

# 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

© 2013 Brooks/Cole, Cengage Learning

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

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

For permission to use material from this text or product, submit  
all requests online at [www.cengage.com/permissions](http://www.cengage.com/permissions)  
Further permissions questions can be emailed to  
[permissionrequest@cengage.com](mailto: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](http://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](http://www.cengage.com/brookscole)

Purchase any of our products at your local college  
store or at our preferred online store  
[www.cengagebrain.com](http://www.cengagebrain.com)

**NOTE: UNDER NO CIRCUMSTANCES MAY THIS MATERIAL OR ANY PORTION THEREOF BE SOLD, LICENSED, AUCTIONED, OR OTHERWISE REDISTRIBUTED EXCEPT AS MAY BE PERMITTED BY THE LICENSE TERMS HEREIN.**

#### 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

Download full file from [answersun.com](http://answersun.com)

# C O N T E N T S

<b>Chapter 1</b>	Arithmetic in $\mathbb{Z}$ Revisited .....	<b>1</b>
<b>Chapter 2</b>	Congruence in $\mathbb{Z}$ and Modular Arithmetic.....	<b>11</b>
<b>Chapter 3</b>	Rings .....	<b>19</b>
<b>Chapter 4</b>	Arithmetic in $F[x]$ .....	<b>45</b>
<b>Chapter 5</b>	Congruence in $F[x]$ and Congruence-Class Arithmetic.....	<b>63</b>
<b>Chapter 6</b>	Ideals and Quotient Rings.....	<b>69</b>
<b>Chapter 7</b>	Groups.....	<b>83</b>
<b>Chapter 8</b>	Normal Subgroups and Quotient Groups.....	<b>113</b>
<b>Chapter 9</b>	Topics in Group Theory.....	<b>133</b>
<b>Chapter 10</b>	Arithmetic in Integral Domains .....	<b>147</b>
<b>Chapter 11</b>	Field Extensions.....	<b>159</b>
<b>Chapter 12</b>	Galois Theory .....	<b>171</b>
<b>Chapter 13</b>	Public-Key Cryptography .....	<b>179</b>
<b>Chapter 14</b>	The Chinese Remainder Theorem .....	<b>181</b>
<b>Chapter 15</b>	Geometric Constructions .....	<b>185</b>
<b>Chapter 16</b>	Algebraic Coding Theory .....	<b>189</b>

Not For Sale

# 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  $0 \leq r < b$ . Multiplying this equation through by  $c$  gives  $ac = (bc)q + rc$ . Further, since  $0 \leq r < b$ , it follows that  $0 \leq rc < bc$ . 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  $0 \leq r < b$ , it follows (since  $c \geq 1$ ) that  $0 \leq r < bc$ . Thus  $a = (bc)k + r$  is the unique representation with  $0 \leq r < bc$ , 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  $0 \leq r < n$  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  $r \geq r'$  (the other case is similar). The given inequalities imply that  $0 \leq (r - r') < n$  and it follows that  $0 \leq (k - q + q') < 1$  and we conclude that  $k - q + q' = 0$ . Therefore  $r - r' = 0$ , so that  $r = r'$  as claimed.

## 1.3 Primes and Unique Factorization

1. (a)  $2^4 \cdot 3^2 \cdot 5 \cdot 7$ . (c)  $2 \cdot 5 \cdot 4567$ .  
(b)  $-5 \cdot 7 \cdot 67$ . (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  $2^j 3^k$  for  $0 \leq j \leq s$  and  $0 \leq k \leq t$ .  
(b) The number of divisors equals  $(r+1)(s+1)(t+1)$ .
6. The possible remainders on dividing a number by 10 are  $0, 1, 2, \dots, 9$ . 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,  
$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \dots + x + 1).$$
  
(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  $\pm 1$  or  $\pm p$  then  $r = p/s$  would equal  $\pm p$  or  $\pm 1$ , 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  $\pm 1$  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  $-p$ .

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  $f(x) \cdot c = a_0c + a_1cx + \cdots + a_ncx^n$ . 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  $a_0b_0 + \cdots + a_nb_mx^{n+m} = 0_R$ . In particular,  $a_nb_m = 0_R$  and  $b_m \neq 0_R$ . 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  $a^3 = 0_R$ .

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  $\tau: R \rightarrow R$  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  $\pi$  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  $\rho: K \rightarrow S$  defined by  $\rho(0_R, s) = s$  shows that  $K \cong S$ .
9. (a) For subtraction: 
$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} - \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} a - a' & 0 \\ b - b' & c - c' \end{pmatrix}. \quad \text{For multiplication:}$$
$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \begin{pmatrix} a' & 0 \\ b' & c' \end{pmatrix} = \begin{pmatrix} aa' & 0 \\ ba' + cb' & cc' \end{pmatrix}. \quad \text{Therefore } R \text{ is a subring of } M(\mathbb{Z}) \text{ and } R \text{ contains the identity matrix.}$$
  
(b) The map  $f$  is surjective since for every  $a \in \mathbb{Z}$ :  $f\left(\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}\right) = a$ . 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  $\varphi: \mathbb{R} \rightarrow \mathbb{C}$  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.



Not For Sale

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,  $g \in \bigcap C(a)$ .
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  $[a]^{p-1} \equiv [1] \pmod{p}$  and consequently  $a^p \equiv a \pmod{p}$ . If  $(a, p) > 1$  then  $p \mid a$  and  $a \equiv 0 \pmod{p}$ . In this case it is clear that  $a^p \equiv a \pmod{p}$ .
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 “ $a \equiv 1 \pmod{k}$ ” 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  $r \equiv 1 \pmod{k}$  does it follow that  $s \equiv 1 \pmod{k}$ ? Yes, because  $[r] = [s]$  so that  $r \equiv s \pmod{n}$  and  $n \mid (r - s)$ . Now since  $k \mid n$  conclude that  $k \mid (r - s)$  and  $r \equiv s$

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 than 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.

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  $s(x) \in J$ . 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.  $\varphi : J \rightarrow C$  defined  $\varphi(s(x)) = [s(x)g(x)]$  is bijective.

Proof.  $\varphi$  is surjective, by part (a). It is easy to check that  $\varphi$  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  $s(x) \in J$  this implies  $s(x) = 0$ . Hence  $\varphi$  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)  $r(\alpha)^3 = (\alpha^i + \alpha^j)^3 = \alpha^{3i} + \alpha^{3j} + \alpha^{i+j}(\alpha^i + \alpha^j) = r(\alpha^3) + \alpha^{i+j}r(\alpha)$ . 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  $7 \times 3$  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  $\alpha^2$  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  $7 \times 3$  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  $g(x) \mid a(x)$ . Factor  $x^7 - 1 = g(x)f(x)$  and compute that  $f(x) = x^4 + x^2 + x + 1$ . Then  $[a(x)]$  is a codeword if and only if  $x^7 - 1$  divides  $a(x)f(x)$ , which says that  $[a(x)] \cdot [f(x)] = [0]$ . This gives a "parity check" criterion for codewords. To change this criterion into a matrix condition, consider multiplication by  $f(x)$ ,  $xf(x)$ ,  $x^2f(x)$ ,  $\dots$ . 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

$$\text{yields } H = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{This does correspond to a } (7, 4) \text{ Hamming code.}$$