

# Solutions Guide to Abstract Algebra

Brian Ward\*

August 26, 2020

## Abstract

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

## Contents

<b>0</b>	<b>Sets and Induction</b>	<b>1</b>
0.1	Q1 . . . . .	1
0.2	Q2 . . . . .	2
0.3	Q3 . . . . .	2
0.4	Q4 . . . . .	2
0.5	Q5 . . . . .	3
0.6	Q6 . . . . .	3
0.7	Q7 . . . . .	3
0.8	Q8 . . . . .	3
0.9	Q9 . . . . .	4
0.10	Q10 . . . . .	4
0.11	Q11 . . . . .	5
0.12	Q12 . . . . .	5
0.13	Q13 . . . . .	5
0.14	Q14 . . . . .	5
0.15	Q15 . . . . .	5
0.16	Q16 . . . . .	6
0.17	Q17 . . . . .	6
0.18	Q18 . . . . .	6
0.19	Q19 . . . . .	7

## 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

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

---

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

## 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

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

As for the right hand side we have

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

and

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

Thus,

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

## 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  $x \in (A \cup B) \cap (A \cup C)$ . 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  $h_1, h_2, \dots, h_m, h_{m+1}$  and considers two subsets of size  $m$ . Subset 1 is  $\{h_1, h_2, \dots, h_m\}$  and subset 2 is  $\{h_2, \dots, h_m, h_{m+1}\}$ . The intersection of these two sets is  $S := \{h_2, \dots, h_m\}$ . 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

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

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

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

We can further simplify the right hand side as

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

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

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

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

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

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

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

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

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

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

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

Let  $E := 2 + 4 + 6 + \dots + 2n$  and  $O := 1 + 3 + 5 + \dots + (2n+1)$ . Then clearly  $O - (2n+1) + E = 1 + 2 + \dots + (2n-1) + 2n = n(2n+1)$ . 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  $k$  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

## 0.13 Q13

## 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

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

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

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

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

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

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

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

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

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

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

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

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  $\underbrace{2 \cdot 2 \cdot 2 \dots 2}_{n \text{ times}} = 2^n$  possible subsets.

## 0.18 Q18

For  $k=1$  we check if  $f_{5,1} = f_5$  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,  $f_{5(n+1)} = 5f_{5n+1} + 3f_{5n} = 5f_{5n+1} + 3 \cdot 5k = 5(f_{5n+1} + 3k) := 5k'$ , 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  $n + 1$ .