Lecture 4:

Binary operations:

Def: A binary operation $*$ on a set S is a function $* : S \times S \to S$

We denote $*(a,b)$ by $a * b$.
(for $a, b \in S$)

Examples:

- $+$ on $\mathbb{R}, \mathbb{Z}, \mathbb{Q} \ldots$
- $\times$ on $\mathbb{R}, \mathbb{Z}, \mathbb{Q}, \ldots$
- $+$ on $\mathbb{Z}_{\geq 0}$
- $\times$ on $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$.
  (multiplication)
- multiplication ~~on~~ $M_n(\mathbb{R})$
  set of $n \times n$ real matrices.
- non-example: multiplication on all real matrices $M(\mathbb{R})$ is not a binary operation because you can't multiply 3×3 and 2×2 matrices.
  So it's not a function
  $\times : M(\mathbb{R}) \times M(\mathbb{R}) \to M(\mathbb{R})$.
- addition on $M_n(\mathbb{R})$ $n \times n$ matrices
- $+, \cdot$ on $\mathbb{Z}/n\mathbb{Z}$.
  $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}\}$.
- multiplication on $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$.
- Let $F = \{f : \mathbb{R} \to \mathbb{R}\}$ set of all functions $f : \mathbb{R} \to \mathbb{R}$.
  Composition on F is a binary operation
- In general, composition on $\mathrm{Fun}(S,S)$ ← set of all $f : S \to S$.

- subtraction on $\mathbb{R}, \mathbb{Q}, \mathbb{Z}, \ldots$

  also a binary operation

  (not on $\mathbb{N}$ since $3-5 \notin \mathbb{N}$).

Definitions: (1) a binary operation $*$ on S is commutative if $\forall a, b \in S$, $a*b = b*a$

(2) is associative if, for all $a, b, c \in S$,

$$a*(b*c) = (a*b)*c.$$

Q: which of the above examples are commutative binary operations?

Remark: If $*$ is associative, then writing

$a*b*c$ makes sense because

$$(a*b)*c = a*(b*c)$$

So it's up to us how to put the parantheses, the answer is the same regardless.

Ex: A non-associative binary operation?

$$(a-b)-c \neq a-(b-c)$$
$$(a-b)+c.$$

Proposition: (Function composition is associative.)

Let $f, g, h \in \mathrm{Fun}(S,S)$. Then:

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

Proof: To show that two functions are equal, we show that they take every $x \in S$ to the same values.

Let $x \in S$.

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

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

Hence $f\circ(g\circ h) = (f\circ g)\circ h$. $\square$.

Remark: Matrix multiplication is also associative. You can prove it using the definition. But there is a nicer way: each $n\times n$ matrix M corresponds to a linear map $T_M : \mathbb{R}^n \to \mathbb{R}^n$. If you multiply the matrices, then you get the matrix of the composition of T_{M_1} and T_{M_2}.

ie

matrix of $T_{M_1}\circ T_{M_2} = M_1 \cdot M_2$.

Hence matrix multiplication is also associative (since function composition is).