b) Similarly the parallelogram admits no reflections and has no 90° rotation, leaving only two elements: $\{r_0,\ r_2\}$.
(c) This figure admits neither 90° rotations nor diagonal reflections so its group is the same as that of the rectangle in part (a).

16. (a) Compute the products:

$$\mathbf{i}^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} i^2 & 0 \\ 0 & (-i)^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathbf{1}$$

$$\mathbf{j}^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathbf{1}$$

$$\mathbf{k}^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} i^2 & 0 \\ 0 & i^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -\mathbf{1}$$

$$\mathbf{ij} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ (-i)(-1) & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \mathbf{k}$$

$$-\mathbf{ji} = -\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = -\begin{pmatrix} 0 & -i \\ (-1)i & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \mathbf{k}.$$

Since these matrices are all in $GL(2, \mathbb{C})$, multiplication is associative. Then using the equalities above, together with the obvious fact that $-(-\mathbf{1}) = \mathbf{1}$, we get

$$\begin{aligned} \mathbf{jk} &= \mathbf{j}(-\mathbf{ji}) = -\mathbf{j}^2\mathbf{i} = \mathbf{i} \\ -\mathbf{kj} &= -\mathbf{ijj} = -\mathbf{ij}^2 = \mathbf{i} \\ \mathbf{ki} &= -\mathbf{jii} = -\mathbf{ji}^2 = \mathbf{j} \\ -\mathbf{ik} &= -\mathbf{iij} = -\mathbf{i^2j} = \mathbf{j}. \end{aligned}$$

(b) The multiplication table is

·	**1**	**i**	**−1**	**−i**	**j**	**k**	**−j**	**−k**
1	**1**	**i**	**−1**	**−i**	**j**	**k**	**−j**	**−k**
i	**i**	**−1**	**−i**	**1**	**k**	**−j**	**−k**	**j**
−1	**−1**	**−i**	**1**	**i**	**−j**	**−k**	**j**	**k**
−i	**−i**	**1**	**i**	**−1**	**−k**	**j**	**k**	**−j**
j	**j**	**−k**	**−j**	**k**	**−1**	**i**	**1**	**−i**
k	**k**	**j**	**−k**	**−j**	**−i**	**−1**	**i**	**1**
−j	**−j**	**k**	**j**	**−k**	**1**	**−i**	**−1**	**i**
−k	**−k**	**−j**	**k**	**j**	**i**	**1**	**−i**	**−1**

17. (a) Answered in the text.
(b) Closure: if a, $b \neq 0$ then $ab \neq 0$ in $\mathbb{Q}$ so that $a{*}b \in G$.
Associativity: $(a{*}b){*}c = (ab/3)c/3 = abc/3$. Similarly $a{*}(b{*}c) = abc/3$. The commutative law also holds: $a{*}b = b{*}a$. The identity element is 3 since: $3{*}a = a{*}3 = 3a/3 = a$.
For $a \in G$ the inverse is $9/a$, since $(9/a){*}a = ((9/a)a)/3 = 9/3 = 3$.

18. Function composition is always associative. The identity element is $i \in G$.
Inverses: To find the inverse of a function f, set $x = f(y)$ and solve for y. If $x = f(y) = 1/(1 - y)$ then $y = 1 - 1/x = (x - 1)/x = g(x)$. Then $f^{-1} = g$. Similarly, $g^{-1} = f$, $h^{-1} = h$, $j^{-1} = j$ and $k^{-1} = k$.
Closure. For example $f^2(x) = 1/(1 - f(x)) = (1 - x)/(-x) = g(x)$. There are 36 such compositions to verify.

A somewhat shorter method is to verify that $f^3 = i$, $j^2 = i$ and $f^2 j = jf$. From these relations it follows that all the functions expressible as compositions of f and j are: i, f, f^2, j, f_j, $f^2{}_j$. Therefore this set of six functions is closed under composition. These functions are i, f, g, j, h, k.

19. Answered in the text.

20. Let $f \in S_n$. There are n possibilities for $f(1)$. After one such image has been chosen, there remain $n - 1$ possibilities for $f(2)$. After one such image has been chosen there remain $n - 2$ possibilities for $f(3)$. This process continues until we have 2 possibilities for $f(n - 1)$ and once that is chosen there is only one possibility for $f(n)$. Then altogether there are $n \cdot (n - 1) \ldots 2 \cdot 1 = n!$ possible permutations f.

21. Certainly g is closed under #. The associative law follows: $(a\#b)\#c = c*(b*a) = (c*b)*a = a\#(b\#c)$. The identity element and the inverses for the operation $*$ also work for #.

22. All rotations are taken counterclockwise around the center. Let r_k be the rotation through 72k°. Then there are 5 rotations preserving the pentagon: r_0, r_1, r_2, r_3, r_4. For each vertex A of the pentagon let ℓ_A be the line through A and the center. The reflection τ_A through the line ℓ_A also preserves the pentagon. There are 5 such reflections, so we have found 10 symmetries so far. An argument similar to that in Exercise 12 shows that every rigid motion preserving the pentagon must be one of these 10. Therefore D_5 consists of these 10 elements.

23. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ define det $A = ad - bc$. We must verify that $\det(AB) = (\det A)(\det B)$ whenever $A, B \in \boldsymbol{M}(\mathbb{R})$. Let $G = SL(2, \mathbb{R})$. If $A, B \in G$ then $\det(AB) = 1$ so that $AB \in G$. The associative law is automatic here and the identity matrix is in $SL(2, \mathbb{R})$. If $A \in G$ then det $A \neq 0$ so A is invertible and $\det(A^{-1}) = (\det A)^{-1} = 1$ so mat $A^{-1} \in G$ as well.

24. Let $G =\{$nonzero real numbers$\}$. If $a, b \in G$ then from the definition it is clear that $a*b \in G$.
Associativity: Here is a chart of the possibilities, depending on the signs of a and b:

a	b	$(a*b)*c$	$a*(b*c)$
$+$	$+$	$(ab)c$	$a(bc)$
$+$	$-$	$(ab)/c$	$a(b/c)$
$-$	$+$	$(a/b)/c$	$a/(bc)$
$-$	$-$	$(a/b)c$	$a/(b/c)$

In each case the associative law is verified.
Identity. The number 1 is the identity element for this operation.

Inverses. The inverse of a is $\begin{cases} 1/a & \text{if} \quad a > 0 \\ a & \text{if} \quad a < 0. \end{cases}$

25. Closure. if (a,b) and $(a', b') \in \mathbb{R}^* \times \mathbb{R}$ then $aa' \neq 0$ so also $(aa', ba' + b') \in \mathbb{R}^* \times \mathbb{R}$.
Associativity. First: $(a, b)*((a', b')*(a'', b'')) = (a, b)*(a'a'', b'a'' + b'') = (a(a'a''), b(a'a'') + (b'a'' + b'')$.
Second: $((a, b)*(a', b'))*(a'', b'') = (aa', ba' + b')*(a'', b'') = ((aa')a'', (ba' + b')a'' + b'')$.
These quantities are equal.
Identity. The element (1, 0) is the identity element.
Inverses, The inverse of $(a,$ b) is $(1/a, -b/a)$.

26. Closure is clear. Associativity follows from the separate associative laws in G and H, by the same argument used for rings. The identity element is (e_G, e_H). The inverses also work componentwise: If g' is the inverse of $g \in G$ asnd h' is the inverse of $h \in H$ then (g', h') is an inverse for (g, h). Also if G, H both satisfy the commutative law then so does $G \times H$. It is generally true for any two finite sets G, H that $|\text{G} \times H| = |G|\cdot|H|$.

27. Answered in the text.

28. Suppose $G = \{g_1, g_2, \ldots, g_n\}$ has n distinct elements. The i^{th} row of the operation table consists of the elements: $g_ig_1, g_ig_2, \ldots, g_ig_n$. If two of these quantities were equal we would have $g_ig_r = g_ig_s$ for some $r < s$. But by Exercise 25 this implies $g_r = g_s$, contrary to the hypothesis that these g_j are distinct. Therefore there are no repetitions among the elements in the i^{th} row. Let g_i' be the inverse of g_i. For any $a \in G$, $g_i'a$ is some element of G so it equals g_k for some k. Then $a = g_ig_i'a = g_ig_k$ does lie in the i^{th} row of the table. Therefore every element of G occurs exactly once in the i^{th} row. A similar argument applies to the j^{th} column of the table.

29. To avoid repetitions in a row or column we see that be cannot equal a, b or c. Then $bc = d$. Similarly $cb = d$. The rest of the table is easily completed.

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

30. First by the associative law, $ba = a^2a = aa^2 = ab = e$ and $bb = a^2b = a(ab) = ae = a$. Also $af \neq a, b, d, e, f$ since there can be no repetitions in a row or column. Therefore $af = c$. The products ad, bc, bd, bf follow similarly. The same argument shows that $da = c$, $fa = d$ and $db = f$. Again by the associative law we find $dc = cbc = cf = a$. By the row and column argument, we get $c^2 = b$ or e. Since b and c do not commute we must have $c^2 = e$. The rest of the table is easily done:

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

This group is isomorphic to S_3 as seen by comparing tables, where $a = (123)$, $b = (132)$, $c = (12)$, $d = (13)$ and $f = (23)$.

31. Answered in the text.

32. If $f \in A(T)$ let $S_f = \{t \in T \mid \mathrm{f}(t) \neq t\}$. If $f(t) = g(t) = t$ then $fg(t) = t$ as well. Then $S_{fg} \subseteq S_f \cup S_g$. Similarly, $f(t) = t$ if and only if $f^{-1}(t) = t$ so that $S_{f\text{-}1} = S_f$. Since $M = \{f \in A(T) \mid S_f \text{ is finite}\}$ it follows that M is closed under composition and inverses. Certainly the identity map is in M and the associative law is automatic. Hence M is a group.

33. <u>Closure</u>. $T_{a,b}(T_{c,d}\cdot(x)) = T_{a,b}(cx + d) = a(cx + d) + b = acx + ad + b$. Therefore $\mathrm{T}_{a,b} \circ T_{c,d} = T_{ac,\,ad+b}$.
<u>Identity</u>. $T_{1,0}$ is the identity map. <u>Inverses</u>. The inverse of $\mathrm{T}_{a,b}$ is $\mathrm{T}_{1/a,\ b/a}$. The associative law holds generally for compositions of functions. Hence G is a group. It is nonabelian since $T_{1,1}T_{1,0} \neq T_{0,1}T_{1,1}$.

34. By the formula above we have $T_{1,b}T_{1,d} = T_{1,b+d}$. Therefore H is closed under composition, the identity $T_{1,0}$ is in H, and the inverse of $T_{1,b}$ is $T_{1,-b}$. Then H is a group, and the commutative law is clear from the formula.

35. Among the list of powers $f, f^2, f^3, f^4, \ldots$ there can be at most $n! = |S_n|$ different elements involved. Therefore there is an equality $f^r = f^5$ for some $r < s$. Successively cancelling f's (using Exercise 25), conclude that $I = f^{s-r}$ where $s - r$ is a positive integer.

36. $0{*}1 \neq 0$ and ≤ 1 so that $0{*}1 = 1$. Similarly $0{*}k = k{*}0 = k$ for each k, and 0 is the identity element. Also $1{*}2 \neq 0, 1$ and is ≤ 3 sothat $1{*}2 = 3$. Operating by 1 yields $1{*}3 = 1{*}(1{*}2) = (1{*}1){*}2 = 0{*}2 = 2$. Similarly $1{*}4 \neq 0, 1, 2, 3, 4$ so that $1{*}4 = 5$ and $1{*}5 = 1{*}1{*}4 = 4$. Verify that $1{*}5 = 7$ and $1{*}7 = 6$ and argue that $k{*}1 = 1{*}k$. Also $2{*}3 = 2{*}2{*}1 = 1$. The rest of the table is computed by the same methods.

	0	1	1	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	I	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

7.2 Basic Properties of Groups

1. Answered in the text.

2. $(ab)^{-1} = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}^{-1} = \begin{pmatrix} 1\,2\,3 \\ 3\,2\,1 \end{pmatrix}$ while $a^{-1}b^{-1} = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}\begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix} = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}$.

3. $d^{-1}c^{-1}b^{-1}a^{-1}$.

4. If $ab = e$ then $b = a^{-1}$ and therefore $ba = a^{-1}\ a = e$.

5. Injective. Answered in the text.
   Subjective. For $g \in\ G$ note that $f(g^{-1}) = (g^{-1})^{-1} = g$ using Corollary 7.6.

6. U_8 has 4 elements, each satisfying $x^2 = 1$.

7. (a) 2 (b) 7 (c) 6 (d) 3.

8. $\mathbb{Z}_2 \times \mathbb{Z}$ using the operation of addition.

9. (a) $|U_{10}| = 4$. $|U_{12}| = 4$. $|U_{24}| = 8$.
   (b) 1 has order 1; 9, 11, 19 have order 2; 3, 7, 13, 17 have order 4.

10. (a) $\mathbb{Z}_4$: 0 has order 1; 2 has order 2; 1 and 3 have order 4.
    (b) $\mathbb{Z}_5$: 0 has order 1; the other four elements have order 5.
    (c) S_3: The identity has order 1; the 3 non-identity elements which fix one symbol have order 2; the 2 elements which fix no symbols have order 3.
    (d) D_4: The identity r_0 has order 1; the elements r_2 d, h, t, v have order 2; the elements r_1 and r_3 have order 4.

11. In an additive group, the sum of a with itself n times is written na. So statement (2) of Theorem 7.8 becomes

$$\text{If } ia = ja \text{ with } i \neq j\text{, then } a \text{ has finite order,}$$

and statements (1)-(3) of Theorem 7.9 becomes

$$ka = e \text{ if and only if } n \mid k$$
$$ia = ij \text{ if and only if } i \equiv j \pmod{n}$$
$$\text{If } n = td\text{, with } d \geq 1\text{, then } ta \text{ has order } d.$$

12. Since

$$(aba^{-1})^n = aba^{-1}aba^{-1}aba^{-1}\dots aba^{-1},$$

all the occurrences of $a^{-1}a$ become e, so what is left is n copies of b, and the product is ab^na^{-1}. An alternative, more precise, method of proof is using induction on n: the statement is clearly true for $n = 1$. Assume it is true for $n = k$; then

$$(aba^{-1})^{k+1} = (aba^{-1})^k(aba^{-1}) = ab^ka^{-1}aba^{-1} = ab^kba^{-1} = ab^{k+1}a^{-1}.$$

13. Answered in the text.

14. False. Look at S_3 with no element of order 6.

15. (a) By Theorem 7.8, $|a|$ divides 12 so $|a| = 1, 2, 3, 4, 6$ or 12.
    (b) By Theorem 7.8, $|a|$ divides p and it is not 1 since $a \neq e$. Hence $|a| = p$.

16. (a) $|a| = 12$; $|a\ | = 6$; $|a\ | = 4$; $|a\ | = 3$; $|a\ | = 12$; $|a\ | = 2$; $|a\ | = 12$; $|a\ | = 3$; $|a\ | = 4$; $|a\ | = 6$; $|a^{11}| = 12$
    (b) $|a^k| = n/(n, k)$.

17. (a) Answered in the text
    (b) If $a = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}, b = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix}$ then $x = ab, \quad y = ba \quad$ and $x \neq y$.

18. The elements $a_n^{-1}, \ldots, a_1^{-1}$ form a complete list of the elements of G (see Exercise 5). Therefore their product is also equal to x. Then $x^2 = (a_1 a_2 \ldots a_n)(a_n^{-1} \ldots a_1^{-1}) = e$.

19. Claim. $(bab^{-1})^k = ba^k b^{-1}$ for every positive integer k.
    Proof. For example $(bab^{-1})^2 = bab^{-1}\ bab^{-1} = ba^2 b^{-1}$. The higher exponents work similarly.
    Now if $a^k = e$ then by the claim, $(bab^{-1})^k = ba^k b^{-1} = beb^{-1} = e$. Similarly if $(bab^{-1})^k = e$ conclude that $a^k = e$. These two implications suffice to prove that a and bab^{-1} have the same order.

20. (a) This is a verification of some matrix products.
    (b) $ab = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. Prove by induction that $(ab)^k = \begin{pmatrix} 1 & 0 \\ -k & 1 \end{pmatrix}$ for every positive integer k.
    Therefore $(ab)^k \neq \mathrm{I}$ for every $k > 0$ and ab has infinite order.

21. The proof for positive integers is the same as that done for rings in Exercise 3.2.17. In fact the first statement is proved using additive notation in Exercise 3.2.17(i). It can be noted as well that Exercise 3.2.21(ii) implies:
    Lemma. If $ab = ba$ in a group G then $(ab)^n = \mathrm{a}^n b^n$ for every integer n.

    It remains to prove $(a^m)^n = a^{mn}$ when m or n is not positive. The cases were $m = 0$ or $n = 0$ are easily checked.

    Suppose $m, n > 0$. By definition $a^{-n} = (a^{-1})^n$ and repeated application of Corollary 7.6 shows that $a^{-a} = (a^n)^{-1}$ as well. Therefore: $(a^m)^{-n} = ((a^m)^n)^{-1} = (a^{-mn})^{-1} = a^{-mn}$. Similarly, $(a^{-m})^n = ((a^{-1})^m)^n = (a^{-1})^{mn} = a^{-mn}$ and using the previous case we get $(a^{-m})^{-n} = ((a^{-1})^m)\text{–}^{mn} = (a^{mn})$.

22.

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

23. Suppose $a,\ b \in\ G$ and let $c\ = aba^{-1}$. Then $ab = ca$ and the hypothesis implies $b = c$. Therefore $ab = ba$ and G is abelian.

24. Given $aabb = abab$. Cancelling yields $ab = ba$.

25. Corollary 7.6 states that $(ab)^{-1} = b^{-1}a^{-1}$. If G is abelian then certainly $(ab)^{-1} = a^{-1}b^{-1}$. Conversely, suppose $(ab)^{-1} = a^{-1}b^{-1}$ for every a, b. Then $(ba)^{-1} = a^{-1}b^{-1} = (ab)^{-1}$ so that $ab = ab$ by Corollary 7.6.

26. Suppose $ab \neq ba$. Since a commutes with e, a and a^{-1} we know b cannot equal any of these. The condition $b \neq a^{-1}$ says that $ab \neq e$ and $ba \neq e$. Since $b \neq e$ we know $ab \neq a$ and $ba \neq a$. Similarly $ab \neq b$ and $ba \neq b$. Hence $H= \{e$, a, b, ab, $ba\}$ has 5 distinct elements. Suppose $|G| < 6$ so that $G = H$. Then $a^2 \in H$, and since e, a, b are distinct we see that a, a^2, ab, ba are also distinct. Also $a^2 \neq b$ since a^2 commutes with a. Hence $a^2 = e$. Now aba must be one of the elements of H, If $aba = e$ then $ab = a^{-1} = a$. If $aba = a$ then $ab = e$. If $aba = b$ then $ab = ba^{-1} = ba$. If $aba = ba$ or ab then $a = e$. But then a$ba \notin H$, contrary to the closure property.

27. Answered in the text.

28. Using Exercise 19 we have: If $a^k = e$ then $(a^{-1})^k = (a^k)^{-1} = e$. Similarly if $(a^{-1})^k = e$ then $a^k = e$. It follows that $|a| = |a^{-1}|$.

29. Answered in the text.

30. Since $ab = a(ba)a^{-1}$ this follows from Exercise 17.

31. (a) As noted in the answers to Exercise 19 if $ab = ba$ we have $(ab)^k = a^k b^k$. Let $n = |a|$ and $m = |b|$. Then $(ab)^{mn} = a^{mn}b^{mn} = (a^n)^m(b^m)^n = e$.
    (b) Answered in the text.

32. Suppose G is a finite group with no element of order 2. Then every element $a \neq e$ has $a \neq a^{-1}$ so the non-identity elements come in pairs. Therefore $|G| = 1 + 2k$ is odd, where k is me number of those pairs.

33. Answered in the text.

34. (a) If $|g| = 3$ then $G = (e, g, g^2, d)$ where $g^3 = e$. If $gd = e$ then $gd = g^3$ and $d = g^2$. If $gd = g$ then $d = e$. If $gd = g^2$ then $d = g$. If $gd = d$ then $g = e$. In each case the conclusion is false. Then gd cannot lie in G, contrary to closure.
    (b) By Exercise 11, $|a| \leq 4$ for every $a \in G$. If there is an element of order 4 then G is cyclic. There is no element of order 3 by part (a). Therefore every element has order 1 or 2. Only the identity element has order 1.
    (c)

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

35. Answered in the text.

36. $|b| = 31$. To see this note that $ab = b^2a$. Then $ab^2 = (ab)b = b^2ab = b^2b^2a = b^4a$. Similarly, $ab^k = b^{2k}a$ for every $k = 1, 2, \ldots$ Then $a^2b = a(ab) = a(b^2a) = b^4a^2$ and $a^3b = a(b^4a^2) = b^8a^2$. Continuing we find that $a^nb = b^{2^n}a^n$. In particular since $a^5 = e$ we find that $b = a^5b = b^{32}a^5 = b^{32}$. Hence $b^{31} = e$. Then Theorem 7.8 implies that $|b|$ divides 31. Since $b \neq e$, conclude that $|b| = 31$.

37. $a^3b^3 = (ab)^3 = a(ba)^2b$ and therefore $a^2b^2 = (ba)^2$. Similarly $a^5b^5 = (ab)^5 = a(ba)^4b$ so that $a^4b^4 = (ba)^4$. Combine these equations to find: $a^4b^4 = (ba)^2(ba)^2 = a^2b^2a^2b^2$ which implies that $a^2b^2 = b^2a^2$. Then $b{\cdot}ba{\cdot}a = b^2a^2 = a^2b^2 = (ba)^2 = b{\cdot}ab{\cdot}a$. Conclude that $ba = ab$.

38. Suppose $(ab)^n = a^nb^n$ and $(ab)^{n+1} = a^{n+1}b^{n+1}$ for every $a,\ b \in G$. Note that $(ab)^{n+1} = ab{\cdot}ab{\cdot}ab{\cdot}ab$ $=$ a$\cdot ba{\cdot}ba{\cdot}{\cdot}{\cdot}ba{\cdot}$b $=$ a$(ba)^nb$. Apply this formula to get: $a(ba)^nb = (ab)^{n+1} = a^{n+1}b^{n+1} = a(a^nb^n)b$. Cancellation implies $(ab)^n = a^nb^n = (ba)^n$.

Now suppose $(ab)^{n+2} = a^{n+2}b^{n+2}$ holds as well. Then as above (ab) ${}^{"+1} = (ba)^{n+1}$. Therefore $ab{\cdot}(ab)^n = ba{\cdot}(ba)^n = ba{\cdot}(ab)^n$ and cancellation implies $ab = ba$.

39. (a) Fix an element $a \in G$. Define $\lambda_a : G \to G$ by $\lambda_a(x) = ax$. By hypothesis $\lambda_{a}.$ is injective and since G is finite we conclude λ_a is also subjective. (See Exercise 32 of Appendix B.) Therefore there exists $e \in G$ with $ae = a$. Then for every $x \in G$, $aex = ax$ and cancellation implies $ex = x$ so that e is a "left identity". Similarly the map $p_a(x) = xa$ is surjective and mere exists f with $fa = a$ and $xf = x$ for every $x \in G$. Then $e = ef = f$ and hence this e is an identity element. By the subjectivity of those maps there exist elements a', $a'' \in G$ such that $aa' = e = a''a$. Then $a' = ea' = a''aa' = a''e = a''$ so that a' is an inverse for a. Therefore G is a group.

(b) The set of positive integers under addition provides an example.

40. If $x \in G$ write x' for an element such that $x'x = e$. Claim. If $x^2 = x$ then $x = e$.
Proof. $e = x'x = x'x^2 = (x'x)x = ex = x$.

For any $a \in G$ we have $(aa')^2 = a(a'a)a' = aea' = aa'$. By the Claim it follows that $aa' = e$. Finally $ae = a(a'a) = (aa')a = ea = a$. Therefore G is a group.

41. (a) If $a \in G$, there exist elements $e, f \in G$ with $ae = a = fa$. Also there exist elements a', a'' $\in G$ with $aa' = e = a''a$. Proceed as in Exercise 37.

7.3 Subgroups

1. (a) Answered in the text.
   (b) $\langle 1\rangle = \{1\}$; $\langle 7\rangle = \langle 13\rangle = \{1, 7, 19, 13\}$; $\langle 19\rangle = \{1, 19\}$; $\langle 11\rangle = \{1, 11\}$; $\langle 17\rangle = \langle 23\rangle = \{1, 17, 19, 23\}$; $\langle 29\rangle = \{1, 29\}$.

2. (a) $\langle 1\rangle = \{1\}$; $\langle r_1\rangle = \langle r_3\rangle = \{r_0,\ r_1,\ r_2,\ r_4\}$; $\langle r_2\rangle = \{r_0,\ r_2\}$; $\langle d\rangle = \{r_0,\ d\}$; $\langle h\rangle = [r_0,\ h\}$; $\langle t\rangle = \{r_0,\ t\}$; $\langle v\rangle = \{r_0,\ v\}$.
   (b) D_4 itself is a subgroup which is non-cyclic. Also $H = \{r_0,\ r_2,\ d,\ t\}$ is a non-cyclic subgroup of D_4.

3. $I,\ a,\ a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 2 & 4 & 1 & 5 & 3 & 6 \end{pmatrix},\ a^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 6 & 3 & 5 & 7 & 1 \end{pmatrix},\ a^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 1 & 7 & 5 & 4 & 3 \end{pmatrix}$

   and $a^5 = I. = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 1 & 7 & 5 & 4 & 3 \end{pmatrix}$ and $a^5 = I$.

4. $\langle 2\rangle \subset \mathbb{Z}_{12}$ consists of all multiples of 2, so it is equal to $\{0, 2, 4, 6, 8, 10\}$.

5. $\langle 2\rangle \subset \mathbb{Z}$ consists of all multiples of 2, so it is the set of even integers.

6. Multiplying, we get

$$2^2 = 4, \quad 4 \cdot 2 = 8, \quad 8 \cdot 2 = 16 \equiv 5 \pmod{11}, \quad 5 \cdot 2 = 10, \quad 10 \cdot 2 = 20 \equiv 9 \pmod{11}$$
$$9 \cdot 2 = 18 \equiv 7 \pmod{11}, \quad 7 \cdot 2 = 14 \equiv 3 \pmod{11}, \quad 3 \cdot 2 = 6, \quad 6 \cdot 2 = 12 \equiv 1 \pmod{11}.$$

Thus
$$\langle 2 \rangle = \{2, 4, 8, 5, 10, 9, 7, 3, 6, 1\} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\},$$
which is the entire multiplicative group of nonzero elements of $\mathbb{Z}_{11}$.

7. $\langle 2 \rangle = \{2^k \mid k \in \mathbb{Z}\}$, which is the set
$$\{1, 2, 4, 8, 16, \dots\} \cup \{\frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots\}.$$

8. Multiplying, we get

$$3^2 = 9, \quad 9 \cdot 3 = 27 \equiv 5 \pmod{11}, \quad 5 \cdot 3 = 15 \equiv 4 \pmod{11}, \quad 4 \cdot 3 = 12 \equiv 1 \pmod{11}.$$

Thus
$$\langle 3 \rangle = \{1, 3, 4, 5, 9\}.$$

9. Answered in the text.

10. The multiples of (1, 0) provide all the elements (a, 0). The multiples of (0, 2) provide all the elements (0, b). Then every element (a, b) = (a, 0) + (0, b) can be generated.

11. Answered in the text.

12. Every element g in this group has $4g = (0, 0)$. Therefore (g) can contain at most 4 elements. The elements (1, 0) and (0, 1) generate the group.

13. Answered in the text.

14. (a) In U_8 let $H = \langle 3 \rangle = \{1, 3\}$ and $K = \langle 5 \rangle = \{1,5\}$. Then $H \cup K = \{\text{I}, 3, 5\}$ is not closed.
(b) If $H \subseteq K$ then $H \cup K = K$ and if $K \subseteq H$ then $H \cup K = H$. Conversely suppose $H \cup K$ is not in H or K. Choose x, $y \in H \cup K$ with $x \notin H$ and $y \notin K$. Then $y \in H$ and $x \in K$.
Claim, $xy \notin H \cup K$.
Proof. If $xy \in H$ then $x \in Hy^{-1} \subseteq H$. If $xy \in K$ then $y \in x^{-1}K \subseteq K$. Therefore $H \cup K$ is not closed.

15. (a) Answered in the text.
(b) If a, $b \in \cap H_i$ then a, $b \in H_i$ for every i. Therefore ab, $a^{-1} \in H_i$ for every i so that they lie in the intersection. By Theorem 7.10 this intersection is a subgroup.

16. Suppose (g, h), $(g', h') \in G_1 \times H_1$. Then $(g, h)(g', h') = (gg', hh')$ and $(g, h)^{-1} = (g^{-1}, h^{-1})$ lie in $G_1 \times H_1$. Therefore it is a subgroup.

17. If g is a generator then there exists some $m \in \mathbb{Z}$ with $mg = 1$. But this can be read as an equation in the ring $\mathbb{Z}$ and the only solutions are $m = g = \pm$ l.

18. Let $H = \langle (3, 1), (-2, -1), (4,3) \rangle$. Then $(1,0) = (3, 1) + (-2, -1)$ lies in H and $(0,1) = (4, 3) + 2 \cdot (-2, -1)$ lies in H. It follows that every $(a, b) = a \cdot (\text{l}, 0) + b(0, 1)$ lies in H.

19. If a, $b \in T$ then $a^{-1} \in T$ by Exercise 7.2.26 and $ab \in T$ be Exercise 7.2.29. Therefore T is a subgroup by Theorem 7.10.

20. Note that $|a|$ divides k if and only if $a^k = \mathrm{e}$, as in Theorem 7.8. If a, $b \in H$ then $a^k = b^k = e$ and therefore $(ab)^k = a^k b^k = e$ and $(a^{-1})^k = (a^k)^{-1} = e$. That is, ab, $a^{-1} \in H$ so that H is a subgroup by Theorem 7.10.

21. (a) No. In any group G we have $gg^{-1} = e \in Z(G)$. To get a counterexample choose G and $g \notin Z(G)$.

    (b) If $ab \in Z(G)$ then $(ab)x = x(ab)$ for every x. In particular, $ba = a^{-1}(ab)a = (ab)a^{-1}a = ab$.

22. By exercise 7.2.17, gag^{-1} has order 2, and the uniqueness implies $gag^{-1} = a$. Then $ga = ag$ for every $g \in G$ so that $a \in Z(G)$.

23. Since $a^n = (a^{-1})^{-n}$, every power of a is also a power of a^{-1}. The converse also follows.

24. Suppose $\mathbb{Q}^{**} = \langle r \rangle$ is cyclic. Since $\langle r \rangle = \langle r^{-1} \rangle$ by Exercise 14 we may assume $r > 1$. Then $\cdots r^{-2} < r^{-1} < 1 < r < r^2 < r^3 < \cdots$ and this list must include all positive rationals, since r is a generator. But there is a positive rational number between 1 and r. This contradiction shows that the group cannot be cyclic. (Can $\mathbb{Q}^{**}$ be generated by some finite subset?)

25. Let $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Then $\alpha\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $\sigma\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ so that neither α nor β lies in the center. Since the center is a subgroup it also follows that $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ is not in the center. Similar calculations with $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ show that $\beta\sigma \neq \sigma\beta$ and $\gamma\sigma \neq \sigma\gamma$. Therefore e is the only element in die center.

26. (a) If ab and $a'b'$ are elements of HK then $(ab)(a'b') = (aa')(bb')$ and $(ab)^{-1} = b^{-1}\,a^{-1} = a^{-1}\,b^{-1}$ lie in HK. Therefore HK is a subgroup.

    (b) Use $G = S_3$ and $H = \langle a \rangle$ and $K = \langle b \rangle$, where $a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Then $HK = \{1, a, b, ab\}$ does not contain ba.

27. Answered in the text.

28. (a) If a, $b \in H$, then $(ab^{-1})^n = a^n(b^n)^{-1} = e$ so that $ab^{-1} \in H$. By Exercise 23 H is a subgroup.

    (b) When $n = 2$ and $G = S_3$ show that $H = \left\{ e, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$, a subset not closed under the operation.

29. Answered in the text.

30. If f, $g \in H$ then for every $t \in T_1$ we have $(fg)(t) = f(g(t)) = f(t) = t$ and also $f^{-1}(t) = t$ Therefore fg and $f^{-1} \in H$ so that H is a subgroup.

31. If f, $g \in K$ then $(fg)(T_1) = f(g(T_1)) = f(T_1) = T_1$ and, by the definition of "inverse function", $f^{-1}(T_1) = T_1$. Hence K is a subgroup. By the definitions $H \subseteq K$. If a, $b \in T_1$ are distinct elements let $\alpha \in A(T)$ be defined by setting $\alpha(a) = b$, $\alpha(b) = a$ and $\alpha(x) = x$ for every $x \neq a$, b. Then $\alpha \in K$ but $\alpha \notin H$.

32. Applying the hypothesis to the element x^{-1}, note that $xHx^{-1} \subseteq H$. Multiplying by x^{-1} on the left and x on the right we get $H \subseteq x^{-1}Hx$. Hence these sets are equal.

33. If g, $h \in C(a)$ then $ga = ag$ and $ha = ah$. Then $ag^{-1} = g^{-1}a$ and $(gh)a = a(gh)$. Therefore $C(a)$ is a subgroup.

34. $g \in Z(G)$ if and only if $ag = ga$ for every $a \in G$. This occurs if and only if $g \in C(a)$ for every $a \in G$. Equivalently, $g \in \cap\ C(a)$.

35. $a \in Z(G)$ if and only if $ax = xa$ for every $x \in G$. This occurs if and only if every $x \in G$ lies in $C(a)$. Equivalently, $C(a) = G$.

36. False. U_8 and S_3 are counter examples.

37. Since $(k, n) = 1$, we may choose r and s such that $rk + sn = 1$. Then since a has order n, we know that $a^n = e$, so that

$$a = a^1 = a^{rk+sn} = a^{rk}a^{sn} = (a^k)^r(a^n)^s = (a^k)^r e^s = (a^k)^r.$$

But $a^k \in H$, so that $(a^k)^r = a \in H$.

38. (a) U_p consists of all the nonzero elements of $\mathbb{Z}_p$ (by Corollary 7.3), so $|U_p| = p - 1$. By Theorem 7.15 the group U_p is cyclic, so $U_p = \langle g \rangle$ for some generator g of order $p - 1$. If $b \in U_p$ express $b = g^k$ for some integer k and note that $b^{p-1} = (g^k)^{p-1} = (g^{p-1})^k = 1$.
(b) If $(a, p) = 1$ then $[a] \in \mathbb{Z}_p$ is nonzero and $[a]^{p-1} = [1]$ by part (a). This means that $[a]^{p-1} \equiv [1]$ (mod p) and consequently $a^p \equiv a$ (mod p). If $(a, p) > 1$ then $p \mid a$ and $a = 0$ (mod p). In this case it is clear that $a^p \equiv a$ (mod p).

39. If x, $y \in N_H$ then $x^{-1}Hx = H$ and $y^{-1}Hy = H$. The first equation implies that $H = xHx^{-1}$. Also we have $(xy)^{-1}H(xy) = y^{-1}(x^{-1}Hx)y = y^{-1}Hy = H$. Therefore x^{-1} and xy lie in N_H so that N_H is a subgroup. Since H is a subgroup we know that $hH = Hh = H$ for every $h \in H$. It follows that $H \subseteq N_H$.

40. $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} aa' & aa'+b \\ 0 & 1 \end{pmatrix}$ so the set H is closed. Also $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} a & -ab \\ 0 & 1 \end{pmatrix}$ since $a^2 = 1$. Therefore H is a subgroup.

41. Answered in the text.

42. If $a \in U_n$ we must first check that the statement "$a \equiv 1$ (mod k) " makes sense. The element a is actually a class $[r]$ for some $r \in \mathbb{Z}$. But the same class a can be represented in other ways, say $a = [s]$ for $s \in \mathbb{Z}$. If $r \equiv 1$ (mod k) does it follow that $s \equiv 1$ (mod k) ? Yes, because $[r] = [s]$ so that $r \equiv$ s (mod n) and $n \mid (r - s)$. Now since $k \mid n$ conclude that $k \mid (r - s)$ and $r \equiv s$

(mod n). To stress this point, one can ask whether it makes any sense to consider the elements $a \in \mathbb{Z}_s$ such that $a \equiv 1$ (mod 2).

If $a,\ b \in H_k$ then $a, b \equiv l$ (mod k) and $ab \equiv l$ (mod k). By Theorem 7.11, H_K is a subgroup.

43. The case $\mathbb{Z}_{12}$ is answered in the text. Since $\mathbb{Z}_n$ is cyclic, the subgroups are all cyclic groups, by Theorem 7.16. The subgroups of $\mathbb{Z}_{20}$ are $\langle 1\rangle = \mathbb{Z}_{20}$, $\langle 2\rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18\}$, $\langle 4\rangle = \{0, 4, 8, 12, 16\}$, $\langle 5\rangle = \{0, 5, 10, 15\}$, $\langle 10\rangle = \{0, 10\}$ and $\langle 20\rangle =\{0\}$.

44. (a) If $m = dm_1$ then $a^m = (a^a)^{m_1}$ lies in $\langle a^a\rangle$ so that $\langle a^m\rangle \subseteq \langle a^a\rangle$. By Theorem 1.3 there exist integers u,v with $d = mu + nv$. Then $a^d = a^{mu}a^{nv} = (a^m)^u$ lies in $\langle a^m\rangle$ so that $\langle a^d\rangle \subseteq \langle a^m\rangle$.
(b) Apply part (a) to the case $d = 1$.

45. By Theorem 7.16 $H = \langle a^m\rangle$ for some m. By Exercise 38, $H = \langle a^d\rangle$ for some d dividing n. By Theorems 7.14 and 7.8 we conclude that $|H| = |a^d| = n/d$ is a divisorof n.

46. By Theorems 7,8 and 7.14, $H = \langle a^{n/k}\rangle$ has order k. If K is any subgroup of order k then as in Exercise 39, $K = \langle a^d\rangle$ for some $d \mid n$ and that $k = |K| = n/d$. Therefore $K. = H$.

47. Answered in the text, referring to Exercise 7.2.31.

48. If $G = \langle g\rangle$ is cyclic of infinite order, the equation $x^3 = g$ has no solution in G. (For if $x = g^n$ for some integer n then $g^{3n-1} = e$ implying that g has finite order.) However in $\mathbb{R}^*$ every equation $x^3 = g$ does have a solution. Alternatively, if $\mathbb{R}^*$ were cyclic then by Theorem 7.16, every subgroup would be cyclic. This would imply that $\mathbb{Q}^{**}$ is cyclic, contrary to Exercise 16.

49. Since $x \in G = \langle a\rangle$, we know that $x = na$ for some integer n. Thus $x + x = na + na = 2na = a$, so that $(2n - 1)a = e_G$. But this means that a has finite order, contradicting the assumption that G, an infinite cyclic group, is generated by a.

50. If $G = \langle a\rangle$ is a cyclic group of infinite order, using additive notation, then $2x = a$ has no solution in G. (Compare the proof in Exercise 42.) In the group Q every equation $2x = a$ has a solution.

51. The subset $G' = \{(g, e_H) \mid g \in G\}\}$ is easily seen to be a subgroup of $G \times H$, and therefore by Theorem 7.16 it is cyclic. If $(a,\ e_H)$ is a generator of this subgroup it follows that a is a generator of G so that G is cyclic. Similarly H is cyclic.

52. Let $g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ Using induction we can see that $g^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for every integer n. Therefore g is a generator of that subgroup.

53. Answered in the text in the case $(m,\ n) > 1$, If $(m,\ n) = 1$ then Exercise 41 shows that the group is cyclic.

54. If $e \neq a \in G$ then $\langle a\rangle$ is a subgroup of order > 1. Since it cannot be a proper subgroup, $G = \langle a\rangle$, If the order of a is infinite then $H = \langle a^2\rangle$ is a proper subgroup. Then $|a| = n$ is finite. If n is not prime then $n = rs$ for some integers $r,\ s > 1$. Then $H = \langle a^r\rangle$ is a subgroup of order s (by Theorem 7.8) so it is proper, The only remaining case is that n is prime.

55. No. If there were a generator $x+y\sqrt{2}$ then there would exist integers m, n with $m(x+y\sqrt{2})=1$ and $n(x+y\sqrt{2})=\sqrt{2}$. These imply that $mx = 1$, $my = 0$, $nx = 0$, $ny = 1$, which are impossible to satisfy.

56. $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$ has more than one subgroup of order 2 (generated by 9, 11 or 19). Therefore the group is not cyclic, by Exercise 40).

57. Answered in the text.

58. This is a restatement of Theorem 7.17.

7.4 Isomorphisms and Homomorphisms

1. Answered in the text.

2. Homomorphism. $f(xy) = \sqrt{xy} = \sqrt{x}\sqrt{y} = f(x)f(y)$.

   Injective. If $f(x) = f(y)$ then $\sqrt{x} = \sqrt{y}$ and squaring shows that $x = y$.

   Surjective. If $r \in \mathbb{R}^{**}$ then $f(r^2) = \sqrt{r^2} = r$.

3. The operation table for $GL(2,\mathbb{Z}_2)$ is

$\cdot$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$
$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$
$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$
$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$
$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$
$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$

and the operation table for S_3 is

$\cdot$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$
$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$
$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$
$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$
$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$
$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$	$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$	$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$

An examination of corresponding elements shows that the group tables are actually identical except for labeling.

4. It is 1-1 since $x^3 = y^3$ implies that $x = y$ for real numbers. It is onto since every real number has a cube root. Thus f is a bijection of sets. To see that it is a homomorphism, note that

$$f(xy) = (xy)^3 = x^3y^3 = f(x)f(y).$$

Since f is a bijective homomorphism, it is an isomorphism.

5. Since 2 is invertible in $\mathbb{Z}_9$ $(2^{-1} = 5)$, we see that g is 1-1, since if $g(x) = g(y)$, then $2x = 2y$, so that $5 \cdot 2x = 5 \cdot 2y$ and thus $x = y$. Since it is 1-1 and $\mathbb{Z}_9$ is finite, it is also surjective. It is a homomorphism since

$$g(x + y) = 2(x + y) = 2x + 2y = g(x) + g(y).$$

Since g is a bijective homomorphism, it is an isomorphism.

6. h is not injective since (for example) $h(4) = 2 \cdot 4 \equiv 0 \pmod 8$, so that $h(4) = h(0)$. Since it is not injective, and $\mathbb{Z}_8$ is finite, it cannot be surjective either. However, it is a homomorphism, since

$$h(x + y) = 2(x + y) = 2x + 2y = h(x) + h(y).$$

7. f is surjective, since if $x \in \mathbb{R}^{**}$, then $x > 0$ so that $x = |x|$ and thus $x = f(x)$. However, it is not injective since (for example) $f(-2) = f(2) = 2$. It is a homomorphism since

$$f(xy) = |xy| = |x| \cdot |y| = f(x)f(y).$$

8. f is injective, since if $2^x = 2^y$, then $2^{x-y} = 1$ so that $x - y = 0$ and then $x = y$. However, it is not surjective, since $2^x > 0$ for all $x \in \mathbb{R}$, so that the image of g is only $\mathbb{R}^{**}$. It is a homomorphism since

$$g(x + y) = 2^{x+y} = 2^x2^y = g(x)g(y).$$

9. It is obvious that f is surjective, since if $a \in G$, then $a = f((a, e_H))$. To see that f is a homomorphism, note that

$$f((a,b) * (c,d)) = f((a*c, b*d)) = a*c = f((a,b)) * f((c,d)).$$

10. This is not a homomorphism since (recalling that $\mathbb{R}$ is an additive group) $(x+y)^2 \neq x^2 + y^2$ in general. Thus $f(x+y) = (x+y)^2 \neq x^2 + y^2 = f(x) + f(y)$.

11. It is obviously an injective map, since if $x \neq y$ then $g(x) \neq g(y)$ since the matrices have different lower right entries. It is also clear that the image of the map actually lies in $GL(2, \mathbb{R})$ since any matrix of that form has a nonzero determinant. To see that it is a homomorphism, note that

$$g(x)g(y) = \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & xy \end{pmatrix} = g(xy).$$

12. It is obviously an injective map, since if $x \neq y$ then $h(x) \neq h(y)$ since the matrices have different lower right entries. It is also clear that the image of the map actually lies in $GL(2, \mathbb{R})$ since any matrix of that form has a nonzero determinant. To see that it is a homomorphism, note that

$$h(x)h(y) = \begin{pmatrix} 1 & 0 \\ x & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ y & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x+y & 0 \end{pmatrix} = h(x+y).$$

13. Answered in the text.

14. By Theorem 7.15, orcomputing the order of 3, the group U_7 is cyclic. Apply Theorem 7.18.

15. Answered in the text. For negative n recall from Theorem 7.19 that $f(a^{-1}) = f(a)^{-1}$. Use the result for positive n to get: $f(a^{-n}) = f((a^{-1})^n) = f(a^{-1})^n = (f(a)^{-1})^n = f(a)^{-n}$.

16. If a, $b \in H$ then $a = f(x)$ and $b = f(y)$ for some x, $y \in G$. Then $ab = f(x)f(y) = f(xy) = f(yx) = f(y)f(x) = ba$.

17. First note that f is well-defined; this is so because a has infinite order so that all of the a^k are distinct and therefore the power of a associated with any element of G is unique. Now, for $k \in \mathbb{Z}$, we see that $k = f(a^k)$, so that f is surjective. Further, if $f(a^k) = f(a^l)$, then $k = f(a^k) = f(a^l) = l$, so that $k = l$ and thus f is injective.

18. If α: $G \to G_1$ and $\beta : H \to H_1$ are isomorphisms, define the mapping $\varphi : G \times H \to G_1 \times H_1$ by $\varphi(x, y) = (\alpha(x), \beta(y)$. Check that φ is an isomorphism.

19. ($\Rightarrow$) Answered in the text.
($\Leftarrow$) Use the homomorphism property and the fact that $(a^{-1})^{-1} = a$ to show that for a, $b \in G$, $ab = f(a^{-1})f(b^{-1}) = f(a^{-1}b^{-1}) = f((ba)^{-1}) = ba$.

20. (a) By Theorem 7.11, to show that $a^{-1}Na$ is a subgroup of G it suffices to show that it is nonempty, that it is closed under the operation in G, and that it is closed under inverses. It is clearly nonempty since it contains at least $a^{-1}e_G a = e_G$. Now, if $a^{-1}n_1 a$ and $a^{-1}n_2 a$ are elements of $a^{-1}Na$, where $n_1, n_2 \in N$, then

$$(a^{-1}n_1 a)(a^{-1}n_2 a) = a^{-1}n_1(aa^{-1})n_2 a = a^{-1}n_1 n_2 a.$$

Since N is a subgroup, clearly $n_1 n_2 \in N$, so that the product above is in $a^{-1}Na$. Finally, given an element $a^{-1}na \in a^{-1}Na$, its inverse in G is $(a^{-1}na)^{-1} = a^{-1}n^{-1}(a^{-1})^{-1} = a^{-1}n^{-1}a$. Since N is a subgroup, we know that $n^{-1} \in N$, so it follows that $a^{-1}n^{-1}a \in a^{-1}Na$. Thus $a^{-1}Na$ is a subgroup.

(b) As the hint suggests, define $f : N \to a^{-1}Na : n \mapsto a^{-1}na$. f is clearly surjective. To see that it is injective, suppose $f(n) = f(m)$ for $m, n \in N$. Then $a^{-1}na = a^{-1}ma$. Multiplying on the left by a and on the right by a^{-1} gives $n = m$. It remains to show that f is a homomorphism. But for $m, n \in N$,

$$f(mn) = a^{-1}mna = a^{-1}maa^{-1}na = (a^{-1}ma)(a^{-1}na) = f(m)f(n).$$

Thus f is a bijective homomorphism, so is an isomorphism.

21. $g \circ f$ is injective since if $(g \circ f)(x) = (g \circ f)(y)$, then $g(f(x)) = g(f(y))$. But g is injective, so that $f(x) = f(y)$. Since f is also injective, we get $x = y$. Thus $g \circ f$ is injective. To see that it is surjective, choose $k \in K$. Since g is surjective, there is some $h \in H$ with $g(h) = k$. Since f is surjective, there is some $x \in G$ with $f(x) = h$. But then $(g \circ f)(x) = g(f(x)) = g(h) = k$ so that $g \circ f$ is surjective. Finally, to see that $g \circ f$ is a homomorphism, we have (since both f and g are homomorphisms)

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)(g \circ f)(y).$$

22. f restricts a map f_1: $T \to H$, which is still an injective homomorphism. By Theorem 7.19 $f(T) = f_1(T) = Im\, f_1$ is a subgroup of H and f_1 induces an isomorphism $T \cong f(T)$.

23. (a) We need to show that $f(ab) = f(a)f(b)$. But $f(ab) = (ab)^2 = abab$. Since G is abelian, $abab = aabb = a^2b^2 = f(a)f(b)$ and we are done.

(b) If G is nonabelian, then there are two elements $a, b \in G$ such that $ab \neq ba$. Then $f(ab) = (ab)^2 = abab$ while $f(a)f(b) = a^2b^2 = aabb$. If these two are equal, i.e., if $abab = aabb$, multiply on the left by a^{-1} and on the right by b^{-1} to get $ba = ab$ in contradiction to our assumption. Thus f cannot be a homomorphism, since for these elements $f(ab) \neq f(a)f(b)$.

24. (a) See Exercise 7.1.19.
(b) Define f: $G \to G^{op}$ by $f(x) = x^{-1}$. This f is objective since $f \circ f = \tau$ is the identity map.
Homomorphism. $f(xy) = (xy)^{-1} = y^{-1}\, x^{-1} = f(y)f(x) = f(x) * f(y)$.

25. We first show that f is well-defined. If G is infinite then an element $g \in G$ is uniquely represented as $g = a^m$ for some $m \in \mathbb{Z}$. Then mere is no ambiguity in defining $f(a^m) = b^m$. Since b is also a generator we see that f is an isomorphism. The homomorphism property follows from the rules of exponents.

If $|G| = n$ is finite this representation $g = a^m$ is not unique. The proof of Theorem 7.18 shows that if a is a generator of G, there is an isomorphism φ_{a}: $\mathbb{Z}_n \to G$ with $\varphi_a(1) = a$. Defining $f = \varphi_b \circ \varphi^{-1}_a$: $G \to G_1$ we conclude that f is an isomorphism and $f(a) = \varphi_b(1) = b$.

26. If $h \in H$ then, by subjectivity, $h = f(a^n)$ for some integer n. Then by Exercise 11, $h = f(\mathrm{a})^n$ lies in $\langle f(a)\rangle$.

27. (a) Closure is clear.
Associative. $x*(y*z) = xc(ycz)$ and $(x*y)*z = (xcy)cz$.
Identity, c^{-1} is the identity element for *. Here the exponent −1 refers to the inverse in the group G.
Inverses;. For any $x \in H$ the inverse is $c^{-1}x^{-1}c^{-1}$.
(b) The map $g : H \to G$ defined $g(x) = cx$ is die inverse of f. Therefore f is bijective.
Homomorphism. $f(xy) = c^{-1}\ xy = (c^{-1}\ x)c(c^{-1}\ y) = f(x)cf(y) = f(x)*f(y)$.

28. (a) If a has order k, that means that $a^k = e$. Then by Exercise 15, $f(a)^k = f(a^k) = f(e) = e$ (Theorem 7.20(1)).
(b) By Theorem 7.9, since $f(a)^k = e$, the order of $f(a)$ divides k. But $k = |a|$, so that $|f(a)|$ divides $|a|$.

29. Answered in the text.

30. Let $T = \{a \in G\ [f(a) \in K\}$. If $a,\ b \in T$ then $f(a),\ f(b) \in K$ so that $f(ab) = f(a)f(b) \in K$. Therefore $ab \in T$. Similarly $f(a^{-1}) = f(a)^{-1} \in K$ so that $\mathrm{a}^{-1} \in T$. Therefore T is a subgroup.

31. By Theorem 7.11, in order to show that F is a subgroup of G it suffices to show it is nonempty, closed under the operation of G, and closed under inverses. It is obviously nonempty, since for example $f(e) = e \in F$. To see that it is closed under the operation of G, choose $a, b \in F$. Then since f is a homomorphism, $ab = f(a)f(b) = f(ab)$, so that ab is also fixed by f and thus lies in Finally, if $a \in F$, then $f(a^{-1}) = f(a)^{-1} = a^{-1}$ (since $a \in F$), so that $a^{-1} \in F$ as well.

32. f is clearly surjective, since if $a \in \mathbb{R}^*$, then

$$f\left(\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}\right) = \det \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a \cdot 1 - 0 = a.$$

To see that f is a homomorphism, suppose

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \text{and} \qquad B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

are two matrices in $GL(2, \mathbb{R})$. Then

$$AB = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix},$$

so that

$$\begin{aligned} \det(AB) &= (ae+bg)(cf+dh) - (af+bh)(ce+dg) \\ &= (acef + adeh + bcfg + bdgh) - (acef + adfg + bceh + bdgh) \\ &= adeh + bcfg - adfg - bceh. \end{aligned}$$

But

$$\det(A)\det(B) = (ad - bc)(eh - fg) = adeh - bceh - adfg + bcfg$$

and the two are equal. Thus $\det(AB) = \det(A)\det(B)$ and det is a surjective homomorphism.

33. To show that K_f is a subgroup of G it suffices to show that it is nonempty, closed under the operation of H, and closed under inverses (Theorem 7.11). Clearly $f(1_G) = 1_H$, so that $1_G \in K_f$ and thus K_f is nonempty. Now, suppose $a, b \in K_f$. Then since f is a homomorphism, $f(ab) = f(a)f(b) = 1_H 1_H = 1_H$, so that $ab \in K_f$ as well. Finally, if $a \in K_f$, then $f(a^{-1}) = f(a)^{-1} = e_H^{-1} = e_H$, so that $a^{-1} \in K_f$. Thus K_f is a subgroup of G.

34. $[x] = [0]$ if $x - 0$ is a multiple of 5, i.e., if x is a multiple of 5. Thus K_f is the set of multiples of 5, which is $\{\ldots,\ -10,\ -5,\ 0,\ 5,\ 10,\ \ldots\}$.

35. U_5 is the multiplicative group whose elements are $\{1, 2, 3, 4\}$ and whose operation is given by multiplication modulo 5. Its identity is 1. Since $1^2 = 1$, $2^2 = 4$, $3^2 = 9 \equiv 4 \pmod 5$, and $4^2 = 16 \equiv 1 \pmod 5$, we have $K_f = \{1, 4\}$.

36. If f, $g \in Aut(G)$ then $f \circ g \in Aut(G)$ by Exercise 9. Therefore $Aut(G)$ is closed under composition. The identity map lies in $Aut(G)$ and inverses exist there by Exercise 22. The associative law is automatic for compositions of functions.

37. Answered in the text.

38. Let $\alpha : \mathrm{T} \to \{1, 2, \ldots . \mathrm{n}\}$ be a bijection (a relabeling). If $\sigma \in A(T)$ then define $f(\sigma) \in S_n = \mathrm{A}(\{1{,}2, \ldots . \mathrm{n}\})$ by $f(\sigma) = \alpha \circ \alpha \circ \alpha^{-1}$. Check that $f : A(T) \to S_n$ is an isomorphism.

39. $\mathbb{Z}$ is cyclic but $\mathbb{Q}$ is not, by Exercise 7.3.43.

40. $\mathbb{Z}_6$ is abelian and S_3 is not. Apply Exercise 10.

41. $\mathbb{Z}_4 \times \mathbb{Z}_2$ is abelian and D_4 is not. Apply Exercise 10.

42. $\mathbb{Z}_4 \times \mathbb{Z}_2$ has an element of order 4 and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ does not. Apply Exercise 21.

43. Answered in the text.

44. Every element of U_{12} satisfies $x^2 = 1$ but U_{10} has elements of order 4. Apply Exercise 21.

45. Answered in the text.

46. In the additive group $\mathbb{R}$, every nonzero element has infinite order (for if $nx = 0$ for some positive integer n then $x = 0$). However in $\mathbb{R}^*$ the element –1 has order 2. Apply Exercise 21.

47. D_4 has 5 elements of order 2 and the quaternion group has only one element of order 2. Apply Exercise 21.

48. For every $a \in \mathbb{Q}$ there exists $x \in \mathbb{Q}$ such that $2x = a$. If there were an isomorphism to $\mathbb{Q}^{**}$ then for every $r \in \mathbb{Q}$ there would exist $s \in \mathrm{Q}^{**}$ such that $s^2 = r$. When $r = 2$ for example this is false.

49. If $c \in G$ define $g(c) \in Aut(G)$ by: $g(c)(x) = cxc^{-1}$. Then $g(cd)(x) = (cd) \times (cd)^{-1} = cdxd^{-1}c^{-1} = c(g(d)(x))c^{-1} = g(c)(g(d)(x)) = (g(c) \circ g(d))(x)$. Since this holds for every x we conclude: $g(cd) = g(c) \circ g(d)$. Note. Defining $h : G \to Aug(G)$ by: $h(c)(x)= c^{-1}xc$, yields: $h(cd) = h(d) \circ h(c)$.

50. For every $a, x \in G$ we have $h(ax) = h \circ \varphi_a(x) = \varphi_a \circ h(x) = ah(x)$. Apply this to $x = e$ to find $h(a) = ah(1)$. Define $b = h(l)^{-1}$ and conclude that: $h(a) = ab^{-1}$ for every $a \in G$.

51. (a) Answered in the text.
(b) Injective. If $h(c) = h(d)$ then $\theta_c = \theta_d$ so that $c^{-1} = \theta_c(1) = \theta_d(1) = d^{-1}$ and therefore $c = d$. Homomorphism. For any $c, d, x \in G$ we have: $\theta_{cd}(x) = x(cd)^{-1} = xd^{-1}c^{-1} = \theta_d(x)c^{-1} = \theta_c(\theta_d(x)) = (\theta_c \circ \theta_d)(x)$. Therefore $h(cd) = \theta_{cd} = \theta_c \circ \theta_d = h(c) \circ h(d)$. By Theorem7.19 G ≅ 1m h.

52. (a) $\varphi_0 = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 2 \end{pmatrix}, \varphi_1 = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}, \varphi_1 = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 0 & 1 \end{pmatrix}$.
(b) $\varphi_0 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 \end{pmatrix}, \varphi_1 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix}, \varphi_2 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix}, . \varphi_3 = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix}$
(c) To get reasonable notations, label the elements of S_3 by the six symbols 1, 2, 3, 4, 5, 6 in some order, and compute the action of each left multiplication as an element of S_6. The details are left to the reader.

53. The argument in Exercise 3.3.27 works the same here.

54. (a) Each $\sigma \in D_3$ is a rigid motion carrying the given triangle to itself. Then σ carries a vertex to a vertex, so it permutes the 3 vertices. Labeling the vertices 1, 2, 3, the restriction map induces a map $f : D_3 \to S_3$. Since $f(\sigma)$ is just the restriction of σ to the set of vertices it is clear that f is a homomorphism. Two symmetries of the triangle which are identical on the three vertices must be the same. (Why?) Therefore f is injective. Since $|D_3| = |S_3|$, f is also subjective.
(b) Each $\sigma \in D_4$ carries a vertex of the given square to another vertex, so the restriction map induces a homomorphism $f : D \to S_4$. A symmetry of the square which fixes all 4 vertices must be the identity. It follows that this f is injective. By Theorem 7.19 D_4 is isomorphic to Im f which is a subgroup of S_4.

55. (a) Define $\alpha : \mathbb{Z} \to$ GL(2, $\mathbb{Q}$) by $\alpha(n) = \begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix}$. Then Im α equals the given set H.

Express $\alpha(n) = I + nP$ where I is the identity matrix and $P = \begin{pmatrix} -1 & -1 \\ 1 & 1 \end{pmatrix}$. Since $P^2 = 0$,

calculate: $\alpha(n)\alpha(m) = (I + nP)(I + mP) = I + nP + mP = I + (n + m)P = \alpha(n + m)$.

Therefore α is a homomorphism and Theorem 7.19 implies that $H = Im\ \alpha$ is a group.
(b) By definition, $\alpha : \mathbb{Z} \to H$ is a subjective homomorphism. Injective. If $\alpha(n) = \alpha(m)$ then $I + nP = I + mP$ so that $(n - m)P = 0$, Since $P \neq 0$ conclude that $n = m$.

56. (a) Define β: $\mathbb{Z} \to GL(2, \mathbb{Q})$ by $\beta(n) = I + nQ$ where $Q = \begin{pmatrix} -2 & 1 \\ -4 & 2 \end{pmatrix}$. Since $Q^2 = 0$, check that β is a homomorphism. Since $K = Im\ \beta$, Theorem 7.19 implies that K is a group.
(b) Yes. β is a subjective homomorphism. Check that it is injective, as in Exercise 37.

57. Define $\varphi : \mathbb{Z}[x] \to \mathbb{Q}^{**}$ as in the Hint.
Homomorphism. $\varphi\left(\sum a_k x^k\right) \cdot \varphi\left(\sum b_k x^k\right) = \varphi\left(\prod_{p_k}^{a_k}\right) \cdot \left(\prod_{p_k}^{b_k}\right) = \prod_{p_k}^{a_k+b_k}$ by the rules of exponents. By the definition of addition of polynomials we also have $\varphi\left(\sum a_k x^k\right) + \left(\sum b_k x^k\right) = \varphi\left(\sum(a_k + b_k)x^k\right) = \prod_{p_k}^{a_k+b_k}$.
Subjective. Every positive rational number can be expressed as some $\prod_{p_k}^{a_k}$ for some $a_k \in \mathbb{Z}$ (where $a_k = 0$ for all large values of k). To see this just factor the numerator and denominator and use the rules of exponents.
Injective. To show: if $\prod_{p_k}^{a_k} = 1$ (where $a_k = 0$ for all large k) then $a_k = 0$ for every k. To prove this clear denominators and apply the Unique Factorization Theorem for positive integers.

58. As in Exercise 33 let $g(c)$ be the inner automorphism induced by c. If G is abelian then $g(c)(x) = cxc^{-1} = xcc^{-1} = x$ so $g(c) = \iota_G$ the identity map. Therefore Inn $G=\{\iota_G\}$. Conversely if Inn G has just one element then $g(c) = \iota_G$ for every c. This means that for every c, $x \in G$ we have $cxc^{-1} = g(c)(x) = x$. Therefore $cx = xc$ and G is abelian.

59 (a) Let $g : D_4 \to$ Inn D_4 be the function defined in Exercise 33. Check directly from the operation table that $g(r_2) = \iota_G$. Since $r_1^{-1}r_3 = r_2$, $h^{-1}v = r_2$ and $d^{-1}t = r_2$ we get that $g(r_1) = g(r_3)$, $g(h) = g(v)$ and $g(d) = g(t)$. Check from the table that none of these 3 automorphisms equals ι_G. Therefore Inn $D_4 = \{\iota_G, g(r_1), g(h), g(d)\}$ is a group of exactly 4 elements.
(b) Since $r_1^{\ 2} = r_2$ and $h^2 = d^2 = \iota_G$. conclude that $H = Inn\ D_4$ is a group of order 4 with $x^2 = e$ for every $x \in H$. Constructing the operation table of any such group H, check that $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

60. If $f \in Aut\ \mathbb{Z}$ then $f(1)$ is a generator (by Exercise 18). Therefore $f(1) = \pm$, by Exercise 7.3.19. If $f(1) = 1$ then $f(n) = n$ and $f = i$ is the identity map. If $f(1) = -1$ then $f(n) = -n$ and $f = -\iota$ (as in Exercise 17). Therefore $Aut\ \mathbb{Z} = \{\iota, -\iota\} \cong \mathbb{Z}_2$.

61. If $k \in U_n$ define $\varphi_k : Z_n \to Z_n$ by $\varphi_k(x) = kx$. Then φ_k is a homomorphism (by the distributive law), and φ_k is bijective since k is invertible in $\mathbb{Z}_n$. Then $\varphi_k \in Aut\ \mathbb{Z}_n$. Since $\varphi_k = \varphi_i \circ \varphi_k$, the map $\varphi : U_n \to Aut\ Z_n$ is a homomorphism. Injective. If $\varphi_i = \varphi_k$ then $j = \varphi_i(1) = \varphi_k(1) = k$. Subjective. Suppose $f \in Aut\ Z_n$. Then $f(1)$ is a generator of $\mathbb{Z}_n$ by Exercise 18. By Exercise 7.3.38(b), the generators of $\mathbb{Z}_n$ are exactly the elements $k \in U_n$. Therefore $f(l) = k$ for some $k \in U_n$ and it follows that $f(x) = kx$ for every x (compare Exercise 19). Therefore $f = \varphi_k$ and φ is subjective.

62. If $\alpha \in Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ then $\alpha(0) = 0$ so α permutes the three nonzero elements. This restriction map provides a homomorphism $f : Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \to S_3$. It is injective (if two automorphisms coincide on the nonzero elements they must be equal). It remains to show that these 6 permutations actually are automorphisms.

Suppose H is any additive group of 4 elements generated by elements x, y with $2x = 2y = 0$. Then $H = \{0, x, y, x + y\}$. Since $y + x$ cannot equal e, x or y it must equal $x + y$. Also $2(x + y) = 2x + 2\underline{y} = 0$. Comparing operation tables, conclude that there is an isomorphism $\varphi : H \to \mathbb{Z}_2 \times \mathbb{Z}$ with $\varphi(x) = (1, 0)$ and $(\varphi(y) = (0, 1)$.

Apply this to the case $H = \mathbb{Z}_2 \times \mathbb{Z}_2$ where the elements x, y are any 2 of the 3 nonzero elements. Each of the 6 choices of x, y provides an automorphism. Therefore the map f above is bijective.

An alternative approach to this problem is to argue that $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong GL(2, \mathbb{Z}_2)$ and work directly with matrices. Compare Exercise 3.

7.5 The Symmetric and Alternating Groups

1. (a) (173) (b) (1245789) (c) (1476283) (d) (35798)

2. (a) (1234) (b) (1356247) (c) (14532) (d) (12453)

3. (a) (12)(45)(679) (b) (13)(254)(789) (c) (13)(254)(69)(78)
(d) (1573)(24) (e) (123)(456)(78)

4 (a) (12)(45)(69)(67) (b) (13)(24)(25)(79)(78) (c) (13)(24)(25)(69)(78)
(d) (13)(17)(15)(24) (e) (13)(12)(46)(45)(78)

5. (a) Since $(12)(12) = e$, $|(12)| = 2$.

(b) We have $(123)(123) = (132)$, and $(123)(132) = e$, so that $|(123)| = 3$.

(c) We have $(1234)(1234) = (13)(24)$, $(1234)(13)(24) = (1432)$, $(1234)(1432) = e$, and therefore $|(1234)| = 4$.

(d) $|(123456789)| = 9$.

6. (a) $(13)(24)(13)(24) = e$, so $|(13)(24)| = 2$.

(b) We have

$$((123)(456))^2 = (123)(456)(123)(456) = (132)(465)$$
$$((123)(456))^3 = (132)(465)(123)(456) = e.$$

Thus $Abs(123)(456) = 3$.

(c) We have

$$((123)(435))^2 = (123)(435)(123)(435) = (13425)$$
$$((123)(435))^3 = (13425)(123)(435) = (15243)$$
$$((123)(435))^4 = (15243)(123)(435) = (14532)$$
$$((123)(435))^5 = (14532)(123)(435) = e.$$

Thus $|(123)(435)| = 5$.

(d) Since (1234)(4231) = (132), we want to know the order of (132). But

$$(132)^2 = (132)(132) = (123), \qquad (132)^3 = (123)(132) = e,$$

so that $|(1234)(4231)| = |(123)| = 3$.

(e) Since (1234)(24)(43215) = (13)(45), we want the order of (13)(45). But $(13)(45)(13)(45) = e$, so the order is 2.

7. (b) and (c) are even.

8. (a) {e} (b) {e, (123), (132)}
(c) {e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)}

9. (a) 3 (b) 12 (c) 60 (d) $10\,{}^1\!/_2$=1814400

10. No, B_n is not a subgroup of S_n. B_n consists of those permutations that can be written as a product of an odd number of transpositions. But then a product of any two elements of B_n can be written as a product of an even number of transpositions (since the product is just the transpositions of the two elements written one after the other). Thus the product of any two elements of B_n is even, so is not in B_n. (It is also valid to simply observe that the identity permutation is even, so is not in B_n, so that B_n cannot be a subgroup).

11. The elements (12)(34), (13)(24), and (14)(23) each have order 2. The elements (123), (132), (124), (142), (134), (143), (234), and (243) each have order 3. Finally, the identity element has order 1.

12. For example, (12)(34) = (314)(123).

13. Multiplying (123)(234) gives (123)(234) = (12)(34), so this is the product of two disjoint transpositions. Multiplying the other pair of cycles gives (567)(789 10) = (56789 10). Thus α can be written as a product of disjoint cycles as $\alpha = (12)(34)(56789\ 10)$. The cycles have orders 2, 2, and 6, so that $|\alpha| = \operatorname{lcm}(2, 2, 6) = 6$.

14. Multiplying out the cycles in β gives $\beta = (1236784)(59\ 10)$. Thus β is the product of a 3-cycle and a 7-cycle, so that $|\beta| = \operatorname{lcm}(3, 7) = 21$.

15. Answered in the text.

16. If $\sigma = (a_1 a_2 \ . \ . \ . \ a_k)$ then $\sigma(a_j) = a_{j+1}$ where the subscripts are read modulo k as before. Then $\sigma^{-1}(a_{j+1}) = a_j$, and in cycle notation $\sigma^{-1} = (a_1 a_{k-1} \ . \ . \ . \ a_2 a_1) = (a_1 a_k a_{k-1} \ . \ . \ . \ a_2)$.

17. *If* $\sigma = (a_0, a_1, a_2, \ . \ . \ . \ a_{k-1})$ then $\sigma(a_j) = a_{j+1}$ where the subscripts are viewed as integers modulo k (so that $\sigma(a_{k-1}) = a_0$). Therefore $\sigma^r(a_j) = a_{j+r}$. Therefore $\sigma^r =$ e if and only if $j + r \pmod{k}$ for every j. This occurs if and only if $r = 0 \pmod{k}$. Therefore $|\sigma| = k$.

18. If $i = a_r$ then $\sigma\tau(i) = \sigma(i) = \tau\sigma(i)$. If $i = b_s$ then $\sigma\tau(i) = \tau(i) = \tau\sigma(i)$. Finally if i is not one of the a′s or b′s then $\sigma\tau(i) = i = \tau\sigma(i)$.

19. Suppose $\tau = \sigma_1\ \sigma_2\ .\ .\ .\ \sigma_r$ a product of disjoint cycles, where σ_j is a k_j-cycle. Since these commute (by Exercise 12), $\tau^n = \sigma_1^n\sigma_2^n\ .\ .\ .\ \sigma_r^n$. Claim. $\tau^n = e$ if and only if $\sigma_j^n = e$ for each Proof. ($\Leftarrow$) Easy. ($\Rightarrow$) Suppose $\tau_j = (c_1c_2\ .\ .\ .\ c_{kj})$. Then the other σ's fix these c_i.'s and c $\tau^n(c_i) = \sigma_j^n(c_i)$. Therefore $\sigma_j^n = e$.

By Exercise 9, $\sigma_j^n = e$ if and only if $k_j \mid n$. Then $|\tau|$ is the smallest $n > 0$ where $k_j \mid n$ every j. This is exactly the least common multiple of $k_1, k_2, \ldots, k_r$.

20. (a)

α	β	$\alpha\beta\alpha^{-1}$	$\alpha\beta\alpha^{-1}\beta^{-1}$
even	even	even	even
even	odd	odd	even
odd	even	even	even
odd	odd	odd	even

(b) The conjugate of an even permutation by any permutation is again even, and the conjugate of an odd permutation by any permutation is again odd. The product $\alpha\beta\alpha^{-1}\beta^{-1}$ is always even.

21. $\sigma = (138)(27)(4965)$ so $|\sigma| = 12$, the 1cm of 3, 2 and 4. Then $\sigma_{1000} = \sigma_{4\,+\,12.83} = \sigma_4$ has order 3 by Theorem 7.8.

22. An element of order 10 is, for example, (12345)(67), since this is the disjoint product of a 5-cycle and a 2-cycle and $\text{lcm}(5, 2) = 10$. An element of order 20 is, for example, (12345)(6789), since this is the disjoint product of a 5-cycle and a 4-cycle, and $\text{lcm}(5, 4) = 20$. An element of order 30 is, for example, (12345)(67)(89 10), since this is the disjoint product of a 5-cycle, a 3-cycle, and a 2-cycle, and $\text{lcm}(5, 3, 2) = 30$. There is no element of order 40: note that any such element must have either a 5-cycle or a 10-cycle in its disjoint cycle representation in order for the least common multiple of the cycle components to be 40. If it has a 10-cycle, then this is the complete element since we are working in S_{10}, and this element has order 10. If it has a 5-cycle, then the remaining 5 element must combine to give an 8-cycle, but the maximum cycle length from 5 elements is $6 = \text{lcm}(2, 3)$. Thus there is no element of order 40.

23. Let K be that subset. It is easy to verify that K is closed under composition, hence it is a subgroup. Furthermore since there are only 4 symbols involved, a direct count shows that K contains every $\alpha \in S_4$ which is the product of 2 disjoint 2-cycles. If $\sigma \in S_4$ then $\alpha(12)(34)\sigma^1 = (\sigma(1)\sigma(2))(\sigma(3)\sigma(4))$ is also a product of 2 disjoint 2 cycles, using Exercise 23. Therefore this element lies in K. Similarly we conclude that $\sigma K\sigma^1 \subseteq K$ so that K is normal by Theorem 7.21.

24. (a) Suppose that $f(\alpha) = f(\beta)$. Then $(12)\alpha = (12)\beta$, so (working in S_n), $\alpha = (12)(12)\alpha = (12)(12)\beta = \beta$, so that $\alpha = \beta$. Hence f is injective.

(b) Choose $\beta \in B_n$. Then β can be written with an odd number of transpositions, so that $(12)\beta$ can be written with an even number of transpositions. Thus $(12)\beta \in A_n$, and $f((12)\beta) = (12)(12)\beta = \beta$. Thus f is surjective. Since f is both injective and surjective, it follows that A_n and B_n have the same number of elements.

25. Answered in the text.

26. Suppose α is in the center of S_n and $\alpha \neq e$. Then there exists i where $\alpha(i) = j \neq i$. Since n > 2 there is some k where i, j, k are distinct. Evaluating $\alpha \circ (i, k) = (i, k) \circ \alpha$ at i shows that $\alpha(k)$ = j contrary to the injectivity of α. Therefore $\alpha = e$.

27. By Exercise 9, $\sigma^{k} = e$. Let $\tau = \sigma^{(\mathrm{k}+1)/2}$.

28. As in Exercise 9 suppose $\sigma = (a_0 a_1 a_2 \; . \; . \; . \; a_{k-1})$ and view the subscripts in $\mathbb{Z}_k$. To find the cycle decomposition of σ^2, compute the cycle containing a_0 : $\sigma^2(a_0) = a_2$, $\sigma^2(a_0) = a_4$, . . . , $\sigma^{2r}(a_0) = a_{2r}$. This is an r-cycle where r is the smallest positive integer with $a_{2r} = a_0$. Since the subscripts are in $\mathbb{Z}_k$ this equality means: $2r \equiv 0 \pmod{k}$.
   (a) If k is odd then $r \equiv 0$ (mod k) and the smallest positive solution is k. Therefore σ^2 is a k-cycle.
   (b) If $k = 2t$ is even then $r \equiv 0 \pmod{t}$ and the smallest positive solution is t. Then σ^2 contains a t-cycle starting with a_0. This argument works just as well starting with any a_j: each cycle in the decomposition of σ^2 is a t-cycle. Then σ^2 is a product of 2 disjoint t-cycles.
   Generally, for any m the permutation σ^m is the product of k/d d-cycles, where $d = (m, k)$.

29. Answered in the text.

30. Every element of A_n is a product of an even number of 2-cycles. Every product of two 2-cycles equals a product of 3-cycles, by Exercise 29. Therefore every element of A_n is a product of 3-cycles.

31. If $\sigma = (a_{11}a_{21} \; . \; . \; . \; a_{n1})(a_{12}a_{22} \; . \; . \; . \; a_{a2}) \; . \; . \; . \; (a_{1m}a_{2m} \; . \; . \; . \; a_{nm})$ is a product of m disjoint n-cycles. Define $\tau = (a_{11}a_{12} \; . \; . \; . \; a_{1m}a_{21}a_{22} \; . \; . \; . \; a_{2m} \; . \; . \; . \; a_{n1}a_{n2} \; . \; . \; . \; a_{\mathrm{nm}})$, an nm-cycle, Notethat $\tau^n = \sigma$.

32. Suppose σ permutes the symbols $\{1, 2, . . . , n\}$. Express σ as a product of disjoint cycles, including the trivial 1-cycles. Then every symbol i occurs in exactly one of the given cycles. If i is in a k-cycle then mat cycle must equal (i, σ(i), σ^2(i), . . . , σ^{k-1} (i)) and $\sigma^k(i) = i$. Therefore the cycles in the decomposition are unique, up to the order in which they are written.

33. As in the Hint, $(kr)\tau$ is viewed in S_{n-1} and the induction hypothesis says that $(kr)\tau$ is a product of transpositions. Multiplying by (kr) we see that τ is also such a product.

34. As in the solution to Exercise 11, any k-cycle is a product of k-1 transpositions. Suppose $\sigma \in S_n$ is written as a product of disjoint cycles: $\sigma = \alpha_1\alpha_2 \; . \; . \; . \; \alpha_r$ where α_j is a k_j-cycle. Then $n \geq k_1 + k_2 + . . . + k_r$ and each α_j is a product of $k_j - 1$ transpositions. Then σ is expressed as a product of $(k_1 - 1) + (k_2 - 1) + . . . + (k_r - 1) \leq n - r$ transpositions.

35. Answered in the text.

36. Suppose $\sigma(a_i) = b_i$. for each i, and the indices are viewed modulo k. Then $(\sigma\tau\sigma^{-1})(b_i) = \sigma\tau(a_i) = \sigma(a_{i+1}) = b_{i+1}$. If c is a symbol unequal to any b_i then $\sigma^{-1}(c)$ is unequal to any of the a_i so it is fixed by τ. Hence $(\sigma\tau\sigma^{-1})$(c) $= \sigma(\sigma^{-1}(c)) = c$. Therefore $\sigma\tau\sigma^{-1} = (b_1b_2 \; . \; . \; . \; b_k)$.

37. Clearly H is nonempty since $(1) \in H$. So if H is closed under permutation multiplication, then H is a subgroup. But if α and β each fix 1 and n, then in the product $\alpha\beta$, clearly neither 1 nor n is moved by either factor, so that $\alpha\beta$ also fixes 1 and n, so that $\alpha\beta \in H$. Thus H is a subgroup of S_n.

38. Consider the map f: $D \to S_4$ defined in the Hint. Since f is just a restriction of maps, it is a homomorphism. From the definition of r_1 as a 90° rotation note that $r_1(1) = 2$, $r_1(2) = 3$, etc., showing that $f(r_1) = (1234)$. Also d fixes vertices 1 and 3 and interchanges vertices 2 and 4. That is, $f(d) = (24)$. Therefore $f(D_4) \supseteq G$. By the First Isomorphism Theorem, $f(D_4) \cong D_4/(\text{ker f})$ has at most 8 elements. By Exercise 15 $|\text{G}| = 8$. Conclude that $\text{f}(\text{D}_4) = \text{G}$ has exactly 8 elements and $\text{ker f} = \{\text{e}\}$ so that f is injective.

39. (a) G must have at least one even permutation as well, since $(1) \in G$ is even. Let the even permutations be $e_1, \ldots, e_k$, and let π be the known odd permutation. Consider the set of products $\pi e_1, \ldots, \pi e_k$. Since π is odd and each of the e_i are even, it follows that πe_i is odd for all i. Further, these products are all distinct, for if $\pi e_i = \pi e_j$, multiplying on the left by $\pi^{-1} \in G$ gives $e_i = e_j$ so that $i = j$. Thus there are at least k odd permutations in G. Let the odd permutations be $\pi = o_1, o_2, \ldots, o_l$ where $l \geq k$. Then all the permutations $\pi o_1, \pi o_2, \ldots, \pi o_l$ are even and distinct, by the same argument as above. But there are only k even permutations, so that $k = l$ and the number of odd and even permutations is the same.

    (b) Since every permutation in G is either odd or even, and there are the same number of each, $|G|$ is even, i.e., 2 divides $|G|$.

    (c) Let K be any subgroup of S_n. If K is not a subgroup of A_n, then K must contain at least one odd permutation, since all even permutations lie in A_n. But by part (b), this means that $|K|$ is odd.

40. If $n \leq 3$ the statement is trivial. Suppose $n = 4$ and note that $(123) = (1n(n-1) \ldots 432)(13245 \ldots n)$ is a product of two n-cycles. Similarly every 3-cycIe is a product of two n-cycles. Use Exercise 30 to conclude that every element of A_n is expressible as a product of n-cycles.

41. Let H be the subgroup generated by those transpositions. If 1, a, b are distinct symbols then $(ab) = (1a)(1b)(1a)$ so that every 2-cycIe lies in H. Use Corollary 7.48 to conclude that $H = S_n$.

42. Let K be the subgroup generated by (12) and $\alpha = (123 \ldots n)$. View the symbols as elements of $\mathbb{Z}_\text{n}$ so that: $\alpha(i) = i + \text{l}$. Then by Exercise 24, $\alpha^{k-1}(12)\alpha^{-k+1} = (k(k{+}\text{l}))$ so these transpositions lie in K. Then $(13) = (12)(23)(12) \in K$, and $(14) = (13)(34)(13) \in K$. Continuing this pattern we find $(1k) \in K$ for every $k = 2, \ldots.. , \text{n}$. Therefore $K = S_n$ using Exercise 32.

43. S_3 contains 3 elements of order 2, namely (12), (13), (23). Since the transpositions (12) and (13) generate S_3 (as in Exercise 32), two automorphisms with the same behavior at (12) and (13) must be equal. Also f preserves the orders of elements (by Exercise 7.4.21), Therefore $f(12) = (xy)$ is another 2-cycle.

    Suppose $f(12) = (12)$. Then $f(13)$ is either (13) or (23). If $f(\text{l}3) = (13)$, then f is the identity. If $f(13) = (23)$ then $f(\tau) = (12)\tau(12)$ for every τ, since these two automorphisms agree on the generators (12) and (13).

    Generally if $f(12) = (xy)$, use Exercise 24 to find $\alpha \in S_3$ with $\alpha f(12)\alpha^{-1} = (12)$. Then the automorphism $g(\tau) = \alpha f(\tau)\alpha^{-1}$ fixes (12) and the argument above describes g. Therefore, either f is the identity or $f(\tau) = \sigma\tau\sigma^{-1}$ where $\sigma = \alpha^{-1}$ (12).

44. (a) If $\tau(a_k) = a_j$ for some $j > 1$ then $\tau(a_{k}.) = \tau(a_{j-1})$ contrary to the injectivity of τ. Therefore $\tau(a_k) = \tau(a_1)$.

  (b) Suppose $\tau(b_i) = a_j$ for some j. If $j > 1$ then $\tau(b_i) = \tau(a_k)$. If $j = 1$ then $\tau(b_i) = \tau(a)_k$. In either case this contradicts the injectivity.

  (c), (d) The same argument applies. The permutation τ agrees with the product of the disjoint cycles $(a_1 - a_k)(b_1 - b_r) \ . \ . \ .$, and therefore τ equals this product in S_n.

45. Define $f : S_n \to A_{n+2}$ as follows: if $\alpha \in A_n$, then $f(\alpha) = \alpha$. If α is an odd permutation, then $f(\alpha) = \alpha(n+1\ n+2)$. This is obviously an injective map.

Before proving that f is a homomorphism, observe that if $\alpha \in S_{n+2}$ fixes both $n+1$ and $n+2$, then $\alpha(n+1\ n+2) = (n+1\ n+2)\alpha$. This is true since if we write α as a product of disjoint cycles, those cycles will involve only the numbers 1 through n; by Exercise 18, each of those cycles commutes with $(n+1\ n+2)$, so that α does as well.

Now, if $\alpha, \beta \in A_n$, then $f(\alpha\beta) = \alpha\beta = f(\alpha)f(\beta)$. If $\alpha \in A_n$ and $\beta \in B_n = S_n - A_n$, then $\alpha\beta \in B_n$ as well, since α is even and β is odd so that $\alpha\beta$ is odd. Thus $f(\alpha\beta) = \alpha\beta(n+1\ n+2) = f(\alpha)f(\beta)$. If $\alpha \in B_n$ and $\beta \in A_n$, then $\alpha\beta \in B_n$ as above. Then $f(\alpha\beta) = \alpha\beta(n+1\ n+2)$. By the above observation, this is the same as $\alpha(n+1\ n+2)\beta = f(\alpha)f(\beta)$. Finally, if $\alpha, \beta \in B_n$, then $\alpha\beta \in A_n$, so that $f(\alpha\beta) = \alpha\beta = \alpha\beta(n+1\ n+2)(n+1\ n+2) = \alpha(n+1\ n+2)\beta(n+1\ n+2)$ by the observation above. But this is just $f(\alpha)f(\beta)$. Thus in all cases, $f(\alpha\beta) = f(\alpha)f(\beta)$, so that f is an injective homomorphism and thus its image is a subgroup of A_{n+2} that is isomorphic to S_n.

Chapter 8

Normal Subgroups and Quotient Groups

8.1 Congruence and Lagrange's Theorem

1. ($\Rightarrow$) Answered in the text. ($\Leftarrow$) If $a \in K$ then $a \in Ka \cap K$ so that $Ka = K$ by Corollary 7.19.

2. $Kr_0 = \{r_0, v\}$; $Kr_1 = \{r_1, t\}$; $Kr_2 = \{Kr_2, h\}$; $Kr_3 = \{r_3, d\}$.

3. $Kr_0 = \{r_0, r_1, r_2, r_3\}$; $Kd = \{d, h, t, v\}$.

4. $Ke = \left\{e, \begin{pmatrix}1\,2\,3\\1\,3\,2\end{pmatrix}\right\}$; $K\begin{pmatrix}1\,2\,3\\2\,1\,3\end{pmatrix} = \left\{\begin{pmatrix}1\,2\,3\\2\,1\,3\end{pmatrix}, \begin{pmatrix}1\,2\,3\\3\,1\,2\end{pmatrix}\right\}$; $K\begin{pmatrix}1\,2\,3\\3\,1\,2\end{pmatrix} = \left\{\begin{pmatrix}1\,2\,3\\3\,1\,2\end{pmatrix}, \begin{pmatrix}1\,2\,3\\2\,1\,3\end{pmatrix}\right\}$.

5. $K_1 = \{1, 17\}$; $K3 = \{3, 19\}$; $K5 = \{5, 21\}$; $K7 = \{7, 23\}$; $K9 = \{9, 25\}$; $K11 = \{11, 27\}$; $K13 = (13, 29\}$; $K15 = \{15, 31\}$.

6. $$\begin{aligned} K3 &= \{3, 3\cdot 3 = 9, 9\cdot 3 = 27, 27\cdot 3 = 81 = 17, 17\cdot 3 = 51 = 19, 19\cdot 3 = 57 = 25, 25\cdot 3 = 11, 11\cdot 3 = 1\} \\ &= \{1, 3, 9, 11, 17, 19, 25, 27\} \\ K5 &= \{1\cdot 5 = 5, 3\cdot 5 = 15, 9\cdot 5 = 45 = 13, 11\cdot 5 = 55 = 23, 17\cdot 5 = 85 = 21, 19\cdot 5 = 95 = 31, \\ &\qquad 25\cdot 5 = 125 = 29, 27\cdot 5 = 7\} \\ &= \{5, 7, 13, 15, 21, 23, 29, 31\}. \end{aligned}$$

7. 4

8. 3

9. 1

10. 4

11. 6

12. (a) Using Theorem 7.12, all we need to show is that the elements of K lie in A_4 and that K is closed under the operation of permutation multiplication. Clearly the elements lie in A_4 since they are all written with an even number of disjoint transpositions ((1) being written with zero transpositions). Further, $(1)\pi = \pi = \pi(1)$ for any $\pi \in K$; for the remaining multiplications, we have

$$(12)(34)\cdot(13)(24) = (14)(23) = (13)(24)\cdot(12)(34)$$
$$(12)(34)\cdot(14)(23) = (13)(24) = (14)(23)\cdot(12)(34)$$
$$(13)(24)\cdot(14)(23) = (12)(34) = (14)(23)\cdot(13)(24)$$

(b) Since K has four elements and A_4 has 12 elements, there are $\frac{12}{4} = 3$ cosets of K in A_4, by Lagrange's Theorem.

(c) Since K has four elements and S_4 has 24 elements, there are $\frac{24}{4} = 6$ cosets of K in S_4, by Lagrange's Theorem.

13. (a) These cosets are not identical. $K + 4$ consists of all integers leaving a remainder of 4 when divided by 7; since 3 does not, $3 \notin K + 4$, so that $K + 4$ and $K + 3$ are disjoint.

(b) These cosets are identical, since $K + 137 = K + (19\cdot 7 + 4) = (K + 19\cdot 7) + 4 = K + 4$.

(c) These cosets are identical, since $K + 59 = K + (9\cdot 7 + (-4)) = (K + 9\cdot 7) + (-4) = K + (-4)$.

14. (a) Since $K(12)$ contains the permutation $(12)(34)(12) = (34)$, we see that $(34) \in K(12)$, so that $K(34) \subset K(12)$. Since the cosets are not disjoint, they are equal.

(b) $K(1234)$ contains the elements $(1)(1234) = (1234)$, $(12)(34)(1234) = (24)$, $(13)(24)(1234) = (1432)$, and $(14)(23)(1234) = (13)$. $K(1324)$ contains the element $(13)(24)(1324) = (34)$, which is not in $K(1234)$. Since the cosets are not identical, they are disjoint.

15. (a) From Exercise 6, 17 and 19 are both in the coset $K3$: $3^4 = 81 \equiv 17 \pmod{32}$ and $3^5 = 243 \equiv 19 \pmod{32}$.

(b) From Exercise 6, 9 and 25 are both in the coset $K3$: $3^2 = 9$, and $3^6 = 729 \equiv 25 \pmod{32}$.

16. $Ke = \{1, a^3, a^6, a^9, a^{12}\}$; $Ka = \{a, a^4, a^7, a^{10}, a^{13}\}$; $Ka^2 = \{a^2, a^5, a^8, a^{11}, a^{14}\}$.

17. (a), (c) Answered in the text.
(b) All the positive divisors of 24, as in (a).

18. (a) There are many examples, including $G = \mathbb{Z}$ and $H = n\mathbb{Z}$ and $G = \mathbb{Z}\times\mathbb{Z}_2$ and $H = \mathbb{Z}\times\{0\}$.
(b) For instance $G = \mathbb{R}$ and $H = \mathbb{Z}$ or $G = \mathbb{Z}\times\mathbb{Z}$ and $H = \mathbb{Z}\times\{0\}$.

19. Answered in the text.

20. 50.

21. Answered in the text.

22. $H \cap K$ is a subgroup of H and of K. Lagrange's Theorem implies that $|H \cap K|$ must divide $|H|$ and $|K|$.

23. Answered in the text.

24. Suppose G is not cyclic. If $g \in G$ then $|g|$ divides 25 so it equals 1, 5 or 25. It cannot be 25 since G is not cyclic. If $g \neq e$ then $|g| > 1$ and therefore $|g| = 5$.

25. Answered in the text.

26. Since $|G| = 8$, Corollary 8.6 says that every element of G has order 1, 2, 4, or 8. Choose a nonidentity element a. Then the order of a is 2, 4, or 8. If it is 2, we are done. So suppose the order of a is 4. Then $a^2 \neq e$ but $a^4 = e$. Since $(a^2)^2 = a^4 = e$, we have found an element a^2 with order 2. Finally, suppose the order of a is 8. Then $a^2 \neq e$ but $a^8 = e$. Since $(a^2)^4 = a^8 = e$, we have an element of order 2. So in any case there is an element of order 2.

27. In U_n, we have $(n-1)^2 = n^2 - 2n + 1 \equiv 1 \pmod{n}$, so that $(n-1)^2 = 1$. However, $n - 1 \neq 1$ since $n > 2$. Thus $n - 1$ has order 2.

28. By Corollary 7.27 conclude that 2 divides $|U_n|$.

29. By Lagrange's Theorem applied to the subgroup H of G, we get $|G| = |H|\,[G : H]$. By Lagrange's Theorem applied to the subgroup K of H, we get $|H| = |K|\,[H : K]$. Substituting into the first equality gives $|G| = |K|\,[H : K][G : H] = |K|\,[G : H][H : K]$. But regarding K as a subgroup of G, Lagrange's Theorem gives $|G| = |K|\,[G : K]$. Thus $|K|\,[G : K] = |K|\,[G : H][H : K]$ and thus $[G : K] = [G : H][H : K]$.

30. If G is finite the formula immediately follows from Lagrange's Theorem. But the result remains true when G is infinite: Suppose the distinct cosets of H in G are Hg_1, Hg_2, . . . , Hg_n where $n = [G : H]$. Suppose the distinct cosets of K in H are Kh_1, Kh_2, . . . Kh_m where $m = [H : K]$. Show that the cosets Kh_ig_j for $1 \leq i \leq m$, $1 \leq j \leq n$ forms a list of the distinct cosets of K in G. Therefore $[G : K] = nm = [G : H]\cdot[H : K]$.

31. Suppose that G has no element of order 2. Then for $a \in G$, we know that $a \neq a^{-1}$. Then elements come in pairs, $\{a, a^{-1}\}$, except that e is its own inverse. If there are k such pairs, then $|G| = 2k + 1$, which is odd. Thus if $|G|$ is even, there must be an element of order 2.

32. By Exercise 7.3.36 there is a subgroup of order p in U $_{p2}$. Consequently there is an element of order p. Alternatively expand $(1 + p)^p$ by the Binomial Theorem and reduce each term (mod p^2) to conclude that $1 + p$ has order p in U_{p2}

33. (a) Since a has order 3, we know that $a^3 = e$, so that $a(a^2) = e = (a^2)a$. Thus $a^{-1} = a^2$, and similarly $b^{-1} = b^2$. Since $a^2 = b^2$, we get $a^{-1} = b^{-1}$, so that $a = b$.

    (b) To each $a \in G$ of order 3 associate $a^2 \in G$. Clearly a^2 has order 3 as well. By part (a), if $a \neq b$ both have order 3, then $a^2 \neq b^2$. Thus elements of order 3 can be grouped into pairs, $\{a, a^2\}$. Hence there are an even number of them.

34. G can have no elements of order 2, since by Corollary 8.6, the order of each element divides $|G|$, which is odd. Thus no element is its own inverse. So in the list $a_1a_2\ldots a_{2k+1}$, each nonidentity element appears separately from its inverse. Since G is abelian, reorder the list so that $a_2 = a_1^{-1}$, $a_4 = a_3^{-1}$, until $a_{2k} = a_{2k-1}^{-1}$ and $a_{2k+1} = e$. Then clearly the product of all the a_i is the identity.

35. Answered in the text.

36. $[G{:}\,H \cap K] = p[H : H \cap K]$ by Lagrange's Theorem. Similarly $q \mid [G : H \cap K]$ and since p, q are relatively prime also pq is a factor.

37. f is a homomorphism since $(ab)^k = a^k b^k$. By Corollary 7.27 we know $a^n = e$. Since $(k, n) = 1$ there exist integers x, y with $kx + ny = 1$, Surjective. For any $a \in G$ we have $a = a^{kx+ny} = a^{kx} = f(a^x)$. Since $f : G \to G$ is a surjective map on a finite set, deduce that f must be injective. (One can check injectivity directly by first showing: $f(a) = e \Rightarrow a = e$, (Proof. Given $a^k = e$ deduce $a = a^{kx+ny} = e$.) If $f(a) = f(b)$, note that $(ab^{-1})^k = a^k b^{-k} = e$, then conclude that $ab^{-1} = e$, so that $a = b$.)

38. There are 2^{n-1} subsets of G which contain e. By hypothesis each of these subsets is a subgroup. If $|G| > 2$ let e, a, b be distinct elements. Apply Corollary 7.27, to show that $a^2 = e$ since $\{e, a\}$ is a subgroup and $a^3 = e$ since $\{e, a, b\}$ is a subgroup. But then $a = a^3 a^{-2} = e$, a contradiction.

39. (a) Suppose G has no elements of order 5. By Lagrange's Theorem, every nonidentity element of G must have order 2, 5, or 10. If it has an element a of order 10, then $a^{10} = e$ but $a^2 \neq e$. But then $(a^2)^5 = a^{10} = e$, so that a^2 has order 5. So if G has no elements of order 5, all the nonidentity elements must have order 2. But now Exercise 27 of Section 7.2 shows that G must be abelian, contradicting the assumption that G is nonabelian.

(b) Let a be an element of order 5, by part (a). Then $\{e, a, a^2, a^3, a^4\}$ are five distinct elements of G, which form a cyclic subgroup H. Let b be an element of G that is not in H. Then $H = \{e, a, a^2, a^3, a^4\}$ and $Hb = \{b, ab, a^2b, a^3b, a^4b\}$ are not identical, since $b \in Hb$ and $b \notin H$ by construction. Thus the cosets are disjoint, so $G = H \cup Hb$ as a set. Since G is nonabelian, it cannot be cyclic, so that b cannot have order 10. Thus it has order 2 or 5. Suppose b has order 5, and consider b^2. If $b^2 \in H$, then $b^2 = a^k$ for some $0 \leq k \leq 4$. Then $a^{2k} = b^4 = b^5 b^{-1} = b^{-1}$, so that $b^{-1} \in H$ and thus $b \in H$. This is impossible. Thus $b^2 = a^k b$ for some $0 \leq k \leq 4$; multiplying on the right by b^{-1} gives $b = a^k$, another contradiction. Thus b cannot have order 5, so it has order 2. But we chose b arbitrarily from among the five elements of G not in H. Thus all of those elements have order 2, so that G has five elements of order 2.

40. Let H_1 H_2, . . . , H_k be the distinct subgroups of order p in G. By Lagrange, every nonidentity element of H_j. has order p. If $g \in G$ has order p then $\langle g \rangle = H_j$ for some j. If $g \in Hi \cap H_j$ then $H_i = \langle g \rangle = H_j$. Therefore, the set of all elements of order p in G is exactly the union of the disjoint sets $H_j - \{e\}$. Hence there are $k(p - 1)$ such elements.

41. Suppose $|G| = 33$ and G has no element of order 3. Then by Theorem 7.8 there is no element of order 33, and Lagrange implies that every nonidentity element has order 11. Count the number of subgroups of order 11, as in Exercise 25 below, to obtain a contradiction.

42. Let $N = \langle a \rangle$ so that $|N| = 4$. If $b \in N$ then b commutes with a and $ab = ba = a^3b$. Cancellation implies $a^2 = e$ contrary to hypothesis. Therefore $b \notin N$ and there are 8 elements in $N \cup Nb$. Using the relation $ba = a^3b$, check that $N \cup Nb$ is closed under multiplication. In fact, the entire 8×8 operation table is uniquely determined. Therefore $N \cup Nb$ is a subgroup containing a and b. Then $G = N \cup Nb$, since G is generated by a, b, so that $|G| = 8$. Note that D_4 is generated by the elements $a = r_1$ and $b = h$ satisfying the relation $ba = a^3b$. Since the operation table above is unique, conclude that $G \equiv D_4$.

43. Let $N = \langle a \rangle$ so that $|N| = 4$. As in Exercise 26 show that $b \notin N$, that $N \cup Nb$ is a subgroup with a uniquely determined operation table, using the given relations. Since G is generated by a, b conclude that $G = N \cup Nb$ has 8 elements. The quaternion group Q of Exercise 7.1.14 is generated by the elements i, j where $|i| = 4$, $j^2 = -1 = i^2$ and $ji = -k = -ij = i^3 j$. The uniqueness of the operation table above implies G $\cong Q$.

44. (a) By Exercise 8 in Section 7.5, the elements of A_4 consist of

$$\begin{array}{llllllll}
(1) \\
(12)(34), & (13)(24), & (14)(23) \\
(123), & (132), & (124), & (142), & (134), & (143), & (234), & (243).
\end{array}$$

Since the elements of the form (abc) all have order 3, only the three elements (12)(34), (13)(24), and (14)(23) have order 2.

(b) By Exercise 12(a) in this section, these three elements together with (1) form a subgroup of A_4.

(c) If A_4 had a subgroup G of order 6, it would (by Theorem 8.9) be isomorphic to $\mathbb{Z}_6$ or to S_3. But it could not be isomorphic to $\mathbb{Z}_6$, since then A_4 would have an element of order 6 — and all of the elements listed above have order 1, 2, or 3. Thus such a subgroup must be isomorphic to S_3. Now, both S_3 and A_4 have three elements of order 2, so that an isomorphic image of S_3 in A_4 must contain (1), (12)(34), (13)(24), (14)(23) and two other elements of A_4. By part (b), these four elements form a subgroup of A_4 and thence a subgroup of the image of S_3. But this is impossible, since S_3 has order 6, so it cannot have a subgroup of order 4.

8.2 Normal Subgroups

1. Compare Exercise 7.5.1. If $aK = K$ then $a = ae \in aK = K$. Conversely suppose $a \in K$. Since K is a subgroup, $a^{-1} \in K$ and the closure property implies $aK \subseteq K$ and $a^{-1}K \subseteq K$. Then $K \subseteq aK$ as well, and the equality follows.

2. $r_1 \equiv t \pmod{K}$ since $r_1 t^{-1} = r_1 t = v \in K$, and $r_2 \equiv h \pmod{K}$ since $r_2 h^{-1} = r_2 h = v \in K$. However, $r_1 \circ r_2 = r_3$, and $t \circ h = r_1$, but $r_3 \not\equiv r_1 \pmod{K}$ since $r_3 r_1^{-1} = r_3 r_3 = r_2 \notin K$.

3. The left cosets are N and $r_1 N$ while the right cosets are N and Nr_1. Calculating the products of elements, we find that $r_1 N = Nr_1 = \{r_1, r_3, t, d\}$. (Compare Exercise 20 below.)

4. For any $g \in G$ note that $g\langle e \rangle = \{g\} = \langle e \rangle g$ and $gG = G = Gg$. Therefore these subgroups are normal.

5. (a) H is a subgroup since $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bd' \\ 0 & dd' \end{pmatrix}$ and $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1} = \begin{pmatrix} 1/a & -b/ad \\ 0 & 1/d \end{pmatrix}$ lie in H.

Similarly N is a subgroup since $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b+b' \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$ lie in N.

(b) Answered in the text.

6. K is the subgroup generated by $\begin{pmatrix}1\,2\,3\\2\,1\,3\end{pmatrix}$. The right cosets are K,

   $\left\{\begin{pmatrix}1\,2\,3\\1\,3\,2\end{pmatrix}, \begin{pmatrix}1\,2\,3\\2\,3\,1\end{pmatrix}\right\}$ and $\left\{\begin{pmatrix}1\,2\,3\\3\,2\,1\end{pmatrix}, \begin{pmatrix}1\,2\,3\\3\,1\,2\end{pmatrix}\right\}$. The left cosets are K,

   K $\left\{\begin{pmatrix}1\,2\,3\\3\,2\,1\end{pmatrix}, \begin{pmatrix}1\,2\,3\\2\,3\,1\end{pmatrix}\right\}$ and $\left\{\begin{pmatrix}1\,2\,3\\1\,3\,2\end{pmatrix}, \begin{pmatrix}1\,2\,3\\3\,1\,2\end{pmatrix}\right\}$. These are not the same so K is not normal.

7. Answered in the text.

8. (a) $\langle 1\rangle = \{1\}$; $\langle -1\rangle = \{1, -1\}$; $\langle i\rangle = \{1, i, -1, -i\}$; $\langle j\rangle = \{1, j, -1, -j\}$; $\langle k\rangle = \{1, k, -1, -k\}$.

   (b) The first two subgroups are normal since their elements commute with every element of Q. The remaining subgroups have order 4. Claim. Any subgroup H of order 4 in Q is normal. Rather than writing out the cosets explicitly we refer to the general fact given in Exercise 20 below.

9. If $Na = bN$ then $a = ea \in Na = bN$ and the cosets aN and bN both contain a. Use Corollary 7.24 to conclude that $Na = aN$. Therefore N is normal.

10. Suppose H is a subgroup of $Z(G)$. Then $gh = hg$ for any $g \in G$ and $h \in H$. Therefore Hg $= \{hg \mid h \in H) = gH$ and H is normal.

11. Answered in the text.

12. **Lemma.** If $\varphi : G \to H$ is a surjective homomorphism of groups then $\varphi(Z(G)) \subseteq Z(H)$.
    Proof. Let $z \in Z(G)$ and $h \in H$. Since φ is surjective there exists $g \in G$ with $\varphi(g) = h$. Then $\varphi(z)h = \varphi(z)\varphi(g) = \varphi(gz) = \varphi(zg) = \varphi(z)\varphi(g) = \varphi(z)h$. Then $\varphi(z)$ commutes with everything so it lies in $Z(H)$.
    Consequently for every automorphism f of G we have $f(Z(G)) \subseteq Z(G)$. Therefore $Z(G)$ is characteristic.

13. An inner automorphism f is defined using a fixed $c \in G$ as follows: $f(x) = c^{-1}xc$. By Theorem 7.34 N is normal if and only if $f(N) = N$ for every such f.

14. As suggested in the Hint consider $M \subseteq N \subseteq D_4$ where $|M| = 2$, $|N| = 4$ and $|D_4| = 8$. Checking the operation tables note that these are subgroups, and by Exercise 20 below it follows that M is normal in N and N is normal in D_4. However M is not normal in D_4 as one can see by noting: $t^{-1}Mt = \{h, r_0\} \neq M$.

15. If $\tau \in A_n$, then τ is even. Then by Exercise 20 of Section 7.5, $\sigma^{-1}\tau(\sigma^{-1})^{-1} = \sigma^{-1}\tau\sigma$ is even regardless of the parity of σ, so that for any $\sigma \in S_n$, we have $\sigma^{-1}\tau\sigma \in A_n$. Thus $\sigma^{-1}A_n\sigma \subset A_n$ so that A_n is normal in S_n (see Theorem 8.11).

16. Since K is normal and of order 2, suppose $K = \{e, k\}$ with $k \neq e$. Then if $a \in G$, we know that $aka^{-1} \in K$. If $aka^{-1} = e$, then $ak = a$, which is impossible. Thus $aka^{-1} = k$, so that, multiplying through on the right by a, $ak = ka$. Thus $k \in Z(G)$; since $e \in Z(G)$, it follows that $K \subseteq Z(G)$.

17. If a, $b \in K$ then $f(ab^{-1}) = f(a)f(b)^{-1} = e_H$ so mat $ab^{-1} \in K$. Therefore K is a subgroup. For any $g \in G$ and $a \in K$ we have $f(g^{-1}ag) = f(g)^{-1}f(a)f(g) = f(g)^{-1}f(g) = e_H$. Therefore $g^{-1}ag \in K$ and Theorem 7.34 implies that K is normal.

18. Let $x \in K \cap N$ and $g \in G$. Then $g^{-1}xg \in g^{-1}Kg = K$ since K is normal and $g^{-1}xg \in g^{-1}Ng = N$ since N is normal. Therefore $g^{-1}xg \in K \cap N$ and $K \cap N$ is normal by Theorem 7.34.

19. Answered in the text.

20. (a) If $n \in N$ and $k \in K$ then $(nk)^{-1} = k^{-1}n^{-1} = (k^{-1}n^{-1}n^{-1})k^{-1}$ lies in NK because $k^{-1}n^{-1}k \in k^{-1}Nk = N$. Similarly, let n, $n' \in N$ and k, $k' \in K$. Then $(nk)(n'k') = n(kn'k^{-1})kk'$ lies in NK. Therefore NK is a subgroup.
    (b) For n, k as above and $g \in G$ we have $g^{-1}(nk)g = (g^{-1}ng)(g^{-1}kg) \in (g^{-1}Ng)(g^{-1}Kg) = NK$. Therefore NK is normal by Theorem 7.34.

21. Answered in the text.

22. We may restrict f to a homomorphism $f_1 : N \to H$. Then Theorem 7.19 implies $f(N) = Im\ f_1$ is a subgroup of H. Let $h \in H$ and $x \in f(N)$. By definition $x = f(n)$ for some $n \in N$ and the surjectivity implies that $h = f(g)$ for some $g \in G$. Then $h^{-1}xh = f(g)^{-1}f(n)f(g) = f(g^{-1}ng) \in f(g^{-1}Ng) = f(N)$, since N is normal in G. Therefore $f(N)$ is normal by Theorem 7.34.

23. Suppose $a \in G$. If $a \in N$ then the closure of N implies $aN = N = Na$. Suppose $a \notin N$. Then by Corollary 7.24 and Theorem 7.25, $G = N \cup Na$ and $N \cap Na$ is empty. Consequently $Na = \{g \in G \mid g \notin N\}$. Also the left coset aN contains $a \notin N$ so it must be disjoint from N by the analog of Corollary 7.24. Then $aN \subseteq Na$ by the description of Na above. Therefore $aNa^{-1} \subseteq N$ for every $a \in G$ and Theorem 7.34 applies.

24. Since $\det : GL(2,\mathbb{R}) \to \mathbb{R}^*$ is a homomorphism, we know that if $A, B \in GL(2,\mathbb{R})$, then

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(A)\det(B)\det(A)^{-1} = \det(B).$$

Thus if $B \in N$, so that $\det B \in \mathbb{Q}^*$, it follows that $\det(ABA^{-1}) \in \mathbb{Q}^*$, so that $ABA^{-1} \in N$. Thus $ANA^{-1} \subset N$ for every $A \in GL(2,\mathbb{R})$, so that N is normal in $GL(2,\mathbb{R})$ by Theorem 8.11.

25. Apply Exercise 15 to the homomorphism in Exercise 22.

26. For any $g \in G$ use Exercise 7.4.13 to show that $g^{-1}Hg$ is a subgroup of order n. By the uniqueness, $g^{-1}Hg = H$. Then Theorem 7.34 applies.

27. If N is normal and $ab \in N$ then $ba = b(ab)b^{-1} \in bNb^{-1} = N$. Conversely, suppose N has the stated property. For any $g \in G$ and $n \in N$ we have $g(g^{-1}n) = n \in N$ and the assumed property implies that $g^{-1}ng \in N$. Therefore $g^{-1}Ng \subseteq N$ for every g and N is normal, by Theorem 7.34.

28. If $\langle a\rangle$ is normal then for any $g \in G$, $gag^{-1} \in g\langle a\rangle g^{-1} \subseteq \langle a\rangle$. Therefore $gag^{-1} = a^k$ for some integer k. That is, $ga = ga^k$. Conversely suppose a has the given property: for any $g \in G$ there exists k such that $gag^{-1} = ak$. Then, for any integer n, $ga^ng^{-1} = (gag^{-1})^n = (a^k)^n = a^{kn} \in \langle a\rangle$. Then $g\langle a\rangle g^{-1} \subseteq \langle a\rangle$ for every g. Apply Theorem 7.34.

29. Answered in the text.

30. By Exercise 19 we know that $ab = ba$ for every $a \in A$ and $b \in B$. Define f as in the Hint. Homomorphism. $f((a, b)\cdot(a', b')) = f(aa', bb') = aa'bb' = aba'b' = f(a, b)f(a', b')$. Surjective. $f(A \times B) = AB = G$. Injective. If $f(a, b) = f(a', b')$ then $ab = a'b'$ and $a^{-1}a' = bb'^{-1} \in A \cap B = \{e\}$. Therefore $a' = a$ and $b' = b$ so that $(a, b) = (a', b')$.

31. (a) If $x \in N_H$ then by definition $x^{-1}Hx = H$. Then H is normal in N_H by Theorem 7.34.
(b) If H is normal in K then for every $x \in K$ we have $x^{-1}Hx = H$ by Theorem 7.34. Therefore $x \in N_H$ by definition, and we conclude that $K \subseteq N_H$.

32. As in Exercise 7.4.33, for $c \in G$ let $g(c)$ be the inner automorphism induced by c: $g(c)(x) = cxc^{-1}$. If $f \in Aut(G)$ then $(f\circ g(c))(x) = f(g(c)(x)) = f(cxc^{-1}) = f(c)f(x)f(c)^{-1} = g(f(c))(f(x)) = (g(f(c))\circ f)x)$. Therefore $f\circ g(c) = g(f(c))\circ f$ so that $f\circ g(c)\circ f^{-1} = g(f(c)) \in$ Inn G. Therefore Inn G is normal in $Aut\ G$ by Theorem 7.34.

33. If $f, g \in H_a$ then $(f\circ g)(a) = f(g(a)) = f(a) = a$ so that $f\circ g \in H_a$. Also $f(a) = a$ implies that $a = f^{-1}(a)$ so that $f^{-1} \in H^{a\cdot}$ Hence H^a is a subgroup.

Claim. If $\sigma \in A(T)$ then $\sigma H_a \sigma^{-1} = H_{\sigma(a)}$.

Proof. Let $b = \sigma(a)$. If $f \in H_a$ then $(\sigma f \sigma^{-1})(b) = \sigma(f(\sigma^{-1}(b))) = \sigma(f(a)) = \sigma(a) = b$ so that $\sigma f \sigma^{-1} \in H_b$. Therefore $\sigma H_a \sigma^{-1} \subseteq H_{\sigma(a)}$. Applying this to $a = \sigma^{-1}(b)$ provides the reverse inclusion and the Claim follows.
Suppose $|T| \geq 3$ and let a, b, c be three distinct elements of T. Define $f \in A(T)$ be setting $f(b) = c$, $f(c) = b$ and $f(x) = x$ for every $x \neq b$, c. Then $f \in H_a$ but $f \notin H_b$. Using any $\sigma \in A(T)$ with $\sigma(a) = b$ the Claim implies that $\sigma H_a \sigma^{-1} = H_b \neq H_a$. Therefore H_a is not normal.

34. Suppose $f : S \to T$ is any injective map of sets, and $\mathfrak{F}$ is some family of subsets of S. Then $f(\cap\ Y) = (\cap\ f(Y)$, where the intersection runs over all $Y \in \mathfrak{F}$. In our case this implies: $a^{-1}Na \subseteq \cap\ a^{-1}Ka$ for every $a \in G$. Using Exercise 7.4.13, show that for any fixed $a \in G$, the operation sending K to $a^{-1}Ka$ provides a bijection on the set of all subgroups of order n. Therefore the intersection above runs over all subgroups of order n in G, so that $a^{-1}Na \subseteq N$. Hence N is normal by Theorem 7.34.

35. As in the Hint, N is a subgroup. By definition, $N \subseteq a^{-1}Ha$ for every element a. Let $g \in G$. Therefore $g^{-1}Ng \subseteq g^{-1}a^{-1}Hag = (ag)^{-1}H(ag)$ for every $a \in G$. For any $b \in G$ let $a = bg^{-1}$ and deduce that $g^{-1}Ng \subseteq b^{-1}Hb$. Therefore $g^{-1}Ng \subseteq \bigcap_{b \in g} b^{-1}Hb = N$ and Theorem 7.34 applies.

36. Let $g(c)$ be the inner automorphism induced by c, as in Exercise 7,4.33. Then $g(c)(N) = cNc^{-1} = N$ since N is normal. Therefore the restriction of $g(c)$ to N provides an automorphism $\varphi \in Aut\ N$. Since M is characteristic in N we know that $\varphi(M) \subseteq M$. By the definition of φ this says: $cMc^{-1} \subseteq M$. Since $c \in G$ was arbitrary, M is normal in G.

37. Answered in the text.

8.3 Quotient Groups

1. The order of $13 + N$ in $\mathbb{Z}_{20}/N$ is the smallest integer k such that $k(13 + N) = 13k + N \subset N$, i.e., the smallest integer k such that $13k \in N$. Clearly then $k = 4$, so that the order of this element is 4.

2. The order of $15 + N$ in $G/ < 15 >$ is the smallest integer k such that $k(6 + N) = 6k + N \subset N$, i.e., the smallest integer k such that $6k \in N$. Thus $k = 5$, since $6 \cdot 5 = 30 = 15 \cdot 2$.

3. The completed table is

	Mr_0	Mr_1	Mh	Md
Mr_0	Mr_0	Mr_1	Mh	Md
Mr_1	Mr_1	Mr_0	Md	Mh
Mh	Mh	Md	Mr_0	Mr_1
Md	Md	Mh	Mr_1	Mr_0

since for example $(Mh)(Md) = M(hd) = Mr1$. Since Mr_0 is the identity in this group (because r_0 is the identity in D_4), examining the table shows that $(Mr_0)(Mr_0) = (Mr_1)(Mr_1) = (Mh)(Mh) = (Md)(Md) = Mr_0$, so that every element has order 2.

4. N is normal as seen in Exercise 7.6.3 and the quotient group has 2 elements. There is only one possible operation table for a group of 2 elements (after relabeling) so $G/N \cong \mathbb{Z}_2$.

5. The quotient group has 6 elements, M, $1 + M$, $2 + M$, $3 + M$, $4 + M$ and $5 + M$. Clearly $1 + M$ generates all die others, so the group is cyclic of order 6. By Theorem 7.14 it is isomorphic to $\mathbb{Z}_6$.

6. The cosets are N, $1 + N$ and $2 + N$. Since $1+N$ has order 3 in the group $\mathbb{Z}_6/N$ this group is cyclic, and hence isomorphic to $\mathbb{Z}_3$. (See Theorem 7.14.)

7. Since U_{26} is abelian, $\langle 5\rangle$ is normal. The group $\langle 5\rangle$ is

$$\langle 5\rangle = \{5, 5\cdot 5 = 25, 25\cdot 5 = 125 \equiv 21, 21\cdot 5 = 105\cdot 1\},$$

so that $|\langle 5\rangle| = 4$. But U_{26} has elements $\{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$, so that $|U_{26}| = 12$. Since $[U_{26} : \langle 5\rangle] = 3$, and since by the table at the end of Section 8.1 the only group of order 3 is $\mathbb{Z}_3$, we must have $U_{26}/\langle 5\rangle \cong \mathbb{Z}_3$.

8. $N = \{(0, 0), (3, 2), (2,0), (1, 2)\}$ and there are 4 cosets. Since $(0, 1)$, $(0, 2)$ and $(0, 3)$ are not in N, the coset $(0, 1) + N$ does not have order 1, 2 or 3 in the quotient group. Therefore it is a generator. By Theorem 7.14 the group is $\cong \mathbb{Z}_4$.

9. Answered in the text.

10. (a) $M = \{(0, 0), (0, 2)\}$ and $N = \{(0, 0), (1, 2)\}$ are groups of order 2, so they are isomorphic by Corollary 7.18.

(b)

	$M + (0, 0)$	$M + (1, 0)$	$M + (0, 1)$	$M + (1, 1)$
$M + (0, 0)$	$M + (0, 0)$	$M + (1, 0)$	$M + (0, 1)$	$M + (1, 1)$
$M + (1, 0)$	$M + (1, 0)$	$M + (0, 0)$	$M + (1, 1)$	$M + (0, 1)$
$M + (0, 1)$	$M + (0, 1)$	$M + (1, 1)$	$M + (0, 0)$	$M + (1, 0)$
$M + (1, 1)$	$M + (1, 1)$	$M + (0, 1)$	$M + (1, 0)$	$M + (0, 0)$

(c) $N + (0, 1)$ has order 4 in G/N but there are no elements of order 4 in G/M. Therefore these groups are not isomorphic.

11. Answered in the text.

12. A nonidentity element in G/N is some Nx where $x \notin N$. Since $x^2 \in N$ note that $(Nx)^2 = Nx^2 = N$ so that Nx has order 2.

13. (a) If G is abelian, then $G = Z(G)$ so that $G/Z(G) = \{e\}$ is abelian. Nonabelian examples include D_4 and the quaternion group Q.
    (b) $G = S_3$ has trivial center: $Z(S_3) = \{e\}$, so that $S_3/Z(S_3) = S_3$ is nonabelian.

14. This problem can be done directly using many multiplications of permutations. The 6 right cosets can be listed explicitly and compared to the 6 left cosets to see that V is normal. Then the 6 × 6 operation table can be constructed to prove that $S_4/V \cong S_3$.
    Better proofs are possible using more of the theory of permutation groups. For example see Exercise 7.9.27 below.

15. Recall that an element a has infinite order if $a^k \neq e$ for every positive integer k. Then for example $(1,0)$ has infinite order, since $(1,0)^k = (k,0) \neq (1,1) = e$.

16. Recall that an element a has infinite order if $a^k \neq e$ for every positive integer k. Then for example $(0,1)$ has infinite order, since $(0,1)^k = (0,k) \neq (1,1) = e$.

17. (a) E consists of the set of even numbers, while N is the set of multiples of 8. Thus the cosets of N in E are the congruence classes of 8 among even numbers, which are clearly 0, 2, 4, and 6. Thus E/N has four elements (N is normal since E is abelian).
    (b) Since $(2+N)+(2+N) = 4+N \neq N$, the element $2+N \in E/N$ does not have order 2. Therefore E/N is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, so by Theorem 8.8 it is isomorphic to $\mathbb{Z}_4$.

18. Define $\varphi : U_{32}/N \to U_{16}$ by $\varphi(N[a]_{32}) = [a]_{16}$. To show φ is well-defined suppose a, b are odd integers and $N[a]_{32} = N[b]_{32}$. Then $[a]_{32} \in N[b]_{16} = \{[b]_{32}, [17b]_{32}\}$. Hence, $a \equiv b$ or $17b$ (mod 32) which implies $a \equiv b$ (mod 16). Verify the homomorphism property. Since φ is surjective and both groups have 8 elements the map φ is automatically injective. (See Exercise 32 of Appendix B.) Hence it is an isomorphism.

19. Suppose $g \in G$. Then gN is a square in G/N, so that $gN = (g_1N)^2 = g_1^2N$, so that for some $m, n \in N$, $gm = g_1^2 n$ and thus $g = g_1^2 n m^{-1}$. But $nm^{-1} \in N$, so $nm^{-1} = n_1^2$ for some $n_1 \in N$. Then $g = g_1^2 n_1^2 = (g_1 n_1)^2$ since G is abelian.

20. Since $[G : Z(G)] = 4$, it follows that $G/Z(G) \cong \mathbb{Z}_4$ or $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Suppose that $G/Z(G) \cong \mathbb{Z}_4$, and let $aZ(G)$ be a generator. Then the elements of $G/Z(G)$ are $Z(G)$, $aZ(G)$, $a^2Z(G)$, and $a^3Z(G)$. Since these are the cosets of $Z(G)$ in G, every element of G can be written as $a^k z$ for $k \in \{0,1,2,3\}$ and $z \in Z(G)$. But then if $g, h \in G$, we have $g = a^k z_1$ and $h = a^l z_2$; since $z_i \in Z(G)$, we get $ab = a^k z_1 a^l z_2 = a^{k+l} z_1 z_2 = a^{l+k} z_2 z_1 = a^l z_2 a^k z_1 = ba$. But this means that any two elements of G commute, so that $Z(G) = G$, contradiction. Thus $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

21. Suppose that $gT \in G/T$ has finite order. Then $(gT)^k = g^kT = eT = T$ for some $k \geq 0$, so that $g^k \in T$. But T consists of the set of elements of finite order, so that for some n, $(g^k)^n = g^{kn} = e$. Thus g has finite order, so that $g \in T$ and $gT = T$. So gT is the identity element of G/T, and thus no nonidentity element of G/T has finite order.

22. Define $\varphi : \mathbb{R}^{**} \to \mathbb{R}^{*}/N$ by $\varphi(x) = Nx$. It is easy to check that φ is a homomorphism. Injective. If $\varphi(x) = \varphi(y)$ then $Nx = Ny$ so that $x \in Ny = \{y, -y\}$. Since x, y are positive, conclude that $x = y$. Surjective. For any $x \in \mathbb{R}^{*}$, the absolute value $|x|$ is in $\mathbb{R}^{**}$. Also $|x| \in Nx$ so that $\varphi(|x|) = Nx$. Therefore φ is an isomorphism.

23. Answered in the text.

24. Suppose $G = \langle a \rangle$. If $g \in G$ then $g = a^k$ for some integer k. Therefore $Ng = Na^k = (Na)^k$ so that Na is a generator of the group G/N.

25. (a) Since $9 \cdot \frac{8}{9} = 8 \in \mathbb{Z}$ and no smaller multiple of $\frac{8}{9}$ is an integer, the order of $\frac{8}{9}$ in $\mathbb{Q}/\mathbb{Z}$ is 8. Similarly, the order of $\frac{14}{5}$ in $\mathbb{Q}/\mathbb{Z}$ is 5. Finally, since $\frac{48}{28} = \frac{12}{7}$, and $7 \cdot \frac{12}{7}$ is the smallest integral multiple of $\frac{12}{7}$, the order of $\frac{48}{28}$ in $\mathbb{Q}/\mathbb{Z}$ is 7.

(b) Suppose that $\frac{m}{n} \in \mathbb{Q}/\mathbb{Z}$, where $m, n \in \mathbb{Z}$. Then clearly $n \cdot \frac{m}{n} = m \in \mathbb{Z}$, so that $\frac{m}{n}$ has order at most n and thus has finite order.

(c) For any positive integer n consider the element $\frac{1}{n} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$. Then $n\left(\frac{1}{n} + \mathbb{Z}\right) = 1 + n\mathbb{Z} = \mathbb{Z}$. Now, let k be the order of $\frac{1}{n} + \mathbb{Z}$. Then $\frac{k}{n} \in \mathbb{Z}$, so that $n \mid k$. Thus n is the order of $\frac{1}{n} + \mathbb{Z}$.

26. If $a \in \mathbb{Q}$ then $a + \mathbb{Z}$ has finite order, by Exercise 15. If $a \in \mathbb{R}$ and $a + \mathbb{Z}$ has order n in $\mathbb{R}/\mathbb{Z}$ then $na + Z = n(a + \mathbb{Z}) = 0 + \mathbb{Z}$, so that $na \in \mathbb{Z}$. Therefore $a = m/n$ for some integer m, and $a \in \mathbb{Q}$.

27. (a) Define $\varphi\colon G \to G^*$ by $\varphi(a) = (a, e)$. It is routine to check that φ is an isomorphism.
(b) If $a, g \in G$ and $h \in H$ then $(g, h)^{-1}(a, e)(g, h) = (g^{-1}ag, h^{-1}eh) = (g^{-1}ag, e) \in G^*$. Therefore G^* is normal, by Theorem 7.34.
(c) Define $\psi\colon H \to (G \times H)/G^*$ by $\psi(h) = G^*(e, h)$. The natural embedding $H \to G \times H$ sending h to (e, h) is a homomorphism, and the natural projection $\pi\colon G \times H \to H$ is a homomorphism. Therefore ψ is also a homomorphism. Injective. If $\psi(h) = \psi(h')$ then $(e, h'h^{-1}) = (e, h')(e, h)^{-1} \in G^*$ which implies that $h'h^{-1} = e$ and $h' = h$. Surjective. For any $(g, h) \in G \times H$ we have $\psi(h) = G^*(e, h) = G^*(g, e)(e, h) = G^*(g, h)$. Therefore ψ is an isomorphism.

28. Define $\alpha : G \to (G/M) \times (G/N)$ by $\alpha(g) = (Mg, Ng)$. Check that α is a homomorphism. Injective. If $\alpha(x) = \alpha(y)$ then $Mx = My$ and $Nx = Ny$. Therefore $xy^{-1} \in M \cap N = \{e\}$ so that $x = y$. Now let $H = Im\ \alpha$ be the image, a subgroup of $(G/M) \times (G/N)$. Then α induces an isomorphism $G \cong H$.

29. Let $g \in G$. Since gN has finite order in G/N, there exists an integer $r > 0$ with $g^rN = (gN)^r = N$, so that $g^r \in N$. This element of N has finite order so there exists an integer $s > 0$ with $(g^r)^s = e$. Then $g^{rs} = e$ and g has finite order.

30. Suppose gN has order n in G/N. Then $g^nN = (gN)^n = N$ so that $g^n \in N$. Since N is finite there exists $t > 0$ with $(g^n)^t = e$. Then g has finite order $k = |\text{g}|$. Hence $(gN)^k = g^kN = N$ so that $n \mid k$ by Theorem 7.8(2) and Theorem 7.8(3) implies that $|g^{k/n}| = n$ in G.

31. Suppose $Z(G) \neq G$ and $\neq \langle e \rangle$. Then Lagrange implies that $Z(G)$ has index p or q and Theorem 7.28 implies that $G/Z(G)$ is cyclic. Apply Theorem 7.38 to conclude G is abelian. But then $Z(G) = G$, contrary to hypothesis.

32. Suppose $N = \langle x_1,\ x_2, \dots,\ x_n \rangle$ and $G/N = \langle Ny_1,\ Ny_2, \dots,\ Ny_m \rangle$ for some $x_i, y_j, \in G$. Certainly $Ng \subseteq (x_1, x_2, . . . , x_n, g)$ for any $g \in G$. Therefore $G \subseteq \langle x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m \rangle$ and G is finitely generated.

33. (a) Answered in the Hint.
(b) Since $(G'a)(G'b) = G'ab = G'(aba^{-1}b^{-1})ba = G'ba = (G'b)(G'a)$. In fact, if N is a normal subgroup of G then Theorem 7.37 implies that G/N is abelian if and only if $G' \subseteq N$.

34. (a) $N = \{(x, -x) \mid x \in \mathbb{R}\}$. It is easy to see that N is closed under addition and negatives, so N is a subgroup.
(b) $(\mathbb{R} \times \mathbb{R})/N \cong \mathbb{R}$ Use the mapping $f : \mathbb{R} \to (\mathbb{R} \times \mathbb{R})/N$ defined by $f(x) = (x, -x)$.

35. (a) For any $n \in N$ and $g \in G$ we have $gn^{-1}g^{-1} \in gNg^{-1} = N$. Then $ngn^{-1}g^{-1} \in N \cap G' = \{e\}$ which implies that $ng = gn$. Therefore $N \subseteq Z(G)$.

(b) If $z \in Z(G)$ then $zg = gz$ for any $g \in G$, so that $(Nz)(Ng) = Nzg = Ngz = (Ng)(Nz)$. Hence $Nz \in Z(G/N)$. Conversely, if Na is in the center of G/N then $Nag = (Na)(Ng) = (Ng)(Na) = Nga$ for every $g \in G$. Therefore $aga^{-1}g^{-1} \in N$ and it clearly lies in G' as well. Therefore $aga^{-1}g^{-1} = e$ and $ag = ga$. Hence $a \in Z(G)$ so that $Na \in Z(G)/N$.

36. As in Exercise 7.4.33 the map $g : G \to Aut(G)$ defined by $g(u)(x) = uxu^{-1}$ is a homomorphism. By definition, the image of this map is *Inn* G, and we have a surjective homomorphism $g : G \to Inn\ G$. Define an induced map $\overline{g} : G/Z(G) \to Inn\ G$ by $\overline{g}\ (Z(G)u) = g(u)$. To prove $\overline{g}$ is well-defined suppose $Z(G)u = Z(G)v$. Then $vu^{-1} \in Z(G)$ and for any $x \in G$ we have $g(u)(x) = uxu^{-1} = uxv^{-1}(vu^{-1}) = (vu^{-1})uxv^{-1} = vxv^{-1} = g(v)(x)$. Therefore $g(u) = g(v)$ and $\overline{g}$ is well-defined. Verify that $\overline{g}$ is a surjective homomorphism. Injective. If $\overline{g}\ (Z(G)u) = \overline{g}(Z(G)v)$ then $g(u) = g(v)$ and $g(vu^{-1}) = 1_G$. Therefore $(vu^{-1})x(vu^{-1})^{-1} = x$ for every $x \in G$ and we conclude that $vu^{-1} \in Z(G)$ so that $Z(G)u = Z(G)v$.

37. Define $f : A/N \times B/N \to G/N$ by $f(Na, Nb) = Nab$. Well-defined. If $Na = Na'$ and $Nb = Nb'$ then $Nab = NaNb = Na'Nb' = Na'b'$ since N is normal. Claim. If $a \in A$ and $b \in B$ then $Nab = Nba$. Proof As in Exercise 7.6.28, consider $(aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in A \cap B = N$. This proves the Claim. Homomorphism. $f((Na, Nb)\cdot(Na', Nb')) = f(Naa', Nbb') = Naa'bb' = (Na)(Na')(Nb)(Nb') = (Na)(Nb)(Na')(Nb') = f(Na, Nb)f(Na', Nb')$ using the Claim. Injective. If $f(Na, Nb) = N$ then $ab \in N$ so that $a \in Nb^{-1} \subseteq B$. Then $a \in A \cap B = N$ and $Na = N$. Similarly $Nb = N$. Surjective. By hypothesis every $g \in G$ can be written as $g = ab$ for some $a \in A$ and $b \in B$. Then $Ng = f(Na, Nb)$.

8.4 Quotient Groups and Homomorphisms

1. The function is a homomorphism since $f((a+bi)+(c+di)) = f((a+c)+(b+d)i) = b+d = f(a+bi)+f(c+di)$. Its kernel is the set of all $a+bi$ such that $f(a+bi) = b = 0$, so that $\ker f = \{a+0i\} \subset \mathbb{C}$.

2. To see that g is a homomorphism, note that if x and y have the same sign, then $xy > 0$, so that $g(xy) = 0$. Since x and y have the same sign, $g(x) = g(y)$, so that in $\mathbb{Z}_2$, $g(x)+g(y) = 0$. Then in this case $g(xy) = 0$ and $g(x)+g(y) = 0$ so that $g(xy) = g(x)+g(y)$. If x and y have opposite signs, then $xy < 0$, so that $g(xy) = 1$. Also, one of $g(x)$ and $g(y)$ is 1 and the other is 0, so that $g(x)+g(y) = 1$. Thus again $g(xy) = g(x)+g(y)$, so g is a homomorphism. $\ker g$ is the set of nonzero reals whose image is zero; by definition of g, this is obviously $\mathbb{R}^{**}$, the set of positive real numbers.

3. h is a homomorphism since $h(xy) = (xy)^3 = x^3y^3 = h(x)h(y)$. Since $x^3 = 1$ implies that $x = 1$, we see that $\ker h = \{1\}$.

4. f is a homomorphism since $|xy| = |x|\cdot|y|$, so that $f(xy) = f(x)f(y)$. The identity element in both $\mathbb{Q}^*$ and $\mathbb{Q}^{**}$ is 1, and $f(x) = 1$ when $|x| = 1$, i.e., when $x = \pm 1$. The kernel of f is $\{-1, 1\}$.

5. g is a homomorphism since $g((q_1,n_1)+(q_2,n_2)) = g((q_1+q_2,n_1+n_2)) = n_1+n_2 = g((q_1,n_1)) + g((q_2,n_2))$. $\ker g$ is the set of all elements whose image is $0 \in \mathbb{Z}$, but $g((x,y)) = y = 0$ exactly when $y = 0$, so that the kernel of g is $\mathbb{Q} \times \{0\} \subset \mathbb{Q} \times \mathbb{Z}$.

6. h is a homomorphism since $h(xy) = (xy)^4 = x^4y^4 = h(x)h(y)$. The identity element of $\mathbb{C}^*$ is 1, so $\ker h$ is the set of elements of $\mathbb{C}^*$ whose fourth power is 1, i.e. the fourth roots of unity. These are $\{1, -1, i, -i\}$.

7. If σ and τ are both even or both odd, then $\sigma\tau$ is even, so that $f(\sigma\tau) = 0$. But in this case $f(\sigma) = f(\tau)$ since the two permutations have the same parity, so that $f(\sigma) + f(\tau) = 0$ in $\mathbb{Z}_2$. Thus $f(\sigma\tau) = f(\sigma) + f(\tau)$. If one of σ and τ is even and the other is odd, then $\sigma\tau$ is odd, so that $f(\sigma\tau) = 1$. But in this case one of $f(\sigma)$ and $f(\tau)$ is 1 and the other is 0, so that $f(\sigma) + f(\tau) = 1$. Thus again $f(\sigma\tau) = f(\sigma) + f(\tau)$, so that f is a homomorphism. The kernel of f is the set of permutations whose image is $0 \in \mathbb{Z}_2$, which is obviously the set of even permutations.

8. Answered in the text.

9. Homomorphism. $f(a + b) = ([a + b]_2, [a + b]_4) = \{[a]_2 + [b]_2, [a]_4 + [b]_4) = f(a) + f(b)$.

10. Homomorphism with kernel $\{e\}$.

11. If $[a]_n = [b]_n$, then $[ra]_k = f([a]_n) = f([b]_n) = [rb]_k$. The middle equality holds since $[a]_n = [b]_n$.

12. The function is well-defined by Exercise 11 (with $n = 12$, $k = 6$, $r = 1$). It is a homomorphism since (using the addition $[a]_n + [b]_n = [a + b]_n$ in $\mathbb{Z}_n$)

$$h([a]_{12} + [b]_{12}) = h([a + b]_{12}) = [a + b]_6 = [a]_6 + [b]_6 = h([a]_{12}) + h([b]_{12}).$$

To see that it is surjective, choose $x \in \mathbb{Z}_6$ and choose any a so that $x = [a]_6$. Then $x = [a]_6 = h([a]_{12})$. The kernel of h is elements of $\mathbb{Z}_{12}$ which are congruent to 0 (mod 6); these elements are $[0]_{12}$ and $[6]_{12}$, so that the kernel is $\{[0]_{12}, [6]_{12}\}$. This is a two-element group, so it must be congruent to $\mathbb{Z}_2$, and in fact $[6]_{12} + [6]_{12} = [12]_{12} = [0]_{12}$.

13. This function is well-defined by Exercise 11 (with $n = 16$, $k = 4$, and $r = 3$). It is a homomorphism since (using the addition $[a]_n + [b]_n = [a + b]_n$ in $\mathbb{Z}_n$)

$$h([a]_{16} + [b]_{16}) = h([a + b]_{16}) = [3(a + b)]_4 = [3a + 3b]_4 = [3a]_4 + [3b]_4 = h([a]_{16}) + h([b]_{16}).$$

To see that it is surjective, choose $x \in \mathbb{Z}_4$, and choose any a such that $3x = [a]_4$. Then $3x \equiv a \pmod 4$, so that $3 \cdot 3x \equiv 3a \pmod 4$, i.e., $x \equiv 3a \pmod 4$, so that $x = [3a]_4$. Then $x = [3a]_4 = h([a]_{16})$, so that h is surjective. Now, $[a]_{16} \in \ker h$ means that $[3a]_4 = [0]_4$, so that $3a \equiv 0 \pmod 4$ and thus $3 \cdot 3a \equiv 3 \cdot 0 \equiv 0 \pmod 4$. Thus $a \equiv 0 \pmod 4$. So the kernel consists of congruence classes modulo 16 that are $0 \pmod 4$; these classes are $[0]_{16}$, $[4]_{16}$, $[8]_{16}$, and $[12]_{16}$. Thus the kernel is a group of order 4; since $[4]_{16} + [4]_{16} = [8]_{16} \neq [0]_{16}$, it has an element that is not of order 2, so it must be congruent to $\mathbb{Z}_4$ rather than to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

14. Answered in the text.

15. Define $f : \bar{H} \to H : (e_G, h) \mapsto h$. Clearly f is surjective. It is also clear that it is injective: if $f((e_G, h)) = f((e_G, k))$, then using the definition of f gives $h = k$. Thus it is a bijection, and it is a homomorphism since

$$f((e_G, h)(e_G, k)) = f((e_Ge_G, hk)) = f((e_G, hk)) = hk = f((e_G, h))f((e_G, k)).$$

Thus f is an isomorphism, so that $\bar{H} \cong H$.

16. Note that for $z \in$ ₵ $*$, $f(z) = |z|^2$ and the homomorphism property follows from the usual "norm property": $|zw| = |z||w|$. A simple proof can also be given using just the definition of multiplication in ₵.
<u>Surjective</u>. If $r \in \mathbb{R}^{**}$ then $\sqrt{r}$ is real and $f(\sqrt{r}) = r$.

17. (a) Answered in the text.
(b) $\langle 0 \rangle$, $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{20}$

18. Suppose that $f : D_4 \to G$ is a surjective homomorphism. Then if $K = \ker f$, we have $D_4/K \cong G$, and $|D_4/K| = [D_4 : K]$, which by Lagrange's Theorem must divide $|D_4| = 8$. Thus any homomorphic image of D_4 must have order 1, 2, 4, or 8. Clearly the trivial group is a homomorphic image of D_4 under the map $f : D_4 \to \{0\} : x \mapsto 0$. Also, the only group of order 8 that is a homomorphic image of D_4 is D_4 itself, since if $f : D_4 \to G$ is a surjective homomorphism with trivial kernel, then $D_4 \cong G$ by the first isomorphism theorem. This leaves groups of order 2 and 4. By Example 1 in Section 8.3, we know that $N = \{r_0, r_1, r_2, r_3\}$ is a normal subgroup with $D_4/N \cong \mathbb{Z}_2$, so that $\mathbb{Z}_2$ is a homomorphic image of D_4. By Example 2 in the same section, we know that $M = \{r_0, r_2\}$ is a normal subgroup with $D_4/M \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, so that $\mathbb{Z}_2 \times \mathbb{Z}_2$ is a homomorphic image of D_4. The only remaining possibility is $\mathbb{Z}_4$. Now, if $f : D_4 \to \mathbb{Z}_4$ is a surjective homomorphism, its kernel must be a normal subgroup of D_4 of order 2, so it must be generated by an element of order 2. The elements of order 2 in D_4 are r_2, h, v, d, and t. We know from the above that $D_4/\langle r_2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Also, $\{r_0, h\}$ is not normal, since for example $r_1 h r_1^{-1} = r_1 h r_3 = r_1 t = v \notin \{r_0, h\}$. Similarly, none of $\{r_0, v\}$, $\{r_0, d\}$, or $\{r_0, t\}$ is normal. Thus $\{r_0, r_2\}$ is the only normal subgroup of order 2, so that $\mathbb{Z}_4$ is not a homomorphic image of D_4. So the only homomorphic images of D_4 are $\{0\}$, D_4, $\mathbb{Z}_2$, and $\mathbb{Z}_2 \times \mathbb{Z}_2$.

19. Since $|S_3| = 6$, homomorphic images of S_3 must have order 1, 2, 3, or 6. Clearly the trivial group is a homomorphic image of S_3 under the map $f : S_3 \to \}0\} : x \mapsto 0$. Also, the only group of order 6 that is a homomorphic image of S_3 is S_3 itself, since if $f : S_3 \to G$ is a surjective homomorphism with trivial kernel, then $S_3 \cong G$ by the first isomorphism theorem. This leaves groups of order 2 and 4. By Exercise 15 in Section 8.2, A_3 is a normal subgroup of S_3; since $|A_3| = 3$, we know that S_3/A_3 must have two elements so is isomorphic to $\mathbb{Z}_2$. If S_3 has a group of order 3 as a homomorphic image, that group is perforce isomorphic to $\mathbb{Z}_3$, so that there must be a surjective homomorphism $f : S_3 \to \mathbb{Z}_3$. If N is the kernel of this map, then N must be a normal subgroup of S_3 of order 2, so it consists of (1) together with an element of S_3 of order 2. Those elements are (12), (13), and (23). However, $\{(1), (12)\}$ is not normal in S_3 since for example $(123)(12)(123)^{-1} = (123)(12)(132) = (23) \notin \{(1), (12)\}$. So S_3 has no normal subgroups of order 2. Thus the only homomorphic images of S_3 are the trivial group, S_3 itself, and $\mathbb{Z}_2$.

20. (a) Use list in Exercise 7.3.37 and the discussion of Theorem 7.43 These subgroups are: $\{H\}$, $\{H, 3 + H\}$, $\{H, 2 + H, 4 + H\}$ and $\mathbb{Z}_{12}/H$.
(b) $\{K\}$, $\{K, 2 + K\}$ and $\mathbb{Z}_{20}/K$.

21. If $K = ker\ f$ then Theorem 7.39 and the simplicity of G imply mat K is either $\langle e \rangle$ or G. If $K = \langle e \rangle$ then f is injective (by Theorem 7.40), so that f is an isomorphism. If $K = G$ then $H = f(G) = \{e\}$.

22. (a) $K = \{a \in G \mid a^2 = e\}$. If a, $b \in K$ then $(ab)^2 = a^2b^2 = e$ so $ab \in K$. If $a \in K$ then $a^{-1} = a \in K$. Hence K is a subgroup.
(b) If x^2, $y^2 \in H$ then $x^2y^2 = (xy)^2$ and $(x^2)^{-1} = (x^{-1})^2$ lie in H. Hence H is a subgroup.
(c) Define $f : G \to H$ by $f(x) = x^2$. It is easily checked that f is a surjective homomorphism and its kernel is K. The First Isomorphism Theorem then implies $G/K \cong H$.

23. It suffices to show that H is closed under the operation of G. Suppose that $a, b \in H$. Then $N(ab) = (Na)(Nb)$ since N is normal in G. But $a \in H$, so that $Na \in T$; similarly $Nb \in T$. Since T is a subgroup of G/N, it follows that $(Na)(Nb) \in T$. Thus $N(ab) \in T$, so by definition of H, we get $ab \in H$. Thus H is a subgroup of G.

24. Well-defined. If $[x]_n = [y]_n$ then $n \mid (x - y)$. Then $k \mid n$ implies that $k \mid (x - y)$ and $[x]_k = [y]_k$. Homomorphism. $f([x]_n[y]_n = f([xy]_n) = [xy]_k = [x][y]_k = f([x]_n)f([y]_n)$.
The kernel $K = \{x \in U_n \mid x \equiv 1 \pmod{k}\}$. Compare Exercise 7.3.36. Is this map f also surjective?

25. Define $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} : (a, b) \mapsto a - b$. To see that f is surjective, choose $x \in \mathbb{Z}$. Then $x = f((x, 0)) = x - 0$. Also, f is a homomorphism, since

$$f((a,b) + (c,d)) = f((a+c, b+d)) = (a+c) - (b+d) = (a-b) + (c-d) = f((a,b)) + f((c,d)).$$

If $K = \ker f$, then $(\mathbb{Z} \times \mathbb{Z})/K \cong \mathbb{Z}$ by the First Isomorphism Theorem. So it remains to determine $\ker f$. But $f((a,b)) = a - b = 0$ if and only if $a = b$, so that $\ker f = \{(a,a)\} = \{a(1,1)\} = \langle(1,1)\rangle$ and thus $(\mathbb{Z} \times \mathbb{Z})/\langle(1,1)\rangle \cong \mathbb{Z}$.

26. Define $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}_2 : (a, b) \mapsto (a - b, [b]_2)$. To see that f is surjective, choose $x \in \mathbb{Z}$. Then $f((x, 0)) = (x - 0, [0]_2) = (x, [0]_2)$ and $f((x+1, 1)) = (x + 1 - 1, [1]_2) = (x, [1]_2)$. Thus each element of $\mathbb{Z} \times \mathbb{Z}_2$ is in the image of f, so that f is surjective. Also, f is a homomorphism since

$$\begin{aligned} h((a,b) + (c,d)) = h((a+c, b+d)) &= ((a+c) - (b+d), [b+d]_2) = ((a-b) + (c-d), [b]_2 + [d]_2) \\ &= (a-b, [b]_2) + (c-d, [d]_2) = h((a,b)) + h((c,d)). \end{aligned}$$

If $K = \ker h$, then $(\mathbb{Z} \times \mathbb{Z})/K \cong \mathbb{Z} \times \mathbb{Z}_2$ by the First Isomorphism Theorem. So it remains to determine $\ker h$. Now, $f((a,b)) = (a - b, [b]_2) = (0, [0]_2)$ if and only if b is even and $a - b = 0$. Thus $\ker f = \{(2b, 2b)\} = \{b(2,2)\} = \langle(2,2)\rangle$ and thus $(\mathbb{Z} \times \mathbb{Z})/\langle(2,2)\rangle \cong \mathbb{Z} \times \mathbb{Z}_2$.

27. Define φ: $G \times H \to G/M \times H/N$ by $\varphi(g, h) = (Mg, Nh)$. It is easy to check that φ is a surjective homotnorphism and that the kernel is exactly $M \times N$. Apply Theorems 7.39 and 7.42 to conclude that $M \times N$ is normal and $(G \times H)/(M \times N) \cong G/M \times H/N$.

28. The determinant mapping $f : GL(2, \mathbb{R}) \to \mathbb{R}^*$ is a surjective homomorphism with kernel $SL(2, \mathbb{R})$. The claims follow from Theorems 7.39 and 7.42.

29. Define $f : \mathbb{Z}_n \to \mathbb{Z}_k : [a]_n \mapsto [a]_k$. This is well-defined by Exercise 11. It is surjective, since if $x \in \mathbb{Z}_k$, choose a with $x = [a]_k$; then $x = [a]_k = f([a]_n)$. It is a homomorphism since

$$f([a]_n + [b]_n) = f([a+b]_n) = [a+b]_k = [a]_k + [b]_k = f([a]_n) + f([b]_n).$$

It remains to determine the kernel of f. Now, $f([a]_n) = [a]_k$ if and only if $k \mid a$, so that the congruence classes in $\mathbb{Z}_n$ that are taken to zero by f are the congruence classes containing multiples of k, which are $0, k, 2k, \ldots, (n/k - 1)k = \langle k\rangle$. Thus $\ker f = \langle k\rangle$, so that $\mathbb{Z}_n/\langle k\rangle = \mathbb{Z}_k$.

30. By Theorem 7.20(3), $\operatorname{Im} f$ is a subgroup of H, so that by Lagrange's Theorem, $|\Im f|$ divides $|H|$. Let $K = \ker f$. Then by the First Isomorphism Theorem, since $f : G \to \operatorname{Im} f$ is a surjective homomorphism of groups, $G/K \cong \operatorname{Im} f$. But then

$$|\operatorname{Im} f| = |G/K| = [G : K] = |G| \,/\, |K|$$

again by Lagrange's Theorem. Thus $|\operatorname{Im} f|$ divides $|G|$.

31. Define $f : \mathbb{Z} \to \mathbb{Z}_3 \times \mathbb{Z}_4 : a \mapsto ([a]_3, [a]_4)$. This is a homomorphism, since

$$f(a+b) = ([a+b]_3, [a+b]_4) = ([a]_3 + [b]_3, [a]_4 + [b]_4) = ([a]_3, [a]_4) + ([b]_3, [b]_4) = f(a) + f(b).$$

To see that it is surjective, choose $(x, y) \in \mathbb{Z}_3 \times \mathbb{Z}_4$. Then $[x]_3 = [x+3]_3 = [x+6]_3 = [x+9]_3$, and also $[x+9]_4 = [x+1+8]_4 = [x+1]_4$ and $[x+6]_4 = [x+2+4]_4 = [x+2]_4$. So one of those four is congruent to $y \pmod 4$. Set a equal to that number, so that $([a]_3, [a]_4) = (x, y)$. Then $f(a) = (x, y)$. It remains to determine $\ker f$. Now, $f(a) = ([a]_3, [a]_4) = (0, 0)$ if and only if $a \equiv 0 \pmod 3$ and $a \equiv 0 \pmod 4$. But a is divisible by 3 and 4 if and only if it is divisible by 12, so that $f(a) = (0, 0)$ if and only if $a \equiv 0 \pmod{12}$. Thus $\ker f = \langle 12 \rangle$, so that $\mathbb{Z}/\langle 12 \rangle = \mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$.

32. Suppose that Mx and My are two representatives of the same coset of M in G. Then $xy^{-1} \in M$, so that $x = ym$ for some $m \in M$. But then

$$g(Mx) = Nf(x) = Nf(ym) = Nf(y)f(m) = f(y)Nf(m) = f(y)N = Nf(y) = g(My)$$

since $f(M) \subseteq N$ and N is normal in H. Thus g is well-defined. Since M is normal in G, we get that G/M is a group; the map is a homomorphism since

$$g((Mx)(My)) = g(Mxy) = Nf(xy) = Nf(x)f(y) = Nf(x)Nf(y) = g(Mx)g(My)$$

again using normality.

33. Answered in the text.

34. (a) $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{bmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{bmatrix} = \begin{pmatrix} 1 & a+a' & b+ac'+b' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$. Therefore G is a group.

(b) $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ lies in the center if and only if $b + ac' + b' = b' + a'c + b$ for every a', $b' \in \mathbb{Q}$. This occurs if and only if $a = c = 0$. Then C is the set of all matrices of the form $\begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ Define $\varphi : \mathbb{Q} \to C$ by setting $\varphi(b)$ to be the matrix above. By formula in part (a), check that φ is an isomorphism.

(c) Define $f : G \to \mathbb{Q} \times \mathbb{Q}$ by $f\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = (a, c)$. The formulas in part (a) show that f is a homomorphism and it is certainly surjective with kernel equal to C. The First Isomorphism Theorem applies.

35. Define $f\colon G \to \mathbb{R}^*$ by $f(T_{a,b}) = a$. Homomorphism. $f(T_{a,b} \circ T_{c,d}) = f(T_{ac,\ ad+b}) = ac = f(T_{a,b})f(T_{c,d})$. Surjective. For any $a \in \mathbb{R}^*$, $a = f(T_{a,0})$. The kernel is exactly the subgroup H. By Theorem 7.39 H is normal, and the First Isomorphism Theorem implies that $G/H \cong \mathbb{R}^*$.

36. K and N are normal subgroups of G. The injectivity of f implies that $K \cap N = \{e\}$. Claim, $G = NK$. Proof. Let $g \in G$. Then $f(g) \in H$ and the surjectivity of the restriction of f implies that $f(g) = f(n)$ for some $n \in N$. Therefore $f(n^{-1}g) = e$ so that $n^{-1} g \in K$ and $g \in nK \subseteq NK$.
The result now follows using Exercise 7.6.28.

37. Since $\mathbb{Q}^*$ is abelian, $\mathbb{Q}^{**}$ is a normal subgroup. Now, with $f : \mathbb{Q}^* \to \mathbb{Q}^{**} : x \to |x|$, the restriction of f to $\mathbb{Q}^*$ is the identity map, since $|x| = x$ for $x > 0$. Thus this situation satisfies the conditions of Exercise 36, where $G = \mathbb{Q}^*$ and $N = H = \mathbb{Q}^{**}$. It follows that $\mathbb{Q}^* \cong \mathbb{Q}^{**} \times \ker f$. But by Exercise 4, $\ker f = \{-1, 1\}$, which is a two-element multiplicative group and thus isomorphic to $\mathbb{Z}_2$. Thus $\mathbb{Q}^* \cong \mathbb{Q}^{**} \times \mathbb{Z}_2$.

38. By Theorem 7.44 and Exercise 19 there is a bijection between the set S of normal subgroups of G which contain N and the set T of all normal subgroups of G/N. Therefore G/N is simple if and only if the only normal subgroups of G containing N are N and G.

39. The given map T is easily seen to be a group homomorphism.
Surjective. For any $g(x) = c_0 + c_1x + \ldots + c_nx^n \in \mathsf{Z}[x]$ we have $\mathsf{Z} + g(x) = T(h(x))$ where $h(x) = c_1 + c_2x + \ldots + c_nx^{n-1}$.
Infective. If $f(x)$ is in the kernel then $xf(x) \in \mathsf{Z}$. Comparing degrees shows that $f(x) = 0$. Then T is injective by Theorem 7.40.

40. (a) Since N is normal in G we have $g^{-1}Ng = N$ for every $g \in G$. In particular this holds for every $g \in NK$, so N is normal in NK.
(b) f is certainly a homomorphism since N is normal. Surjective. If $g \in NK$ then $g = nk$ for some $n \in N$ and $k \in K$. Then $Ng = Nnk = Nk = f(k)$. Kernel. An element $k \in K$ lies in the kernel if and only if $Nk = N$. Equivalently, $k \in K \cap N$.
(c) Apply the First Isomorphism Theorem.

41. (a) Claim. $f_x \circ f_y = f_{yx}$. Proof. $(f_x \circ f_y)(Kb) = (f_x(f_y(Kb)) = Kbyx = f_{yx}(Kb)$. Since $f_e = \imath$ is the identity map we see that $f_{a^{-1}}$ is the inverse of the map f_a. Therefore f_a is a bijection, that is, a permutation.
(b) Using the Claim above we have $\varphi(xy) = f_{(xy)^{-1}} = f_{y^{-1}x^{-1}} = f_{x^{-1}} \circ f_{y^{-1}} = \varphi(x) \circ \varphi(y)$. An element a is in the kernel if and only if $Kba = Kb$ for every $b \in G$. Equivalently $bab^{-1} \in K$ so that $a \in b^{-1} Kb$ for every $b \in G$. Therefore kernel $\varphi = \cap\, b^{-1} Kb$ where the intersection is taken over all $b \in G$. In particular, kernel $\varphi \subseteq K$.
(c) If K is normal then $b^{-1}Kb = K$ for every b and kernel $\varphi = K$.
(d) When $K = \langle e \rangle$, every right coset is a singleton and $T = G$. Also kernel $\varphi = \langle e \rangle$ and by Theorem 7.40, φ is injective. Cayley's Theorem easily follows.

42. (a) Apply Exercise 7.7.1.

We will prove the results in (b) and (c) assuming the Second Isomorphism Theorem, given in Exercise 24.

(b) Let G be metabelian with its special subgroup N as above. By the First Isomorphism Theorem any homomorphic image of G is isomorphic to G/K for some normal subgroup K of G. By Exercise 7.6.18, NK is a normal subgroup of G. The Third Isomorphism Theorem says that $(G/K)/(NK/K) \cong G/NK \cong (G/N)/(NK/N)$ which is a homomorphic image of the abelian group G/N. The Second Isomorphism Theorem implies that $NK/K \cong N/(N \cap K)$ which is a homomorphic image of the abelian group N. Since a homomorphic image of an abelian group is also abelian, the subgroup NK/K in G/K shows that G/K is metabelian.

(c) For G and N as above let H be a subgroup of G. Then $H \cap N$ is a subgroup of the abelian group N. The Second Isomorphism Theorem implies that $H \cap N$ is normal in H and $H/(H \cap N) \cong HN/N$ which is a subgroup of the abelian group G/N. Therefore H is metabelian using the subgroup $H \cap N$.

8.5 The Simplicity of A_n

1. (a) Answered in the text.
   (b) $e = (123)(132)$; the 8 3-cycles are obviously products of 3-cycles. $(12)(34) = (123)(234)$, $(13)(24) = (132)(243)$, $(14)(23) = (143)(243)$.

2. (a) The order of A_n is $n!/2$. When $n = 2$ this equals 1.
   (b) $|A_3| = 3!/2 = 3$ and any group of order 3 is cyclic.

3. $\langle e \rangle$ A direct computation.

4. $\langle e \rangle$. This follows from the simplicity, since the center is a normal subgroup.

5. $\sigma = \tau_1 \ . \ . \ . \ \tau_n$ where $\tau_\iota^2 = e$ and these τ commute. Then $\sigma^2 = e$.

6. By Exercise 30 in Section 8.2, any subgroup of index 2 is normal. Since $|A_5| = 60$, a subgroup of order 30 would be normal. But since A_5 is simple, it has no proper normal subgroups.

7. By Exercise 23 in Section 7.5, these four elements form a subgroup N. The elements of A_4 other than these elements are (123), (132), (124), (142), (134), (143), (234), and (243). The following table shows the result of computing gng^{-1} where g is one of these three-cycles and $n \in N$. It is clear that in all cases, $gng^{-1} \in N$, so that N is normal:

$n \quad g$	(123)	(132)	(124)	(142)	(134)	(143)	(234)	(243)
(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)	(1)
(12)(34)	(14)(23)	(13)(24)	(13)(24)	(14)(23)	(14)(23)	(13)(24)	(13)(24)	(14)(23)
(13)(24)	(12)(34)	(14)(23)	(14)(23)	(12)(34)	(12)(34)	(14)(23)	(14)(23)	(12)(34)
(14)(23)	(13)(24)	(12)(34)	(12)(34)	(13)(24)	(13)(24)	(12)(34)	(12)(34)	(13)(24)

8. (Assume $n \geq 3$.) As in Exercise 7.6.32 the subgroup of order 2 must lie in the center, contrary to Exercise 6.

9. Since $\sigma^2 = e$ for every $\sigma \in N$ it follows from Exercise 7.9.13 that $\sigma = e$ or σ is a product of disjoint 2-cycles. If σ, τ are nonidentity elements of N then $\sigma\tau = e$ implies that $\sigma = \tau^{-1} = \tau$. Therefore $|N| \leq 2$.

10. Since $N \cap A_n = A_n$, it follows that $N \supseteq A_n$ (since $x \in A_n$ implies that $x \in N \cap A_n$ implies that $x \in N$). Clearly $N \subseteq S_n$. Now, $|N|$ divides $|S_n|$ by Lagrange's Theorem. But since $|S_n| / |A_n| = 2$ and $A_n \subseteq N$, we must have $|S_n| / |N| \leq 2$, so that it equals 1 or 2. If it equals 1, then obviously $N = S_n$, while if it equals 2, then obviously $N = A_n$.

11. Any subgroup of index 2 in S must be normal (see Exercise 7.6.20). Apply Corollary 7.55.

12. Let K be the kernel of f. By Corollary 7.55, $K = (1)$, A_n or S_n. If $A_n \subseteq K$ then $f(A_n) = (1) \subseteq A_n$. Otherwise $K = (1)$ and f is an isomorphism. Then $f(A_n)$ is a subgroup of index 2 in S_n and Exercise 10 applies.

Chapter 9

Topics in Group Theory

9.1 Direct Products

1. If $(a, b) \in G \times H$ then the order is $|(a, b)| = lcm\ \{|a|, |b|\}$. With this information the numerical questions here are easily done.

2. $4{\cdot}2{\cdot}6{\cdot}4 = 192$.

3. (a) Answered in the text. (b) $\{(0, 0)\}$ is the subgroup of 1 element; there are 7 subgroups of 2 elements; there are 7 subgroups of 4 elements; there is 1 subgroup of 8 elements (namely, the whole group).

4. Define $\varphi : G \times H \to H \times G$ by $\varphi(x, y) = (y, x)$ and verify that it is an isomorphism.

5. $\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic.

6. (a) $\mathbb{Z}_{12} \cong \mathbb{Z}_3 \times \mathbb{Z}_4$. Explicitly let $A = \langle [4]_{12} \rangle$ and $B = \langle [9]_{12} \rangle$ and show that $\mathbb{Z}_{12} = A \times B$.
   (b) $Z_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_5$
   (c) $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_{15} \cong \mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_5 \times \mathbb{Z}_6$

7. $(\Rightarrow)$ Clear since G_i is isomorphic to a subgroup of the product.
   $(\Leftarrow)$ $(a_1, a_2, \ldots)(b_1, b_2, \ldots) = (a_1b_1, a_2b_2, \ldots) = (b_1a_1, b_2a_2, \ldots) = (b_1, b_2, \ldots)(a_1, a_2, \ldots)$.

8. Since $\pi_i(e_1, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) = a_i$ the projection map is surjective. The homomorphism property follows quickly from the definitions.

9. No. $\mathbb{Z}_4 \times \mathbb{Z}_2$ has no element of order 8.

10. (a) Since f, g are bijective it is routine to check that θ is bijective. Also $\theta((a, b){\cdot}(a', b')) = \theta(aa', bb') = (f(aa'), g(bb')) = (f(a)f(a'), g(b)g(b')) = (f(a), g(b)){\cdot}(f(a'), g(b')) = \theta(a, b) \cdot (a', b')$.
    (b) *Induction* on n. The case $n = 2$ is done in (a). Suppose $n > 2$. By the inductive hypothesis $G_1 \times \ldots \times G_{n-1} \cong H_1 \times \ldots \times H_{n-t}$. Apply (a) to complete the proof.

11. Let $\alpha : K \to M \times N$ bean isomorphism with $\alpha(x) = (\alpha_1(x), \alpha_2(x))$. Define $\varphi : H \times K \to H \times M \times N$ by $\varphi(h, k) = (h, \alpha_1(k), \alpha_2(k))$. Verify that φ is an isomorphism.

12. (a) Define $\varphi_i : G_1 \times \cdots \times G_n \to G_1 \times \cdots \times G_{i-1} \times G_{i+1} \times \cdots \times G_n$ by

$$\varphi_i((g_1, g_2, \ldots, g_{i-1}, g_i, g_{i+1}, \ldots, g_n)) = (g_1, g_2, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n).$$

It is easy to see that this is a homomorphism, since the operation in the cross product is the component-wise operations. Further, the kernel of φ_i is exactly $\bar{G}_i$. Thus $\bar{G}_i$ is a normal subgroup.

(b) Define $\delta_i : G_i \to G_1 \times \cdots \times G_n : x \mapsto (e_1, \ldots, e_{i-1}, x, e_{i+1}, \ldots, e_n)$. Then δ_i is obviously injective, and $\operatorname{Im} \delta_i = \bar{G}_i$. Also, δ_i is a homomorphism since the operation in the cross-product is simply the component-wise operation. Thus $G_i \cong \bar{G}_i$.

(c) If $g = (g_1, \ldots, g_n)$, then $\delta_i(\pi_i(g)) = \delta_i(g_i) = (e_1, \ldots, e_{i-1}, g_i, e_{i+1}, \ldots, e_n)$. Thus

$$g = \delta_1(\pi_1(g))\delta_2(\pi_2(g)) \ldots \delta_n(\pi_n(g)),$$

so every element of $G_1 \times \ldots \times G_n$ can be written as a product of elements of $\bar{G}_1, \ldots, \bar{G}_n$. But this representation is clearly unique, since in any product of elements from the $\bar{G}_1, \ldots, \bar{G}_n$, the i^{th} component is e_i except in $\bar{G}_i$. Theorem 9.1 then gives us that $G_1 \times \cdots \times G_n$ is the internal direct product of its subgroups $\bar{G}_1, \ldots, \bar{G}_n$.

13. (a) Closure under multiplication and inverses is easily verified.
(b) (⇒) Answered in the text. (⇐) $G \times G \times G$ is abelian so every subgroup is normal.

14. If k is any common multiple of $|a_1|, \ldots, |a_n|$ then $a_i^k = e_i$ for every index i. Therefore $(a_1, \ldots, a_a)^k = (e_1, \ldots, e_n)$. The order of this element is the smallest positive such k. That is the 1cm.

15. Define $\sigma \in S_n$ by $\sigma(j) = i_j$. Define the map f from $G_1 \times \ldots \times G_n$ to $G_{i_1} \times \ldots \times G_{i_n}$ by $f(a_1, \ldots, a_n) = (a_{\sigma(1)}, \ldots, a_{\sigma(1)}, \ldots, a_{\sigma(n)})$. Verify that this f is an isomorphism.

16. View $G = NK$ as an internal direct product so that $xy = yx$ for every $x \in N$ and $y \in K$. For any $a \in M$ we have $(xy)^{-1}a(xy) = y^{-1}(x^{-1}ax)y = x^{-1}ax \in M$ since M is normal in N.

17. Every element $r \in \mathbb{Q}^*$ can be uniquely written as $r = \varepsilon \cdot |r|$ where $\varepsilon = \pm 1$ and $|r|$ is the absolute value of r. Apply Theorem 8.1.

18. $U_{16} = \{1, 3, 5, 7, 9, 11, 13, 15\}$. Clearly $\{1, 15\}$ is a subgroup since $15^2 = 225 \equiv 1 \pmod{16}$. This subgroup must be isomorphic to $\mathbb{Z}_2$, since this is the only group of order 2. Also, $\{1, 3, 9, 11\}$ is a subgroup since $3^2 = 9$, $3 \cdot 9 = 27 \cong 11 \pmod{16}$, and $3 \cdot 11 = 33 \cong 1 \pmod{16}$. Since 3 has order four in the subgroup, the subgroup is cyclic, so is isomorphic to $\mathbb{Z}_4$. Hence U_{16} has subgroups M and N isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_4$ respectively, and $M \cap N = \{1\}$. But also $11 \cdot 15 = 165 \equiv 5 \pmod{16}$, $9 \cdot 15 = 135 \equiv 7 \pmod{16}$, and $3 \cdot 15 = 45 \equiv 13 \pmod{16}$, so that $U_{16} = MN$ (the other elements of U_{16} are already in either M or N, so are in the product). Thus by Theorem 9.3, $U_{16} = \{1, 15\} \times \{1, 3, 9, 11\} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

19. (a) $f^*(xy) = (f_1(xy), \ldots, f_n(xy)) = (f_1(x)f_1(y), \ldots, f_n(x)f_n(y)) = f^*(x)f^*(y)$. Also $\pi_i(f^*(x)) = \pi_i(f_1(x), \ldots, f_n(x)) = f_i(x)$.
(b) If g is any such homomorphism then as in Exercise 12 $g(x) = \delta_1(\pi_1(g(x))) \ldots \delta_n(\pi_n(g(x)) = \delta_1(f_1(x)) \ldots \delta_n(f_n(x) = f^*(x)$.

20. Suppose $g \in G$ can be expressed in 2 ways: $g = a_1. . .a_n = b_1. . .b_n$ where a_i, $b_i \in N_i$. Then $(a_1^{-1}b_1) . . . (a_n^{-1}b_n) = e$ since G is abelian. Then the hypothesis implies $a_i^{-1}b_i = e$ for each i, so that $a_i = b_i$. Apply Theorem 8.1.

21. If $G = H \times K$ then use δ_i. and π_i. as in Exercise 12. Conversely suppose δ_i and $\pi_{i;}$ are given. Define $H^* = \delta_1(H)$ and $K^* = \delta_2(K)$. These are subgroups of G, automatically normal since G is abelian. Since $\pi_i^{\circ}\delta_1$ is the identity, δ_i is injective so that $H \cong H^*$ and $K \cong K^*$. The condition $\delta_1\pi_1+\delta_2\pi_2 = 1_G$ implies $H^* + K^* = G$. The conditions $\pi_i\delta_j = 0$ imply that $H^* \cap K^* = \{0\}$, and Theorem 8.3 applies.

22. Let $g \in G$ and $h \in H$ be generators, so $|g| = n$ and $|h| = m$. Lagrange's Theorem implies that $n \mid |G|$ and $m.| \; |H|$ By Exercise 14, $|(g, h)| = 1cm\{n, m\}$. The result follows since $1cm\{n, m\} = nm$ if and only if $(n, m) = 1$.

23. (a) Answered in the text. (b) Use the same example.

24. No. Use die example of 23(a) noting that M is normal in S_3.

25. Induction on k. Let $H = N_1. . .N_{k-1}$. Then H is a normal subgroup (see Exercise 7.6.18) and by hypothesis $H \cap N_k = \langle e\rangle$. By Theorem 8.3 $G \cong H \times N_k$. Apply the induction hypothesis to H.

26. We use a modified statement and prove it by induction on k.
<u>Claim</u>, Let N_i be normal subgroups of a finite group G. Then $|N_1. . .N_k|$ divides $|N_1|. . .|N_k|$ with equality if and only if and only if $N_1. . .N_k \cong N_1 \times . . . \times N_k$.
<u>Proof</u>. Suppose $k \geq 2$ and let $H = N_1. . .N_{k-1}$. Then H is normal and $|N_1. . .N_k| = |H|\cdot|N_k \; | / | \; H \cap N_k|$, using the Second Isomorphism Theorem (see Exercise 7.8.24). By the induction hypothesis (or trivially if $k = 2$) this divides $|N_1|. . .|N_{k-1}|\cdot|N_k \; | / | \; H \cap N_k|$ which divides $|N_1|. . .|N_k|$. Equality holds here if and only if $|H| = |N_1|. . .|N_{k-1}|$ and $H \cap N_k = \langle e\rangle$. By induction (or trivially if $k = 2$), this occurs if and only if $H \cong N_1 \times . . . \times N_{k-1}$ and $H \cap N_k = \langle e\rangle$. Apply Theorem 8.3.

27. (a) Use the subgroups in the answer to Exercise 23.
(b) Let $N = \langle r_1\rangle$ and $H = \langle h\rangle$.
(c) Use $N = A_4$ and $H\langle(12)\rangle$.

28. <u>Claim</u>. If G is nonabelian with $|G| < 12$ then G is indecomposable.
<u>Proof</u>. If not then $G = A \times B$ for proper subgroups A, B. Then $|A|$, $|B| \leq |G| \; /2 < 6$ so that A, B are abelian (see Theorems 7.28 and 7.29). But then G would also be abelian (see Exercise 7).
This Claim settles (a), (b)
(c) Any two nonzero subgroups of $\mathbb{Z}$ meet nontrivially. (Compare Exercise 30.)

29. The only nonzero subgroups are $\langle 1\rangle$, $\langle p\rangle$, $\langle p^2\rangle$, . . . $\langle p^{n-1}\rangle$. Since any two of these meet nontrivially, the group is indecomposable.

30. If A_1, A_2 are nonzero subgroups of $\mathbb{Q}$ let $a_i / b_i \in A_i$ be nonzero elements. Then $a_1a_2 = (a_2b_1)$. $a_1 / b_1 = (a_1b_2) \cdot a_2 / b_2$ is in $A1 \cap A2$. Then $\mathbb{Q}$ cannot be the direct product of A_1 and A_2.

31. $\mathbb{Z}$ is indecomposable but $\mathbb{Z}_6$ is decomposable.

32. Apply the definition of "indecomposable".

33. This is a straightforward check of the definitions.

34. If $c = (c_1, c_2, \ldots) \in \Sigma\ G_i$. and $a = (a_1, a_2, \ldots) \in \Pi\ G_i$ then $a^{-1}ca = (a_1^{-1}c_1a_1, a_2^{-1}c_2a_2, \ldots)$. Whenever $c_i = e_i$ we also have $a_i^{-1}c_ia_i = e_i$. Therefore $a^{-1}ca \in \Sigma\ G_i$ and it is normal.

35. The proof of Theorem 8.1 is easily adapted to this case.

36. Define $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ by $f([a]_{mn}) = ([a]_m, [a]_n)$ and note that f is a ring homomorphism. If $(m, n) = 1$ then the kernel is $\{0\}$ and f is injective. Since the orders of these rings are equal it follows that f is an isomorphism. Since isomorphic rings have isomorphic unit groups the result follows. (Compare Lemma 8.8 and Corollary 13.5.)

37. Let $G = G_1 \times \ldots \times G_n$ with projections] $\pi_i.$: $G \to G_i$. By hypothesis there is a unique $g^* : G \to H$ with $\tau_i{}^\circ g^* = \pi_i$. Exercise 19 provides a unique homomorphism $f^* : H \to G$ with $\pi_i{}^\circ f^* = \tau_i$. Now $g^*f^* : H \to H \to H$ is the unique homomorphism with $\tau_i{}^\circ g^*f^* = \tau_i$. It follows that $g^*f^* = 1_H$. Similarly $f^*g^* = 1_G$. Therefore f^* and g^* are isomorphisms.

9.2 Finite Abelian Groups

1. Answered in the text.

2. pG is the image of the homomorphism f: $G \to G$ defined: $f(x) = px$. Checking the homomorphism property is routine.

3. (a), (c), (e), (g) are answered in the text.
   (b) $\mathbb{Z}_{15}$ (d) $\mathbb{Z}_8 \oplus 2_9$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.
   (f) Use the decompositions: $2^4 = 2^3 2^1 = 2^2 2^2 = 2^2 2^1 2^1 = 2^1 2^1 2^1 2^1$ combined with $3^2 = 3^1 3^1$ to get 10 non-isomorphic groups.
   (h) $1160 = 2^3 5^1 29^1 = 2^2 2^1 5^1 29^1 = 2^1 2^1 2^1 5^1 29^1$ yields 3 groups.

4. Since $f(x) = px$ is a homomorphism we have $pG = pG_1 + \ldots + pG_n$. This sum is easily seen to be direct.

5. (a), (c) are answered in the text. (b) 2, 2, 2^2, 3, 3, 3^2 (d) 2, 2^2, 2^2, 2^4, 3, 3, 3, 5, 5, 5^2

6. (a) 250 (b) 6, 6, 36 (c) 2, 10, 20, 40 (d) 2, 60, 60, 1200

7. (a) 2,2, and 2,2 (b) 16 and 16 (c) 2,4 and 2 ,4
   (d) 2, 2, 2, 2 and 2, 2, 2, 2

8. Elements of $G(p)$ are $n/p^k + \mathbb{Z}$

9. (a) Answered in the text, (b) Since $n/2^k + \mathbb{Z} = 2(n/2^{k+1} + \mathbb{Z})$ we see that $2 \cdot G(2) = G(2)$ when $G = \mathbb{Q}/\mathbb{Z}$.

10. The homomorphism property is easy to check. Suppose $a \in G$ is given and let $p^k = |a|$. Since $(p, n) = 1$ there exist integers x, y such that $nx + p^k y = 1$. Then $a = x(na) + y(p^k a) = xf(a)$. Injective. If $f(a) = 0$ then $a = 0$. Surjective. $a = f(xa)$.

11. Note that $p\mathbb{Z}_p{}^{\text{n}} = \{0\}$ if and only if n $= 1$. Apply Theorem 8.7.

12. The Fundamental Theorem 8.7 says that G is isomorphic to a direct sum of cyclic groups of prime power order. Since $|G|$ is the product of these prime powers, some power of p must occur. Then one of the direct summands must be $\mathbb{Z}_p{}^k$ for some $k \geq 1$ Then G contains an element of order p^k and hence an element of order p by Theorem 7.8.

13. Answered in the text.

14. Exercise 13 implies that $|G(p_i)| = p_i{}^{k1}$ for some k_1. By Theorem 8.5 we know that $p^t m = |G| = |G(p_1)| \ldots |G(p_n)| = p_1{}^{kl} \ldots p_n{}^{kn}$ where $p = p_1$, and $p_1, \ldots, p_n$ are distinct primes. It follows that $t = k_l$.

15. Say $|G| = p^t m$ where $(p, m) = 1$, Then $n \leq t$. The Fundamental Theorem implies that $G(\text{p}) \cong \mathbb{Z}_p{}^{k1} \oplus \ldots \oplus \mathbb{Z}_{pk1}$ where $t = k_1 + \ldots + k_3$. Note that $p\mathbb{Z}p^k$ is a subgroup of order p^{k-1}. Altering one summand in this way we find subgroups of every order $p^1, \text{p}^{1-1}, \ldots, p^2, p$.

16. This occurs if and only if n is squarefree (*i.e.* either $n = 1$ or n is a product of one or more distinct primes).

17. (a), (b) Compare the elementary divisors and apply Theorem 8.12.

18. Using Exercise 15 it follows that if d / n (and $d > 0$) there is a subgroup N of G with $|N| = d$. Applying this to $d = n/k$ we use $H = G/N$.

19. (a) Answered in the text. (b) If $a + T$ is of finite order in G/T, $n(a + T) = 0 + T$ for some positive integer n. Then $na \in T$ so it has finite order, say k. But then $kna = 0$ and a itself has finite order, so that $a \in T$. Then $0 + T$ is the only element of finite order in G/T.

20. Not necessarily. As in the Hint, $(1, 1) + (-1, 0) = (0, 1)$ is a sum of two elements of infinite order equal to one of finite order in $\mathbb{Z} \oplus \mathbb{Z}_3$.

21. Let $h \in G$ with $f(h) = 1$, and set $H = \langle h \rangle$. Let K be the kernel of f. For any $x \in G$ we have $f(x) = f(h^n)$ for some $n \in \mathbb{Z}$ so that $xh^{-n} \in K$ and $x \in h^n K \subseteq HK$. Then $G = HK$ and certainly $H \cap K = \langle \text{e} \rangle$. Apply Theorem 8.3.

22. First let us suppose G and H are p-groups. Let $N_G(m)$ be the number of elements of G with order p^m. Recall that Zp^n has unique subgroup of order p^k for every $k = 1, 2, \ldots, n$ (by Exercise 7.3.40). Therefore the number of elements of order p^k in $\mathbb{Z}p^n$ is a function $\varphi(p^k)$ independent of n, as long as $n \geq k$. (This is often called the Euler φ-function.)

Now suppose the invariant factors of G are p, p,.., p^2, p^2, ... where there are k_j copies of p_j, for each j, and each k_j. ≥ 0. Then $N_G(p) = (k_1 + k_2 + k_3 + \ . \ . \ .)\varphi(p)$, $N_G(p^2) = (k_2 + k_3 + \ . \ . \ .)\varphi(p^2)$, $N_G(p^3) = (k_3 + \ . \ . \ .)\varphi(p^3)$, *etc.* Consequently, $k_m = NG(p^{m+1})/\varphi(p^{m+1}) - N_G(p^m)/\varphi(p^m)$ is determined entirely by the values of N_G, Therefore if $N_G = N_H$ it follows that G and H have the same elementary divisors and hence are isomorphic.

The extension of the argument beyond the case of p-groups is left to the reader.

23. The equation $x^m = e$ has almost m solutions in G. The proof of Theorem 7.41 (or Corollary 8.11) applies to G.

24. Given the invariant factors m_1, m_2, ..., m_1 in a divisor chain, we can re-build the elementary divisors: Factor $m_3 = p_1^{k_{ij}} \cdots p_s^{k_{sj}}$. The divisor conditions imply: $0 \leq k_{i1} \leq \mathrm{k}_{i2} \leq \ . \ . \ . \leq k_{it}$. for each i = 1, 2, ..., s. The elementary divisors are then easily read off this array: p_1^{k11}, p_1^{k12}, . . . , p_1^{k11}, p_2^{k21}, . . . , p_2^{k2}, . . . , p_s^{ks1} . . . , p_s^{kst}, where we omit any entry equal to 1. Now apply Theorem 8.12.

25. By Lemma 8.4: If $a \in G$ then $a = \Sigma a_p$ where $a_p \in G(p)$. The sum is taken over all prime numbers p, noting that $a_p = 0$ for all but finitely many p (since $a_p \neq 0$ only if p divides $|a|$). The proof of the uniqueness is the same as in the proof of Theorem 8.5, using the finiteness of the sums to reduce to the case there. By Exercise 8.1.5 conclude that $G \cong \Sigma G(p)$.

9.3 The Sylow Theorems

1. $H_1 = \{e, (abcd), (ac)(bd), (adcb)\}$. There are 45 subgroups of this type. (There are 6·5·4·3 = 360 ways of choosing an ordered 4-tuple from 6 symbols, and each 4-cycle can be written 4 ways: 360/4 = 90. Such a group contains 2 4-cycles, so we have 90/2 = 45 subgroups.)
   $H_2 = \{e, (abcd)(ef), (ac)(bd), (adcb)(ef)\}$ Similarly there are 45 subgroups of this type.
   $H_3 = \{e, (ab), (cd), (ab)(cd)\}$. There are 45 subgroups of this type. (There are 15 2-cycles and each appears in 6 such groups, and each group is counted twice here, so we get $15 \cdot 6/2 = 45$ subgroups.)
   $H_4 = \{e, (ab), (cd)(ef), (ab)(cd)(ef)\}$. There are 45 subgroups of this type. (There are 15 2-cycles each appearing in 3 such groups.)
   $H_5 = \{e, (ab)(cd), (ac)(bd), (ad)(bc)\}$. There are 15 subgroups of this type. (There are 15 subsets of 4 elements from 6 symbols, and each such S_4 contains one such subgroup.)
   Altogether we have discovered 195 subgroups of order 4 in S_6.

2. (a) $H = \{e, (13), (24), (13)(24), (12)(34), (14)(23), (1234), (1432)\}$. Permuting the symbols yields 3 such subgroups.
   (b) $K = \{e, (123), (132)\}$. Permuting symbols yields 4 such subgroups, one for each copy of S_3 in S_4.

3. Answered in the text.

4. $\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \{0\}$, $\{0\} \times \{0\} \times \mathbb{Z}_5$.

5. (a) 1 or 4 (b) 1 or 6.

6. $115 = 5{\cdot}23$, $143 = 11{\cdot}13$, $391 = 17{\cdot}23$. In each case Corollary 8.18 applies to provide a unique group of each order.

7. (a) The number of Sylow p-subgroups must be 1 for a suitable prime p in each case, (a) $p = 7$ (b) $p = 5$ (c) $p = 11$ (d) $p = 17$.

8. If q is a prime $\neq p$, and q divides $|G|$ then Cauchy's Theorem implies that G has an element of order q, contrary to hypothesis. Therefore $|G|$ has only p as a prime divisor, so it is a power of p.

9. Answered in the text.

10. By Exercise 8.4.24, H is contained in some Sylow p-subgroup P of G. If K is any Sylow p-subgroup then the Second Sylow Theorem implies that $K = xPx^{-1}$ for some $x \in G$. Then since H is normal, $H = xHx^{-1} \subseteq xPx^{-1} = K$.

11. No. Inner automorphisms preserve a subgroup only when it is normal.

12. No. Let $G = S_4$, $H = S_3$ and $p = 3$ with $K = \{e, (124), (142)\}$.

13. Answered in the text.

14. Any Sylow p-subgroup has index 2 so it must be normal, by Exercise 7.6.20.

15. (a) Define $f : H \times K \to HK$ by $f(x, y) = xy$. Generally this is not a homomorphism, but it certainly is surjective. If $f(h, k) = f(h_1, k_1)$ then $hk = h_1k_1$ and $h_1^{-1}h = k_1k^{-1} \in H \cap K = \langle e \rangle$. Then $h = h_1$, and $k = k_1$ so that f is injective. Then f is a bijection so the orders of the two sets coincide.
    (b) The argument above shows that if $f(h, k) = f(h_1, k_1)$ then there is some $w \in H \cap K$ where $h_1 = hw_{-1}$ and $k_1 = wk$. Therefore every image element in HK arises from exactly $|H \cap K|$ pre-images. Consequently, $|H \times K| = |HK|{\cdot}|H \cap K|$.

16. Let P be the normal Sylow 3-subgroup and consider G/P. It is a group of order 20 and hence must have a normal Sylow 5-subgroup M (by the Third Sylow Theorem). Then by Theorem 7.44, there is a normal subgroup N of G such that N/P is isomorphic to M. Hence N has order 15 so it contains at least one Sylow 5-subgroup of G. The normality of N implies that N contains all the Sylow 5-subgroups of G (by the Second Sylow Theorem). Since $|N| = 15$ it has a unique Sylow 5-subgroup (by the Third Sylow Theorem), and therefore G must have a unique Sylow 5-subgroup.

17. Let n_p denote the number of Sylow p-subgroups. By the Third Sylow Theorem deduce that $n_7 = 1$ and $n_3 = 1$ or 7. As in the proof of Corollary 8.18, if $n_3 = 1$ then G is cyclic. Since this is false by hypothesis conclude that $n_3 = 7$.

18. By the Third Sylow theorem the number n_7 of Sylow 7-subgroups must divide $168/7 = 24$ and satisfy $n_7 \equiv 1 \pmod 7$. Therefore $n_7 = 1$ or 8. Since G is simple Corollary 8.16 shows that $n_7 > 1$. Therefore $n_7 = 8$.

19. Suppose $|G| = pq$ where $p > q$. By the first part of the proof of Corollary 8.18, the Sylow p-subgroup is normal.

20. Let n_f be the number of Sylow p-subgroups. By the Third Sylow Theorem, n_p divides m and $n_p \equiv 1 \pmod{p}$. But then $n_p \le m < p$ forcing $n_p = 1$. Then by Corollary 8.16, the Sylow p-subgroup is normal and G is not simple.

21. Answered in the text.

22. Let n_p denote the number of Sylow p-subgroups in G. By the Third Sylow Theorem $n = 1$ or q and $n_a = 1$, p or p^2. If G is simple, $n_p = q$ so that $q \equiv 1 \pmod{p}$ and $p \mid (q-1)$. In particular, $p < q$. Similarly if $n_q = p$ then $q < p$, a contradiction. Therefore $n_q = p$ and there are $p\ (q-1)$ elements in G of order q. That leaves only p^2 elements of order $\neq q$. Since there exists a Sylow p-subgroup of order p^2 it must consist exactly of those remaining p^2 elements. But then it is unique, and $n_p = 1$, a contradiction.

23. (a) Let A be a Sylow 5-subgroup and B a Sylow 7-subgroup. Let n_p be the number of Sylow p-subgroups. The Third Sylow Theorem implies that $n_7 =1$ or 15 and $n_5 =$ l or 21. If $n_7 = 15$ then there are $15{\cdot}6 = 90$ elements of order 7. If $n_5 = 21$ then there are $21{\cdot}4 = 84$ elements of order 5. These cannot both occur, so Corollary 8.16 implies that A or B is normal. Then AB is a subgroup (see Exercise 7.6.18) and Exercise 16 implies AB has order 35.

    (b) The Third Sylow Theorem implies $n_5 = 1$ so that the Sylow 5-subgroup P is normal. Let H be any subgroup of order 3 (use Cauchy's Theorem). The argument in (a) shows that PH has order 15.

24. The Second Isomorphism theorem (Exercise 7.8.24) implies that $[K : K \cap N] = [NK : N]$, Computing $[NK : K \cap N]$ in two ways (see Exercise 7.8.18) then implies that $[N : K \cap N] = [NK : K]$ which divides $[G : K]$, Since $[G : K]$ is relatively prime to p it follows that $[N : K \cap N]$ is prime to p. Also since $|K|$ is a power of p Lagrange's Theorem implies that $|K \cap N|$ is a power of p. Therefore $K \cap N$ is a Sylow p-subgroup of N.

25. The number n_r of Sylow r-subgroups is $1,\ p,\ q$ or pq by the Third Sylow Theorem. Suppose $n_r \neq 1$. Since $n_r \equiv 1 \pmod{r}$ and $r > p, q$, conclude that $n_r = pq$. Then the number of elements of order r is $pq\ (r-1)$. Similarly the number of order p is $n_p(p-1)$ and the number of order q is $n_q(q-1)$. Counting all these elements and the identity e, yields: $pqr - pq + n_p(p-1) + n_p(q-1) + 1 \le |G| = pqr$. Then $n_p(p-1) + n_q(q-1) \le pq - 1$. If $n_q \neq 1$ then the Third Sylow Theorem implies $n_q \ge$ r and the inequality yields a contradiction. Therefore $n_q =1$ and there is a normal Sylow q-subgroup Q, by Corollary 8.16. (From here we know that G is not simple.)

    Consider the homomorphism $\pi : G \to G/Q$. As in the proof of Corollary 8.18, me group G/Q of order pr has a unique Sylow r-subgroup. Therefore there are exactly r elements in G/Q satisfying the equation $x^r = e$. Since π is a q-to-1 mapping it follows that there are exactly qr elements of G satisfying the condition $x^r \in Q$. The pq$(r-1)$ elements of order r and the q elements of Q satisfy this condition. Therefore: $pq(r-1) + q \le qr$. This is a contradiction since $p > 1$. Therefore the hypothesis $n_r \neq 1$ fails.

9.4 Conjugacy and the Proof of the Sylow Theorems

1. (a) Answered in the text.
   (b) {e}, {(12), (13), (14), (23), (24), (34)} {(12)(34),(I3)(24),(I4)(23)}, {(123), (124), (132), (134), (142), (143), (234), (243)}, {(1234), (1243), (1324), (1342), (1423), (1432)}.
   (c) {e}, {(12)(34), (13)(24), (14)(23)}, {(123), (134), (142), (243)}, {(132), (124), (143), (234)}.

2. Done in the Hint.

3. Answered in the text.

4. $$\begin{aligned} f(Cy) = f(Cx) &\Rightarrow y^{-1}ay = x^{-1}ax && \textit{[Definition of } f\textit{]} \\ &\Rightarrow a = yx^{-1}axy^{-1} && \textit{[Left multiply by } y \textit{ and right multiply by } y^{-1}\textit{]} \\ &\Rightarrow a = (xy^{-1})^{-1}a(xy^{-1}) && \textit{[Definition of inverse; see Corollary 7.6(a)]} \\ &\Rightarrow (xy^{-1})a = a(xy^{-1}) && \textit{[Left multiply by } xy^{-1}\textit{]} \\ &\Rightarrow xy^{-1} \in C = C(a) && \textit{[Definition of the centralizer } C(a)\textit{]} \\ &\Rightarrow Cx = Cy && \textit{[Theorem 8.2; cosets are disjoint or equal]} \end{aligned}$$

   Thus $f(Cy) = f(Cx)$ implies that $Cy = Cx$, so that f is an injective map of cosets.

5. ⟨((123)⟩. ⟨((124)⟩, ⟨((134)⟩, ⟨((234)⟩

6. Since H is normal in K we know that $X^{-1}HX = H$ for every $x \in K$. Therefore $K \subseteq N(H)$ by definition.

7. (a) If $x \in A$ the closure implies $x^{-1}Ax = A$ so that $x \in N(A)$. Therefore A is a subgroup of $N(A)$.
   (b) By definition, $g \in N(A)$ if and only if $g^{-1}Ag = A$. Multiply on the left by g to see that this is equivalent to: $Ag = gA$.

8. For $x \in G$, and $y \in N$ then $xy = yx$ so that $x^{-1}yx = x \in N$. Therefore $x^{-1}Nx = N$.

9. Let $a \in C$. If $b \in C$ then $b = x^{-1}ax$ for some $x \in G$, and $f(b) = f(x)^{-1}f(a)f(x)$ is conjugate to $f(a)$. The implications are reversible, so that $f(C) =$ the conjugacy class of $f(a)$.

10. Suppose a, $b \in H$. Let $a = a_1, a_2, \ldots, a_m$ be the conjugates of a and $b = b_1, b_2, \ldots, b_n$ be the conjugates of b. Since $x^{-1}(ab)x = (x^{-1}ax)(x^{-1}bx)$, every conjugate of ab is one of the a_ib_j. Then the conjugacy class of ab has at most mn elements, and $ab \in H$. Also the conjugacy class of a^{-1} is just $a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1}$ so that $a^{-1} \in H$.

11. Suppose $|G| = n = p_1^{e1}p_2^{e2}. . .p_k^{ek}$ where the p$_j$. are distinct primes and $m_j > 0$. By Sylow there is a subgroup P_j. of order p_j^{ej}. Since m|n the factorization is $m = p_1^{f1}p_2^{f2}. . .p_k^{fk}$ for some integers f_j. with $0 \leq f_j. \leq e_j$ By repeated application of Exercise 22 (an induction!) there exists a subgroup $Q_j \subseteq P_j$ of order p_j^{fj}. Since G is nilpotent it is a direct product of the subgroups P_j. Therefore the subgroup $H = Q_1\ Q_2 \ldots\ Q_k$ is a direct product of the $Q_j's$ and $|H| = m$.

12. If f is any automorphism of N then $f(K)$ is another Sylow p-subgroup of N. Then Corollary 8.16 implies that $f(K) = K$. Now if $x \in G$ then $x^{-1}Nx = N$ so that $f : N \to N$ defined $f(a) = x^{-1}ax$ is an automorphism of N. Therefore $x^{-1}Kx = f(K) = K$ as above.

13. Write $A \sim B$ if A is H-conjugate to B. Since $A = e^{-1} Ae$, $A \sim A$. If $A \sim B$ then $B = x^{-1}Ax$ for some $x \in H$. Then $A = xBx^{-1}$ and $B \sim A$. If $A \sim B$ and $B \sim C$ then $B = x^{-1}Ax$ and $C = y^{-1}$ By for some $x, y \in H$. Then $C = (xy)^{-1} A(xy)$ and $xy \in H$ so that $A \sim C$.

14. (a) If $a \in N$ then $x^{-1}ax \in x^{-1}Nx = N$. Therefore $C \subseteq N$. The converse is clear.
    (b) If $C_i \cap N$ is not empty then part (a) implies $C_i \subseteq N$.
    (c) This follows easily from part (b).

15. Answered in the text. As one special case conclude that if G is a non-trivial p-group then $Z(G) \neq \langle e \rangle$.

16. If $g, h \in N(A)$ then $(gh)A = g(Ah) = (Ag)h = A(gh)$ so $gh \in N(A)$, Also $gA = Ag$ implies $Ag^{-1} = g^{-1}A$ so that $g^{-1} \in N(A)$. Therefore $N(A)$ is a subgroup.

17. $x^{-1}Ax = y^{-1}Ay \Leftrightarrow A = (yx^{-1})^{-1} A (yx^{-1}) \Leftrightarrow yx^{-1} \in N(A)$. If $x, y \in H$ then $yx^{-1} \in H \cap N(A)$ and $(H \cap N(A))x = (H \cap N(A))y$. The converse also holds. This provides a bijection between the set of H-conjugates of A and the right cosets of $H \cap N(A)$ in H.

18. The Second and Third Sylow Theorems imply that the number of conjugates of K in G equals the number of Sylow p-subgroups and this number is $\equiv 1 \pmod{p}$. By Theorem 8.25 this number is the index of the normalizer: $[G : N(K)] \equiv 1$ (mod p). Since $N(K) \subseteq H$ this argument also applies to K as a Sylow p-subgroup of H: $[\,H : N(K)] \equiv 1$ (mod p). Since the indexes multiply it follows that $[G : H] \equiv 1 \pmod{p}$.

19. Answered in the text.

20. There are $m = [G : N(H)]$ distinct conjugates of H in G. Note that $m \cdot |H| \leq m \cdot |N(H)| = G$ by Lagrange. Any two of these conjugates have at least $\{e\}$ in common, possibly more. Therefore the number of elements in the union of all the conjugates of H is at most $1 + m \cdot (|H| - 1) = m–|H| - (m - 1) \leq |G| - (m - 1) \leq |G|$. If this union is all of G these inequalities are equalities, implying m=l. But then $G = N(H)$ and H is normal in G. Then the only conjugate of H is H itself, and G = union of the conjugates = H. But H is a proper subgroup.

21. Answered in the text.

22. From Exercise 15, or by Theorem 8.27 below, we know that $Z(G) \neq \{e\}$. (Compare Theorem 8.27.) To solve the problem, use induction on n, and assume $n \geq 2$. Since $Z(G)$ is nontrivial there exists $a \in Z(G)$ with $|a| = p$ (by Cauchy). The subgroup $N = \langle a \rangle$ is normal in G (by Exercise 8) and Lagrange implies that G/N has order p^{n-1}. By the induction hypothesis there is a subgroup T of G/N having $|T| = p^{n-2}$. By Theorem 7.44 there is a subgroup H of G with $N \subseteq H$ and $T = H/N$. Therefore $|H| = |T|$-$|N| = p^{n-1}$.

23. As in Exercise 22 we use induction on n. Suppose H is a subgroup of G of index p. By Exercise 15 there exists $a \in H \cap Z(G)$ of order p. Let $N = \langle a \rangle$ and use Theorem 7.44 to see that H/N has index p in G/N. By inductive hypothesis H/N is normal in G/N and Theorem 7.44 implies that H is normal in G.

24. Every H-conjugacy class has order dividing $|H|$ which is a p-power. Since there are t Sylow p-subgroups and $(p, t) = 1$ there must be some H-conjugacy class of these subgroups of order 1. Then there is a Sylow p-subgroup K where $x^{-1}Kx = K$ for every $x \in H$. But then Lemma 8.26 implies that $x \in K$ and we conclude that $H \subseteq K$.

9.5 The Structure of Finite Groups

1. Theorem 8.30 applies except in the case $p^2 \equiv 1 \pmod{q}$. In that case $q \mid (p-1)(p+1)$. Certainly q cannot divide $p - 1$, since $p < q$. Therefore $q \mid (p+1)$ so that $p < q \leq p + 1$. But then $q = p + 1 \equiv 1$ (mod p), contrary to hypothesis.

2. The number n_3 of Sylow 3-subgroups must equal 1 or 4, by the Sylow Theorems. If $n_3 = 1$ the Sylow 3-subgroup is normal. Otherwise $n_3 = 4$ and we count 8 elements of order 3. This leaves only 4 elements of order $\neq 3$. Since a Sylow 2-subgroup has 4 elements it fills up those 4 elements and therefore it must be unique, hence normal.

3. By Theorem 9.33, since S_3 has order 6, it is isomorphic to either $\mathbb{Z}_6$ or D_3. But it cannot be isomorphic to $\mathbb{Z}_6$ since it is not abelian. Thus $S_3 \cong D_3$.

4. (a) The missing corner of the table is:

e	a^3	a^2	a
a	e	a^3	a^2
a^2	a	e	a^3
a^3	a^2	a	e

(b) A direct comparison of the operation tables does show that the correspondence described in an isomorphism. Details are omitted.

5. (a) Answered in the text.
(b) A direct comparison of the operation tables does show that the correspondence described in an isomorphism. Details are omitted.

6. There are Theorems classifying groups of order p, p^2, $6, 8, 12$, pq (when $p < q$ and $q \not\equiv 1$ (mod p)), and $p^z q$ (when $q \not\equiv 1 \pmod{p}$ and $p^2 \not\equiv 1 \pmod{q}$). *H*ere p and q are distinct odd primes. These cases include the numbers: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 19, 22, 23, 25, 26, 29, 31, 33, 34, 35, 37, 38, 41, 43, 46, 47, 49, 51, 53, 58, 59, 61, 65, 67, 69, 71, 73, 74, 77, 79, 82, 83, 85, 86, 87, 89, 91, 94, 95, 97, 99.

7. By Exercise 8.3.13 G is the direct product of its Sylow subgroups. Since these Sylow subgroups are cyclic of relatively prime orders, Theorem 8.9 implies that G is cyclic.

8. Let $r = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $d = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ Then $r^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ and $r^m d = \begin{pmatrix} -1 & m \\ 0 & 1 \end{pmatrix}$. Therefore G is contained in the group $H = \langle r, d \rangle$. Since the coefficients are in $\mathbb{Z}_n$ we see that $|r| = n$ and $|d| = 2$. Moreover $r^{-1}d = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} = dr$. By Theorem 8.32, $H \equiv D_n$ is a group with 2n elements. But G has $2n$ elements listed. Conclude that $G = H$.

9. Define a map $f: D_p \rightarrow G$ by $f(r^1) = a^1$ and $f(r^1 d) = a^1 b$ whenever $0 \leq i < p$. This map is certainly a well-defined bijective map. Since r and a both have order p these formulas hold for every integer i. Then $f(r^i r^j) = f(r^{i+j}) = a^i + a^j = a^i a^j = f(r^i)f(r^j)$ and similarly for $f(r^i \cdot r^j d)$. From $dr = r^{-1}d$ deduce that $dr^k = r^{-k}d$. Then $r^i d \cdot r^j = r^{i-j}d$ and $r^i d \cdot r^j d = r^{i-j}$. Analogous formulas hold with a, b in place of r, d. The homomorphism properties for $f(r^i d \cdot r^j)$ and for $f(r^i d \cdot r^j d)$ now follow easily.

10. D_6 is generated by r and d such that $|r| = 6$. $|d| = 2$ and $dr = r^{-1}d$, Then $r^3 \in Z(D_6)$ because $dr^3 = r^{-3}\text{d} = r^3\text{d}$. Therefore $K = \langle r^3 \rangle$ is a normal subgroup of order 2. Let $H = \langle r^2, d \rangle$. Since $|r^2| = 3$ and $dr^2 = r^{-2}\text{d}$ it follows that $H \equiv D_3 \cong S_3$. Since H has index 2 it is normal, and certainly $H \cap K = \langle e \rangle$. Counting shows that HK has 12 elements so that $G = HK$ and Theorem 8.3 implies that $G = H \times K$.

11. (a) From $r^k = r^{-k}$ conclude that r^k and d commute. Therefore r^k commutes with every $r^i d$ and $r^k \in Z(D_n)$.

(b), (c) For the dihedral group D_n we always assume $n \geq 3$. Then $r^2 \neq e$ so that $r^j d \cdot r = r^{j-1}d \neq r^{j+1}d = r \cdot r^j d$. This says that $r^j d \notin Z(D_n)$. Then every element of the center is of the form r^j. From $r^j d = dr^j = r^{-j}d$, conclude that $r^{2j} = e$, and hence $n|2j$. If n is odd this implies $n|j$ so that $r^j = e$. Consequently, $Z(D_a) = \langle e \rangle$. If $n = 2k$ is even then $k|j$ and the only central elements are e and r^k.

12. (a) By the proof of Theorem 9.32, the elements of D_n are $\{e, r, r^2, \ldots, r^{n-1}, d, rd, r^2 d, \ldots, r^{n-1}d\}$. Then it is clearly that φ is surjective, since if $\bar{r}^i d^j$ is an element of D_e (for $0 \leq i \leq 2, 0 \leq j \leq 2$), then $\bar{r}^i d^j = \varphi(r^i d^j)$. To see that it is a homomorphism, write

$$\begin{aligned}\varphi(r^i d^j r^k d^l) = \varphi(r^i r^{-k} d^{j+l}) = \varphi(r^{i-k} d^{j+l}) = \bar{r}^{i-k} d^{j+l} = \bar{r}^i \bar{r}^{-k} d^j d^l &= \bar{r}^i d^j \bar{r}^k d^l \\ &= \varphi(r^i d^j)\varphi(r^k d^l).\end{aligned}$$

Thus φ is a surjective homomorphism. If $\bar{r}^i d^j = e \in D_3$, then clearly $j = 0$ and i is a multiple of 3. The only elements of D_6 satisfying these restrictions are $r^0 d^0 = r^0$ and $r^3 d^0 = r^3$. Thus the kernel of φ is the subgroup $\{r^0, r^3\}$ of D_6.

(b) Since $r^0 = e$ in D_n, the kernel of φ is $\{e, r^3\}$, which, by Exercise 11(b), is equal to $Z(D_6)$. Since $\varphi : D_6 \rightarrow D_3$ is a surjective homomorphism with kernel $\{e, r^3\} = Z(D_6)$, the First Isomorphism Theorem shows that $D_6/Z(D_6) \cong D_3$.

13. $Z(Q) = \{1, -1\}$.

14. Certainly the subgroups $\langle e \rangle$ and Q are normal. Any subgroup of order 4 is normal by Exercise 7.6.20. It is not hard to see that -1 is the only element of order 2. Therefore there is only one subgroup of order 2 in Q, and his certainly normal. This covers all the possibilities.

15. $b^6 = (b^2)^3 = (a^3)^3 = a^9 = a$ so that $ab = b^6b = bb^6 = ba$ and G is abelian.

16. (a) The powers of a and b are easily computed. Also ba = ((12)(123), 2+1) = ((23), 3) and $a^{-1}\ b$ = ((132)(12),-2+l) = ((23), 3) are equal.
    (b) The 12 elements can be written explicitly. Alternatively note that $\langle a\rangle$ is a subgroup of 6 elements and $b \notin \langle a\rangle$ since the second component is odd. Then $T = \langle a\rangle \cup \langle a\rangle b$ contains 12 elements.
    (c) Certainly $a^ia^j = a^{i+j} \in T$ and $a^i{\cdot}a^jb = a^{i+j}b \in T$. Since $ba^k = a^{-k}b$ show that $a^ib{\cdot}a^j = a^{i-j}b$ and $a^ib{\cdot}a^jb = a^i{\cdot}a^{-j}{\cdot}b^2 = a^{i\text{-}j+3} \in T$. Therefore T is a subgroup by Theorem 7.11.
    (d) The element b has order 4 in T but D_6 has no element of order 4. The element a has order 6 in T but A_4 has no element of order 6.

17. Suppose G is simple and $|G| = p^mk$ where $p\not| k$. From the Third Sylow Theorem, the number of Sylow p-subgroups must equal 1. By Corollary 8.16, the Sylow p-subgroup is normal in G. Since G is simple it must equal its Sylow p-subgroup, so $n = p^m$, By Exercise 8.4.23 G has a normal subgroup of order p^{m-1}, and the simplicity implies $m - 1{=}0$. But then $|G| = p$, contrary to the hypothesis that n is composite.

18. Suppose G is a group and K is a subgroup of index n. Then G acts on the set T of the n right cosets of K in G. This action induces a homomorphism $\varphi : G - A(T) = S_n$ as in Exercise 7.8.25. Moreover ker φ is contained in K and by the First Isomorphism Theorem, $G/\ker\varphi$ is isomorphic to a subgroup of S_n. In particular, the index $[G : \ker\ \varphi]$ divides $n!$. If G is simple then ker φ must be $\langle e\rangle$ and $|G|$ divides $n!$.

19. Suppose $|G| = 21$. By the Sylow Theorems there is a unique Sylow 7-subgroup A. Then $A = \langle a\rangle$ where $|a| = 7$. Let b be any element of order 3 (which exists by Sylow theory). Then a and b generate G. The element bab^{-1} must lie in A so that $bab^{-1} = a^k$ for some k between 0 and 7. Then $b^2ab^{-2} = b(bab^{-1})^{-1} = b(a^k)b^{-1} = (bab^{-1})^k = (a^k)^k = a^{k2}$. Similarly $a = b^3ab^{-3} = a^{k3}$ so that $k^3 \equiv$ 1(mod7). Therefore $k = 1$, 2 or 4. If $k = 1$ then $ab = ba$ and $G \cong \mathbb{Z}_{21}$. Suppose $k = 2$. Then $b^2ab^{-2} = a^4$ and b^2 is also an element of order 3. Therefore using b^2 in place of b yields the case $k = 4$. So there are only two possibilities for G *:* either $\mathbb{Z}_{21}$ or the nonabelian group generated by a of order 7, b of order 3 and satisfying $bab^{-1} = a^2$.

But does that nonabelian group really exist? Just writing down these generators and relations does not produce an explicit group. It can be constructed by considering a 7-cycle a = (1234567) in S_7. Then a^2 = (1357246) and we search for b with $bab^{-1} = a^2$. It turns out that b = (235)(476) does the job.

20. Here are four groups of order 66: $\mathbb{Z}_{66}$, D_{33}, $D_{11} \times \mathbb{Z}_3$, $S_3 \times \mathbb{Z}_{11}$. These are non-isomorphic since their centers are all different (see Exercise 10). Suppose G is any group of order 66. To prove; G must be isomorphic to one of the four listed. By Sylow Theory there exist a, b, $c \in G$ of orders 2, 3, 11, respectively. Also there is only one Sylow 11-subgroup, so $\langle c\rangle$ is normal. By Exercise 7.6.18, $H = \langle b, c\rangle = \langle b\rangle\langle c\rangle$ is a subgroup of order 33 which must be cyclic by Corollary 8. 18. In fact, $bc = cb$ has order 33. Then $aHa^{-1} = H$ which implies $a(bc)a^{-1} = (bc)^k$ for some k determined (mod 33). Since $a^2 = e$ deduce that $k^2 \equiv 1$ (mod 33). There are exactly 4 solutions to this congruence: $k \equiv \pm 1, \pm 10$ (mod 33). (This can be seen by solving the congruence (mod 3) and (mod 11), to obtain $k \equiv \pm 1$ (mod 3) and $k \equiv \pm 1$ (mod 11). Then "glue" these together in all possible ways.) This completes the proof since there are at most four possibilities for G here, determined by the four values of k, and we already listed four non-isomorphic groups of order 66.

21. By Exercise 8.4.22, a group of order p^n is not simple, provided p is prime and $n > 1$. Groups of order p are abelian simple groups so they don't count here. A group of order pq where $p < q$ has a normal Sylow q-subgroup as in Corollary 8.18. Groups of order p^2q and pqr are not simple, by Corollary 8.2.1 and Exercise 8.3.25. The remaining numbers less that 60 not included in one of these cases are: 24, 36, 40, 48, 54 and 56. By Exercise 16: If G is simple and has a subgroup of index n, then $|G|$ divides $n!$. If $|G| = 24$, 36, 48 or 54, one of the Sylow subgroups has a small index, contrary to this restriction on $|G|$. If $|G| = 40$, the Third Sylow Theorem implies that the Sylow 5-subgroup is normal. The case $|G| = 56$ is done in the second Example after Theorem 8.17.

Chapter 10

Arithmetic in Integral Domains

10.1 Euclidean Domains

1. $\mathbb{Z}[\sqrt{d}]$ is a subset of $\mathbb{C}$. It is easy to check it is closed under addition and multiplication. For example, $(r + s\sqrt{d}\ )(t + u\sqrt{d}\ ) = (rt + dsu) + (ru + st)\sqrt{d}$. Hence it is a subring. If $d \geq 0$ then $\sqrt{d}$ is a real number.

2. We know $x^2 - d$ is irreducible in $\mathbb{Q}[x]$, by Eisenstein's criterion. Therefore $\sqrt{d}$ is irrational. If $r + s\sqrt{d}$ $= r_1 + s_1\sqrt{d}$ and $s \neq s_1$ then $\sqrt{d} = (r - r_1)/(s - s_1) \in \mathbb{Q}$. Therefore $s = s_1$ and $r = \mathrm{r}_1$. If $d = 4$ then $0{+}1\sqrt{4}\ = 2 + 0\sqrt{4}$.

3. (a) Answered in the text.

   (b) False. In $\mathbb{Z}$ use $a = b = c = 1$ and $d = 2$ for a counterexample.

4. ($\Rightarrow$) If $c = du$ for a unit $u \in R$, then $d = cu^{\ 1}$. Therefore $d \mid c$ and $c \mid d$. ($\Leftarrow$) Given $c = dx$ and $d = cy$ for some $x, y \in R$. If $c = 0_R$ then also $d = 0_R$ and c, d are associates. Suppose $c \neq 0_R$. Since $c = (cy)x$ and R is an integral domain we may cancel c to conclude $\mathrm{l}_R = yx$. Then y and x are units so that c, d are associates.

5. Answered in the text.

6. (i) $r = r \cdot l$ so $r \sim r$. (ii) If $r \sim s$ then $r = su$ for a unit u. Then $s = ru^{-1}$ and $s \sim r$. (iii) If $r \sim$ s and $s \sim t$ then $r = su$ and $s = tv$ for units u, v. Then $r = tvu$ and vu is a unit, so that $r \sim t$.

7. Answered in the text.

8. $u = v(v^{\ 1}u)$ and $v^{\ 1}u$ is a unit.

9. Apply the division algorithm to a and $|b|$, giving $a = |b|\,q + r$ with $0 \leq r < |b|$. Since $b < 0$, this is the same as $a = b(-q) + r$. Since $r \geq 0$, we know that $r = |r| = \delta(r)$, and $\delta(b) = |b|$, so that $0 \leq \delta(r) < \delta(b)$. Thus property (ii) holds for $b < 0$.

10. $2x + 2 = 2(x + 1)$ and neither 2 nor $x + 1$ is a unit.

11. This is an easy multiplication.

12. (a) Check the Definition. Certainly $\delta(ab) = (ab)^2 = a^2b^2 \geq a^2 = \delta(a)$. If $a, b \in \mathbb{Z}$ and $b \neq 0$ then usual division yields $a = bq + r$ where $0 \leq r < |b|$. Then $\delta(r) = r^2 < b^2 = \delta(b)$.
    (b) Yes. If $a, b \in \mathbb{Q}$ and $b \neq 0$ then $q = a/b \in \mathbb{Q}$ and $a = bq + r$ where $r = 0$.

13. (a) It is easy to check that $\theta(ab) = \delta(ab) + k \leq \delta(a)\delta(b) + k \leq (\delta(a) + k)(\delta(b) + k) = \theta(a)\theta(b)$. Now suppose $a = bq + r$ where either $r = 0$ or $\delta(r) < \delta(b)$. In the case $r \neq 0$ check that $\theta(a) = \delta(a) + k \leq \delta(b) + k = \theta(b)$.
    (b) Check that $\beta(ab) = k\delta(ab) \leq k\delta(a)\delta(b) \leq k^2\delta(a)\delta(b) = \beta(a)\beta(b)$. Suppose $a = bq + r$ where either $r = 0$ or $\delta(r) < \delta(b)$. In the case $r \neq 0$ check that $\beta(a) = k\delta(a) \leq k\delta(b) = \beta(b)$.

14. Certainly $\delta(ab) \leq \delta(a)\delta(b)$. If a, $b \in F$ and $b \neq 0$ then $q = ab^{-1} \in F$ and $a = bq + r$ where $r = 0$.

15. For any nonzero $a \in R$, certainly $\delta(1_R) \leq \delta(1_R a) = \delta(a)$. If u is a unit there exists v such that $uv = 1_R$. Then $\delta(u) \leq \delta(uv) = \delta(1_R)$. Therefore $\delta(u) = \delta(1_R)$. Conversely if $\delta(u) = \delta(1_R)$ the argument (2) $\Rightarrow$ (3) $\Rightarrow$ (1) in Theorem 9.2 shows that u is a unit.

16. Suppose d is a greatest common divisor of a and b in the Euclidean domain R. If d' is an associate of d then $d' = du$ for some unit u. Using u^{-1} check that $d' \mid a$ and $d' \mid b$. Also $\delta(d') = \delta(d)$ by Theorem 9.2(3) and the Definition shows that d' is a gcd of a and b.

17. Answered in the text.

18. Suppose d satisfies properties (i) and (ii). Property (i) in the Definition of greatest common divisor is the same. To Show: If $c \mid a$ and $c \mid b$ then $\delta(c) \leq \delta(d)$. By the hypothesis we know that $c \mid$ d. That is, $d = cs$ for some $s \in R$. Therefore $\delta(c) \leq \delta(cs) = \delta(d)$.

19. Answered in the Hint. The two remainders are $1 + 4i$ and $4 - i$.

20. Any nonzero element is an associate of 1_R so it is a unit.

21. Answered in the text.

22. (a) $(1+i)^{-1} = (1/2) - (1/2)i$ is not in $\mathbb{Z}[i]$.
    (b) $2 = (1 + i)(1 - i)$ and these factors are not units in $\mathbb{Z}[i]$.

23. Answered in the text.

24. No. Consider the natural homomorphism $\pi : \mathbb{Z} \to \mathbb{Z}_p$.

25. (a) $\delta(1_R) \leq \delta(a \cdot 1_R) = \delta(a)$ for any $a \neq 0_R$.
    (b) If $a = bu$ where u is a unit then $\delta(a) \leq \delta(b)$ and since $b = au^{-1}$ we also have $\delta(b) \leq \delta(a)$.
    (c) The Euclidean property says that $b = aq + r$ where either $r = 0_R$ or $\delta(r) < \delta(b)$. Then $a \mid$ r. If $r \neq 0_R$ then $\delta(a) \leq \delta(r) < \delta(b) = \delta(a)$. Therefore $r = 0_R$ and $a \mid b$. Hence a, b are associates.

26. Let $R = \mathbb{Z}[\sqrt{-2}]$. In analogy with Exercise 15 we have $\delta(ab) = \delta(a)\delta(b)$. Also, $\delta(a) \geq 1$ whenever $a \neq 0_R$. Therefore if a, b are nonzero then $\delta(a) \leq \delta(ab)$. Suppose a, $b \in R$ and $b \neq 0_R$. Then $a/b = x + y\sqrt{-2}$ where x, $y \in \mathbb{Q}$. Let m, n be integers with $|\ x - m\ | \leq 1/2$ and $|\ y - \mathrm{n}\ | \leq 1/2$. Define $q = m + n\sqrt{-2}$ and $r = a - \mathrm{bq}$. Then $r/b = a/b - q = (x - m) + (y - n)\sqrt{-2}$ so that $\delta(r) = ((x - m)^2 + 2(y - m)^2)\cdot\delta(b) \leq (3/4)\,\delta(b) < \delta(b)$.

27. It is routine to verify that $R = \mathbb{Z}[\omega]$ is a ring and that $\delta(ab) = \delta(a)\delta(b)$. Also $u^2 - uv + v^2 = (u - v/2)^2 + 3(v/2)^2 \geq 0$ with equality only if $u = v = 0$. Therefore $\delta(a) \geq 1$ whenever $a \neq 0_R$ and $\delta(a) \leq \delta(ab)$ whenever a, b are nonzero. Suppose a, $b \in R$ and $b \neq 0_R$. Then $a/b = x + y\omega$ for some x, $y \in \mathbb{Q}$. As in Exercise 24 choose those integers m, n and define $q = m + n\omega$ and $r = a - bq = ((a/b) - q)\cdot b = ((x - m) + (y - n)\omega)\cdot b$.
<u>Claim</u>. If $|u|$, $|v| \leq 1/2$ then $|u^2 - uv + v^2| \leq 3/4$.
<u>Proof</u>. By the equation above, $|u^2 - uv + v^2| \leq |u - v/2|^2 + 3|\,v/2\,|^2 \leq (3/4)^2 + 3(1/4)^2 = 3/4$.
Therefore $\delta(r) \leq (3/4)\,\delta(b) < \delta(b)$.

28. False even in $\mathbb{Z}$.

29. Answered in the text.

30. (a) If $1 + i = ab$ then $2 = \delta(1 + i) = \delta(a)\delta(b)$ in $\mathbb{Z}$. Then either $\delta(a) = 1$ or $\delta(b) = 1$ so either a or b is a unit, by Exercise 22.
(b) $2 = (1 + i)(1 - i)$

31. The procedure is the same as explained in Theorem 1.6. The conditions on the remainders become: either $r_j = 0_R$ or $\delta(r_j) < \delta(r_{j-1})$. The last nonzero remainder is a gcd for a, b. For the proof we use the analog of Lemma 1.7: If $a = bq + r$ then $(a, b) \sim (b, r)$.

32. Suppose $a = bq + r = bq' + r'$ are divisions satisfying the conditions, and suppose $r \neq r'$ If $r' = 0_R$ then $r \neq 0_R$ and $b \mid r$ implies $\delta(b) \leq \delta(r) < \delta(b)$ which is impossible. Then $r' \neq 0_R$ and similarly $r \neq 0_R$. Then $\delta(b) \leq \delta(b(q' - q)) = \delta(r - r') \leq \max\{\delta(r), \delta(r')\}$. This contradicts the original inequalities for r, r'. Therefore $r = r'$ and we also get $q = q'$.

10.2 Principal Ideal Domains and Unique Factorization Domains

1. Answered in the text.

2. Induction on n. The case $n = 2$ is assumed. Suppose $n \geq 3$ and $p\ |a_1a_2 \cdots a_n$. By that hypothesis either $p \mid a_1$ or $p \mid a_2 \cdots a_{\mathrm{n}}$. Apply the inductive hypothesis.

3. (a) Suppose $f(x)g(x) = 1$ in $\mathbb{Q}_{\mathbb{Z}}[x]$. Compare degrees to see that $f(x)$ and $g(x)$ are nonzero constants: $f(x) = a$ and $g(x) = b$ and $ab = 1$. By definition, a, $b \in \mathbb{Z}$ so that $a = b = \pm 1$.
(b) An associate of $f(x)$ is $f(x)\cdot\mathrm{u}$ where u is a unit. But the only units are ±1.

4. Yes. In a field there are no nonzero nonunits elements so the requirements are trivially satisfied.

5. Answered in the text.

6. Suppose $2f(x) + xg(x) = 1$ for some $f(x)$, $g(x) \in \mathbb{Z}[x]$. Evaluating at $x = 0$ shows that $2\cdot f(0)=l$ in $\mathbb{Z}$ which is impossible.

7. Let $d' = du$ where u is a unit. For any $x \in R$ show that: $d \mid x$ if and only if $d' \mid x$; and: $x \mid d$ if and only if $x \mid d'$. From this observation and the definition of gcd the Exercise is done.

8. ($\Rightarrow$) If $p \mid a$ then p divides the gcd of p and a, so that gcd $\neq 1_R$.
($\Leftarrow$) Suppose $p \nmid a$ and d is a gcd of p and a. Then $d \mid p$ so $d$is either a unit or an associate of p. If d is an associate of p then $d \mid a$ implies $p \mid$ a, contrary to hypothesis. Then d is a unit, and Exercise 7 implies that 1_R is also a ged of p and a.

9. We may assume $(c) \neq R$ so that c is not a unit. By Theorem 9.12 R is a UFD so that $c = P_1P_2 \cdots P_k$ for some irreducible elements p_i in R. By Theorem 9.13 there are only finitely many divisors d of c which are not associates. Therefore there are finitely many ideals (d) containing (c).

10. (p) is maximal if and only if the only ideal properly containing (p) is the unit ideal R. Equivalently, the only proper divisors of p are units. This is the definition of "irreducible".

11. Answered in the text.

12. A maximal ideal is always prime. Suppose (p) is a prime ideal. By Exercise 9.1.21, p is irreducible and Exercise 10 applies.

13. (a) See Exercise 6.2.20. (b) Answered in the text.

14. Compare Exercise 6.1.40.

(a) Certainly $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$ and the closure properties are easily checked.
(b) If $p \nmid a$ then $b/a \in R$.
(c) I contains a nonzero element x which is not a unit. Then $x = p'a/b$ where p does not divide a or b, and $t > 0$. Therefore $p' = xb/a \in I$.
(d) Part (c) shows that if $x \neq 0$ then $(x) = (p^k)$ for some $k \geq 0$. Also if $y \notin (p^t)$ then $(y) = (p^k)$ for some k < t. Now suppose I is an ideal $\neq (0)$, $\neq R$. By (c) there exists a smallest integer $t > 0$ with $(p^t) \subseteq I$. If $y \in I$ and $y \notin (p^t)$ then $(p^k) = (y) \subseteq I$ for some $k <$ t, contrary to the choice of t. Therefore $I = (p^{\mathrm{t}})$.

15. Answered in the text.

16. (a) If $p = f(x)g(x)$ in $\mathbb{Q}_{\mathbb{Z}}[x]$, compare degrees to show that $f(x) = a$, $g(x) = b$ are nonzero constants. Since $ab = p$ in $\mathbb{Z}$, either a or b is ± 1.
(b) The only units are 1 and –1 by Exercise 3. Then p and q are associates if and only if $p = \pm q$.

17. (a) If $x = f(x)g(x)$ then deg $f(x) \leq 1$. If deg $f(x) = 0$ then by comparing coefficients we find $f(x) = a$ and $g(x) = a^{-1}x$. Here a can be any nonzero integer. If deg $f(x) = 1$ then by comparing coefficients show that $f(x) = ax$, $g(x) = a^{-1}$. All the constant terms here are integers so we must have $a = 1/n$ for some nonzero integer n.
(b) Note that if $a \in \mathbb{Q}$ then ax is not irreducible in $\mathbb{Q}_{\mathbb{Z}}[x]$because it has proper factorizations:
$ax = (2)\cdot((a/2)x)$. Then the only irreducible factors of x in $\mathbb{Q}_{\mathbb{Z}}[x]$ are the primes of $\mathbb{Z}$. No product of such primes can equal x.

18. Suppose $I_1 \subseteq I_2 \subseteq \cdots$ is a chain of ideal in R. Let J be union of these I_k, s. Then J is an ideal (as in the proof of Lemma 9.10). By hypothesis J is finitely generated, say $J = (a_1 ,a_2 , \ldots a_s)$ for some $a_k \in J$. Since J is the union, each a_k lies in some $I_{n(k)}$ for some integer $n(k)$. Let m be the maximum of $n(1),\ldots, n(s)$. Then every $I_{nk} \subseteq I_m$ so that $a_k \in I_m$ for every k. But then $J = (a_1, \cdots a_s) \subseteq I_m \subseteq I_{m+1} \subseteq \cdots \subseteq J$. Conclude that $I_j = I_m$ for every $j \geq m$.

19. (a) Let $I_m = (2^m)$ in $\mathbb{Z}$. Then $I_1 \supseteq I_2 \supseteq \ldots$ is an infinite descending chain.
(b) Suppose R has DCC and $0 \neq a \in R$. By DCC there exists n such that $(a^j) = (a^n)$ for every $j \geq n$. In particular, $(a^n) = (a^{n+1})$ so that $a^n = a^n + 1\ c$ for some $c \in R$. Since R is an integral domain, factors of a can be cancelled so that $1 = ac$. But then a is a unit.

20. Since (a), $(b) \subseteq (d)$ conclude that $d \mid a$ and $d \mid b$. If $c \mid a$ and $c \mid b$ then (a) and $(b) \subseteq (c)$. Since a, b generate (d) we have $(d) \subseteq (c)$ so $c \mid d$.

21. Answered in the text.

22. Let $a_1, \ldots a_n$ be elements that are not all zero and let (d) be the ideal generated by $a_1, \ldots. a_n$. The same argument as in Exercise 20 shows that d is a gcd.

23. If $p \nmid b$ then by Exercise 8 there exist $x, y \in R$ such that $px + by = 1_R$. Then $cpx + (bc)y = c$ is a multiple of p.

24. If I is an ideal of R then by (i), I is generated by some $a_1,\ldots, a_n$. That is, $I = (a_1) + \cdots + (a_n)$. Choose n minimal here and suppose $n > 1$. Then by (ii) $(a_1) + (a_2) = (c)$ for some c, and $I = (c) + (a_3) \cdots + (a_n)$ is a sum of $n - 1$ principal ideals, contrary to the minimality. Therefore $n = 1$ and I is principal.

25. (a) Since $s \sim t$, we have $s = tu$ for some unit u. Multiplying on the left by r gives $rs = rtu = (rt)u$. Since rs is the product of rt by a unit, we have $rs \sim rt$.

(b) Let $d = (r, s)$ and $e = (r, t)$. By Exercise 10.1.4 it suffices to show that $d \mid e$ and $e \mid d$. Since $d \mid s = tu$, we have $dx = tu$ for some $x \in R$ and thus $dxu^{-1} = t$ so that $d \mid t$. Thus $d \mid r$ and $d \mid t$, so that $d \mid (r, t)$. Similarly, $e \mid t$ so that $e \mid tu = s$ and thus $e \mid r$ and $e \mid s$ so that $e \mid (r, s)$. Thus d and e are associates.

(c) By Exercise 10.1.4 it suffices to show that $r(s, t) \mid (rs, rt)$ and $(rs, rt) \mid r(s, t)$. Certainly $r(s, t) \mid rs$ since $(s, t) \mid s$, and similarly $r(s, t) \mid rt$. Thus $r(s, t) \mid (rs, rt)$. For the other direction, $r \mid (rs, rt)$, so that $(rs, rt) = rd$ for some d. Since $rd \mid rs$ and R is an integral domain, it follows that $rs = rdk \Rightarrow s = dk$ so that $d \mid s$. Similarly, $d \mid t$, so that $d \mid (s, t)$ and hence $(rs, rt) = rd \mid r(s, t)$.

(d) Clearly $d = (r, (s, t))$ is a divisor of r and of (s, t), hence is a divisor of r, s, and t. If c is any common divisor of r, s, and t, then $c \mid r$, $c \mid s$, and $c \mid t$, so that also $c \mid (s, t)$. Thus $c \mid d$, so that d is a gcd of r, s, and t. Similarly $((r, s), t)$ is a gcd of r, s, and t, so that the two are associates.

26. By Exercise 25(c), $(bd, cd) \sim d(b, c) \sim d1_R = d$. Then by Exercise 25(b), $1_R \sim (b, d) \sim (b, (bd, cd))$. But $(b, (bd, cd)) \sim ((b, bd), cd)$ by Exercise 25(d). Now, $(b, bd) \sim b(1_R, d)$ by Exercise 25(c), and 1_R is a gcd of 1_R and d, so that $(b, bd) \sim b$. Then by Exercise 25(b), since $(b, bd) \sim b$ we get $((b, bd), cd) \sim (b, cd)$. Putting this string of associates together gives
$$1_R \sim (b, d) \sim (b, (bd, cd)) \sim ((b, bd), cd) \sim (b, cd),$$
as desired.

27. Suppose $p \nmid c$ and $p \nmid d$. By Exercise 8. $(p,\ c) \sim (p,\ d) \sim 1_R$. By Exercise 26, $(p,\ cd) \sim 1_R$ contrary to the hypothesis $p \mid cd$.

28. Let $a = p_1 \cdots p_s$, $b = q_1 \cdots q_1$ where p_i, q_j are irreducibles. Since $(a,\ b) \sim 1_R$, no p_i and q_j are associates. Since $a \mid c$ show that $c = p_1 \cdots p_s p_{s+1} \cdots p_n$ for some irreducibles p_i for $s < i \leq n$. Since $b \mid c$ the factor $q_1 \cdots q_t$ must occur among these irreducible factors, but not among the first s terms. Therefore they occur among $P_{s+1} \cdots P_n$ so that $ab \mid$ c.

29. Answered in the text.

30. Using the notation in the proof of Corollary 9.18 we let s_j be the maximum of m_{11}, m_{21},..., m_{n1}. Use Theorem 9.13 to verify that $p_1^{s_1} p_2^{s_2} \cdots p_t^{s_t}$ is the 1cm.

31. By definition, s is the 1cm of a, b if and only if $s \in (a) \cap (b)$ and whenever $c \in (a) \cap (b)$ then $c \in (s)$. This says: $(a) \cap (b) = (s)$.

32. (a), (b) are direct verifications of the definitions, and part (c) is done in the Hint.

33. $(\Leftarrow)$ If $p(x)$ is a prime integer then it is prime by Exercise 16. Suppose $p(x)$ is irreducible in $\mathbb{Q}[x]$ and has constant term ± 1. If it factors in $\mathbb{Q}_{\mathbb{Z}}[x]$ one of the terms must be of degree 0. Compare the constant terms to show that it must be ± 1, and hence is a unit.
$(\Rightarrow)$ Let $p(x)$ be irreducible in $\mathbb{Q}_{\mathbb{Z}}[x]$. If it is constant then factorizations must involve only integers, so p is a prime number. Suppose deg $p(x) \geq 1$ and $p(x) = a(x)b(x)$ in $\mathbb{Q}[x]$. Claim. $p(x) = a'(x)b'(x)$ in $\mathbb{Q}_{\mathbb{Z}}[x]$ where deg $a'(x) =$ deg $a(x)$ and deg $b'(x) =$ deg $b(x)$.
Proof. Suppose the constant terms are $a(0) = r/s$ and $b(0) = u/v$ in lowest terms in $\mathbb{Q}$. Since z is an integer so that $s \mid u$ and $v \mid r$ by Theorem 1.5. Define $a'(x) = (s/v)a(x)$ and $b'(x) = (v/s)b(x)$. Then $a'(0) = r/v$ and $b'(0) = u/s$ are integers.
Therefore $p(x)$ must be irreducible in $\mathbb{Q}[x]$. Furthermore if $p(0)$ is a multiple of some prime number q, then $p(x) = q \cdot (1/q)p(x)$ is a nontrivial factorization in $\mathbb{Q}_{\mathbb{Z}}[x]$. Then the integer $p(0)$ is not divisible by any prime number so it must equal ± 1.
The final assertion can be quickly deduced from the following claim. The proofs are omitted. Claim.
(1) Let $p \in \mathbb{Z}$ be prime and $f(x) \in \mathbb{Q}_{\mathbb{Z}}[x]$. Then $p \mid f(x)$ in $\mathbb{Q}_{\mathbb{Z}}[x]$ if and only if $p \mid f(0)$ in $\mathbb{Z}$.
(2) Let $f(x)$, $p(x) \in \mathbb{Q}_{\mathbb{Z}}[x]$ with $p(x)$ irreducible. Then $p(x) \mid f(x)$ in $\mathbb{Q}_{\mathbb{Z}}[x]$ if and only if $p(x) \mid f(x)$ in $\mathbb{Q}[x]$.

34. By the unique factorization in $\mathbb{Q}[x]$. $f(x)$ is a product of irreducible. Among these factors, replace each associate of x by x, and replace every $p(x)$ which is not an associate of x by $p(0)^{-1}p(x)$. These adjustments leave a constant term factor, so that $f(x) = cx^n p_1(x) \cdots p_k(x)$ where $c \in \mathbb{Q}$, $n \geq 0$ and each $p_i(x)$ is irreducible in $\mathbb{Q}[x]$ with constant term 1. By Exercise 33 each $p_i(x)$ is irreducible in $\mathbb{Q}_{\mathbb{Z}}[x]$. (Note that if $n = 0$ then $c \in \mathbb{Z}$.) Uniqueness. With the two given factorizations, no $p_i(x)$ or $q_i(x)$ is an associate of x. Also if $p_i(x)$ is an associate of $q_i(x)$ in $\mathbb{Q}[x]$ then $p_i(x) = q_i(x)$ since their constant terms equal 1. The uniqueness in $\mathbb{Q}[x]$ then implies that $n = m$, $k = t$ and the $q_i(x)$'s are just a rearrangement of the $p_i(x)$'s. Compare the leading coefficients of the two factorizations to conclude finally that $c = d$.

35. By Exercise 34 every nonzero $f(x) \in \mathbb{Q}_{\mathbb{Z}}[x]$ can be written as $f(x) = cx^n p_1(x)^{n1} \cdots p_k(x)^{nk}$ where $c \in \mathbb{Q}$, $n \geq 0$, the $p_1(x), \ldots, p_k(x)$ are distinct irreducibles with constant term 1, and each $n_i \geq 0$. This decomposition is unique up to the order of the factors. If $g(x) = c'x^m p_1(x)^{m1} \cdots p_k(x)^{mk}$ is factored similarly (using the same set of irreducibles by inserting zero exponents), then let $d = \min\{n, m\}$ and $d_i = \min\{n_i, m_i\}$. The gcd is $(c, c')x^d p_1(x)^{d_1} \cdots p_k(x)^{d_k}$ as in Theorem 9.18.

36. (a) ($\Rightarrow$) If $f(x) = p$ is prime then any factorization of it in $\mathbb{Z}[x]$ must already be in $\mathbb{Z}$. So it remains irreducible. Suppose $f(x) \in \mathbb{Z}[x]$ has the gcd of its coefficients $= 1$ and $f(x)$ is irreducible in $\mathbb{Q}[x]$. If $f(x) = a(x)b(x)$ in $\mathbb{Z}[x]$ then either $a(x)$ or $b(x)$ is a constant, by the irreducibility in $\mathbb{Q}[x]$, Since the gcd of the coefficients is 1 that constant must be a unit (i.e. it is ± 1).
($\Leftarrow$) Suppose $f(x)$ is irreducible in $\mathbb{Z}[x]$. If $f(x) = n$ is a nonzero constant, it is irreducible in $\mathbb{Z}$ so it is a prime. Suppose deg $f(x) > 0$. Theorem 4.22 implies that $f(x)$ is irreducible in $\mathbb{Q}[x]$. If the gcd of the coefficients of $f(x)$ is > 1 factor it out to get a nontrivial factorization in $\mathbb{Z}[x]$. Therefore that gcd is 1.
(b) Any nonzero $f(x) \in \mathbb{Z}[x]$ can be factored as a nonzero constant times a product of (zero or more) irreducibles in $\mathbb{Q}[x]$. Altering each irreducible by a constant we may assume that each is in $\mathbb{Z}[x]$ and has relatively prime coefficients. All those constants are put together to get: $f(x) = cp_1(x)p_2(x) \cdots p_k(x)$ where (by part (a)) each $p_i(x)$ is an irreducible in $\mathbb{Z}$[x] of degree ≥ 1. By Lemma 4.21 applied to the product of the $p_i(x)$'s, the gcd of the coefficients of $p_1(x)p_2(x) \cdots p_k(x)$ is 1. Therefore c must be an integer (in fact $c =$ gcd(coefficients of $f(x)$)). Factor c into primes in $\mathbb{Z}$ to obtain the factorization of $f(x)$ into irreducibles in $\mathbb{Z}[x]$. The uniqueness follows from the unique factorization in $\mathbb{Z}$ and in $\mathbb{Q}[x]$.

10.3 Factorization of Quadratic Integers

1. Answered in the text.

2. Since every power ω^k reduces to one of $1, \omega, \ldots, \omega^{p-1}$ the closure properties are easily checked. Hence $\mathbb{Z}[\omega]$ is a subring of $\mathcal{C}$.

3. Answered in the text.

4. If it were Euclidean it would be a UFD contrary to the Example after Theorem 9.23.

5. Let $a = r/s$ where r, s are coprime integers. By hypothesis a is a root of some $x^n + c_{n-1}x^{n-1} + \cdots + c_0$ where all the $c_i \in \mathbb{Z}$. By the Rational Root Test (Theorem 4.20), $s \mid 1$ so that $a \in \mathbb{Z}$.

6. (a) irreducible. (b) reducible $(2 + i)(2 - i)$ (c) irreducible

7. Check that $1 \pm \sqrt{-7}$ and 2 are irreducible by noting that if any of them factored nontrivially we would find some a with $N(a) = 2$. No such a exists.

8. (a) 3 (b) 7 (c) $(2 - i)(1 + 2i)$ (d) $(1 + i)(1 + 2i)(1 - 4i)$

9. (a) Their norms are primes.

   (b) $11 - 7\sqrt{2} = u\cdot(5 + \sqrt{2})$ and $2 + \sqrt{2} = u^{-1}\cdot(2 - \sqrt{2})$ where $u = 3 - 2\sqrt{2}$ is a unit with $u^{-1} = 3 + 2\sqrt{2}$.

10. $9 = 3\cdot3 = (2 + \sqrt{-5})\cdot(2 - \sqrt{-5})$. These factors are irreducible since mere is no element a with $N(a) = 3$.

11. $10 = 2.5 = (2 + \sqrt{-6})\cdot(2 - \sqrt{-6})$. The factors are irreducible since there is no element a with $N(a) = 2$ or 5.

12. $6 = 2\cdot3 = (2 + \sqrt{10})(-2 + \sqrt{10})$. The factors are irreducible since there is no integer solution to $x^2 - 10y^2 = 2, 3$ (look at it (mod 5)).

13. $N(a) = 1$ occurs if and only if $a = \pm1$. $N(a) = 6$ if and only if $a = \pm1 \pm \sqrt{-5}$. $N(a) = 4$ if and only if $a = \pm2$. $N(a) = 2$, 3 or 12 is impossible. Checking these quantities we see that the common divisors are: ±1, ±2, $\pm(1 + \sqrt{-5})$. None of these is divisible by all the others.

14. If a is a common divisor then $N(a)$ divides $N(2) = 4$ and $N(1 + \sqrt{-5}) = 6$, so it divides 2. Since $N(a) = 2$ is impossible we have $N(a) = 1$ and $a = \pm1$. Therefore 1 is aged. If $1 = 2a + (1 + \sqrt{-5})b$ we set $a = x + y\sqrt{-5}$, $b = u + v\sqrt{-5}$ and conclude that $2x + u + 5v = 1$ and $2y + u + v = 0$. This implies $u + v$ is both even and odd, which is impossible.

15. In a UFD a principal ideal (c) is prime if and only if c is irreducible (see Theorem 9.16 and Exercise 9.1.21). Note that we can cancel principal ideals: If I, J are ideals and $0 \neq a \in R$ then $(a)I = (a)J$ implies $I =$ J. Suppose (c) is the given ideal and factor $c = p_1p_2\cdots p_k$ where p_i is irreducible. Then (c) is the product of the prime ideals (p_j). Suppose $(c) = Q_1\ Q_2 \cdots Q_m$ is another factorization into prime ideals. Re-number the Q's to assume Q_1 is minimal among the Q_i. Since $(p_1p_2\cdots p_k) = (c) \subseteq Q_1$ and Q_1 is prime, there is some j where $(p_j) \subseteq Q_1$ (see Exercise 6.3.18). Re-numbering the p's, assume $j = 1$. Similarly $Q_1 \cdots Q_m = (c) \subseteq (p_1)$ so there is some i with $Q_i \subseteq (p_1)$. By the minimality of Q_1, conclude that $Q_1 = (p_1)$. Cancel this ideal to conclude that $(p_2 \cdots p_k) = Q_2 \cdots Q$. Continue this process to show that each Q_i equals one of the (p_j) and the uniqueness of factorizations in R finishes the proof.

16. If R is any integral domain and $a, b \in R$ then $(a)(b) = (ab)$. This follows easily from the definition of the product ideal.

17. (a) Answered in the text.
   (b) if $r \equiv$ s (mod 2) write $\tau = 2m + s$. Then $r + s\sqrt{-5} = 2m = s(1 + \sqrt{-5})$.

18. P is generated by $a = 2$ and $b = 1+\sqrt{-5}$, so that P^2 is generated by the products a^2, ab and b^2. Since each of these is a multiple of 2 conclude: $P^2 \subseteq (2)$. On the other hand $2 = ab - a^2 - b^2 \in P^2$ so that $(2) \subseteq P^2$.

19. (a) If $r = 3m + s$ then certainly $r + s\sqrt{-5} \in Q_1$ Conversely suppose that $r + s\sqrt{-5} = 3(x + y\sqrt{-5}) + (1 + \sqrt{-5})(u + v\sqrt{-5})$ for some integers x, y, u, v. Reduce everything modulo 3 to find: $r \equiv u - 5v \equiv u + v \equiv$ s (mod 3).

(b) $r + s\sqrt{-5} = r - s + s(I + \sqrt{-5}\ ) \equiv r -$ s (mod Q_t). Adjusting by a multiple of 3 we find: $r + s\sqrt{-5} \equiv 0$, 1 or 2 (mod Q_1). These three values are not congruent by part (a). Hence there are 3 cosets.
(c) The natural ring homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}[\sqrt{-5}]/Q_1$ is surjective by part (*b*). Its kernel is the ideal (3) and the First Isomorphism Theorem provides the required isomorphism.
(d) The arguments are easily altered to show that $r + s\sqrt{-5} \in Q_2$ if and only if $r \equiv -s$ (mod 3) and that $\mathbb{Z}[\sqrt{-5}]/Q_2 \equiv \mathbb{Z}_3$.
(e) $Q_1\ Q_2$ is generated by the products $3{\cdot}3 = 9$, $3{\cdot}(1 + \sqrt{-5}\ )$, $3{\cdot}(1 - \sqrt{-5}\ )$ and $(1 + \sqrt{-5}\ ){\cdot}(1 - \sqrt{-5}\ ) = 6$. Since each term is a multiple of 3, $Q_1\ Q_2 \subseteq (3)$. Since $3 = 9 - 6 \in Q_1Q_2$ the reverse inclusion holds.

20. If 2 is in the ideal (a) where $a = r + s\sqrt{-5}$ then $a \mid 2$ so that $N(a) \mid 4$. Then $r^2 + 5s^2 = N(a) \leq 4$ forcing $s = 0$.

21. **Lemma**. If $\alpha, \beta \in \mathbb{Z}[\sqrt{d}\ ]$ with $(\alpha) \subseteq (\beta)$ and $N(\alpha) = \pm N(\beta)$ then $(\alpha) = (\beta)$.

<u>Proof</u>. Given $\alpha = \beta\gamma$ for some γ. Compute mat $N(\gamma) = \pm 1$ so that γ is a unit in $\mathbb{Z}[\sqrt{d}\ ]$. Q.E.D. Now suppose $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$ is a chain of principal ideals in $\mathbb{Z}[\sqrt{d}]$. Then $a_{i+1} \mid a_i$ in $\mathbb{Z}\sqrt{d}$ so that $N(a_{i+1}) \mid N(a_i)$ in $\mathbb{Z}$. Since $\mathbb{Z}$ has ACC on ideals there exists m so that $N(a_i)$ and $N(a_m)$ generate the same ideal for every $i \geq m$. That is, $N(a_i) = \pm N(a_m)$ and by the Lemma, $(a_i) = (a_m)$ for every $i \geq m$.

22. (a) If $a = x + y\sqrt{d}$ let t be the 1cm of the denominators of x, y. Then $x = r/t$ and $y = s/t$ where r, s, t are relatively prime integers.
(b) Multiply out $(x - a)(x - a\ )$.
(c) If $p(x)$ factors in $\mathbb{Q}[x]$ then its root a lies in $\mathbb{Q}$, but $s \neq 0$.
(d) Done in the Hint.
(e) By (*b*) and (*d*) show that $t \mid 2r$ and $t^2 \mid (r^2 - ds^2)$, so that $t^2 \mid 4ds^2$. Suppose p is an odd prime and $p \mid t$. Then $p \mid r$ so that s and hence $4s^2$ are prime to p. But then $p^2 \mid d$ contrary to the hypothesis that d is square free. Therefore $t = 2^m$ for some m. If $m > 1$ then $4 \mid t$ so that $2 \mid r$ and s must be odd. Then $16 \mid 4d$ forcing $4 \mid d$ with a contradiction as before. Therefore $m \leq 1$.
(f) Done in the Hint.
(g) Suppose $t = 2$. By (*b*) and (*d*), a is a quadratic integer if and only if $r^2 \equiv ds^2 \equiv s^2$ (mod 4). This occurs if and only if $r \equiv s$ (mod 2). Since $(r, s, t) = 1$ we know r, s are not both even.
(h) This summarizes parts (*f*) and (*g*).

10.4 The Field of Quotients of an Integral Domain

1. (1) $0_R d = b0_R$. (2) $a(bk) = b(ak)$ (3) $ac = ca$.

2. (a) $[a, b] + ([c, d] + [e, f]) = [a(df) + b(cf + de), b(df)]$ and $([a, b] + [c, d]) + [e, f] = [(ad + bc)f + (bd)e, (bd)f]$. They are equal.
(b) $[a, b]{\cdot}([c, d]{\cdot}[e, f]) = [a(ce), b(df)]$ *and* $([a, b]{\cdot}[c, d]){\cdot}[e, f] = [(ac)e, (bd)f]$. They are equal.
(c) $[a, b]{\cdot}[c, d] = [ac, bd] = [ca, db] = [c, d][a, b]$.

3. Answered in the text.

4. View $R = \mathrm{R}^* \subseteq F$ and note that $[a, b] = [ab^{-1}, 1_R] \in R$.

5. Answered in the text.

6. Define f : $R \to \mathbb{Q}[\sqrt{d}]$ by $f(x + y\sqrt{d}\ ,\ u + v\sqrt{d}\ ) = (xu - dyv)/\delta + (yu - xv)/\delta\sqrt{d}$ where $\delta^2 = u^2 - dv^2$. Verify that f is an isomorphism.

7. If R is a ring with $\mathbb{Z} \subseteq R \subseteq \mathbb{Q}$, it is easy to check that R is an integral domain $\mathbb{Q}$ as its field of quotients. As in Exercise 3.1.23, for each prime p there is a ring $\mathrm{R_p}$ consisting of all rationals having denominator equal to a power of p. These rings are all different since $1/p \notin R_p$ for unequal primes p, q. Compare Exercise 6.1.40.

8. <u>Well-defined</u>. If $[a, b] = [c, d]$ then $ad = bc$ so that $f(a)f(d) = f(b)f(c)$. Then $[f(a), f(b)] = [f(c), f(d)]$. Therefore $f^*(a/b)$ does make sense.
<u>Homomorphism</u>. $f*((a/b)+(c/d)) = f*((ad+bc)/bd) = f(ad+bc)/f(bd = (f(a)f(d)+f(b)f(c))/f(b)f(d)$
$= f(a)/f(b)+f(c)/f(d) = f*(a/b)+f*(c/d).$
$f*((a/b)(c/d)) = f*(ac/bd) = f(ac)/f(bd) = f(a)f(c)/f(b)f(d) = (f(a)/f(b))(f(c)/f(d)) = f*(a/b)f*(c/d).$
<u>Injective</u>. $x/y = 0_F$ if and only if $x = 0_R$. Therefore $f*(a/b) = 0_{F_1}$ implies $f(a) = 0_{R1}$. Since f is injective, $a = 0_R$ and $a/b = 0_F$.
<u>Surjective</u>. For any $x/y \in F_1$ we have $x = f(a)$, $y = f(b)$ for some a, $b \in R$ since f is surjective. Then $f*(a/b) = x/y$.

9. If $a/b = c/d$ in F then $ad = bc$ in $R \subseteq K$. Then $ab^{-1} = cd^{-1}$ in K.

10. (a) Done in the Hint.
(b) $f((a/b)+(c/d)) = f((ad+bc)/bd) = (ad+bc)(bd)^{-1} = ab^{-1}+cd^{-1} = f(a/b)+f(c/d)$. Also
$f((a/b)(c/d)) = f(ac/bd) = (ac)(bd)^{-1} = (ab^{-1})(cd^{-1}) = f(a/b)f(c/d)$.

11. Answered in the text.

12. (a) The map $\varphi : \mathbb{Z} \to R$ by $\varphi(n) = n\ 1_R$ is a homomorphism (see Exercise 3.2.21). Since R has characteristic 0 this φ is injective, so that $\mathbb{Z}$ is isomorphic to the subring $\varphi(\mathbb{Z}) \subseteq R$.
(b) If K is a field of characteristic 0, view $\mathbb{Z} \subseteq K$ by part (a). By Theorem 9.31 K has a subfield $\equiv \mathbb{Q}$.

13. The identity element 1_R was not mentioned in this Section before Lemma 9.22. Since $[a, a]/x, y] = [ax, ay] = [x, y]$ the element $[a, a]$ is an identity element in F. The rest of the proof that F is a field is unchanged. Define α: $R \to F$ by $\alpha(r) = [ra, a]$ for any nonzero $a \in R$. This map is well-defined since $[ra, a] = [rb, b]$ for any nonzero a, $b \in R$. It is routine to check that α is a ring homomorphism. Since R has no zero divisors, α is injective, so that $R \cong \alpha(R) \subseteq F$.

10.5 Unique Factorization in Polynomial Domains

1. ($\Rightarrow$) Suppose p is irreducible in R and $p = a(x)b(x)$ in $R[x]$. Then $a(x)$, $b(x)$ have degree 0 so they are in R, and one of them must be a unit. ($\Leftarrow$) Answered in the text.

2. The constant polynomials 2 and 3 in $\mathbb{Z}[x]$ are associates in $\mathbb{Q}[x]$ but not in $\mathbb{Z}[x]$, There is no contradiction since they are not primitive.

3. Answered in the text.

4. Suppose $g(x) = a(x)b(x)$ in $R[x]$ and $a(x)$ is nonconstant. Write $a(x) = ca_1(x)$ and $b(x) = c'b_1(x)$ where c, $c' \in R$ and $a_1(x)$, $b_1(x)$ are primitive. Then $g(x) = cc'a_1(x)b_1(x)$ and Gauss's Lemma and Theorem 9.35 imply that cc' is a unit in R. Therefore c is a unit and $a(x)$ is primitive.

5. If $f(x) = a_nx^n + \cdots + a_1x + a_0$ and $c \in R$ then $c \mid f(x)$ if and only if c is a common divisor of the coefficients a_i. The claim quickly follows.

6. If $f(x) = a(x)b(x)$ is a nontrivial factorization in $R[x]$ then the irreducibility in $F[x]$ implies that one of the factors has degree 0. If $a(x) = c$ has degree 0, then $c \mid f(x)$ and the primitivity implies $c = a(x)$ is a unit.

7. Answered in the text.

8. Since $R[x]$ is an integral domain it follows that R is an integral domain. Let a ba a nonzero element of R. The ideal J generated by a and x is principal, say $J = (f(x))$. Then $a = f(x)g(x)$ for some $g(x)$, and degrees imply that $f(x) = c \in R$. Then $x = ch(x)$ for some $h(x)$ and leading coefficients imply that c is a unit in R. Therefore $J = R[x]$ and have $I_R = a{\cdot}u(x) + x{\cdot}v(x)$ for some $u(x)$, $v(x) \in R[x]$. Comparing constant terms, we see that a is a unit in R. Hence R is a field.

9. The key step is that every element of F can be written as r/s where $r, s \in R$ and 1_R is a gcd of r, s (For any a/b, factor out and cancel the gcd of a and b.) Then if $r \mid a_0s^n$ conclude (using Exercise 9.2.29) that $r \mid a_0$. The proof of Theorem 4.20 is easily completed.

10. Let $f(x) \in R[x]$ and $f(x) = a(x)b(x)$ in $F[x]$. We may write $f(x) = rf_1(x)$, $a(x) = \mathrm{c}a_1(x)$ and $b(x) = c'b_1(x)$ where $r \in R$, c, $c' \in F$ and $f_1(x)$, $a_1(x)$, $b_1(x)$ are primitive in $R[x]$. Then $f_1(x)$ and $a_1(x)b_1(x)$ are primitive and are associates in $F[x]$, hence they are associates in $R[x]$, by Corollary 9.36. Therefore $f(x) = rua_1(x)b_1(x)$ for some unit u, and $rea_1(x)$, $b_1(x)$ have the same degrees as $a(x)$, $b(x)$, respectively.

11. The same proof works, using Theorem 9.15 in place of Theorem 1.8.

12. The irreducible element $1 - i$ divides -6, $4i$ and $1 + 3i$, and $(1 - i)^2 = -2i$ does not divide $1 + 3i$. Eisenstein's Criterion applies.

Chapter 11

Field Extensions

11.1 Vector Spaces

1. Check the axioms to show that $M(\mathbb{R})$ is a vector space over $\mathbb{R}$. An element of $M(\mathbb{R})$ is given by an ordered 4-tuple, with addition and scalar multiplication given componentwise. Then $M(\mathbb{R})$ is essentially the same as $\mathbb{R}^4$. See Exercise 6.

2. Check the axioms. This is a special case of Exercise 6.

3. The axioms showing that $\mathbb{R}[x]$ is a vector space over $\mathbb{R}$ immediately follow from the knowledge that $\mathbb{R}[x]$ is a commutative ring containing $\mathbb{R}$ as a subring.

4. Checking the axioms is straightforward. In fact, since the operations are restrictions of the operations of $\mathbb{R}[x]$, the important thing to check is that $\mathbb{R}_n[x]$ is closed under addition and scalar multiplication.

5. From group theory recall that the direct product of groups is a group. Then $F^n = F \times F \times \cdots \times F$ is an abelian group, using componentwise operations. Checking the axioms for vector spaces is routine. For example, suppose $a \in F$ and $v_1, v_2 \in F^n$. Express $v_1 = (s_1, ..., s_n)$ and $v_2 = (t_1, ..., t_n)$ and compute $a(v_1 + v_2) = a \cdot (s_1 + t_1, ..., s_n + t_n) = (a(s_l + t_1), ..., a(s_n + t_n)) = (as_1 + at_1, ..., as_n + at_n) = (as_1, ..., as_n) + (at_1, ..., at_n) = av_1 + av_2$.

6. An expression $w = c_1v_1 + \cdots + c_nv_n$ exists for some c_j since $\{v_1, ..., v_n\}$ spans K. Then $w = 0 \cdot w + c_1v_1 + \cdots + c_nv_n$ also lies in the span of $\{w, v_1, ..., v_n\}$.

7. Answered in the text.

8. Suppose $c_1(1, 0, 0) + c_2(0, 1, 0) + c_3(0, 0, 1) = (0, 0, 0)$ for some $c_i \in \mathbb{Q}$. To Show: each $c_j = 0$. Multiply this out to find: $(c_1, c_2, c_3) = (0, 0, 0)$ and use the definition of equality in $\mathbb{Q}^3$ to conclude that $c_1 = c_2 = c_3 = 0$.

9. Answered in the text.

10. Suppose $av = 0_v$ for some $a \in F$. If $a \neq 0_F$ then a^{-1} exists in F and $v = 1_Fv = (a^{-1}a)v = a^{-1}(av) = a^{-1}\ 0_v = 0_v$, contrary to hypothesis $v \neq 0_v$. (We used the property $0_Fv = 0_v$ proved below in Exercise 21(a).)

11. For any v_i, note that $1_F \cdot 0_v + 0_F v_1 + \cdots + 0_F v_n = 0_v$. (Again Exercise 21(a) was used.)

12. If $au + b(u + v) + c(u + v + w) = 0_v$ for some a, b, $c \in F$, then $(a + b + c)u + (b + c)v + cw = 0_v$. By the independence of u, v, w conclude: $a + b + c = 0_F$, $b + c = 0_F$ and $c = 0_F$. Hence $a = b = c = 0_F$.

13. Answered in the text.

14. A dependence relation among the elements of the subset is automatically a dependence relation among the elements of T, using coefficient 0_F for those elements not in the subset.

15. See the answer in the text. If $xb + y(c + di) = 0$ for some x, $y \in \mathbb{R}$ then $xb + yc = 0$ and $yd = 0$. Since b, $d \neq 0$ it follows that x, $t = 0$. Hence the set in linearly independent.

16. If $v_1, . . . , v_n$ is a basis then every element of K equals $a_1v_1 + \cdots + a_nv_n$ for some $a_i \in \mathbb{Z}_p$. There are p^n possible choices for these coefficients, so $|K| \leq p^n$.

17. Since $v_i = c_i^{-1}\ (c_iv_i)$ the new set also spans K. If $a_1(c_1v_1) + \cdots + a_n(c_nv_n) = 0_v$ then the independence of the v_i implies that $a_ic_i = 0_F$ and hence $a_i = 0_F$ for every i.

18. For any $f(x) \in \mathbb{Z}_2[x]$, divide by $x^2 + x +1$ to find a, $b \in \mathbb{Z}_2$ with $f(x) \equiv ax + b \pmod{x^2 + x + 1}$. Therefore $[f(x)] = a[x] + b[1]$ so the set spans everything. Also If $a[x] + b[1] = 0$ for some a, $b \in \mathbb{Z}_2$ then $ax + b \equiv 0 \pmod{x^2 + x + 1}$. Hence $a = b = 0$.

19. For any vectors $w_1, \ldots, w_k$ the set $\{0_v, w_1, \ldots, w_k\}$ is linearly dependent. This is proved by exhibiting a nontrivial relation $1_F \cdot 0_v + 0_F \cdot w_1 + \cdots + 0_F \cdot w_k = 0_v$. Therefore the vector 0_v can never be an element of an independent set.

20. For any $w \in L$ the hypothesis implies that $w = c_1v_l + \cdots + c_nv_n$ for some $c_j \in F$. But certainly $c_j \in K$ as well, so every w is a linear combination of $\{v_1, \ldots, v_n\}$ over K.

21. (a) $0_Fv = (0_F + 0_F)v = 0_Fv + 0_Fv$ and since V is an abelian group conclude $0_v = 0_Fv$.
(b) $a0_v = a(0_v + 0_v) = a0_v + a0_v$. Since V is an abelian group conclude $0_v = a0_v$.
(c) $av + (-a)v = (a - a)v = 0_Fv = 0_v$. Therefore $(-a)v = -(av)$.
Similarly $av + a(-v) = a(v + (-v)) = a0_v = 0_v$ so that $a(-v) = -(av)$.

22. (a) Suppose $a + b\sqrt{2} = 0$ for some a, $b \in \mathbb{Q}$ which are not both zero. If $b = 0$ then $a = 0$, contrary to hypothesis. Then $b \neq 0$ and $\sqrt{2} = -a/b$ lies in $\mathbb{Q}$. This is a contradiction since $\sqrt{2}$ is irrational.
(b) If $\sqrt{3} = a + b\sqrt{2}$ for some a, $b \in \mathbb{Q}$ then $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$. Since $\sqrt{2}$ is irrational conclude that $2ab = 0$. If $a = 0$ then $3 = 2b^2$ so that $6 = (2b)^2$. If $b = 0$ then $3 = a^2$. Since $\sqrt{6}$ and $\sqrt{3}$ are irrational these equations are impossible.

23. (a) Answered in the text, (b) Suppose $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} = 0$ for some a, b, c, $d \in \mathbb{Q}$ which are not all 0. Then c, d are not both 0, since $\{1, \sqrt{2}\}$ is independent over $\mathbb{Q}$. Then $\sqrt{3} = (a + b\sqrt{2})(c + d\sqrt{2})^{-1} \in \mathbb{Q}(\sqrt{2})$, which contradicts part (a) (or Exercise 22(b)).

24. If v is rational then $v{\cdot}1 + (-1){\cdot}v = 0$ is a dependence relation. Conversely, if $\{1, v\}$ is linearly dependent then $a + bv = 0$ for some rational a, b which are not both 0. Then $b \neq 0$ (for if $b = 0$ then $a = 0$). Then $v = a/b \in \mathbb{Q}$.

25. Suppose there is a relation $c_0 1 + c_1 x + c_2 x^2 + \cdots + c_k x^k = 0$ in $\mathbb{R}[x]$, for some $c_j \in \mathbb{R}$. By basic properties of polynomials, each $c_j = 0$. This proves the independence.

26. By definition, $\mathbb{R}_n[x]$ is spanned by $\{1, x, x^2, \cdots, x^n\}$. By Exercise 25 this set is also linearly independent, so it is a basis. Therefore $\mathbb{R}_n[x]$ has dimension n + 1.

27. Let $e_1 = (1, 0, ..., 0)$, $e_2 = (0, 1, 0 , ..., 0)$, etc. Then any $v \in F^n$ can be expressed: $v = (s_1, s_2, ..., s_n) = s_1 e_l + s_2 e_2 + \cdots + s_n e_n$ for some $s_j \in F$. Therefore $\{e_1, ..., e_n\}$ spans F^n. That set is also linearly independent (compare Exercise 8), so it is a basis. Conclude that F^n has dimension n.

28. Suppose K has only one basis $\{u_1, u_2 \ldots, u_n\}$ over F. If $n > 1$ it is not hard to check that $\{u_1 + u_2, \mathrm{u}_2, \ldots, u_n\}$ is also a basis. The uniqueness implies that u_1 equals one of the elements of the second basis, but each case is impossible by the independence of the u_i. Therefore $n = 1$ and $K = F$. For any nonzero $a \in F$, $\{a\}$ is a basis of F over F (independent since $a \neq 0$ and it spans since $x = (xa^{-1})$ a for any $x \in F$). The uniqueness implies F has only 2 elements, so $F \cong \mathbb{Z}_2$.

29. If $a(u + v) + b(v + w) + c(u + w) = 0_v$ then $(a + c)u + (a + b)v + (b + c)w = 0_v$ and the independence implies $a + c = a + b = b + c = 0_F$. These imply $a = b = c$ and $2a = 0_F$. Then $a = b = c = 0_F$ since 2 is invertible in F. Note that $2u = (u + v) - (v + w) + (u + w)$. Since 2 is invertible, u is in the span of $\{u + v, v + w, u + w\}$. Similarly v and w are in this span. Since $\{u, v, w\}$ spans V it follows that $\{u + v, v + w, u + w\}$ also spans V.

30. (⇒). Since the set spans V every element can be written as a linear combination. For the uniqueness, suppose $c_1 v_1 + \cdots + c_n v_n = d_1 v_1 + \cdots + d_n v_n$. Then $(c_1 - d_1)v_1 + \cdots + (c_n - d_n)v_n = 0_v$. By the independence conclude that $c_i = d_i$ for every i.
(⇐) Since every element is a linear combination of the v_i, the set spans V. By the uniqueness, a relation $a_1 v_1 + \cdots + a_n v_n = 0_v$ must coincide with the relation $0_F v_1 + \cdots + 0_F v_n = 0_v$. Hence $a_i = 0_F$ for all i.

31. By Theorem 5.10 L is a field. Corollary 5.5 says that every element of L can be expressed uniquely as some $[a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}]$. That is, every element is written in a unique way as a linear combination of $[1_F]$, $[x]$,…,$[x^{n-1}]$. By Exercise 30, $[L : F] = n$.

32. If S is linearly dependent, Lemma 10.1 implies that some v_i is a linear combination of the previous v_j's. Then $S' = \{v_1, ..., v_{i-1}, v_{i+1}, ..., v_t\}$ still spans K. If S' is linearly independent then it is a basis. Otherwise, repeat the argument with S' in place of S.

33. Answered in the text.

34. V does not have a finite basis. By Exercise 32 deduce that there is no finite subset of V which spans V. If $V = \{0_v\}$ then V is spanned by the one element set $\{0_v\}$. This contradiction shows that there exists $v \in V$ with $V \neq 0_v$. By Exercise 10 $\{v\}$ is a linearly independent set of 1 element. Use induction on k that V contains a linearly independent set

of k elements. The case $k = 1$ is done. Suppose the statement is true for $k = n$. That is, suppose there is a linearly independent set $\{v_1, ..., v_n\}$ in V. By hypothesis this finite set cannot span V so there exists $w \in V$ which is not expressible as a linear combination of $v_1, ..., v_n$. By Lemma 10.1 the set $\{v_1 ..., v_n, w\}$ is a linearly independent set of $n + 1$ elements. This is the induction step needed.

35. If that set is linearly dependent then $a_1(w - v_1) + \cdots + a_n(w - v_n) = 0_v$ for some a_i not all zero. Then $a_1v_1 + \cdots + a_nv_n = \delta w = \delta c_1v_1 + \cdots + \delta c_nv_n$ where $\delta = a_1 + \cdots + a_n$. Since the v_i are independent, $a_i = \delta c_i$ for all i. Consequently $\delta \neq 0_F$ and $c_1 + \cdots + c_n = \delta(a_1 + \cdots + a_n) = 1_F$. Conversely if that sum equals 1_F then $c_1(w - v_1) + \cdots + c_n(w - v_n) = w - (c_1v_1 + \cdots + c_nv_n) = 0_F$.

36. Done in the Hint.

37. (i) $\Rightarrow$ (iii) is done in the text. Clearly, (iii) $\Rightarrow$ (i) and (ii).
(ii) $\Rightarrow$ (iii): By Exercise 36 the given set S is a subset of a basis T. Since $[K : F] = n$, T has n elements and $S = T$.

38. The proof of Theorem 10.4 also settles this question.
Corollary. Let F, K, L be fields with $F \subseteq K \subseteq L$. If $[L : F]$ is finite then $[L : K]$ and $[K : F]$ are also finite.
Proof. Suppose $\{u_1, ..., u_m\}$ is a set of elements of K which is independent over F, and $\{v_1, ..., v_n\}$ is a set of elements of L which is independent over K. The proof of Theorem 10.4 shows that $\{u_iv_j\}$ is independent over F. By Exercise 36 this set is contained in a basis of L over F, so that $mn \leq [L : F]$. If either $[L : K]$ or $[K : F]$ is infinite we could arrange m or n to be arbitrarily large, which is impossible.

39. If $F \subseteq E \subseteq K$ and $[K : F] = p$ is finite then Exercise 38 and Theorem 10.4 imply that $p = [K:E] \cdot [E : F]$. Since p is prime, one of these factors is 1, so that either $E = K$ or $E = F$.

11.2 Simple Extensions

1. Let F be the intersection. If $a, b \in F$ then $a + b$ and ab lie in every E_i so they are in F. Also if $a \neq 0_F$ then a^{-1} lies in every E_i. so it also lies in F.

2. $u^2 \in F(u)$ and $F(u^2)$ is the smallest field containing F and u^2.

3. Answered in the text.

4. Clearly $3 + i \in \mathbb{Q}(i)$ and $i = (3 + i)–3 \in \mathbb{Q}(3 + i)$. Hence $\mathbb{Q}(3 + i) = \mathbb{Q}(i)$. Similarly $\mathbb{Q}(1 - i) = \mathbb{Q}(i)$.

5. (a), (c) done in the text. (b) Root of $(x^4 - 1)^2 + 2$.

6. Suppose u^2 is a root of $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in K[x]$. Then u is a root of $f(x^2) = x^{2n} + c_{n-1}x^{2n-2} + \cdots + c_0 \in K[x]$.

7. Answered in the text.

8. If $u + v$ is a root of some $f(x) \in F[x]$, then u is a root of $f(x + v) \in F(v)[x]$.

9. Answered in the text.

10. If $0_F \neq c \in F$ and $u + c$ is a root of $f(x) \in F[x]$ then u is a root of $f(x - c) \in F[x]$. If cu is a root of $g(x) \in F[x]$ then u is a root of $g(c^{-1}x) \in F[X]$. Therefore $u + c$ and cu are transcendental. By Exercise 6, u^2 is also transcendental.

11. degree 6, since $x^6 - 2$ is irreducible by Eisenstein.

12. $i = b^{-1}(a + bi) - b^{-1}\, a \in \mathbb{R}(a + bi)$. Therefore $\mathbb{C} \subseteq \mathbb{R}(a + bi) \subseteq \mathbb{C}$.

13. $F \subseteq F(u) \subseteq K$. Apply Exercise 10.2.39.

14. By the Rational Root Test, any rational root must be in $\{\pm 1, \pm 2, \pm 4\}$. Check these to see that there are no roots in $\mathbb{Q}$, hence no linear factors. As in Section 4.5, If the polynomial factors nontrivially then: $x^4 - 16x^2 + 4 = (x^2 + ax + b)(x^2 + cx + d)$ for some $a, b, c, d \in \mathbb{Z}$. Then $a + c = 0$, $ac + b + d = -16$, $bc + ad = 0$ and $bd = 4$. If $a = 0$ then $c = 0$, and $b + d = -16$, which is impossible for integers with $bd = 4$. Then $c = -a \neq 0$, and $a(-b + d) = 0$ implies $b = d$. Consequently $-a^2 + 2b = -16$ and $b^2 = 4$. Then $b = \pm 2$ and $a^2 = 20$ or 12, which is impossible in $\mathbb{Z}$. Hence no factorization exists.

15. Answered in the text.

16. See Exercise 10.

17. (a) $(x^2 - 1)^2 - 5 = x^4 - 2x^2 - 4$ (b) $(x^2 + 1)^2 + 24 = x^4 + 2x^2 + 25$. These can be proved irreducible as in Exercise 14.

18. Over $\mathbb{Q}$: $(x^2 + 1)^2 + 8 = x^4 - 2x^2 + 9$. Prove irreducibility as in Exercise 14.
Over $\mathbb{R}$: $(x - \sqrt{2})^2 + 1 = x^2 - 2\sqrt{2}x + 3$.

19. By Theorem 10.7, $[F(u) : F] = p$ is prime. Apply Exercise 10.1.39.

20. We know $F \subseteq F(u^2) \subseteq F(u)$. Since u is a root of $x^2 - u^2$, the minimal polynomial of u over $F(u^2)$ must have degree 1 or 2. By Theorem 10.7, $[F(u) : F(u^2)] = 1$ or 2. That Theorem also implies that $[F(u) : F]$ is odd. Theorem 10.4 then applies.

21. Answered in the text.

22. $(\Leftarrow)$ $\sqrt{r} = t\sqrt{s}$ and t ≠ 0 so the fields coincide. $(\Rightarrow)$ If $\sqrt{s}$ is rational then $r = u^2$ and $s = v^2$ for some $u, v \in \mathbb{Q}$. Let $t = u/v$. If $\sqrt{2}$ is irrational we have $\sqrt{r} = a + b\sqrt{s}$ for some $a, b \in \mathbb{Q}$. Then $r = a^2 + sb^2 + 2ab\sqrt{s}$. By the irrationality, $r = a^2 + sb^2$ and $ab = 0$. If b = 0 then $\sqrt{r} = \pm a \in \mathbb{Q}$ which implies that $\sqrt{s} \in \mathbb{Q}$, contrary to hypothesis. Hence $a = 0$ and $r = sb^2$.

23. Let $\{1, c\}$ be a basis of K over $\mathbb{Q}$. Then $c^2 \in K$ is expressible as $c^2 = rc + s$ for some $r, s \in \mathbb{Q}$, and c is a root of $x^2 - rx - s \in \mathbb{Q}[x]$. If this polynomial factors in $\mathbb{Q}[x]$ its roots would be rational, but $c \notin \mathbb{Q}$ since $\{1, c\}$ is linearly independent. By the quadratic formula, $c = (r \pm \sqrt{d})/2$ where $d = r^2 + 4s$. Then $\sqrt{d} = \pm(2c - r) \in K$ and $K = \mathbb{Q}(c) \subseteq \mathbb{Q}(\sqrt{d}) \subseteq K$. Then $K = \mathbb{Q}(\sqrt{d})$. Altering d by a nonzero square factor in $\mathbb{Q}$ changes $\sqrt{d}$ by a rational multiple, and this generates the same field. Therefore we may assume d is a square-free integer.

24. The evaluation map $\varphi : F[x] \to F[u]$ sending $f(x)$ to $f(u)$ is a surjective ring homomorphism. Since u is transcendental, the kernel is $\{0_F\}$ and the map is an isomorphism. Suppose $F[u] \subseteq K$ for some field K.
The results on fields of quotients in Section 9.4 imply that φ extends to a homomorphism $\tilde{\varphi} : F(x) \to K$ where $\tilde{\varphi}(f(x)/g(x)) = f(u)g(u)^{-1}$ (compare Exercise 9.4.8). Since $F(u)$ is the smallest field containing $F[u]$ this provides an isomorphism $F(x) \cong F(u)$.

25. Suppose $w \in F(u)$ is algebraic over F and $w \notin F$. Let $f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_0$ be its minimal polynomial. Note that $n \geq 2$ and $c_0 \neq 0$ since $w \notin F$ and $f(x)$ is irreducible. Express $w = a(u)/b(u)$ where $a(u), b(u) \in F[u]$ are polynomials with $gcd = 1$ (see Exercise 24). The analog of the Rational Root Test (see Exercise 9.5.11) implies that $b(u)/1$ and $a(u)|c_0$ in the ring $F[u]$. This implies that $a(u)$, $b(u)$ are units, and hence lie in F. Then $w \in F$, contrary to hypothesis.

26. By Exercises 24 and 25 we need only check that $x^3/(x+1) \notin F$.

11.3 Algebraic Extensions

1. Both equal $F(u, v)$.

2. Certainly $[K : F]$ is finite. Use Theorem 10.9.

3. (a), (c) answered in the text. (b) $\{1, \sqrt{5}, \sqrt{7}, \sqrt{35}\}$ (d) $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{3}, \sqrt{3}\sqrt[3]{2}, \sqrt{3}\sqrt[3]{4}\}$

4. $\{1, \sqrt{2}\}$

5. Answered in the text.

6. The given field is $\mathbb{Q}(\sqrt{2}, \sqrt{5})$. Verify that $\sqrt{5} \notin \mathbb{Q}(\sqrt{2})$.

7. Answered in the text.

8. If $\{v_1, \ldots, v_n\}$ is a basis of K over F and $w \in K(u)$ then $w = a_0 + a_1 u + \cdots + a_m u^m$ for some $a_j \in K$. Express each a_j as a linear combination of the v_i over F and collect terms to see that w is a combination of the v_i with coefficients in $F(u)$. Hence $\{v_1, \ldots, v_n\}$ contains a basis of $K(u)$ over $F(u)$, and $[K(u) : F(u)], \leq n$.

9. Answered in the text.

10. (⇐) This is Theorem 10.10. (⇒) If $\{v_1, . . . , v_n\}$ is a basis of K over F then certainly $K = F(v_1, . . . , v_n)$. By Theorem 10.9 each v_i is algebraic over F.

11. (a) Answered in the text, (b) Use $u = v = i$ over $\mathbb{R}$. (c) 6 using part (a) with $x^2 - 2$ and $x^3 - 2$.

12. Suppose $u \in D$ and $u \notin F$. By Theorem 10.9 u has a minimal polynomial $x^n + c_{n-1}x^{n-1} + \cdots + c_0$. Then $n > 1$ and $c_0 \neq 0$ so that $u^{-1} = c_0^{-1}\cdot(u^{n-1} + c_{n-1}u^{n-2} + \cdots + c_1) \in F[u] \subseteq D$.

13. Answered in the text.

14. (a) Check closure under addition, multiplication and inverse.
    (b) If c is in the union then $c \in F_i$ for some i and hence c is algebraic over F_1.

15. Answered in the text.

16. The number $2^{1/n}$ is a root of $x^n - 2$, which is irreducible over $\mathbb{Q}$ by Eisenstein. Then it lies in E and $n = [\mathbb{Q}(2^{1/n}) : \mathbb{Q}] \leq [E : \mathbb{Q}]$. Since this holds for every n, the degree $[E : \mathbb{Q}]$ must be infinite.

17. If $u = v$ the result is clear. If $u \neq v$, compute $2(u - v)\sqrt{v} = (\sqrt{u} + \sqrt{v})^3 - (u + 3v)(\sqrt{u} + \sqrt{v})$. Since $2\cdot 1_F \neq 0_F$ and $u - v \neq 0_F$, conclude that $\sqrt{v} \in F(\sqrt{u} + \sqrt{v})$. Similarly for $\sqrt{u}$.

18. Consider the tower $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{n_1}) \subseteq \mathbb{Q}(\sqrt{n_1}, \sqrt{n_2}) \subseteq . . .$ and apply Theorem 10.4.

19. It is perhaps easier to prove a stronger result:

    Lemma. Let $a_1, a_2, . . .$ be square-free integers where $a_i \neq 1$ and $(a_i, a_j) = 1$ for every $i \neq j$.

    Then $r(a_{k+1}) \notin \mathbb{Q}(\sqrt{a_1}, \cdots, \sqrt{a_k})$.

    Proof. Suppose $\sqrt{a_{k+1}}$ is in that field. First let $k = 1$.Then by Exercise 10.2.22, $a_2 = t^2 a_1$ for some $t \in \mathbb{Q}$. Expressing $t = r/s$ in lowest terms we get $s^2 a_2 = r^2 a_1$ in $\mathbb{Z}$. Since a_1, a_2 are square-free it follows that $a_1 = a_2$ and $1 = (a_1, a_2) = a_1$ contrary to hypothesis. Now assume the result true for sequences of $k - 1$ terms. Let $u = a_{k+1}$, $v = a_k$ and $E = \mathbb{Q}(\sqrt{a_1}, . . . , \sqrt{a_{k-1}})$. Then $\sqrt{u} \in E(\sqrt{v})$ and Exercise 10.2.22 implies that $u = t^2 v$ for some $t \in E$. But then $\sqrt{uv} \in E$, contradicting the inductive hypothesis applied to the sequence $a_1, . . . , a_{k-1}, uv$.

11.4 Splitting Fields

1. If $\sqrt{2} \in \mathbb{Q}(i)$ then it is a real number in $\mathbb{Q}(i)$, so it must lie in $\mathbb{Q}$. But $\sqrt{2}$ is irrational.

2. They are irreducible by Eisenstein. The roots of $x^2 - 3$ are $\pm\sqrt{3}$. the roots of $x^2 - 2x - 2$ are $1 \pm \sqrt{3}$.

3. Answered in the text.

4. By the Fundamental Theorem of Algebra (see Corollary 4.27) $f(x)$ splits in $\mathbb{C}$. Then there is a splitting field E of $f(x)$ with $\mathbb{R} \subseteq E \subseteq \mathbb{C}$. Since $[\mathbb{C}\colon \mathbb{R}] = 2$ we know that $E = \mathbb{R}$ or $E = \mathbb{C}$.

5. Let $u_1 \; . \; . \; . \; , u_n$ be the roots of $f(x)$ in K. Then $K = F(u_1 \; .. \; . \; , u_n)$ so that $K = E(u_1 \; . \; . \; . \; , u_n)$.

6. $F \subseteq F(u) \subseteq K$ and apply Exercise 10.2.39.

7. Answered in the text.

8. (a) normal (b) not normal (c) normal

9. The given polynomial $\in F[x]$ has no root in F.

10. $(x^2 + 4x + 1)(x^2 - 2x - 1)$. The quadratic formula gives the roots.

11. Answered in the text.

12. (a) $\mathbb{Q}(\sqrt[4]{2}, \mathrm{i})$ (b) $\mathbb{C}$

13. Since $(x^6 + x^3 + 1)(x^3 - 1) = x^9 - 1$, deMoivre's Theorem implies that the complex roots of the given polynomial are α, α^2, α^4, α^5, α^7, α^8 where $\alpha = e^{2\pi i/9} = \cos(2rc/9) + i \cdot \sin(2rc/9)$. The splitting field is $\mathbb{Q}(\alpha)$, which has degree 6 over $\mathbb{Q}$.

14. The roots are $\sqrt{2} \pm i$.

15. Answered in the text.

16. Let $K = \mathbb{Z}_2[x]/(x^3 + x + 1)$. This is a field of 8 elements, since that polynomial is irreducible. The element $\alpha = [x] \in K$ is one root. The elements α^2 and $\alpha^2 + \alpha$ are the other 2 roots in K. Hence K is a splitting field.

17. Suppose $f(x) \in F[x]$ is irreducible and has a root $c \in K$. Then $f(x)$ is the minimal polynomial of c and $deg\ f(x) = [F(c) : F] \leq [K : F] = 2$. Therefore $f(x) = (x - c)q(x)$ for some $q(x) \in K[x]$ of degree ≤ 1. Hence every root of $q(x)$ also lies in K and $f(x)$ splits in K.

18. $(\Rightarrow)$ see Exercise 5. $(\Leftarrow)$ Given $K = E(u_1, \; . \; . \; . \; , u_n)$ where $f(x) = c(x - u_j) \cdot \cdot \cdot (x - u_n)$. Since $E = F(u_1, \; . \; . \; . \; , u_t)$ conclude that $F(u_1, \; . \; . \; . \; , u_n) = E(u_1, \; . \; . \; . \; , u_n) = K$ as well.

19. (i) $\Rightarrow$ (ii). Let $f(x)$ be a nonconstant polynomial of degree n in $K[x]$. By (i) there exists $c \in K$ with $f(x) = (x - c)f_1(x)$ where $deg\ f_1(x) = n - 1$. If $f_1(x)$ is nonconstant apply (i) again to get another linear factor.

Repeating this n times shows that $f(x)$ splits in $K[x]$.

(ii) $\Rightarrow$ (iii). If $f(x)$ is irreducible then by (ii) it splits into linear factors. Since there are no nontrivial factorizations there can be only one factor.

(iii) $\Rightarrow$ (iv). If $K \subseteq E$ is an algebraic extension with $K \neq E$ let $u \in E$ with $u \neq K$. Then the minimal polynomial $p(x) \in K[x]$ for u over K must be irreducible of degree > 1, contrary to (iii).

(iv) $\Rightarrow$ (i). If $f(x) \in K[x]$ is nonconstant, let $E = K(u)$ be a field obtained by adjoining a root u of $f(x)$.

By (iv) $E = K$ so that $u \in K$.

20. By Corollary 10.12 E is algebraic over F. If $f(x) \in E[x]$ is a nonconstant polynomial then it has a root $u \in K$ since K is algebraically closed. By Corollary 10.11 $E(u)$ is algebraic over F, so that u is algebraic over F and $u \in E$. By Exercise 19 E is algebraically closed.

21. Answered in the text.

22. If $F = K$ we are done. Otherwise choose $u \in K$ with $u \notin F$ and define $F = F(u)$. Since $[K : F]$ is finite, u is algebraic over F and has a minimal polynomial $p(x) \in F[x]$. Let K' be an extension of K containing a root of $\sigma p(x)$. By Corollary 10.8 there is a homomorphism σ' : $F \to K'$ extending σ. Now if $F' = K$ we are done. Otherwise choose $u' \in K$ with $u' \notin F'$, let $F'' = F'(u')$ and repeat the argument. After a finite number of such steps we get an extension of σ to the field K.

23. ($\Rightarrow$). Suppose K is a normal extension and $\sigma : K \to L$ is given. For $u \in K$, let $p(x)$ be the minimal polynomial of u over F. Then $\sigma(u)$ is a root of $\sigma p(x) = p(x)$. Since all the roots of $p(x)$ lie in K by hypothesis, we conclude $\sigma(u) \in K$.

    ($\Leftarrow$). Let $p(x)$ be the minimal polynomial of u over F. (u is algebraic since $[K : F]$ is finite.) Let M be a splitting field of $p(x)$ over K and let w be another root of $p(x)$ in M. By Corollary 10.8 there is an isomorphism $\sigma : F(u) \to F(w)$ where $\sigma(a) = a$ for every $a \in F$ and $\sigma(u) = w$. Exercise 22 provides an extension L of M and a homomorphism $\varphi : M \to L$ extending σ. By hypothesis $\sigma(K) \subseteq K$ and therefore $w = \varphi(u) \in K$. Therefore every root of $f(x)$ lies in K, so that K is normal.

11.5 Separability

1. Answered in the text.

2. $n1_K = n1_F \neq 0_F$.

3. The homomorphism $\varphi : \mathbb{Z} \to F$ is injective.

4. (a) If $f(x) = \Sigma\ a_m x^m$ and $g(x) = \Sigma\ b_m x^m$ then $(f + g)'(x) = (\Sigma\ (a_m + b_m)x^m)' = \Sigma\ (a_m + b_m)mx^{m-1} = \Sigma\ a_m mx^{m-1} + \Sigma\ b_m mx^{m-1} = f(x)\cdot g'(x)$.
   (b) $(cf)'(x) = (\Sigma\ ca_m x^m)' = \Sigma\ ca_m mx^{m-1} = cf'(x)$.

5. (a) $(fg)'(x) = \Sigma\ cb_m x^{m+n} = \Sigma\ cb_m(m + n)x^{m+n-1} = cx^n\ \Sigma\ b_m mx^{m-1} + cnx^{n-1}\Sigma\ b_m x^m = f(x)g'(x) + f'(x)g(x)$.
   (b) Use the Hint.

6. The case $n = 1$ is clear. Suppose $n > 1$ and the result is true for $n - 1$. Then $(f^n)' = (f\cdot f^{n-1})' = f'\cdot f^{n-1} + f\cdot(f^{n-1})' + f\cdot(f^{n-1})' = f'\cdot f^{n-1} + f\cdot((n-1)f^{n-2}\cdot f') = f^{n-1}\cdot f'$.

7. (a) Answered in the text.
   (b) $f(x) = x^2$ has $f'(x) = 0$ in $\mathbb{Z}_2[x]$.

8. $f'(x) = (x - u)^{m-1}(mg(x) + (x - u)g'(x))$. Since $mg(u) \neq 0_F$ we see that $m > 1$ if and only if $f'(u) = 0_F$.

9. Answered in the text.

10. If $p(x)$ is separable then $p(x)$ and $p'(x)$ are relatively prime. Since $p(x)$ is nonconstant this implies that $p'(x) \neq 0_F$. Conversely if $p(x)$ is not separable then the gcd is not a unit. It divides $p(x)$ so the irreducibility implies the gcd is an associate of $p(x)$. Therefore $p(x) \mid p'(x)$. Comparing degrees we get a contradiction unless $p'(x) = 0_F$.

11. If u is a root of F use the factorization in Exercise 8 to see that $(x - u)^{m-1}$ is the largest power of $(x - u)$ dividing $d(x)$. Therefore $(x - u)$ divides $h(x)$ but $(x - u)^2$ does not. Parts (a) and (b) now follow.

12. (a) $\mathbb{Q}(\sqrt{2} + c\sqrt{3})$ for any $c \neq 0$ in $\mathbb{Q}$.
    (b) $\mathbb{Q}(\sqrt{3} + ci)$ for any $c \neq 0$ in $\mathbb{Q}$.
    (c) $\mathbb{Q}(\sqrt{2} + c\sqrt{3} + d\sqrt{5})$ for any $c,\ d \neq 0$ in $\mathbb{Q}$.

13. Answered in the text.

14. The proof of Theorem 10.18 never uses the assumption that v is separable.

15. (a) Use the analog of Eisenstein for the domain $\mathbb{Z}_2[x]$, as in Exercise 9.5.13.
    (b) Done in the hint. In fact, if α is a root then $x^2 - t = (x - \alpha)^2$.

11.6 Finite Fields

1. See Exercise 3.2.21.

2. (a)0 (b) 6 (c) 3 (d) 0 (e) 3

3. Answered in the text.

4. If P is the prime subfield then it is generated by 1_k so it is contained in every subfield.

5. Answered in the text.

6. $x^k - 1_k$ has every $a \neq 0_k$ as a root (see the proof of Theorem 10.25). Therefore it has $k = p^n - 1$ distinct roots, so it splits into linear factors in $K[x]$. That is, all the roots lie in K.

7. Given $a^{p^n} = a$. Then $(-a)^{p^n} = -a$ if p is odd. If $p = 2$ then $-1 = 1$ in $\mathbb{Z}_2$ and $(-a)^{p^n} = a = -a$.

8. Since $p{\cdot}1 = 0$ we know $\mathbb{Z}_p(x)$ has characteristic p. Since 1, x, x^2, x^3, . . . are distinct polynomials the field is infinite.

9. As in Exercise 7 note that $(-1)^{p^n} = -1$. The claim follows by Lemma 10.24.

10. $f(ab) = (ab)^p = a^p b^p = f(a)f(b)$ and $f(a + b) = f(a) + f(b)$ by Lemma 10.24. If a is in the kernel then $a^p = 0$ which implies $a = 0$ since we are in a field. Therefore f is injective. Since K is finite f is automatically surjective (see Exercise 32 of Appendix B).

11. In $\mathbb{Z}_6$ $(1 + 1)^6 = 4$ while $1^6 + 1^6 = 2$. In $M(\mathbb{Z}_2)$ let a $= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then $a^2 + b^2 = 0$ while $(a + b)^2 = \text{I}$.

12. Apply the isomorphism of Exercise 10 to the equation $f(c) = 0$.

13. Answered in the text.

14. $f(x)$ has only finitely many roots so the set E is finite. Since it is a field, Theorem 10.23 implies that deg $f(x) = |E| = p^n$ for some prime p and integer $n \geq 1$. Theorem 10.25 states that E is exactly the set of roots of $g(x) = x^{p^n} - x$. Therefore $g(x)$ and $f(x)$ have the same set of roots, and they are both separable. Therefore $f(x) = cg(x)$ for some $c \in E$. Since both polynomials are monic we find $c = 1$.

15. In each case the field is $K = \mathbb{Z}_p[x]/(g(x))$ where $g(x)$ is the given irreducible polynomial.

    (a) The polynomial has no root in $\mathbb{Z}_2$ so it is irreducible. (See Corollary 4.18.)

    (b) It has no root in $\mathbb{Z}_3$ so it is irreducible.

    (c) It has no root in $\mathbb{Z}_2$ and it is not the square of the only irreducible quadratic polynomial $x^2 + x + 1$. Hence it is irreducible.

16. (a) Check closure under addition and multiplication, using Lemma 10.24.
    (b) As in Exercise 10 the map $\varphi_m : K \to K$ defined by $\varphi_m(c) = c^{p^m}$ is an isomorphism. Clearly $\varphi_m(F) \subseteq F$ for any subfield. Since φ_m is bijective we see that $\varphi_m(F) = F$. The set L is defined to be $L = \varphi_m^{-1}(F) = F$.

17. Answered in the text.

18. Done in the Hint.

19. (a) $|F| = p^d$ for some d using Theorem 10.23. Since the group F* of nonzero elements of F is a subgroup of K*, Lagrange's Theorem implies that $(p^d - 1) \mid (p^n - 1)$. Then $d \mid n$ by Exercise 18.
    (b) Exercise 18(b) implies that $(p^d - 1) \mid (p^n - 1)$. By Exercise 18(a), $(x^{pd} - x) \mid (x^{pn} - x)$. By Theorem 10.25, $x^{p^n} - x$ splits in $K[x]$. Therefore $x^{p^d} - x$ also splits in K. The set E of the p^d roots of this polynomial provides the desired subfield, by Theorem 10.25. The uniqueness follows since any subfield of p^d elements must consist exactly of the roots of $x^{p^d} - x$.

20. See Exercise 10.3.13. Let α be a root of $f(x)$ is a splitting field of $f(x)$ over K. Then $3[K(\alpha): K] = [K(\alpha): \mathbb{Z}_p\ ] = 2[K(\alpha): \mathbb{Z}_{\mathrm{p}}(\alpha)]$. Therefore $[K(\alpha): K] \geq 2$ so that $f(x)$ is irreducible over K.

21. Let K be the given field with p^n elements. If $p = 2$ then every element is a square, by Exercise 10. Suppose p is odd and let $S = \{a^2 \mid a \in K\}$ the set of all squares in K. If a, b are nonzero in K then: $a^2 = b^2$ if and only if $a = b$ or $-b$. (Why?) Therefore exactly half of the nonzero elements of K are squares. Since 0 is a square, S contains more than half the elements of K. For any given $c \in K$ let $T = \{c - b^2 \mid b \in K\}$. Again T contains more than half of the elements of K. Therefore S and T cannot be disjoint sets, so there exists $a^2 = c - b^2$ for some $a, b \in K$. Therefore c is a sum of two squares.

22. Since the set K* of nonzero elements of K is a group of order $p^n - 1$, Lagrange's Theorem (Corollary 7.27) implies that $c^{p^n - 1} = 1_k$ for every $c \neq 0_k$. Then every $c \in K$ satisfies $c^{p^n} = c$ so it is a root of $x^{p^n} - x$. Therefore K is the splitting field of $x^{p^n} - x$. The proof of the other direction in Theorem 10.25 remains the same.

Chapter 12

Galois Theory

12.1 The Galois Group

1. Answered in the text.

2. Yes, by Theorem 11.4.

3. Answered in the text.

4. This is easily done since $\tau^2 = \alpha^2 = \beta^2 = \iota$ and $\tau\alpha = \beta$.

5. Answered in the text.

6. Since σ is an automorphism for the additive group we see that $\sigma(n) = n \cdot \sigma(1) = n$. Also, $n \cdot \sigma(m/n) = \sigma(m) = m$ so that $\sigma(m/n) = m/n$ Therefore σ fixes $\mathbb{Q}$.

7. (a) $\mathbb{Q}(\sqrt{2})$ is the splitting field of $x^2 - 2$ so there are at most 2 elements in the Galois group. Since $x^2 - 2$ is irreducible, Corollary 10.8 implies the existence of an automorphism σ with $\sigma(\sqrt{2}) = -\sqrt{2}$.
   (b) The same argument applies since $x^2 - d$ is irreducible.

8. If $c = \sqrt[4]{2}$ then c and $-c$ are roots of $x^4 - 2$. This polynomial is irreducible in $\mathbb{Q}[x]$ and Corollary 10.8 provides an automorphism σ of $\mathbb{Q}(c)$ with $\sigma(c) = -c$.

9. Answered in the text.

10. (a) The group is $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
    (b) By Exercise 10.3.19, $\mathbb{Q}\{\sqrt{p},\ \sqrt{q})$ has degree 4 over $\mathbb{Q}$. It follows that $x^2 - 3$ is irreducible over $\mathbb{Q}$ and $x^2 - 5$ is irreducible over $\mathbb{Q}(\sqrt{3})$. The argument in Example 2.A is valid here, replacing 3 by p and 5 by q.

11. As in Exercise 10.3.5 we know the degree is 4. Proceed as in Exercise 10.

12. Since any automorphism sends $\sqrt{c}$ to $\pm\sqrt{c}$ there are at most 8 automorphisms. By Exercise 10.3.19 the degree of this field is 8. Therefore $x^2 - 5$ is irreducible over $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ so that each of the 4 automorphisms of K extends to the whole field in 2 ways, (sending $\sqrt{5}$ to $\pm\sqrt{5}$). Then we have constructed 8 automorphisms, each with square $= \iota$.

13. Theorems 10.17 and 10.18 imply that $K = F(u)$ for some u. Let $p(x)$ be the minimal polynomial of u over F. Since K is a splitting field, it is normal by Theorem 10.15. Since $p(x)$ has one root in K it must split: $p(x) = (x - u_1)(x - u_2)\cdots(x - u_n)$ where $u = u_1$. Note that $n = deg\ p(x) = [K : F]$. Any $\sigma \in Gal_F K$ must have $\sigma(u) = u_i$ for some i. Theorem 11.4 then implies that there are at most n elements in that group.
Since the characteristic is 0, the roots u_i are distinct. Corollary 10.8 provides an F-isomorphism $K = F(u) \to F(u_i) = K$ sending $u \to u_i$. Then we have n different elements of $Gal_F K$, and therefore $|Gal_F K| = n = [K : F]$.

14. That degree in the Hint is 2 since $[\mathbb{Q}(\sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 4$.

15. (a) Any automorphism sends squares to squares. Hence it sends positives to positives.
    (b) Apply the Hint and part (a).
    (c) As in Exercise 6, σ fixes $\mathbb{Q}$. Then if $r \in \mathbb{R}$ and $c < r < d$ for $c, d \in \mathbb{Q}$ then $c < \sigma(r) < d$. This implication forces $r = \sigma(r)$. (The proof involves the definition of $\mathbb{R}$. For example, let $C(r) = \{(a \in \mathbb{Q} \mid a < r\}$. Then r is the least upper bound of the set $C(r)$. Since $C(r) = C(\sigma(r))$ it follows that $r = \sigma(r)$.)

16. Any $\sigma, \tau \in Gal_{\mathbb{Q}}\mathbb{Q}(\zeta)$ have $\sigma(\zeta) = \zeta^i$ and $\tau(\zeta) = \zeta^j$ for some i, j (by Theorem 11.2). Then $\sigma\tau(\zeta = \sigma(\zeta^j) = \sigma(\zeta)^j = \zeta^{ij} = \tau(\zeta)$. By Theorem 11.4 conclude that $\sigma\tau = \tau\sigma$.

17. For $u \in E$ let $p(x)$ be the minimal polynomial of u over F. Since $p(x)$ has one root in E and E is normal over F we know that $p(x)$ splits in $E[x]$. By Theorem 11.2 $\sigma(u)$ is a root of $p(x)$ and hence $\sigma(u) \in E$.

12.2 The Fundamental Theorem of Galois Theory

1. Answered in the text.

2. K is a Galois extension of $\mathbb{Q}$ and $|Gal_{\mathbb{Q}}K| = [K : \mathbb{Q}] = p$ by the Fundamental Theorem 11.11. So it must be $\cong \mathbb{Z}_p$.

3. $\omega^2 = (-1 - \sqrt{3}i)/2$ so that $\omega^3 = \omega\omega^2 = 1$. Also $\omega + \omega^2 = -1$ so that $(x - \omega)(x - \omega^2) = x^2 + x + 1$. Alternatively we can apply the quadratic formula to $x^2 + x + 1$ to see that ω and ω^2 are roots.

4. In each case we have a field K with $[K : \mathbb{Q}] = 2$. Such an extension is always Galois with group $G \cong \mathbb{Z}_2$. The only intermediate fields are $\mathbb{Q} \subseteq K$; the only subgroups are $G \supseteq \langle e \rangle$.

5. Answered in the text.

6. $F = \mathbb{Q}$, $\quad K = \mathbb{Q}(\sqrt{2})$, $\quad L = \mathbb{Q}(\sqrt{3})$.

7. Let $K = F(\sqrt{a}, \sqrt{b})$ be an extension of F of degree, and assume the characteristic is $\neq 2$ so that the extension is separable. Then K is a Galois extension of F and the Galois group is $G = \{\iota, \alpha, \beta, \alpha\beta\}$ where α fixes $\sqrt{a}$ and sends $\sqrt{b}$ to its negative, and β fixes $\sqrt{b}$ and sends $\sqrt{a}$ to its negative. The intermediate fields are F, $F(\sqrt{a})$, $F(\sqrt{b})$, $F(\sqrt{ab})$, and K. The corresponding subgroups are G, $\langle\alpha\rangle$, $\langle\beta\rangle$, $\langle\alpha\beta\rangle$, $\langle \mathrm{e}\rangle$.

8. In fact if E is any intermediate field then it is normal over F. This follows from Theorem 11.11, since its corresponding subgroup is normal in the abelian group $G = Gal_F K$. Note that $Gal_E K \subseteq G$ and $Gal_F E$ is a quotient group of G. Therefore these groups are also abelian.

9. (a) Answered in the text. (b) By Exercise 7.3.40 there is exactly one subgroup of $\mathbb{Z}_n$ for every positive divisor of n. Apply the Galois correspondence.

10. ($\Rightarrow$) Suppose $\sigma(E) = L$. If $\alpha \in Gal_E K$ then $\alpha(x) = x$ for every $x \in E$. Check that $\sigma\alpha\sigma^{-1}$ fixes L so it lies in $Gal_L K$. Therefore $\sigma(Gal_E K)\sigma^{-1} \subseteq Gal_L K$. The same argument applied to $\sigma^{-1}(L) = E$ provides the reverse inclusion. Hence $Gal_E K$ and $Gal_L K$ are conjugate.

    ($\Leftarrow$) Suppose $\sigma(Gal_E K)\sigma^{-1} = Gal_L K$. If $c \in E$ then c is fixed by every $\sigma^{-1}\beta\sigma$ for $\beta \in Gal_L K$. Then $\beta\sigma(c) = \sigma(c)$ so that $\sigma(c)$ is fixed by $Gal_L K$. The Galois correspondence (Theorem 11.9) implies that $\sigma(c) \in L$. Therefore $\sigma(E) \subseteq L$. The same argument applied to σ^{-1} provides the reverse inclusion.

11. (a) Let $c = \sqrt[4]{2}$. The roots of $x^4 - 2$ are c, ic, $-c$, $-ic$, so the splitting field is generated by c and i.
    (b) Answered in the text.
    (c) Using (b) we see that $x^4 - 2$ is still irreducible in $\mathbb{Q}(i)[x]$. Since c and ci are roots, Corollary 9.8 implies that there is an automorphism σ fixing $\mathbb{Q}(i)$ sending c to ci. Then $\sigma^2(c) = \sigma(ci) = (ci)i = -c$. Similarly we compute $\sigma^3(c) = -ci$ and $\sigma^4(c) = c$. Therefore $|\sigma| = 4$.
    (d) These 8 elements are distinct since they act differently on the generators c and i.
    (e) Since $|Gal_{\mathbb{Q}} K| = [K : \mathbb{Q}] = 8$ we have a complete list of the Galois group. Note that $\tau\sigma\tau = \sigma^{-1}$. Mapping σ to r_1 and τ to d, check the tables to see that this group is $\cong D_4$.

12. The element σ fixes $\mathbb{Q}(i)$ and has order 4. Since that Galois group has order $= [K : \mathbb{Q}(i)] = 4$, it must be $\langle\sigma\rangle$.

13. Here is a chart of the correspondence. Let $c = \sqrt[4]{2}$.

Subgroups of G	Intermediate fields
G	$\mathbb{Q}$
$\langle\sigma\rangle$	$\mathbb{Q}(i)$
$\langle\sigma^2\rangle$	$\mathbb{Q}(i, \sqrt{2})$
$\langle\tau, \sigma^2\rangle$	$\mathbb{Q}(\sqrt{2})$
$\langle\tau\rangle$	$\mathbb{Q}(c)$
$\langle\sigma\tau\rangle$	$\mathbb{Q}((1 + i)\mathrm{c})$
$\langle\sigma^3\tau\rangle$	$\mathbb{Q}((1 - i)\mathrm{c})$
$\langle e\rangle$	K

14. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and $G = Gal_{\mathbb{Q}}$K. Let $\alpha \in G$ be the automorphism fixing $\sqrt{2}$ and $\sqrt{3}$ and sending $\sqrt{5}$ to its negative. Similarly let β fix $\sqrt{2}$ and $\sqrt{5}$ and send $\sqrt{3}$ to its negative, and let γ fix $\sqrt{3}$, $\sqrt{5}$ and send $\sqrt{2}$ to its negative.

    The $G = \{e, \alpha, \beta, \gamma, \alpha\beta, \alpha\gamma, \beta\gamma, \alpha\beta\gamma\}$ and the subgroups are easy to write out. The intermediate fields are generated by some of: $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{10}$, $\sqrt{15}$, $\sqrt{130}$. Listing the explicit groups and fields is straightforward.

12.3 Solvability by Radicals

1. (a) Answered in the text.
   (b) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}\,, i) \subseteq \mathbb{Q}(\sqrt{2},\ i,\ \sqrt[3]{5}) \subseteq \mathbb{Q}(\sqrt{2},\ i,\ \sqrt[3]{5},\ \sqrt[5]{\sqrt{2}+1})$
   (c) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2},\ \sqrt[3]{3-\sqrt{2}})$.

2. Compute the roots by the quadratic formula and note that $\mathbb{Q}(\sqrt{3})$ is the splitting field in each case.

3. There is a chain $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_t = K$ where $F_i = F_{i-1}(u_i)$ and $u_i^{ni} \in F_{i-1}$. Theorem 10.7 implies that $[F_i : F_{i-1}] \leq n_i$. Then Theorem 10.4 implies that $[K : F] \leq n_1\ n_2 \cdots n_t$.

4. If A_n is solvable then there is a chain of subgroups $A_1 = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_t = \langle e \rangle$ with abelian quotients. But then $S_n \supseteq A_n \supseteq H_1 \supseteq \cdots \supseteq H_1 = \langle e \rangle$ is a similar chain, contradicting Theorem 11.14. Compare Exercise 10 below.

5. (a) Answered in the text.
   (b) D_4 has a subgroup H of order 4. Then H is abelian and has index 2, so it is normal with abelian quotient. The chain is $D_4 \supseteq H \supseteq \langle e \rangle$.

6. If G is solvable there is a chain $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \langle e \rangle$ with each G_i normal in $G_{i\text{-}1}$ with abelian quotient. We may delete repetitions to assume that $G_i \neq G_{i\text{-}1}$ for each i. Since G is simple the only possibility for the proper normal subgroup G_1 is $\langle e \rangle$. But then $G \cong G/G_1$ is abelian, contrary to hypothesis.

7. (a), (c), (e) Answered in the text.
   (b) $1,\ (-1 \pm i\cdot 1, (- \pm i \cdot \sqrt{3})/2$
   (d) $\cos(2\pi k/5) + i \cdot \sin(2\pi k/5)$ for $k = 0, 1, 2, 3, 4$. If $\zeta = \cos(2\pi/5) + i \cdot \sin(2\pi/5)$, then the roots are $1,\ \zeta,\ \zeta^2\ ,\ \zeta^3,\ \zeta^4$. These quantities can be expressed explicitly in terms of radicals. For example, $\zeta = (1+\sqrt{5})/4 + \mathrm{i} \cdot \sqrt{(5+\sqrt{5}))/8}$.

8. Compare Exercise 7.9.34. (a) The values $\alpha(r)$, $\alpha^2(r)$, . . . range over all 5 symbols since α is a 5-cycle. One of those symbols is s, so that $\alpha^k(r) = s$ for some k.
   (b) Direct calculation. Compare Exercise 7.9.24.
   (c) $(12)(23)(12) = (13)$, $(13)(34)(13) = (14)$, etc.
   (d) If $a,\ b \neq 1$ then $(ab) = (1a)(1b)(1a) \in G$.

9. (a) Free choice of 4 elements of G has n^4 possibilities.
   (b) This follows since a composition of cyclic permutations is another cyclic permutation.
   (c) Suppose 2 elements of an equivalence class are the same. For example, $(r, s, t, u, v) = (t, u, v, r, s)$. Then $r = t$, $s = u$, $t = v$, $u = r$, $v = s$. Then $r = t = v = s = u$, so all the entries are equal. The other cases are similar.
   (d) S is a union of the disjoint equivalence classes. Since $|S| = n^4$ is a multiple of 5 and every class has 1 or 5 elements, the number of singleton classes must be a multiple of 5. Since (e, e, e, e, e) provides one singleton class, there must be at least 4 others.
   (e) Suppose $c \neq e$ and $\{(c, c, c, c, c)\}$ is a singleton class. The definition of S implies $c^5 = e$. Then $|c|$ divides 5 and is $\neq 1$, so $|c| = 5$.

10. Suppose $G/N = T_0 \supseteq T_1 \supseteq \cdots \supseteq T_k\langle Ne\rangle$ is a chain of subgroups with successive quotients abelian. By Theorem 7.44 there are subgroups H_i of G with $N \subseteq H_i$ and $H_i/N = T_i$. Then $G = H_0 \supseteq H_1 \supseteq \cdots \supseteq H_k = N$. Applying Theorem 7.44 to $N \subseteq H_i \subseteq H_{i-1}$ we find that H_i is normal in H_{i-1} and Theorem 7.43 implies that $H_{i-1}/H_i \cong T_{i-1}/T_i$ is abelian. Now since N is also solvable, we can lengthen this chain of subgroups from N down to $\langle e\rangle$. Therefore G is solvable.

11. As in the Hint, H_i is normal in H_{i-1} Define the homomorphism $\varphi : H_{i-1} \to G_{i-1}/G_i$ by $\varphi(x) = G_i x$. Then x lies in the kernel if and only if $x \in H_{i-1} \cap G_i = (H \cap G_{i-1}) \cap G_i = H \cap G_i = H_i$. By the First Isomorphism Theorem, $H_{i/1}/H_i$ is isomorphic to a subgroup of G_{i-1}/G_i which is abelian.

12. The splitting field has degree 2 so the Galois group has 2 elements.

13. Answered in the text.

14. By Corollary 11.5 the Galois group G is isomorphic to a subgroup of S_4. By Exercises 5 and 11 G is solvable.

15. The splitting field is $K = F(u, v)$. If $v \in F(u)$ then $K = F(u)$ is a quadratic extension and the group is $\mathbb{Z}_2$. Otherwise $[K : F] = 4$ and we can write out the automorphisms explicitly as in Example 2.A.

16. Let K be the splitting field of the given polynomial, and $G = Gal_F K$. K is not affected by linear factors of $f(x)$ since their roots lie in F. Therefore assume $f(x)$ has no linear factors.
    Cases: (1) $f(x)$ is an irreducible quadratic. Use Exercise 12.
    (2) $f(x)$ is an irreducible cubic. Use Exercise 13.
    (3) $f(x)$ is a product of 2 irreducible quadratics. Use Exercise 15.
    (4) $f(x)$ is an irreducible quartic. Use Exercise 14.

17. (a), (c), (e) Answered in the text.
    (b) $(x^2 - 2)(x^2 - 3)$ has splitting field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ with $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.
    (d) $(x^3 - 2)(x + 3)$ has splitting field $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ as in Example 3. By Exercise 13 the group is S_3.

18. (a) Solvable. $(x^3 + 1^2)$ factors with linear and quadratic factors.
    (b) Not solvable. It is irreducible by Eisenstein and has 3 real roots.
    (c) Not solvable. It is irreducible by Eisenstein and has 3 real roots.
    (d) Solvable since it factors into linear and quadratic factors.

19. (a) Every quadratic extension is normal.
    (b) $(\sqrt[4]{2}(1-i))^2 = -2\sqrt{2i}$ and a quadratic extension is normal.
    (c) It is certainly a radical extension and each step has degree 2.
    (d) Done in the Hint.
    (e) $x^4 + 8$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein, and has one root u in L but v is a root not in L. Therefore L is not normal over $\mathbb{Q}$.

20. $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$. That degree 4 factor is irreducible in $\mathbb{Q}[x]$, as in Exercise 4.5.20. If ζ is a root of that polynomial, then every power of ζ is also a root of $x^5 - 1$. Therefore the roots of that degree 4 factor are: $\zeta\ \zeta^2$, ζ^3, ζ^4 and $K = \mathbb{Q}\ (\zeta)$ is the splitting field. Let $G = Gal_{\mathbb{Q}}K$ so that $|G| = [K : \mathbb{Q}] = 4$. By Corollary 10.8 there exists $\alpha \in G$ with $a(\zeta) = \zeta^2$. Then $\alpha^2(\zeta) = \alpha(\zeta^2) = (\zeta^2)^2 = \zeta^4$ and $\alpha^3(\zeta) = \alpha(\zeta^4) = \zeta^8 = \zeta^3$. Therefore $G = \{\iota, \alpha, \alpha^2, \alpha^3\} \cong \mathbb{Z}_4$.

21. The roots of $x^5 + 32$ are $-2\zeta^k$ for $k = 0, 1, 2, 3, 4$, where ζ is given as in Exercise 20. The splitting field is again $K = \mathbb{Q}(\zeta)$.

22. $K = F(u)$ where $u^n = c$. Then $\alpha(u) = \zeta^k u$ for some k. This k is uniquely determined modulo n, because if $\zeta^k u = \zeta^m u$ then $\zeta^{k-m} = 1$ so that $n \mid (k-m)$ and $k \equiv m \pmod{n}$. Therefore $f : Gal_F K \to \mathbb{Z}_n$ is well defined. If $\sigma, \tau \in Gal_F K$ and $\sigma(u) = \zeta^k u$ and $\tau(u) = \zeta^j u$ then $\alpha\tau(u) = \alpha(\zeta^k u) = \zeta^k \alpha(u) = \zeta^{k+j} u$. Hence f is a homomorphism. Since an automorphism σ is determined by the value $\sigma(u)$ the map is injective. Therefore $Gal_F K$ is isomorphic to a subgroup of a cyclic group, so it is cyclic.

23. (Compare Exercise 7.9.34.) We may relabel to assume $(12) \in G$ and $\alpha \in G$ is a p-cycle. Since $\alpha(1)$, $\alpha^2(1)$, . . . runs through all of the p symbols, there exists k with $\alpha^k(1) = 2$. Since k and p are relatively prime, α^k is another p-cycle. Replacing α by α^k we may relabel the symbols 3, 4, . . . , p to assume $\alpha = (123 \cdots p)$. From Exercise 7.9.24 we know that $(m, m{+}1) = \alpha^{m-1}(12)\alpha^{-m+1} \in G$. As in Exercise 8 conclude that $(1k) \in G$ and finally show that every 2-cycle is in G. Therefore $G = S_n$.

24. The Galois group G is a subgroup of S_p by Corollary 11.5 and $|G| = [K : F]$ is a multiple of p. Cauchy's Theorem implies that G has an element of order p. The only elements of order p in S_p are p-cycles (since p is prime). Therefore G contains a p-cycle. The complex conjugation map induces an automorphism σ of the splitting field. Since there are exactly 2 nonreal roots this σ is a 2-cycle, when viewed as a permutation of the roots. Apply Exercise 23.

25. As in Exercise 24, if $f(x)$ is irreducible of degree 7 in $\mathbb{Q}[x]$ and has exactly 2 nonreal roots, then the Galois group is all of S_7. There are many ways of finding examples. One way is to consider $f(x) = (x-3)(x-2)(x-1)x(x+1)(x+2)(x+3) = x^7 - 14x^5 + 49x^3 - 36x$. Graphing this shows that there are the 7 given roots, and relative maxima and minima of approximately 95.84, -23.15, 12.36, -12.36, 23.15, -98.84.

Then adding a constant between 13 and 23 will yield a polynomial with exactly 5 real roots. The difficulty is to get irreducibility. One method is to add 14 and alter the x coefficient: $f_1(x) = x^7 - 14x^5 + 49x^3 - 35x + 14$.
Then this is irreducible by Eisenstein but must be analyzed again to ensure that there are still exactly 5 real roots.

The following general result provides another method.

Lemma. If F has characteristic p and $f(x) = x^p - x + a \in F[x]$ has no roots in F, then it is irreducible.

Proof. Suppose α is a root in an extension field. The set of roots is $\{\alpha, \alpha + 1, \alpha + 2, \ldots, \alpha + p - 1\}$. If $f(x)$ factors nontrivially in $F[x]$ then some proper subset forms the roots of a factor. In particular the sum of this subset is in F. This implies $\alpha \in F$.

Let $f_2(x) = x^7 - 14x^5 + 49x^3 - 35x + 15 \in \mathbb{Z}[x]$. Reducing (mod 7), show that $\overline{f}_2(x)$ is irreducible in $\mathbb{Z}_7[x]$ and deduce that $f_2(x)$ is irreducible in $\mathbb{Q}[x]$.

Chapter 13

Public-Key Cryptography

1. Answered in the text.

2. If $q \mid pk$ then Theorem 1.8 implies $q \mid p$ or $q \mid k$. But the first case cannot happen, for the only positive divisors of p are 1 and p, and neither of these equals q. Therefore $k = qm$ for some integer m so that $c = pqm$.

3. (a) Answered in the text.
   (b) 1392 1818 0008 0165 1595
   (c) 2131 0835 0064 1497 1933

4. If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$, by Lemma 12.2. Multiplying by a we obtain $a^p \equiv a \pmod{p}$. If $p \mid a$ then $a^p \equiv 0 \equiv a \pmod{p}$.

5. The decoding algorithm sends the code word C to the least residue of C^d (mod 2773) where d is a solution to $3d \equiv 1 \pmod{2668}$. (As in the Example we have $k = 46 \cdot 58 = 2668$.) Since $1 + 2 \cdot 2668 = 5337 = 3 \cdot 1779$ we see that $d = 1779$.

6. Suppose the gcd is $a = (C, n) \neq 1$. Then $1 \; a \leq C < n = pq$. Since the only positive divisors of $n = pq$ are 1, p, q and pq it follows that $a = p$ or q. Knowing one of the factors immediately yields the other one by dividing. Therefore, knowing a we also know p and q and hence we can find $k = (p - 1)(q - 1)$. Euclid's algorithm then provides the solution d to the congruence $ed \equiv 1 \pmod{k}$. Therefore the decoding algorithm $C \to C^d$ is known.

Chapter 14

The Chinese Remainder Theorem

14.1 Proof of the Chinese Remainder Theorem

1. By Theorem 2.2, $6v + 5 \equiv 6u + 5 \equiv 7 \pmod{n}$.

2. If u is a solution there exists some $r \in \{0, 1, 2, . . ., n - 1\}$ such that $u \equiv r \pmod{n}$. By Exercise 1 this r is also a solution.

3. Answered in the text.

4. Every integer u with $u \equiv 2 \pmod{5}$ is a solution.

5. If they are not relatively prime then the gcd is > 1 so it is divisible by some prime p (by Theorem 1.10). Then $p \mid m_{k+1}$ and $p \mid m_1m_2 \cdots m_k$. By Theorem 1.9 then $p \mid m_i$ for some $i \in \{1, 2, . . . , k\}$. But then $p \mid (m_i, m_k)$ contrary to the hypothesis.

6. See Exercise 1.2.17.

7. Since $(m_1, m_2) = 1$ Exercise 6 implies that $m_1m_2 \mid d$. Exercise 5 implies that $(m_1m_2, m_3) = 1$ so we can apply Exercise 6 again to conclude $m_1m_2m_3 \mid d$. Continue in this fashion until all the m_i are used. This proof could be made more formal by using induction on r.

8. $29 \pmod{66}$

9. $-30 \equiv 157 \pmod{187}$

10. $-7 \equiv 23 \pmod{30}$

11. $-18 \equiv 192 \pmod{210}$

12. $621 \pmod{4290}$

13. $204 \pmod{204204}$

14. If n is the number of coins, the conditions state that $n \equiv 3 \pmod{7}$, $n \equiv 10 \pmod{16}$, $n \equiv 4 \pmod{11}$ and $n \equiv 0 \pmod{7}$. The solution is $n \equiv 2842 \pmod{10944}$. Then the smallest positive solution is 2842 coins.

15. By Theorem 1.3 there exist integers u, v with $au + nv = d$. Therefore $au \equiv d \pmod{n}$. Given $b = dc$ for some integer c, deduce that $auc \equiv dc \equiv b \pmod{n}$ and $x = uc$ is a solution.

16. If x is a solution then $ax - b = ny$ for some integer y. Use $d \mid a$ and $d \mid n$ to show: $d \mid ax - ny = b$.

17. Since $as \equiv b \equiv at$ (mod n) we find that $a(s - t) \equiv 0$ (mod n) so that $n \mid a(s - t)$. Since $(a, n) = 1$, Theorem 1.5 implies that $n \mid (s - t)$ and $s \equiv t$ (mod n).

18. As in Exercise 17, $n \mid a(s - t)$ so that $a(s - t) = nx$ for some integer x. Let $a = da_1$ and $n = dn_1$. Then $(a_1, n_1) = 1$ (see Exercise 1.2.16) and $a_1(s - t) = n_1x$. Theorem 1.5 then implies that $n_l \mid (s - t)$. Conclude that $s \equiv t$ (mod n_1).

19. Solving the given system of congruences is equivalent to finding an integer t such that $mt \equiv (b - a)$ (mod n). For given such t define $x = a + mt$. By Exercise 15, this congruence has a solution t if and only if $d \mid (b - a)$. This occurs if and only if $a \equiv b$ (mod d).

20. Given $s \equiv a \equiv t$ (mod m) so that $m \mid (s - t)$ and $s \equiv b \equiv t$ (mod n) so that $n \mid (s - t)$. By the definition of the $1cm$ (see Exercise 1.2.31) it follows that $r \mid (s - t)$ so that $s \equiv t$ (mod r).

21. (a) The prime factors of N_i consist of the primes appearing in each of m_1, m_1; . . . ;m_{i-1}, $m_{i+1,}$ . . .; m_r. Since the m_i are pairwise relatively prime, m_i is not divisible by any of those primes. Thus $(N_i, m_i) = 1$. Then by Theorem 1.2, there are integers u_i and v_i such that $N_iu_i + m_iv_i = (N_i, m_i) = 1$.
(b) If $i \neq j$, then $m_j \mid N_i$ by definition of N_{i}, so that $Ni \equiv 0$ (mod m_j) and thus $N_iu_i \equiv 0$ (mod m_j).
(c) Since $N_iu_i + m_iv_i = 1$, we see that $N_iu_i - 1 = m_iv_i$, so that $N_iu_i \equiv 1$ (mod m_i).
(d) Modulo m_i we have

$$t \ (\text{mod}\, m_i) = (a_1N_1u_1 + a_2N_2u_2 + \cdots + a_rN_ru_r) \quad (\text{mod}\, mi)$$

$$\equiv a_1N_1u_1 \quad (\text{mod} \ \ mi) + a_2N_2u_2 \quad (\text{mod}\, m_i) + \cdots + a_rN_ru_r \quad (\text{mod}\, m_i).$$

By parts (b) and (c), the only summand that is nonzero is $a_iN_iu_i$ (mod m_i), and since $N_iu_i \equiv 1$ (mod m_i), we have $t \equiv a_iN_iu_i \equiv a_i$ (mod m_i). Thus t is a solution of the system.

14.2 Applications of the Chinese Remainder Theorem

1. A calculation left to the reader.

2. (a) $64 = 6{\cdot}10 + 4 \equiv 4$ (mod 12). Then $643 = 64{\cdot}10 + 3 \equiv 4{\cdot}10 + 3 \equiv 7$ (mod 12). Then $6439 = 643{\cdot}10 + 9 \equiv 7{\cdot}10 + 9 \equiv 7$ (mod 12). Finally $64397 = 6439{\cdot}10 + 7 \equiv 7{\cdot}10 + 7 \equiv 5$ (mod 12).

3. Answered in the text. The answer is $7 \cdot 8 \equiv 11$ (mod 15).

4. (a) If $f(r) = f(s)$ then $r \equiv s$ (mod 3), (mod 4) and (mod 5). That is, $r - s$ is a common multiple of 3, 4 and 5. By Exercise 13.1.7, $60 = 3 \cdot 4 \cdot 5$ divides $r - s$. But $-60 < r - s < 60$ so this divisibility forces $r - s = 0$ and $r = s$.
(b) Use $r = 0$ and $s = 60$ for example.

5. If $f(r) = f(s)$ then $m_i \mid (r - s)$ for each i and Exercise 13.1.7 implies that $M \mid (r - s)$. Since $-M < (r - s) < M$ it follows that $r = s$.

6. Choose $m_1 = 2^{35} - 1$, $m_2 = 2^{34} - 1$, $m_3 = 2^{33} - 1$, $m_4 = 2^{31} - 1$, $m_5 = 2^{29} - 1$ and $m_6 = 2^{23} - 1$. These are pairwise relatively prime by Exercise 7(c). With these choices, we can do arithmetic with integers as large as $M = m_1 m_2 \ldots m_6$. Note that $M = 2^{185} -$ (some 6 terms each $\leq 2^{162}$) + (other terms)…. Making some rough estimates of the sizes of the negative terms we find that $M > 2^{184}$.

7. (a) We have $a = bq + r$ where $0 \leq r < b$. Since $2^b \equiv 1 \pmod{2b - 1}$ we have $2^a - 1 = 2^{bq}2^r - 1 \equiv 2^r - 1 \pmod{2^b - 1}$. Since $0 \leq 2^r - 1 < 2^b - 1$ we know it is the least residue.

   (b) The Euclidean algorithm for (a, b) can be stated as:
   $a \equiv r_1 \pmod{b}$ and $0 \leq r_1 < b$.
   $b \equiv r_2 \pmod{r_1}$ and $0 \leq r_2 < r_1$.
   $r_2 \equiv r_3 \pmod{r_2}$ and $0 \leq r_3 < r_2$.
   The process continues, and $t = (a, b)$ is the last nonzero r_k. Now apply part (a) to see that:
   $2^a - 1 \equiv 2^{r_1} - 1 \pmod{2^b - 1}$.
   $2^b - 1 \equiv 2^{r_2} - 1 \pmod{2^{r_1} - 1}$.
   $2^{r_2} - 1 \equiv 2^{r_3} - 1 \pmod{2^{r_2} - 1}$.
   The process continues, and as in (a) we have a least residue at each step. Since $2^r - 1 = 0$ if and only if $r = 0$, the last nonzero term here is $2^{r_k} - 1 = 2^t - 1$. Therefore this is the gcd.

   (c) $(2^a - 1, 2^b - 1) = 1$ if and only if $2^{(a,b)} - 1 = 1$, by part (b). This occurs if and only if $(a, b) = 1$.

14.3 The Chinese Remainder Theorem for Rings

1. (a) Answered in the text.
   (b) Yes, both are $\cong \mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_7$.

2. $ab \in Ib \subseteq I$ and $ab \in aJ \subseteq J$.

3. Done in the hint.

4. The 2nd, 3rd, 4th and 6th rings are $\cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_7$. The 1st and 5th rings are $= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7$.

5. Following the Hint, $r = i_1t_2 + (i_1t_3 + i_3t_2 + i_3t_3) \in I_1 \cap I_2 + I_3$. We used Exercise 2 to see that i_1t_2 is in the intersection.

6. By Theorem 13.3 the first two congruences have a solution s. Furthermore $x \in R$ is a solution of those two if and only if $x \equiv s \pmod{I_1 \cap I_2}$. By Exercise 5 and Theorem 13.3 we can solve the system stated in the Hint.

CHAPTER 15

Geometric Constructions

1. Draw a circle with the center at the origin and radius r. Since r is constructible this is a constructible circle. It meets the x-axis at the points $(r, 0)$ and $(-r, 0)$. Therefore $-r$ is constructible.

2. Draw a circle with center $(a, 0)$ and radius $|b|$. This is a constructible circle since $(a, 0)$ is a constructible point and $|b|$ is the distance between the constructible points (0, 0) and (b, 0). This circle meets the x-axis at the points $(a + b, 0)$ and $(a - b, 0)$. Therefore $a + b$ and a $- b$ are constructible.

3. (a) Answered in the text.
   (b) Use the construction of perpendiculars to make a square. Draw a diagonal of the square and use the resulting 45° angle. More generally, any angle can be bisected using straightedge and compass.
   (c) Answered in the text.

4. If n is constructible then Exercise 2 implies that $n + 1$ and $n - 1$ are constructible. All integers can be constructed this way. (Use induction).

5. Answered in the text.

6. No for the first question: If $1/3 = \cos 3t = 4\cos^3 t - 3\cos t$ then cos t is a root of $12x^3 - 9x + 1$. The Rational Root Test implies that this polynomial has no root in $\mathbb{Q}$, and Theorem 15.9 applies. Yes for the second question: $11/16 = \cos 3t = 4\cos^3 t - 3\cos t$ shows that cos t is a root of $64x^3 - 48x - 11 = (4x + 1)(16x^2 - 4x - 11)$. Therefore cos t is a constructible number so that an angle of t degrees can be constructed.

7. No. Since $x^2y = 3$ and $2x^2 + 4xy = 7$ we find that $2x^3 - 7x + 12 = 0$. Apply the Rational Root Test and Theorem 15.9.

8. Construct a segment of length $\sqrt{3}$ as in Theorem 15.1, using a circle of radius 2. Add $\sqrt{3}$ and 1 by striking off a segment of length 1 adjacent to the segment of length $\sqrt{3}$.

9. If the base is $2x$ and the other two sides have length y then the height h satisfies $x^2 + h^2 = y^2$. The area is $xh = 1$ and the perimeter is $2x + 2y = 8$. Express y, h in terms of x to find that $4x^3 - 4x^2 + 1 = 0$. Apply the Rational Root Test and Theorem 15.9.

10. (a) If ABC is a given triangle and $A'B'$ is a segment equal in length to AB, then the triangle can be (constructibly) "copied" to yield a triangle $A'B'C'$ congruent to ABC. Then if two angles α and β are given, we can "copy" the angle β to yield an equal angle β' having one line in common with the angle α. Depending on which way it is constructed we get $\alpha + \beta$ and $\alpha - \alpha$. Alternatively, we could use Exercise 11 and note that the result follows from the formula for $\cos(\alpha + \beta)$.

    (b) By part (a) if 1° is constructible then so is 20°, contrary to the discussion on trisection in the text.

11. If an angle of t degrees is constructible, strike off a unit length along one of the sides of the angle, and drop a perpendicular to the other side. The segment cut off on that side has length $\cos t$. Conversely, if $\cos t$ is constructible, strike off that length along a radius of a unit circle from the center O to a point P. Construct the perpendicular to OP at P and let Q be one of the points where it meets the circle. Then the (constructible) angle POQ measures t degrees.

12. If r is constructible then the point $(r, 0)$ can be constructed by straightedge and compass starting with the origin and the point $(1, 0)$. The segment from $(0, 0)$ to $(r, 0)$ has length $|r|$. Conversely if a segment of that length is constructible, use the given unit length to define the measurement along an axis, set up a coordinate system and construct the point $(r, 0)$. Therefore r is a constructible number.

13. By Exercise 1, a number d is constructible if and only if $|d|$ is a constructible (positive) number. Then the question reduces immediately to the positive case (which is done in the proof of Theorem 15.1).

14. The set C of constructible numbers is a subset of $\mathbb{R}$, it is closed under addition and multiplication and contains inverses of its nonzero elements, by Theorem 15.1. Hence C is a subfield of $\mathbb{R}$.

15. Closure under addition and multiplication follow by simply collecting terms. The inverses are given in the answers in the text. Hence it is a subfield.

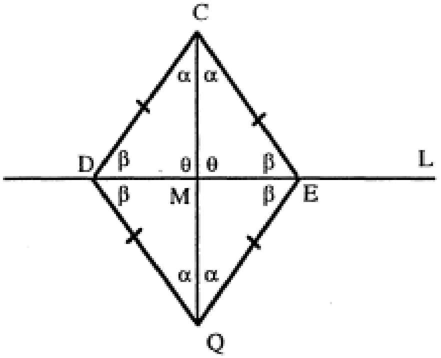
16. Define a subfield F of $\mathbb{R}$ to be called "constructible" if $F \subseteq C$, the field of all constructible numbers (see Exercise 14).

    Claim. If F is a constructible field and c is a positive element of F, then $\mathrm{F}(\sqrt{\mathrm{c}})$ is also a constructible field.

    Proof. By Theorem 15.1, $\sqrt{\mathrm{c}}$ is constructible. Then F and $\sqrt{\mathrm{c}}$ are in C so the field they generate is also inside C.

Suppose $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n \subseteq \mathbb{R}$ is a chain of fields, where $F_{i+1} = F_i\left(\sqrt{c_i}\right)$ for some $c_i \in F_i$, for each $i = 0, 1, \ldots, n - 1$. The Claim implies that every element $r \in F_n$ is a constructible number.

17. Following the Hint, let M be the intersection point of the lines L and CQ. By the construction, $CD = CE = QD = QE$. Therefore $\alpha = \angle DCQ = \angle DQC$, and $\beta = \angle CDE = \angle CED$. Examining sides yields congruent triangles $\Delta CDE \cong \Delta QDE$ and $\Delta CDQ \cong \Delta CEQ$. Then s.a.s implies that $\Delta DMC \cong \Delta EMC$ so that $\theta = \angle DMC = \angle EMC$. Since these angles are supplements it follows that θ is a right angle and CQ is perpendicular to the line L.



18. Since the x-axis is constructible and (r, s) is constructible, Exercise 17 implies that the vertical line through (r, s) is constructible. This line and the x-axis meet at the point $(r, 0)$. Therefore $(r, 0)$ is constructible so that r is a constructible number, Similarly $(0, s)$ is a constructible point, and it is easy to use it to construct $(s, 0)$ and conclude that s is a constructible number.

19. Done in the Hint.

20. Let A and B be the given constructible points and draw the circle with center A and radius AB and the circle with center B and radius AB. Let P, Q be the points where these two circles intersect. The line PQ then meets the segment AB at the midpoint M. All the points and lines mentioned here are constructible. The proof that M is the midpoint is done as in Exercise 17.

21. Set up the coordinate system using the given radius as the unit length 1. Then the area of the given circle (in these units) is π. If a square of side s units has the same area then $s^2 = \pi$ so that $s = \sqrt{\pi}$. Then such a square is constructible if and only if $\sqrt{\pi}$ is a constructible number. By Theorem 15.1 this is equivalent to saying that π is constructible. If this occurs then Theorem 15.6 says that π lies in some quadratic extension chain, $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n$. Using ideas from Section 10.1 deduce that $[F_{i+1} : F_i] = 2$ whenever $0 \le i < n$, so that Theorem 10.4 implies that $[F_n : \mathbb{Q}] = 2^n$.

However the assumption that π is not the root of any polynomial in $\mathbb{Q}[x]$ implies that the set $\{1, \pi, \pi^2, \pi^3, \ldots\}$ is a linearly independent set. Proof. If not then there is a linear dependence relation $c_0 \cdot 1 + c_2\pi^2 + \ldots + c_k\pi^k = 0$ for some integer k and some coefficients $c_i \in \mathbb{Q}$, not all equal to zero. But this says that $f(\pi) = 0$ where $f(x) = c_0 + c_1x + c_2x^2 + \ldots + c_kx^k \in \mathbb{Q}[x]$, contrary to assumption.

Since $\pi \in F_n$, this independence implies that $[F_n : \mathbb{Q}]$ is infinite, contrary to the bound obtained above.

CHAPTER 16

Algebraic Coding Theory

16.1 Linear Codes

1. Answered in the text.

2. (a) 4 (b) 6 (c) 1 (d) 8

3. (a) 1 (b) 5 (c) 4 (d) 1

4. (a) 0111 (b) 1101
   (c) at least one error was made, but there is not a unique closest codeword (1011010 and 1010101 are closest codewords).
   (d) 0010

5. (a), (c) Answered in the text.
   (b) 00000, 01010, 10111, 11101
   (d) 000000, 001110, 101010, 011011, 100111, 101001, 110010, 111100

6. (a) detects 0, corrects 0 (b) detects 1, corrects 0
   (c) detects 0, corrects (d) detects 2, corrects 1

7. For any message word abcde $\in B(5)$, the corresponding codeword is $(abcde)G = abcdef$ where f is the sum $a + b + c + d + e$ in $\mathbb{Z}_2$. This is exactly the way the (6, 5) parity-check code was defined.

8. Any message word $ab \in B(2)$, the corresponding codeword is $(ab)G = ababababab$. This is exactly the way the (10, 2) repetition code is defined.

9. The message word $a \in B(1)$ has corresponding codeword $(a)G = aaaa$.

10. The set does have order 2^n and it is certainly closed under the operation. The zero element is 00…0 and every element is its own inverse: $a + a = 0$. The associative and commutative laws are easily checked componentwise.

11. (a) $d(u, v)$ = number of coordinates in which u and v differ. The same coordinates occur for v and u.
    (b) f two words differ in zero coordinates, they are equal.
    (c) Answered in the text.

12. Given six elements of $\mathbb{Z}_2$. The sum of the 6 elements is zero if and only if the last element is the sum of the first 5 elements.

13. C $= \{abcdef \in B(6) \mid a + b + c + d + e + f = 0\}$. It is easy to check that this set is closed under addition, and hence is a subgroup.

14–15. By the definition of "corrects t errors", any possible received message is of Hamming distance $\leq t$ from a unique codeword. Suppose there are two codewords u, v with $d(u, v) = k \leq 2t$. Then there is a "path" of words $u = u_0, u_1, \ldots, u_k = v$ where $d(u_i, u_{i+1}) = 1$ for every $i = 0, 1, \ldots, k - 1$. If $k < t$ then the message word u is distance 0 from the codeword u and distance $k < t$ from the codeword v, contrary to the uniqueness hypothesis. If $t \leq k \leq 2t$ then the message word u_t is distance t from the codeword u and distance $k - t \leq t$ from the codeword v, again contrary to the uniqueness. Therefore $d(u, v) \leq 2t$ is impossible.

16. Suppose there are codewords u, v with $d(u, v) = r \leq t$. If the codeword u is sent, possibly exactly r errors could occur to yield the received word v. The receiver would believe that v was the correct codeword, and those r errors would go undetected. Then the code would not be detecting t errors.

17. Answered in the text.

18. Such a code is a subgroup of 8 elements in the group $B(6)$. Theorem 16.2 implies that the Hamming distance between any 2 codewords is ≥ 5. In particular, every nonzero codeword has Hamming weight ≥ 5, so the codewords are in the set: {111111, 111110, 111101, 111011, 110111, 101111, 011111}. Since any two elements in this set have Hamming distance ≤ 2, such a code cannot exist.

19. Many correct answers, including: 0000000, 1111000, 0011110, 1100110, 1010101, 0101101, 1001011, 0110011.

20. Yes. For example: 000000, 111100, 001111, 110011.

21. We need $2^k \geq 3$ codewords, so that $k \geq 2$, and we need the minimum Hamming weight ≥ 3. This can be achieved in a (5, 2) code.

22. (a) Just multiply uG.
    (b) If v is a codeword then those relations follow from the expression in (a). Conversely if v satisfies those conditions, we can replace v_5, v_6, v_7 in terms of $v_1 \ldots, v_4$ and write out the word v. It comes out to be exactly the expression in (a), with v replacing u. Then, v is the codeword corresponding to the message word $v_1v_2v_3v_4$.

23. Since the first k columns of G form the identity matrix I_k, the first k entries of uG are $uI_k = u$.

24. Claim. The mapping $f: B(n) \rightarrow \mathbb{Z}_2$ with $f(u) = [Wt(u)]_2$ is a homomorphism.

    Proof. In fact, if $u = u_1u_2 \ldots u_n$ then $f(u) = u_1 + u_2 + \ldots + u_n$, the sum in $\mathbb{Z}_2$. From this it is clear that $f(u + v) = f(u) + f(v)$. Another way to state this observation is: $Wt(u + v) \cong Wt(u) + Wt(v) \pmod 2$.

Let C_0 be the subset of C consisting of all codewords of even weight. Since C_0 is exactly the kernel of f, it is a subgroup. If $C_0 \neq C$ let $w \in C$ with $w \notin C_0$. Then the only cosets are C_0 and $w + C_0$, so that C_0 contains exactly half of the elements of C. Stated more simply, if there is a codeword w of odd weight then $w + C_0$ is the set of all codewords of odd weight, and this set has the same size as C_0.

25. By Exercise 24 there are 2^{n-1} elements of $B(n)$ with even weight. They form a subgroup so we have an $(n, n-1)$ code.

26. Im f is a code since it is a subgroup. Im f is an (n, j) code if Im f contains 2^j elements. If f is not injective then Im f has fewer than 2^k elements so it is not an (n, k) code.

27. (a), (c), (e) Answered in the text.

    (b) .03881196 (d) .00000001 (f) .00000397 Here is an explanation of the calculation in calculation of (c): consider a message $abcd$ where a, b are transmitted correctly (probability $(.99)^2$) and c, d are transmitted erroneously (probability $(.01)^2$). The probability of this event is $(.99)^2\,(.01)^2 = .00009801$. This event is one way of making exactly 2 errors. The errors could have occurred elsewhere, perhaps in b and d, or in a and b,... There are altogether 6 ways of choosing 2 places out of 4 coordinates, so the probability of exactly 2 errors is: $(.00009801\,).6 = .00058806$

28.

no errors:	.9509900499	1 error:	.0480298005
2 errors:	.000970299	3 errors:	.000009801
4 errors:	.0000000495	5 errors:	.0000000001

29. A received digit of 0 was probably (with probability $> 50\%$) transmitted as a 1, and a received digit 1 was probably transmitted as a 0.

30. (a) $(.99)^{500} = .006570483$

    (b) Sending a single digit as aaa leads to an incorrect decoding provided there are 2 or 3 errors in this 3 digit transmitted word. The probability of that event is $(.99)(.01)^2.3+(.01)^3 = .000298$. Then the probability of a correct decoding of a 500 digit message is $(.999702)^{500} = .86155003$.

31. (a) The k errors could occur at any k of the n coordinates. There are exactly $\binom{n}{k}$ ways of choosing a k-element subset from an n-element set.

    (b) Suppose the first k digits contain errors and the last n - k digits are correct. Assuming that multiple errors occur independently, the probability of that event is $p^k q^{n-k}$. The k errors could occur at any of the $\binom{n}{k}$ k-element subsets of the n coordinates, and the formula follows.

16.2 Decoding Techniques

1. (a), (c) Answered in the text.

   (b) $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

   (d) $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

2. $\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

3. Answered in the text.

4. It is a 10 × 8 matrix with top two rows = $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$, and with an 8 × 8 identity matrix as the last 8 rows.

5. Answered in the text.

6. By Corollary 16.4 a code which can correct every single error must have every nonzero codeword of weight ≥3. For the given code, $x_1x_2\cdots x_6$ is a codeword if and only if $x_1+x_3+x_5 = 0$ and $x_2+x_4+x_6 = 0$. For example 101000 is a codeword of weight 2.

7.

0000	0101	1011	1110	Codewords
1000	1101	0011	0110	
0100	0001	1111	1010	Received words
0010	0111	1001	1100	

The parity check matrix is $H = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}$ and the syndrome of w is wH.

Syndrome	00	11	10	01
Coset leader	0000	1000	0100	0010

8.

000000	001110	010101	011011	100011	101101	110110	111000
100000	101110	110101	111011	000011	001101	010110	011000
010000	011110	000101	001011	110011	111101	100110	101000
001000	000110	011101	010011	101011	100101	111110	110000
000100	001010	010001	011111	100111	101001	110010	111100
000010	001100	010111	011001	100001	101111	110100	111010
000001	001111	010100	011010	100010	101100	110111	111001
100100	101010	110001	111111	000111	001001	010010	011100

Here is a chart of the syndromes and the coset leaders:

000	011	101	110	100	010	001	111
000000	100000	010000	001000	000100	000010	000001	100100

9. The cosets are listed as the rows of the standard array. Any element of the row could be chosen as the "leader". For example, in every row after the first we can choose the second entry as the new leader, and recompute the rows. In the new array, the rows of the old array have been permuted.

00000	10110	01101	11011
00110	10000	01011	11101
11110	01000	10011	00101
10010	00100	11111	01001
10100	00010	11001	01111
10111	00001	11010	01100
Oino	11000	00011	10101
00111	10001	01010	11100

10. If v is the column vector with entries $c_1, \ldots, c_n$ then $e_iv = 0\cdot c_1 + \cdot\cdot + 1\cdot c_i + \cdot\cdot + 0\cdot c_n = c_i$. If $H = (a_{ij})$ is an $n \times k$ matrix, the j^{th} entry of the row e_iH is the product of the row e_i and the j^{th} column of H. By the comment above, that entry is a_{ij}. Therefore $e_iH = (a_{i1}, a_{i2}, \ldots, a_{ik})$ which is the i^{th} row of H.

11. The method will decode w as the codeword u' which is in the top of the column in which w appears. If w appears in the row with coset leader e, then the construction of the array implies that $w = e + u'$, so that $u' = w - e$. Then w is decoded as u if and only if $w - e = u$. This occurs exactly when $w - u = e$ is a coset leader.

12. Suppose a codeword u is transmitted and w is received. If at most t errors occurred then $e = w - u$ has $Wt(e) \le t$. By hypothesis this word e is a coset leader, and Exercise 11 implies that w is correctly decoded to be u.

13. Answered in the text.

14. Answered in the Hint, after a direct matrix calculation.

15. C corrects single errors if and only if every nonzero $u \in C$ has $Wt(u) \ge 3$, by Corollary 16.4. Equivalently, if $u \ne 0$ and $Wt(u) \le 2$ then $u \notin C$. By Theorem 16.9 this can be restated as: if $Wt(u) = 1$ or 2 then $uH \ne 0$. Let $r_1, \ldots, r_n$ be the n rows of H. If $Wt(u) = 1$ then $u = e_i$ for some i and Exercise 10 implies that $uh = r_i$. If $Wt(u) = 2$ then $u = e_i + e_j$ for some indices $i \ne j$. Then $uH = r_i + r_j$. Therefore C corrects single errors if and only if $r_i \ne 0$ and $r_i \ne r_j$ for every choice of unequal indices i, j. Equivalently, the rows of H are nonzero and distinct.

16. In the list of codewords in the Example after Corollary 16.4, we see that 0000000 and 0010110 are codewords. If 0000000 was sent and three errors occurred, possibly 0010110 is received and that is decoded as the codeword 0010110 with no errors made in transmission. The 3 errors went undetected.

17. By definition the parity check matrix of any Hamming code are distinct and nonzero. By Exercise 15 the code can correct single errors. Therefore every nonzero codeword has weight ≥ 3, by Corollary 16.4.

18. (a) $(.99)^5 = .95099$
    (b) Raise to the 100^{th} power: $(.99)^{500} \ge .00657048$
    (c) $(.99)^4(.01)\cdot 5 = .0480298$. From the formula see Exercise 16.1.31.
    (d) 0 or 1 errors, add the quantities in (a) and (c): probability $\ge .9990198$
    (e) Probability $\ge (.9990198)^{100} \ge .9065$.

16.3 BCH Codes

1. (a) Answered in the text.
   (b) If $u = [f(x)]$ then $u + u = [f(x) + f(x)] = [0]$.

2. The polynomials of degree 2 are: x^2, $x^2 + 1 = (x+1)^2$, $x^2 + x = x(x+1)$ and $x^2 + x + 1$. Since the last one has no root it is irreducible.

3. Answered in the text.

4. $1+\alpha^5 + (\alpha^5)^2 = 1 + (\alpha + \alpha^2) + (1+\alpha+ \alpha^2) = 0$. Then α^5 is a root of the irreducible polynomial $1 + x + x^2$.

5. (a) Answered in the text. Since $(1+x+x^2)^2 = 1+x^2+x^4$ is not equal to the given polynomial, and since 0 and 1 are not roots, that polynomial is irreducible.

   (b) By the argument in the text, $m_1(\alpha^4) = 1 + (\alpha^4) + (\alpha^4)^4 = (1 + \alpha + \alpha^4)^4 = 0$ by the Freshman's Dream (Lemma 10.24). Of course this equality can also be verified easily using the table of powers of α.

6. Let $f(x) = c_0 + c_1x +\cdots+ c_nx^n$ where $c_i \in \mathbb{Z}_2$. Note that $(u + v)^2 = u^2 + v^2$ in that field, and $c_i^2 = c_i$ (since $c_i = 0$ or 1). Therefore for any u in an extension field: $f(u^2) = \sum c_i(u^2)^i = \sum(c_iu^i)^2 = f(u)^2$. Apply this to $u = \alpha^k$.

7. (a) From the formula we see that any element $(a_0, a_1, \ldots , a_{n\text{-}1})$ in $B(n)$ does equal $f([h(x)])$ for $h(x) = a_0 + a_1x +\cdots+ a_{n\text{-}1}x^{n\text{-}1}$.

   (b) This is clear since addition of polynomials and addition of elements of $B(n)$ are both performed "componentwise".

   (c) Answered in the text.

8. (a) Following the Hint, since $p(x)|q(x)h(x)$ and $p(x) \nmid q(x)$ (since they are distinct irreducibles), Theorem 4.11 implies $p(x)|h(x)$. Then $h(x) = p(x)g(x)$ for some $g(x)$, so that $f(x) = p(x)q(x)g(x)$.

   (b) Use induction of k. The case $k = 2$ is done in (a). Suppose the result is true for k and $m_1(x)$, . . . , $m_{k+1}(x)$ divide $f(x)$. By the induction hypothesis, $f(x) = m_1(x) \cdots m_k(x)q(x)$ for some polynomial $q(x)$. Since $m_{k+1}(x)$ divides this product, and $m_{k+1}(x)$ does not divide any of the $m_i(x)$ in the product, Corollary 4.12 implies $m_{k+1}(x) \mid q(x)$. The result follows.

9. (a), (c) Answered in the text.

   (b) $D(x) = x^2 + \alpha^6x + \alpha^7$ has roots α^8 and α^{14}. Therefore errors occurred in the coefficients of x^8 and x^{14}, so the corrected word is $c(x) = 1 + x^3 + x^4 + x^5 + x^8 + x^{14} = 100111001000001$.

   (d) $D(x) = x^2 + \alpha^{14}x + \alpha^{13}$ has roots α^4 and α^9. Therefore errors occurred in the coefficients of x^4 and x^9, so the corrected word is $c(x) = 1 + x^4 + x^6 + x^7 + x^8 = 100010111000000$.

10. The field K is the same as in the Example. Let $m_i(x)$ be the minimal polynomial for $\ ^i$. Then $m_1(x) = 1 + x + x^4$. By Exercise 6, $m_1(x) = m_2(x) = m_4(x)$ and $m_3(x) = m_6(x)$. The polynomials $m_3(x)$ and $m_5(x)$ are calculated in Exercise 5, and $g(x) = m_1(x)m_3(x)m_5(x)$. Multiplying this out gives the stated value.

11. The nonzero elements of K form a group of order $n = 2^r - 1$ with generator α. Therefore $\alpha^n = 1$ so that every α^i is a root of x^n - 1. By Theorem 10.6, each minimal polynomial $m_i(x)$ divides $x^n - 1$.

12. $g(x)$ is a product of distinct minimal polynomials $m_i(x)$ and $m_i(x)$ divides $x^n - 1$, as in Exercise 11. By Exercise 8 we conclude $g(x)$ divides $x^n - 1$.

13. Done in the Hint, using the fact that $g(x)|(x^n - 1)$ (see Exercise 12).

14. (a) Let x^n - $1 = g(x)f(x)$ so that deg $f(x) = n - m = k$. A typical element of C is $[h(x)g(x)]$ for some polynomial $h(x)$. Divide h by f to obtain: $h(x) = f(x)q(x) + s(x)$ for some $q(x)$, $s(x)$ where either $s(x) = 0$ or deg $s(x) < k$. This condition says exactly that $s(x)$ ε J. Multiplying by $g(x)$, conclude that $h(x)g(x) = (x^n - 1)q(x) + s(x)g(x)$ and $[h(x)g(x)] = [s(x)g(x)]$.

    (b) Claim. $\varphi : J \to C$ defined $\varphi\ (s(x)) = [s(x)g(x)]$ is bijective.

    Proof. φ is surjective, by part (a). It is easy to check that φ is a homomorphism of additive groups. If $s(x)$ is in the kernel then $[s(x)g(x)] = [0]$ so that $s(x)g(x) = (x^n - 1)Q(x)$ for some $Q(x)$. Cancel $g(x)$ to deduce that $s(x) = f(x)Q(x)$. Since deg $f(x) = k$ and $s(x)$ ε J this implies $s(x) = 0$. Hence φ is injective.

    Therefore $|C| = |J| = 2^k$ and C is an (n, k) code.

15. (a) The received word $r(x)$ and the codeword $c(x)$ differ at exactly the two places x^i and x^j.

    (b) By definition of $g(x)$ we have $g(\alpha^k) = 0$ for $k = 1, 2, 3, 4$. Since $c(x)$ is a codeword it is a multiple of $g(x)$ and the claim follows from (a).

    (c) Multiplying out D(x) yields the first formula. By (b) we know that $a^i + a^j = r(\alpha)$.

    (d) $r(a)^3 = (\alpha^i + \alpha^j)^3 = \alpha^{3i} + \alpha^{3j} + \alpha^{i+j}(\alpha^i + \alpha^j) = r(\alpha^3) + \alpha^{i+j}\mathrm{r}(\alpha)$. Therefore $\alpha^{i+j} = r(\alpha)^2 + r(\alpha^3)/r(\alpha)$. By the Freshman's Dream 10.24, $r(\alpha)^2 = r(\alpha^2)$.

16. A (7, 4) Hamming code is one whose parity check matrix H is a 7×3 matrix whose rows are the 7 distinct nonzero elements of $B(3)$. The BCH code constructed with $t = 1$ and $r = 3$ has $n = 2^r$-$1 = 7$ and field K of $2^r = 8$ elements. For example $K = \mathbb{Z}_2[x]/(x^3 + x + 1)$ has generator $\alpha = [x]$ with minimal polynomial $m_1(x) = x^3 + x + 1$. As before the minimal polynomial for α^2 is also $m_1(x)$, so that $g(x) = x^3 + x + 1$. Then $m =$ deg $g(x) = 3$ and $k = n - m = 4$. Therefore we have a (7, 4) BCH code. By the theory of BCH codes this one corrects single errors. Then by Exercise 16.2.15, the parity check matrix H must have rows which are distinct and nonzero. However, this H is a 7×3 matrix so that all 7 of the nonzero elements of $B(3)$ must occur as rows of H, and we have a Hamming code.

    We can identify H more explicitly. Recall that $[a(x)] \in \mathbb{Z}_2[x]/(x^7 - 1)$ is a codeword when $g(x) \mid \mathrm{a}(x)$. Factor $x^7 - 1 = g(x)f(x)$ and compute that $f(x) = x^4 + x^2 + x + 1$. Then $[\mathrm{a}(x)]$ is a codeword if and only if $x^7 - 1$ divides $\mathrm{a}(x)f(x)$, which says that $[\mathrm{a}(x)]\cdot[f(x)] = [0]$. This gives a "parity check" criterion for codewords. To change this criterion into a matrix condition, consider multiplication by $f(x)$, $xf(x)$, $x^2f(x)$, . . . But $x^3f(x)$ can be expressed in terms of the earlier terms (mod $x^7 - 1$). Then the parity check matrix H has columns $f(x)$, $xf(x)$, $x^2f(x)$. (View them as columns since we want to multiply them by rows). Writing out these columns

$$\text{yields H} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{This does correspond to a (7, 4) Hamming code.}$$