# Binary operations

Suppose $G$ is a set. A binary operation on $G$ is a function $*: G \times G \to G$.

Notation: $*(a,b) = a * b$.

Examples and non-examples:

Which of the following are binary operations?

$+$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$

$-$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$

$\cdot$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$

$\div$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$

$\div$ on $\mathbb{Z}\setminus\{0\}$

$\div$ on $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, or $\mathbb{C}\setminus\{0\}$

$\times$ (cross product) on $\mathbb{R}^3$

$\cdot$ (dot product) on $\mathbb{R}^3$

$+$ on $M_{m,n}(\mathbb{R})$ ($M_{m,n}(\mathbb{R}) = \{m\times n$ mats. w/ coeffs. in $\mathbb{R}\}$)

$\cdot$ on $M_{n,n}(\mathbb{R})$

$+$ on $GL_2(\mathbb{R})$ ($GL_2(\mathbb{R}) = \{A \in M_{2,2}(\mathbb{R}) : \det(A) \neq 0\}$)

$\cdot$ on $GL_2(\mathbb{R})$

$\Delta$ on $\mathcal{P}(S)$ ($S$ a set)

Answer:

- Binary operations:

  $+$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$

  $-$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$

  $\cdot$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$

  $\div$ on $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, or $\mathbb{C}\setminus\{0\}$

  $\times$ (cross product) on $\mathbb{R}^3$

  $+$ on $M_{m,n}(\mathbb{R})$     $\cdot$ on $GL_2(\mathbb{R})$

  $\cdot$ on $M_{n,n}(\mathbb{R})$     $\Delta$ on $\mathcal{P}(S)$

- Not binary operations:

  $\div$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$

  $1 \div 0$ not defined

  $\div$ on $\mathbb{Z}\setminus\{0\}$

  $1 \div 2 \notin \mathbb{Z}\setminus\{0\}$

  $\cdot$ (dot product) on $\mathbb{R}^3$

  for $\vec{u}, \vec{v} \in \mathbb{R}^3$, $\underbrace{\vec{u}\cdot\vec{v}}_{}^{\in\mathbb{R}} \notin \mathbb{R}^3$

  $+$ on $GL_2(\mathbb{R})$     $(A, B \in GL_2(\mathbb{R}))$

  Let $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Then $\det A = \det B = 1$,

  but $\det(A+B) = \det\left(\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\right) = 0$.     $(A+B \notin GL_2(\mathbb{R}))$

Some properties that a binary operation

$*: G \times G \to G$ could have:

- Associativity:

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

- Commutativity:

  $\forall a, b \in G, \quad a*b = b*a.$

Exs:

$+$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ (associative, commutative)

$-$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ (not associative, not commutative)

- $(a-b)-c = a-(b+c) \neq a-(b-c)$, in general

  Ex: $a=b=c=1$, $(a-b)-c = (1-1)-1 = -1$

  $a-(b-c) = 1-(1-1) = 1$

- $a-b \neq b-a$, in general

  Ex: $a=1$, $b=0$, $a-b = 1-0 = 1$

  $b-a = 0-1 = -1$

$\cdot$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ (associative, commutative)

$\div$ on $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, or $\mathbb{C}\setminus\{0\}$

(not associative, not commutative)

- $(1\div 2)\div 2 = \frac{1}{2}\div 2 = \frac{1}{4}$
  $\not=$
  $1\div(2\div 2) = 1\div 1 = 1$

- $1\div 2 = \frac{1}{2}$
  $\not=$
  $2\div 1 = 2$

$\times$ (cross product) on $\mathbb{R}^3$ (not associative, not commutative)

- $(\vec{i}\times\vec{i})\times\vec{j} = \vec{0}\times\vec{j} = \vec{0}$
  $\not=$
  $\vec{i}\times(\vec{i}\times\vec{j}) = \vec{i}\times\vec{k} = -\vec{j}$

- $\vec{i}\times\vec{j} = \vec{k}$
  $\not=$
  $\vec{j}\times\vec{i} = -\vec{k}$

$+$ on $M_{m,n}(\mathbb{R})$ (associative, commutative)

$\cdot$ on $M_{n,n}(\mathbb{R})$ (associative, not commutative unless $n=1$)

- Ex of non-com. when $n\geq 2$:

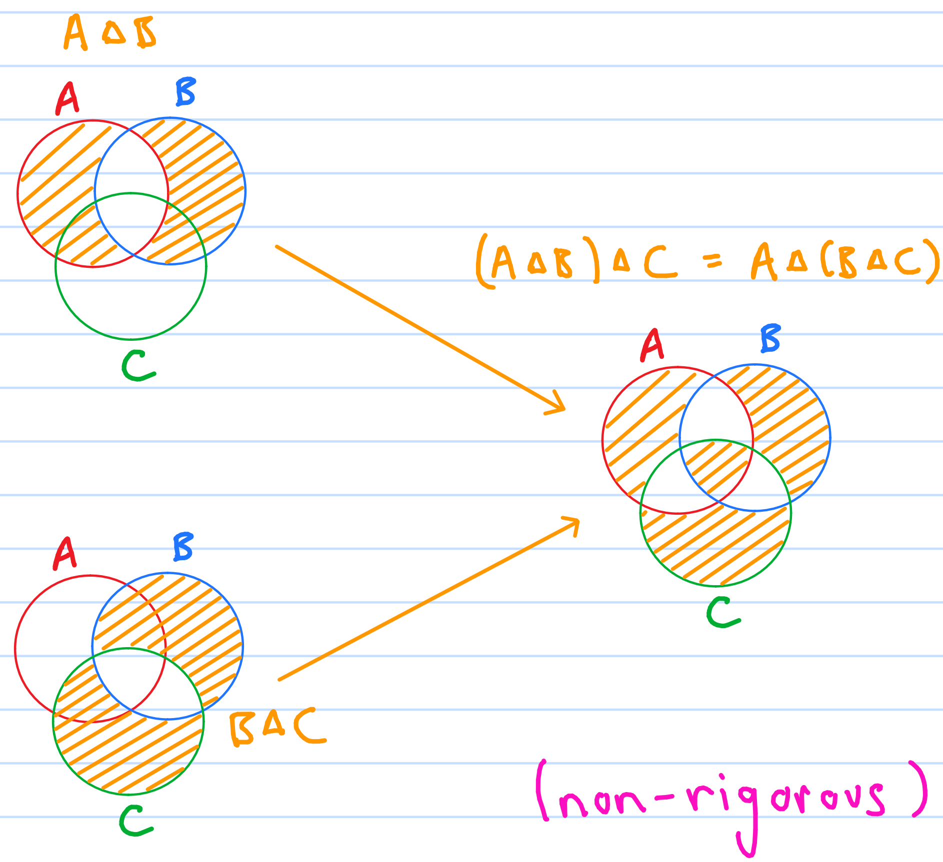
Let $A = \begin{pmatrix} 1 & 0 & \cdots & 0 & 2 \\ 0 & 1 & 0 & & 0 \\ \vdots & & \ddots & & \vdots \\ \vdots & & & \ddots & 0 \\ 0 & \cdots & & 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$.

Then $\underbrace{AB}_{(1,n)\text{ coefficient is } 2} \neq \underbrace{BA}_{(1,n)\text{ coefficient is } 4}$

$\cdot$ on $GL_2(\mathbb{R})$ (associative, not commutative)

$\Delta$ on $\mathcal{P}(S)$ (associative, commutative)

- Associativity: Suppose $A, B, C \in \mathcal{P}(S)$.



# Groups

A <u>group</u> is a pair $(G, *)$, where $G$ is a set and $*$ is a binary operation on $G$, satisfying:

1) $*$ is associative, (identity element)

2) $\exists e \in G$ s.t. $\forall g \in G$, $e * g = g * e = g$, and

   (existence of identity) (inverse of g)

3) $\forall g \in G$, $\exists h \in g$ s.t. $g * h = h * g = e$.

   (existence of inverses)

If, in addition, $*$ is commutative, then we say that $(G, *)$ is an <u>Abelian</u> group.

Otherwise, it is <u>non-Abelian</u>.

$+$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ (associative, commutative)

- $(\mathbb{Z},+)$: (Abelian group)

  identity: Let $e=0$. Then $\forall n \in \mathbb{Z}$,

  $e+n=n+e=n$. ✓

  inverses: $\forall n \in \mathbb{Z}$ let $m=-n \in \mathbb{Z}$. Then

  $n+m=m+n=0$. ✓

- $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$: (Abelian groups)

  identity $=0$ ✓

  inverse of $x=-x$ ✓

$\cdot$ on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$ (associative, commutative)

- $(\mathbb{Z},\cdot)$: (not a group)

  identity: Let $e=1$. Then $\forall n \in \mathbb{Z}$,

  $e\cdot n=n\cdot e=n$. ✓

  inverses: Consider $2 \in \mathbb{Z}$. If

  $2\cdot m=1$ then $m=\frac{1}{2} \notin \mathbb{Z}$. Therefore,

  $2$ is non-invertible in $(\mathbb{Z},\cdot)$. ×

- $(\mathbb{Q},\cdot), (\mathbb{R},\cdot), (\mathbb{C},\cdot)$ : (not groups)

  identity $= 1$ ✓

  inverse of $x = \frac{1}{x}$ if $x \neq 0$.

  inverse of $0$ ? does not exist. x

  $(0 \cdot m = 1)$

- on $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, or $\mathbb{C}\setminus\{0\}$ (associative, commutative)

  - $(\mathbb{Q}\setminus\{0\},\cdot), (\mathbb{R}\setminus\{0\},\cdot), (\mathbb{C}\setminus\{0\},\cdot)$ : (Abelian groups)

    identity $= 1$ ✓

    inverse of $x = \frac{1}{x}$ ✓

$+$ on $M_{m,n}(\mathbb{R})$ (associative, commutative)

  - $(M_{m,n}(\mathbb{R}), +)$ : (Abelian group)

    identity $= \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$ ($0$ matrix) ✓

    inverse of $A = -A$. ✓

- on $M_{n,n}(\mathbb{R})$ (associative, not commutative unless $n=1$)

  - $(M_{n,n}(\mathbb{R}), \cdot)$ : (not a group)

    identity $= I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix}$ (identity matrix) ✓

    inverse of zero matrix does not exist x

- $\cdot$ on $GL_2(\mathbb{R})$ (associative, not commutative)

  - $(GL_2(\mathbb{R}), \cdot)$: (non-Abelian group)

    identity $= I_2$ ✓

    inverses: If $A \in GL_2(\mathbb{R})$ then

    $\det A \neq 0 \Rightarrow \exists B \in GL_2(\mathbb{R})$ s.t. $AB = BA = I_2$.

    $\left( A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow B = \frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \right)$

- $\Delta$ on $\mathcal{P}(S)$ (associative, commutative)

  - $(\mathcal{P}(S), \Delta)$: (Abelian group)

    identity: Let $e = \phi \in \mathcal{P}(S)$. Then, $\forall A \in \mathcal{P}(S)$,

    $e \Delta A = A \Delta e = (A \setminus \phi) \cup (\phi \setminus A) = A$. ✓

    inverses: $\forall A \in \mathcal{P}(S)$, let $B = A$. Then

    $A \Delta B = B \Delta A = A \Delta A = (A \setminus A) \cup (A \setminus A) = \phi$. ✓