MATH 541 L1 Notes

Jan 30, 2023

We will cover basics of **groups**, **rings**, and **modules**. There are all **sets** with additional structures.

Example 0.1

$\mathbb{R}$ is a ring (a field). A vector space over $\mathbb{R}$ is a module.

1 Recap of Sets

A, B are sets, $f : A \to B$ is a function.

Definition 1.1 Injection

f is an **injection** if $f(a) = f(b) \implies a = b$.

Example 1.1

$f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ is not an injection. $f(2) = f(-2), 2 \neq -2$

Definition 1.2 Surjection

f is a **surjection** if $\forall b \in B, \exists a \in A, \text{s.t. } f(a) = b$

Definition 1.3 Bijection

f is a **bijection** if f is both a **surjection** and an **injection**. f is bijective $\iff$ f has an unique inverse function f^{-1}.

$$f^{-1}(f(a)) = a \; \forall a \in A, \quad f(f^{-1}(b)) = b \; \forall b \in B$$

1.1 Products of Sets

Definition 1.4 Products of Sets

A, B are sets, $A \times B$ is the set of all ordered pairs (a, b) where $a \in A, b \in B$. $A \times B = \{(a, b) | a \in A, b \in B\}$

Example 1.2

$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$

2 Binary Operation

Definition 2.1 Binary Operation

Binary Operation on a set X is a function $*$

$$* : X \times X \to X, (x, y) \mapsto x + y$$

Example 2.1

$X = \mathbb{Z}$, $* = +$ is a binary operation on $\mathbb{R}$, $3 + 5 = 8$

Example 2.2

Consider the set $[n] = \{1, 2, \cdots, n\}$,

$$\mathrm{Aut}([n]) = \{f : [n] \to [n] \mid f \text{ is bijective}\}$$

$n = 3,\ f = (2, 1, 3) = (1, 3, 2)$ (Cycle Representation), can form

$$\begin{tikzcd} [n] \arrow[r, "g"] \arrow[rr, bend right, "f \circ g"'] & [n] \arrow[r, "f"] & [n] \end{tikzcd}$$

$$\begin{aligned} f \circ g(1) &= f(g(1)) = f(1) = 3 \\ f \circ g(2) &= f(g(2)) = f(3) = 2 \\ f \circ g(3) &= f(g(3)) = f(2) = 1 \\ f \circ g &= (3, 1) = (1, 3) \end{aligned}$$

$(\mathrm{Aut}[n], \circ)$ forms a group.

3 Group

Definition 3.1 Group

A group G is a **set** equipped with a binary operation $*$ such that:

- Associative: $(a * b) * c = a * (b * c),\ \forall a, b, c \in G$
- Identity: $\exists e \in G,\ e * a = a * e = a,\ \forall a \in G$
- Inverse: $\forall a \in G,\ \exists a^{-1} \in G,\ a * a^{-1} = a^{-1} * a = e$

Example 3.1

Check $(\mathrm{Aut}[n], \circ)$ is a group.

- Associative: $(f \circ g) \circ h = f \circ (g \circ h)$. This is an equality of functions: $[n] \to [n]$.
  i.e. $\forall x \in [n], (f \circ g) \circ h(x) = f \circ (g \circ h)(x) = f(g(h(x)))$
- Identity: $\exists e \in \mathrm{Aut}[n],\ e \circ f = f \circ e = f$. i.e $\mathrm{id}_{[n]}(x) = x, \forall x \in [n]$, namely the permutation that does nothing.
- Inverse: $f \in \mathrm{Aut}([n])$ is bijective.
  i.e. $\forall f \in \mathrm{Aut}[n],\ \exists f^{-1} \in \mathrm{Aut}[n],\ f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_{[n]}$.

Exercise 1. Compute $(1,2,3) \circ (2,3)$ and $(2,3) \circ (1,2,3)$

$$(1,2,3) \circ (2,3) = (2,1,3)$$
$$(2,3) \circ (1,2,3) = (1,3)$$

In general, for a group $(G, *)$, $a * b \neq b * a$ (not necessarily)

Definition 3.2 Abelian Group

If $a * b = b * a, \forall a, b \in G$, then G is called **abelian**, or **commutative**.

Example 3.2

$(\mathbb{Z}, +)$ is an abelian group.
$(\mathbb{Z}, *)$ is **NOT** a group! (Inverse of 0 does not exist)
$(\pm 1, \times)$ is an abelian group.
$M_{n\times n} = \{n \times n \text{ matrices} / \mathbb{R}\}$ $(M_{n\times n}, +)$ is an abelian group.
$M^{\times}_{n\times n} = \{A \in M_{n\times n} |\, \det(A) \neq 0\}$. Then $(M^{\times}_{n\times n}, \times)$ is a group.
$\mathbb{R}^n \to \mathbb{R}^n$ usually not commutative.