Solutions Manual to Accompany

Introduction to ABSTRACT ALGEBRA

Fourth Edition

W. KEITH NICHOLSON

WILEY

Solutions Manual to Accompany Introduction to Abstract Algebra

Solutions Manual to Accompany Introduction to Abstract Algebra

Fourth Edition

W. Keith Nicholson
University of Calgary
Calgary, Alberta, Canada

WILEY
A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey
Published simultaneously in Canada

Library of Congress Cataloging-in-Publication Data:

Nicholson, W. Keith.
Introduction to abstract algebra / W. Keith Nicholson. – 4th ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-1-118-28815-3 (cloth)
1. Algebra, Abstract. I. Title.
QA162.N53 2012
512'.02–dc23 2011031416

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Contents

Chapter 0

Preliminaries

0.1 PROOFS

1. (a) (1) If $n = 2k$, k an integer, then $n^2 = (2k)^2 = 4k^2$ is a multiple of 4.

   (2) The converse is true: If n^2 is a multiple of 4 then n must be even because n^2 is odd when n is odd (Example 1).

   (c) (1) Verify: $2^3 - 6 \cdot 2^2 + 11 \cdot 2 - 6 = 0$ and $3^3 - 6 \cdot 3^2 + 11 \cdot 3 - 6 = 0$.

   (2) The converse is false: $x = 1$ is a counterexample. because

   $$1^3 - 6\,1^2 + 11 \cdot 1 - 6 \neq 0.$$

2. (a) Either $n = 2k$ or $n = 2k + 1$, for some integer k. In the first case $n^2 = 4k^2$; in the second $n^2 = 4(k^2 + k) + 1$.

   (c) If $n = 3k$, then $n^3 - n = 3(9k^3 - k)$; if $n = 3k + 1$, then

   $$n^3 - n = 3(9k^3 + 9k^2 + 2k);$$

   if $n = 3k + 2$, then $n^3 - n = 3(9k^3 + 18k^2 + 11k + 2)$.

3. (a) (1) If n is not odd, then $n = 2k$, k an integer, $k \geq 1$, so n is not a prime.

   (2) The converse is false: $n = 9$ is a counterexample; it is odd but is not a prime.

   (c) (1) If $\sqrt{a} > \sqrt{b}$ then $(\sqrt{a})^2 > (\sqrt{b})^2$, that is $a > b$, contrary to the assumption.

   (2) The converse is true: If $\sqrt{a} \leq \sqrt{b}$ then $(\sqrt{a})^2 \leq (\sqrt{b})^2$, that is $a \leq b$.

4. (a) If $x > 0$ and $y > 0$ assume $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$. Squaring gives $x + y = x + 2\sqrt{xy} + y$, whence $2\sqrt{xy} = 0$. This means $xy = 0$ so $x = 0$ or $y = 0$, contradicting our assumption.

Student Solution Manual to Accompany Introduction to Abstract Algebra, Fourth Edition.
W. Keith Nicholson.

(c) Assume all have birthdays in different months. Then there can be at most 12 people, one for each month, contrary to hypothesis.

5. (a) $n = 11$ is a counterexample because then $n^2 + n + 11 = 11 \cdot 13$ is not prime. Note that $n^2 + n + 11$ *is* prime if $1 \le n \le 9$ as is readily verified, but $n = 10$ is also a counterexample as $10^2 + 10 + 11 = 11^2$.

   (c) $n = 6$ is a counterexample because there are then 31 regions. Note that the result holds if $2 \le n \le 5$.

0.2 SETS

1. (a) $A = \{x \mid x = 5k,\ k \in \mathbb{Z},\ k \ge 1\}$
2. (a) $\{1, 3, 5, 7, \dots\}$

   (c) $\{-1, 1, 3\}$

   (e) $\{\ \} = \varnothing$ is the empty set by Example 3.
3. (a) Not equal: $-1 \in A$ but $-1 \notin B$.

   (c) Equal to $\{a, l, o, y\}$.

   (e) Not equal: $0 \in A$ but $0 \notin B$.

   (g) Equal to $\{-1, 0, 1\}$.
4. (a) $\varnothing$, $\{2\}$

   (c) $\{1\}$, $\{3\}$, $\{1, 2\}$, $\{1, 3\}$, $\{2, 3\}$, $\{1, 2, 3\}$
5. (a) True. $B \subseteq C$ means each element of B (in particular A) is an element of C.

   (c) False. For example, $A = \{1\}$, $B = C = \{\{1\}, 2\}$.
6. (a) Clearly $A \cap B \subseteq A$ and $A \cap B \subseteq B$; If $X \subseteq A$ and $X \subseteq B$, then $x \in X$ implies $x \in A$ and $x \in B$, that is $x \in A \cap B$. Thus $X \subseteq A \cap B$.
7. If $x \in A \cup (B_1 \cap B_2 \cap \dots \cap B_n)$, then $x \in A$ or $x \in B_i$ for all i. Thus $x \in A \cup B_i$ for all i, that is $x \in (A \cup B_1) \cap (A \cup B_2) \cap \dots \cap (A \cup B_n)$. Thus

$$A \cup (B_1 \cap B_2 \cap \dots \cap B_n) \subseteq (A \cup B_1) \cap (A \cup B_2) \cap \dots \cap (A \cup B_n),$$

   and the reverse argument proves equality. The other formula is proved similarly.
9. $A = \{1, 2\}$, $B = \{1, 3\}$, $C = \{2, 3\}$.
10. (a) Let $A \times B = B \times A$, and fix $a \in A$ and $b \in B$ (since these sets are nonempty). If $x \in A$, then $(x, b) \in A \times B = B \times A$. This implies $x \in B$; so $A \subseteq B$. Similarly $B \subseteq A$.

    (c) If $x \in A \cap B$, then $x \in A$ and $x \in B$, so $(x, x) \in A \times B$. If $(x, x) \in A \times B$, then $x \in A$ and $x \in B$, so $x \in A \cap B$.
11. (a) $(x, y) \in A \times (B \cap C)$

$$\begin{aligned} &\text{if and only if} \quad x \in A \text{ and } y \in (B \cap C) \\ &\text{if and only if} \quad (x, y) \in A \times B \text{ and } (x, y) \in A \times C \\ &\text{if and only if} \quad (x, y) \in (A \times B) \cap (A \times C). \end{aligned}$$

(c) $(x, y) \in (A \cap B) \times (A' \cap B')$
if and only if $x \in A \cap B$ and $y \in A' \cap B'$
if and only if $(x, y) \in A \times A'$ and $(x, y) \in (B \times B')$
if and only if $(x, y) \in (A \times A') \cap (B \times B')$.

0.3 MAPPINGS

1. (a) Not a mapping: $\alpha(1) = -1$ is not in $\mathbb{N}$.
   (c) Not a mapping: $\alpha(-1) = \sqrt{-1}$ is not in $\mathbb{R}$.
   (e) Not a mapping: $\alpha(6) = \alpha(2 \cdot 3) = (2, 3)$ and $\alpha(6) = \alpha(1 \cdot 6) = (1, 6)$.
   (g) Not a mapping: $\alpha(2)$ is not defined.
2. (a) Bijective. $\alpha(x) = \alpha(x_1)$ implies $3 - 4x = 3 - 4x_1$, so $x = x_1$, and α is one-to-one. Given $y \in \mathbb{R}$, $y = \alpha\left[\frac{1}{4}(3 - y)\right]$, so α is onto.
   (c) Onto: If $m \in N$, then $m = \alpha(2m - 1) = \alpha(2m)$. Not one-to-one: In fact we have $\alpha(1) = 1 = \alpha(2)$.
   (e) One-to-one: $\alpha(x) = \alpha(x_1)$ implies $(x + 1, x - 1) = (x_1 + 1, x_1 - 1)$, whence $x = x_1$. Not onto: $(0, 0) \neq \alpha(x)$ for any x because $(0, 0) = (x + 1, x - 1)$ would give $x = 1$ and $x = -1$.
   (g) One-to-one: $\alpha(a) = \alpha(a_1)$ implies $(a, b_0) = (a_1, b_0)$ implies $a = a_1$. Not onto if $|B| \geq 2$ since no element (a, b) is in $\alpha(A)$ for $b \neq b_0$.
3. (a) Given $c \in C$, let $c = \beta\alpha(a)$ with $a \in A$ (because $\beta\alpha$ is onto). Hence $c = \beta(\alpha(a))$, where $\alpha(a) \in B$, so β is onto.
   (c) Let $\beta(b) = \beta(b_1)$. Write $b = \alpha(a)$ and $b_1 = \alpha(a_1)$ (since α is onto). Then
   $$\beta\alpha(a) = \beta(\alpha(a)) = \beta(b) = \beta(b_1) = \beta(\alpha(a_1)) = \beta\alpha(a_1),$$
   so $a = a_1$ (because $\beta\alpha$ is one-to-one), and hence $b = b_1$ as required.
   (e) Let $b \in B$. As α is onto, let $b = \alpha(a)$, $a \in A$. Hence
   $$\beta(b) = \beta(\alpha(a)) = \beta\alpha(a) = \beta_1\alpha(a) = \beta_1(\alpha(a)) = \beta_1(b).$$
   Since $b \in B$ was arbitrary, this shows that $\beta = \beta_1$.
5. (a) If $\alpha^2 = \alpha$, let $x \in \alpha(A)$, say $x = \alpha(a)$. Then $\alpha(x) = \alpha^2(a) = \alpha(a) = x$. Conversely, let $\alpha(x) = x$ for all $x \in \alpha(A)$. If $a \in A$, write $\alpha(a) = x$. Then $\alpha^2(a) = \alpha(\alpha(a)) = \alpha(x) = x = \alpha(a)$, so $\alpha^2 = \alpha$.
   (c) $\alpha^2 = (\beta\gamma)(\beta\gamma) = \beta(\gamma\beta)\gamma = \beta(1_A)\gamma = \beta\gamma = \alpha$.
7. (a) If $y \in \mathbb{R}$, write $\alpha^{-1}(y) = x$. Hence $y = \alpha(x)$, that is $y = ax + b$. Solving for x gives $\alpha^{-1}(y) = x = \frac{1}{a}(y - b)$. As this is possible for all $y \in \mathbb{R}$, this shows that $\alpha^{-1}(y) = \frac{1}{a}(y - b)$ for all $y \in \mathbb{R}$.
   (c) First verify that $\alpha^2 = 1_{\mathbb{N}}$, that is $\alpha\alpha = 1_{\mathbb{N}}$. Hence $\alpha^{-1} = \alpha$ by the definition of the inverse of a function.
9. Let $\beta\alpha = 1_A$. Then α is one-to-one because $\alpha(a) = \alpha(a_1)$ implies that $a = \beta\alpha(a) = \beta\alpha(a_1) = a_1$; and β is onto because if $a \in A$ then $a = \beta\alpha(a) = \beta(\alpha(a))$ and $\alpha(a) \in B$. Hence both are bijections as $|A| = |B|$ (Theorem 2), and hence α^{-1} and β^{-1} exist. But then $\beta^{-1} = \beta^{-1}1_A = \beta^{-1}(\beta\alpha) = \alpha$. Similarly $\alpha^{-1} = \beta$.

11. Let $\varphi(\alpha) = \varphi(\alpha_1)$ where α and α_1 are in M. Then $(\alpha(1), \alpha(2)) = (\alpha_1(1), \alpha_1(2))$, so $\alpha(1) = \alpha_1(1)$ and $\alpha(2) = \alpha_1(2)$. Thus $\alpha = \alpha_1$ (by Theorem 1), so φ is one-to-one. Conversely, let $(x, y) \in B \times B$, and define $\alpha_2 : \{1, 2\} \to B$ by $\alpha_2(1) = x$ and $\alpha_2(2) = y$. Then $\alpha_2 \in \mathsf{M}$, and $\varphi(\beta) = (\alpha_2(1), \alpha_2(2)) = (x, y)$. Thus φ is onto. Then $\varphi^{-1} : B \times B \to \mathsf{M}$ has action $\varphi^{-1}(x, y) = \alpha_2$ where $\alpha_2(1) = x$ and $\alpha_2(2) = y$.

13. For each $a \in A$ there are m choices for $\alpha(a) \in B$. Since $|A| = n$, there are m^n choices in all, and they all lead to different functions α because α is determined by these choices.

15. (a) $\Rightarrow$ (b) Given $b \in B$, write $A_b = \{a \in A \mid \alpha(a) = b\}$. Then $A_b \neq \emptyset$ for each b (α is onto), so choose $a_b \in A_b$ for each $b \in B$. Then define $\beta : B \to A$ by $\beta(b) = a_b$. Then $\alpha\beta(a) = \alpha(\beta(b)) = \alpha(a_b) = b$ for each b; that is $\alpha\beta = 1_B$.

    (c) $\Rightarrow$ (a) If $b_0 \in B - \alpha(A)$, we deduce a contradiction. Choose $a_0 \in A$, and define $\beta : B \to B$ by:

$$\beta(b) = \begin{cases} b & \text{if } b \neq b_0 \\ \alpha(a_0) & \text{if } b = b_0. \end{cases}$$

    Then $\alpha(a) \neq b_0$ for all $a \in A$, so

$$\beta\alpha(a) = \beta(\alpha(a)) = \alpha(a) = 1_B(\alpha(a)) = 1_B\alpha(a)$$

    for all $a \in A$. Hence, $\beta\alpha = 1_B\alpha$, so $\beta = 1_B$ by (c). Finally then $b_0 = \beta(b_0) = \alpha(a_0)$, a contradiction.

0.4 EQUIVALENCES

1. (a) It is an equivalence by Example 4.

$$[-1] = [0] = [1] = \{-1, 0, 1\},\ [2] = \{2\}, [-2] = \{-2\}.$$

   (c) Not an equivalence. $x \equiv x$ only if $x = 1$, so the reflexive property fails.

   (e) Not an equivalence. $1 \equiv 2$ but $2 \not\equiv 1$, so the symmetric property fails.

   (g) Not an equivalence. $x \equiv x$ is *never* true. Note that the transitive property also fails.

   (i) It is an equivalence by Example 4. $[(a, b)] = \{(x, y) \mid y - 3x = b - 3a\}$ is the line with slope 3 through (a, b).

2. In every case $(a, b) \equiv (a_1, b_1)$ if $\alpha(a, b) = \alpha(a_1, b_1)$ for an appropriate function $\alpha : A \to \mathbb{R}$. Hence $\equiv$ is the kernel equivalence of α.

   (a) The classes are indexed by the possible sums of elements of U.

      Sum is 2: $[(1, 1)] = \{(1, 1)\}$
      Sum is 3: $[(1, 2)] = [(2, 1)] = \{(1, 2), (2, 1)\}$
      Sum is 4: $[(1, 3)] = [(2, 2)] = [(3, 1)] = \{(1, 3), (2, 2), (3, 1)\}$
      Sum is 5: $[(2, 3)] = [(3, 2)] = \{(2, 3), (3, 2)\}$
      Sum is 6: $[(3, 3)] = \{(3, 3)\}$.

(c) The classes are indexed by the first components.

First component is 1: $[(1,1)] = [(1,2)] = [(1,3)] = \{(1,1),(1,2),(1,3)\}$
First component is 2: $[(2,1)] = [(2,2)] = [(3,2)] = \{(2,1),(2,2),(2,3)\}$
First component is 3: $[(3,1)] = [(3,2)] = [(3,3)] = \{(3,1),(3,2),(3,3)\}$.

3. (a) It is the kernel equivalence of $\alpha : \mathbb{Z} \to \mathbb{Z}$ where $\alpha(n) = n^2$. Here $[n] = \{-n, n\}$ for each n. Define $\sigma : \mathbb{Z}_\equiv \to B$ by $\sigma[n] = |n|$, where $|n|$ is the absolute value. Then $[m] = [n] \Leftrightarrow m \equiv n \Leftrightarrow |m| = |n|$. Thus σ is well-defined and one-to-one. It is clearly onto.

(c) It is the kernel equivalence of $\alpha : \mathbb{R} \to \mathbb{R}$ where $\alpha(x, y) = y$. Define $\sigma : (\mathbb{R} \times \mathbb{R})_\equiv \to B$ by $\sigma[(x, y)] = y$. Then

$$[(x, y)] = [(x_1, y_1)] \Leftrightarrow (x, y) \equiv (x_1, y_1) \Leftrightarrow y = y_1,$$

so σ is well-defined and one-to-one. It is clearly onto.

(e) Reflexive: $x \equiv x \in \mathbb{Z}$;
Symmetric: $x \equiv y \Rightarrow x - y \in \mathbb{Z} \Rightarrow y - x \in \mathbb{Z} \Rightarrow y \equiv x$;
Transitive: $x \equiv y$ and $y \equiv z$ gives $x - y \in \mathbb{Z}$ and $y - z \in \mathbb{Z}$. Hence

$$x - z = (x - y) + (y - z) \in \mathbb{Z}, \text{ that is } x \equiv z.$$

Now define $\sigma : \mathbb{R}_\equiv \to B$ by $\sigma[x] = x - \lfloor x \rfloor$ where $\lfloor x \rfloor$ denotes the greatest integer $\leq x$. Then $[x] = [y] \Rightarrow x \equiv y \Rightarrow x - y = n,\ n \in \mathbb{Z}$. Thus $x = y + n$, so $\lfloor x \rfloor = \lfloor y \rfloor + n$. Hence,

$$x - \lfloor x \rfloor = (y + n) - (\lfloor y \rfloor + n) = y - \lfloor y \rfloor,$$

and σ is well-defined. To see that σ is one-to-one, let $\sigma[x] = \sigma[y]$, that is $x - \lfloor x \rfloor = y - \lfloor y \rfloor$. Then $x - y = \lfloor y \rfloor - \lfloor x \rfloor \in \mathbb{Z}$, so $x \equiv y$, that is $\lfloor x \rfloor = \lfloor y \rfloor$. Finally, σ is onto because, if $0 \leq x < 1$, $\lfloor x \rfloor = 0$, so $x = \sigma[x]$.

5. (a) If $a \in A$, then $a \in C_i$ and $a \in D_j$ for some i and j, so $a \in C_i \cap D_j$. If $C_i \cap D_j \neq C_{i'} \cap D_{j'}$, then either $i \neq i'$ or $j \neq j'$. Thus

$$(C_i \cap D_j) \cap (C_{i'} \cap D_{j'}) = \emptyset$$

in either case.

7. (a) Not well defined: $\alpha(2) = \alpha\left(\frac{2}{1}\right) = 2$ and $\alpha(2) = \alpha\left(\frac{4}{2}\right) = 4$.

(c) Not well defined: $\alpha\left(\frac{1}{2}\right) = 3$ and $\alpha\left(\frac{1}{2}\right) = \alpha\left(\frac{2}{4}\right) = 6$.

9. (a) $[a] = [a_1] \Leftrightarrow a \equiv a_1 \Leftrightarrow \alpha(a) = \alpha(a_1)$. The implication $\Rightarrow$ proves σ is well defined; the implication $\Leftarrow$ shows it is one-to-one. If α is onto, so is σ.

(c) If we regard $\sigma : A_\equiv \to a(A)$, then σ is a bijection.

Chapter 1

Integers and Permutations

1.1 INDUCTION

1. In each case we give the equation that makes p_k imply p_{k+1}.
   (a) $k(2k-1)+(4k+1)=2k^2+3k+1=(k+1)(2k+1)$
   (c) $\frac{1}{4}k^2(k+1)^2+(k+1)^3=\frac{1}{4}(k+1)^2(k^2+4k+4)=\frac{1}{4}(k+1)^2(k+2)^2$
   (e) $\frac{1}{12}k(k+1)(k+2)(3k+5)+(k+1)(k+2)^2$
   $=\frac{1}{12}(k+1)(k+2)(3k^2+17k+24)=\frac{1}{12}(k+1)(k+2)(k+3)(3k+8)$
   (g) $\frac{k}{3}(4k^2-1)+(2k+1)^2=\frac{k}{3}(2k-1)(2k+1)+(2k+1)^2$
   $=\frac{1}{3}(2k+1)[2k^2+5k+3]=\frac{1}{3}(2k+1)(k+1)(2k+3)$
   $=\frac{1}{3}(k+1)[4(k+1)^2-1]$
   (i) $1-\frac{1}{(k+1)!}+\frac{k+1}{(k+2)!}=1-\frac{1}{(k+2)!}[(k+2)-(k+1)]=1-\frac{1}{(k+2)!}$
2. In each case we give the inequality that makes p_k imply p_{k+1}.
   (a) $2^{k+1}=2\cdot 2^k>2\cdot k\geq k+1$.
   (c) If $k!\leq 2^{k^2}$, then $(k+1)!=(k+1)k!\leq(k+1)2^{k^2}\leq 2^{(k+1)^2}$ provided $k+1\leq 2^{2k+1}$. This latter inequality follows, again by induction on $k\geq 1$, because $2^{2k+3}=4\cdot 2^{2k+1}\geq 4(k+1)\geq k+2$.
   (e) $\frac{1}{\sqrt{1}}+\cdots+\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{k+1}}\geq\sqrt{k}+\frac{1}{\sqrt{k+1}}=\frac{\sqrt{k^2+k}+1}{\sqrt{k+1}}\geq\frac{k+1}{\sqrt{k+1}}=\sqrt{k+1}$.
3. In each case we give the calculation that makes p_k imply p_{k+1}.
   (a) If $k^3+(k+1)^3+(k+2)^3=9m$, then
   $(k+1)^3+(k+2)^3+(k+3)^3=9m-k^3+(k+3)^3=9m+9k^2+27k+27$.
   (c) If $3^{2k+1}+2^{k+2}=7m$, then

$$3^{2k+3}+2^{k+3}=9(7m-2^{k+2})+2^{k+3}=9\cdot 7m-2^{k+2}(9-2).$$

Student Solution Manual to Accompany Introduction to Abstract Algebra, Fourth Edition.
W. Keith Nicholson.