Groups

Def: Let A be a set. A binary operation on A is a function

$$* : A \times A \to A$$

Notation: $(a, b) \longmapsto a * b$

Examples:

- $+$, $-$, and $\cdot$ are binary operations on $\mathbb{Z}$
- $\div$ is not a binary operation on $\mathbb{Z}$
- $\div$ is a binary operation on $\mathbb{Q} \setminus \{0\}$
- $a * b = a^b$ is a binary operation on $\mathbb{R}_{>0}$.
- $a * b = \sqrt{ab}$ is a binary operation on $\mathbb{R}_{>0}$.
- matrix addition and matrix multiplication are binary operations on $M_n(\mathbb{R})$.

Def: Let $*$ be a binary operation on a set A.

① We say $*$ is <u>associative</u> if

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

for all $a,b,c \in A$.

② We say $*$ is <u>commutative</u> if

$$a*b = b*a$$

for all $a,b \in A$.

③ Let $e \in A$. We say e is an <u>identity element</u> for $*$ if

$$e*a = a \quad \text{and} \quad a*e = a$$

for all $a \in A$

(4) Let $a, b \in A$. If e is an identity element for $*$ and

$$a * b = e \quad \text{and} \quad b * a = e,$$

then we say b is an <u>inverse of a</u> under $*$.

<u>Ex</u>:
- $+$ on $\mathbb{Z}$:
  - associative ✓
  - commutative ✓
  - identity element 0 ✓
  - $n \in \mathbb{Z}$ has inverse $-n$ ✓
- $\cdot$ on $\mathbb{Z}$
  - associative ✓
  - commutative ✓
  - identity element 1 ✓
  - 1 is inverse for 1,
    -1 is inverse for -1,
    but no other $n \in \mathbb{Z}$ has an inverse ✗

- $\cdot$ on $\mathbb{Q}$:
  - associative ✓
  - commutative ✓
  - identity element 1 ✓
  - $r \in \mathbb{Q}$ has inverse $\frac{1}{r}$ if $r \neq 0$,
    0 has no inverse ✗

- $a * b = a^b$ on $\mathbb{R}_{>0}$:
  - not associative $\left((2^2)^3 = 2^6 \neq 2^{(2^3)} = 2^8\right)$ ✗
  - not commutative $(2^3 \neq 3^2)$ ✗
  - no identity element ✗
  - therefore cannot even define inverses ✗

- Matrix mult. on $M_n(\mathbb{R})$:
  - associative ✓
  - not commutative ✗
  - identity element $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ ✓
  - some matrices have inverses,
    some do not (determinant) ✗

Some basic uniqueness properties:

Thm: Let $*$ be a binary operation on a set A.

① If there is an identity element for $*$ in A, then it is unique.

② Suppose $*$ is associative. If $a \in A$ has an inverse under $*$, then this inverse is unique. We denote it a^{-1}.

③ Suppose $*$ is associative and $a, b \in A$.

- If a has an inverse under $*$, then so does a^{-1}, and $(a^{-1})^{-1} = a$.

- If a and b each have an inverse under $*$, then so does $a * b$, and

$$(a * b)^{-1} = b^{-1} * a^{-1}$$

Proof: ① Suppose $e_1, e_2 \in A$ are each identity elements for $*$.

Then $e_1 \underset{\substack{\uparrow \\ e_2 \text{ is} \\ \text{identity}}}{=} e_1 * e_2 \underset{\substack{\uparrow \\ e_1 \text{ is} \\ \text{identity}}}{=} e_2$

② Let $a \in A$, and suppose $b_1, b_2 \in A$ are each inverses for a under $*$.

Then
$$\begin{aligned} b_1 &= b_1 * e \\ &= b_1 * (a * b_2) \\ &= (b_1 * a) * b_2 \\ &= e * b_2 \\ &= b_2. \end{aligned}$$

So we write a^{-1} for the element $b_1 = b_2$.

③ If a and b are invertible, then

$$a^{-1} * a = e \quad \text{and} \quad a * a^{-1} = e,$$

so a is an inverse for a^{-1}. By uniqueness, $(a^{-1})^{-1} = a$.

Also,

$$\begin{aligned}(a*b) * (b^{-1} * a^{-1}) &= a * (b * b^{-1}) * a^{-1} \\ &= a * e * a^{-1} \\ &= a * a^{-1} \\ &= e.\end{aligned}$$

Similarly, $(b^{-1} * a^{-1}) * (a * b) = e$.

By uniqueness of inverses, then,

$$(a*b)^{-1} = b^{-1} * a^{-1}.$$

∎

Def: A <u>group</u> $(G, *)$ is a set G with a binary operation $*$ on G such that

1. $*$ is associative;
2. there exists an identity element $e \in G$ for $*$; and
3. each $a \in G$ has an inverse $a^{-1} \in G$ under $*$.

Note: By the theorem, the identity and inverses in a group are unique.

Ex:
- $(\mathbb{Z}, +)$ is a group
- $(\mathbb{Z}, \cdot)$ and $(\mathbb{Q}, \cdot)$ are not
- $(\mathbb{Q} \setminus \{0\}, \cdot)$ is a group

Def: A group $(G, *)$ is called <u>abelian</u> if $*$ is commutative.