Lecture Notes For: Abstract Algebra

Ali Fele Paranj
alifele@student.ubc.ca

March 22, 2023

1 Sets

1.1 General Review on the Basics

This section will be a very quick review on the set theory. I will not go through the details here because it will have a very large overlap with my other lecture notes (like the one for mathematical proof). So I will keep it shot and only include the questions that I managed to solve in this chapter.

Example:

Question. Let R, S, T be sets with $R \subseteq S$. Show that $R \cup T \subseteq S \cup T$.

Solution. Let R, S, T be sets. Then $R \subseteq S$ means:

$$R \subseteq S \equiv x \in R \Rightarrow x \in S.$$

By starting with the LHS of the statement that we want to prove, we can write:

$$\begin{aligned} R \cup T &= \{x : x \in R \wedge x \in T\} \\ &= \{x : x \in S \wedge x \in T\} \\ &= S \cup T. \end{aligned}$$

In which we utilized the fact that $R \subseteq S$ and its equivalent implication statement.

Example: Number of Subsets

Question. Show that the number of subsets of a set with n elements is equal to $2 * *n$.

Solution. This is a sort of a general proof with any set with any elements. However it is more beneficial with finding the number of subset of the set $S = \{1, 2, 3, \ldots, n\}$ for some positive integer n. We will use the proof by induction and start with counting the number of subsets of an empty set. Let set S_0 be an empty set. So the set of its subsets will be:

$$\mathcal{P}(S_0) = \{\varnothing\}.$$

So $|\mathcal{P}(S_0)| = 2^0 = 1$. Let $S_1 = 1$. Its power set will be:

$$\mathcal{P}(S_1) = \{\varnothing, \{1\}\},$$

hence $|\mathcal{P}(S_1)| = 2^1 = 2$. Let $S_k = \{1, 2, 3, \ldots, k\}$ for integer $k < n$. The induction hypothesis is $|\mathcal{P}(S_k)| = 2^k$. Let's assume the induction hypothesis is true and we want to find the cardinality of the set $S_{k+1} = \{1, 2, 3, \ldots, k, k+1\}$. Let's divide the number subsets of S_{k+1} into two sets, meaning:

$$\mathcal{P}(S_{k+1}) = \mathcal{P}_1 \cup \mathcal{P}_2,$$

in which $\mathcal{P}_1$ is the set of all subsets that do not contain the element $k+1$ while $\mathcal{P}_2$ is the set of all subsets that do contain the element $k+1$. we know that $\mathcal{P}_1 = \mathcal{P}(S_k)$ and $\mathcal{P}_2 = \mathcal{P}(S_k \cup \{k+1\})$. Since the cardinality of S_k is k, using the induction hypothesis we know that $|\mathcal{P}_1| = 2^k$ and $|\mathcal{P}_2| = 2^k$. Since $\mathcal{P}_1 \cap \mathcal{P}_2 = \varnothing$ so $|P(S_{k+1})| = |\mathcal{P}_1 \cup \mathcal{P}_2| = 2^k + 2^k = 2^{k+1}$. □

Example: Distributive law

Question. Let R, S and T be any sets. Show that $R \cup (S \cap T) = (R \cup S) \cap (R \cup T)$.

Proof. To show the equality of sets we need to show $R \cup (S \cap T) \subseteq (R \cup S) \cap (R \cup T)$ and $(R \cup S) \cap (R \cup T) \subseteq R \cup (S \cap T)$.

First inclusion. We need to show $R \cup (S \cap T) \subseteq (R \cup S) \cap (R \cup T)$ is true. This statement can be translated into the following implication:

$$x \in R \cup (S \cap T) \Rightarrow x \in (R \cup S) \cap (R \cup T) \quad \text{we need to show is true.}$$

. Let's assume that the antecedent is true. Then we

$$x \in R \vee x \in (S \cap T) \quad \text{is true.}$$

Then we have three cases where $x \in R$ is true or $x \in (S \cap T)$ is true or both are true at the same time. We really need to consider the first two cases as the third cases is obvious as we do the proof for the first and the second case.

- $x \in R$ is true: The following implications are true (following the properties of the unions of sets):

  $$x \in R \Rightarrow x \in R \cup S \text{ (is true)},$$
  $$x \in R \Rightarrow x \in R \cup T \text{ (is true)},$$

  and since we know $x \in R$ is true, using Modus Ponens we can infer that $x \in R \cup S$ and $x \in R \cup T$ are also true. The following equivalence is true following the definition of intersection:

  $$(x \in R \cup S \wedge x \in R \cup T) \equiv (x \in ((R \cup S) \cap (R \cup T)).$$

  And again using Modus Ponens we can infer that $x \in ((R \cup S) \cap (R \cup T)$ is also true. So we proved (for this single case) that $R \cup (S \cap T) \subseteq (R \cup S) \cap (R \cup T)$ is true.

- $x \in (S \cap T)$ is true: This statement translates to $x \in S \wedge x \in T$ is true. So using the corresponding implications from the properties of intersection and then utilizing Modus Ponens, we can infer that $(x \in S \cup R) \wedge (x \in T \cup R)$ is also true that translate into the expression $x \in (R \cup S) \cap (R \cup R)$ is true. So the proof for this case is also complete.

Second inclusion. Here we need to show $(R \cup S) \cap (R \cup T) \subseteq R \cup (R \cap T)$ that similarly to the first part of the proof translates into the following implication:

$$x \in (R \cup S) \cap (R \cup T) \Rightarrow x \in R \cup (S \cap T) \quad \text{we need to show is true.}$$

Let's assume that $x \in (R \cup S) \cap (R \cup T)$ is true. Then:

$$x \in (R \cup S) \text{ (is true)},$$
$$x \in (R \cup T) \text{ (is true)}.$$

which translates into the following cases:

1. $x \in R \wedge x \in R \equiv x \in R$.
2. $x \in R \wedge x \in T$.
3. $x \in S \wedge x \in R$.

4. $x \in S \wedge x \in T$.

The cases $1, 2, 3$ are similar to each other since $x \in R$ is the common statement in all of them. Following the following implication from the properties of union

$$x \in R \Rightarrow x \in R \cup (S \cap T),$$

and then using Modus Ponens we prove the second inclusion. However for the last case, we utilize the following true implication (that follows from the properties of unions in set theory)

$$x \in S \wedge x \in T \Rightarrow (x \in S \wedge x \in T) \vee x \in R,$$

which is equivalent to:

$$(x \in S \wedge x \in T) \vee x \in R \equiv x \in R \cup (S \cap T).$$

which proves the second inclusion for the forth case and finishes the proof. □

1.2 Relations

Relations of one of those fundamental topics in mathematics that is very simple and at the same time very important.

Definition: Relations

Let S and T be sets. Then a **relation** from S to T is a subset $\mathcal{R}$ of $S \times T$. For $s \in S$ and $t \in T$ if $(s, t) \in \mathcal{R}$, then we write $S\mathcal{R}T$. In particular a relation on S is a subset of $S^2 = S \times S$.

Relations can be studies thoroughly based on properties that they posses. But that will be the subject of math proof lecture notes and here I will only discuss a very important type or relations called equivalence relations. To understand the equivalence relations we need to know some terminology.

- **Reflexive Relation:** Let $\mathcal{R}$ be a relation on S. We say this relation is reflexive iff $\forall x \in S, x\mathcal{R}x$. I need to emphasis that *for every* element $x \in S$ we should have $x\mathcal{R}x$.
- **Symmetric Relation:** Let $\mathcal{R}$ be a relation on S. This relation is symmetric iff for $a, b \in S$, $a\mathcal{R}b$ implies $b\mathcal{R}a$. For example, on $\mathbb{Z}$, neither $\leq$ nor $<$ are symmetric. However the $\mathcal{R}$ defined as $a\mathcal{R}b$ iff $|a - b| \leq 10$ is a symmetric relation.
- **Transitive Relation:** Let $\mathcal{R}$ be a relation on S and $a, b, c \in S$. We say the relation is symmetric iff $a\mathcal{R}b$ and $b\mathcal{R}c$ imply $a\mathcal{R}c$.

Example: Relations

Question. Define relation $\mathcal{R}$ on $\mathbb{Z}$ via $a\mathcal{R}b$ iff ab is even. Is this relation reflexive? Symmetric? Transitive?

Solution. This relation shows the ordered pairs in which at least one of the elements is an even number. So it will be ordered pairs of the form: $(2k, 2l + 1)$ or $(2k + 1, 2l)$ or $(2k, 2l)$ for some integers k, l.

- So it turns out that this relation is not reflexive because we don't have the pairs of the form $(2k + 1, 2l + 1)$. For example we don't have elements like $(1, 1)$ and etc in the relation.
- This relation is symmetric. Suppose for $a, b \in \mathbb{Z}$ we have $a\mathcal{R}b$. Based on the definition of relation $\mathcal{R}$ we have $ab = 2k$ for some integer k. It follows from the properties of integer arithmetic that

$ab = ba = 2k$ so $b\mathcal{R}a$

- This relation is not transitive. As an counter example $1\mathcal{R}2$ and $2\mathcal{R}3$ but $1 \not\mathcal{R}3$ since $3 \neq 2k$ for any integer k

Example:

Question. How many relations can be defined on the set $A = \{1, 2, 3\}$. How many of them are symmetric?

Solution. To find the number of total relations on the set A, we need to know how many ordered pairs can be built from it. Since the ordered pair has two positions and each of them has 3 possibilities (the elements of the set A), then we can build a total of $3 * 3 = 9$ ordered pair. Let the set T be the set of all ordered pairs. Then the number of all relations on A will be the cardinal number of the power set of the set T. This can be generalized to any set with n elements. Then the number of all relations can be defined on that set is:

$$\text{Total number of relations} = 2^{n^2}$$

To find the total number of relations that are symmetric, we need to build the atomic sets (smallest sets) that are symmetric:

$$S_1 = \{(1, 1)\}$$
$$S_2 = \{(2, 2)\}$$
$$S_3 = \{(3, 3)\}$$
$$S_4 = \{(1, 2), (2, 1)\}$$
$$S_5 = \{(1, 3), (3, 1)\}$$
$$S_6 = \{(2, 3), (3, 2)\}$$

Any union of these sets will also be a symmetric relation on A. So the total number of symmetric relations will be the cardinal number of the power set of the set $S = \{S_1, S_2, S_3, S_4, S_5, S_6\}$ which is $2^6 = 64$. This can be generalized to any set with n elements. Then the number of relations that are symmetric will be:

$$\text{Total number of symmetric relations} = 2^{n(n+1)/2}$$

You can gain insights about the prove of this relation by doing the same thing we did here for the set $B = \{1, 2, 3, 4\}$ then you can see the pattern!

Example: Relations

Question. For each of the eight subsets of the set $\{\text{Reflexive}, \text{Symmetric}, \text{Transitive}\}$, define a relation on the set $A = \{1, 2, 3\}$ such that the relation has the properties that are in the subset.

Solution. Let's write the power set of the set A. To keep the stuff clean, I will replace the words Reflexive, Symmetric, and Transitive with their initials i.e. R, S, T.

$$\mathcal{P} = \{\{R\}, \{S\}, \{T\}, \{R, S\}, \{R, T\}, \{S, T\}, \{R, S, T\}, \{\}\}$$

So the relations will be like the following:

- $S_1 = \{R\}$:
$$R_1 = \{(1,1),(2,2),(3,3)\}$$
- $S_2 = \{S\}$:
$$R_2 = \{(1,2),(2,1)\}$$
- $S_3 = \{T\}$:
$$R_3 = \{(1,2),(2,1)\}$$
- $S_4 = \{R,S\}$:
$$R_4 = \{(1,1),(2,2),(3,3)\}$$
- $S_5 = \{R,T\}$:
$$R_5 = \{(1,1),(2,2),(3,3)\}$$
- $S_6 = \{S,T\}$:
$$R_6 = \{(1,2),(2,1),(1,1)\}$$
- $S_7 = \{R,S,T\}$:
$$R_7 = \{(1,1),(2,2),(3,3)\}$$

2 Induction and well ordering

Here in this section I will go through some topics in modular arithmetic which are the basis for more complicated stuff in the later chapters. Let's begin with the well ordering axiom.

Definition: Well Ordering Axiom

Well Ordering Axiom: Let S be a set. We say this set is well ordered if for each subset of it, we can find a smallest element in that subset.

At first this might sound obvious. But with this definition the set $\mathbb{R}^+$ is not a well ordered set. But the set of natural integers $\mathbb{N}$ is indeed a well ordered set.