Mathematics

Linear Algebra I

Preface to the Linear Algebra Course

Alexander Mendoza

August 26, 2023

Prologue

Contents

Chapter 1

Revisiting Algebra

Many mathematical theories rely on previous concepts to being built and Linear Algebra is not the exception, this is why we start the course by revisiting a concept that should be very familiar, such as algebra. Let us commence by playing around with operations.

1.1 Operations

But, what an operation is? Well, an operation defined in a non-empty set A is a function that takes two or more elements from the set A and returns a single element of the same set A. Think of it as a machine that takes two or more inputs and returns a single output. For now, we are going to focus on a particular type of operation, called the binary operation. As you may have guessed, the binary operation takes two inputs and returns a single output. Now that we have the intuitive idea of what a binary operation is, let's define it properly:

> **Definition**
>
> **Binary Operation.** Let A be a set, a binary operation $\oplus$ over A is defined as a function $\oplus : A \times A \to A$.

We can try to define our own operation as follows. First, we define the set in which our operation would live, let's take $\mathbb{Z}$ for example. Then we define the operation and the criteria for generating the output based on the input, let $\oplus : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ such that for all $x, y \in \mathbb{R}$:

$$x \oplus y = x + y + 2$$

Now we can try to prove properties for this operation. Usually, the first property that is analyzed is the associative property. This is because the associative property gives us flexibility when operating chained operations.

Associative property

Let $x, y, z \in \mathbb{Z}$,

$$(x \oplus y) \oplus z = x \oplus (y \oplus z)$$

Proof. For the proof, we are going to use the properties of the sum in the integers since our operation is defined on the aforementioned sum.

$$
\begin{aligned}
(x \oplus y) \oplus z &= (x + y + 2) + z + 2 && \text{Definition of operation } \oplus \\
&= x + y + z + 2 + 2 && \text{Commutative property of sum} \\
&= x + (y + z + 2) + 2 && \text{Associative property of sum} \\
&= x \oplus (y \oplus z) && \text{Definition of operation } \oplus
\end{aligned}
$$

Therefore, the operation $\oplus$ is associative.

Commutative property

Let $x, y \in \mathbb{Z}$,

$$x \oplus y = y \oplus x$$

Proof. The proof will be similar to the associative one, we'll use the already defined properties of the sum.

$$
\begin{aligned}
x \oplus y &= x + y + 2 && \text{Definition of operation } \oplus \\
&= y + x + 2 && \text{Commutative property of sum} \\
&= x \oplus y && \text{Definition of operation } \oplus
\end{aligned}
$$

Therefore, the operation $\oplus$ is commutative.

Identity or Neutral element

Let $x \in \mathbb{Z}$,

$$x \oplus -2 = x$$

Proof. As with the previous proofs, we continue to use the properties of the sum.

$$
\begin{aligned}
x \oplus id &= x && \text{Hypothesis} \\
x + id + 2 &= x && \text{Definition of operation } \oplus \\
id &= -2 && \text{Equality properties}
\end{aligned}
$$

Inverse element

Let $x \in \mathbb{Z}$,

$$x \oplus x^{-1} = -2$$

Proof.

$$
\begin{aligned}
x \oplus x^{-1} &= -2 && \text{Hypothesis} \\
x + x^{-1} + 2 &= -2 && \text{Definition of operation } \oplus \\
x^{-1} &= -x - 4 && \text{Equality properties}
\end{aligned}
$$

We will now see operations between equivalence classes, but first, we have to study equivalence classes.

1.2   Equivalence relations

In mathematics, we can think of a relation between two things as if they have something in common, then they are related. Take, for example, the relation that assigns to each child its mother; this relation can be defined in the set of all people, and then every person in that set will be related to its mother. More formally, a relation on a set A can be defined as a subset of $A \times A$, so if $a, b \in A$, then it's said that a is related to b if the ordered pair $(a, b) \in A \times A$. With these ideas, let's properly define what a relation is.

Definition

Relation. Let A and B be non-empty sets. A relation R from A to B is a subset $R \subseteq A \times B$. If $a \in A$ and $b \in B$, we write aRb if $(a, b) \in R$ and $a \not{R} b$ if $(a, b) \notin R$. A relation on A is a relation from A to A.

Relations have various properties, such as reflexivity that is when an element relates to itself. There are special types of relations, one of them is the equivalence relation, which definition is as follows.

Let A be a set and $\sim$ be a relation on A. The relation $\sim$ is said to be an equivalence relation if it meets the following properties:

- Reflexivity: $\sim$ is reflexive if $a \sim a$.

- Symmetric: $\sim$ is symmetric if $a \sim b$ then $b \sim a$.

- Transitivity: $\sim$ is transitive if $a \sim b$ and $b \sim c$, then $a \sim c$.

An example of an equivalence relation would be the relation of equality in the real numbers, you can verify that it satisfies all of the necessary properties. An equivalence relation is said to "partition" the set in which its defined, by partition we mean that it divides the set into other sets called partition or equivalence classes. More formally the definition of equivalence classes is as follows:

Definition

Equivalence class. Let A be a non-empty set and $\sim$ be an equivalence relation on A. The equivalence class of x with respect to $\sim$, written as $[x]$, is defined as follows $[x] = \{y \in A | x \sim y\}$ for all y in A.

A very important theorem of equivalence classes goes as follows.

Theorem

Let A be a non-empty set, and let $\sim$ be an equivalence relation on A.

1. Let $x, y \in A$. If $x \sim y$, then $[x] = [y]$. If $x \not\sim y$, then $[x] \cap [y] = \emptyset$.

2. $\bigcup_{x \in A}[x] = A$.

As expected, when we join all the equivalence classes of a set, we obtain the whole set. The set that contains all the equivalence classes of a set A is called the quotient set of A and is written as $A/\sim$.

Now that we know the necessary things, let's play around with equivalence relations and operations.

Let $\sim$ be a relation on $\mathbb{Z}$ such that $a \sim b$ if and only if $5|b - a$.

Let's see if $\sim$ is an equivalence relation by proving reflexivity, symmetry and transitivity.

Reflexivity. $a \sim a$ for all $a \in \mathbb{Z}$.

Proof. Let $a \in \mathbb{Z}$, then

$$a \sim a = 5|a - a$$
$$= 5|0$$

This means there exists $n \in \mathbb{Z}$ such that

$$5n = 0$$
$$5 \cdot 0 = 0$$

Therefore the relation is reflexive.

1.3   Algebraic Structures

Now that we have the concepts of relations and operations clear, we can define what we call algebraic structures. An algebraic structure consists of a non-empty set A, a collection of operations on A and a finite set of identities, known as axioms, that these operations must satisfy. As an example, take the integers. The integers is a set that has two binary operations (addition and multiplication) with certain axioms. There are many algebraic structures, we will begin studying the most important ones.

> **Definition**
>
> ***Semigroup.*** A semigroup is a set G together with a binary operation $\cdot$ that satisfies the associative property.

> **Definition**
>
> ***Monoid.*** A monoid is a semigroup that has an identity element.

> **Definition**
>
> ***Group.*** A group is a monoid with a unary operation (inverse).

> **Definition**
>
> ***Abelian group.*** An Abelian group is a group whose binary operation is commutative.

> **Definition**
>
> ***Field.*** A field is a set F together with two binary operations on F called addition and multiplication. Each of these operations together with F forms an abelian group, and the multiplication is distributive over the addition.

General properties of groups

When we study groups we must have in count some properties that can be inferred from the definition of group.

1. Let $a, b, c \in G$ if $a = b$ then $a * c = b * c$ and $c * a = c * b$

   Proof. Let $a, b, c \in G$. We know that $a = b$, now $a * c = a * c$ because $a = b$, $a * c = b * c$. The second statement can be verify with a similar method.

2. e, the identity element of $(G, *)$ is unique.

The idea behind this proof is to suppose there is another element, namely e' that behaves as the identity and then conclude e and e' are equal using the characteristic that an operation is a function.

Proof. Let $e' \in G$ such that $e' * x = x * e' = x$ for all $x \in G$. Now if $x = e$ then we have

$$e * e' = e' * e = e$$

Now if $x = e'$ then

$$e' * e = e * e' = e'$$

Because $*$ is a function $e = e'$ by definition.

Whenever we have an algebraic structure with an identity element it can be proved that it is unique using only the existence of the element. The proof always is similar to the one above.

3. For every $x \in G$, $-x \in G$ is unique.

As many of uniqueness proofs, we wil consider that there exists another inverse element and then conclude that it must be the same as the inverse element previously defined.

Proof. We know that $x * -x = -x * x = e$ for all $x \in G$. Now let $-x' \in G$ such that $x * -x' = -x' * x = e$ for all $x \in G$. Then

$$
\begin{aligned}
x * -x' &= -x * x & &\text{Replacing } e. \\
-x * x * -x' &= -x * x * -x' & &\text{Operate } x \text{ on both sides.} \\
(-x * x) * -x' &= -x * (x * -x) & &\text{Associative property of } *. \\
e * -x' &= -x * e & &\text{Replace } e. \\
-x' &= -x & &\text{Definition of identity element.}
\end{aligned}
$$

Therefore, the inverse element is unique.

4. For all $a, b \in G$, if $a * b = e$ then $b = -a$.

> **Idea for Proof**
>
> The idea to prove this property is using the equality $a * b = -a * a$.

Proof. Let $a, b \in G$ and suppose that $a * b = e$. We know that $-a * a = e$, then

$$a * b = -a * a \qquad \text{Replace } e.$$
$$-a * a * b = -a * a * -a \qquad \text{Operate } -a \text{ on both sides.}$$
$$b = -a$$

5. For all $x \in G$, $-(-x) = x$.

Proof. let $x \in G$, then we know that

$$-x * x = e$$
$$-(-x) * -x * x = e * -(-x) \qquad \text{Operate } -(-x) \text{ on both sides}$$
$$e * x = e * -(-x)$$
$$x = -(-x)$$

6. For all $a, b \in G$, $a = b$ if and only if $-a = -b$.

Proof. Let $a, b \in G$ and suppose $-a = -b$, Then

$$-a = -b$$
$$-(-a) = -(-b)$$
$$a = b$$

7. For all $a, b \in G$, $-(a * b) = -b * -a$.

Proof. Let $a, b \in G$. Then

$$(a * b) * (-b * -a) = a * (b * (-b * -a)) \qquad \text{Associative property.}$$
$$= a * ((b * -b) * -a) \qquad \text{Associative property.}$$
$$= a * (e - a) \qquad \text{Definition of identity.}$$
$$= a * -a \qquad \text{Definition of identity.}$$
$$= e \qquad \text{Definition of inverse.}$$

Therefore, because $(a * b) * (-b * -a) = e$, $-(a * b) = -b * -a$.

9

In an abelian group, by commutative property, we can conclude the following corollary.

Corollary

Let $(G, *)$ be an abelian group. Then $-(a * b) = -a * -b = -b * -a$.

1.4 Isomorphisms

Consider a function $\phi : (\mathbb{R}, +) \to (\mathbb{R}', \cdot)$ ($\mathbb{R}'$ is the same set $\mathbb{R}$ only differentiated from the domain), and let ϕ be defined as $\phi(x) = e^x$ then, for all $x, y \in \mathbb{R}$, $\phi(x + y) = e^{x+y} = e^x \cdot e^y = e(x) \cdot e(y)$

Definition

Isomorphism. Let $(G, *)$ and $(H, \circ)$ be abelian groups. Let $f : G \to H$ be a bijective function, such that for every $x, y \in G$

$$f(x * y) = f(x) \circ f(y)$$

We say that f is an isomorphism and that G and H are isomorph.

You can think intuitively of an isomorphism as two objects being the same essentially altough they may seem different in the surface. Consider two objects A and B, if there exists an isomorphism between these two objects, that would mean that there is a mapping or a function between the elements of A and B, and this mapping not only links them up, but also respects the structural properties and operations inherent to both A and B. Let's review another example to be more familiar with the concept of isomorphism.

Let's construct an isomorphism between $\mathbb{R}$ and $(-1, 1)$ to define a new operation on $(-1, 1)$. What we want to achieve is to copy the structure of $\mathbb{R}$ in $(-1, 1)$ and define a new "addition" operation. Consider the function $t : \mathbb{R} \to (-1, 1)$ such that

$$t(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$$

You can verify that this function is both injective and surjective and that its inverse is $t^{-1} : (-1, 1) \to \mathbb{R}$ such that $t^{-1}(x) = \ln(\sqrt[2]{\frac{1+x}{1-x}})$. @ith our definition of isomorphism we can now define our new operation $\oplus$ on $(-1, 1)$.

Let $x, y \in (-1, 1)$

$$x \oplus y = t(t^{-1}(x) + t^{-1}(y))$$

$$= \frac{e^{ln(\sqrt[2]{\frac{1+x}{1-x}})+ln(\sqrt[2]{\frac{1+y}{1-y}})} - e^{-ln(\sqrt[2]{\frac{1+x}{1-x}})-ln(\sqrt[2]{\frac{1+y}{1-y}})}}{e^{ln(\sqrt[2]{\frac{1+x}{1-x}})+ln(\sqrt[2]{\frac{1+y}{1-y}})} + e^{-(ln(\sqrt[2]{\frac{1+x}{1-x}})+ln(\sqrt[2]{\frac{1+y}{1-y}}))}}$$

$$= \frac{x + y}{xy + 1}$$

We can now verify that our new operation has the same structure as the addition on $\mathbb{R}$.

We now are ready to start looking at a direction that is closer to linear algebra by reviewing vector spaces. We shall review this concept in the next chronicle.