Herstein Topics in Algebra Second Edition Exercise Solutions

Gaurish Sharma

December 21, 2023

Contents

1 Set Theory

1.1 Solution 1

1. $A \subseteq B$ and $B \subseteq C$. Then let $x \in A \Rightarrow x \in B \Rightarrow x \in C$. Hence, for all $x \in A, x \in C$. Therefore $A \subseteq C$.

2. $B \subseteq A$. This means $x \in B \Rightarrow x \in A$. So, all elements of B are in A. Now, we show that $A \cup B = A$. Let $x \in A \cup B$ then $x \in A$ or $x \in B$.

   If $x \in A$ then we have nothing more to show. Otherwise if $x \in B$. Since B is a subset of A. This means that $x \in A$ as well. Hence in either eventuality $x \in A$. So, for all $x \in A \cup B$, $x \in A$. Hence $A \cup B \subseteq A$.

   It remains to show that $A \subseteq A \cup B$. Let $x \in A$. then by definition of union $x \in A \cup B$.

   Hence, for all $x \in A$, $x \in A \cup B$. Therefore, $A \subseteq A \cup B$.

   Hence we haveshown that $A \subseteq A \cup B$ and $A \cup B \subseteq A$. Therefore, $A \cup B = A$.

3. $B \subseteq A$, so $x \in B \Rightarrow x \in A$. Now, let $x \in B \cup C$. then $x \in B$ or $x \in C$.

   If $x \in B$ then $x \in A$, hence $x \in A \cup C$.

   Otherwise if $x \in C$. then $x \in A \cup C$ by definition of union.

   So, in either eventuality $x \in A \cup C$. Now, we show that $B \cap C \subseteq A \cap C$.

   If $x \in B \cap C$, $x \in B$ and $x \in C$. Since, $x \in B$, $x \in A$. So, $x \in A$. and $x \in C$. Therefore, $x \in A$ and $x \in C$. Therefore, $x \in A \cap C$.

1.2 Solution 2

1. Let $x \in A \cap B$ then $x \in A$ and $x \in B$. Hence, $x \in A \cap B$ by definition. Therefore, $A \cap B \subseteq B \cap A$.

   Let $x \in B \cap A$, then $x \in B$ and $x \in A$. Hence $x \in A \cap B$. Therefore, $B \cap A \subseteq A \cap B$.

   Now we show that $A \cup B = B \cup A$. Similar to above, trivial.

2. Let $x \in A \cap (B \cap C)$. Then $x \in A$ and $x \in B \cap C \Rightarrow x \in B$ and $x \in C$. Hence $x \in A$ and $x \in (B \cap C)$. Therefore by definition $x \in A \cap (B \cap C)$.

1.3 Solution 3

1. Let $x \in A \cup (B \cap C)$, then $x \in A$ or $x \in B \cap C$.

   If $x \in A$ the $x \in (A \cup B)$ and $x \in (A \cup C)$. Hence, $x \in (A \cup B) \cap (A \cup C)$.

   Otherwise if $x \in B \cap C$, $x \in B$and $x \in C$. So, $x \in A \cup B$ and $x \in A \cup C$. Hence, $x \in (A \cup B) \cap (A \cup C)$.

   Hence in either eventuality $x \in (A \cup B) \cap (A \cup C)$. Therefore,

   $$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C) .$$

   Now, let $x \in (A \cup B) \cap (A \cup C)$. So, $x \in A \cup B$ and $x \in A \cup C$.

Since, $x \in A \cup B$, $x \in A$ or $x \in B$. If $x \in A$ then $x \in A \cup (B \cap C)$. If $x \in B$ then since we know that $x \in A \cup C$. x is also in either A or C. If $x \in B$ then since we know $x \in A \cup C$. x is also in either A or C. If its in A then $x \in A \cup (B \cap C)$ again holds. As we have that $x \in B \Rightarrow x \in B \cap C \Rightarrow x \in A \cup (B \cap C)$. Therefore, $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. We have proven the subset relations in both directions. Hence, $(A \cap C) \cap (A \cup C) = A\,(B \cap C)$.

1.4 Solution 4

1. Let $x \in (A \cup B)' = (A \cup B) - S$. Hence, $x \in A \cup B$ but $x \notin S$. If $x \in A \cup B$, then $x \in A$, $x \in B$. B since $x \notin S$ then in both of these cases we have $x \in A - S = A'$ and $x \in B - S = B'$ respectively. Hence in both cases we have $x \in A' \cup B'$. Hence, $A \cup B \subseteq A' \cap B'$.

   Now we need to show reverse containment. Let $x \in A' \cap B'$ then $x \in A'$ and $x \in B'$. Hence, $x \in A$ and $x \notin B$. Therefore, $x \in (A \cup B)'$. Hence, $A' \cup B'$. Hence, $A' \cap B' \subseteq (A \cup B)'$.

2. We first show $(A \cup B)' \subseteq A' \cap B'$. Let $x \in (A \cup B)'$ then $x \notin A \cup B$. Hence, $x \notin B$, $x \notin A$. If $x \notin A$. Then $x \in A'$ and similarly $x \in B'$. Hence $x \in A' \cap B'$. Therefore, $(A \cup B)' \subseteq A' \cap B'$. Now, reverse containment. Let $x \in A' \cap B'$ then $x \in A'$ and $x \in B'$. So, $x \notin A$ and $x \notin B$. Hence, $x \notin A \cup B$ and so $x \in (A \cup B)'$.

1.5 Solution 5

$A \cap B \subseteq A$ and $A \cap B \subseteq B$. So,

$$o\,(A \cup B) = o\,(A - B) + o\,(B - A) + o\,(A \cap B)$$
.

But $o\,(A - b) = o(A) - o\,(A \cap B)$ and $o\,(B - A) = o\,(B) - o\,(A \cap B)$

$$\begin{aligned} o\,(A \cup B) &= o\,(A) - o\,(A \cap B) + o\,(B) - o\,(A \cap B) + o\,(A \cap B) \\ &= o\,(A) + o\,(B) - o\,(A \cap B) \end{aligned}$$
.

1.6 Solution 9

$$\begin{aligned} (A + B) + C &= ((A - B) \cup (B - A)) + C \\ &= (((A - B) \cup (B - A)) - C) \cup (C - ((A - B) \cup (B - A)))\,. \end{aligned}$$

Now we expand the RHS,

$$\begin{aligned} A + (B + C) &= A + ((B - C) \cup (C - B)) \\ &= (A - ((B - C) \cup (C - B))) \cup (((B - C) \cup (C - B)) - A)\,. \end{aligned}$$

Now, let $x \in (A + B) + C$, then there are two cases

- x is an element of $((A - B) \cup (B - A)) - C$. If this is the case then we know that $x \in (A - B)$ or $x \in (B - A)$. However, in either case $x \notin C$. We examine both cases,
  - $x \in (A - B)$ and $x \notin C$: In this case we know that $x \notin B \cup C$. So it is definitely not in a reduced version of this union which is $(B - C) \cup (C - B)$ as this is just removing further elements from B and C before doing a union. Hence $x \notin (B - C) \cup (C - B)$ but $x \in A$. Therefore, $x \in A - ((B - C) \cup (C - B))$ and hence $x \in (A - ((B - C) \cup (C - B))) \cup (((B - C) \cup C - B) - A)$. Hence, in this case the subset relation $(A + B) + C \subset A + (B + C)$ holds.
  - $x \in (B - A)$ and $x \notin C$. Hence, $x \notin B \cap C$. So, it is in $(B - C) \cup (C - B)$ as this is the same as $(B \cup C) - (B \cap C)$ by definition of $B + C$. However, $x \notin A$. Therefore, $x \in ((B - C) \cup (C - B)) - A$ and hence $x \in (A - ((B - C) \cup (C - B))) \cup (((B - C) \cup (C - B)) - A)$. Hence, in this case the subset relation $(A + B) + C \subset A + (B + C)$ holds.
  - not bothered rn come back to this later too tedious

1.7 Solution 10

1. Nope, transitivity is not guaranteed.
2. Nope, transitivity is not satisfied.
3. Yep, all three conditions satisfied, transitivity since uniqueness of father, the other two are trivial.
4. Yep, all three conditions satisfied.

1.8 Solution 11

Not sure about this one.

1.9 Solution 12

The relation of concern is defined as follows. The set S of all integers and let $n > 1$ be a fixed integer. Define for $a, b \in S$, $a \sim b$ if $a - b$ is a multiple of n.

We first prove that this relation is an equivalence relation.

Let $a \in S$ then, $a - a = 0$. Hence, $a \sim a$. Therefore, this relation is reflexive.

Let $a, b \in S$ and $a \sim b$. Then $a - b = k$ where k is a multiple of n. Hence, $b - a = -k$ and $-k$ is also a multiple of n. Therefore, $b \sim a$. Hence, this relation is symmetric.

Let $a, bandc \in S$ and $a \sim b$ and $b \sim c$. Then we know that $a - b$ and $b - c$ are multiples of n. So,

$$a - b = pn \tag{1}$$
$$b - c = qn. \tag{2}$$

For some $p, q \in \mathbb{Z}$. Now we consider (1) + (2),

$$\begin{aligned} a - b + b - c &= pn - qn \\ a - c &= (p - q)\, n. \end{aligned}$$

Since, $p - q \in \mathbb{Z}$ as $p, q \in \mathbb{Z}$. Therefore, $a - c$ is a multiple of n. Hence, $a - c$. Therefore, this relation is transitive as well.

So, this relation is, reflexive, symmetric and transitive. Hence this is an equivalence relation.

Now we show that there are only n, equivalence classes for this relation. Note that,

$$\begin{aligned} cl(0) &= \{m \times n \mid m \in \mathbb{Z}\} \\ cl(1) &= \{m \times n + 1 \mid m \in Z\} \\ cl(2) &= \{m \times n + 2 \mid m \in Z\} \\ &\vdots \\ cl(n) &= \{m \times n \mid m \in \mathbb{Z}\} = cl(0). \end{aligned}$$

Hence, by inspection we notice that the equivalence classes start cycling every n terms n. It is also clear that, $\{cl(0), cl(1), \ldots, cl(n-1)\}$, are distinct equivalence classes. Now to show that only n equivalence classes exist we show that $cl(k) \in \{cl(0), \ldots, cl(n-1)\}$ for all $k \in \mathbb{Z}$.

Now, let $k \in \mathbb{Z}$, the we know that, $mod(k, n) = a$ where $m \in \{0, \ldots, n-1\}$.

Therefore, $cl(k) = \{m \times n + a \mid m \in \mathbb{Z}\} \in \{cl(0), cl(1), \ldots, cl(n-1)\}$.

Hence, there are n equivalence classes for this equivalence relation which are $\{cl(0), \ldots, cl(n-1)\}$.

1.10 Solution 13

We state theorem 1.1.1 first below,

> **Theorem 1.** The distinct equivalence classes of an equivalence relation on A, provide us with a decomposition of A as a union of mututally disjoint subsets Conversely, given a decomposition of A as a union of mutually disjoint, non empty subsets, we can define an equivalence relation on A for which these subsets are distinct equivalence classes.

Proof. Let the equivalence relation on A be denoted by $\sim$. We first notice that since for any $a \in A$, $a \sim a$, $cl(a)$, whence the union of the $cl(a)'s$ is all of A. We now assert that given two equivalence classes they are either equal or disjoint. For, suppose that $cl(a)$ and $cl(b)$, are not disjoint; then there is an element $x \in cl(a) \cap cl(b)$. Since $x \in cl(a)$, $a \sim x$; since $x \in cl(b)$, $b \sim x$, whence by symmetry of the relation, $x \sim b$. However, $a \sim x$ and $x \sim b$ by the transitivity of the relation forces $a \sim b$. Suppose now that $y \in cl(b)$; thus $b \sim y$. However, from $a \sim b$ and $b \sim y$, we deduce that $a \sim y$, that is $y \in cl(a)$. Therefore, every element in $cl(b)$ is in $cl(a)$ Which proves that $cl(b) \subset cl(a)$. The converse of this argument implies $cl(a) = cl(b)$ We have thus shown that distinct $cl(a)'s$ are mutually disjoint and that their union is A. This proves the first half of the theorem. Now for the other half.

Suppose that $A = \bigcup_{\alpha \in T} A_\alpha$, where the A_α are mutually disjoint, nonempty sets (α is in some index set T). How shall we use them to define an equivalence relation?. The way is clear; given an element $a \in A$ it is in exactly one A_α. We define for $a, b \in A, a \sim b$ if a and b are in the same A_α.

We now prove that this relation is a equivalence relation on A. Let $a \in A$ then a is in some A_α, then it is clear that $a \sim a$. as a and a are both in the same A_α. Therefore this relation is a reflexive relation.

Now let $a, b \in A$, such that, $a \sim b$. Then a, b are in the same A_α. Therefore, $b \sim a$ as well since clearly b, a are also in the same A_α. Therefore this relation is a symmertric relation.

Now let $a, b, c \in A$ such that $a \sim b$, $b \sim c$. Then $a, b \in A_p$ for some $p \in T$ and $b, c \in A_q$ for some $q \in T$. However, since b can only be in exactly one A_α. p must be equal to q. Hence $A_p = A_q$. Therefore, $a \in A_q$. Therefore $a \sim c$ as $a, c \in A_q$. Therefore, $\sim$ is a transitive relation as well.

Hence $\sim$ is reflexive, symmetric and transitive. Therefore it is an equivalence relation.

Now it remains to prove that thee distinct equivalence classes are the A_α's to be continued.

We know that there are $|T|$ disjoint subsets in our decomposition and hence $|T|$ A_αs. Now, we choose $|T|$ elements from these A_αs each picked from a distinct A_α.

Now, the equivalence classes of all these elements are just all the A_α's. Which are $|T|$ distinct sets. Hence, we have at least $|T|$ equivalence classes. Now we show that any equivalence class of this equivalence relation is among these $|T|$ equivalence classes in other words is one of the A_αs.

Let $a \in S$ such that a is in A_b where $b \in T$. Then we know from definition of the relation that the equivalence class of a is A_b which is among one of the A_αs and hence is one of the $|T|$ already discoverd equivalence classes. Therefore. any equivalence class of this relation is going to be one of the already discovered $|T|$ equivalence classes which were the A_αs. Hence the distinct equivalence classes of the defined relation are just all of the A_αs. $\square$

2 Mappings

2.1 Solution 1

1. This mapping is onto, it is not one to one and the inverse image of any $t \in T$ under σ is $\{\sqrt{t}, -\sqrt{t}\}$.

2. Onto, one to one, the inverse image of any $t \in T$ under σ is $\{\sqrt{t}\}$.
3. Not onto, not one to one and the inverse image of any t under σ is $\{\sqrt{t}\}$ if t is a perfect square. Otherwise, it is the empty set.
4. Not onto, one to one. The inverse image of any $t \in T$ under σ is going to be $\{\frac{1}{2}t\}$ if t is even. Otherwise, it is the empty set.

2.2 Solution 2

We define a mapping $f\colon S \times T \to T \times S$:

$$f\left(a, b\right) = \left(b, a\right).$$

Proving this is one to one is a trivial exercise.