MATH 541 01/25

We will cover basics of groups, rings, and modules

These are all <u>sets</u> w/ additional structures

E.g. $\mathbb{R}$ is a ring (a field)

A vector space over $\mathbb{R}$ is a module

Recap of sets $A, B =$ sets

$f: A \to B$ a function

non-example

f is injective if $f(a) = f(b) \Rightarrow a = b$

$f: \mathbb{R} \to \mathbb{R}$

$x \mapsto x^2$

not inj. $f(2) = f(-2)$

surjective if $\forall b \in B, \exists a \in A,$ s.t. $f(a) = b$

($\forall$: for all; $\exists$: exists; s.t.: such that)

bijective both injective and surjective

unique if exists

f is bijective $\Leftrightarrow$ f has an inverse f^{-1}

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

Products of sets $A, B =$ sets

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

e.g. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$

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

$* : X \times X \to X$

$(x, y) \mapsto x + y$

Example $X = \mathbb{Z}$ (integers)

$* = +$ $\quad 3 + 5 = 8$

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

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

Ex. $n=3$ $\quad f = (2,1,3) = (1,3,2) \quad g = (2,3)$

$2 \mapsto 1,\ 1 \mapsto 3,\ 3 \mapsto 2 \qquad 2 \mapsto 3,\ 3 \mapsto 2,\ 1 \mapsto 1$

can form $f \circ g$

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

$$f \circ g(1) = f(g(1)) = f(1) = 3$$
$$f \circ g(2) = f(g(2)) = f(3) = 2$$
$$f \circ g(3) = f(g(3)) = f(2) = 1$$

$$f \circ g = (3,1) = (1,3)$$

$(\mathrm{Aut}[n], \circ)$ forms a <u>group</u>

A group G is a <u>set</u> equipped w/ a binary operation $*$, s.t.

(i) $(a*b)*c = a*(b*c)$, $\forall a,b,c \in G$

(ii) $\exists e \in G$, s.t. $e*a = a*e = a$, $\forall a \in G$

(iii) $\forall a \in G$, $\exists a^{-1} \in G$ s.t. $a*a^{-1} = a^{-1}*a = e$

Check $(\mathrm{Aut}([n]), \circ)$ as group

(i) associativity $\quad (f \circ g) \circ h = f \circ (g \circ h)$ This is an equality of functions $[n] \to [n]$

Need: $\forall x \in [n]$, $(f \circ g) \circ h(x) = f \circ (g \circ h)(x)$

$$(f \circ g) \circ h(x) = f(g(h(x))) = f \circ (g \circ h)(x)$$

(ii) e is called the identity element

$e \in Aut([n])$ is just the identity function $id_{[n]}(x) = x$, $\forall x \in [n]$

(The permutation that does nothing)

(iii) clear. b/c $f \in Aut([n])$ is bijective

Exercise 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)

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

Ex $(\mathbb{Z}, +)$ is an abelian group

$(\mathbb{Z}, \times)$ is not a group!

(inverses do not always 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

$(M_{n\times n}, \cdot)$ $\quad (\{0\}, \cdot)$

$M^{\times}_{n\times n} = \{A \in M_{n\times n} \mid \det(A) \neq 0\}$

Then $(M^{\times}_{n\times n}, \cdot)$ is a group

$\mathbb{R}^n \to \mathbb{R}^n$ usually not commutative