Solutions Guide to Abstract Algebra

Brian Ward*

February 10, 2021

Abstract

Solutions to the textbook "Abstract Algebra: A First Course", Second Edition by Dan Saracino.

Contents

*Email: bmw2150@columbia.edu. Corresponding author.

0 Sets and Induction

0.1 Q1

With $S = \{2, 5, \sqrt{2}, 25, \pi, 5/2\}$ and $T = \{4, 25, \sqrt{2}, 6, 3/2\}$, we have

$$S \cap T = \{\sqrt{2}, 25\},$$

and

$$S \cup T = \{2, 5, \sqrt{2}, 25, \pi, 5/2, 4, 6, 3/2\}.$$

0.2 Q2

For the first equation, the left hand side is

$$\mathbb{Z} \cap (S \cup T) = \{2, 5, 25, 4, 6\}.$$

As for the right hand side, we have $\mathbb{Z} \cap S = \{2, 5, 25\}.$ and $\mathbb{Z} \cap T = \{4, 25, 6\}.$ Thus,

$$(\mathbb{Z} \cap S) \cup (\mathbb{Z} \cap T) = \{2, 5, 25\} \cup \{4, 25, 6\} = \{2, 5, 25, 4, 6\}.$$

For the second equation, the left hand side is

$$\mathbb{Z} \cup (S \cap T) = \mathbb{Z} \cup \{\sqrt{2}, 25\} = \{\sqrt{2}, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

As for the right hand side we have

$$\mathbb{Z} \cup S = \mathbb{Z} \cup \{2, 5, \sqrt{2}, 25, \pi, 5/2\} = \{\sqrt{2}, \pi, 5/2, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

and

$$\mathbb{Z} \cup T = \mathbb{Z} \cup \{4, 25, \sqrt{2}, 6, 3/2\} = \{\sqrt{2}, 3/2, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Thus,

$$(\mathbb{Z} \cup S) \cap (\mathbb{Z} \cup T) = \{\sqrt{2}, \ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

0.3 Q3

For the first equation, we prove (i) $S \cap (S \cup T) \subseteq S$ and (ii) $S \subseteq S \cap (S \cup T)$.

(i) Suppose $x \in S \cap (S \cup T)$. Because an element is in an intersection whenever it is in both sets of the intersection, we have $x \in S$ and $x \in S \cup T$. Of course, the first suffices for $S \cap (S \cup T) \subseteq S$.

(ii) Suppose $x \in S$. Then $x \in S \cup T$ as well because an element is in a union if it is in at least one of the two sets in that union. Since $x \in S$ and $x \in S \cup T$, we have $x \in S \cap (S \cup T)$ so $S \subseteq S \cap (S \cup T)$.

For the second equation, we prove (iii) $S \cup (S \cap T) \subseteq S$ and (iv) $S \subseteq S \cup (S \cap T)$.

(iii) Suppose $x \in S \cup (S \cap T)$. Then either (a) $x \in S$ or (b) $x \notin S$. In case (a) we clearly have $S \cup (S \cap T) \subseteq S$. In case (b) we must have $x \in S \cap T$ (if $x \notin S \cap T$, then x is in neither S nor $S \cap T$, therefore not in $S \cup (S \cap T)$, which contradicts our assumption $x \in S \cup (S \cap T)$.) This implies case (b) is not possible. $x \in S \cap T$ implies $x \in S$ and $x \in T$, contradicting that $x \notin S$. Since cases (a) and (b) are mutually exclusive and exhaustive we have shown $S \cup (S \cap T) \subseteq S$.

(iv) Suppose $x \in S$. Then $x \in S \cup (S \cap T)$ as well because an element is in a union if it is in at least one of the two sets in that union. Thus, we have $S \subseteq S \cup (S \cap T)$.

0.4 Q4

($\implies$)

Suppose that $S \cup T = T$. We must show $S \subseteq T$. Suppose $x \in S$. Then we have $x \in S \cup T$. As $S \cup T = T$, this implies $x \in T$. Thus, $S \cup T = T \implies S \subseteq T$.

($\impliedby$)

Suppose that $S \subseteq T$. We must show that $S \cup T = T$. Thus, we show (i) $S \cup T \subseteq T$ and (ii) $T \subseteq S \cup T$.

(i) Suppose $x \in S \cup T$. Then, either (a) $x \in S$ or (b) $x \notin S$. In case (a) because we assume $S \subseteq T$, we have $x \in T$. In case (b) we must have $x \in T$ because otherwise $x \notin S$ and $x \notin T$ so x could not be in $S \cup T$. In both cases we have shown $x \in T$ so we have $S \cup T \subseteq T$.

(ii) Suppose $x \in T$. Then we know $x \in S \cup T$ (because it is in one of the sets in the union) so $T \subseteq S \cup T$.

Together (i) and (ii) imply $S \cup T = T$ so $S \subseteq T \implies S \cup T = T$.

0.5 Q5

We show (i) $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ and (ii) $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

(i) Suppose $x \in A \cap (B \cup C)$. Then $x \in A$ and $x \in B \cup C$. Either (a) $x \in B$ or (b) $x \notin B$. In case (a) we have $x \in A$ and $x \in B$ so $x \in A \cap B$. In case (b) we must have $x \in C$ (similar to previous arguments) so $x \in A$ and $x \in C$ implying $x \in A \cap C$. In either case we have shown x is in one of the sets of the union $(A \cap B) \cup (A \cap C)$ so $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$.

(ii) Suppose $x \in (A \cap B) \cup (A \cap C)$. Either (a) $x \in A \cap B$ or (b) $x \notin A \cap B$. In case (a) we have $x \in A$ and $x \in B$. In case (b) we must have $x \in A \cap C$ (similar to previous arguments) so that $x \in A$ and $x \in C$. In either case $x \in A$ and x is either in B or C so that $x \in B \cup C$. Together we have $x \in A \cap (B \cup C)$ so $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

0.6 Q6

We show (i) $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ and (ii) $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

(i) Suppose $x \in A \cup (B \cap C)$. Then either (a) $x \in A$ or (b) $x \notin A$. In case (a) $x \in A$ implies $x \in A \cup B$ and $x \in A \cup C$ so $(A \cup B) \cap (A \cup C)$. In case (b) we must have $x \in B \cap C$ (similar to previous arguments) so $x \in B$ and $x \in C$. That implies $x \in A \cup B$ and $x \in A \cup C$, respectively. In either case, we have $x \in A \cup B$ and $x \in A \cup C$ so $x \in (A \cup B) \cap (A \cup C)$. That means $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

(ii) Suppose $x \in (A \cup B) \cap (A \cup C)$. Then $x \in A \cup B$ and $x \in A \cup C$. Either (a) $x \in A$ or (b) $x \notin A$. In case (a) $x \in A$ implies $x \in A \cup (B \cap C)$. In case (b) we have $x \notin A$, but $x \in A \cup B$ and $x \in A \cup C$. The last two facts respectively imply $x \in B$ and $x \in C$ (otherwise x could not be in those two unions) so $x \in B \cap C$ so that $x \in A \cup (B \cap C)$. Thus, $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

0.7 Q7

The key problem in the proof is the requirement that the subsets overlap. In particular, the book's proof has horses labeled $h_1, h_2, \ldots, h_m, h_{m+1}$ and considers two subsets of size m. Subset 1 is $\{h_1, h_2, \ldots, h_m\}$ and subset 2 is $\{h_2, \ldots, h_m, h_{m+1}\}$. The intersection of these two sets is $S := \{h_2, \ldots, h_m\}$. We know from the fact that S is in subset 1, that S are all of the same color, say C_1. Moreover, this is the color of h_1. We also know from the fact that S is in subset 2, that S are all of the same color, say C_2. Moreover, this is the color of h_{m+1}. Of course, we have just concluded S has color C_1 *and* color C_2 so $C_1 = C_2$. Finally, that indicates h_1's color, C_1 must equal that of h_{m+1}'s color, C_2 and so all $m + 1$ horses are the same color.

However, S is empty when $m = 1$ so this first inductive step cannot be carried forward. Intuitively, If I have a group of two horses and I know that all subsets of size less than two are groups of the same color, it does not imply both horses are the same color. For example, if I have one white horse and one black horse then the inductive hypothesis is satisfied by this collection of horses: any subset of size less than two (i.e. a subset of size one) is a group of horses of the same color (pick any individual horse, it is the same color as itself). However, it is obviously not true that the two horses are the same color in spite of the inductive hypothesis holding.

0.8 Q8

When $n = 1$, the left hand side is $1^3 = 1$. The right hand side is $\left(\frac{1(1+1)}{2}\right)^2 = \left(\frac{1\cdot 2}{2}\right)^2 = 1^2 = 1$. Now assume

$$1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2,$$

then by adding $(n+1)^3$ to both sides we obtain

$$1^3 + 2^3 + \ldots + n^3 + (n+1)^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3.$$

We can further simplify the right hand side as

$$\begin{aligned}\left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3 = \left[\left(\frac{n}{2}\right)^2 + (n+1)\right](n+1)^2 &= \frac{1}{4}\left(n^2 + 4(n+1)\right)(n+1)^2 \\ &= \frac{1}{4}\left(n^2 + 4n + 4\right)(n+1)^2 \\ &= \frac{1}{4}(n+2)^2(n+1)^2 \\ &= \left(\frac{(n+1)(n+2)}{2}\right)^2,\end{aligned}$$

which is the right hand side for $n + 1$, exactly as required.

0.9 Q9

When $n = 1$ the left hand side is $1 + (2 \cdot 1 + 1) = 4$. The right hand side is $(1+1)^2 = 2^2 = 4$. Now assume

$$1 + 3 + 5 + \ldots + (2n+1) = (n+1)^2,$$

then adding $2(n+1) + 1 = 2n + 3$ to both sides we obtain

$$1 + 3 + 5 + \ldots + (2n+1) + 2n + 3 = (n+1)^2 + 2n + 3.$$

We can further simplify the right hand side as

$$(n+1)^2 + 2n + 3 = n^2 + 2n + 1 + 2n + 3 = n^2 + 4n + 4 = (n+2)^2,$$

which is the right hand side for $n + 1$, exactly as required.

0.10 Q10

When $n = 1$ the left hand side is $2 \cdot 1 = 2$. The right hand side is $1 \cdot (1 + 1) = 1 \cdot 2 = 2$. Now assume

$$2 + 4 + 6 + \ldots + 2n = n(n + 1),$$

then adding $2(n + 1) = 2n + 2$ to both sides we obtain

$$2 + 4 + 6 + \ldots + 2n + 2n + 2 = n(n + 1) + 2n + 2.$$

We can further simplify the right hand side as

$$n(n + 1) + 2n + 2 = n^2 + n + 2n + 2 = n^2 + 3n + 2 = (n + 1)(n + 2),$$

which is the right hand side for $n + 1$, exactly as required.

(*) For an alternative proof, note that for $m = 2n$, Equation [0.1] on page 5 of the textbook gives

$$1 + 2 + \ldots + (2n - 1) + 2n = \frac{2n(2n + 1)}{2} = n(2n + 1).$$

Let $E := 2 + 4 + 6 + \ldots + 2n$ and $O := 1 + 3 + 5 + \ldots + (2n + 1)$. Then clearly $O - (2n + 1) + E = 1 + 2 + \ldots + (2n - 1) + 2n = n(2n + 1)$. In Problem 0.9 we proved $O = (n + 1)^2$. Thus,

$$\begin{aligned} O - (2n + 1) + E = n(2n + 1) &\implies (n + 1)^2 - (2n + 1) + E = n(2n + 1) \\ &\implies E = n(2n + 1) + (2n + 1) - (n + 1)^2. \end{aligned}$$

We can further simplify the right hand side as

$$n(2n + 1) + (2n + 1) - (n + 1)^2 = 2n^2 + n + 2n + 1 - n^2 - 2n - 1 = n^2 + n = n(n + 1),$$

exactly as required.

0.11 Q11

The proof is very similar to the proof of Theorem [0.2]. Suppose $P(n)$ is false for some positive n. Then $S := \{n \in \mathbb{Z}_+ : P(n) \text{ is False.}\}$ is a non-empty subset of $\mathbb{Z}_+$. Therefore it has a smallest element, say n_0. Observe that $n_0 \neq 1$ because we know $P(1)$ is true from assumption (i). Thus, $n_0 > 1$ and $n_1 := n_0 - 1 > 0$ is a positive integer. We know that $P(k)$ is true for all positive integers $k \leq n_1$. If, on the other hand, $P(k)$ were false for some positive $k' \leq n_1$, then $k\prime$ would be a member of S. However, $k' \leq n_1 = n_0 - 1 < n_0$ means n_0 is not the least member of S, which is a contradiction.

Now we may apply assumption (ii) for $m = n_0$ as we know for all positive $k \leq n_1 = n_0 - 1 < n_0$ that $P(k)$ is true. Assumption (ii) implies $P(n_0)$ is true, which is a contradiction. Thus, the assumption that $P(n)$ is false for some positive n cannot be correct and $P(n)$ is true for all positive n.

0.12 Q12

The proof is very similar to the proof of Theorem [0.2]. Suppose $P(n)$ is false for some $n \geq c$. Then $S := \{n \geq c : P(n) \text{ is False.}\}$ is a non-empty subset of $\mathbb{Z}_+$. Therefore it has a smallest element, say n_0. Observe that $n_0 \neq c$ because we know $P(c)$ is true from assumption (i). Thus, $n_0 > c$ or $n_0 \geq c + 1$ and $n_1 := n_0 - 1 \geq c$. We know that $P(n_1)$ is true because otherwise n_1 would be a member of S. However, $n_1 = n_0 - 1 < n_0$ means n_0 is not the least member of S, which is a contradiction.

Now we may apply assumption (ii) for $m = n_1$ as we know $P(n_1)$ is true. Assumption (ii) implies $P(n_1 + 1) = P(n_0)$ is true, which is a contradiction. Thus, the assumption that $P(n)$ is false for some $n \geq c$ cannot be correct and $P(n)$ is true for all $n \geq c$.

0.13 Q13

The proof is very similar to the proof of Theorem [0.2]. Suppose $P(n)$ is false for some $n \geq c$. Then $S := \{n \geq c : P(n) \text{ is False.}\}$ is a non-empty subset of $\mathbb{Z}_+$. Therefore it has a smallest element, say n_0. Observe that $n_0 \neq c$ because we know $P(c)$ is true from assumption (i). Thus, $n_0 > c$ or $n_0 \geq c+1$ and $n_1 := n_0 - 1 \geq c$. We know that $P(k)$ is true for all positive integers $k \leq n_1$. If, on the other hand, $P(k)$ were false for some positive $k' \leq n_1$, then k' would be a member of S. However, $k' \leq n_1 = n_0 - 1 < n_0$ means n_0 is not the least member of S, which is a contradiction.

Now we may apply assumption (ii) for $m = n_0$ as we know for all positive $k \leq n_1 = n_0 - 1 < n_0$ that $P(k)$ is true. Assumption (ii) implies $P(n_0)$ is true, which is a contradiction. Thus, the assumption that $P(n)$ is false for some $n \geq c$ cannot be correct and $P(n)$ is true for all $n \geq c$.

0.14 Q14

Having proved the modified version of Theorem [0.2] in Problem 0.12, we can apply it with $c = 2$.

For $n = 2$, the left hand side is $1 \cdot 2 = 2$. The right hand side is $\frac{(2-1)\cdot 2\cdot(2+1))}{3} = \frac{1\cdot 2\cdot 3}{3} = 2$. Now assume

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + (n-1)n = \frac{(n-1)n(n+1)}{3},$$

then adding $n(n+1)$ to both sides we obtain

$$1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \ldots + (n-1)n + n(n+1) = \frac{(n-1)n(n+1)}{3} + n(n+1).$$

We can further simplify the right hand side as

$$\begin{aligned}\frac{(n-1)n(n+1)}{3} + n(n+1) = \frac{(n-1)n(n+1)}{3} + \frac{3n(n+1)}{3} &= \frac{(n-1)n(n+1) + 3n(n+1)}{3} \\ &= \frac{((n-1)+3)n(n+1)}{3} \\ &= \frac{(n+2)n(n+1)}{3} \\ &= \frac{n(n+1)(n+2)}{3}\end{aligned}$$

which is the right hand side for $n+1$, exactly as required.

0.15 Q15

When $n = 2$ we obtain $\frac{1}{(2-1)\cdot 2} = \frac{1}{2}$. For $n = 3$ we will add $\frac{1}{(3-1)\cdot 3} = \frac{1}{6}$ to that for a total of $\frac{2}{3}$. For $n = 4$ we will add $\frac{1}{(4-1)\cdot 4} = \frac{1}{12}$ to that for a total of $\frac{3}{4}$. At this point it seems the answer is $\frac{n-1}{n}$. Let us see if this is correct by induction.

We already know the base case $n = 2$ is true from the above calculations. Now assume

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \ldots + \frac{1}{(n-1)n} = \frac{n-1}{n},$$

then adding $\frac{1}{n(n+1)}$ to both sides we obtain

$$\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \frac{1}{3\cdot 4} + \ldots + \frac{1}{(n-1)n} + \frac{1}{n(n+1)} = \frac{n-1}{n} + \frac{1}{n(n+1)}.$$

We can further simplify the right hand side as

$$\frac{n-1}{n} + \frac{1}{n(n+1)} = \frac{(n-1)(n+1)}{n(n+1)} + \frac{1}{n(n+1)} = \frac{(n-1)(n+1)+1}{n(n+1)} = \frac{n^2-1+1}{n(n+1)} = \frac{n^2}{n(n+1)} = \frac{n}{n+1},$$

which is the right hand side for $n+1$, exactly as required.

0.16 Q16

For $n = 1$ we check if 3 divides $1^3 - 1 = 1 - 1 = 0$. As $0 = 3 \cdot 0$ we see indeed 3 divides 0. For a non-trivial base case we can also check for $n = 2$ if 3 divides $2^3 - 2 = 8 - 2 = 6$. As $6 = 3 \cdot 2$ we see 3 divides 6.

Now assume that 3 divides $n^3 - n$. Consider $(n+1)^3 - (n+1)$. Expanding this out, we have

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = \left(n^3 - n\right) + 3n^2 + 3n = \left(n^3 - n\right) + 3(n^2 + n).$$

By assumption we know 3 divides $n^3 - n$ and therefore, $n^3 - n = 3k$ for some integer k. Thus,

$$(n+1)^3 - (n+1) = \left(n^3 - n\right) + 3(n^2 + n) = 3k + 3(n^2 + n) = 3\left(k + n^2 + n\right) := 3k',$$

where $k' := k + n^2 + n$ is an integer. This demonstrates that 3 divides $(n+1)^3 - (n+1)$, which is exactly the statement for $n + 1$.

0.17 Q17

We give the proof by induction first as this is in the section on mathematical induction. However, the combinatorial proof is clearer for this particular statement.

A set $S = \{x\}$ with $n = 1$ element has $2^n = 2^1 = 2$ subsets: either $\emptyset$ or S itself. Thus, the base case is true. Now assume a set with n elements has 2^n subsets and consider any set with $n + 1$ elements. Pick any element, y in the set. There are two cases. Either (a) the subset contains y or (b) the subset does not contain y. Thus, the number of subsets of a set of n elements is equal to Y, the number of subsets of S containing y plus N, the number of subsets of S not containing y.

Each subset of case (a) is formed by taking a union between $\{y\}$ and any subset of $S - \{y\}$. Because S has $n + 1$ elements, $S - \{y\}$ has n elements. Thus, there are 2^n such subsets and $Y = 2^n$. Each subset of case (b) is formed simply by taking a subset of $S - \{y\}$. Again this set has n elements so there are 2^n such subsets and $N = 2^n$. We conclude that the number of subsets of a set of $n + 1$ elements is $Y + N = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}$, which is exactly the statement for $n + 1$

(*) For an alternative proof consider directly counting the subsets. For each element in S it is either in the subset or not. Thus, each subset is equivalent to a list of flags 0/1 for whether or not to include the element. E.g. $(0, 1, 1)$ for a 3 element set indicates to omit the first element and keep the other two. Each element can be 0 or 1 so there are two choice for n elements, therefore there are $\underbrace{2 \cdot 2 \cdot 2 \ldots 2}_{n \text{ times}} = 2^n$ possible subsets.

0.18 Q18

For $k = 1$ we check if $f_{5 \cdot 1} = f_5$ is divisible by 5. Indeed $f_5 = 5$ is divisible by 5 as $5 = 5 \cdot 1$. Now assume that f_{5n} is divisible by 5. Then,

$$\begin{aligned} f_{5(n+1)} = f_{5n+5} = f_{5n+4} + f_{5n+3} = (f_{5n+3} + f_{5n+2}) + f_{5n+3} = 2f_{5n+3} + f_{5n+2} &= 2(f_{5n+2} + f_{5n+1}) + f_{5n+2} \\ &= 3f_{5n+2} + 2f_{5n+1} \\ &= 3(f_{5n+1} + f_{5n}) + 2f_{5n+1} \\ &= 5f_{5n+1} + 3f_{5n}. \end{aligned}$$

Thus, $f_{5(n+1)} = 5f_{5n+1} + 3f_{5n}$. By the induction hypothesis we know that 5 divides f_{5n} so there is an integer k such that $f_{5n} = 5k$. Thus, $f_{5(n+1)} = 5f_{5n+1} + 3f_{5n} = 5f_{5n+1} + 3 \cdot 5k = 5\left(f_{5n+1} + 3k\right) := 5k'$, where k' is an integer. We conclude that 5 divides $f_{5(n+1)}$, which is exactly the statement for $n + 1$.

0.19 Q19

When $n = 1$ the left hand side is $f_{1+1}^2 - f_1 f_{1+2} = f_2^2 - f_1 f_3 = 1^2 - 1 \cdot 2 = 1 - 2 = -1$. The right hand side is $(-1)^1 = -1$. Now assume $f_{n+1}^2 - f_n f_{n+2} = (-1)^n$. Then,

$$\begin{aligned} f_{n+2}^2 - f_{n+1}f_{n+3} = f_{n+2}^2 - f_{n+1}(f_{n+2} + f_{n+1}) = f_{n+2}^2 - f_{n+1}f_{n+2} - f_{n+1}^2 &= (f_{n+2} - f_{n+1})f_{n+2} - f_{n+1}^2 \\ &= ((f_{n+1} + f_n) - f_{n+1})f_{n+2} - f_{n+1}^2 \\ &= f_n f_{n+2} - f_{n+1}^2 \\ &= -(f_{n+1}^2 - f_n f_{n+2}) \\ &= -(-1)^n = (-1)^{n+1}, \end{aligned}$$

where the second to last equality follows from the induction hypothesis. That demonstrates $f_{n+2}^2 - f_{n+1}f_{n+3} = (-1)^{n+1}$, which is exactly the statement for $n + 1$.

0.20 Q20

Because the Fibonacci Series relies on its prior two values to generate the current value, we need to use the second form of induction from Theorem [0.3]. However, the inductive step will not make sense for $m = 2$ because we would be looking at $f_m = f_{m-1} + f_{m-2}$ and there is no $f_{m-2} = f_{2-2} = f_0$ (although traditionally $f_0 = 0$, it has not been defined in the textbook.) Therefore we simply prove the result for $n = 1$ directly as a separate fact first. Then, we rely on the slightly modified version of Theorem [0.3] that we proved in Problem 0.13 to prove this result for all $n \geq 2$.

($n = 1$) When $n = 1$ the left hand side is $f_1 = 1$. The right hand side is

$$\frac{\alpha^1 - \beta^1}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}-1+\sqrt{5}}{2}}{\sqrt{5}} = \frac{\frac{2\sqrt{5}}{2}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1.$$

($n \geq 2$) When $n = 2$, the left hand side is $f_2 = 1$. The right hand side is

$$\begin{aligned} \frac{\alpha^2 - \beta^2}{\sqrt{5}} = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^2}{\sqrt{5}} = \frac{\frac{\left(1+\sqrt{5}\right)^2}{4} - \frac{\left(1-\sqrt{5}\right)^2}{4}}{\sqrt{5}} &= \frac{\frac{1+2\sqrt{5}+5}{4} - \frac{1-2\sqrt{5}+5}{4}}{\sqrt{5}} \\ &= \frac{\frac{1+2\sqrt{5}+5-1+2\sqrt{5}-5}{4}}{\sqrt{5}} \\ &= \frac{\frac{4\sqrt{5}}{4}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1. \end{aligned}$$

Now assume for all $2 \leq k < m$ that $f_k = \frac{\alpha^k - \beta^k}{\sqrt{5}}$. Then,

$$\begin{aligned} f_m = f_{m-1} + f_{m-2} = \frac{\alpha^{m-1} - \beta^{m-1}}{\sqrt{5}} + \frac{\alpha^{m-2} - \beta^{m-2}}{\sqrt{5}} &= \frac{\alpha^{m-1} - \beta^{m-1} + \alpha^{m-2} - \beta^{m-2}}{\sqrt{5}} \\ &= \frac{\alpha^{m-2}(\alpha + 1) - \beta^{m-2}(\beta + 1)}{\sqrt{5}}. \end{aligned}$$

Next, observe that $\alpha + 1 = \frac{1+\sqrt{5}}{2} + 1 = \frac{3+\sqrt{5}}{2}$. Moreover,

$$\alpha^2 = \left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{\left(1+\sqrt{5}\right)^2}{4} = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = \alpha + 1.$$

Similarly, $\beta + 1 = \frac{1-\sqrt{5}}{2} + 1 = \frac{3-\sqrt{5}}{2}$ and

$$\beta^2 = \left(\frac{1-\sqrt{5}}{2}\right)^2 = \frac{\left(1-\sqrt{5}\right)^2}{4} = \frac{1-2\sqrt{5}+5}{4} = \frac{6-2\sqrt{5}}{4} = \frac{3-\sqrt{5}}{2} = \beta + 1.$$

Continuing the above equalities we have

$$f_m = \frac{\alpha^{m-2}(\alpha+1) - \beta^{m-2}(\beta+1)}{\sqrt{5}} = \frac{\alpha^{m-2}\alpha^2 - \beta^{m-2}\beta^2}{\sqrt{5}} = \frac{\alpha^m - \beta^m}{\sqrt{5}},$$

which is exactly the statement for m.

(*) There is one final technicality worth noting. With $c = 2$, assumption (ii) of the variant of Theorem [0.3] from Problem 0.13 says *"for every $m > 2$, if $P(k)$ is true for all k such that $2 \leq k < m$ then $P(m)$ is true."* In truth, we have verified this assumption only for $m > 3$ because then $m - 2 > 1$ or $m - 2 \geq 2$. That is required for us to be able to use the Fibonacci Series definition which recurses twice backwards in the series ($f_m = f_{m-1} + f_{m-2}$) and still have two indices ≥ 2 for which we know the result to be true.

The problem I am getting at is that when $m = 3$ the set of k such that $2 \leq k < m$ is simply $\{2\}$ and not $\{1, 2\}$ but calculating f_3 relies on f_2 and f_1. However, we can treat the statement here for $n = 1$ as a separate fact that is just *always* true regardless of any induction. In this case, then for $m = 3$ it is sufficient to assume $P(2)$ *only* to get $P(3)$ to be true inductively as we can call on this separate fact (i.e. $P(1)$) as needed to complete our proof.

0.21 Q21

When $n = 1$ the left hand side is $F_0 F_1 \dots F_{n-1} = F_0 = 2^{2^0} + 1 = 2^1 + 1 = 2 + 1 = 3$. The right hand side is $F_1 - 2 = 2^{2^1} + 1 - 2 = 2^2 - 1 = 4 - 1 = 3$. Now assume $F_0 F_1 \dots F_{n-1} = F_n - 2$, then mulitplying both sides by F_n we have $F_0 F_1 \dots F_{n-1} F_n = F_n^2 - 2F_n$. We can simplify the right hand side as

$$\begin{aligned} F_n^2 - 2F_n = \left(2^{2^n}+1\right)^2 - 2\left(2^{2^n}+1\right) = \left(2^{2^n}\right)^2 + 2 \cdot 2^{2^n} + 1 - 2 \cdot 2^{2^n} - 2 = \left(2^{2^n}\right)^2 - 1 &= 2^{2^n} \cdot 2^{2^n} - 1 \\ &= 2^{2 \cdot 2^n} - 1 \\ &= 2^{2^{n+1}} + 1 - 2 \\ &= F_{n+1} - 2 \end{aligned}$$

which is the right hand side for $n + 1$, exactly as required.

0.22 Q22

We prove this by induction on n. When $n = 1$ we have a $2^n \times 2^n = 2^1 \times 2^1 = 2 \times 2$ checkerboard. In Figure 1 we show a 2×2 checkerboard. Consider removing any of the 4 squares in the checkerboard, what is remaining? No matter what square is chosen, there are 3 squares left, and they are always shaped like an "L" or reverse "L" (henceforth, an "L-shaped region"). Thus, the base case holds.

Now assume the statement to be true for $n \geq 1$ and consider a $2^{n+1} \times 2^{n+1}$ checkerboard. In fact, this checkerboard is actually just four $2^n \times 2^n$ sub-checkerboards arranged two by two. As an example, we demonstrate this for $n = 1$ in Figure 2. This is a $2^{n+1} \times 2^{n+1} = 2^2 \times 2^2 = 4 \times 4$ checkerboard with the bolded outlines delineating the four $2^n \times 2^n = 2^1 \times 2^1 = 2 \times 2$ sub-checkerboards.

Consider removing any square. This square will be in one of the four sub-checkerboards of size $2^n \times 2^n$ and we know, by the inductive hypothesis, that this can be broken up into L-shaped regions of three squares. How about the other three sub-checkerboards of size $2^n \times 2^n$? We know if we remove any one square from each of these (three in total) that the inductive hypothesis guarantees we can break each of them up into L-shaped regions of three squares. However, we cannot just remove any

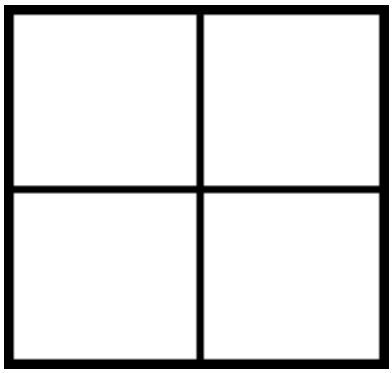

Figure 1: Graphic for the base case in Problem 0.22.

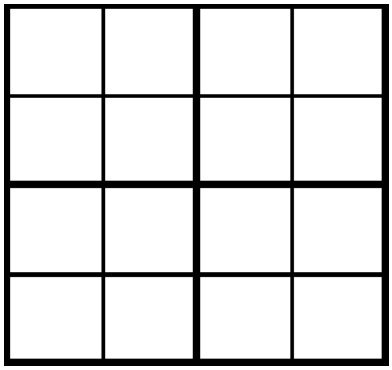

Figure 2: Graphic for the inductive step in Problem 0.22.

squares we want as we must break up this remaining figure into L-shaped regions of three squares. In fact, the centermost squares (where all three sub-checkerboards meet) constitue an L-shaped region and better yet, removing this (which we can) removes exactly one square from each of the three sub-checkerboards. At this point, we know we can break up what remains in L-shaped regions of three squares as we have three $2^n \times 2^n$ checkerboards with one square removed from each. Thus, any $2^{n+1} \times 2^{n+1}$ checkerboard with exactly one square removed can be broken up into L-shaped regions of three squares.

1 Binary Operations

1.1 Q1

(a) With $S = \{2, 5, \sqrt{2}, 25, \pi, 5/2\}$ and $T = \{4, 25, \sqrt{2}, 6, 3/2\}$, we have

$$S - T = \{2, 5, \pi, 5/2\},$$

and

$$T - S = \{4, 6, 3/2\},$$

so that

$$S \triangle T = (S - T) \cup (T - S) = \{2, 5, \pi, 5/2\} \cup \{4, 6, 3/2\} = \{2, 5, \pi, 5/2, 4, 6, 3/2\}.$$

As a check, recall from Problem 0.1 that $S \cap T = \{\sqrt{2}, 25\}$ and $S \cup T = \{2, 5, \sqrt{2}, 25, \pi, 5/2, 4, 6, 3/2\}$. Thus, we can also obtain $S \triangle T$ via

$$S \triangle T = (S \cup T) - (S \cap T) = \{2, 5, \sqrt{2}, 25, \pi, 5/2, 4, 6, 3/2\} - \{\sqrt{2}, 25\} = \{2, 5, \pi, 5/2, 4, 6, 3/2\},$$

which verifies our prior computation.

(b) With $S = \left\{ \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 8 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & \pi \end{pmatrix} \right\}$ and $T = \left\{ \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 8 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right\}$, we have

$$\begin{aligned} S - T &= \left\{ \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 8 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & \pi \end{pmatrix} \right\} - \left\{ \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 8 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & \pi \end{pmatrix} \right\}, \end{aligned}$$

and

$$\begin{aligned} T - S &= \left\{ \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 8 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right\} - \left\{ \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 8 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & \pi \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right\}, \end{aligned}$$

so that

$$S \triangle T = (S - T) \cup (T - S) = \left\{ \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & \pi \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & \pi \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right\}.$$

In a similar way, one may also verify this with the formula $S \triangle T = (S \cup T) - (S \cap T)$. Of course, $S \cup T = \left\{ \begin{pmatrix} 1 & 3 \\ 4 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 8 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & \pi \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \right\}$ and $S \cap T = \left\{ \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 5 & 8 \\ 0 & -1 \end{pmatrix} \right\}$. Then, $(S \cup T) - (S \cap T)$ is exactly as above.

1.2 Q2

In Figure 3, the blue x's mark $(A \triangle B) \triangle C$.

To understand why, first consider $A \triangle B$. The purple x's mark $A \triangle B$: those elements of exactly one of A or B. The green x is in $A \cap B$ so cannot be in $A \triangle B$. It is also not in C either so cannot be in $(A \triangle B) \triangle C$ hence it is not colored blue. The sub-regions of $A \triangle B$ with purple x's but without blue x's overlap with C so they cannot be in $(A \triangle B) \triangle C$ and hence are not colored blue either. The trickiest region is the very center, which *is* in $(A \triangle B) \triangle C$. That is because it is in $A \cap B$ so is not in $A \triangle B$, but it *is* in C so is in exactly one of $A \triangle B$ or C and hence in $(A \triangle B) \triangle C$. The remaining regions (the outermost regions with their red text letters) are all in exactly one of $A \triangle B$ or C.

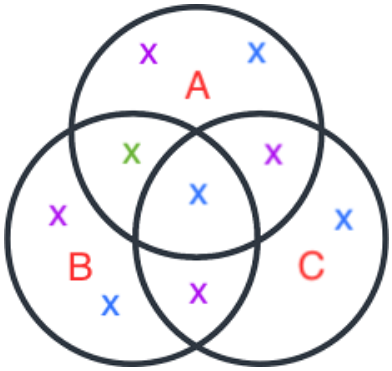

Figure 3: Graphic for the solution to Problem 1.2.

1.3 Q3

To ensure an operation is a binary operation we require (i) the operation can be computed for any element of $S \times S$ (i.e. any ordered pair of elements of S) and (ii) the operation returns an element of S.

(a) Yes, for any pair of integers (a, b) one can compute b^2 and obtain an integer. Then we have a and b^2 as two integers and the sum of two integers is also an integer.

(b) Yes, for any pair of integers (a, b) one can compute a^2 and b^3 and obtain integers. Then we have a^2 and b^3 as two integers and the product of two integers is also an integer.

(c) No, the operation cannot be computed for the ordered pair $(0, 0)$.

(d) No, the operation cannot be computed for the ordered pair $(0, 0)$.

(e) Yes, for any pair of integers (a, b) one can compute $-a \cdot b$ and obtain an integer. Then we have a, b, and $-a \cdot b$ as three integers and the sum of three integers is also an integer.

(f) Yes, for any pair of real numbers (a, b) one can simply return b and this yields another real number.

(g) No, $1 * -4 = |-4| = 4 \notin$S.

(h) No, $3 * 3 = 3 \cdot 3 = 9 \notin S$

(i) Yes, for any pair of 2×2 matrices of real numbers (a, b) computing $a * b$ is tantamount to computing 4 sums of pairs of real numbers. Of course, the sum of real numbers yields another real number so $a * b$ is a 2×2 matrix of real numbers.

(j) Yes, certainly for any pair of subsets of X, (A, B) we can compute $A \triangle B$ as the set of elements of A or B, but not in both A and B. However, we must check that $(A \triangle B) \triangle B$ is a subset of X. Let $x \in (A \triangle B) \triangle B$. Then (using the result proved in the remark in Problem 1.7) we know either (a) $x \in A \triangle B$, $x \notin B$ or (b) $x \notin A \triangle B$, $x \in B$. In case (a) we know that $x \in A \triangle B$ further expands to two subcases. Thus, we know either (a1) $x \in A$, $x \notin B$ or (a2) $x \notin A$, $x \in B$. Recall in case (a) that $x \notin B$ so only case (a1) is possible. However, because $x \in A \subseteq X$ we know $x \in X$ in case (a). In case (b) we know $x \in B \subseteq X$ so we know $x \in X$ in case (b). Thus, $(A \triangle B) \triangle B \subseteq X$.

1.4 Q4

Let $a * b := a/b$ for any pair of $(a, b) \in \mathbb{R}^+ \times \mathbb{R}^+$. Then, $*$ is not commutative. For example, $1 * 2 = 1/2 = 0.5 \neq 2 = 2/1 = 2 * 1$. It is also not associative. For example,

$$(3 * 1) * 2 = (3/1) * 2 = 3 * 2 = 3/2 = 1.5,$$

while

$$3 * (1 * 2) = 3 * (1/2) = 3 * (0.5) = 3/0.5 = 6.$$

1.5 Q5

Recall that for any $A \subseteq X$ and $B \subseteq X$, the definition of $A \cap B$ is $\{x \in X : x \in A, \text{ and } x \in B\}$. Then, let $A * B := A \cap B$. We will show $*$ is a binary operation on S (the set of all subsets of X) that is both commutative and associative.

($*$ is a binary operation on S) To show that $*$ is a binary operation we need to show (i) the operation can be computed for any element of $S \times S$ and (ii) the operation returns an element of S. The first property is clear from the definition: we simply need to return the set of elements that are in both A and B to compute $A * B$. For (ii), suppose $x \in A * B := A \cap B$. Then, $x \in A \subseteq X \implies x \in X$. This is sufficient to show that $A * B \subseteq X$.

($*$ is commutative) We need to show for any $(A, B) \in S \times S$, that $A * B = B * A$ or $A \cap B = B \cap A$. This is almost trivial though. Suppose $x \in A \cap B$, then $x \in A$ and $x \in B$. Re-ordering, we have $x \in B$ and $x \in A$ so $x \in B \cap A$. Thus, $A \cap B \subseteq B \cap A$. For the reverse, suppose $x \in B \cap A$, then $x \in B$ and $x \in A$. Re-ordering, we have $x \in A$ and $x \in B$ so $x \in A \cap B$. Thus, $B \cap A \subseteq A \cap B$ as well and the proof is complete.

($*$ is associative) We need to show for any $A, B, C \in S$ that $(A * B) * C = A * (B * C)$ or $(A \cap B) \cap C = A \cap (B \cap C)$. This is again almost trivial. Suppose $x \in (A \cap B) \cap C$, then $x \in A \cap B$ and $x \in C$. The former implies $x \in A$ and $x \in B$. Since $x \in B$ and $x \in C$, we know $x \in B \cap C$. Thus, since $x \in A$ and $x \in B \cap C$, we have $x \in A \cap (B \cap C)$. Thus, $(A \cap B) \cap C \subseteq A \cap (B \cap C)$. For the reverse, suppose $x \in A \cap (B \cap C)$, then $x \in A$ and $x \in B \cap C$. The latter implies $x \in B$ and $x \in C$. Since $x \in A$ and $x \in B$, we know $x \in A \cap B$. Thus since $x \in A \cap B$ and $x \in C$, we have $x \in (A \cap B) \cap C$. Thus, $A \cap (B \cap C) \subseteq (A \cap B) \cap C$ as well and the proof is complete.

1.6 Q6

(a) It is neither commutative nor associative. Let $a = 1, b = 2, c = 3$ then $a * b = 1 * 2 = 1 + 2^2 = 5 \neq 3 = 2 + 1^2 = 2 * 1 = b * a$. Moreover, $(a * b) * c = (1 * 2) * 3 = (1 + 2^2) * 3 = 5 * 3 = 5 + 3^2 = 14$, while $a * (b * c) = 1 * (2 * 3) = 1 * (2 + 3^2) = 1 * 11 = 1 + 11^2 = 122$.

(b) It is neither commutative nor associative. Let $a = 1, b = 2, c = 3$ then $a * b = 1 * 2 = 1^2 \cdot 2^3 = 1 \cdot 8 = 8$, while $b * a = 2 * 1 = 2^2 \cdot 1^3 = 4 \cdot 1 = 4$. Moreover, $(a * b) * c = (1 * 2) * 3 = (1^2 \cdot 2^3) * 3 = 8 * 3 = 8^2 \cdot 3^3 = 64 \cdot 27 = 1728$, while $a * (b * c) = 1 * (2 * 3) = 1 * (2^2 \cdot 3^3) = 1 * 108 = 1^2 \cdot 108^3 = 1259712$.

(e) It is both commutative and associative. Observe that $a * b = a + b - ab = b + a - ba = b * a$ so $*$ is commutative. Moreover, $(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab)c = a + b + c - ab - ac - bc + abc$ and $a * (b * c) = a * (b + c - bc) = a + (b + c - bc) - a(b + c - bc) = a + b + c - bc - ab - ac + abc$ so $*$ is associative.

(f) It is associative but not commutative. Let $a = 1, b = 2, c = 3$ then $a * b = 1 * 2 = 2 \neq 1 = 2 * 1 = b * a$. Observe that $(a * b) * c = b * c = c$ and $a * (b * c) = a * c = c$ so $*$ is associative.

(i) It is both commutative and associative. Let $a, b, c \in S$, where $a = \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix}$, $b = \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix}$, and $c = \begin{pmatrix} f_1 & f_2 \\ f_3 & f_4 \end{pmatrix}$. Then

$$a * b = \begin{pmatrix} d_1 + e_1 & d_2 + e_2 \\ d_3 + e_3 & d_4 + e_4 \end{pmatrix} = \begin{pmatrix} e_1 + d_1 & e_2 + d_2 \\ e_3 + d_3 & e_4 + d_4 \end{pmatrix} = b * a,$$

so $*$ is associative. Moreover,

$$(a*b)*c = \begin{pmatrix} d_1+e_1 & d_2+e_2 \\ d_3+e_3 & d_4+e_4 \end{pmatrix} * c = \begin{pmatrix} (d_1+e_1)+f_1 & (d_2+e_2)+f_2 \\ (d_3+e_3)+f_3 & (d_4+e_4)+f_4 \end{pmatrix}$$
$$= \begin{pmatrix} d_1+(e_1+f_1) & d_2+(e_2+f_2) \\ d_3+(e_3+f_3) & d_4+(e_4+f_4) \end{pmatrix},$$

where the final equality uses associativity of real number addition. Finally,

$$a*(b*c) = a * \begin{pmatrix} e_1+f_1 & e_2+f_2 \\ e_3+f_3 & e_4+f_4 \end{pmatrix} = \begin{pmatrix} d_1+(e_1+f_1) & d_2+(e_2+f_2) \\ d_3+(e_3+f_3) & d_4+(e_4+f_4) \end{pmatrix},$$

which is the right hand side of $(a*b)*c$ calculated above, so $*$ is associative.

(j) It is associative but not commutative. In Problem 1.8 we verify that $\triangle$ is an associative binary operation. That implies that $(A\triangle B)\triangle B = A\triangle(B\triangle B)$. However, $B\triangle B = B \cup B - B \cap B = B - B = \emptyset$. Thus, $A * B = A\triangle(B\triangle B) = A\triangle\emptyset = (A \cup \emptyset) - A \cap \emptyset = A - \emptyset = A$. Now consider $A, B, C \subseteq$ we have $(A*B)*C = A*C = A$ and $A*(B*C) = A*B = A$ so $*$ is associative.

1.7 Q7

Remark 1.1 *This exercise and the one following it concern the symmetric difference, $\triangle$. Throughout these two exercises we make use of the following.*

For any sets, C and D, $x \in C\triangle D$ if and only if either (a) $x \in C$, $x \notin D$ or (b) $x \notin C$, $x \in D$.

We start with the definition from the text ($C\triangle D = (C-D) \cup (D-C)$) and then prove the above equivalent definition.

($\implies$) Suppose $x \in C\triangle D = (C-D) \cup (D-C)$. Then either (a) $x \in C - D$ or (b) $x \notin C - D$. In case (a), by definition of set difference $x \in C$ and $x \notin D$. In case (b), we must have $x \in D - C$ (similar to previous arguments). By definition of set difference, $x \in D$ and $x \notin C$. Thus, if $x \in C\triangle D$ then either (a) $x \in C$, $x \notin D$ or (b) $x \notin C$, $x \in D$.

($\impliedby$) Suppose either (a) $x \in C$, $x \notin D$ or (b) $x \notin C$, $x \in D$. In case (a), by definition of set difference, $x \in C - D$. It follows that $x \in (C-D) \cup (D-C)$ because x is in at least one set of this union. In case (b), by definition of set difference, $x \in D - C$. It follows that $x \in (C-D) \cup (D-C)$ because x is in at least one set of this union. Thus if either (a) $x \in C$, $x \notin D$ or (b) $x \notin C$, $x \in D$, then $x \in (C-D) \cup (D-C) = C\triangle D$.

Now to solve Problem 1.7. To show $\triangle$ is commutative, we must show $A\triangle B = B\triangle A$. To that end, we show (i) $A\triangle B \subseteq B\triangle A$ and (ii) $B\triangle A \subseteq A\triangle B$.

(i) Suppose $x \in A\triangle B$. Then our fact tells us either (a) $x \in A$, $x \notin B$ or (b) $x \notin A$, $x \in B$. In case (a), the second condition of the above fact holds when we take $C = B$ and $D = A$. That is, $x \notin C = B$ and $x \in D = A$. Thus, the fact implies $x \in C\triangle D = B\triangle A$. In case (b), the first condition of the above fact holds when we again take $C = B$ and $D = A$. That is, $x \in C = B$ and $x \notin D = A$. Thus, the fact implies $x \in C\triangle D = B\triangle A$. Thus, we have $A\triangle B \subseteq B\triangle A$.

(ii) Suppose $x \in B\triangle A$. Then our fact tells us either (a) $x \in B$, $x \notin A$ or (b) $x \notin B$, $x \in A$. In case (a), the second condition of the above fact holds when we take $C = A$ and $D = B$. That is, $x \notin C = A$ and $x \in D = B$. Thus, the fact implies $x \in C\triangle D = A\triangle B$. In case (b), the first condition of the above fact holds when we again take $C = A$ and $D = B$. That is, $x \in C = A$ and $x \notin D = B$. Thus, the fact implies $x \in C\triangle D = A\triangle B$. Thus, we have $B\triangle A \subseteq A\triangle B$.

1.8 Q8

Remark 1.2 *For any element x and sets C and D there are four possibilities:*

(a) $x \in C$, $x \notin D$,

(b) $x \notin C$, $x \in D$,

(c) $x \in C$, $x \in D$,

(d) $x \notin C$, $x \notin D$.

Cases (a) and (b) comprise the two possibilities for $x \in C \triangle D$ as demonstrated in the prior remark. Therefore $x \notin C \triangle D$ is equivalent to the two possibilities (c) and (d). This fact will be used in the proof below.

The full proof started on page 13. The only thing remaining is the reverse inclusion $A\triangle(B\triangle C) \subseteq (A\triangle B)\triangle C$. If we prove this, it then follows that $A\triangle(B\triangle C) = (A\triangle B)\triangle C$. That is precisely what it means for $\triangle$ to be an associative operation. Suppose $x \in A\triangle(B\triangle C)$. Then either (a) $x \in A$, $x \notin B\triangle C$ or (b) $x \notin A$, $x \in B\triangle C$.

In case (a), there are two subcases (a1) $x \in A$, $x \in B$ and $x \in C$ or (a2) $x \notin A$, $x \notin B$, and $x \notin C$. In case (a1), $x \in A$ and $x \in B$ implies (cf. case (c) of the above remark) that $x \notin A\triangle B$. Thus, $x \notin A\triangle B$ and $x \in C$ so $x \in (A\triangle B)\triangle C$. In case (a2) $x \notin A$, $x \notin B$ implies (cf. case (d) of the above remark) that $x \notin A\triangle B$. Once again, $x \notin A\triangle B$ and $x \in C$ so $x \in (A\triangle B)\triangle C$. Therefore, in case (a) $x \in (A\triangle B)\triangle C$.

In case (b), there are two subcases (b1) $x \notin A$, $x \in B$ and $x \notin C$ or (b2) $x \notin A$, $x \notin B$, and $x \in C$. In case (b1), $x \notin A$ and $x \in B$ implies (cf. case (b) of the above remark) that $x \in A\triangle B$. Thus, $x \in A\triangle B$ and $x \notin C$ so $x \in (A\triangle B)\triangle C$. In case (b2) $x \notin A$, $x \notin B$ implies (cf. case (d) of the above remark) that $x \notin A\triangle B$. Thus, $\notin A\triangle B$ and $x \in C$ so $x \in (A\triangle B)\triangle C$. Therefore, in case (b) $x \in (A\triangle B)\triangle C$.

Thus, in both case (a) and (b) we have shown $x \in (A\triangle B)\triangle C$ which implies $A\triangle(B\triangle C) \subseteq (A\triangle B)\triangle C$.

1.9 Q9

For the operation to be commutative we need this table to be symmetric. That is sufficient because then we know the value in "row s_1, column s_2" equals the value in "row s_2, column s_1." However, the table is constructed such that the respective values are $s_1 * s_2$ and $s_2 * s_1$. Thus, a symmetric table implies $s_1 * s_2 = s_2 * s_1$, which means $*$ is commutative. In this case, by inspection, the table is symmetric so it is indeed commutative.

However, it is not associative. For it to be associative we would need $(a * b) * b = a * (b * b)$. The left hand side is $(a * b) * b = c * b = d$. The right hand side is $a * (b * b) = a * a = a$.

1.10 Q10

A binary operation is simply a map from $S \times S$ back to S. For each pair $(a, b) \in S \times S$ we need to assign another value $c \in S$. There are n^2 such pairs (a, b) and each of them can be assigned one of n values. That means there are n^{n^2} binary operations on a set of n elements.

For the operation to be commutative, we require $a * b = b * a$. This is automatically satisfied when $a = b$, so we only need to worry about $a \neq b$. We know there are n^2 pairs $(a, b) \in S \times S$, n of which have $a = b$. That leaves $n^2 - n = n(n-1)$ pairs where $a \neq b$. When we count the number of commutative binary operations, we know that given the value of $a * b = c$ we "force" the value of $b * a = c$. Thus, we only need to count the number of possible choices for half of the $n(n-1)$ pairs where $a \neq b$ as the other half are "forced." There are $\frac{1}{2}n(n-1)$ such pairs and each one can get one of n possible values so there are $n^{\frac{1}{2}n(n-1)}$ possibilities. We must multiply this by the number of possible

assignments to the n pairs of the form (a, a). Because there are n elements with n possible values, this is n^n. The result is that there are

$$n^{\frac{1}{2}n(n-1)} \cdot n^n = n^{\frac{1}{2}n^2 - \frac{1}{2}n + n} = n^{\frac{1}{2}n^2 + \frac{1}{2}n} = n^{\frac{1}{2}n(n+1)}$$

commutative binary operations on a set of n elements.

(*) For an alternative proof, consider the representation of a binary operation from Problem 1.9. In that problem, the binary operation is represented by an $n \times n$ table with the value in "row a, column b" being the value assigned to $a * b$. The question is how many such tables are there? Since there are n^2 entries in the table, with n possible values for each entry, the total number is $\underbrace{n \cdot n \ldots n}_{n^2 \text{ times}} = n^{n^2}$.

We can use this representation to count the number of commutative binary operations as well. In this case we need only concern ourselves with assigning a value to the "lower left half" or "lower triangle" part of the table. Given an entry below the diagonal, we know the value of the corresponding entry in the "upper right half" or "upper triangle" part of the table. Thus, we need to know how many ways to assign values to the diagonal plus the lower half. There are $n + \frac{1}{2}(n^2 - n) = n + \frac{1}{2}n^2 - \frac{1}{2}n = \frac{1}{2}n^2 + \frac{1}{2}n = \frac{1}{2}n(n+1)$ entries to be assigned, each of which can have one of n values. The result is $n^{\frac{1}{2}n(n+1)}$ possible tables.

2 Groups

2.1 Q1

(a) No this is not a group because there can be no identity. An identity element e must satisfy $x * e = x$ for all $x \in \mathbb{R}^+$. Thus, $x + e = x$ which implies $e = 0$, which is not in $\mathbb{R}^+$.

(b) Yes, let $x, y \in 3\mathbb{Z}$. Then there exist $k_x, k_y \in \mathbb{Z}$ such that $x = 3k_x$ and $y = 3k_y$. Thus, $x * y = x + y = 3k_x + 3k_y = 3(k_x + k_y)$, which is a multiple of 3 so is in $3\mathbb{Z}$. Thus, we have a binary operation on $3\mathbb{Z}$. Associativity follows because addition of integers is associative. 0 serves as an identity because for any $x \in 3\mathbb{Z}$ we have $0 * x = 0 + x = x$ and $x * 0 = x + 0 = x$. Finally, for any $x \in 3\mathbb{Z}$, $-x \in 3\mathbb{Z}$. That is because there is a $k_x \in \mathbb{Z}$ such that $x = 3k_x$. Thus, $-x = -3k_x = 3(-k_x)$ is in $3\mathbb{Z}$. Moreover, $-x$ serves as an inverse because $x*(-x) = x+(-x) = x - x = 0$ and $(-x) * x = -x + x = 0$.

(c) No this is not a group because there can be no identity. An identity element e must satisfy $x * e = x$ for all $x \in \mathbb{R} - \{0\}$. Thus, we must have $|xe| = x$. However, if $x < 0$ then the right hand side is < 0 but the left hand side is *always* ≥ 0 so this equation can never be satisfied for any $x < 0$.

(d) Yes, multiplying any pair of elements in $\{-1, 1\}$ returns an element in $\{-1, 1\}$ so this is a binary operation. It is associative because multiplication of real numbers is associative. 1 serves as an identity element because $1 * x = 1 \cdot x = x$ and $x * 1 = x \cdot 1 = x$ for all $x \in \{-1, 1\}$. Finally 1 is its own inverse, and -1 is its own inverse: $1 * 1 = 1 \cdot 1 = 1$ and $(-1) * (-1) = (-1) \cdot (-1) = 1$.

(e) Yes, let q_1, q_2 be two positive rational numbers and r_1, r_2 be their rational square roots. Thus, $r_1^2 = q_1$ and $r_2^2 = q_2$. Moreover, $q_1 * q_2 = q_1 \cdot q_2$, which has the rational square root $r_1 \cdot r_2$. To show this, first note that $r_1 \cdot r_2$ is rational because the rational numbers are closed under multiplication. Moreover, $(r_1 \cdot r_2)^2 = r_1^2 \cdot r_2^2 = q_1 \cdot q_2$. It is associative because multiplication of rational numbers is associative. The number 1 is a positive rational number with rational square root 1 and serves as an identity. In particular, for any positive rational q with a rational square root, $q * 1 = q \cdot 1 = q$ and $1 * q = 1 \cdot q = q$. Finally, if q is a rational number with rational square root r then $r^2 = q$. Thus, $\frac{1}{q}$ has square root $\frac{1}{r}$ because $\left(\frac{1}{r}\right)^2 = \frac{1}{r^2} = \frac{1}{q}$. Moreover, both $\frac{1}{q}$ and $\frac{1}{r}$ are rational. That is because if x is a rational number, it can be expressed as $\frac{p}{q}$ for integers, p and q. It follows that $\frac{1}{x} = \frac{q}{p}$ is also a rational number. Finally, $\frac{1}{q}$ serves as an inverse for any q. That is because $q * \frac{1}{q} = q \cdot \frac{1}{q} = 1$ and $\frac{1}{q} * q = \frac{1}{q} \cdot q = 1$. Note also that $\frac{1}{q}$ is well-defined for any rational q because q is positive, hence non-zero (and similarly for $\frac{1}{r}$).

(f) No this is not a group because there can be no identity. An identity element $e := (e_1, e_2)$ must satisfy $x*e = x$ for all pairs of real numbers $x := (x_1, x_2)$. Thus, $(x_1, x_2)*(e_1, e_2) = (x_1, x_2)$ which implies $(x_1 + e_1, x_2 - e_2) = (x_1, x_2)$. Componentwise we must have $x_1 + e_1 = x_1$ and $x_2 - e_2 = x_2$. That implies $e_1 = e_2 = 0$. However, $(0, 0) * x = (0, 0) * (x_1, x_2) = (0 + x_1, 0 - x_2) = (x_1, -x_2)$ which does not equal (x_1, x_2) for all x. In particular, whenever $x_2 \neq 0$ we cannot have this equality.

(g) Yes, consider $(a_1, b_1), (a_2, b_2)$ with $b_1 \neq 0$ and $b_2 \neq 0$. We have $(a_1, b_1)*(a_2, b_2) = (a_1 + a_2, b_1 \cdot b_2)$. For this to be in the group we must have $b_1 \cdot b_2 \neq 0$. That is indeed the case because both multiplicants are non-zero. Thus, we have a binary operation. Consider also (a_3, b_3) then,

$$[(a_1, b_1) * (a_2, b_2)] * (a_3, b_3) = (a_1 + a_2, b_1 \cdot b_2) * (a_3, b_3) = (a_1 + a_2 + a_3, b_1 \cdot b_2 \cdot b_3)$$

and

$$(a_1, b_1) * [(a_2, b_2) * (a_3, b_3)] = (a_1, b_1) * (a_2 + a_3, b_2 \cdot b_3) = (a_1 + a_2 + a_3, b_1 \cdot b_2 \cdot b_3).$$

Thus, $*$ is associative[1]. For an element $e := (e_1, e_2)$ to be an identity we must have $(a, b) * (e_1, e_2) = (a, b)$ for all pairs of real numbers a and b. Thus, $(a + e_1, b \cdot e_2) = (a, b)$. Componentwise

[1]Note we can unambiguously write $a_1 + a_2 + a_3$ and $b_1 \cdot b_2 \cdot b_3$ because addition and multiplication of real numbers are associative operations.

we must have $a + e_1 = a$ and $b \cdot e_2 = b$ which implies $e_1 = 0$ and $e_2 = 1$ (the latter follows from $b \neq 0$.) Indeed $(a, b) * (0, 1) = (a + 0, b \cdot 1) = (a, b)$ and $(0, 1) * (a, b) = (0 + a, 1 \cdot b) = (a, b)$. One may observe that this group is simply pairs of elements of the groups $(\mathbb{R}, +)$ and $(\mathbb{R} - \{0\}, \cdot)$ from examples 1 and 2 in the textbook. For this reason, we immediately suggest that the inverse element of (a, b) must be $\left(-a, \frac{1}{b}\right)$. Indeed $(a, b) * \left(-a, \frac{1}{b}\right) = \left(a - a, b \cdot \frac{1}{b}\right) = (0, 1)$ and $\left(-a, \frac{1}{b}\right) * (a, b) = \left(-a + a, \frac{1}{b} \cdot b\right) = (0, 1)$.

(h) Yes, consider $a, b \in \mathbb{R} - \{1\}$ then we must show $a * b \in \mathbb{R} - \{1\}$. Suppose to the contrary that $a * b = 1$ for some a, b. Then we have $a + b - ab = 1$, which implies $(1 - a)b = 1 - a$. Because $a \neq 1$, we can divide both sides by $1 - a$ and we obtain $b = 1$, which is a contradiction since $b \in \mathbb{R} - \{1\}$. Thus, it can never be the case that $a * b = 1$ so $*$ is indeed a binary operation. Consider also $c \in \mathbb{R} - \{1\}$ then,

$$(a * b) * c = (a + b - ab) * c = (a + b - ab) + c - (a + b - ab) \cdot c = a + b + c - ab - ac - bc + abc,$$

and

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

Thus, $*$ is associative[2]. An identity element e must satisfy $x * e = x$ for all $x \in \mathbb{R} - \{1\}$. Thus, $x + e - xe = x$ which implies $e = xe$. For this to hold we need $e = 0$. Indeed $x * 0 = x + 0 - x \cdot 0 = x$ and $0 * x = 0 + x - 0 \cdot x = x$ for all $x \in \mathbb{R} - \{1\}$. Let x^{-1} denote an inverse element. We must have $x * x^{-1} = 0$ which implies $x + x^{-1} - x \cdot x^{-1} = 0$ or $x^{-1} = \frac{-x}{1-x}$. Note this element is well defined because $x \neq 1$. Moreover, if $x^{-1} = 1$ we would have $\frac{-x}{1-x} = 1$, which implies $-x = 1 - x \implies 0 = 1$, which is of course a contradiction so $x^{-1} \neq 1$ for any x. Thus, $x^{-1} \in \mathbb{R} - \{1\}$. Finally, we have $x^{-1} * x = \left(\frac{-x}{1-x}\right) * x = \frac{-x}{1-x} + x - \frac{-x}{1-x} \cdot x = \frac{-x}{1-x} + \frac{x-x^2}{1-x} + \frac{x^2}{1-x} = 0$.

(i) Yes, consider $a, b \in \mathbb{Z}$. Then $a * b = a + b - 1 \in \mathbb{Z}$ so $*$ is a binary operation. Consider also $c \in \mathbb{Z}$ then,

$$(a * b) * c = (a + b - 1) * c = (a + b - 1) + c - 1 = a + b + c - 2$$

and

$$a * (b * c) = a * (b + c - 1) = a + (b + c - 1) - 1 = a + b + c - 2.$$

Thus, $*$ is associative[3]. An identity element e must satisfy $x * e = x$ for all $x \in \mathbb{Z}$. Thus, $x + e - 1 = x$, which implies $e = 1$. Indeed $x * 1 = x + 1 - 1 = x$ and $1 * x = 1 + x - 1 = x$ for all $x \in \mathbb{Z}$. Let x^{-1} denote an inverse element. We must have $x * x^{-1} = 1$ which implies $x + x^{-1} - 1 = 1$ or $x^{-1} = 2 - x$ and this is an element of $\mathbb{Z}$. Indeed $x * x^{-1} = x * (2 - x) = x + (2 - x) - 1 = 1$ and $x^{-1} * x = (2 - x) * x = (2 - x) + x - 1 = 1$.

2.2 Q2

(a) They are all Abelian.

(b) Let $a, b \in 3\mathbb{Z}$. Then $a * b = a + b = b + a = b * a$, where the second equality follows because addition of integers is commutative.

(d) Let $a, b \in \{-1, 1\}$. Then $a * b = a \cdot b = b \cdot a = b * a$, where the second equality follows because multiplication of integers is commutative.

(e) Let $a, b \in \mathbb{Q}^+$ be two positive rational numbers with rational square roots. Then $a * b = a \cdot b = b \cdot a = b * a$, where the second equality follows because multiplication of rational numbers is commutative.

[2]Similar to the prior footnote, addition and multiplication of real numbers are associative so we can be ambiguous about the way we write the sum $a + b + c$ and the product abc.

[3]For the final time on this problem, we can be ambiguous about $a + b + c$ because addition of integers is associative.

(g) Let $(a_1, b_1), (a_2, b_2)$ be two pairs of real numbers. Then,

$$(a_1, b_1) * (a_2, b_2) = (a_1 + a_2, b_1 \cdot b_2) = (a_2 + a_1, b_2 \cdot b_1) = (a_2, b_2) * (a_1, b_1),$$

where the second equality follows because addition and multiplication of real numbers are commutative operations.

(h) Let $a, b \in \mathbb{R} - \{1\}$. Then $a * b = a + b - ab = b + a - ba = b * a$, where the second equality follows because addition and multiplication of real numbers are commutative operations.

(i) Let $a, b \in \mathbb{Z}$. Then, $a * b = a + b - 1 = b + a - 1 = b * a$, where the second equality follows because addition of integers is commutative.

(b) Each example is actually multiple examples. We address only the examples that are actually groups and skip the non-groups as identified on pages 17-20 of the textbook.

1. All three of $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ and $(\mathbb{R}, +)$ are Abelian groups. That follows because for any integer, rational or real numbers a, b, we have $a + b = b + a$.
2. All four of $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R}^+, \cdot)$, $(\mathbb{R} - \{0\}, \cdot)$, and $(\mathbb{Q} - \{0\}, \cdot)$ are Abelian groups. That follows because for any rational or real numbers a, b (positive, zero, or otherwise), we have $a \cdot b = b \cdot a$.
3. $\mathbb{R}^n$ with componentwise addition is an Abelian group. Let $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{R}^n$. Then,

$$\begin{aligned}(a_1, \ldots, a_n) * (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n) &= (b_1 + a_1, \ldots, b_n + a_n) \\ &= (b_1, \ldots, b_n) * (a_1, \ldots, a_n),\end{aligned}$$

where the second equality follows because addition of real numbers is commutative.

4. $\mathbb{R} - \{0\}$ with the binary operation $a * b = 2ab$ is an Abelian group. Let $a, b \in \mathbb{R} - \{0\}$. Then, $a * b = 2ab = 2ba = b * a$, where the second equality follows because multiplication of real numbers is commutative.
5. This is not an Abelian group. Consider $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$. Notice that $\det A = 0 \cdot 0 - 1 \cdot 1 = -1$ and $\det B = 1 \cdot 4 - 2 \cdot 3 = 4 - 6 = -2$ so both A and B are members of $GL(2, \mathbb{R})$. However,

$$A \cdot B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 1 & 2 \end{pmatrix},$$

while

$$B \cdot A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix},$$

so $A \cdot B \neq B \cdot A$.

6. This is an Abelian group. Let $f, g \in G$. To show that G is Abelian we must show that $f + g = g + f$. To show the functions $f + g$ and $g + f$ are equal requires us to show that $(f + g)(x) = (g + f)(x)$ for all $x \in \mathbb{R}$. To wit,

$$(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x),$$

where the second equality follows because addition of real numbers is commutative.

7. This is an Abelian group. Let $A, B \in P(X)$. Then, using the second equivalent definition of symmetric difference on page 12 of the textbook, we have

$$A \triangle B = A \cup B - A \cap B = B \cup A - B \cap A = B \triangle A,$$

where the second equality follows because unions and intersections of sets are commutative operations[4].

[4]Unlike the prior uses of commutativity of e.g. real numbers, this one is not axiomatic, but still pretty obvious. We provide a heuristic proof here. $A \cup B$ is the set of elements either in A or B. The set of elements either in A or B is the same as the set of elements in B or A, which is $B \cup A$. $A \cap B$ is the set of elements in both A and B. The set of elements in both A and B is the same as the set of elements in B and A, which is $B \cap A$.

8. This is an Abelian group. Let $a, b \in \mathbb{Z}_n$. Then suppose that $a+b = kn+c$, where $c \in \mathbb{Z}_n$ (i.e. $0 \leq c < n$). It follows that $a \bigoplus b = c$, where $\bigoplus$ indicates we are adding modulo n. Observe that $b + a = a + b = kn + c$ so it follows that $b \bigoplus a = c$ and hence, $a \bigoplus b = c = b \bigoplus a$.

2.3 Q3

In the footnote to Problem 2.2, we show informally that both unions and intersections are binary operations. However, we briefly state here that it is intuitively clear the union and intersection of two subsets A, B of another set X will also be subsets of X. That is because we have elements that are in X that we are combining (union) or subsetting (intersection) so of course all elements in those combinations or subsets will be in X as well.

$(A \cup B)$ An identity element e for $A \cup B$ must satisfy $A \cup e = e \cup A = A$ for every $A \subseteq X$. Clearly $e = \emptyset$ satisfies this requirement because if $x \in A \cup \emptyset$ then either (a) $x \in A$ or (b) $x \notin A$. However, case (b) is actually not possible because then we must have $x \in \emptyset$, which is not possible. Thus, $x \in A \cup \emptyset$ implies $x \in A$ so that $A \cup \emptyset \subseteq A$. If $x \in A$ then clearly $x \in A \cup \emptyset$ so $A \subseteq A \cup \emptyset$ so $A \cup \emptyset = A$. The proof that $\emptyset \cup A = A$ is symmetric (and also obvious because $A \cup B = B \cup A$ for any sets A and B).

However, that implies that an inverse A^{-1} must satisfy $A \cup A^{-1} = \emptyset$. We trivially have $A \subseteq A \cup A^{-1}$ so that implies $A \subseteq \emptyset$. This in turn implies that A is in fact equal to $\emptyset$, which need not be the case. Thus, this cannot be a group because there can be no inverse.

$(A \cap B)$ An identity element e for $A \cap B$ must satisfy $A \cap e = e \cap A = A$ for every $A \subseteq X$. Clearly $e = X$ satisfies this requirement because if $x \in A \cap X$ then $x \in A$ and $x \in X$ so clearly $x \in A$. This implies $A \cap X \subseteq A$. Now suppose $x \in A$. Then because $A \subseteq X$ we have $x \in X$ which implies $x \in A \cap X$ and hence, $A \subseteq A \cap X$ and we have $A \cap X = A$. The proof that $X \cap A = A$ is symmetric (and also obvious because $A \cap B = B \cap A$ for any sets A and B).

However, that implies that an inverse A^{-1} must satisfy $A \cap A^{-1} = X$. Here we can just provide a concrete counterexample. Suppose $X = \{0, 1\}$ and $A = \{1\}$. No matter what set A^{-1} we choose, we will always have $A \cap A^{-1} \subseteq A = \{1\} \subsetneq \{0, 1\} = X$. The more general concept is that if A is a *proper* subset of X then we will always have $A \cap A^{-1} \subseteq A \subsetneq X$. Thus, this cannot be a group because there can be no inverse.

(*) The group with the operation $A \cup B$ can be salvaged if it is always the case that $A = \emptyset$. I.e. every subset of X must be $\emptyset$. The *only* set X satisfying this is $X = \emptyset$ so that $P(X) = \{\emptyset\}$. However, this is a trivial group since it contains only one element. Thus, we learn absolutely nothing about unions from this "group" since it may as well be the set containing 0, 7, or a french bulldog with the operation $e * e = e$.

(**) It is also worth noting that in Section 3 of the book we prove that the identity element is unique. A careful reading of that proof shows us that it only depends on properties (i) and (iii) from page 16. In particular, this means that the unique identity can be obtained *only* using properties of the binary operation. The reason to note that here is that in showing that $\cup$ and $\cap$ cannot be operations on a group, we first derived an identity by looking at the equation $a * e = e * a = a$ for all A. One could ask: is this identity "wrong" in the sense that there is some other identity element for which inverses *do* exist? The proof in Section 3 shows the answer is no. If $\cup$ and $\cap$ are to be valid operations to form groups, then their identity elements *must be* $\emptyset$ and X, respectively.

2.4 Q4

(a) The table is as follows, each element can be computed directly.

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

(b) The table is as follows, each element can be computed directly.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

(c) The table is as follows, each element can be computed directly.

	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

2.5 Q5

No it is not a group. Observe that a is an identity element because (1) $a * a = a$, (2) $a * b = b * a = b$, and (3) $a * c = c * a = c$. However, although a is its own inverse, b and c do not have inverses (there do not exist x such that $x * b = b * x = a$ and $x * c = c * x = a$).

2.6 Q6

Not it is not a group. This operation is not associative because $b * (c * b) = b * b = a$ and $(b * c) * b = c * b = b$.

2.7 Q7

We already know that by writing down a table with elements from the original set, we have a binary operation.[5] Consider the table below. Frankly, it was chosen because it is "nice" in that it is pretty simple and seems reasonable since both a and b can be returned.

	a	b
a	a	b
b	b	a

In any case, an identity must satisfy $a * e = e * a = a$ and $b * e = e * b = b$. Observe that $a * a = a$ so $e = a$ meets the condition that $a * e = e * a = a$ (they are both the same condition when $e = a$).

[5]The table represents the value of $a * b$ for each $(a, b) \in S \times S$, so it is computable. Moreover, as long as each entry in the table is a member of S, we know $*$ always returns a member of S.

Moreover, $b * a = a * b = b$ so $e = a$ meets the condition that $b * e = e * b = b$. Thus, e serves as an identify. Furthermore, we see that a is its own inverse since $a * a = a$. As for b we need an x such that $b * x = x * b = a$. We know $b * b = a$ from the table so b is also its own inverse (again, the required conditions are the same when $x = b$). Finally for associativity, we need to check for all $x, y, z \in \{a, b\}$ that $(x * y) * z = x * (z * y)$. That is fairly manageable to check directly.

$$\begin{aligned}
(a * a) * a = a * (a * a) &\iff a * a = a * a \iff a = a \\
(a * a) * b = a * (a * b) &\iff a * b = a * b \iff b = b \\
(a * b) * a = a * (b * a) &\iff b * a = a * b \iff b = b \\
(a * b) * b = a * (b * b) &\iff b * b = a * a \iff a = a \\
(b * a) * a = b * (a * a) &\iff b * a = b * a \iff b = b \\
(b * a) * b = b * (a * b) &\iff b * b = b * b \iff a = a \\
(b * b) * a = b * (b * a) &\iff a * a = b * b \iff a = a \\
(b * b) * b = b * (b * b) &\iff a * b = b * a \iff b = b
\end{aligned}$$

2.8 Q8

Yes this is a group. First, the binary operation can be computed for each pair of functions (f, g) as we simply need to return that function whose value at each point $x \in \mathbb{R}$ is $f(x) \cdot g(x)$, which can be performed by computing the product of real numbers $f(x)$ and $g(x)$. Moreover, this defines a function from $\mathbb{R}$ to $\mathbb{R}$. Moreover, $\times$ is associative because for any $f, g, h \in G$, $(f \times g) \times h = f \times (g \times h)$ if and only if for all x

$$(f \times g)(x) \cdot h(x) = f(x) \cdot (g \times h)(x).$$

Of course, this is true because $(f \times g)(x) = f(x) \cdot g(x)$ and $(g \times h)(x) = g(x) \cdot h(x)$. Thus, both the left and right hand sides are $f(x) \cdot g(x) \cdot h(x)$ so $\times$ is associative.

For there to be an identity element e we would need for all $f \in G$ that $f \times e = f$. That means for all $x \in \mathbb{R}$ that $(f \times e)(x) = f(x)$ or $f(x) \cdot e(x) = f(x)$. Since we require $f(x) \neq 0$ for all $x \in \mathbb{R}$, we obtain that $e(x) = 1$ for all $x \in \mathbb{R}$. To completely verify that e is an identity we must also check that $e \times f = f$ for all $f \in G$ (for our candidate e). This is so because for all $x \in \mathbb{R}$ we have $f(x) = f(x)$. The left hand side can be re-written as $1 \cdot f(x) = f(x)$ and again as $e(x) \cdot f(x) = f(x)$, for all $x \in \mathbb{R}$. This is the meaning of $e \times f = f$ so e is indeed an identity.

Finally, for each $f \in G$ we need an inverse function f' such that $f \times f' = f' \times f = e$. A natural guess for f' is that function defined such that $f'(x) = \frac{1}{f(x)}$ for all $x \in \mathbb{R}$ (which is well-defined because $f(x) \neq 0$ for all $x \in \mathbb{R}$). For this f' we have $f(x) \cdot f'(x) = f(x) \cdot \frac{1}{f(x)} = 1 = e(x)$, for all $x \in \mathbb{R}$. Moreover, we have $f'(x) \cdot f(x) = \frac{1}{f(x)} \cdot f(x) = 1 = e(x)$, for all $x \in \mathbb{R}$. Thus, f' is an inverse for each x.

2.9 Q9

(a) Let $A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$ and $B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}$. Then of course, $\det(A) = a_1 a_4 - a_2 a_3$ and $\det(B) = b_1 b_4 - b_2 b_3$ and

$$A \cdot B = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} a_1 b_1 + a_2 b_3 & a_1 b_2 + a_2 b_4 \\ a_3 b_1 + a_4 b_3 & a_3 b_2 + a_4 b_4 \end{pmatrix}.$$

Thus,

$$\begin{aligned}\det(A\cdot B) &= (a_1b_1+a_2b_3)(a_3b_2+a_4b_4)-(a_1b_2+a_2b_4)(a_3b_1+a_4b_3)\\ &= a_1b_1a_3b_2+a_1b_1a_4b_4+a_2b_3a_3b_2+a_2b_3a_4b_4-a_1b_2a_3b_1-a_1b_2a_4b_3-a_2b_4a_3b_1-a_2b_4a_4b_3\\ &= (a_1a_4b_1b_4-a_1a_4b_2b_3)+(a_2a_3b_2b_3-a_2a_3b_1b_4)\\ &\qquad +(a_1a_3b_1b_2-a_1a_3b_1b_2)+(a_2a_4b_3b_4-a_2a_4b_3b_4)\\ &= a_1a_4(b_1b_4-b_2b_3)-a_2a_3(b_1b_4-b_2b_3)\\ &= (a_1a_4-a_2a_3)(b_1b_4-b_2b_3)\\ &= \det(A)\cdot\det(B),\end{aligned}$$

exactly as desired.

(b) The reverse implication is obvious from the top of page 19 of the textbook (second paragraph): if the determinant of A is not 0 then the matrix given in the textbook is an inverse of A. Namely,

$$A\cdot A^{-1}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot\begin{pmatrix}\frac{d}{ad-bc} & \frac{-b}{ad-bc}\\ \frac{-c}{ad-bc} & \frac{a}{ad-bc}\end{pmatrix}=\begin{pmatrix}\frac{ad-bc}{ad-bc} & \frac{-ab+ab}{ad-bc}\\ \frac{cd-cd}{ad-bc} & \frac{-bc+ad}{ad-bc}\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=I$$

and

$$A^{-1}\cdot A=\begin{pmatrix}\frac{d}{ad-bc} & \frac{-b}{ad-bc}\\ \frac{-c}{ad-bc} & \frac{a}{ad-bc}\end{pmatrix}\cdot\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}\frac{ad-bc}{ad-bc} & \frac{bd-bd}{ad-bc}\\ \frac{-ac+ac}{ad-bc} & \frac{-bc+ad}{ad-bc}\end{pmatrix}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=I.$$

Now suppose A is invertible (i.e. that $A\in GL(2,\mathbb{R})$). Then there is an A^{-1} such that $AA^{-1}=I$. By part (a) we know that $\det(AA^{-1})=\det(A)\cdot\det(A^{-1})$. On the other hand, $\det(I)=1$ by direct computation and since $AA^{-1}=I$ are equal matrices, their determinants must be equal as well. That follows because matrices are equal if and only if they are equal entry by entry. Thus, $\det(A)\cdot\det(A^{-1})=1$. It follows that neither $\det(A)$ nor $\det(A^{-1})$ can be 0 because otherwise the product cannot equal 1. Thus, $\det(A)\neq 0$, exactly as desired.

(c) The fact we need to prove here is that (a) and (b) imply the following: if A and B are two invertible matrices, then AB is invertible. If we have that, then we know we have a binary operation, it is associative, and there are inverses as well. All of that follows simply from the same discussion from the bottom of page 18 to the top of page 19 of the textbook. Thus, if we prove that fact, then we prove that $GL(2,\mathbb{R})$ would be a group.

Suppose A, B are two invertible matrices. Then by part (b) ($\implies$ direction) we have $\det(A)\neq 0$ and $\det(B)\neq 0$. By part (a), $\det(AB)=\det(A)\cdot\det(B)$. The right hand side is not 0, otherwise one of the two determinants must be 0. Thus, $\det(AB)\neq 0$ and it follows that AB is invertible by part (b) ($\impliedby$ direction). This is what we needed to show, so $GL(2,\mathbb{R})$ is a group.

2.10 Q10

Let $A=\begin{pmatrix}a_1 & a_2\\ -a_2 & a_1\end{pmatrix}$ and $B=\begin{pmatrix}b_1 & b_2\\ -b_2 & b_1\end{pmatrix}$ with both $a_1^2+a_2^2\neq 0$ and $b_1^2+b_2^2\neq 0$. Then,

$$A\cdot B=\begin{pmatrix}a_1 & a_2\\ -a_2 & a_1\end{pmatrix}\cdot\begin{pmatrix}b_1 & b_2\\ -b_2 & b_1\end{pmatrix}=\begin{pmatrix}a_1b_1-a_2b_2 & a_1b_2+a_2b_1\\ -a_2b_1-a_1b_2 & -a_2b_2+a_1b_1\end{pmatrix}.$$

Indeed $A \cdot B$ is in this group because (i) the diagonal entries are equal, (ii) the off-diagonal entries are negatives of each other and (iii) we have

$$\begin{aligned}
\det A \cdot B &= \det \begin{pmatrix} a_1b_1 - a_2b_2 & a_1b_2 + a_2b_1 \\ -a_2b_1 - a_1b_2 & -a_2b_2 + a_1b_1 \end{pmatrix} \\
&= (a_1b_1 - a_2b_2)(-a_2b_2 + a_1b_1) - (-a_2b_1 - a_1b_2)(-a_2b_2 + a_1b_1) \\
&= (a_1b_1 - a_2b_2)^2 + (-a_2b_1 - a_1b_2)^2 \\
&= a_1^2b_1^2 - 2a_1b_1a_2b_2 + a_2^2b_2^2 + a_2^2b_1^2 + 2a_ab_1a_2b_2 + a_1^2b_2^2 \\
&= a_1^2b_1^2 + a_2^2b_2^2 + a_2^2b_1^2 + a_1^2b_2^2 \\
&= a_1^2b_1^2 + a_2^2b_1^2 + a_2^2b_2^2 + a_1^2b_2^2 \\
&= b_1^2(a_1^2 + a_2^2) + b_2^2(a_2^2 + a_1^2) \\
&= (b_1^2 + b_2^2)(a_2^2 + a_1^2),
\end{aligned}$$

which is non-zero because both terms in the product are non-zero by assumption. Thus, we have a valid binary operation on this set of matrices.

2.11 Q11

2.12 Q12

2.13 Q13

2.14 Q14

When $n = 1$ we have one set in $A_1 \triangle A_2 \ldots \triangle A_n$ so we simply have $A_1 \triangle A_2 \ldots \triangle A_n = A_1$. Thus, if $x \in A_1 \triangle A_2 \ldots \triangle A_n = A_1$ then $x \in A_1$, which is an odd number of sets. When $n = 2$ we have $A_1 \triangle A_2$. We have seen that if $x \in A_1 \triangle A_2$ it is in *exactly* one of A_1 or A_2, which is again an odd number.

Suppose that for fixed $n \geq 1$, if $x \in A_1 \triangle A_2 \ldots \triangle A_n$ then $x \in A_j$ for an odd number of js. Now consider $A_1 \triangle A_2 \ldots \triangle A_n \triangle A_{n+1}$. Although we can write this unambiguously without parentheses, it is helpful to write this as $(A_1 \triangle A_2 \ldots \triangle A_n) \triangle A_{n+1}$. Now suppose $x \in (A_1 \triangle A_2 \ldots \triangle A_n) \triangle A_{n+1}$. Then, we know x is in *exactly* one of $A_1 \triangle A_2 \ldots \triangle A_n$ or A_{n+1}. In the first case, we know $x \notin A_{n+1}$ and $x \in A_1 \triangle A_2 \ldots \triangle A_n$. by the inductive hypothesis that x is in A_j for an odd number of j. In the second case, we know

3 Fundamental Theorems about Groups

3.1 Q1

In $(\mathbb{Z}_n, \oplus)$, the inverse of $x \neq 0$ is $n - x$ and the identity is 0 (cf. page 22 of the textbook.) We use this fact to cancel the constants on either side of x in the given equation, $2 \oplus x \oplus 7 = 1$. Recalling that we can group the operations in any way we like (cf. Problem 2.13), we begin by canceling the 2 by adding 10 to both sides of the equation on the left as

$$10 \oplus 2 \oplus x \oplus 7 = 10 \oplus 1 \iff 0 \oplus x \oplus 7 = 11 \iff x \oplus 7 = 11.$$

Then, we can cancel the 7 by adding 5 to both sides of the equation on the right as

$$x \oplus 7 \oplus 5 = 11 \oplus 5 \iff x \oplus 0 = 4 \iff x = 4.$$

As a check, $2 \oplus 4 \oplus 7 = 6 \oplus 7 = 1$.

3.2 Q2

In $(P(X), \triangle)$, the inverse of A is A and the identity is $\emptyset$ (cf. page 20 of the textbook.) Using this fact, we can can cancel A from the left hand side of the given equation, $A * x = B$ as

$$\begin{aligned} A * A * x = A * B \iff \emptyset * x = A * B \iff x = A * B &= A \triangle B \\ &= A \cup B - A \cap B \\ &= \{1,4,5,7,8\} \cup \{2,4,6\} - \{1,4,5,7,8\} \cap \{2,4,6\} \\ &= \{1,2,4,5,6,7,8\} - \{4\} \\ &= \{1,2,5,6,7,8\}. \end{aligned}$$

As a check

$$\begin{aligned} A * \{1,2,5,6,7,8\} = A \triangle \{1,2,5,6,7,8\} &= A \cup \{1,2,5,6,7,8\} - A \cap \{1,2,5,6,7,8\} \\ &= \{1,4,5,7,8\} \cup \{1,2,5,6,7,8\} - \{1,4,5,7,8\} \cap \{1,2,5,6,7,8\} \\ &= \{1,2,4,5,6,7,8\} - \{1,5,7,8\} \\ &= \{2,4,6\} = B. \end{aligned}$$

3.3 Q3

Consider $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $C = \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix}$. Then,

$$AB = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix},$$

and

$$BC = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 4 & 3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 4 & 3 \end{pmatrix}.$$

Thus, for these three matrices $A, B, C \in GL(2\mathbb{R})$ we have $AB = BC$, yet $A \neq C$.

(*) One may wonder how to "derive" these matrices from first principles. There is no direct way to do this, but we can motivate how to think about the above. First, we know B is the most important matrix to get the property $AB = BC$ to hold so we focus on that. To keep it simple, one first considers matrices with 0s and 1s as entries. The identity matrix immediately comes to mind. However, this

is not a choice for B because then $AB = BC$ *implies* $A = C$. To try to retain the simplicity, we try flipping and using a matrix with 1s only on the off diagonal (i.e. B above). Finally, if one considers arbitrary matrices A and C and explicitly writes out the four equations derived from $AB = BC$ we find a set of conditions on C, given the values of A. Specifically, $a_1 = c_4$, $a_2 = c_3$, $a_3 = c_2$, and $a_4 = c_1$. Thus, A can be any matrix you like, and you know immediately what C must be.

3.4 Q4

Because G is a group, each element $x \in G$ has an inverse, x^{-1}. Thus, we can left multiply both sides of the equation $x * g = x$ by x^{-1} to obtain

$$x^{-1} * x * g = x^{-1} * x \iff e * g = e \iff g = e.$$

3.5 Q5

First, we apply Theorem 3.4 with $x := x$ and $y := y * z$. We have

$$(x * y * z)^{-1} = (x * (y * z))^{-1} = (y * z)^{-1} * x^{-1}.$$

Second, applying Theorem 3.4 with $x := y$ and $y := z$. We have

$$(y * z)^{-1} = z^{-1} * y^{-1}.$$

Finally, putting these two equations together we have

$$(x * y * z)^{-1} = (y * z)^{-1} * x^{-1} = \left(z^{-1} * y^{-1}\right) * x^{-1} = z^{-1} * y^{-1} * x^{-1}.$$

3.6 Q6

Let $(G, *)$ be a group and $x, y, z \in G$. To prove (i) we assume $x * y = x * z$ and we must show $y = z$. Because $x \in G$ there exists x^{-1} such that $x * x^{-1} = x^{-1} * x = e$, where e is the identity element in G. From $x * y = x * z$ we can left multiply both sides by x^{-1} to obtain $x^{-1} * (x * y) = x^{-1} * (x * z)$. Using associativity we obtain $(x^{-1} * x) * y = (x^{-1} * x) * z$. That implies $e * y = e * z$, which in turn implies $y = z$, exactly as desired. To prove (ii) we assume $y * x = z * x$. This time, we can right multiply both sides by x^{-1} to obtain $(y * x) * x^{-1} = (z * x) * x^{-1}$. Using associativity we obtain $y * (x * x^{-1}) = z * (x * x^{-1})$. That implies $y * e = z * e$, which in turn implies $y = z$, exactly as desired.

3.7 Q7

Suppose for some row there is an element, say x, such that it appears more than once in that row. Further suppose that this row represents the left multiplication table for a. I.e. reading this row gives you the values of $a * g$ for all g in G. Thus, the assumption that x appears more than once means there must be more than one solution g to $a * g = x$. This implies there must exist elements y and z with $y \neq z$ such that $a * y = a * z$ because both sides equal x. However, the left Cancellation Law implies $y = z$ contradicting our assumption that for some row there is an element appearing more than once. Now suppose for some row there is an element that never appears in that row. By the Pigeonhole Principle there must be some other element that appears more than once in that row and we have already seen that is not possible. Thus, it also cannot be possible that for some row there is an element that never appears in that row or appears more than once. Finally, we can conclude that every element of G occurs precisely once in each row of the table.

The proof that every element of G occurs precisely once in each column of the table is exactly the same as the above proof replacing the word "row" with the word "column." These two facts together comprise our desired result.

(*) We can spell out the application of the Pigeonhole Principle more carefully. Suppose $|G| = n$. We are assumping for some row there is an element that never appears in that row. Suppose further that each of the other $n-1$ elements appear at most once in each row. Then there are at most $n-1$ entries to fill a row that needs to contain n total entries. Thus, it cannot be the case that the other $n-1$ elements appear at most once and there is some other element that appears more than once.

3.8 Q8

(a) By way of contradiction assume there are two identity elements e and e' with $e \neq e'$. Because e is an identity, for all $x \in G$, $e * x = x * e = x$. Setting $x = e'$ we have (i) $e * e' = e' * e = e'$. Similarly, because e' is an identity, for all $x \in G$, $e' * x = x * e' = x$. Setting $x = e'$ we have (ii) $e' * e' = e'$. Thus, observe that $e * e' = e' * e'$ because both sides are e'. (The left hand side equals e' by (i) and the right hand side equals e' by (ii).) Finally using the right Cancellation Law we can cancel e' from both sides to obtain $e = e'$, contradicting that $e \neq e'$. Thus, there is only one identity element in G.

(b) Suppose $x, y \in G$. Then there exist x^{-1}, y^{-1} such that $x * x^{-1} = x^{-1} * x = e$ and $y * y^{-1} = y^{-1} * y = e$, where e is the identity element in G. Thus, we can write down the equation $x * x^{-1} = y * y^{-1}$ because both sides equal e. Now we use the assumption $x^{-1} = y^{-1}$ and denote their common value as z. Thus, we can write $x * z = y * z$ and use the right Cancellation Law to cancel z and obtain $x = y$, exactly as desired.

3.9 Q9

($\implies$)

We know from Theorem 3.4 that for any $x, y \in G$, $(x * y)^{-1} = y^{-1} * x^{-1}$. Since $x^{-1}, y^{-1} \in G$, the fact that $(G, *)$ is abelian implies $y^{-1} * x^{-1} = x^{-1} * y^{-1}$. Thus, the fact that $(G, *)$ is abelian implies for all $x, y \in G$, $(x * y)^{-1} = y^{-1} * x^{-1} = x^{-1} * y^{-1}$.

($\impliedby$)

Let $x, y \in G$ then we have $(x * y)^{-1} = x^{-1} * y^{-1}$ (by assumption). However, by Theorem 3.4, the left hand side expands as $(x * y)^{-1} = y^{-1} * x^{-1}$. We conclude that for all $x, y \in G$ that $x^{-1} * y^{-1} = y^{-1} * x^{-1}$ (both being equal to $(x * y)^{-1}$.) By Theorem 3.2, the inverse is unique so we can take the inverse of both sides to obtain

$$\begin{aligned} \left(x^{-1} * y^{-1}\right)^{-1} = \left(y^{-1} * x^{-1}\right)^{-1} &\implies \left(y^{-1}\right)^{-1} * \left(x^{-1}\right)^{-1} = \left(x^{-1}\right)^{-1} * \left(y^{-1}\right)^{-1} \\ &\implies y * x = x * y. \end{aligned}$$

The first implication is due to Theorem 3.4, while the second is due to Theorem 3.3. Thus, we have shown for all $x, y \in G$ we have $x * y = y * x$. I.e. $(G, *)$ is abelian.

3.10 Q10

Let $(G, *)$ be a group and $g \in G$ be a fixed element. Denote $\widetilde{G} := \{g * x : x \in G\}$. We will show $G = \widetilde{G}$ by showing (i) $G \subseteq \widetilde{G}$ and (ii) $\widetilde{G} \subseteq G$.

(i) Suppose $y \in G$. To show that $y \in \widetilde{G}$, we must find an $x \in G$ such that $y = g * x$. Because $g \in G$, we know there is a $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$, where e is the identity element in G. Left multiplying the equation $y = g * x$ by g^{-1} yields $g^{-1} * y = g^{-1} * (g * x) = (g^{-1} * g) * x = e * x = x$. Thus, for $x = g^{-1} * y$, we can write $y = g * x$. Thus, $y \in \widetilde{G}$.

(ii) Suppose $y \in \widetilde{G}$. By definition of $\widetilde{G}$, there is an $x \in G$ such that $y = x * g$. However, because $*$ is a binary operation and $x, g \in G$ we know $y = x * g \in G$.

3.11 Q11

Let $x, y \in G$. Then, by definition of G we have $x * x = y * y = e$. Observe that this fact immediately implies $x^{-1} = x$ and $y^{-1} = y$. To show that $x*y = y*x$ it is equivalent to show that $(x*y)^{-1}*(y*x) = e$. By Theorem 3.4, for all $x, y \in G$, $(x * y)^{-1} = y^{-1} * x^{-1}$. Thus, we can expand the left hand side as $(x * y)^{-1} * (y * x) = (y^{-1} * x^{-1}) * (y * x) = (y * x) * (y * x) = (y * x)^2 = e$. The final equality holds because $*$ is a binary operation so $z := x * y \in G$ and by definition of G, $z^2 = (y * x)^2 = e$.

3.12 Q12

($\implies$) Suppose $x, y \in G$ and that G is Abelian. Then,

$$(x * y)^2 = (x * y) * (x * y) = x * (y * x) * y = x * (x * y) * y = (x * x) * (y * y) = x^2 * y^2,$$

exactly as desired. (Note the use of G being Abelian in the third equality.)

($\impliedby$) Suppose $x, y \in G$. By assumption $(x * y)^2 = x^2 * y^2$. Writing this out entirely, we have

$$\begin{aligned}(x * y) * (x * y) = (x * x) * (y * y) \implies ((x * y) * x) * y = ((x * x) * y) * y &\implies (x * y) * x = (x * x) * y \\ &\implies x * (y * x) = x * (x * y) \\ &\implies y * x = x * y,\end{aligned}$$

exactly as desired. (Note the use of the Cancellation Laws in the second and fourth implications to (i) right cancel y and (ii) left cancel x.)

(*) Cf. Problem 2.13 for why we can move parentheses however we like.

3.13 Q13

The assumption that there is a left identity, e means for every $g \in G$ we have $e*g = g$. The assumption that every element has a left inverse means for every $g \in G$ there is a g^{-1} such that $g^{-1} * g = e$. Similar to the proof of Theorem 3.7, we must show (i) that e is also a right identity (that is, for every $g \in G$, we have $g * e = g$) and (ii) that g^{-1} is also a right inverse (that is, $g * g^{-1} = e$).

(i) Letting $g = e$ in the assumption for a left identity means $e * e = e$. Consider an arbitary $x \in G$. Then there is an x^{-1} such that $x^{-1} * x = e$. We can insert this into the equation $e * e = e$ to obtain $(x^{-1} * x) * e = x^{-1} * x$. Using associativity we obtain $x^{-1} * (x * e) = x^{-1} * x$. Since $x^{-1} \in G$ it also has a left inverse, say y, such that $y * x^{-1} = e$. Left multiplying by y we have $y*(x^{-1}*(x*e)) = y*(x^{-1}*x)$. Again using associativity we obtan $(y*x^{-1})*(x*e) = (y*x^{-1})*x$. Thus we obtain $e * (x * e) = e * x$. Because e is a left identity we have $x * e = x$ for all $x \in G$. I.e., e is a right identity.

(ii) Consider any $x \in G$ and let x^{-1} be the left inverse. We know that $x^{-1} * x = e$ and we want to show that $x * x^{-1} = e$. We know there is also a left inverse of x^{-1}, say y, for which we can write $y * x^{-1} = e$. Left multiplying both sides of $x^{-1} * x = e$ by y we obtain $y * (x^{-1} * x) = y$. Using associativity we obtain $(y * x^{-1}) * x = y$. Because y is the left inverse of x^{-1} we have $e * x = y$ or $x = y$ (because e is a left identity.) Finally, from the equation $y * x^{-1} = e$ and $y = x$ we have $x * x^{-1} = e$. I.e. x^{-1} is the right inverse of x.

3.14 Q14

Let us take $a = b$ in the given conditions. Then there is an element[6] $e_a^{(R)}$ such that $a * e_a^{(R)} = a$. Now consider any other element b. Then, we know there is a y such that $y * a = b$ (from the second condition). We use this to show that $b * e_a^{(R)} = b$ as follows

$$b * e_a^{(R)} = (y * a) * e_a^{(R)} = y * \left(a * e_a^{(R)}\right) = y * a = b.$$

The first equality follows from $y * a = b$, the second by associativity, the third by $a * e_a^{(R)} = a$, and the final equality by $y * a = b$ once again. As b was arbitrary, we have shown that there is an element, $e_a^{(R)}$ such that $b * e_a^{(R)} = b$ for all $b \in G$ (right identity). Next, for any $x \in G$, we set $a = x$ and $b = e_a^{(R)}$ in the given condition to find a $y \in G$ such that $x * y = e_a^{(R)}$ (first condition with x now taking the place of y). Thus, we have all the conditions of Theorem 3.7, so $(G, *)$ is a group.

3.15 Q15

Recall that we can represent a binary operation on a finite set via a multiplication table. Now consider any given row of that table. I.e. we consider all elements of the form $a * x$ for some fixed $a \in G$. Suppose for some $x \neq y$ we have $a * x = a * y$. Since the left Cancellation Law holds, we conclude $x = y$, which is a contradiction. It follows that in any given row, all elements are unique. Since a row contains exactly $|G|$ elements, each row must contain all unique elements of G. Symmetrically, consider any given column of the table. I.e. consider all elements of the form $x * a$ for some fixed $a \in G$. If $x * a = y * a$, then because the right Cancellation Law holds, we have $x = y$. It follows each column contains all unique elements of G.

Now consider arbitrary $a, b \in G$. By the above, we know that b must be somewhere on a's row. That is, there exists an element x such that $a * x = b$. Similarly by the above, we know that b must be somewhere on a's column. That is, there exists an element y such that $y * a = b$. Thus, we have all of the conditions of Problem 3.14 (G has been assumed non-empty, and $*$ is assumed to be an associative binary operation) so we can conclude that $(G, *)$ is a group.

(*) It is worth emphasizing that the proof does not stop after the first paragraph here. One might think we can appeal to Problem 3.7 here and conclude that we are done. However, that is a misreading of Problem 3.7. Finiteness of G is useful to prove the *result* of Problem 3.7, which in turn is useful to prove the *conditions* of Problem 3.14.

3.16 Q16

An example is $(\mathbb{Z}^+, \cdot)$. This is the set of positive integers together with multiplication. Clearly $\mathbb{Z}^+$ is not finite, but is non-empty. Moreover, $+$ is an associative binary operation on Z^+ since the sum of any two positive integers is positive, and addition of integers is associative. Let $x, y, z \in \mathbb{Z}^+$, and suppose $x \cdot y = x \cdot z$. Since $x > 0$ we can divide both sides by x to obtain $y = z$ so the left Cancellation Law holds. Now suppose $y \cdot x = z \cdot x$. Again, since $x > 0$ we can divide both sides by x to obtain $y = z$ so the right Cancellation Law holds. However, as discussed on page 17 of the textbook, "$(\mathbb{Z}^+, \cdot)$ is *not* a group, since no element other 1 has an inverse."

(*) In trying to solve this problem we should consider examples of sets together with operations that we already know are *not* groups. Specifically here we looked back at the second set of examples on page 17 of the textbook. There are two reasons this set is relevant here. First, the examples are infinite sets so that meets one of the conditions of the problem. Second, the operation is multiplication and this is amenable to thinking about the Cancellation Laws and whether or not they hold.

[6]The notation is meant to emphasize that as of right now, we believe that $e_a^{(R)}$ is a *right* (superscript (R)) identity (named e) for a only (subscript a). Our proof goes on to show that we can drop the subscript so that $e^{(R)}$ is a right identity for *every* element. Being able to drop the superscript will be due to Theorem 3.7.

3.17 Q17

The first condition tells us there is a unique value $e \in G$ such that for all $x \in G$, $x * e = x$ (unique right identity). The second condition tells us for any $x \in G$ there is an $x' \in G$ such that $x' * x = e$ (existence of a left inverse).

Consider any $x \in G$. As above, there is an x' such that $x' * x = e$. Similarly, there is an x'' such that $x'' * x' = e$. Left multiplying $x' * x = e$ by x'', we obtain

$$x'' * (x' * x) = x'' * e \implies (x'' * x') * x = x'' * e \implies e * x = x'' * e \implies e * x = x''$$

Because $e \in G$, it has a left inverse, say e', such that $e' * e = e$. However, because e is a right identity, we must have $e' * e = e'$. Thus, $e = e'$. Now for any x, y, denote by x', y' their left inverses (respectively). What is the left inverse of $x * y$? By Theorem 3.4, we guess that it should be $y' * x'$. We demonstrate that as follows

$$(x * y) * (y' * x') = (x * y) * (y' * x')$$

By way of contradiction, assume that $x * x' = z$, where $z \in G$ is not equal to e. Left multiplying both sides of this equation by x', we have

$$x' * (x * x') = x' * z \implies (x' * x) * x' = x' * z \implies e * x' = x' * z \implies x' * z = x',$$

where the first implication is due to associativity, the second is due to x' being a left inverse, and the final one due to e being the unique right identity and a little re-arrangement. Now, the equation $x' * z = x'$ implies that z is a right identity different from e, which is a contradiction of the uniqueness of the right identity. Thus, it must be the case that $x * x' = e$ so that x' is a right inverse, exactly as desired.

4 Powers of an Element; Cyclic Groups

We use the following definition for the first two problems. In general, for a group G and an element $g \in G$, we have $\langle g \rangle := \{g^n : n \in \mathbb{Z}\}$, where $g^n := \underbrace{g * g * g * \ldots * g}_{n \text{ times}}$.

4.1 Q1

In the case of $(\mathbb{Z}_{10}, +)$, $\langle g \rangle = \{ng : n \in \mathbb{Z}, \text{ and } 0 \leq ng < 10\}$, where the added condition guarantees that we only deal with elements within $\mathbb{Z}_{10}$. Thus,

- $\langle 0 \rangle = \{n \cdot 0 : n \in \mathbb{Z}, \text{ and } 0 \leq n \cdot 0 < 10\} = \{0 : n \in \mathbb{Z}, \text{ and } 0 \leq 0 < 10\} = \{0 : n \in \mathbb{Z}\} = \{0\}$, where the second to last equality follows because the statement $0 \leq 0 < 10$ is always true, independent of n. The final equality is because the typical term preceding the colon does not vary with n.
- $\langle 1 \rangle = \{n \cdot 1 : n \in \mathbb{Z}, \text{ and } 0 \leq n \cdot 1 < 10\} = \{n : n \in \mathbb{Z}, \text{ and } 0 \leq n < 10\} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ because the typical term enumerates all integers, and the second condition requires those integers be between 0 (inclusive) and 10 (exclusive).
- $\langle 2 \rangle = \{n \cdot 2 : n \in \mathbb{Z}, \text{ and } 0 \leq n \cdot 2 < 10\} = \{2n : n \in \mathbb{Z}, \text{ and } 0 \leq 2n < 10\} = \{0, 2, 4, 6, 8\}$ because the typical term enumerates all multiples of 2 so we list all multiples of 2 between 0 (inclusive) and 10 (exclusive).
- $\langle 3 \rangle = \{n \cdot 3 : n \in \mathbb{Z}, \text{ and } 0 \leq n \cdot 3 < 10\} = \{3n : n \in \mathbb{Z}, \text{ and } 0 \leq 3n < 10\} = \{0, 3, 6, 9\}$ because the typical term enumerates all multiples of 3 so we list all multiples of 3 between 0 (inclusive) and 10 (exclusive).
- $\langle 4 \rangle = \{n \cdot 4 : n \in \mathbb{Z}, \text{ and } 0 \leq n \cdot 4 < 10\} = \{4n : n \in \mathbb{Z}, \text{ and } 0 \leq 4n < 10\} = \{0, 4, 8\}$ because the typical term enumerates all multiples of 4 so we list all multiples of 4 between 0 (inclusive) and 10 (exclusive).
- $\langle 5 \rangle = \{n \cdot 5 : n \in \mathbb{Z}, \text{ and } 0 \leq n \cdot 5 < 10\} = \{5n : n \in \mathbb{Z}, \text{ and } 0 \leq 5n < 10\} = \{0, 5\}$ because the typical term enumerates all multiples of 5 so we list all multiples of 5 between 0 (inclusive) and 10 (exclusive).

(*) Note we could also have simplified some of the expressions to figure out which values of n to use and then list the typical terms based on this. For example, we had that $\langle 2 \rangle = \{2n : n \in \mathbb{Z}, \text{ and } 0 \leq 2n < 10\} =$. The second condition can be re-written $0 \leq n < 5$. Thus, the condition says $n \in \{0, 1, 2, 3, 4\}$. We insert those to the typical term of $2n$ to obtain $\{0, 2, 4, 6, 8\}$.

4.2 Q2

In the case of $(G, +)$, where G is the set of all real valued functions on the real line under addition of functions, $\langle g \rangle := \{ng : n \in \mathbb{Z}\}$. Here ng denotes a function such that $(ng)(x) = n \cdot g(x)$ for all $x \in \mathbb{R}$. Therefore, with $g = f$ as given in the problem (defined such that $f(x) = 1$ for all x), we have $(nf)(x) = n \cdot f(x) = n \cdot 1 = n$ for all x. Thus, the set $\langle f \rangle$ is simply the set of constant, integer valued functions. It follows that the configuration from drawing all such functions on one set of axes would be a set of horizontal straight lines, each spaced 1 unit apart vertically from the closest other lines.

4.3 Q3

In the discussion that $(P(X), \triangle)$ is a group on page 20 of the textbook, it was established that $A^{-1} = A$ for every $A \subseteq X$ and that $\emptyset$ is the identity element. Thus, $A \triangle A = \emptyset$ for every $A \subseteq X$. Moreover, $\emptyset \triangle A = A$ (again because $\emptyset$ is the identity element). It is now clear that A^n equals A when n is odd. When $n = 1$, $A^n = A^1 = A$. Consider now an abitrary odd value of $n \geq 1$. Then, $A^{n+1} = A * A^n = A * A = A \triangle A = \emptyset$, implying that $A^{n+2} = A * A^{n+1} = A * \emptyset = A$. As $n + 2$ is the

next odd integer after n, the induction is complete. We can similarly show that A^n equals $\emptyset$ when n is even. When $n = 2$, $A^n = A^2 = A * A = A \triangle A = \emptyset$. Consider now an arbitrary even value of $n \geq 2$. Then, $A^{n+1} = A^n * A = \emptyset * A = \emptyset \triangle A = A$, implying that $A^{n+2} = A^{n+1} * A = A * A = A \triangle A = \emptyset$. As $n + 2$ is the next even integer after n, the inducton is complete.

Finally, we can show that $A^n = A^{-n}$ for every n. This is obviously true when $n = 1$ because $A^n = A^1 = A$ and $A^{-n} = A^{-1} = A$. Suppose $A^n = A^{-n}$ for arbitrary n. Assume n is odd, then $A^n = A$ by the above. It then follows that

$$A^{-(n+1)} = A^{-n-1} = A^{-n} * A^{-1} = A^n * A^{-1} = A^n * A = A^{n+1},$$

which is the statement for $n + 1$. Next assume n is even, then $A^n = \emptyset$ by the above. It then follows that

$$A^{-(n+1)} = A^{-n-1} = A^{-n} * A^{-1} = A^n * A^{-1} = A^n * A = \emptyset * A = \emptyset = A^{n+1},$$

where the final equality follows because $n + 1$ is odd so $A^{n+1} = A$. This is the statement for $n + 1$. All of this shows that A^n is either $\emptyset$ or A for any integer n in the group $(P(X), \triangle)$.

With the above proof complete, the answer is obvious: there are exactly two elements in $\langle x \rangle$, $\emptyset$ and $\{1, 4, 5\}$.

(*) We have extensively used part (i) of Theorem 4.1.

4.4 Q4

In the case of $(\mathbb{Z}_{30}, +)$, we write g^n as ng and the identity element is 0 (cf. page 22 of the textbook). Thus, we seek the smallest $n > 0$ such that $ng \equiv 0 (\text{mod } 30)$ or equivalently, such that ng is a multiple of 30.

- $(n = 10)$ Setting $g = 3$ we have $ng = n \cdot 3 = 3n$. In order to have $3n = 0$ in $(\mathbb{Z}_{30}, +)$, we must have $3n$ equal to a multiple of 30. I.e. we must have $3n = 30k$ for some k. Equivalently, we require $n = 10k$. Minimizing n requires minimizing k so consider $k = 1$, implying $n = 10$. Indeed $ng = 10 \cdot 3 = 30$ is a multiple of 30.
- $(n = 15)$ Setting $g = 4$ we have $ng = n \cdot 4 = 4n$. In order to have $4n = 0$ in $(\mathbb{Z}_{30}, +)$, we must have $4n$ equal to a multiple of 30. I.e. we must have $4n = 30k$ for some k. Equivalently, we require $2n = 15k$. Because the right hand side has factors of 3 and 5, so too must the left hand side. The smallest n satisfying this is $n = 15$ and hence, $k = 2$. Indeed $ng = 15 \cdot 4 = 60$ is a multiple of 30.
- $(n = 5)$ Setting $g = 6$ we have $ng = n \cdot 6 = 6n$. In order to have $6n = 0$ in $(\mathbb{Z}_{30}, +)$, we must have $6n$ equal to a multiple of 30. I.e. we must have $6n = 30k$ for some k. Equivalently, we require $n = 5k$. Minimizing n requires minimizing k so consider $k = 1$, implying $n = 5$. Indeed $ng = 5 \cdot 6 = 30$ is a multiple of 30.
- $(n = 30)$ Setting $g = 7$ we have $ng = n \cdot 7 = 7n$. In order to have $7n = 0$ in $(\mathbb{Z}_{30}, +)$, we must have $7n$ equal to a multiple of 30. I.e. we must have $7n = 30k$ for some k. Because the left hand side has a factor of 7, so too must the right hand side. The smallest k satisfying this is $k = 7$ and hence, $n = 30$. Indeed $ng = 30 \cdot 7 = 210$ is a multiple of 30.
- $(n = 5)$ Setting $g = 18$ we have $ng = n \cdot 18 = 18n$. In order to have $18n = 0$ in $(\mathbb{Z}_{30}, +)$, we must have $18n$ equal to a multiple of 30. I.e. we must have $18n = 30k$ for some k. Equivalently, we require $3n = 5k$. Because the right hand side has a factor of 5, so too must the left hand side. The smallest n satisfying this is $n = 5$ and hence, $k = 3$. Indeed, $ng = 5 \cdot 18 = 90$ is a multiple of 30.

4.5 Q5

We can apply part (iii) of Theorem 4.4 with $n = 18$ and m equal to each of the values given.

($m = 2$) We have $d = (n, m) = (18, 2) = 2$. Thus, $o(x^2) = n/m = 18/2 = 9$. Moreover, $(x^2)^9 = x^{18} = e$.

($m = 3$) We have $d = (n, m) = (18, 3) = 3$. Thus, $o(x^3) = n/m = 18/3 = 6$. Moreover, $(x^3)^6 = x^{18} = e$.

($m = 4$) We have $d = (n, m) = (18, 4) = 2$. Thus, $o(x^4) = n/m = 18/2 = 9$. Moreover, $(x^4)^9 = x^{36} = (x^{18})^2 = e^2 = e$.

($m = 5$) We have $d = (n, m) = (18, 5) = 1$. Thus, $o(x^5) = n/m = 18/1 = 18$. Moreover, $(x^5)^{18} = x^{90} = (x^{18})^5 = e^5 = e$.

($m = 12$) We have $d = (n, m) = (18, 12) = 6$. Thus, $o(x^{12}) = n/m = 18/6 = 3$. Moreover, $(x^{12})^3 = x^{36} = (x^{18})^2 = e^2 = e$.

4.6 Q6

An element $g \in \mathbb{Z}_{45}$ has order 15 if $15g = 0 \mod 45$. Or put another way, we need $15g = 45k$ for some $k \in \mathbb{Z}$. This is equivalent to having $g = 3k$ for some $k \in \mathbb{Z}$. Thus, the complete set of elements of order 15 in $\mathbb{Z}_{45}$ are those elements elements $3k$ such that $0 \leq 3k < 45$. In particular this requires $0 \leq k < 15$. That gives us the following set of elements of order 15:

$$\{0, 3, 6, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36, 39, 42\}.$$

4.7 Q7

By the finite case of Theorem 4.5, the unique elements of $\langle x \rangle$ are $e, x, x^2, \ldots x^{23}$. By Theorem 4.4, part (iii), we can directly compute the order of every such element, x^m, by computing $d = (m, 24)$. The result will give $o(x^m) = 24/d$. The question at hand is, for which $m \in \{0, 1, \ldots, 23\}$, do we obtain $o(x^m) = 4$? I.e. for which m do we have $24/(m, 24) = 4$ or $(m, 24) = 6$. Because 6 must divide m, we consider $m \in \{6, 12, 18\}$:

($m = 6$) We have $(6, 24) = 6$ so $o(x^6) = 4$.

($m = 12$) We have $(12, 24) = 12$ so $o(x^{12}) \neq 4$.

($m = 18$) We have $(18, 24) = 6$ so $o(x^{18}) = 4$.

Thus, the only elements of order 4 are x^6 and x^{18}.

4.8 Q8

Yes, it is generated by the element 2, i.e. $\langle 2 \rangle = 2\mathbb{Z}$. This is clearly true, because the left hand side is the set of elements of the form $2k$ for $k \in \mathbb{Z}$, while the right hand side is precisely the same thing (the set of even integers is simply the set of integers of the form $2k$ for $k \in \mathbb{Z}$).

4.9 Q9

The proof of this is very similar to the proof that $(\mathbb{Q}, +)$ is not cyclic on page 39 of the textbook. The only difference is that our special case is $q = 1$ rather than $q = 0$. $q = 1$ could not be a generator of the group because $1^i = 1$ for all i so it cannot generate all positive rational numbers.

Now suppose that some positive $q \neq 1$ were a generator for $(\mathbb{Q}^+, \cdot)$. If $q > 1$, then $q^i > q$ for all $i > 1$ and $q^i < q$ for all $i < 1$. In particular $q^2 > q$ so that $\frac{q^2+q}{2}$ is a positive rational number[7] halfway between q and q^2. Thus, it is obviously not equal to q^i for $i \in \{1, 2\}$. Moreover, since $q^i \geq q^2 > \frac{q^2+q}{2}$

[7]This is so because the positive rationals are closed under multiplication so q^2 is a positive rational. The sum of two positive rational numbers is a positive rational number so $q + q^2$ is a positive rational number. Finally the positive rational numbers are closed under multiplication so multiplying $q + q^2$ and $\frac{1}{2}$ yields a positive rational number.

for all $i \geq 2$, $\frac{q^2+q}{2}$ cannot be equal to q^i for any $i \geq 1$. Finally, since $q^i \leq q < \frac{q^2+q}{2}$ for all $i \leq 1$, $\frac{q^2+q}{2}$ cannot be equal to q^i for any $i \leq 1$. Consequently, no $q > 1$ can be a generator for $(\mathbb{Q}^+, \cdot)$.

A symmetric argument applies if $q < 1$. In this case $q^i < q$ for all $i > 1$ and $q^i > q$ for all $i < 1$. Thus, $\frac{q+q^2}{2}$ will be a positive rational halfway between q^2 and q (this time with $q^2 < q$.) Thus, it is obviously not equal to q^i for $i \in \{1, 2\}$. Moreover, since $q^i \leq q^2$ for all $i \geq 2$, $\frac{q+q^2}{2}$ cannot be equal to q^i for any $i \geq 1$. Finally, since $q^i \geq q > \frac{q+q^2}{2}$ for all $i \leq 1$, $\frac{q+q^2}{2}$ cannot be equal to q^i for any $i \leq 1$. Thus, there can be no generator $q < 1$ either and we finally conclude that $(\mathbb{Q}^+, \cdot)$ is not cyclic.

4.10 Q10

(a) Consider any $a, b \in \{1, 2, 3, 4, 5, 6\}$, then $ab > 0$ because $a, b > 0$. In particular, we have $ab \geq 1$. It follows that $\overline{ab} \geq 1$ and since $\overline{ab}$ is the remainder of ab when divided by 7 we have $\overline{ab} < 7$. Thus, $1 \leq \overline{ab} \leq 6$ so that $\bigodot$ is a binary operation. Let $a, b, c \in \{1, 2, 3, 4, 5, 6\}$, then

$$a \bigodot (b \bigodot c) = a \bigodot \overline{b \cdot c} = \overline{a \cdot \overline{b \cdot c}}$$

Let us suppose that $b \cdot c = 7q + r$, with $0 \leq r < 7$ by the Division Algorithm. Then, $\overline{b \cdot c} = r$. Consequently, $a \cdot b \cdot c = 7aq + a \cdot \overline{b \cdot c}$. This implies that $\overline{a \cdot b \cdot c} = \overline{a \cdot \overline{b \cdot c}}$. Thus, the right hand side of the above is $\overline{a \cdot b \cdot c}$. Now consider

$$(a \bigodot) \bigodot c = \overline{a \cdot b} \bigodot c = \overline{\overline{a \cdot b} \cdot c}.$$

By a similar argument as above, the right hand side is $\overline{a \cdot b \cdot c}$. Thus, $a \bigodot (b \bigodot c) = (a \bigodot b) \bigodot c$ and $\bigodot$ is associative. Clearly, 1 is an identity because for any $a \in \{1, 2, 3, 4, 5, 6\}$ we have $a \bigodot 1 = \overline{a \cdot 1} = \overline{a} = a$ and $1 \bigodot a = \overline{1 \cdot a} = \overline{a} = a$. Finally, we can directly observe the following inverse pairs:

$1 \bigodot 1 = \overline{1 \cdot 1} = \overline{1} = 1$.
$2 \bigodot 4 = \overline{2 \cdot 4} = \overline{8} = 1$. Similarly, $4 \bigodot 2 = 1$.
$3 \bigodot 5 = \overline{3 \cdot 5} = \overline{15} = 1$. Similarly, $5 \bigodot 3 = 1$.
$6 \bigodot 6 = \overline{6 \cdot 6} = \overline{36} = 1$.

(b) Yes it is cyclic and 3 generates the group:

$3^1 = 3$.
$3^2 = \overline{3 \cdot 3} = \overline{9} = 2$.
$3^3 = 3 * 3^2 = 3 * 2 = \overline{3 \cdot 2} = \overline{6} = 6$.
$3^4 = 3 * 3^3 = 3 * 6 = \overline{3 \cdot 6} = \overline{18} = 4$.
$3^5 = 3 * 3^4 = 3 * 4 = \overline{3 \cdot 4} = \overline{12} = 5$.
$3^6 = 3 * 3^5 = 3 * 5 = \overline{3 \cdot 5} = \overline{15} = 1$.

5 also generates the group. One can check that in a similar manner.

4.11 Q11

4.12 Q12

First consider a^n for $n \geq 1$. We have $a^2 = a * a = a + a - 1 = 2a - 1$. Thus, $a^3 = a * a^2 = a * (2a - 1) = a + (2a - 1) - 1 = 3a - 2$. It appears that $a^n = na - n + 1$. We already have a few base cases, so assume $a^n = na - n + 1$ for arbitrary $n \geq 1$. Then,

$$a^{n+1} = a * a^n = a * (na - n + 1) = a + (na - n + 1) - 1 = (n + 1)a - n = (n + 1)a - (n + 1) + 1,$$

which is exactly the statement for $n + 1$. This statement is also true for $n \leq 0$. To prove that, we need to find a^{-1}, which in turn means we need to find the identity element e in this group. If the

above is to be correct for $n \leq 0$, then setting $n = 0$ suggests that $e = a^0 = 0 \cdot a - 0 + 1 = 1$. Indeed, $a * 1 = a + 1 - 1 = a$ and $1 * a = 1 + a - 1 = a$.

Next, setting $n = -1$ in the above suggests $a^{-1} = (-1) \cdot a - (-1) + 1 = 2 - a$. Indeed $a * (2 - a) = a + (2 - a) - 1 = 1$ and $(2 - a) * a = (2 - a) + a - 1 = 1$. Thus, replacing a by a^{-1} in $a^n = na - n + 1$, we obtain

$$a^{-n} = (a^{-1})^n = na^{-1} - n + 1 = n(2 - a) - n + 1 = 2n - na - n + 1 = (-n)a - (-n) + 1,$$

which is exactly the statement for $-n$. Together with our proof that $a^0 = e = 1$, we have shown that for all n, $a^n = na - n + 1$.

Now, if a is to be a generator for $\mathbb{Z}$, we need a to be such that for all $x \in \mathbb{Z}$, we can find an n such that $a^n = x$. This implies

$$na - n + 1 = x \implies n(a - 1) = x - 1 \implies n = \frac{x - 1}{a - 1}.$$

However, for this n to be an integer, we need $a-1$ to be either 1 or -1. Were it not one of those values, then $\frac{x-1}{a-1}$ would, in general, be non-integral. It follows that either 2 ($a - 1 = 1$) or 0 ($a - 1 = -1$) can be a generator and that this group is cyclic. Indeed, with $a = 0$, we have $a^n = n \cdot 0 - n + 1$. To obtain $x \in \mathbb{Z}$ we need $x = a^n = -n + 1$, which implies $n = 1 - x$.

(*) It is worth noting that 0 and 2 are inverses of each other in this group. In this case, Problem 4.16 guarantees that if 0 generates the group, then $0^{-1} = 2$ also generates the group. Because $\mathbb{Z}$ is infinite, Problem 4.17 guarantees that *only* 0 and 2 can generate this group.

4.13 Q13

Let g be an arbitrary element of a finite group G. Then consider the sequence of elements $g, g^2, g^3, \ldots$ Observe that each $g^i \in G$. This is clearly true when $i = 1$ because $g \in G$. Now suppose it is true for arbitrary i that $g^i \in G$. Then, $g^{i+1} := g * g^i$ is an element of G because the right hand side is the binary operation $*$ applied to a pair of elements, g and g^i, both of which are in G. Thus, $g^{i+1} \in G$ and the induction is complete.

With that observation we can now show that there must be a repeat element at some point in the sequence $g, g^2, g^3, \ldots$ In fact, by the pigeonhole principle, $g^{|G|+1}$ must be equal to some g^i with $i \leq |G|$. If that were not the case, then $g, g^2, \ldots, g^{|G|}, g^{|G|+1}$ would be a set of $|G| + 1$ unique elements all of which belong to G. However, there are only $|G|$ such unique elements so this cannot be possible. Thus, we have $g^i = g^{|G|+1}$, which we can write as $g^i * e = g^{|G|+1} * e$. We can apply the left Cancellation Law to this equation i times to obtain $e = g^{|G|+1-i} * e$ or $g^{|G|+1-i} = e$ which shows that g has finite order. Because g was arbitrary, we conclude that every element of a finite group must have finite order.

(*) It is worth noting that $|G| + 1 - i \geq 1$ because $1 \leq i \leq |G|$. That implies that $-|G| \leq -i \leq -1$, which in turn implies $1 \leq |G| + 1 - i \leq |G|$. Thus, we have not only shown that g has finite order (because $|G| + 1 - i \geq 1$), but we have also shown that the order of g is at most $|G|$.

4.14 Q14

Any group $(P(X), \triangle)$, where X is infinite meets this requirement. We know that for any $A \subseteq X$, that $A \triangle A = \emptyset$. Thus, no matter what set X, $(P(X), \triangle)$ has the property that every element has order 2. In particular, X is infinite, then $P(X)$ is infinite so that $(P(X), \triangle)$ is an infinite group where every element has finite order.

4.15 Q15

We simply apply the Division Algorithm directly.

(a) First, $(321, 123)$:

$$\begin{aligned}
321 &= 2 \cdot 123 + 75 \\
123 &= 1 \cdot 75 + 48 \\
75 &= 1 \cdot 48 + 27 \\
48 &= 1 \cdot 27 + 21 \\
27 &= 1 \cdot 21 + 6 \\
21 &= 3 \cdot 6 + 3 \\
6 &= 2 \cdot 3 + 0.
\end{aligned}$$

Thus, $(321, 123) = 3$. We invert the equations to find (x, y) such that write $321x + 123y = 3$

$$\begin{aligned}
3 &= 21 - 3 \cdot 6 \\
3 &= 21 - 3 \cdot (27 - 1 \cdot 21) \\
3 &= 4 \cdot 21 - 3 \cdot 27 \\
3 &= 4 \cdot (48 - 1 \cdot 27) - 3 \cdot 27 \\
3 &= 4 \cdot 48 - 7 \cdot 27 \\
3 &= 4 \cdot 48 - 7 \cdot (75 - 1 \cdot 48) \\
3 &= 11 \cdot 48 - 7 \cdot 75 \\
3 &= 11 \cdot (123 - 1 \cdot 75) - 7 \cdot 75 \\
3 &= 11 \cdot 123 - 18 \cdot 75 \\
3 &= 11 \cdot 123 - 18 \cdot (321 - 2 \cdot 123) \\
3 &= 47 \cdot 123 - 18 \cdot 321.
\end{aligned}$$

Thus, $(x, y) = (47, -18)$.

(b) First, $(862, 347)$:

$$\begin{aligned}
862 &= 2 \cdot 347 + 168 \\
347 &= 2 \cdot 168 + 11 \\
168 &= 15 \cdot 11 + 3 \\
11 &= 3 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0.
\end{aligned}$$

Thus, $(862, 347) = 1$. We invert the equations to find (x, y) such that write $862x + 347y = 1$

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
1 &= 3 - 1 \cdot (11 - 3 \cdot 3) \\
1 &= 4 \cdot 3 - 1 \cdot 11 \\
1 &= 4 \cdot (168 - 15 \cdot 11) - 1 \cdot 11 \\
1 &= 4 \cdot 168 - 61 \cdot 11 \\
1 &= 4 \cdot 168 - 61 \cdot (347 - 2 \cdot 168) \\
1 &= 126 \cdot 168 - 61 \cdot 347 \\
1 &= 126 \cdot (862 - 2 \cdot 347) - 61 \cdot 347 \\
1 &= 126 \cdot 862 - 313 \cdot 347.
\end{aligned}$$

Thus, $(x, y) = (126, -313)$.

(c) First, $(7469, 2464)$:

$$7469 = 3 \cdot 2464 + 77$$
$$2464 = 32 \cdot 77 + 0.$$

Thus, $(7469, 2464) = 77$. We can immediately write $77 = 1 \cdot 7469 - 3 \cdot 2464$ so that $(x, y) = (1, -3)$ in $77 = 7469x + 2464y$.

4.16 Q16

If $G = \langle x \rangle$ then for any $g \in G$ we have $g = x^j$ for some $j \in \mathbb{Z}$.

4.17 Q17

4.18 Q18

(ii) The statement of this part of the Theorem is equivalent to saying that the inverse of x^n is x^{-n}. To wit,

$$x^n * x^{-n} = x^{n+(-n)} = x^{n-n} = x^0 = e,$$

and

$$x^{-n} * x^n = x^{(-n)+n} = x^{-n+n} = x^0 = e,$$

where we used the first part of the Theorem to add exponents. These equations are sufficient to show that the inverse of x^n is x^{-n}.

(iii) We take a different approach and prove (a) $(x^m)^n = x^{nm}$ (for all n, m) and (b) $x^{nm} = (x^n)^m$ (for all n, m) by induction on n for an arbitrary m.

(a) When $n = 1$ the left hand side is $(x^m)^n = (x^m)^1 = x^m$ and the right hand side is $x^{nm} = x^{1 \cdot m} = x^m$. Now suppose that $(x^m)^n = x^{nm}$ and multiply both sides by x^m. The left hand side simply becomes $(x^m)^{n+1}$ since we have an additional copy of x^m. The right hand side is $x^m * x^{nm} = x^{m+nm} = x^{(n+1)m}$. Thus, $(x^m)^{n+1} = x^{(n+1)m}$, which is exactly the statement for $n + 1$.

(b)

4.19 Q19

4.20 Q20

First, we show for any $a, x \in G$ and $n \geq 1$, we have $(xax^{-1})^n = xa^n x^{-1}$. When $n = 1$, the left hand side is $(xax^{-1})^n = (xax^{-1})^1 = xax^{-1}$, while the right hand side is $xa^n x^{-1} = xa^1 x^{-1} = xax^{-1}$. Now suppose for arbitrary $n \geq 1$ that $(xax^{-1})^n = xa^n x^{-1}$. Right multiplying by xax^1 we obtain

$$(xax^{-1})^{n+1} = xa^n x^{-1} xax^{-1} = xa^n eax^{-1} = xa^n ax^{-1} = xa^{n+1} x^{-1},$$

which is the equation for $n + 1$ so the induction is complete.

Now suppose $o(a) = n < \infty$. Then, we know $a^n = e$. Left multiplying both sides by x and right multiplying by x^{-1} we obtain $xa^n x^{-1} = xex^{-1} = xx^{-1} = e$. From the above we conclude that $(xax^{-1})^n = xa^n x^{-1} = e$, which implies $o(xax^{-1}) \leq n$. Now suppose (by way of contradiction) that there is an $m < n$ such that $(xax^{-1})^m = e$. By the above, we have $xa^m x^{-1} = (xax^{-1})^m = e$, which implies $xa^m x^{-1} = e$. Left multiplying by x^{-1} and right multiplying by x we have $a^m = e$, which

implies $o(a) \leq m < n$, which is a contradiction. Thus, we conclude there is no such $m < n$ and $o(xax^{-1}) \geq n$. Combining this with our proof that $o(xax^{-1}) \leq n$, we conclude $o(xax^{-1}) = n = o(a)$.

Next suppose $o(a) = \infty$. Then, $a^n \neq e$ for every $n \geq 1$. Suppose (by way of contradiction) that there is an $n \geq 1$ such that $(xax^{-1})^n = e$. Then, by the above, we have $xa^nx^{-1} = (xax^{-1})^n = e$, which implies $xa^nx^{-1} = e$. Left multiplying by x^{-1} and right multiplying by x we have $a^n = e$, which implies $o(a) \leq n < \infty$. That contradicts $o(a) = \infty$, so the assumption cannot be true and we conclude $(xax^{-1})^n \neq e$ for every $n \geq 1$, i.e. $o(xax^{-1}) = \infty$.

4.21 Q21

Suppose $o(xy) = n$

4.22 Q22

First, we show for any $x, y \in G$ and $n \geq 1$, that $(xy)^n = x^n y^n$. When $n = 1$, the left hand side is $(xy)^n = (xy)^1 = xy$, while the right hand side is $x^n y^n = x^1 y^1 = xy$. Now suppose for arbitrary $n \geq 1$ that $(xy)^n = x^n y^n$. Right multiplying by xy we obtain

$$(xy)^{n+1} = x^n y^n xy = x^n y^n yx = x^n y^{n+1} x = x^n xy^{n+1} = x^{n+1} y^{n+1},$$

which is exactly the equation for $n + 1$ so the induction is complete.

Now consider $(xy)^{o(x)o(y)}$. By the above, we have

$$(xy)^{o(x)o(y)} = x^{o(x)o(y)} y^{o(x)o(y)} = \left(x^{o(x)}\right)^{o(y)} \left(y^{o(y)}\right)^{o(x)} = e^{o(y)} e^{o(x)} = ee = e,$$

which shows $o(xy) \leq o(x)o(y)$ and is thus, finite. By the division algorithm, we can find integers q, r such that $o(x)o(y) = qo(xy) + r$ and $0 \leq r < o(xy)$. We have

$$e = (xy)^{o(x)o(y)} = (xy)^{qo(xy)+r} = (xy)^{qo(xy)}(xy)^r = \left((xy)^{o(xy)}\right)^q (xy)^r = e^q (xy)^r = e(xy)^r = (xy)^r.$$

If $r > 0$ then we have $1 \leq r < o(xy)$ with $(xy)^r = e$. However, $o(xy)$ is the smallest integer n such that $(xy)^n = e$ so we must have $r = 0$. Thus, $o(x)o(y) = qo(xy)$, which implies $o(xy)$ divides $o(x)o(y)$.

4.23 Q23

From Problem 4.22, we know that there is a q such that $o(xy) = qo(x)o(y)$. Since $o(xy), o(x), o(y) \geq 1$ it must also be the case that $q \geq 1$. Moreover, because $(o(x), o(y)) = 1$ we know there exist n_x, n_y such that $n_x o(x) + n_y o(y) = 1$. Multiplying both sides by $o(y)$ we obtain

$$n_x o(x)o(y) + n_y o(y)^2 = o(y) \implies n_x qo(xy) + n_y o(y)^2 = o(y) \implies$$

4.24 Q24

The result is that $o(x) = \infty$. First, we claim that $x^{2n} = yx^n y^{-1}$ for every $n \geq 1$. The base case $n = 1$ is given by assumption. Now suppose this holds for arbitrary $n \geq 1$. Then,

$$x^{2n} = yx^n y^{-1} \implies x^{2n}x^2 = (yx^n y^{-1})(yxy^{-1}) \implies x^{2n+2} = yx^n y^{-1} yxy^{-1} \implies x^{2(n+1)} = yx^{n+1} y^{-1},$$

which is precisely the statement for $n + 1$.

Next, we show by induction that $x^n \neq e$ for every $n \geq 1$. Observe that we are given $x \neq e$. Suppose $x^2 = e$. Then, we have

$$e = x^2 = yxy^{-1} \implies e * y = (yxy^{-1})y \implies y = (yx)(y^{-1}y) = (yx)e = yx \implies x = e,$$

which is a contradiction. Thus, $o(x) \geq 3$. Now consider the given equation and square both sides to obtain

$$(x^2)^2 = (yxy^{-1})^2 \implies x^4 = (yxy^{-1})(yxy^{-1}) = yx^2y^{-1} = y(yxy^{-1})y^{-1}$$

$$(x^2)^2 = (yxy^{-1})^2 \implies x^4 = (yxy^{-1})(yxy^{-1}) = yx^2y^{-1} = y(yxy^{-1})y^{-1}$$

4.25 Q25

4.26 Q26

4.27 Q27

The statement is clearly true when $s = 1$ because there is only one term in $q_1 \dots q_s = q_1$. Thus, if p divides $q_1 \dots q_s$ it divides q_1, i.e. some q_i. Assume the statement is true for fixed, but arbitrary $s \geq 1$. Now suppose p divides $q_1 \dots q_s \cdot q_{s+1}$. There are two cases:

- Case 1: p divides q_{s+1}. Then clearly p divides some q_i, namely $i = s + 1$.
- Case 2: p does not divide q_{s+1}. Then because p is prime, the greatest common divisor of p and q_{s+1} is 1. By Theorem 4.3[8], p must divide $q_1 \dots q_s$. By the inductive hypothesis, p must divide some q_i (where $1 \leq i \leq s$).

In either case we have shown that p divides q_i for some i, exactly as desired.

4.28 Q28

4.29 Q29

4.30 Q30

4.31 Q31

4.32 Q32

4.33 Q33

[8]Take $r = p$, $s = q_{s+1}$ and $t = q_1 \dots q_s$.