Lecture Notes For: Abstract Algebra

Ali Fele Paranj
alifele@student.ubc.ca

May 28, 2023

Contents

Chapter 1

Sets and Modular Arithmetic

1.1 Sets, Relations, and Functions

1.1.1 Set Theory

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. □

1.1.2 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 {Reflexive, Symmetric, 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:

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

1.1.3 Functions

Function is a very important function in mathematics that appears in almost everywhere! That is because without functions, the world of mathematics will not have any sort of dynamics. It is the function that relates the elements of different set to each other. Although all of us have a intuitive definition of function, it is useful to define the function in a more rigorous way.

Definition: Definition of Function

A function f from set A to set B is a subset of $A \times B$ (thus it is kind of relation) with two more properties:

- $\forall x \in A, \exists y \in B$ s.t. $(x, y) \in f$
- $(x, y_1) \in f \wedge (x, y_2) \in f \Rightarrow y_1 = y_2$

Then we call the set A the domain and the set B the co-domain of the function f and we represent it as:

$$f : A \to B.$$

Also for the pair $(a, b) \in f$, we write it as $f(a) = b$, or $a \mapsto b$.

A function can have more properties among which some properties are very important.

Definition: One-to-One or Injective Function

We say a function f is one-to-one or injective if

$$(a_1, b) \in f \wedge (a_2, b) \in f \Rightarrow a_1 = a_2$$

In a nutshell, the injective function is a function that sends every element in its domain to a *unique* element in its co-domain.

Example: Injective functions

Question. Prove that the function $f : \mathbb{R} \mapsto \mathbb{R}, f(x) = x^2$ is not one-to-one.

Proof. Let's review what was the definition of a one-to-one function. Let P be the statement $(a_1, b) \in f \wedge (a_2, b) \in f$ in which $a_1, a_2, b \in \mathbb{R}$. And let Q be the statement $a_1 = a_2$. To show that the implication $P \Rightarrow Q$ is false, we need to show $P \wedge \neg Q$ is true (which means P is true but Q is false that makes the implication $P \Rightarrow Q$ false). So in a nutshell:

Objective: To show f is not one-to-one we need to show $P \wedge \neg Q$ is true.

To show this, both P and $\neg Q$ must be true. The following statements are good examples:

$P : (-2, 4) \in f \wedge (2, 4) \in f$
$Q : -2 = 2$

Not since $P \wedge \neg Q$ is true, then the function f is not one-to-one. □

Definition: Onto or Surjective Function

The function $f : A \mapsto B$ is surjective iff

$$\forall b \in B, \exists a \in A \quad \text{s.t.} \quad (a, b) \in f$$

Example: Surjective Functions

Question. Show that the function $f(x) = x^3$ is surjective but $g(x) = x^2$ is not.

Proof. The function $f(x) = x^2$ is not surjective since there is no x in domain that maps to $y = -1$. But for the function $f(x) = x^3$, for every y in co-domain, $x = (y)^{1/3}$ is the corresponding element in the domain.

The function that has the *surjective* and *injective* properties at the same time are very important. The following definition box will introduce such functions.

Definition: Bijective Functions

Function $f : A \mapsto B$ is said to be bijective if it is **surjective** and **injective** at the same time. Such a function is known as **one-to-one correspondence**.

The idea of the bijective functions can be used to define the inverse for a function. However, to do that, we need to define a special operation that combines two functions and generates a new functions: composition of functions.

Definition: Composition of Functions

Let R, S, T be sets and let $f : R \mapsto S$ and $g : S \mapsto T$ be functions. Then the compositions of two functions denoted as $f \circ g$ or in a simpler notation fg, is a new function from R to T such that for $x \in R, f \circ g(x) = (fg)(x) = f(g(x))$

There are certain properties that composition of functions hold. These properties are summarized in the following box.

Theorem: Properties of the function composition

Let $\alpha : R \mapsto S, \beta : S \mapsto T$, and $\gamma : T \mapsto U$ be functions. Then we have:

1. $(\gamma\beta)\alpha = \gamma(\beta\alpha)$.
2. If α and β are one-to-one, then so is $\alpha\beta$.
3. If α and β are onto, then so is $\alpha\beta$

Proof.

1. Let $x \in R$. Then $(\gamma\beta)\alpha(x) = (\gamma\beta)(\alpha(x)) = \gamma(\beta(\alpha(x))) = \gamma((\beta\alpha)(x))$.

Observation. Let H be the set of bijective functions. Then H seems to form a special kind of structure (similar to other algebraic structure). By defining the function addition like

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

and the multiplication of functions as the conventional function composition, then I can observe the following properties:

- the set is closed under the $\circ$ and $+$ operations (in other words the adding or composing two bijective functions will be another bijective function).
- $f + g = g + f$ (additive commutativity)
- $(f + g) + h = f + (g + h)$ (additive associativity)
- There exist an element of H denoted by 0, such that for all $f \in H, f + 0 = 0$ (existence of additive identity)
- For every element $f \in H$, there exist a function $g \in H$ s.t. $f + g = g + f = 0$ (existence of additive inverse)
- **No multiplicative commutativity**
- $(f \circ g) \circ h = f \circ (g \circ h)$
- There exist and element of H denoted by 1, such that for all $f \in H, f \circ 1 = 1 \circ f = f$
- For every element $f \in H$, there exist a function $g \in H$ s.t. $f \circ g = g \circ f = 1$
- $f \circ (g + h) = f \circ g + f \circ h$

Seeing these properties give me the hint that $(H, \circ, +)$ form something very similar to fields. But the only difference is that field holds the multiplicative commutativity which is not true in $(H, \circ, +)$. The thing that I am fully sure is that this structure is a non-abelian group.

Theorem: Algebraic structure of the bijective maps

The set of all bijective maps from S to T form a non-abelian group (as explained above).

1.2 Modular Arithmetic

Given any set, we can put an equivalence relation on the set and then look at the set of all equivalence classes of the that relation. This new set will often has very nice properties that can be utilized for different purposes. In fact, the set of rational numbers ($\mathbb{Q}$) is derived in exactly the same way from the integers ($\mathbb{Z}$).

Definition: Definition of rational numbers

Let $\mathbb{Z}$ be the set of integers. Then define the following equivalence relation on this set:

$$(a, b) \sim (c, d) \quad iff \quad ad = bc.$$

This equivalence relation will produce the following equivalence classes:

$$\frac{a}{b} = \{(x, y) : (a, b) \sim (x, y)\}.$$

The set of all rational numbers is in fact the set of all equivalence classes defined as above.

Now we can define the addition and multiplication between the elements of the new set.

Definition: Addition and Multiplication in $\mathbb{Q}$

Let $\mathbb{Q}$ be the set of all rational numbers. Then the multiplication and addition is defined as:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{cd},$$
$$\frac{a}{b} * \frac{c}{d} = \frac{ac}{bd}.$$

Note that $\frac{a}{b}$ is not a single number. But in fact it is the set of all ordered pairs of integers that has relation with that. As an example $\frac{1}{2} = \{(1, 2), (-1, -2), (2, 4), (-2, -4), (3, 6), (-3, -6), \cdots\}$. Then the new definitions of addition and multiplication will me more appreciated. Also note that we need to show that these new operations are well-defined. This means that we need to show that the result will not depend on the choice of representative of a class. For example if $(a, b) \sim (a', b')$ and $(c, d) \sin(c', d')$, then we should have $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$. But this kind of construction we can build more richer sets. In the example shown above, the set $\mathbb{Q}$ has much richer structure than the set $\mathbb{Z}$. Using the Dedekind construction we can build the set of real numbers $\mathbb{R}$ from the set of rationals.

We can put another equivalence relation on the set of integers and get new sets. One good candidate is the modulus relation. As a very quick reminder, we say that two integers a, b are equal modulus n if both of them has the same reminder if divided by n. For example $5 \overset{3}{\equiv} 8$. Or we can have the following alternative definition:

Definition: Modulus

Let $a, b \in \mathbb{Z}$ and $n \geq 2$ and $n \in \mathbb{N}$. Then we say a is **congruent** to b **modulo** n, and write $a \equiv b \pmod{n}$, if $n|(a - b)$; that is, if a and b have the same reminder when divided by n. Note that although the standard notation is the one written above, but for the sake of simplicity I will write $a \overset{n}{\equiv} b$ instead of the standard notation.

Now we can use this concept to define an equivalence relation on the set of integers. We can define this relation as: integers a, b has the relation $a \sim b$ if a and b are congruent to each other modulo n. We can show that this relation is a equivalence relation. Because:

$$\forall a \in \mathbb{Z},\ a \overset{n}{\equiv} a, \quad \text{(Reflective property)}.$$

This is obviously true since $n|0$ for all integers $n \geq 2$. The other property that we need to check is the symmetric property. Let $a, b \in \mathbb{Z}$, then

$$a \overset{n}{\equiv} b \Rightarrow b \overset{n}{\equiv} a, \quad \text{Symmetric property.}$$

This is also true since $n|(a-b) \Rightarrow n|(b-a)$. And lastly, we need to check the transitivity property. Let $a, b, c \in \mathbb{Z}$, then:

$$((a \overset{n}{\equiv} b) \wedge (b \overset{n}{\equiv} c)) \Rightarrow a \overset{n}{\equiv} c, \quad \text{transitivity property.}$$

This is true since $a \overset{n}{\equiv} b$ means $k_1 = (a-b)/n$ for some integer k_1. Similarly, $b \overset{n}{\equiv} c$ means that $\exists k_2 \in \mathbb{Z}$ such that $k_2 = (c-b)/n$. Now by adding these two equations we will have $k_1 + k_2 = \frac{c-a}{n}$. So we can write $a \overset{n}{\equiv} c$. Having this relation on a set will make the equivalence classes $[a]_n = \{x : a \overset{n}{\equiv} x\}$. The following definition defines a very important set called the set of integers modulo n.

Definition: Set of integers modulo n

Let $n \geq 1$ be an integer. The of **integers modulo n**, denoted by $\mathbb{Z}_n$, is the set of all equivalence classes of $\mathbb{Z}$ with respect to the equivalence relation $a \overset{n}{\equiv} b$ for $a, b \in \mathbb{Z}$. We call these the congruent classes modulo n. Specifically $\mathbb{Z}_n = \{[0], [1], [2], \cdots, [n-1]\}$.

Example: Set of integers modulo 4

The set of integers modulo 4 is $\mathbb{Z} = \{[0], [1], [2], [3]\}$, where

$$\begin{aligned}
[0] &= \{\cdots, -8, -4, 0, 4, 8, \cdots\}, \\
[1] &= \{\cdots, -7, -3, 1, 5, 9, \cdots\}, \\
[2] &= \{\cdots, -6, -2, 2, 6, 10, \cdots\}, \\
[3] &= \{\cdots, -5, -1, 3, 7, 11, \cdots\}.
\end{aligned}$$

In the similar way that we defined the addition and multiplication on the set of rational numbers, we can define the same kind of operations on the set of integers modulo n. For that we can have the following definition:

Definition: L

et $[a], [b] \in \mathbb{Z}_n$. Then we can define the multiplication and addition as:

$$\begin{aligned}
[a] + [b] &= [a + b], \\
[a][b] &= [ab].
\end{aligned}$$

Exactly the same way that we showed for the addition and multiplication of rational numbers, we need to show that this definition is well-defined, meaning that the result does not depend of the representative of the equivalence classes. In other words if $a \overset{n}{\equiv} a'$ and $b \overset{n}{\equiv} b'$, then $[a] + [b] = [a'] + [b']$.

Chapter 2

Introduction to Groups