Solutions Guide to Abstract Algebra

Brian Ward*

August 31, 2020

Abstract

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

Contents

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,

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

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

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,

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

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

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 1, 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.

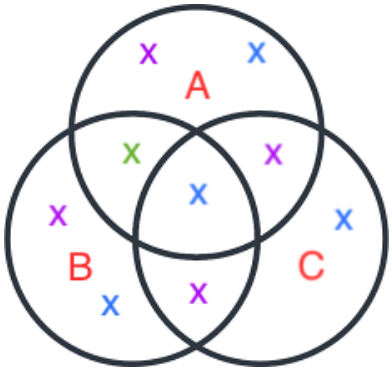

Figure 1: Graphic for the solution to Problem 1.2.

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)

(j)

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

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 *This exercise is made a lot easier by utilizing the following.*

$$\textit{For any sets, } C \textit{ and } D, \ (C \triangle D)^c = (C \cap D) \cup (C \cup D)^c.$$

The 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) $x \in A$, $x \notin B\triangle C$. In case (a), there are two

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.