INSTRUCTOR'S SOLUTIONS MANUAL

JOHN B. FRALEIGH AND NEAL BRAND

A FIRST COURSE IN ABSTRACT ALGEBRA

EIGHTH EDITION

John B. Fraleigh
University of Rhode Island

Neal Brand
University of North Texas

Pearson

The author and publisher of this book have used their best efforts in preparing this book. These efforts include the development, research, and testing of the theories and programs to determine their effectiveness. The author and publisher make no warranty of any kind, expressed or implied, with regard to these programs or the documentation contained in this book. The author and publisher shall not be liable in any event for incidental or consequential damages in connection with, or arising out of, the furnishing, performance, or use of these programs.

Reproduced by Pearson from electronic files supplied by the author.

ISBN-13: 978-0-32-139037-0
ISBN-10: 0-321-39037-7

Preface for Seventh Edition

This manual contains solutions to all exercises in the text, except those odd-numbered exercises for which fairly lengthy complete solutions are given in the answers at the back of the text. Then reference is simply given to the text answers to save typing.

I prepared these solutions myself. While I tried to be accurate, there are sure to be the inevitable mistakes and typos. An author reading proof tends to see what he or she wants to see. However, the instructor should find this manual adequate for the purpose for which it is intended.

Morgan, Vermont J.B.F
July, 2002

Preface for Eighth Edition

In keeping with the seventh edition, this manual contains solutions to all exercises in the text except for some of the odd-numbered exercises whose solutions are in the back of the text book. I made few changes to solutions to exercises that were in the seventh edition. However, solutions to new exercises do not always include as much detail as would be found in the seventh edition. My thinking is that instructors teaching the class would use the solution manual to see the idea behind a solution and they would easily fill in the routine details.

As in the seventh edition, I tried to be accurate. However, there are sure to be some errors. I hope instructors find the manual helpful.

Denton, Texas N.B.
March, 2020

CONTENTS

I. Groups and Subgroups

II. Structure of Groups

III. Homomorphisms and Factor Groups

VI. Advanced Group Theory

V. Rings and Fields

VI. Constructing Rings and Fields

VII. Commutative Algebra

VIII. Extension Fields

IX. Galois Theory

0. Sets and Relations

1. $\{\sqrt{3}, -\sqrt{3}\}$

2. $\{2, -3\}$.

3. $\{1, -1, 2, -2, 3, -3, 4, -4, 5, -5, 6, -6, 10, -10, 12, -12, 15, -15, 20, -20, 30, -30, 60, -60\}$

4. $\{2, 3, 4, 5, 6, 7, 8\}$

5. It is not a well-defined set. (Some may argue that no element of $\mathbb{Z}^+$ is large, because every element exceeds only a finite number of other elements but is exceeded by an infinite number of other elements. Such people might claim the answer should be $\emptyset$.)

6. $\emptyset$

7. The set is $\emptyset$ because $3^3 = 27$ and $4^3 = 64$.

8. $\{ r \in \mathbb{Q} \mid r = \frac{a}{2^n}$ for some a $a \in \mathbb{Z}^+$ and some integer n $\geq 0\}$.

9. It is not a well-defined set.

10. The set containing all numbers that are (positive, negative, or zero) integer multiples of 1, 1/2, or 1/3.

11. $\{(a, 1), (a, 2), (a, c), (b, 1), (b, 2), (b, c), (c, 1), (c, 2), (c, c)\}$

12. **a.** This is a function which is both one-to-one and onto B.

b. This not a subset of $A \times B$, and therefore not a function.

c. It is not a function because there are two pairs with first member 1.

d. This is a function which is neither one-to-one (6 appears twice in the second coordinate) nor onto B (4 is not in the second coordinate).

e. It is a function. It is not one-to-one because there are two pairs with second member 6. It is not onto B because there is no pair with second member 2.

f. This is not a function mapping A into B since 3 is not in the first coordinate of any ordered pair.

13. Draw the line through P and x, and let y be its point of intersection with the line segment CD.

14. **a.** $\phi\colon [0,1] \to [0,2]$ where $\phi(x) = 2x$

b. $\phi\colon [1,3] \to [5,25]$ where $\phi(x) = 2x + 3$

c. $\phi\colon [a, b] \to [c, d]$ where $\phi(x) = c + \dfrac{d-c}{b-a}(x-a)$

15. Let $\phi : S \to \mathbb{R}$ be defined by $\phi(x) = \tan(\pi(x - \frac{1}{2}))$.

16. **a.** $\varnothing$; cardinality 1

b. $\varnothing, \{a\}$; cardinality 2

c. $\varnothing, \{a\}, \{b\}, \{a, b\}$; cardinality 4

d. $\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$; cardinality 8

17. Conjecture: $|P(A)| = 2^s = 2^{|A|}$.

Proof The number of subsets of a set A depends only on the cardinality of A, not on what the elements of A actually are. Suppose $B = \{1, 2, 3, \cdots, s - 1\}$ and $A = \{1, 2, 3, \cdots, s\}$. Then A has all the elements of B plus the one additional element s. All subsets of B are also subsets of A; these are precisely the subsets of A that do not contain s, so the number of subsets of A not containing s is $|P(B)|$. Any other subset of A must contain s, and removal of the s would produce a subset of B. Thus the number of subsets of A containing s is also $|P(B)|$. Because every subset of A either contains s or does not contain s (but not both), we see that the number of subsets of A is $2|P(B)|$.

We have shown that if A has one more element that B, then $|P(A)| = 2|P(B)|$. Now $|P(\emptyset)| = 1$, so if $|A| = s$, then $|P(A)| = 2^s$.

18. We define a one-to-one map ϕ of B^A onto $P(A)$. Let $f \in B^A$, and let $\phi(f) = \{x \in A \mid f(x) = 1\}$. Suppose $\phi(f) = \phi(g)$. Then $f(x) = 1$ if and only if $g(x) = 1$. Because the only possible values for $f(x)$ and $g(x)$ are 0 and 1, we see that $f(x) = 0$ if and only if $g(x) = 0$. Consequently $f(x) = g(x)$ for all $x \in A$ so $f = g$ and ϕ is one to one. To show that ϕ is onto $P(A)$, let $S \subseteq A$, and let $h : A \to \{0, 1\}$ be defined by $h(x) = 1$ if $x \in S$ and $h(x) = 0$ otherwise. Clearly $\phi(h) = S$, showing that ϕ is indeed onto $P(A)$.

19. Picking up from the hint, let $Z = \{x \in A \mid x \notin \phi(x)\}$. We claim that for any $a \in A$, $\phi(a) \neq Z$. Either $a \in \phi(a)$, in which case $a \notin Z$, or $a \notin \phi(a)$, in which case $a \in Z$. Thus Z and $\phi(a)$ are certainly different subsets of A; one of them contains a and the other one does not.

Based on what we just showed, we feel that the power set of A has cardinality greater than $|A|$. Proceeding naively, we can start with the infinite set $\mathbb{Z}$, form its power set, then form the power set of that, and continue this process indefinitely. If there were only a finite number of infinite cardinal numbers, this process would have to terminate after a fixed finite number of steps. Since it doesn't, it appears that there must be an infinite number of different infinite cardinal numbers.

The set of everything is not logically acceptable, because the set of all subsets of the set of everything would be larger than the set of everything, which is a fallacy.

20. a. The set containing precisely the two elements of A and the three (different) elements of B is $C = \{1, 2, 3, 4, 5\}$ which has 5 elements.

i) Let $A = \{-2, -1, 0\}$ and $B = \{1, 2, 3, \cdots\} = \mathbb{Z}^+$. Then $|A| = 3$ and $|B| = \aleph_0$, and A and B have no elements in common. The set C containing all elements in either A or B is $C = \{-2, -1, 0, 1, 2, 3, \cdots\}$. The map $\phi : C \to B$ defined by $\phi(x) = x + 3$ is one to one and onto B, so $|C| = |B| = \aleph_0$. Thus we consider $3 + \aleph_0 = \aleph_0$.

ii) Let $A = \{1, 2, 3, \cdots\}$ and $B = \{1/2, 3/2, 5/2, \cdots\}$. Then $|A| = |B| = \aleph_0$ and A and B have no elements in common. The set C containing all elements in either A of B is $C = \{1/2, 1, 3/2, 2, 5/2, 3, \cdots\}$. The map $\phi : C \to A$ defined by $\phi(x) = 2x$ is one to one and onto A, so $|C| = |A| = \aleph_0$. Thus we consider $\aleph_0 + \aleph_0 = \aleph_0$

b. We leave the plotting of the points in $A \times B$ to you. Figure 0.15 in the text, where there are $\aleph_0$ rows each having $\aleph_0$ entries, illustrates that we would consider that $\aleph_0 \cdot \aleph_0 = \aleph_0$.

21. There are $10^2 = 100$ numbers (.00 through .99) of the form .##, and $10^5 = 100,000$ numbers (.00000 through .99999) of the form .#####. Thus for .##### · · ·, we expect $10^{\aleph_0}$ sequences representing all numbers $x \in \mathbb{R}$ such that $0 \le x \le 1$, but a sequence trailing off in 0's may represent the same $x \in \mathbb{R}$ as a sequence trailing of in 9's. At any rate, we should have $10^{\aleph_0} \ge |[0, 1]| = |\mathbb{R}|$; see Exercise 15. On the other hand, we can represent numbers in $\mathbb{R}$ using any integer base $n > 1$, and these same $10^{\aleph_0}$ sequences using digits from 0 to 9 in base $n = 12$ would not represent all $x \in [0, 1]$, so we have $10^{\aleph_0} \le |\mathbb{R}|$. Thus we consider the value of $10^{\aleph_0}$ to be $|\mathbb{R}|$. We could make the same argument using any other integer base $n > 1$, and thus consider $n^{\aleph_0} = |\mathbb{R}|$ for $n \in \mathbb{Z}^+$, $n > 1$. In particular, $12^{\aleph_0} = 12^{\aleph_0} = |\mathbb{R}|$.

22. $\aleph_0, |\mathbb{R}|,\ 2^{|\mathbb{R}|},\ 2^{(2^{|\mathbb{R}|})}, 2^{(2^{(2^{|\mathbb{R}|})})}$

23. 1. There is only one partition $\{\{a\}\}$ of a one-element set $\{a\}$.

24. There are two partitions of $\{a, b\}$, namely $\{\{a, b\}\}$ and $\{\{a\}, \{b\}\}$.

25. There are five partitions of $\{a, b, c\}$, namely $\{\{a, b, c\}\}$, $\{\{a\}, \{b, c\}\}$, $\{\{b\}, \{a, c\}\}$, $\{\{c\}, \{a, b\}\}$, and $\{\{a\}, \{b\}, \{c\}\}$.

26. 15. The set $\{a, b, c, d\}$ has 1 partition into one cell, 7 partitions into two cells (four with a 1,3 split and three with a 2,2 split), 6 partitions into three cells, and 1 partition into four cells for a total of 15 partitions.

27. 52. The set $\{a, b, c, d, e\}$ has 1 partition into one cell, 15 into two cells, 25 into three cells, 10 into four cells, and 1 into five cells for a total of 52. (Do a combinatorics count for each possible case, such as a 1,2,2 split where there are 15 possible partitions.)

28. *Reflexive:* In order for $x\ R\ x$ to be true, x must be in the same cell of the partition as the cell that contains x. This is certainly true.

Transitive: Suppose that $x\ R\ y$ and $y\ R\ z$. Then x is in the same cell as y so $\overline{x} = \overline{y}$, *and y is in* the same cell as z so that $\overline{y} = \overline{z}$. By the transitivity of the set equality relation on the collection of cells in the partition, we see that $\overline{x} = \overline{z}$ so that x is in the same cell as z. Consequently, $x\ R\ z$.

29. Not an equivalence relation; 0 is not related to 0, so it is not reflexive.

30. Not an equivalence relation; $3 \ge 2$ but $2 \not\ge 3$, so it is not symmetric.

31. Not an equivalence relation since transitivity fails: $3 \mathscr{R} 15$ and $15 \mathscr{R} 5$, but $3 \mathscr{R} 5$. Also not reflexive: $1 \mathscr{R} 1$.

32. $\overline{0} = (0,0)$ and $\overline{(x, y)}$ is the circle centered at the origin with radius $\sqrt{x^2 + y^2}$.

33. (See the answer in the text.)

34. It is an equivalence relation;

$\overline{1} = \{1,\ 11,\ 21,\ 31, \cdots\},\ \overline{2} = \{2,\ 12,\ 22,\ 32, \cdots\}, \cdots,\ \overline{10} = \{10,\ 20,\ 30,\ 40, \cdots\}.$

35. **a.** $\{\ldots, -3, 0, 3, \ldots\}, \{\ldots, -2, 1, 4, \ldots\}, \{\ldots, -1, 2, 5, \ldots\}$

b. $\{\ldots, -4, 0, 4, \ldots\}, \{\ldots, -3, 1, 4, \ldots\}, \{\ldots, -6, -2, 2, \ldots\}, \{\ldots, -5, -1, 3, \ldots\}$

c. $\{\ldots, -5, 0, 5, \ldots\},\ \{\ldots, -4, 1, 6, \ldots\}, \{\ldots, -3, 2, 7, \ldots\}, \{\ldots, -2, 3, 8, \ldots\}.$ $\{\ldots, -1, 4, 9, \ldots\}$

36. **a.** $\{\overline{0}, \overline{1}, \overline{2}\}$ **b.** $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ **c.** $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

37. $\bar{1} = \{x \in \mathbb{Z} \mid x \div n$ has remainder $1\}$ depends on the value of n.

38. **a.** Let h, k, and m be positive integers. We check the three criteria.

Reflexive: $h - h = n0$ so $h \sim h$.

Symmetric: If $h \sim k$ so that $h - k = ns$ for some $s \in \mathbb{Z}$, then $k - h = n(-s)$ so $k \sim h$.

Transitive: If $h \sim k$ and $k \sim m$, then for some $s, t \in \mathbb{Z}$, we have $h - k = ns$ and $k - m = nt$. Then $h - m = (h - k) + (k - m) = ns + nt = n(s + t)$, so $h \sim m$.

b. Let $h, k \in \mathbb{Z}$. In the sense of this exercise, $h \sim k$ if and only if $h - k = nq$ for some $q \in \mathbb{Z}$. In the sense of Example 0.19, $h \equiv k \pmod{n}$ if and only if h and k have the same remainder when divided by n. Write $h = nq_1 + r_1$ and $k = nq_2 + r_2$ where $0 \le r_1 < n$ and $0 \le r_2 < n$. Then

$$h - k = n(q_1 - q_2) + (r_1 - r_2)$$

and we see that $h - k$ is a multiple of n if and only if $r_1 = r_2$. Thus the conditions are the same.

39. $(a_1 + b_1) - (a_2 + b_2) = (a_1 - a_2) + (b_1 - b_2)$ which is the sum of two multiples of n. Since the sum of two multiples of n is also a multiple of n, $(a_1 + b_1) \sim (a_2 + b_2)$.

40. $(a_1b_1) - (a_2b_2) = (a_1b_1) - (a_1b_2) + (a_1b_2) - (a_2b_2) = a_1(b_1 - b_2) + (a_1 - a_2)b_2$ which is the sum of two multiples of n. Since the sum of two multiples of n is also a multiple of n, $(a_1b_1) \sim (a_2b_2)$.

41. The name *two-to-two function* suggests that such a function f should carry every pair of distinct points into two distinct points. Such a function is one-to-one in the conventional sense. (If the domain has only one element, the function cannot fail to be two-to-two, because the only way it can fail to be two-to-two is to carry two points into one point, and the set does not have two points.) Conversely, every function that is one-to-one in the conventional sense carries each pair of distinct points into two distinct points. Thus the functions conventionally called one-to-one are precisely those that carry two points into two points, which is a much more intuitive unidirectional way of regarding them. Also, the standard way of trying to show that a function is one-to-one is precisely to show that it does not fail to be two-to-two. That is, proving that a function is one-to-one becomes more natural in the two-to-two terminology.

1. Binary Operations

1. $b * d = e, \qquad c * c = b, \qquad [(a * c) * e] * a = [c * e] * a = a * a = a$

2. $(a * b) * c = b * c = a$ and $a * (b * c) = a * a = a$, so the operation might be associative, but we can't tell without checking all other triple products.

3. $(b * d) * c = e * c = a$ and $b * (d * c) = b * b = c$, so the operation is not associative.

4. It is not commutative because $b * e = c$ but $e * b = b$.

5. Now $d * a = d$ so fill in d for $a * d$. Also, $c * b = a$ so fill in a for $b * c$. Now $b * d = c$ so fill in c for $d * b$. Finally, $c * d = b$ so fill in b for $d * c$.

6. $d * a = (c * b) * a = c * (b * a) = c * b = d$. In a similar fashion, substituting $c * b$ for d and using the associative property, we find that $d * b = c$, $d * c = c$, and $d * d = d$. a is an identity.

7. It is not commutative because $1 - 2 \neq 2 - 1$. It is not associative because $2 = 1 - (2 - 3) \neq (1 - 2) - 3 = -4$. No identity.

8. Commutative since $2ab + 3 = 2ba + 3$. Not associative since $(1 * 2) * 3 = 45$ and $1 * (2 * 3) = 33$. No identity since $0 * e = 3 \neq 0$.

9. Commutative since $a * b = ab + a + b = b * a$. Associative since $a * b = (a + 1)(b + 1) - 1$ making it easy to see that $(a * b) * c = (a + 1)(b + 1)(c + 1) - 1 = a * (b * c)$. The identity is 0.

10. It is commutative because $2^{ab} = 2^{ba}$ for all $a, b \in \mathbb{Z}^+$. It is not associative because $(a * b) * c = 2^{ab} * c = 2^{(2^{ab})c}$, but $a * (b * c) = a * 2^{bc} = 2^{a(2^{bc})}$. No identity.

11. It is not commutative because $2 * 3 = 2^3 = 8 \neq 9 = 3^2 = 3 * 2$. It is not associative because $a * (b * c) = a * b^c = a^{(b^c)}$, but $(a * b) * c = a^b * c = (a^b)^c = a^{bc}$, and $bc \neq b^c$ for some $b, c \in \mathbb{Z}^+$. No identity.

12. If S has just one element, there is only one possible binary operation on S; the table must be filled in with that single element. If S has two elements, there are 16 possible operations, for there are four places to fill in a table, and each may be filled in two ways, and $2 \cdot 2 \cdot 2 \cdot 2 = 16$. There are 19,683 operations on a set S with three elements, for there are nine places to fill in a table, and $3^9 = 19,\ 683$. With n elements, there are n^2 places to fill in a table, each of which can be done in n ways, so there are $n^{(n^2)}$ possible tables.

13. A commutative binary operation on a set with n elements is completely determined by the elements on or above the *main diagonal* in its table, which runs from the upper left corner to the lower right corner. The number of such places to fill in is

$$n + \frac{n^2 - n}{2} = \frac{n^2 + n}{2}.$$

Thus there are $n^{(n^2+n)/2}$ possible commutative binary operations on an n-element set. For $n = 2$, we obtain $2^3 = 8$, and for $n = 3$ we obtain $3^6 = 729$.

14. $n^{n(n-1))}$ since there are $n^2 - n = n(n - 1)$ spots to be filled once the diagonal is filled.

15. $n^{((n-1)^2)}$ since after the first row and column are determined there are $(n-1)^2$ spots to be filled.

16. It is incorrect. Mention should be made of the underlying set for $*$ and the universal quantifier, *for all*, should appear.

A binary operation $*$ on a set S is **commutative** if and only if $a * b = b * a$ for all $a, b \in S$.

17. The definition is correct.

18. It is incorrect. Replace the final S by H.

19. An identity in the set S with operation $*$ is element $e \in S$ such that for all $a \in S$, $a * e = e * a = a$.

20. No, because $e_1 * e_2 = e_1$ and $e_1 * e_2 = e_2$.

21. This is an operation.

22. No. Condition 2 is violated. $1 * 2$ should be 0, but $0 \notin \mathbb{R}^+$.

23. No. Condition 2 is violated. $2 * 1$ should be 0, but $0 \notin \mathbb{R}^+$.

24. No. Condition 1 is violated since the value of $1 * 2$ is not well defined as it could either be 1 or –1. Also, Condition 2 is violated since $-1 * 2$ is undefined.

25. It is not a binary operation. Condition 1 is violated, for $2 * 3$ might be any integer greater than 9.

26. It is not a binary operation. Condition 2 is violated, for $1 * 1 = 0$ and $0 \notin \mathbb{R}^+$.

27. **a.** Yes. $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -(b+d) \\ b+d & a+c \end{bmatrix}.$

b. Yes. $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{bmatrix}.$

28. F T F F F T T T T F F F T F

29. (See the answer in the text.)

30. We have $(a * b) * (c * d) = (c * d) * (a * b) = (d * c) * (a * b) = [(d * c) * a] * b$, where we used commutativity for the first two steps and associativity for the last.

31. The statement is true. Commutativity and associativity assert the equality of certain computations. For a binary operation on a set with just one element, that element is the result of every computation involving the operation, so the operation must be commutative and associative.

32. The statement is false. Consider the operation on $\{a, b\}$ defined by the table. Then $(a * a) * b = b * b = a$ but $a * (a * b) = a * a = b$.

$*$	a	b
a	b	a
b	a	a

33. It is associative.

Proof: $[(f + g) + h](x) = (f + g)(x) + h(x) = [f(x) + g(x)] + h(x) = f(x) + [g(x) + h(x)] = f(x) + [(g + h)(x)] = [f + (g + h)](x)$ because addition in $\mathbb{R}$ is associative.

34. It is not commutative. Let $f(x) = 2x$ and $g(x) = 5x$. Then $(f - g)(x) = f(x) - g(x) = 2x - 5x = -3x$ while $(g - f)(x) = g(x) - f(x) = 5x - 2x = 3x$.

35. It is not associative. Let $f(x) = 2x$, $g(x) = 5x$, and $h(x) = 8x$. Then $[f - (g - h)](x) = f(x) - (g - h)(x) = f(x) - [g(x) - h(x)] = f(x) - g(x) + h(x) = 2x - 5x + 8x = 5x$, but $[(f - g) - h](x) = (f - g)(x) - h(x) = f(x) - g(x) - h(x) = 2x - 5x - 8x = -11x$.

36. No identity.

37. The constant function $f(x) = 1$ is an identity element in F.

38. It is commutative.

Proof: $(f \cdot g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x) = (g \cdot f)(x)$ because multiplication in $\mathbb{R}$ is commutative.

39. It is associative.

Proof: $[(f \cdot g) \cdot h](x) = (f \cdot g)(x) \cdot h(x) = [f(x) \cdot g(x)] \cdot h(x) = f(x) \cdot [g(x) \cdot h(x)] = [f \cdot (g \cdot h)](x)$ because multiplication in $\mathbb{R}$ is associative.

40. It is not commutative. Let $f(x) = x^2$ and $g(x) = x + 1$. Then $(f \text{ o } g)(3) = f(g(3)) = f(4) = 16$ but $(g \text{ o } f)(3) = g(f(3)) = g(9) = 10$.

41. It is not true. Let $*$ be $+$ and let $*'$ be $\cdot$ and let $S = \mathbb{Z}$. Then $2 + (3 \cdot 5) = 17$ but $(2 + 3) \cdot (2 + 5) = 35$.

42. Let $a, b \in H$. By definition of H, we have $a * x = x * a$ and $b * x = x * b$ for all $x \in S$. Using the fact that $*$ is associative, we then obtain, for all $x \in S$,

$$(a*b)*x = a*(b*x) = a*(x*b) = (a*x)*b = (x*a)*b = x*(a*b).$$

This shows that $a * b$ satisfies the defining criterion for an element of H, so $(a*b) \in H$.

43. Let $a, b \in H$. By definition of H, we have $a * a = a$ and $b * b = b$. Using, one step at a time, the fact that $*$ is associative and commutative, we obtain

$$\begin{aligned}(a*b)*(a*b) &= [(a*b)*a]*b = [a*(b*a)]*b = [a*(a*b)]*b \\ &= [(a*a)*b]*b = (a*b)*b = a*(b*b) = a*b.\end{aligned}$$

This show that $a * b$ satisfies the defining criterion for an element of H, so $(a*b) \in H$.

44. For any $x,\ y \in S$, $x * y = (x * y) * (x * y) = ((x * y) * x) * y = ((y * x) * x) * y = ((x * x) * y) * y = (x * y) * y = (y * y) * x = y * x$. So $*$ is commutative. Since $*$ is commutative, $(x * y) * z = (y * z) * x = x * (y * z)$ for and $x,\ y \in S$. So $*$ is associative.