https://selldocx.com/products
/solution-manual-a-first-course-in-abstract-algebra-7e-fraleigh

Instructor's Solutions Manual

to accompany

A First Course in Abstract Algebra

Seventh Edition

John B. Fraleigh
University of Rhode Island

Preface

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 rends 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

CONTENTS

VI. Extension Fields

VII. Advanced Group Theory

VIII. Groups in Topology

IX. Factorization

X. Automorphisms and Galois Theory

0. Sets and Relations

1. $\{\sqrt{3}, -\sqrt{3}\}$ **2.** The set is empty.

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. $\{-10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

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 $\varnothing$.)

6. $\varnothing$ **7.** The set is $\varnothing$ because $3^3 = 27$ and $4^3 = 64$.

8. It is not a well-defined set. **9.** $\mathbb{Q}$

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.** It is a function. It is not one-to-one since there are two pairs with second member 4. It is not onto B because there is no pair with second member 2.

b. (Same answer as Part(**a**).)

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

d. It is a function. It is one-to-one. It is onto B because every element of B appears as second member of some pair.

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. It is not a function because there are two pairs with first member 2.

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

14. **a.** $\phi : [0,1] \to [0,2]$ where $\phi(x) = 2x$ **b.** $\phi : [1,3] \to [5,25]$ where $\phi(x) = 5 + 10(x-1)$
c. $\phi : [a,b] \to [c,d]$ where $\phi(x) = c + \frac{d-c}{b-a}(x-a)$

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:** $|\mathcal{P}(A)| = 2^s = 2^{|A|}$.

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 $|\mathcal{P}(B)|$. 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 $|\mathcal{P}(B)|$. 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 $2|\mathcal{P}(B)|$.

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

18. We define a one-to-one map ϕ of B^A onto $\mathcal{P}(A)$. 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 $\mathcal{P}(A)$, 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 $\mathcal{P}(A)$.

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 0.14 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 .##### $\cdots$, we expect $10^{\aleph_0}$ sequences representing all numbers $x \in \mathbb{R}$ such that $0 \leq x \leq 1$, 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 $10^{\aleph_0} \geq |[0, 1]| = |\mathbb{R}|$; 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 $10^{\aleph_0} \leq |\mathbb{R}|$. 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, $12^{\aleph_0} = 2^{\aleph_0} = |\mathbb{R}|$.

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 $x \mathcal{R} x$ 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 $x \mathcal{R} y$ and $y \mathcal{R} z$. 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, $x \mathcal{R} z$.

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

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

31. It is an equivalence relation; $\overline{0} = \{0\}$ and $\overline{a} = \{a, -a\}$ for $a \in \mathbb{R}, a \neq 0$.

32. It is not an equivalence relation; $1 \mathcal{R} 3$ and $3 \mathcal{R} 5$ but we do not have $1 \mathcal{R} 5$ because $|1 - 5| = 4 > 3$.

33. (See the answer in the text.)

34. It is an equivalence relation;

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

35. (See the answer in the text.)

36. **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 $0 \leq r_1 < n$ and $0 \leq r_2 < n$. 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.

c. **a.** $\overline{0} = \{\cdots, -2, 0, 2, \cdots\}, \quad \overline{1} = \{\cdots, -3, -1, 1, 3, \cdots\}$

b. $\overline{0} = \{\cdots, -3, 0, 3, \cdots\}, \quad \overline{1} = \{\cdots, -5, -2, 1, 4, \cdots\}, \quad \overline{2} = \{\cdots, -1, 2, 5, \cdots\}$

c. $\overline{0} = \{\cdots, -5, 0, 5, \cdots\}, \quad \overline{1} = \{\cdots, -9, -4, 1, 6, \cdots\}, \quad \overline{2} = \{\cdots, -3, 2, 7, \cdots\},$
$\overline{3} = \{\cdots, -7, -2, 3, 8, \cdots\}, \quad \overline{4} = \{\cdots, -1, 4, 9, \cdots\}$

37. 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. Introduction and Examples

1. $i^3 = i^2 \cdot i = -1 \cdot i = -i$ **2.** $i^4 = (i^2)^2 = (-1)^2 = 1$ **3.** $i^{23} = (i^2)^{11} \cdot i = (-1)^{11} \cdot i = (-1)i = -i$

4. $(-i)^{35} = (i^2)^{17}(-i) = (-1)^{17}(-i) = (-1)(-i) = i$

5. $(4-i)(5+3i) = 20 + 12i - 5i - 3i^2 = 20 + 7i + 3 = 23 + 7i$

6. $(8+2i)(3-i) = 24 - 8i + 6i - 2i^2 = 24 - 2i - 2(-1) = 26 - 2i$

7. $(2-3i)(4+i) + (6-5i) = 8 + 2i - 12i - 3i^2 + 6 - 5i = 14 - 15i - 3(-1) = 17 - 15i$

8. $(1+i)^3 = (1+i)^2(1+i) = (1+2i-1)(1+i) = 2i(1+i) = 2i^2 + 2i = -2 + 2i$

9. $(1-i)^5 = 1^5 + \frac{5}{1}1^4(-i) + \frac{5\cdot4}{2\cdot1}1^3(-i)^2 + \frac{5\cdot4}{2\cdot1}1^2(-i)^3 + \frac{5}{1}1^1(-i)^4 + (-i)^5 = 1 - 5i + 10i^2 - 10i^3 + 5i^4 - i^5 = 1 - 5i - 10 + 10i + 5 - i = -4 + 4i$

10. $|3-4i| = \sqrt{3^2 + (-4)^2} = \sqrt{9+16} = \sqrt{25} = 5$ 11. $|6+4i| = \sqrt{6^2 + 4^2} = \sqrt{36+16} = \sqrt{52} = 2\sqrt{13}$

12. $|3-4i| = \sqrt{3^2 + (-4)^2} = \sqrt{25} = 5$ and $3 - 4i = 5(\frac{3}{5} - \frac{4}{5}i)$

13. $|-1+i| = \sqrt{(-1)^2 + 1^2} = \sqrt{2}$ and $-1 + i = \sqrt{2}(-\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i)$

14. $|12+5i| = \sqrt{12^2 + 5^2} = \sqrt{169}$ and $12 + 5i = 13(\frac{12}{13} + \frac{5}{13}i)$

15. $|-3+5i| = \sqrt{(-3)^2 + 5^2} = \sqrt{34}$ and $-3 + 5i = \sqrt{34}(-\frac{3}{\sqrt{34}} + \frac{5}{\sqrt{34}}i)$

16. $|z|^4(\cos 4\theta + i\sin 4\theta) = 1(1+0i)$ so $|z| = 1$ and $\cos 4\theta = 1$ and $\sin 4\theta = 0$. Thus $4\theta = 0 + n(2\pi)$ so $\theta = n\frac{\pi}{2}$ which yields values $0, \frac{\pi}{2}, \pi$, and $\frac{3\pi}{2}$ less than 2π. The solutions are

$$z_1 = \cos 0 + i\sin 0 = 1, \qquad z_2 = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i,$$

$$z_3 = \cos\pi + i\sin\pi = -1, \text{ and } z_4 = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} = -i.$$

17. $|z|^4(\cos 4\theta + i\sin 4\theta) = 1(-1+0i)$ so $|z| = 1$ and $\cos 4\theta = -1$ and $\sin 4\theta = 0$. Thus $4\theta = \pi + n(2\pi)$ so $\theta = \frac{\pi}{4} + n\frac{\pi}{2}$ which yields values $\frac{\pi}{4}, \frac{3\pi}{4}, \frac{5\pi}{4}$, and $\frac{7\pi}{4}$ less than 2π. The solutions are

$$z_1 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i, \qquad z_2 = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i,$$

$$z_3 = \cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = -\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i, \text{ and } z_4 = \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4} = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}i.$$

18. $|z|^3(\cos 3\theta + i\sin 3\theta) = 8(-1+0i)$ so $|z| = 2$ and $\cos 3\theta = -1$ and $\sin 3\theta = 0$. Thus $3\theta = \pi + n(2\pi)$ so $\theta = \frac{\pi}{3} + n\frac{2\pi}{3}$ which yields values $\frac{\pi}{3}, \pi$, and $\frac{5\pi}{3}$ less than 2π. The solutions are

$$z_1 = 2(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}) = 2(\frac{1}{2} + \frac{\sqrt{3}}{2}i) = 1 + \sqrt{3}i, \qquad z_2 = 2(\cos\pi + i\sin\pi) = 2(-1+0i) = -2,$$

and

$$z_3 = 2(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}) = 2(\frac{1}{2} - \frac{\sqrt{3}}{2}i) = 1 - \sqrt{3}i.$$

19. $|z|^3(\cos 3\theta + i\sin 3\theta) = 27(0-i)$ so $|z| = 3$ and $\cos 3\theta = 0$ and $\sin 3\theta = -1$. Thus $3\theta = 3\pi/2 + n(2\pi)$ so $\theta = \frac{\pi}{2} + n\frac{2\pi}{3}$ which yields values $\frac{\pi}{2}, \frac{7\pi}{6}$, and $\frac{11\pi}{6}$ less than 2π. The solutions are

$$z_1 = 3(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}) = 3(0+i) = 3i, \qquad z_2 = 3(\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}) = 3(-\frac{\sqrt{3}}{2} - \frac{1}{2}i) = -\frac{3\sqrt{3}}{2} - \frac{3}{2}i$$

and

$$z_3 = 3(\cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6}) = 3(\frac{\sqrt{3}}{2} - \frac{1}{2}i) = \frac{3\sqrt{3}}{2} - \frac{3}{2}i.$$

20. $|z|^6(\cos 6\theta + i\sin 6\theta) = 1 + 0i$ so $|z| = 1$ and $\cos 6\theta = 1$ and $\sin 6\theta = 0$. Thus $6\theta = 0 + n(2\pi)$ so $\theta = 0 + n\frac{2\pi}{6}$ which yields values $0, \frac{\pi}{3}, \frac{2\pi}{3}, \pi, \frac{4\pi}{3}$, and $\frac{5\pi}{3}$ less than 2π. The solutions are

$$z_1 = 1(\cos 0 + i\sin 0) = 1 + 0i = 1, \qquad z_2 = 1(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}) = \frac{1}{2} + \frac{\sqrt{3}}{2}i,$$

$$z_3 = 1(\cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3}) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \qquad z_4 = 1(\cos\pi + i\sin\pi) = -1 + 0i = -1,$$

$$z_5 = 1(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i, \qquad z_6 = 1(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}) = \frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

21. $|z|^6(\cos 6\theta + i\sin 6\theta) = 64(-1+0i)$ so $|z| = 2$ and $\cos 6\theta = -1$ and $\sin 6\theta = 0$. Thus $6\theta = \pi + n(2\pi)$ so $\theta = \frac{\pi}{6} + n\frac{2\pi}{6}$ which yields values $\frac{\pi}{6}, \frac{\pi}{2}, \frac{5\pi}{6}, \frac{7\pi}{6}, \frac{3\pi}{2}$ and $\frac{11\pi}{6}$ less than 2π. The solutions are

$$\begin{aligned}
z_1 &= 2(\cos\frac{\pi}{6} + i\sin\frac{\pi}{6}) = 2(\frac{\sqrt{3}}{2} + \frac{1}{2}i) = \sqrt{3} + i,\\
z_2 &= 2(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}) = 2(0+i) = 2i,\\
z_3 &= 2(\cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6}) = 2(-\frac{\sqrt{3}}{2} + \frac{1}{2}i) = -\sqrt{3} + i,\\
z_4 &= 2(\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}) = 2(-\frac{\sqrt{3}}{2} - \frac{1}{2}i) = -\sqrt{3} - i,\\
z_5 &= 2(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}) = 2(0-i) = -2i,\\
z_6 &= 2(\cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6}) = 2(\frac{\sqrt{3}}{2} - \frac{1}{2}i) = \sqrt{3} - i.
\end{aligned}$$

22. $10 + 16 = 26 > 17$, so $10 +_{17} 16 = 26 - 17 = 9$.

23. $8 + 6 = 14 > 10$, so $8 +_{10} 6 = 14 - 10 = 4$.

24. $20.5 + 19.3 = 39.8 > 25$, so $20.5 +_{25} 19.3 = 39.8 - 25 = 14.8$.

25. $\frac{1}{2} + \frac{7}{8} = \frac{11}{8} > 1$, so $\frac{1}{2} +_1 \frac{7}{8} = \frac{11}{8} - 1 = \frac{3}{8}$.

26. $\frac{3\pi}{4} + \frac{3\pi}{2} = \frac{9\pi}{4} > 2\pi$, so $\frac{3\pi}{4} +_{2\pi} \frac{3\pi}{2} = \frac{9\pi}{4} - 2\pi = \frac{\pi}{4}$.

27. $2\sqrt{2}+3\sqrt{2}=5\sqrt{2}>\sqrt{32}=4\sqrt{2}$, so $2\sqrt{2}+_{\sqrt{32}}\ 3\sqrt{2}=5\sqrt{2}-4\sqrt{2}=\sqrt{2}$.

28. 8 is not in $\mathbb{R}_6$ because $8>6$, and we have only defined $a+_6 b$ for $a,b\in\mathbb{R}_6$.

29. We need to have $x+7=15+3$, so $x=11$ will work. It is easily checked that there is no other solution.

30. We need to have $x+\frac{3\pi}{2}=2\pi+\frac{3\pi}{4}=\frac{11\pi}{4}$, so $x=\frac{5\pi}{4}$ will work. It is easy to see there is no other solution.

31. We need to have $x+x=7+3=10$, so $x=5$ will work. It is easy to see that there is no other solution.

32. We need to have $x+x+x=7+5$, so $x=4$ will work. Checking the other possibilities 0, 1, 2, 3, 5, and 6, we see that this is the only solution.

33. An obvious solution is $x=1$. Otherwise, we need to have $x+x=12+2$, so $x=7$ will work also. Checking the other ten elements, in $\mathbb{Z}_{12}$, we see that these are the only solutions.

34. Checking the elements $0,1,2,3\in\mathbb{Z}_4$, we find that they are all solutions. For example, $3+_4 3+_4 3+_4 3=(3+_4 3)+_4(3+_4 3)=2+_4 2=0$.

35. $\zeta^0\leftrightarrow 0,\quad \zeta^3=\zeta^2\zeta\leftrightarrow 2+_8 5=7,\quad \zeta^4=\zeta^2\zeta^2\leftrightarrow 2+_8 2=4,\quad \zeta^5=\zeta^4\zeta\leftrightarrow 4+_8 5=1,$
$\zeta^6=\zeta^3\zeta^3\leftrightarrow 7+_8 7=6,\quad \zeta^7=\zeta^3\zeta^4\leftrightarrow 7+_8 4=3$

36. $\zeta^0\leftrightarrow 0,\quad \zeta^2=\zeta\zeta\leftrightarrow 4+_7 4=1,\quad \zeta^3=\zeta^2\zeta\leftrightarrow 1+_7 4=5,\quad \zeta^4=\zeta^2\zeta^2\leftrightarrow 1+_7 1=2,$
$\zeta^5=\zeta^3\zeta^2\leftrightarrow 5+_7 1=6,\quad \zeta^6=\zeta^3\zeta^3\leftrightarrow 5+_7 5=3$

37. If there were an isomorphism such that $\zeta\leftrightarrow 4$, then we would have $\zeta^2\leftrightarrow 4+_6 4=2$ and $\zeta^4=\zeta^2\zeta^2\leftrightarrow 2+_6 2=4$ again, contradicting the fact that an isomorphism $\leftrightarrow$ must give a *one-to-one correpondence*.

38. By Euler's fomula, $e^{ia}e^{ib}=e^{i(a+b)}=\cos(a+b)+i\sin(a+b)$. Also by Euler's formula,

$$\begin{aligned} e^{ia}e^{ib} &= (\cos a+i\sin a)(\cos b+i\sin b)\\ &= (\cos a\cos b-\sin a\sin b)+i(\sin a\cos b+\cos a\sin b). \end{aligned}$$

The desired formulas follow at once.

39. (See the text answer.)

40. a. We have $e^{3\theta}=\cos 3\theta+i\sin 3\theta$. On the other hand,

$$\begin{aligned} e^{3\theta} &= (e^{\theta})^3=(\cos\theta+i\sin\theta)^3\\ &= \cos^3\theta+3i\cos^2\theta\sin\theta-3\cos\theta\sin^2\theta-i\sin^3\theta\\ &= (\cos^3\theta-3\cos\theta\sin^2\theta)+i(3\cos^2\theta\sin\theta-\sin^3\theta). \end{aligned}$$

Comparing these two expressions, we see that

$$\cos 3\theta=\cos^3\theta-3\cos\theta\sin^2\theta.$$

b. From Part(**a**), we obtain

$$\cos 3\theta=\cos^3\theta-3(\cos\theta)(1-\cos^2\theta)=4\cos^3\theta-3\cos\theta.$$

2. Binary Operations

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

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 $d * d = d$.

7. It is not commutative because $1-2 \neq 2-1$. It is not associative because $2 = 1-(2-3) \neq (1-2)-3 = -4$.

8. It is commutative because $ab + 1 = ba + 1$ for all $a, b \in \mathbb{Q}$. It is not associative because $(a * b) * c = (ab + 1) * c = abc + c + 1$ but $a * (b * c) = a * (bc + 1) = abc + a + 1$, and we need not have $a = c$.

9. It is commutative because $ab/2 = ba/2$ for all $a, b \in \mathbb{Q}$. It is associative because $a*(b*c) = a*(bc/2) = [a(bc/2)]/2 = abc/4$, and $(a * b) * c = (ab/2) * c = [(ab/2)c]/2 = abc/4$ also.

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 $a * (b * c) = a * 2^{bc} = 2^{a(2^{bc})}$.

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 $b, c \in \mathbb{Z}^+$.

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. 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 $a, b \in S$.

15. The definition is correct.

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

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

18. This does define a binary operation.

19. This does define a binary operation.

20. This does define a binary operation.

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

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

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

24. F T F F F T T T T F **25.** (See the answer in the text.)

26. 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.

27. 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.

28.

$*$	a	b
a	b	a
b	a	a

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

29. 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.

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

31. 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 $[(f - g) - h](x) = (f - g)(x) - h(x) = f(x) - g(x) - h(x) = 2x - 5x - 8x = -11x$.

32. 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.

33. 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.

34. It is not commutative. Let $f(x) = x^2$ and $g(x) = x + 1$. Then $(f \circ g)(3) = f(g(3)) = f(4) = 16$ but $(g \circ f)(3) = g(f(3)) = g(9) = 10$.

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

36. 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 $(a * b) \in H$.

37. 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 $(a * b) \in H$.

3. Isomorphic Binary Structures

1. i) ϕ must be one to one. ii) $\phi[S]$ must be all of S'. iii) $\phi(a * b) = \phi(a) *' \phi(b)$ for all $a, b \in S$.

2. It is an isomorphism; ϕ is one to one, onto, and $\phi(n+m) = -(n+m) = (-n) + (-m) = \phi(n) + \phi(m)$ for all $m, n \in \mathbb{Z}$.

3. It is not an isomorphism; ϕ does not map $\mathbb{Z}$ onto $\mathbb{Z}$. For example, $\phi(n) \neq 1$ for all $n \in \mathbb{Z}$.

4. It is not an isomorphism because $\phi(m+n) = m+n+1$ while $\phi(m)+\phi(n) = m+1+n+1 = m+n+2$.

5. It is an isomorphism; ϕ is one to one, onto, and $\phi(a+b) = \frac{a+b}{2} = \frac{a}{2} + \frac{b}{2} = \phi(a) + \phi(b)$.

6. It is not an isomorphism because ϕ does not map $\mathbb{Q}$ onto $\mathbb{Q}$. $\phi(a) \neq -1$ for all $a \in \mathbb{Q}$.

7. It is an isomorphism because ϕ is one to one, onto, and $\phi(xy) = (xy)^3 = x^3y^3 = \phi(x)\phi(y)$.

8. It is not an isomorphism because ϕ is not one to one. All the 2×2 matrices where the entries in the second row are double the entries above them in the first row are mapped into 0 by ϕ.

9. It is an isomorphism because for 1×1 matrices, $[a][b] = [ab]$, and $\phi([a]) = a$ so ϕ just removes the brackets.

10. It is an isomorphism. For any base $a \neq 1$, the exponential function $f(x) = a^x$ maps $\mathbb{R}$ one to one onto $\mathbb{R}^+$, and ϕ is the exponential map with $a = 0.5$. We have $\phi(r+s) = 0.5^{(r+s)} = (0.5^r)(0.5^s) = \phi(r)\phi(s)$.

11. It is not an isomorphism because ϕ is not one to one; $\phi(x^2) = 2x$ and $\phi(x^2+1) = 2x$.

12. It is not an isomorphism because ϕ is not one to one: $\phi(\sin x) = \cos 0 = 1$ and $\phi(x) = 1$.

13. No, because ϕ does not map F onto F. For all $f \in F$, we see that $\phi(f)(0) = 0$ so, for example, no function is mapped by ϕ into $x + 1$.

14. It is an isomorphism. By calculus, $\phi(f) = f$, so ϕ is the identity map which is always an isomorphism of a binary structure with itself.

15. It is not an isomorphism because ϕ does not map F onto F. Note that $\phi(f)(0) = 0 \cdot f(0) = 0$. Thus there is no element of F that is mapped by ϕ into the constant function 1.

16. **a.** For ϕ to be an isomorphism, we must have

$$m * n = \phi(m-1) * \phi(n-1) = \phi((m-1) + (n-1)) = \phi(m+n-2) = m+n-1.$$

The identity element is $\phi(0) = 1$.

b. Using the fact that ϕ^{-1} must also be an isomorphism, we must have

$$m * n = \phi^{-1}(m+1) * \phi^{-1}(n+1) = \phi^{-1}((m+1) + (n+1)) = \phi^{-1}(m+n+2) = m+n+1.$$

The identity element is $\phi^{-1}(0) = -1$.

17. **a.** For ϕ to be an isomorphism, we must have

$$m * n = \phi(m-1) * \phi(n-1) = \phi((m-1) \cdot (n-1)) = \phi(mn - m - n + 1) = mn - m - n + 2.$$

The identity element is $\phi(1) = 2$.

b. Using the fact that ϕ^{-1} must also be an isomorphism, we must have

$$m * n = \phi^{-1}(m+1) * \phi^{-1}(n+1) = \phi^{-1}((m+1) \cdot (n+1)) = \phi^{-1}(mn + m + n + 1) = mn + m + n.$$

The identity element is $\phi^{-1}(1) = 0$.

18. **a.** For ϕ to be an isomorphism, we must have

$$a * b = \phi\left(\frac{a+1}{3}\right) * \phi\left(\frac{b+1}{3}\right) = \phi\left(\frac{a+1}{3} + \frac{b+1}{3}\right) = \phi\left(\frac{a+b+2}{3}\right) = a+b+1.$$

The identity element is $\phi(0) = -1$.

b. Using the fact that ϕ^{-1} must also be an isomorphism, we must have

$$a * b = \phi^{-1}(3a-1) * \phi^{-1}(3b-1) = \phi^{-1}((3a-1) + (3b-1)) = \phi^{-1}(3a+3b-2) = a+b-\frac{1}{3}.$$

The identity element is $\phi^{-1}(0) = 1/3$.

19. **a.** For ϕ to be an isomorphism, we must have

$$a * b = \phi\left(\frac{a+1}{3}\right) * \phi\left(\frac{b+1}{3}\right) = \phi\left(\frac{a+1}{3} \cdot \frac{b+1}{3}\right) = \phi\left(\frac{ab+a+b+1}{9}\right) = \frac{ab+a+b-2}{3}.$$

The identity element is $\phi(1) = 2$.

b. Using the fact that ϕ^{-1} must also be an isomorphism, we must have

$$a * b = \phi^{-1}(3a-1) \cdot \phi^{-1}(3b-1) = \phi^{-1}((3a-1) \cdot (3b-1)) = \phi^{-1}(9ab - 3a - 3b + 1) = 3ab - a - b + \frac{2}{3}.$$

The identity element is $\phi^{-1}(1) = 2/3$.

20. Computing $\phi(x * y)$ is done by first executing the binary operation $*$, and then performing the map ϕ. Computing $\phi(x) *' \phi(y)$ is done by first performing the map ϕ, and then executing the binary operation $*'$. Thus, reading in left to right order of peformance, the isomorphism property is

$$\text{(binary operation)(map)} = \text{(map)(binary operation)}$$

which has the formal appearance of commutativity.

21. The definition is incorrect. It should be stated that $\langle S, * \rangle$ and $\langle S', *' \rangle$ are binary structures, ϕ must be one to one and onto S', and the universal quantifier "for all $a, b \in S$" should appear in an appropriate place.

Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary structures. A map $\phi : S \to S'$ is an **isomorphism** if and only if ϕ is one to one and onto S', and $\phi(a * b) = \phi(a) *' \phi(b)$ for all $a, b \in S$.

22. It is badly worded. The "for all $s \in S$" applies to the equation and not to the "is an identity for $*$".

Let $*$ be a binary operation on a set S. An element e of S is an **identity element** for $*$ if and only if $s * e = e * s = s$ for all $s \in S$.

23. Suppose that e and $\overline{e}$ are two identity elements and, viewing each in turn as an identity element, compute $e * \overline{e}$ in two ways.

24. a. Let $*$ be a binary operation on a set S. An element e_L of S is a **left identity element** for $*$ if and only if $e_L * s = s$ for all $s \in S$.

b. Let $*$ be a binary operation on a set S. An element e_R of S is a **right identity element** for $*$ if and only if $s * e_R = s$ for all $s \in S$.

A one-sided identity element is not unique. Let $*$ be defined on S by $a * b = a$ for all $a, b \in S$. Then every $b \in S$ is a right identity. Similarly, a left identity is not unique. If in the proof of Theorem 3.13, we replace e by e_L and $\overline{e}$ by $\overline{e}_L$ everywhere, and replace the word "identity" by "left identity", the first incorrect statement would be, "However, regarding $\overline{e}_L$ as left identity element, we must have $e_L * \overline{e}_L = e_L$."

25. No, if $\langle S* \rangle$ has a left identity element e_L and a right identity element e_R, then $e_L = e_R$.

Proof Because e_L is a left identity element we have $e_L * e_R = e_R$, but viewing e_R as right identity element, $e_L * e_R = e_L$. Thus $e_L = e_R$.

26. *One-to-one:* Suppose that $\phi^{-1}(a') = \phi^{-1}(b')$ for $a', b' \in S'$. Then $a' = \phi(\phi^{-1}(a')) = \phi(\phi^{-1}(b')) = b'$, so ϕ^{-1} is one to one.

Onto: Let $a \in S$. Then $\phi^{-1}(\phi(a)) = a$, so ϕ^{-1} maps S' onto S.

Homomorphism property: Let $a', b' \in S'$. Now

$$\phi(\phi^{-1}(a' *' b')) = a' *' b'.$$

Because ϕ is an isomorphism,

$$\phi(\phi^{-1}(a') * \phi^{-1}(b\ ,')) = \phi(\phi^{-1}(a')) *' \phi(\phi^{-1}(b')) = a' *' b'$$

also. Because ϕ is one to one, we conclude that

$$\phi^{-1}(a' * b') = \phi^{-1}(a') *' \phi^{-1}(b').$$

27. *One-to-one:* Let $a, b \in S$ and suppose $(\psi \circ \phi)(a) = (\psi \circ \phi)(b)$. Then $\psi(\phi(a)) = \psi(\phi(b))$. Because ψ is one to one, we conclude that $\phi(a) = \phi(b)$. Because ϕ is one to one, we must have $a = b$.

Onto: Let $a'' \in S''$. Because ψ maps S' onto S'', there exists $a' \in S'$ such that $\psi(a') = a''$. Because ϕ maps S onto S', there exists $a \in S$ such that $\phi(a) = a'$. Then $(\psi \circ \phi)(a) = \psi(\phi(a)) = \psi(a') = a''$, so $\psi \circ \phi$ maps S onto S''.

Homomorphism property: Let $a, b \in S$. Since ϕ and ψ are isomorphisms, $(\psi \circ \phi)(a * b) = \psi(\phi(a * b)) = \psi(\phi(a) *' \phi(b)) = \psi(\phi(a)) *'' \psi(\phi(b)) = (\psi \circ \phi)(a) *'' (\psi \circ \phi)(b)$.

28. Let $\langle S, * \rangle, \langle S', *' \rangle$ and $\langle S'', *'' \rangle$ be binary structures.

Reflexive: Let $\iota : S \to S$ be the identity map. Then ι maps S one to one onto S and for $a, b \in S$, we have $\iota(a * b) = a * b = \iota(a) * \iota(b)$, so ι is an isomorphism of S with itself, that is $S \simeq S$.

Symmetric: If $S \simeq S'$ and $\phi : S \to S'$ is an isomorphism, then by Exercise 26, $\phi^{-1} : S' \to S$ is an isomorphism, so $S' \simeq S$.

Transitive: Suppose that $S \simeq S'$ and $S' \simeq S''$, and that $\phi : S \to S'$ and $\psi : S' \to S''$ are isomorphisms. By Exercise 27, we know that $\psi \circ \phi : S \to S''$ is an isomorphism, so $S \simeq S''$.

29. Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be isomorphic binary structures and let $\phi : S \to S'$ be an isomorphism. Suppose that $*$ is commutative. Let $a', b' \in S'$ and let $a, b \in S$ be such that $\phi(a) = a'$ and $\phi(b) = b'$. Then $a' *' b' = \phi(a) *' \phi(b) = \phi(a * b) = \phi(b * a) = \phi(b) *' \phi(a) = b' * a'$, showing that $*'$ is commutative.

30. Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be isomorphic binary structures and let $\phi : S \to S'$ be an isomorphism. Suppose that $*$ is associative. Let $a', b', c' \in S'$ and let $a, b, c \in S$ be such that $\phi(a) = a', \phi(b) = b'$ and $\phi(c) = c'$. Then

$$\begin{aligned} (a' *' b') *' c' &= (\phi(a) *' \phi(b)) *' \phi(c) = \phi(a * b) *' \phi(c) = \phi((a * b) * c)) \\ &= \phi(a * (b * c)) = \phi(a) *' \phi(b * c) = \phi(a) *' (\phi(b) *' \phi(c)) = a' *' (b' *' c'), \end{aligned}$$

showing that $*'$ is associative.

31. Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be isomorphic binary structures and let $\phi : S \to S'$ be an isomorphism. Suppose that S has the property that for each $c \in S$ there exists $x \in S$ such that $x * x = c$. Let $c' \in S'$, and let $c \in S$ such that $\phi(c) = c'$. Find $x \in S$ such that $x * x = c$. Then $\phi(x * x) = \phi(c) = c'$, so $\phi(x) *' \phi(x) = c'$. If we denote $\phi(x)$ by x', then we see that $x' *' x' = c'$, so S' has the analagous property.

32. Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be isomorphic binary structures and let $\phi : S \to S'$ be an isomorphism. Suppose that S has the property that there exists $b \in S$ such that $b * b = b$. Let $b' = \phi(b)$. Then $b' *' b' = \phi(b) *' \phi(b) = \phi(b * b) = \phi(b) = b'$, so S' has the analogous property.

33. Let $\phi : \mathbb{C} \to H$ be defined by $\phi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{R}$. Clearly ϕ is one to one and onto H.

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

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

34. Let the set be $\{a, b\}$. We need to decide whether interchanging the names of the letters everywhere in the table and then writing the table again in the order a first and b second gives the same table or a different table. The same table is obtained if and only if in the body of the table, diagonally opposite entries are different. Four such tables exist, since there are four possible choices for the first row; Namely, the tables

$*$	a	b
a	a	a
b	b	b

$*$	a	b
a	a	b
b	a	b

$*$	a	b
a	b	a
b	b	a

and

$*$	a	b
a	b	b
b	a	a

.

The other 12 tables can be paired off into tables giving the same algebraic structure. One table of each pair is listed below. The number of different algebraic structures is therefore $4 + 12/2 = 10$.

$*$	a	b
a	a	a
b	a	a

$*$	a	b
a	a	a
b	a	b

$*$	a	b
a	a	a
b	b	a

$*$	a	b
a	a	b
b	a	a

$*$	a	b
a	b	a
b	a	a

$*$	a	b
a	a	b
b	b	a

4. Groups

1. No. G_3 fails. **2.** Yes **3.** No. G_1 fails. **4.** No. G_3 fails. **5.** No. G_1 fails.

6. No. G_2 fails.

7. The group $\langle U_{1000}, \cdot\rangle$ of solutions of $z^{1000} = 1$ in $\mathbb{C}$ under multiplication has 1000 elements and is abelian.

8.

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

9. Denoting the operation in each of the three groups by $*$ and the identity element by e for the moment, the equation $x*x*x*x = e$ has four solutions in $\langle U, \cdot\rangle$, one solution in $\langle \mathbb{R}, +\rangle$, and two solutions in $\langle \mathbb{R}^*, \cdot\rangle$.

10. **a.** *Closure:* Let nr and ns be two elements of $n\mathbb{Z}$. Now $nr + ns = n(r+s) \in n\mathbb{Z}$ so $n\mathbb{Z}$ is closed under addition.

Associative: We know that addition of integers is associative.

Identity: $0 = n0 \in n\mathbb{Z}$, and 0 is the additive identity element.

Inverses: For each $nm \in n\mathbb{Z}$, we also have $n(-m) \in n\mathbb{Z}$ and $nm + n(-m) = n(m-m) = n0 = 0$.

b. Let $\phi : \mathbb{Z} \to n\mathbb{Z}$ be defined by $\phi(m) = nm$ for $m \in \mathbb{Z}$. Clearly ϕ is one to one and maps $\mathbb{Z}$ onto $n\mathbb{Z}$. For $r, s \in \mathbb{Z}$, we have $\phi(r+s) = n(r+s) = nr + ns = \phi(r) + \phi(s)$. Thus ϕ is an isomorphism of $\langle \mathbb{Z}, + \rangle$ with $\langle n\mathbb{Z}, + \rangle$.

11. Yes, it is a group. Addition of diagonal matrices amounts to adding in $\mathbb{R}$ entries in corresponding positions on the diagonals, and that addition is associative. The matrix with all entries 0 is the additive identity, and changing the sign of the entries in a matrix yields the additive inverse of the matrix.

12. No, it is not a group. Multiplication of diagonal matrices amounts to muliplying in $\mathbb{R}$ entries in corresponding positions on the diagonals. The matrix with 1 at all places on the diagonal is the identity element, but a matrix having a diagonal entry 0 has no inverse.

13. Yes, it is a group. See the answer to Exercise 12.

14. Yes, it is a group. See the answer to Exercise 12.

15. No. The matrix with all entries 0 is upper triangular, but has no inverse.

16. Yes, it is a group. The sum of upper-triangular matrices is again upper triangular, and addition amounts to just adding entries in $\mathbb{R}$ in corresponding positions.

17. Yes, it is a group.

Closure: Let A and B be upper triangular with determinant 1. Then entry c_{ij} in row i and column j in $C = AB$ is 0 if $i > j$, because for each product $a_{ik}b_{kj}$ where $i > j$ appearing in the computation of c_{ij}, either $k < i$ so that $a_{ik} = 0$ or $k \geq i > j$ so that $b_{kj} = 0$. Thus the product of two upper-triangular matrices is again upper triangular. The equation $\det(AB) = \det(A) \cdot \det(B)$, shows that the product of two matrices of determinant 1 again has determinant 1.

Associative: We know that matrix multiplication is associative.

Identity: The $n \times n$ identity matrix I_n has determinant 1 and is upper triangular.

Inverse: The product property $1 = \det(I_n) = \det(A^{-1}A) = \det(A^{-1}) \cdot \det(A)$ shows that if $\det(A) = 1$, then $\det(A^{-1}) = 1$ also.

18. Yes, it is a group. The relation $\det(AB) = \det(A) \cdot \det(B)$ show that the set of $n \times n$ matrices with determinant ± 1 is closed under multiplication. We know matrix multiplication is associative, and $\det(I_n) = 1$. As in the preceding solution, we see that $\det(A) = \pm 1$ implies that $\det(A^{-1}) = \pm 1$, so we have a group.

19. a. We must show that S is closed under $*$, that is, that $a+b+ab \neq -1$ for $a, b \in S$. Now $a+b+ab = -1$ if and only if $0 = ab + a + b + 1 = (a+1)(b+1)$. This is the case if and only if either $a = -1$ or $b = -1$, which is not the case for $a, b \in S$.

b. *Associative:* We have

$$a * (b * c) = a * (b + c + bc) = a + (b + c + bc) + a(b + c + bc) = a + b + c + ab + ac + bc + abc$$

and

$$(a * b) * c = (a + b + ab) * c = (a + b + ab) + c + (a + b + ab)c = a + b + c + ab + ac + bc + abc.$$

Identity: 0 acts as identity elemenr for $*$, for $0 * a = a * 0 = a$.

Inverses: $\frac{-a}{a+1}$ acts as inverse of a, for

$$a * \frac{-a}{a+1} = a + \frac{-a}{a+1} + a\frac{-a}{a+1} = \frac{a(a+1) - a - a^2}{a+1} = \frac{0}{a+1} = 0.$$

c. Because the operation is commutative, $2 * x * 3 = 2 * 3 * x = 11 * x$. Now the inverse of 11 is -11/12 by Part(**b**). From $11 * x = 7$, we obtain

$$x = \frac{-11}{12} * 7 = \frac{-11}{12} + 7 + \frac{-11}{12}7 = \frac{-11 + 84 - 77}{12} = \frac{-4}{12} = -\frac{1}{3}.$$

20.

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table I

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Table II

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Table III

Table I is structurally different from the others because every element is its own inverse. Table II can be made to look just like Table III by interchanging the names a and b everywhere to obtain

	e	b	a	c
e	e	b	a	c
b	b	e	c	a
a	a	c	b	e
c	c	a	e	b

and rewriting this table in the order e, a, b, c.

a. The symmetry of each table in its main diagonal shows that all groups of order 4 are commutative.

b. Table III gives the group U_4, upon replacing e by 1, a by i, b by -1, and c by $-i$.

c. Take $n = 2$. There are four 2×2 diagonal matrices with entries ± 1, namely

$$E = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, A = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \text{ and } C = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

If we write the table for this group using the letters E, A, B, C in that order, we obtain Table I with the letters capitalized.

21. A binary operation on a set $\{x, y\}$ of two elements that produces a group is completely determined by the choice of x or y to serve as identity element, so just 2 of the 16 possible tables give groups. For a set $\{x, y, z\}$ of three elements, a group binary operation is again determined by the choice x, y, or z to serve as identity element, so there are just 3 of the 19,683 binary operations that give groups. (Recall that there is only one way to fill out a group table for $\{e, a\}$ and for $\{e, a, b\}$ if you require e to be the identity element.)

22. The orders $G_1G_3G_2, G_3G_1G_2$, and $G_3G_2G_1$ are not acceptable. The identity element e occurs in the statement of G_3, which must not come before e is defined in G_2.

23. Ignoring spelling, punctuation and grammar, here are some of the mathematical errors.

a. The statement "x = identity" is wrong.

b. The identity element should be e, not (e). It would also be nice to give the properties satisfied by the identity element and by inverse elements.

c. Associativity is missing. Logically, the identity element should be mentioned before inverses. The statement "an inverse exists" is not quantified correctly: for each element of the set, an inverse exists. Again, it would be nice to give the properties satisfied by the identity element and by inverse elements.

d. Replace " such that for all $a, b \in G$" by " if for all $a \in G$". Delete "under addition" in line 2. The element should be e, not $\{e\}$. Replace "$= e$" by "$= a$" in line 3.

24. We need only make a table that has e as an identity element and has an e in each row and each column of the body of the table to satisfy axioms G_2 and G_3. Then we make some row or column contain some element twice, and it can't be a group, so G_1 must fail.

$*$	e	a	b
e	e	a	b
a	a	e	b
b	b	a	e

25. F T T F F T T T F T

26. Multiply both sides of the equation $a * b = a * c$ on the left by the inverse of a, and simplify, using the axioms for a group.

27. Show that $x = a' * b$ is a solution of $a * x = b$ by substitution and the axioms for a group. Then show that it is the only solution by multiplying both sides of the equation $a * x = b$ on the left by a' and simplifying, using the axioms for a group.

28. Let $\phi : G \to G'$ be a group isomorphism of $\langle G, * \rangle$ onto $\langle G', *' \rangle$, and let $a, a' \in G$ such that $a * a' = e$. Then $\phi(e) = \phi(a * a') = \phi(a) *' \phi(a')$. Now $\phi(e)$ is the identity element of G' by Theorem 3.14. Thus the equation $\phi(a) *' \phi(a') = \phi(e)$ shows that $\phi(a)$ and $\phi(a')$ are inverse pairs in G', which was to be shown.

29. Let $S = \{x \in G \mid x' \neq x\}$. Then S has an even number of elements, because its elements can be grouped in pairs x, x'. Because G has an even number of elements, the number of elements in G but not in S (the set $G - S$) must be even. The set $G - S$ is nonempty because it contains e. Thus there is at least one element of $G - S$ other than e, that is, at least one element other than e that is its own inverse.

30. **a.** We have $(a * b) * c = (|a|\, b) * c\ |(|a|b)|c = |\, ab|c$. We also have a $*(b * c) = a * (|\, b|c) = |a||\, b|c = |\, ab|c$, so $*$ is associative.

b. We have $1 * a = |1|\, a = a$ for all $a \in \mathbb{R}^*$ so 1 is a left identity element. For $a \in \mathbb{R}^*, 1/|\, a|$ is a right inverse.

c. It is not a group because both 1/2 and -1/2 are right inverse of 2.

d. The one-sided definition of a group, mentioned just before the exercises, must be all left sided or all right sided. We must not mix them.

31. Let $\langle G, * \rangle$ be a group and let $x \in G$ such that $x * x = x$. Then $x * x = x * e$, and by left cancellation, $x = e$, so e is the only idempotent element in a group.

32. We have $e = (a*b)*(a*b)$, and $(a*a)*(b*b) = e*e = e$ also. Thus $a*b*a*b = a*a*b*b$. Using left and right cancellation, we have $b*a = a*b$.

33. Let $P(n) = (a*b)^n = a^n * b^n$. Since $(a*b)^1 = a*b = a^1*b^1$, we see $P(1)$ is true. Suppose $P(k)$ is true. Then $(a*b)^{k+1} = (a*b)^k*(a*b) = (a^k*b^k)*(a*b) = [a^k*(b^k*a)]*b = [a^k*(a*b^k]*b = [(a^k*a)*b^k]*b = (a^{k+1}*b^k)*b = a^{k+1}*(b^k*b) = a^{k+1}*b^{k+1}$. This completes the induction argument.

34. The elements $e, a, a^2, a^3, \cdots, a^m$ aren't all different since G has only m elements. If one of $a, a^2, a^3, \cdots, a^m$ is e, then we are done. If not, then we must have $a^i = a^j$ where $i < j$. Repeated left cancellation of a yields $e = a^{j-i}$.

35. We have $(a*b)*(a*b) = (a*a)*(b*b)$, so $a*[b*(a*b)] = a*[a*(b*b)]$ and left cancellation yields $b*(a*b) = a*(b*b)$. Then $(b*a)*b = (a*b)*b$ and right cancellation yields $b*a = a*b$.

36. Let $a*b = b*a$. Then $(a*b)' = (b*a)' = a'*b'$ by Corollary 4.17. Conversely, if $(a*b)' = a'*b'$, then $b'*a' = a'*b'$. Then $(b'*a')' = (a'*b')'$ so $(a')'*(b')' = (b')'*(a')'$ and $a*b = b*a$.

37. We have $a*b*c = a*(b*c) = e$, which implies that $b*c$ is the inverse of a. Therefore $(b*c)*a = b*c*a = e$ also.

38. We need to show that a left identity element is a right identity element and that a left inverse is a right inverse. Note that $e*e = e$. Then $(x'*x)*e = x'*x$ so $(x')'*(x'*x)*e = (x')'*(x'*x)$. Using associativity, $[(x')'*x']*x*e = [(x')'*x']*x$. Thus $(e*x)*e = e*x$ so $x*e = x$ and e is a right identity element also. If $a'*a = e$, then $(a'*a)*a' = e*a' = a'$. Multiplication of $a'*a*a' = a'$ on the left by $(a')'$ and associativity yield $a*a' = e$, so a' is also a right inverse of a.

39. Using the hint, we show there is a left identity element and that each element has a left inverse. Let $a \in G$; we are given that G is nonempty. Let e be a solution of $y*a = a$. We show at $e*b = b$ for any $b \in G$. Let c be a solution of the equation $a*x = b$. Then $e*b = e*(a*c) = (e*a)*c = a*c = b$. Thus e is a left identity. Now for each $a \in G$, let a' be a solution of $y*a = e$. Then a' is a left inverse of a. By Exercise 38, G is a group.

40. It is easy to see that $\langle G, *\rangle$ is a group, because the order of multiplication in G is simply reversed: $(a*b)*c = a*(b*c)$ follows at once from $c\cdot(b\cdot a) = (c\cdot b)\cdot a$, the element e continues to act as identity element, and the inverse of each element is unchanged.

Let $\phi(a) = a'$ for $a \in G$, where a' is the inverse of a in the group $\langle G, \cdot\rangle$. Uniqueness of inverses and the fact that $(a')' = a$ show at once that ϕ is one to one and onto G. Also, $\phi(a\cdot b) = (a\cdot b)' = b'\cdot a' = a'*b' = \phi(a)*\phi(b)$, showing that ϕ is an isomorphism of $\langle G, \cdot\rangle$ onto $\langle G, *\rangle$.

41. Let $a, b \in G$. If $g*a*g' = g*b*g'$, then $a = b$ by group cancellation, so i_g is a one-to-one map. Because $i_g(g'*a*g) = g*g'*a*g*g' = a$, we see that i_g maps G onto G. We have $i_g(a*b) = g*a*b*g' = g*a*(g'*g)*b*g' = (g*a*g')*(g*b*g') = i_g(a)*i_g(b)$, so i_g satisfies the homomorphism property also, and is thus an isomorphism.

5. Subgroups

1. Yes **2.** No, there is no identity element. **3.** Yes **4.** Yes **5.** Yes

6. No, the set is not closed under addition. **7.** $\mathbb{Q}^+$ and $\{\pi^n \mid n \in \mathbb{Z}\}$

8. No. If $\det(A) = \det(B) = 2$, then $\det(AB) = \det(A)\det(B) = 4$. The set is not closed under multiplication.

9. Yes **10.** Yes, see Exercise 17 of Section 4.

11. No. If $\det(A) = \det(B) = -1$, then $\det(AB) = \det(A)\det(B) = 1$. The set is not closed under multiplication.

12. Yes, see Exercise 17 of Section 4.

13. Yes. Suppose that $(A^T)A = I_n$ and $(B^T)B = I_n$. Then we have $(AB)^T AB = B^T(A^T A)B = B^T I_n B = B^T B = I_n$, so the set of these matrices is closed under multiplication. Since ${I_n}^T = I_n$ and $I_n I_n = I_n$, the set contains the identity. For each A in the set, the equation $(A^T)A = I_n$ shows that A has an inverse A^T. The equation $(A^T)^T A^T = AA^T = I_n$ shows that A^T is in the given set. Thus we have a subgroup.

14. a) No, $\tilde{F}$ is not closed under addition. b) Yes

15. a) Yes b) No, it is not even a subset of $\tilde{F}$.

16. a) No, it is not closed under addition. b) Yes

17. a) No, it is not closed under addition. b) Yes

18. a) No, it is not closed under addition. b) No, it is not closed under multiplication.

19. a) Yes b) No, the zero constant function is not in $\tilde{F}$.

20. $G_1 \le G_1,\ G_1 < G_4$ $G_2 < G_1,\ G_2 \le G_2,\ G_2 < G_4,\ G_2 < G_7,\ G_2 < G_8$ $G_3 \le G_3,\ G_3 < G_5$
$G_4 \le G_4$ $G_5 \le G_5$ $G_6 \le G_5,\ G_6 \le G_6$ $G_7 < G_1,\ G_7 < G_4,\ G_7 \le G_7$
$G_8 < G_1,\ G_8 < G_4,\ G_8 < G_7,\ G_8 \le G_8$ $G_9 < G_3,\ G_9 < G_5,\ G_9 \le G_9$

21. **a.** -50, -25, 0, 25, 50 **b.** 4, 2, 1, $\frac{1}{2}, \frac{1}{4}$ **c.** $1, \pi, \pi^2, \frac{1}{\pi}, \frac{1}{\pi^2}$ **22.** $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

23. All the matrices $\begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$ for $n \in \mathbb{Z}$. **24.** All the matrices $\begin{bmatrix} 3^n & 0 \\ 0 & 2^n \end{bmatrix}$ for $n \in \mathbb{Z}$.

25. All matrices of the form $\begin{bmatrix} 4^n & 0 \\ 0 & 4^n \end{bmatrix}$ or $\begin{bmatrix} 0 & -2^{2n+1} \\ -2^{2n+1} & 0 \end{bmatrix}$ for $n \in \mathbb{Z}$.

26. G_1 is cyclic with generators 1 and -1. G_2 is not cyclic. G_3 is not cyclic.
G_4 is cyclic with generators 6 and -6. G_5 is cyclic with generators 6 and $\frac{1}{6}$. G_6 is not cyclic.

To get the answers for Exercises 27 - 35, the student computes the given element to succesive powers (or summands). The first power (number of summands) that gives the identity element is the order of the cyclic subgroup. After students have studied Section 9, you might want to come back here and show them the easy way to handle the row permutations of the identity matrix in Exercises 33 - 35 by writing the permutation as a product of disjoint cycles. For example, in Exercise 35, row 1 is in row 4 place, row 4 is in row 2 place, and row 2 is in row 1 place, corresponding to the cycle (1,4,2). Row 3 is left fixed.

27. 4 **28.** 2 **29.** 3 **30.** 5 **31.** 4 **32.** 8 **33.** 2 **34.** 4 **35.** 3

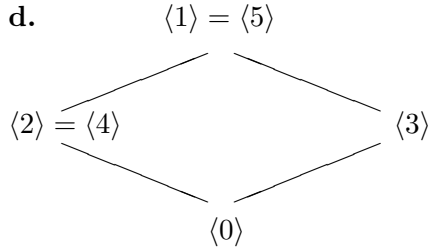
36. a.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

b. $\langle 0\rangle = \{0\}$
$\langle 2\rangle = \langle 4\rangle = \{0, 2, 4\}$
$\langle 3\rangle = \{0, 3\}$
$\langle 1\rangle = \langle 5\rangle = \mathbb{Z}_6$

c. 1 and 5

d.



37. Incorrect, the closure condition must be stated.

A **subgroup** of a group G is a subset H of G that is closed under the induced binary operation from G, contains the identity element e of G, and contains the inverse h^{-1} of each $h \in H$.

38. The definition is correct. **39.** T F T F F F F F T F

40. In the Klein 4-group, the equation $x^2 = e$ has all four elements of the group as solutions.

41. *Closure:* Let $a, b \in H$ so that $\phi(a), \phi(b) \in \phi[H]$. Now $(a * b) \in H$ because $H \leq G$. Since ϕ is an isomorphism, $\phi(a) *' \phi(b) = \phi(a * b) \in \phi[H]$, so $\phi[H]$ is closed under $*'$.

Identity: By Theorem 3.14, $e' = \phi(e) \in \phi[H]$.

Inverses: Let $a \in H$ so that $\phi(a) \in \phi[H]$. Then $a^{-1} \in H$ because H is a subgroup of G. We have $e' = \phi(e) = \phi(a^{-1} * a) = \phi(a^{-1}) *' \phi(a)$, so $\phi(a)^{-1} = \phi(a^{-1}) \in \phi[H]$.

42. Let a be a generator of G. We claim $\phi(a)$ is a generator of G'. Let $b' \in G'$. Because ϕ maps G onto G', there exists $b \in G$ such that $\phi(b) = b'$. Because a generates G, there exists $n \in \mathbb{Z}$ such that $b = a^n$. Because ϕ is an isomorphism, $b' = \phi(b) = \phi(a^n) = \phi(a)^n$. Thus G' is cyclic.

43. *Closure:* Let $S = \{hk \mid h \in H, k \in K\}$ and let $x, y \in S$. Then $x = hk$ and $y = h'k'$ for some $h, h' \in H$ and $k, k' \in K$. Because G is abelian, we have $xy = hkh'k' = (hh')(kk')$. Because H and K are subgroups, we have $hh' \in H$ and $kk' \in K$, so $xy \in S$ and S is closed under the induced operation.

Identity: Because H and K are subgroups, $e \in H$ and $e \in K$ so $e = ee \in S$.

Inverses: For $x = hk$, we have $h^{-1} \in H$ and $k^{-1} \in K$ because H and K are subgroups. Then $h^{-1}k^{-1} \in S$ and because G is abelian, $h^{-1}k^{-1} = k^{-1}h^{-1} = (hk)^{-1} = x^{-1}$, so the inverse of x is in S. Hence S is a subgroup.

44. If H is empty, then there is no $a \in H$.

45. Let H be a subgroup of G. Then for $a, b \in H$, we have $b^{-1} \in H$ and ab^{-1} H because H must be closed under the induced operation.

Conversely, suppose that H is nonempty and $ab^{-1} \in H$ for all $a, b \in H$. Let $a \in H$. Then taking $b = a$, we see that $aa^{-1} = e$ is in H. Taking $a = e$, and $b = a$, we see that $ea^{-1} = a^{-1} \in H$. Thus H contains the identity element and the inverse of each element. For closure, note that for $a, b \in H$, we also have $a, b^{-1} \in H$ and thus $a(b^{-1})^{-1} = ab \in H$.

46. Let $B = \{e, a, a^2, a^3, \cdots, a^{n-1}\}$ be a cyclic group of n elements. Then $a^{-1} = a^{n-1}$ also generates G, because $(a^{-1})^i = (a^i)^{-1} = a^{n-i}$ for $i = 1, 2, \cdots, n-1$. Thus if G has only one generator, we must have $n - 1 = 1$ and $n = 2$. Of course, $G = \{e\}$ is also cyclic with one generator.

47. *Closure:* Let $a, b \in H$. Because G is abelian, $(ab)^2 = a^2b^2 = ee = e$ so $ab \in H$ and H is closed under the induced operation.

Identity: Because $ee = e$, we see $e \in H$.

Inverses: Because $aa = e$, we see that each element of H is its own inverse. Thus H is a subgroup.

48. *Closure:* Let $a, b \in H$. Because G is abelian, $(ab)^n = a^nb^n = ee = e$ so $ab \in H$ and H is closed under the induced operation.

Identity: Because $e^n = e$, we see that $e \in H$.

Inverses: Let $a \in H$. Because $a^n = e$, we see that the inverse of a is a^{n-1} which is in H because H is closed under the induced operation. Thus H is a subgroup of G.

49. Let G have m elements. Then the elements $a, a^2, a^3, \cdots, a^{m+1}$ cannot all be different, so $a^i = a^j$ for some $i < j$. Then multiplication by a^{-i} shows that $e = a^{j-i}$, and we can take $j - i$ as the desired n.

50. Let $a \in H$ and let H have n elements. Then the elements $a, a^2, a^3, \cdots, a^{n+1}$ are all in H (because H is closed under the operation) and cannot all be different, so $a^i = a^j$ for some $i < j$. Then multiplication by a^{-i} shows that $e = a^{j-i}$ so $e \in H$. Also, $a^{-1} \in H$ because $a^{-1} = a^{j-i-1}$. This shows that H is a subgroup of G.

51. *Closure:* Let $x, y \in H_a$. Then $xa = ax$ and $ya = ay$. We then have $(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy)$, so $xy \in H_a$ and H_a is closed under the operation.

Identity: Because $ea = ae = a$, we see that $e \in H_a$.

Inverses: From $xa = ax$, we obtain $xax^{-1} = a$ and then $ax^{-1} = x^{-1}a$, showing that $x^{-1} \in H_a$, which is thus a subgroup.

52. **a.** *Closure:* Let $x, y \in H_S$. Then $xs = sx$ and $ys = sy$ for all $s \in S$. We then have $(xy)s = x(ys) = x(sy) = (xs)y = (sx)y = s(xy)$ for all $s \in S$, so $xy \in H_S$ and H_S is closed under the operation.

Identity: Because $es = se = s$ for all $s \in S$, we see that $e \in H_S$.

Inverses: From $xs = sx$ for all $s \in S$, we obtain $xsx^{-1} = s$ and then $sx^{-1} = x^{-1}s$ for all $s \in S$, showing that $x^{-1} \in H_S$, which is thus a subgroup.

b. Let $a \in H_G$. Then $ag = ga$ for all $g \in G$; in particular, $ab = ba$ for all $b \in H_G$ because H_G is a subset of G. This shows that H_G is abelian.

53. *Reflexive:* Let $a \in G$. Then $aa^{-1} = e$ and $e \in H$ since H is a subgroup. Thus $a \sim a$.

Symmetric: Let $a, b \in G$ and $a \sim b$, so that $ab^{-1} \in H$. Since H is a subgroup, we have $(ab^{-1})^{-1} = ba^{-1} \in H$, so $b \sim a$.

Transitive: Let $a, b, c \in G$ and $a \sim b$ and $b \sim c$. Then $ab^{-1} \in H$ and $bc^{-1} \in H$ so $(ab^{-1})(bc^{-1}) = ac^{-1} \in H$, and $a \sim c$.

54. *Closure:* Let $a, b \in H \cap K$. Then $a, b \in H$ and $a, b \in K$. Because H and K are subgroups, we have $ab \in H$ and $ab \in K$, so $ab \in H \cap K$.

Identity: Because H and K are subgroups, we have $e \in H$ and $e \in K$ so $e \in H \cap K$.

Inverses: Let $a \in H \cap K$ so $a \in H$ and $a \in K$. Because H and K are subgroups, we have $a^{-1} \in H$ and $a^{-1} \in K$, so $a^{-1} \in H \cap K$.

55. Let G be cyclic and let a be a generator for G. For $x, y \in G$, there exist $m, n \in \mathbb{Z}$ such that $x = a^m$ and $y = b^n$. Then $xy = a^m b^n = a^{m+n} = a^{n+m} = a^n a^m = yx$, so G is abelian.

56. We can show it if G is abelian. Let $a, b \in G$ so that $a^n, b^n \in G_n$. Then $a^n b^n = (ab)^n$ because G is abelian, so G_n is closed under the induced operation. Also $e = e^n \in G_n$. Finally $(a^n)^{-1} = (a^{-1})^n \in G_n$, so G_n is indeed a subgroup of G.

57. Let G be a group with no proper nontrivial subgroups. If $G = \{e\}$, then G is of course cyclic. If $G \neq \{e\}$, then let $a \in G, a \neq e$. We know that $\langle a \rangle$ is a subgroup of G and $\langle a \rangle \neq \{e\}$. Because G has no proper nontrivial subgroups, we must have $\langle a \rangle = G$, so G is indeed cyclic.

6. Cyclic Groups

1. $42 = 9 \cdot 4 + 6, q = 4, r = 6$ **2.** $-42 = 9(-5) + 3, q = -5, r = 3$ **3.** $-50 = 8(-7) + 6, q = -7, r = 6$

4. $50 = 8 \cdot 6 + 2, q = 6, r = 2$ **5.** 8 **6.** 8 7. 60

8. 1, 2, 3, and 4 are relative prime to 5 so the answer is 4.

9. 1, 3, 5, and 7 are relatively prime to 8 so the answer is 4.

10. 1, 5, 7, and 11 are relatively prime to 12 so the answer is 4.

11. 1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53,and 59 are relatively prime to 60 so the answer is 16.

12. There is one automorphism; 1 must be carried into the only generator which is 1.

13. There are 2 automorphisms; 1 can be carried into either of the generators 1 or 5

14. There are 4 automorphisms; 1 can be carried into any of the generators 1, 3, 5, or 7.

15. There are 2 automorphisms; 1 can be carried into either of the generators 1 or -1.

16. There are 4 automorphisms; 1 can be carried into any of the generators 1, 5, 7, or 11.

17. gcd(25, 30) = 5 and 30/5 = 6 so $\langle 25 \rangle$ has 6 elements.

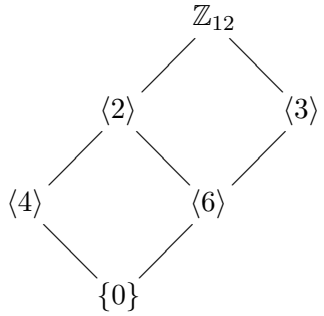
18. gcd(30, 42) = 6 and 42/6 = 7 so $\langle 30 \rangle$ has 7 elements.

19. The polar angle for i is $\pi/2$, so it generates a subgroup of 4 elements.

20. The polar angle for $(1 + i)/\sqrt{2}$ is $\pi/4$, so it generates a subgroup of 8 elements.

21. The absolute value of $1 + i$ is $\sqrt{2}$, so it generates an infinite subgroup of $\aleph_0$ elements.

22. Subgroup diagram:



23. (See the answer in the text.)

24. Subgroup diagram:

25. 1, 2, 3, 6 **26.** 1, 2, 4, 8 **27.** 1, 2, 3, 4, 6, 12 **28.** 1, 2, 4, 5, 10, 20 **29.** 1, 17

30. Incorrect; n must be minimal in $\mathbb{Z}^+$ with that property.

An element a of a group G has **order** $n \in \mathbb{Z}^+$ if $a^n = e$ and $a^m \neq e$ for $m \in \mathbb{Z}^+$ where $m < n$.

31. The definition is correct.

32. T F F F T F F F T T f) The Klein 4-group is an example. g) 9 generates $\mathbb{Z}_{20}$.

33. The Klein 4-group **34.** $\langle \mathbb{R}, + \rangle$ **35.** $\mathbb{Z}_2$

36. No such example exists. Every infinite cyclic group is isomorphic to $\langle \mathbb{Z}, + \rangle$ which has just two generators, 1 and -1.

37. $\mathbb{Z}_8$ has generators 1, 3, 5, and 7. **38.** i and $-i$

39. Corresponding to polar angles $n(2\pi/6)$ for $n = 1$ and 5, we have $\frac{1}{2}(1 \pm i\sqrt{3})$.

40. Corresponding to polar angles $n(2\pi/8)$ for $n =$ 1,7,3, and 5, we have $\frac{1}{\sqrt{2}}(1 \pm i)$ and $\frac{1}{\sqrt{2}}(-1 \pm i)$.

41. Corresponding to polar angles $n(2\pi/12)$ for $n =$ 1,11,5, and 7, we have $\frac{1}{2}(\sqrt{3} \pm i)$ and $\frac{1}{2}(-\sqrt{3} \pm i)$.

42. Expressing two elements of the group as powers of the same generator, their product is the generator raised to the sum of the powers, and addition of integers is commutative.

43. Asuming the subgroup isn't just $\{e\}$, let a be a generator of the cyclic group, and let n be the smallest positive integer power of a that is in the subgroup. For a^m in the subgroup, use the division algorithm for n divided by m and the choice of n to argue that $n = qm$ for some integer q, so that $a^m = (a^n)^q$.

44. By the homomorphism property $\phi(ab) = \phi(a)\phi(b)$ extended by induction, we have $\phi(a^n) = (\phi(a))^n$ for all $n \in \mathbb{Z}+$. By Theorem 3.14, we know that $\phi(a^0) = \phi(e) = e'$. The equation $e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$ shows that $\phi(a^{-1}) = (\phi(a))^{-1}$. Extending this last equation by induction, we see that $\phi(a^{-n}) = (\phi(a))^{-n}$ for all negative integers $-n$. Because G is cyclic with generator a, this means that for all $g = a^n \in G, \phi(g) = \phi(a^n) = [\phi(a)]^n$ is completely determined by the value $\phi(a)$.

45. The equation $(n_1r + m_1s) + (n_2r + m_2s) = (n_1 + n_2)r + (m_1 + m_2)s$ shows that the set is closed under addition. Because $0r + 0s = 0$, we see that 0 is in the set. Because $[(-m)r + (-n)s] + (mr + ns) = 0$, we see that the set contains the inverse of each element. Thus it is a subgroup of $\mathbb{Z}$.

46. Let n be the order of ab so that $(ab)^n = e$. Multiplying this equation on the left by b and on the right by a, we find that $(ba)^{n+1} = bea = (ba)e$. Cancellation of the first factor ba from both sides shows that $(ba)^n = e$, so the order of ba is $\leq n$. If the order of ba were less than n, a symmetric argument would show that the order of ab is less than n, contrary to our choice of n. Thus ba has order n also.

47. a. As a subgroup of the cyclic group $\langle \mathbb{Z}, + \rangle$, the subgroup $G = r\mathbb{Z} \cap s\mathbb{Z}$ is cyclic. The positive generator of G is the **least common multiple** of r and s.

b. The least common multiple of r and s is rs if and only if r and s are relative prime, so that they have no common prime factor.

c. Let $d = ir + js$ be the gcd of r and s, and let $m = kr = qs$ be the least common multiple of r and s. Then $md = mir + mjs = qsir + krjs = (qi + kj)rs$, so rs is a divisor of md. Now let $r = ud$ and let $s = vd$. Then $rs = uvdd = (uvd)d$, and $uvd = rv = su$ is a multiple of r and s, and hence $uvd = mt$. Thus $rs = mtd = (md)t$, so md is divisor of rs. Hence $md = rs$.

48. Note that every group is the union of its cyclic subgroups, because every element of the group generates a cyclic subgroup that contains the element. Let G have only a finite number of subgroups, and hence only a finite number of cyclic subgroups. Now none of these cyclic subgroups can be infinite, for every infinite cyclic group is isomorphic to $\mathbb{Z}$ which has an infinite number of subgroups, namely $\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \cdots$. Such subgroups of an infinite cyclic subgroup of G would of course give an infinite number of subgroups of G, contrary to hypothesis. Thus G has only finite cyclic subgroups, and only a finite number of those. We see that the set G can be written as a finite union of finite sets, so G is itself a finite set.

49. The Klein 4-group V is a counterexample.

50. Note that $xax^{-1} \neq e$ because $xax^{-1} = e$ would imply that $xa = x$ and $a = e$, and we are given that a has order 2. We have $(xax^{-1})^2 = xax^{-1}xax^{-1} = xex^{-1} = xx^{-1} = e$. Because a is given to be the *unique* element in G of order 2, we see that $xax^{-1} = a$, and upon multiplication on the right by x, we obtain $xa = ax$ for all $x \in G$.

51. The positive integers less that pq and relatively prime to pq are those that are not multiples of p and are not multiples of q. There are $p - 1$ multiples of q and $q - 1$ multiples of p that are less than pq. Thus there are $(pq - 1) - (p - 1) - (q - 1) = pq - p - q + 1 = (p - 1)(q - 1)$ positive integers less than pq and relatively prime to pq.