Abstractions Over Algebraic Structures

Aditya M

July 2023

What is Algebra?

I guess that's what we're here to figure out..

Contents

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Eu mi bibendum neque egestas congue quisque egestas.

Haha just kidding, this is a book about algebraic structures, not Latin.

Part I

Preliminaries

Chapter 1

Set Theory

The chapter starts off with what is a set, then I introduce you to common sets you will find along your journey, and then I show you some set operations.

1.1 Sets and Operations over Sets

A **set** is a collection of objects called elements. The elements in a set have no order and no repetition. We describe the contents of a set using { and }. An example of a set containing elements 1 and 2 called A is:

$$A = \{1, 2\} = \{2, 1\} = \{x \in \mathbb{N} : x = 1, 2\}.$$

If we want to show an element, x, is a set, A, we say: $x \in A$. Many sets can also have an infinite number of elements, for example, $\mathbb{R}, \mathbb{N}$, and $\mathbb{Z}$ all have an infinite number of elements. We can indicate this with ellipsis:

$$\mathbb{N} = \{1, 2, \dots\},\ \mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}.$$

Another way of writing these is using **set builder notation**,

$$\mathbb{Q} = \left\{ \frac{q}{p} : q, p \in \mathbb{Z}, p \neq 0 \right\},$$

you write the structure of the set before the colon and statements about it after the colon.

$$\{x \in A : P(x)\}$$

Sets can contain all sorts of elements besides numbers, think functions, other sets, ***"Algebraic Structures"***, functions, etc. For example, the set of real functions whose value at $x = 2$ is 6 (the arrow will be explained later)

$$\{(f : \mathbb{R} \mapsto \mathbb{R}) : f(2) = 6\}$$

and the set of differentiable real functions whose derivative is $6x^2$:

$$\left\{ (f : \mathbb{R} \mapsto \mathbb{R}) : f \text{ is differentiable}, \frac{df}{dx} = 6x^2 \right\}$$

both functions $2x^3$ and $2x^3 + 8$ are in that set. Here is another set:

$$K = \{A = \{a\}, B = \{b\}\}$$

a in that set is described as $a \in A \in K$. You could have a set called "animals", featuring dogs and cats:

$$\text{Animals} = \{\text{Cats}, \text{Dogs}\}$$

(all the other animals are inferior).

And with that, and our new understanding of sets, comes out first definition:

Definition 1.1: Set

A **set** is a collection of objects called elements. The elements in a set have no order and no repetition.

There are many operations one can apply on sets, the most common ones are: union, intersection, and complement. The **Union** of two sets is a set containing all of the elements of both sets, for example:

$$A = \{1, 2, 3\}, B = \{3, 4, 5\}$$
$$A \cup B = \{1, 2, 3, 4, 5\}.$$

The formal definition of a union is

$$A \cup B = \{x : x \in A \text{ or } x \in B\}.$$

The **Intersection** of two sets is a set containing all of the elements that are in both sets, for example:

$$A = \{1, 2, 3\}, B = \{3, 4, 5\}$$
$$A \cap B = \{3\}.$$

The formal definition of an intersection is

$$A \cap B = \{x : x \in A \text{ and } x \in B\}.$$

Before I can define the complement of a set, I need to define a couple more things. If every element in a set, A, is in another set, B, then A is a **subset** of B, we write this as $A \subseteq B$ or $A \subset B$. If every element in A is in B, and every element in B is in A, then A and B are **equal**, we write this as $A = B$. The **Difference** of two sets, A and B, in that order $(A \setminus B)$, is the set containing all the elements of A that are not in B. For example:

$$A = \{1, 2, 3\}, B = \{3, 4, 5\}$$
$$A \setminus B = \{1, 2\}.$$

The formal definition of a set difference is

$$A \setminus B = \{x : x \in A \text{ and } x \notin B\}.$$

If $A \subseteq U$, then U can be described as the **universal set** of A. The **Complement** of A is $A^c = U \setminus A$.

Next, probably one of the most important operations on a set you will encounter in set theory is the **Cardinality** of a set. The cardinality of a set is the number of elements it contains. For example, the cardinality of $\{1, 2\}$ is 2. We write the cardinality of a set A as $|A|$.

$$|\{1, 2, \ldots, n\}| = n.$$

The next operations I will introduce are the Cartesian Product and the power set. The **Cartesian Product** of two sets is essentially each all the possible coordinates you can make with the elements of the set. The Cartesian Product of two sets, A and B, is written as $A \times B$. For example,

$$\{1, 2\} \times \{2, 3\} = (1, 2), (1, 3), (2, 2), (2, 3).$$

Many people shorten something like $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}^2$. And now I think it is due time for our first theorem:

Theorem 1.1: Cardinality of Cartesian Product

The cardinality of the Cartesian Product of two sets is the product of the cardinalities of the two sets.

$$|A \times B| = |A| \cdot |B|.$$

Proof. This result is relatively easy to show, for each possible element, there are $|A|$ possible values for the first coordinate, and $|B|$ possible values for the second coordinate, so there are $|A| \cdot |B|$ possible coordinates, and thus $|A| \cdot |B|$ elements in the Cartesian Product.

□

This is more clear in this diagram:

δ	2	3
1	{1,2}	{1,3}
2	{2,2}	{2,3}

Now that we understand Cardinality, I can introduce these theorems:

Theorem 1.2: Cardinality of Union

The cardinality of the union of two sets is the sum of the cardinalities of the two sets minus the cardinality of their intersection.

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Proof. This is a bit more complicated to show, but it is still relatively easy. We can split the union into two parts, the intersection and the union of the two sets without the intersection. The intersection is counted twice, so we subtract it once.

□

The second theorem is a corollary of the first:

Theorem 1.3: Cardinality of Intersection

The cardinality of the intersection of two sets is the sum of the cardinalities of the two sets minus the cardinality of their union.

$$|A \cap B| = |A| + |B| - |A \cup B|.$$

Proof. This is a corollary of the previous theorem, we can just switch the union and intersection. We know $|A| + |B|$ is the union + an extra counting of the intersection, so we subtract the union to get the intersection.

□

Another important theorem that involves unions and intersections is De Morgan's Laws:

Theorem 1.4: De Morgan's Laws

$$(A \cup B)^c = A^c \cap B^c$$
$$(A \cap B)^c = A^c \cup B^c$$

Proof. This is much harder than the others. I will only prove the first one, the second one will be left as an exercise to the reader. First I will assume $A, B \subseteq U$. So to prove the result we must show

$$(A \cup B)^c \subseteq A^c \cap B^c$$

and

$$(A^c \cap B^c) \subseteq (A \cup B)^c.$$

First, let there exist some $x \in (A \cup B)^c$, that means $x \notin (A \cup B)$. Had x been in A or B, it would have been in $A \cup B$, therefore $x \notin A$ and $x \notin B$. That is the same as saying $x \in A^c$ and $x \in B^c$. This means $x \in (A^c \cap B^c)$. And that implies

$$(A \cup B)^c \subseteq A^c \cap B^c.$$

Now to prove it in the other direction. Suppose some $x \in (A^c \cap B^c)$, this is the same as saying $x \in A^c$ and $x \in B^c$. That means $x \notin A$ and $x \notin B$. This implies $x \notin (A \cup B)$, or $x \in (A \cup B)^c$. This means that $(A^c \cap B^c) \subseteq (A \cup B)^c$, and thus

$$(A \cup B)^c = A^c \cap B^c.$$

□

The last thing I will show in this section is **Power Sets**. The power set of a set is the set of all subsets of that set. This includes the empty set and the set itself. Each and every element of the set is also a subset of it too. We denote the power set with $\mathcal{P}(A)$, where A is the set we are operating on. An example of a power set is:

$$\mathcal{P}(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}.$$

The formal definition of the power set is:

$$\mathcal{P}(A) = \{x : x \subseteq A\}.$$

I think it is important to notice the cardinality of the power set. The original set had 3 elements, and the power set has 8 elements, which just so happens to be 2^3. This is not a coincidence, and in fact, it is true for all sets. I think this calls for another theorem!

Theorem 1.5: Cardinality of Power Set

The cardinality of the power set of a set is $2^{|A|}$.

$$|\mathcal{P}(A)| = 2^{|A|}.$$

Proof. I'll prove this in two different ways, one is a bit more formal, and the other is a bit more intuitive. First I'll do the formal proof. For each possible subset of A, each element of A is either in or not in that subset. That makes $|A|$ binary choices for each element, making the number of subsets $2^{|A|}$. □

Proof. The other way to prove this is to describe the cardinality of the power set in a different way. The power set contains each **grouping** of elements in A. In other words, out of all the elements in A, the power set contains all the groups of 0 elements, + all the groups of 1 elements, ...

$$|\mathcal{P}(A)| = \binom{|A|}{0} + \binom{|A|}{1} + \cdots + \binom{|A|}{|A|}.$$

This can easily be re-arranged into

$$\sum_{k=0}^{|A|} \binom{|A|}{k}$$

Now all we have to do is show this sum equals $2^{|A|}$, which is easy to do with the Binomial Theorem.

$$2^{|A|} = (1+1)^{|A|} = \sum_{k=0}^{|A|} \binom{|A|}{k} 1^k 1^{n-k} = \sum_{k=0}^{|A|} \binom{|A|}{k}.$$

□

And with that, I think this is a great conclusion to the section.

Exercises

1. Show that $A \subseteq B$ if and only if $A \cap B = A$.
2. Show that the set $\{k \in \mathbb{Z} : k = 12a, a \in \mathbb{Z}\}$ is a subset of $\{k \in \mathbb{Z} : k = 3a, a \in \mathbb{Z}\}$.

1.2 Relations

A relation can be described as a subset of the Cartesian product of two sets. So in other words, a relation is a set of ordered pairs. For example, I'm sure you will recognise this function from your days in middle school:

$$y = f(x), f(x) = x$$

This is an example of a relation. It is a set, and it is relating y and x.

$$f(x) = \{(x, y) \in \mathbb{R}^2 : x = y\}.$$

So, the set's elements are ordered pairs of $\mathbb{R} \times \mathbb{R}$, that satisfy the condition $x = y$. This is a special type of relation called a ***function***, which I am sure you have heard of before.

A little interjection here, before I continue I will introduce a new operation on integers called ***modulo***. Modulo takes the remainder of a division. For example, 12/5 is 2 remainder 2, so 12 mod $5 = 2$. Notation $a \equiv b(\bmod n)$ means that a and b have the same remainder when divided by n, or $a \bmod n = b \bmod n$.

Another thing I will introduce for later is the concept of two numbers "dividing" eachother. a divides b if b/a is an integer. This is denoted as $a|b$.

$$a|b \implies b = ka, k \in \mathbb{Z}.$$

A relation R has no restrictions. In R^2, the relation $\{(0,1),(0,2),(1,1)\}$ is a valid relation. The first relation I will explore is

$$R = \{(a, b) \in \mathbb{Z}^2 : a \equiv b(\bmod\ n)\}.$$

This relation is very interesting because both of the values in each pair are either both even or both odd. For example, $(4, 6)$ is a part of this relation, but $(4, 5)$ is not. I'll use this to introduce different *types* of relations. The relation R is called an ***equivalence relation***. For a relation to be an equivalence relation, it must satisfy three properties:

1. Reflexivity: $(a, a) \in R$ for all $a \in A$.
2. Symmetry: $(a, b) \in R \implies (b, a) \in R$.
3. Transitivity: $(a, b) \in R \wedge (b, c) \in R \implies (a, c) \in R$.

The relation R satisfies all three of these properties, so it is an equivalence relation. I'll show that it satisfies all three of these properties.

1. $a \in \mathbb{Z}, 2|(a - a) \implies a \equiv a(\bmod\ 2) \implies (a, a) \in R$.
2. $(a, b) \in R \implies a \equiv b(\bmod\ n) \implies b \equiv a(\bmod\ n) \implies (b, a) \in R$.
3. $(a, b) \in R \wedge (b, c) \in R \implies a \equiv b(\bmod\ n) \wedge b \equiv c(\bmod\ n) \implies a \equiv c(\bmod\ n) \implies (a, c) \in R$.

Basically, for Reflexivity, I show that 2 divides $a - a$ for all $a \in \mathbb{Z}$, which is obviously true because $a - a = 0$, and all numbers divide 0. For Symmetry, I show that if $a \equiv b(\bmod\ n)$, $b \equiv a(\bmod\ n)$, which is also obviously true because you can always flip equality. For Transitivity, in English, I basically show that if a and b have the same remainder, lets call it r ($a \bmod b = r$), and b and c have the same remainder, r, then a and c have the same remainder, r, so that implies $(a, c) \in R$.

Now I will use this relation to introduce new notation. If $(a, b) \in R$, we write this as $a \, R \, b$, if it is not in R, we write it as $a \not R \, b$. The "equality" symbol is a relation. It is the set of pairs whoose elements equal eachother. That is why we write $a = b$, to show $(a, b) \in$ " $=$ ", or that they are "equal". If a relation is an equivalence relation, we write it with a $\sim$ instead of an $=$, as there can be many equivalence relations other than $=$. I will leave proving $=$ is an equivalence relation as an exercise to the reader. If you are dealing with many equivalence relations, for example A and B, you may have $\sim_A$ and $\sim_B$ as the equivalence relations for A and B respectively.

Because R is an equivalence relation, I will use $\sim$ or $\sim_R$ to refer to it. An ***equivalence class*** is a set of elements that are all related to eachother. For example, the equivalence class of 1 is $\{1, 3, 5, 7, 9, \dots\}$, because all of these numbers have the same remainder when divided by 2. We denote an equivalence class as $[a]$ or $[a]_A$, where a is the element of the equivalence class of R.

$$[a]_R = \{b \in Z : a \sim_R b\}.$$

$$[a] = \{b : a \sim b\}$$

$[1]_R = \{1, 3, 5, 7, 9, \dots\}$ because $1 \sim_R 1, 1 \sim_R 3, 1 \sim_R 5, \dots$. An equivalence class is a set of elements that are all related to eachother. This calls for a new pair of theorems!

Theorem 2.1: Elements of Equivalence Classes are Locally Unique

The equivalence class of some element in another equivalence class is itself.

$$b \in [a] \implies [a] = [b]$$

Proof. Let $b \in [a]$. Then $a \sim b$. Let $c \in [a]$. Then $a \sim c$. Because $a \sim b$ and $a \sim c$, $b \sim c$ (Transivity). Because $b \sim c$, $c \in [b]$. Because $c \in [b]$, $[a] \subseteq [b]$. Because $b \in [a]$, $[b] \subseteq [a]$. Therefore, $[a] = [b]$. □

Theorem 2.2: Equivalence Class Theorem

Let R be an equivalence relation on a set A. Then for all $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$.

Proof. Let R be an equivalence relation on a set A. Then for all $a, b \in A$, $[a] = [b]$ or $[a] \cap [b] = \emptyset$. Let $a, b \in A$. If $[a] = [b]$, then we are done. Assume $[a] \neq [b]$. Then there exists some $c \in [a]$ such that $c \notin [b]$. Then $c \sim a$ and $c \not\sim b$. Because $c \sim a$, $a \sim c$, and because $c \not\sim b$, $b \not\sim c$. Then $a \sim c \sim a$ and $b \not\sim c \not\sim b$, so $a \not\sim b$. Then $[a] \cap [b] = \emptyset$. □

Exercises

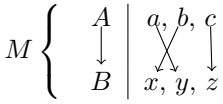
1. Prove that $=$ is an equivalence relation.
2. Find another equivalence relation and prove it is an equivalence relation.

1.3 Functions and Maps

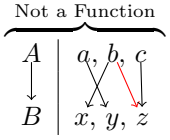
In the previous section, I introduced equivalence relations, a special type of relation. This section is dedicated to another special type of relation, ***functions***. A function is a relation where for each input there is exactly one output. In other words "forall inputs to a function F, there is one unique output". In middle school this was called the vertical line test. If two coordinates have the same x value, they have the same y value (In other words it is the only point, meaning there can only be one point intersecting the vertical line).

A function is sometimes called a ***map*** because it is a correspondence between some input and a ***unique*** output, like a point on a map corresponds with a unique point in space If a map M maps two sets, A and B, we write $M : A \to B$. In this case, A is called the ***domain*** and B is called the ***codomain***.

$$\text{Let } M : A \to B, A = a, b, c, B = x, y, z$$
$$M(a \in A) = y \in B, M(b \in A) = x \in B, M(c \in A) = z \in B$$
$$M = \{(a, y), (b, x), (c, z)\}$$



Had there been two arrows coming out of one element in the domain, both leading to different elements in the codomain, it would not be a function. It still would have been a function two different elements in the domain pointed to the same one element in the codomain.

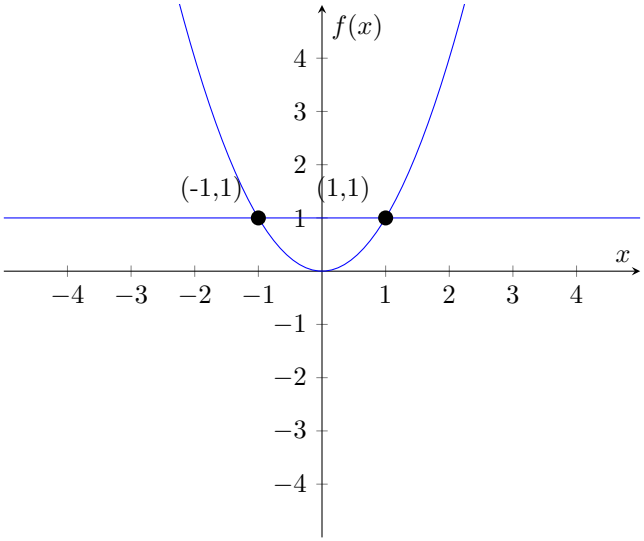


Notice that this is not a function because b maps to both x and z, not because b and c both map to z.

We call a function $f : A \to B$ ***injective*** if each element in the domain maps to one and only one element in the codomain. You can also describe this relationship as "unique", if something is unique that means there is only one of it. In math terms an injective function has this property:

$$f : A \to B$$
$$\forall a, b \in A, f(a) = f(b) \implies a = b$$

In $\mathbb{R}$, the function $f(x) = x^2$ is not injective because $f(-1) = f(1) = 1$. A good way to check if a function in $\mathbb{R}$ is injective is to see if it passes the "horizontal line test". It is similar to the vertical line test, but instead of checking if there is only one point on the vertical line, you check if there is only one point on the horizontal line. A parabola clearly does not pass this line test, so it is not injective as we verified above.



If a function $f : A \to B$ is injective, then: $|A| \leq |B|$, because if $|A| > |B|$, then there would be more elements in the domain than in the codomain, and therefore atleast one element in the codomain would have to be mapped to by more than one element in the domain.

Theorem 3.1: Pigeonhole Principle pt. 1

If a function $f : A \to B$ is injective, then $|A| \leq |B|$.

It is called the pigeonhole principle because if you have n pigeons and m pigeonholes, and $n > m$, then at least one pigeonhole must have more than one pigeon in it. An injective function might also be called "one to one".

A function is ***surjective*** if every element in the codomain is mapped to by at least one element in the domain. In math terms, the codomain is equal to the ***range*** of the function. The range is the set of all possible outputs of the function.

$$f : A \to B$$

$$\text{range } f = \{f(a) \in B : a \in A\}$$

For example, a function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2$ is not surjective because there is no $x \in \mathbb{R}$ such that $f(x) = -1$. All the function tables I used in the examples above were surjective because the codomain was equal to the range. Here is an example of a non-surjective function:

A	a, b, c
$\downarrow$	$\swarrow$ $\swarrow$ $\swarrow$
B	x, y, z, ϑ

Clearly the codomain contains ϑ, but the range does not, so this function is not surjective. If a function $f : A \to B$ is surjective, then: $|A| \geq |B|$, because if $|A| < |B|$, then there would be more

elements in the codomain than in the domain, and therefore there would be at least one element in the codomain that is not mapped to by any element in the domain, which is not allowed for a surjective function.

Theorem 3.2: Pigeonhole Principle pt. 2

If a function $f : A \to B$ is surjective, then $|A| \geq |B|$.

A function might also be called "onto" if it is surjective.

Finally, if a function is both injective and surjective it is called ***bijective***. Bijective functions have many interesting properties to them, being one to one and onto. First, if a function is bijective, then it has an inverse function. This is because if it is injective, then its inverse will be a function (otherwise it would not pass the vertical line test). If it is surjective, then the domain of its inverse will be the codomain of the original function, and the codomain of its inverse will be the domain of the original function. Another interesting property of bijective functions is that the composition of two bijective functions is also bijective. This is because if f and g are bijective, then f^{-1} and g^{-1} exist, and $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$. Probably the most interesting property of bijective functions is that if $f : A \to B$ is bijective, then $|A| = |B|$.

Theorem 3.3: Pigeonhole Principle pt. 3

If a function $f : A \to B$ is bijective, then $|A| = |B|$.

Proof. If f is bijective, then it is both injective and surjective. If it is injective, then $|A| \leq |B|$. If it is surjective, then $|A| \geq |B|$. Therefore, $|A| = |B|$. □

Also, if two sets have the same cardinality (called ***equinumerous***), then there exists a bijective function between them. Often times, we can prove that two sets are equinumerous by finding a bijective function between them. Another theorem that is useful for proving that two sets are equinumerous is the ***Cantor-Bernstein-Schroeder Theorem***. This theorem states that if there exists an injective function $f : A \to B$ and an injective function $g : B \to A$, then there exists a bijective function $h : A \to B$.

Theorem 3.4: Cantor-Bernstein-Schroeder Theorem

If there exists an injective function $f : A \to B$ and an injective function $g : B \to A$, then there exists a bijective function $h : A \to B$.

I cannot provide proof for this theorem, but I can make sense of it. If there is an injective function $f : A \to B$, then $|A| \leq |B|$, and if there is an injective function $g : B \to A$, then $|B| \leq |A|$. If both of these are true, then $|A| = |B|$.

Exercises

1. Show $\mathbb{N}$ is equinumerous to $\mathbb{Z}$.
2. Show $\mathbb{N}$ is equinumerous to $2\mathbb{Z}$ (even integers).