Elements of Algebraic Structures January 9 2024

Lecture 1: Introduction

Lecture: Sujata Ghosh *Scribe: Aranya Kumar Bal, Sandeep Chatterjee*

1 What is this course about

Welcome to the first lecture of the *Elements of algebraic structure* course. The course instructor is Sujata Ghosh, and for this week it's me Aranya, and Sandeep who are scribing (this is in first person from me because I am writing the intro :p). To the folks who are new to this subject, hope you take away how rich and beautiful algebra is. And to those who have seen these things before, hopefully you will take away something new.

A little note : There will be several things in the notes beyond the class as well, like more information, things to look forward to, and exercises. Things will almost always be labelled if they are not from the class. And for exercises, the extra ones will be marked by a $\star$ (but you are encouraged to try all of them!) Yellow boxes will almost always have stuff that are extra, mostly nuances about the topic at hand.

Well, that ends the intro. Have fun!

1.1 High Level Overview

In this course, we shall be studying *algebraic structures*, by which we mean that we have 'collection' of objects (which is the universe of our algebra) and ways to combine/modify said objects (this is the structure) subject to a few rules. We shall be seeing a lot of such algebraic structures.

Oh, and we will almost always let out universe be some sort of a *set* (to be informally defined in a following section). That does not mean that there cannot be other 'collections', but they would lead us too astray so let me put it in a box after we define sets.

2 Topics for this lecture

In this lecture, we shall talk about the following

1. Sets
2. Relations
3. Functions
4. Structures on a set

3 Set

Definition 3.1 (Set) *A collection of objects is called a set.*

The objects can be anything as long as they are well defined[1].

Example *The following are all sets*

1. $\{a, b, 1, 2, \text{☺}\}$

2. $\{\{a, b\}, 1, 2\}$

3. $\mathbb{R}$

Is 2 really also a set?

Yes, it is. It is a valid collection of objects.

Definition 3.3 (Subsets) *A set A is said to be a subset of a set B ($A \subseteq B$) if every element of A is also an element of B.*

Definition 3.4 (Empty Set) *($\varnothing$): A set containing no element.*

$\varnothing$ is not the greek letter ϕ (phi) by the way. This is a symbol for the empty set.

Time for a little exercise

Exercise Prove that $\varnothing \subseteq A$ for any set A.

This exercise should also introduce you to vacuous truths, something that is ubiquitous in logic and almost almost all of mathematics in general.

Maybe this is a good place to introduce some notations properly.

We write $x \in A$ if x is an element of A. We call A a subset of B if $x \in A \Rightarrow x \in B$, and we write this as $A \subseteq B$ (note that this is equivalent to what was expressed in words for subset). We write $A = B$ if A and B have exactly the same elements (formally $A = B$ if $A \subseteq B$ and $B \subseteq A$). If $A \subseteq B$ but $A \neq B$, then we write that as $A \subset B$.

3.1 Set Operations

We now look at several operations that can be done on sets. We might see the word class popping up here and there, but we won't worry much about it, it's just a technicality because the collection of all sets is not a set.

[1] Okay, they can't be *anything* because as we have seen, they can't be every possible set. But other than such paradoxical stuff, almost everything works

3.1.1 Some set operations

1. **Union**

   The union $\cup$ is a binary operation on the class of all sets, V that takes in two sets and spits out another set containing elements that are in one set or the other. Notationally

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

   Example (Union)

   $$\{1,2,3\} \cup \{2,10,3\} = \{1,2,3,10\}$$

2. **Intersection**

   The intersection $\cap$ is a binary operation on V that again takes in two sets and spits out a set that contains the elements in both sets. Notationally

   $$A \cup B = \{x \mid x \in A \text{ and } x \in B\}$$

   Example (Intersection)

   $$\{1,2,3\} \cap \{2,10,3\} = \{3,2\}$$

3. **Complement and Universe**

   The complement $\cdot^C$ or $\bar{\cdot}$ is an unary operation on V that takes in a set and returns a set with the elements not in the set. Notationally

   $$\bar{A} = \{x \mid x \notin A\}$$

   This brings up a question 'what elements are not in a given set?' Like, if we say $\overline{\{1,2,3\}}$ then is this equal to $\{4,5\}$ or all natural numbers other than $1, 2$ and 3 or all the real numbers other than these three number?

   This brings us to the concept of an universe. It's not strictly defined, but is defined 'given a context'. Most of the times, context dictates what 'largest set' we are looking at, whether it's the naturals, reals, complexes etc. That is what we called the universe Ω.

   The complement can now be more precisely defined as

   $$\bar{A} = \{x \in \Omega \mid x \notin A\}$$

   Example (Complement and Universe) *With* $\Omega = \{1,2,3,4,5,6\}$ *we have*

   $$\overline{\{1,2,3\}} = \{4,5,6\}$$

   With $\Omega = \{1,2,3,4,5,6,7\}$ *we have*

   $$\overline{\{1,2,3\}} = \{4,5,6,7\}$$

4. **Power set**

   The power set $\mathcal{P}$ or $2^{\cdot}$ is another unary operation on V that takes in a set and returns the set of all it's subsets. Notationally

   $$\mathcal{P}(A) = \{\sigma \mid \sigma \subseteq A\}$$

   Example (Power set)

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

5. **Set difference**

   The set difference $\cdot \setminus \cdot$ is a binary operation that takes in 2 sets and returns the set of elements of the former set that are not in the latter set. Notationally

   $$A \setminus B = \{x \in A \mid x \notin B\}$$

   Example (Set difference)

   $$\{1,2,3\} \setminus \{2,3,5\} = \{1\}$$

6. **Symmetric difference**

   The symmetric difference $\cdot\Delta\cdot$ is a binary operation that takes in 2 sets and returns the set of elements that are in one set but not in the other for both the sets. Notationally

   $$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

   Example (Symmetric difference)

   $$\{1,2,3\}\Delta\{2,3,5\} = \{1,5\}$$

These set operations satisfy some nice properties. The reader can add more to the list. In fact, readers who know a bit of logic can realise the connections between set theory and logical propositions.

3.1.2 Properties of set operations

1. Union is associative

   $$A \cup (B \cup C) = (A \cup B) \cup C$$

2. Intersection is associative

   $$A \cap (B \cap C) = (A \cap B) \cap C$$

3. Union is commutative

   $$A \cup B = B \cup A$$

4. Intersection is commutative
$$A \cap B = B \cap A$$

5. Intersection distributes over union
$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

6. Union distributes over intersection
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

7. De Morgan's laws holds
$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$
$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

Exercise* Verify the above properties of the set operations.

What other things can exist other than sets?

Sets, as we have seen, are naively defined as *collection of objects*. But that raises several questions. Collections? Objects? How do you formally define such terms?

For now, let us consider them at face value. You can take *anything* and group them together to create a set. Thus you can have sets containing sets etc. Fair enough. Most of mathematics will go through with this intuitive notion. But, poke it deep enough and the demons lurking underneath show.themselves.

Consider the following set
$$S = \{A \mid A \notin A\}$$
That is, this is the collection of all sets who do not contain themselves. Where do these sets come from? Well, the set of all sets! It's clearly a defined set by our definition (let us call it U) and thus so is S. Now, S is also a set and thus must be in U. Then, a valid question is, is S in S? Well, if yes, then by the definition of S, we have S not in S. This is a contradiction so S must not be in S. But then again by definition, S is in S and hence again a contradiction. Thus we have fit a logical fallacy!

This is the well known *Russell's paradox* and shows that the collection of all sets is actually not a set. So there can be collections which are not sets. These things are called *classes* This is the first of many things that are not sets. Such things can be handled formally in formal *set theories* like ZFC (well, actually it is handled in a extenson called TG but ZFC can handle them in via a metalanguage) or Morse-Kelly. I will just leave it at that because things get very dicey and technical very quickly (maybe you will meet them in ma'am's logic course who knows).

Are classes ever used in algebraic structures? Sure they do! The surreal numbers are a proper class that has a field structure on them, in fact they are a totally ordered field. And they pop up in the analysis of the board game Go!

There are obviously other things beyond this whole hierarchy of sets and classes and things. There are topoi, typed and untyped calculi, categories etc. Categories in particular are like a bird's eye view of the whole landscape of mathematics. They can encompass sets (Lawvere[a]), groups, hilbert spaces among countless others. Maybe someday some lecture notes in this course would have a brief look at them.

[a] A very digestible exposition to the topic is by Leinster in his paper Rethinking set theory

4 How to add structures to a set?

As we discussed in the overview, a *structure* on a set is a way to capture the idea of combining elements from the set. The most natural way to define them are via relations and functions.

4.1 Relations

Let us then first look at relations. But before that, we need a couple of definitions.

Definition 4.1 (Cartesian product) *The cartesian product of two sets A and B is denoted as $A \times B$ and is defined as*

$$A \times B = \{(x, y) \mid x \in A, y \in B\}$$

This is what we call a 'interior' definition of the cartesian product. but this is very awkward to generalise, so we also have an 'exterior' definition of the cartesian product which we will get to maybe later, and this definition is more in line with the modern way of thinking.

Exercise* Show that the cartesian product is not commutative, that is, $A \times B \neq B \times A$ in general.

Definition 4.2 *We define the k-fold cartesian product of a set A (written as A^k) inductively*

$$A^1 = A$$

$$A^{k+1} = A \times A^k \textit{ for all } k \in \mathbb{N}, k \geq 2$$

Now we can define what we mean by a relation on a set. Informally, relation tells you exactly what the word *relation* mean - which elements of various sets are related.

Definition 4.3 (Unary relation) *A unary relation R on a set A is simply a subset of A, that is $R \subseteq A$ is a unary relation on A.*

Example (Unary relation) *The following illustrates a couple unary relations.*

1. *Let $A = \{1, 2, 3\}$. Then $R = 1, 2$ is a unary relation on A.*

2. *Let B be any set. Then $\varnothing$ is a unary relation on B, called the empty unary relation on B.*

Definition 4.5 (Binary relation) *A binary relation R on a set A is a subset of $A \times A$, that is, $R \subseteq R \times R$.*

Before moving on to examples, we setup some notations to help us.

Let R be a binary relation on a set A. We have

$$R \subseteq \{(a, b) \mid a, b \in A\} = A \times A$$

If $(a, b) \in R$, then we say 'a is related to b', denoted by aRb or $a \sim_R b$ or just simply $a \sim b$. If $(a, b) \notin R$, then we say 'a is not related to b', denoted by $a\not{R}b$ or $a \not\sim_R b$ or just simply $a \not\sim b$.

Example (Binary relation) *The following serve as examples of some important binary relations.*

1. $(\mathbb{R}, R)$, *where*
   - *R is the set of real numbers*
   - *$a \sim b$ if $a \mid b$, that is, if a divides b.*
2. (A, R), *where*
   - *A is any set*
   - *$a \sim b$ if and only if $a, b \in A$*
3. (A, R) *where*
   - *A is any set*
   - *$a \sim b$ if and only if $a = b$*

   This is called the diagonal relation and is denoted by Δ.

These definitions naturally make way for a general definition.

Definition 4.7 (n-ary relation) *An n-ary relation R on a set A is a subset of A^n, that is, $R \subset A^n$.*

Relations between arbitrary sets can also be defined similarly. We provide the one for bianry relations

Definition 4.8 (Binary relation between two sets) *An binary relation R between a set A and a set B is a subset of $A \times B$, that is, $R \subset A \times B$.*

If we are given two relations, one between A and B, and another between B and C, it should be intuitive that there is some relation between A and C.

Definition 4.9 (Composition of relations) *We define a notation $\circ$ that takes in two relations and outputs a new relation. More precisely, let $R_1 \subseteq A \times B$ and $R_2 \subseteq B \times C$. Then*

$$R_2 \circ R_1 = \{(a, c) \mid \text{ there exists } b \in B \text{ such that } (a, b) \in R_1 \text{ and } (b, c) \in R_2\}$$

Composition is read from right to left. Sometimes we drop the composition symbol if there is no confusion.

4.1.1 Types of binary relations

Now, relations are too general to be typically of any use. It is more useful to look at several classes of relations by putting restrictions on them.

Definition 4.10 (Reflexive relations) *A relation on A is called reflexive if $x \sim x$ for all $x \in A$.*

Example *All these are reflexive relations*

- $(\mathbb{R}, =)$, *where R is the set of real numbers and $a \sim b$ if $a = b$*
- $(\mathbb{R}^+, |)$, *where $\mathbb{R}^+$ is the set of positive real numbers and $a \sim b$ if $a \mid b$ (where we say $a \mid b$ if there exists $k \in \mathbb{N}$ such that b=ka).*

Definition 4.12 (Symmetric relation) *A relation on A is called symmetric if whenever $x \sim y$, then $y \sim x$ for $x, y \in A$*

Example *All these are symmetric relations*

- $(\mathbb{R}, \sim)$, *where $a, b \in \mathbb{R}$, and $a \sim b$ if $a - b$ is divisible by 2*
- $(People, sibling)$, *set of all people, and relation being if they are siblings of each other*

Definition 4.14 (Transitive relation) *A relation on A is called transitive if whenever $x \sim y$ and $y \sim z$, then $x \sim y$ for $x, y, z \in A$*

Example *All these are transitive relations*

- (a, b, c, R): *a, b, c are vertices of a triangle, R is reachablity*
- (a, b, R): *$R = \{(a, a)\}$*

Definition 4.16 (Anti-symmetric relation) *For all $a, b \in A$, if $a \sim b$ and $b \sim a$, then $a = b$.*

Example *All these are anti-symmetric relations*

- (a, b, R), *where $R = \{(a, a)\}$*
- $(\mathbb{R}, \leq)$, *where $\mathbb{R}$ is the set of real numbers*

We can combine some of these to get very interesting relations.

Definition 4.18 (Partial order) *A relation R is a partial order if it is reflexive, anti-symmetric and transitive.*

Example *These are all partial orders*

1. *Let X be a set. Consider the set $\mathcal{P}(X)$ of all it's subsets (called the power set of X). For any $A, B \in \mathcal{P}(X)$, let $A \sim B$ if $A \subseteq B$.*
2. *Let us look at the positive integers $\mathbb{Z}^+$. Let us denote by $a \mid b$ if there exists $k \in \mathbb{N}$ if $b = ka$. Then let $a \sim b$ if $a \mid b$.*

Exercise* Verify that the above are actually partial orders.

And finally, one of the most useful relations

Definition 4.20 (Equivalence relation) *A relation on A is called an equivalence relation if it is reflexive, symmetric and transitive.*

Example *All these are equivalence relations*

1. *Consider a finite graph G with vertices V and edges E. Define the relation $\sim$ on V as follows :*

   $$u \sim v \text{ if there exists a path from } u \text{ to } v \text{ in } G$$

   This relation is an equivalence relation, and the equivalence classes are the connected components of the graph.

   - *Reflexivity: Every vertex is reachable from itself, so $\sim$ is reflexive.*
   - *Symmetry: If there is a path from u to v, there is a path from v to u, making R symmetric.*
   - *Transitivity: If there is a path from u to v and a path from v to w, then there is a path from u to w by composing them, ensuring $\sim$ is transitive.*

The equivalence classes (connected components) under $\sim$ will be sets of vertices that are reachable from each other but not from vertices in other equivalence classes.

2. *Modular Congruence (on the set of integers $\mathbb{Z}$) : Let n be a fixed positive integer. Define the relation $\sim$ on $\mathbb{Z}$ as follows:*

$$a \sim b \text{ if } a \equiv b \pmod{n}$$

This relation is an equivalence relation because:

- *Reflexivity: For every integer a, $a \equiv a \pmod{n}$.*
- *Symmetry: If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.*
- *Transitivity: If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.*

Now you might be thinking, hold on a hot minute, shouldn't reflexive be redundant in the definition of an equivalence relation? After all, if a relation is symmetric and transitive then we have $x \sim y$ and $y \sim x$ by symmetricity, and then by transitivity, we get $x \sim x$. Where's the problem?

Here's an example where this breaks down.

Let $A = \{1, 2, 3\}$ and the relation $R = \{(1, 2), (2, 1), (1, 1), (2, 2)\}$. This is symmetric because when $1 \sim 2$ we have $2 \sim 1$ (and vice versa) and when $1 \sim 1$ (resp $2 \sim 2$) we have $1 \sim 1$ (resp. $2 \sim 2$). This is also transitive as one can check.

But clearly this is not reflexive as $3 \not\sim 3$.

What went wrong? The problem was that 3 was not related to anything and that caused the issue. To fix this, we can define the following.

Definition 4.22 (Serial relation) *A relation on A is called serial if for every $x \in A$, there exists $y \in A$ such that $x \sim y$.*

Then we have the following.

Proposition 4.23 *A relation on A that is serial, symmetric and transitive is reflexive and hence is an equivalence relation.*

Proof. Let $x \in A$. Then since the relation is serial, we can find a $y \in A$ such that $x \sim y$. By symmetricity, $y \sim x$, and then by transitivity $x \sim x$. Since x was arbitrary, this holds for all x and hence the relation is reflexive. Thus we have a relation that is reflexive, symmetric and transitive, and hence is an equivalence relation. □

4.2 Functions

Functions are special relations. They are exactly those relations such that one element (of the first set) is not related to more than two elements, and all elements (of the first set) are related. In some sense, this brings a consistency condition to that of relations - if we ask what something is related to, we always get an answer, and we don't get two different answers. We now formalise this.

Definition 4.24 (Functions) *A function f between two sets A and B is a relation between A and B such that*

1. *for all $a \in A$, there exists a $b \in B$ such that $(a, b) \in f$*
2. *if (a, b) and (a, c) are in f, then $b = c$.*

A function $f \subseteq A \times B$ is generally written as

$$f : A \to B$$

and read as 'a function f from A to B'. Also if $(a, b) \in f$, then we write $f(a) = b$. A function is called a map sometimes.

Example *Consider $A = \{1, 2\},\ B = \{1, 2, 3\}$ and $f(1) = 2,\ f(2) = 3$. Then f is a function. But if $g(1) = 1$ only, then g is not a function (technically not a function on A). Also if $h(1) = 1,\ h(2) = 2,\ h(2) = 3$, then again, h is not a function.*

4.2.1 Arity of a function

A function f is said to be of *arity* n or n-ary if $f \subset A_1 \times A_2 \times \cdots \times A_{n+1}$. In other notation, f is n-ary if

$$f : A_1 \times A_2 \times \cdots A_n \to A_{n+1}$$

This immediately gives us a rather simple result.

Lemma 4.26 *A n-ary function is a $(n + 1)$-ary relation.*

Proof. The formalites are left to the reader. Here is just the hint

$$\begin{array}{rr} \text{Unary } R : R \subseteq A_1 & \text{Unary } f : f : A_1 \to A_2 \\ \text{Binary } R : R \subseteq A_1 \times A_2 & \text{Binary } f : f : A_1 \times A_2 \to A_3 \\ \vdots & \vdots \\ \text{n-ary } R : R \subseteq A_1 \times A_2 \times \cdots A_n & \text{n-ary } f : f : A_1 \times A_2 \times \cdots A_n \to A_{n+1} \end{array}$$

□

Well, how about the converse? Are there relations that are not functions?

Lemma 4.27 *Not all relations are functions.*

Proof. Here's a counter example. Define (A, R) such that

- $A = \{1, 2\}$
- $R = \{(1, 1), (1, 2)\}$

□

Here's a nice little exercise.

Exercise* Let $f \subseteq A \times B$ be a relation such that

$$f^c = \Delta^c \circ f$$

Show that f is a function (remember, Δ is the diagonal relation and ^{c} is set complement).

Now we can finally talk about structures.

4.3 Giving structure to a set

Given a set A, a structure on a set A is a collection of functions and *equational axioms* relating elements and functions (Equational axioms just mean that the axioms are of the form of an identity). As an example of this, we jump a little forward and define what a commutative semigroup is. We will be very pedantic in the definition, and most books don't write it like this, but we must if we are to show it as a structure.

Example (Commutative semiroup as a structure) *A commutative semigroup is a set S and the following map*

$$m : S \times S \to S$$

subject to the following equational axioms: For all $a, b, c \in S$

1. *Commutativity :* $m(a, b) = m(b, a)$
2. *Associativity :* $m(a, m(b, c)) = m(m(a, b), c)$

Here's another slightly complicated example

Example (No idea what to call it) *Consider a set R and the following maps*

$$a : R \times R \to R$$

$$m : R \times R \to R$$

subject to the following equational axioms: For all $x, y, z \in R$

1. *Commutativity of a :* $a(x, y) = a(y, x)$

2. *Commutativity of m : $m(x, y) = m(y, x)$*

3. *Associativity of a : $a(x, a(y, z)) = a(a(x, y), z)$*

4. *Associativity of m : $m(x, m(y, z)) = m(m(x, y), z)$*

5. *Left distributivity of m over a : $m(x, a(y, z)) = a(m(x, y), m(x, z))$*

6. *Right distributivity of m over a : $m(a(x, y), z) = a(m(x, z), m(y, z))$*

To the avid reader, this must look familiar. a behaves just like addition and m behaves just like multiplication. Borrowing some terminology from the future, we can see that this is a ring except we have not really specified if it should have additive and multiplicative identities or not.

An example of the first structure is $\mathbb{N}$ with $m(a, b) = a + b$. In fact, $\mathbb{N} \setminus \{0\}$ with the same map also works.

An example of the second structure is $\mathbb{N}$ with $a(x, y) = x + y$ and $m(x, y) = xy$.

Definition 4.30 (Algebraic structure/Universal algebra) *An algebraic structure, also called an universal algebra, is a set with a collection of functions and equational axioms for the functions.*

Since this is course is about such structures, let us look at some more examples. We will again borrow things from the future, this time the definition of a group.

Example (Group, naive definition) *A group is a set G and the following map*

$$m : G \times G \to G$$

subject to the following axioms: For all $a, b, c \in S$

1. *Associativity: $m(a, m(b, c)) = m(m(a, b), c)$*

2. *Existence of identity: There exists $e \in G$ such that $m(a, e) = a$.*

3. *Existence of inverse: For every $a \in G$, there exists $d \in G$ such that $m(a, d) = e$.*

That's the formal definition of a group given everywhere. But, you will notice that this doesn't fit the universal algebra definition right now because there are *existential axioms* (like existence of identity and inverse) which are not equational. Does that mean a group is not an universal algebra? Not really. Here's how we can modify it.

Example (Group as a universal algebra) *A group is a set G and the following maps*

$$m : G \times G \to G$$

$$e : \varnothing \to G$$

$$\iota : G \to G$$

subject to the following equational axioms: For all $a, b, c \in S$

1. *Associativity:* $m(a, m(b, c)) = m(m(a, b), c)$
2. *Identity:* $m(a, e()) = a$
3. *Inverse:* $m(a, \iota(a)) = e()$

Exercise* Show that the two definitions of a group are equivalent.

We have successfully recasted the group definition to fit the mold of a universal algebra. Almost everything we meet will be universal algebras but they may have existential axioms which can be recasted in the form of equational axioms if required and hence we might not be so pedantic in the future.