Bijections

Definition

A function $f : X \to Y$ is bijective if f maps exactly one element of X to every element of Y. That is, for every $y \in Y$ there exists exactly one $x \in X$ such that $f(x) = y$.

Examples:

- $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = 2x$ is bijective, since only $y/2$ is mapped to y.
- $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = 2^x$ is not bijective, since nothing maps to -1.
- $f : \mathbf{R} \to \mathbf{R}$ defined by $f(x) = x^3 - x$ is not bijective, since $f(-1) = f(0) = f(1) = 0$.

Inverse functions

Definition

Let $f : X \to Y$ be a bijective function. The inverse function $f^{-1} : Y \to X$ is defined by $f^{-1}(y) = x$ if and only if $f(x) = y$.

- For every $x \in X$,
$$f^{-1}(f(x)) = x.$$
- For every $y \in Y$,
$$f(f^{-1}(y)) = y.$$

Permutations

Definition

For a finite set X, a bijective function $\pi : X \to X$ is a permutation on X.

Example: A function defined by

$$\begin{array}{lll} \pi(1) = 1 & \pi(2) = 3 & \pi(3) = 2 \\ \pi(4) = 6 & \pi(5) = 4 & \pi(6) = 5 \end{array}$$

is a permutation on $\{1, 2, 3, 4, 5, 6\}$.

Representation of permutations

$$\pi(1) = 1 \qquad \pi(2) = 3 \qquad \pi(3) = 2$$
$$\pi(4) = 6 \qquad \pi(5) = 4 \qquad \pi(6) = 5$$

- By a table of values:

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5

- By an ordering of the elements (lower line of the table):

$$1, 3, 2, 6, 4, 5$$

Representation of permutations

$\pi(1) = 1$ $\quad$ $\pi(2) = 3$ $\quad$ $\pi(3) = 2$

$\pi(4) = 6$ $\quad$ $\pi(5) = 4$ $\quad$ $\pi(6) = 5$

- By its graph:

- By a list of cycles of the permutation:

$$(1)(23)(465)$$

- By a reduced list of cycles (excluding cycles of length 1):

$$(23)(465)$$

Composition of permutations

Definition

Permutation ρ on a set X is the composition of permutations π and σ if $\rho(x) = \pi(\sigma(x))$ for every $x \in X$. We write

$$\rho = \pi \circ \sigma.$$

Remark: sometimes the opposite notation ($\sigma \circ \pi$) is used.

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)(5)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Example

x	1	2	3	4	5	6
$\sigma(x)$	2	1	4	3	6	5
x	2	1	4	3	6	5
$\pi(x)$	3	1	6	2	5	4
x	1	2	3	4	5	6
$(\pi \circ \sigma)(x)$	3	1	6	2	5	4

$$\pi \circ \sigma = (23)(465) \circ (12)(34)(56) = (13642)$$

Not commutative:

$$\sigma \circ \pi = (12)(34)(56) \circ (23)(465) = (12453)$$

Properties

- Associative:

$$\{\sigma \circ \pi\} \circ \rho = \sigma \circ \{\pi \circ \rho\}$$

$$\begin{aligned}\sigma(\pi(\rho(x))) = \{\sigma \circ \pi\}(\rho(x)) &= [\{\sigma \circ \pi\} \circ \rho](x) \\ = \sigma(\{\pi \circ \rho\}(x)) &= [\sigma \circ \{\pi \circ \rho\}](x)\end{aligned}$$

- Identity permutation:

$$\mathrm{id}(x) = x \quad \text{for all } x$$

$$\mathrm{id} \circ \pi = \pi \circ \mathrm{id} = \pi$$

Application: Puzzles

Initial state:

Requested final state:

Application: Puzzles

Permutation representing the state: $n \mapsto$ number at position n.

$\pi_0 = \mathrm{id}$

$\pi_1 = (5, 6)$

Rotation of the middle piece: $\pi \mapsto \pi \circ (1, 4)(2, 3)$
Shifting the numbers: $\pi \mapsto \pi \circ (1, 2, 3, 4, \ldots, 18, 19)$

Lemma

A position is solvable if and only if its permutation can be expressed as a composition $\sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_m$, where each of σ_1, $\ldots$, σ_m is either $(1, 4)(2, 3)$ or $(1, 2, 3, 4, \ldots, 18, 19)$.

Inverse permutation

Definition

For a permutation $\pi : X \to X$, we call π^{-1} the inverse permutation.

$$\pi^{-1}(y) = x \text{ if and only if } \pi(x) = y$$

$$\pi^{-1} \circ \pi = \pi \circ \pi^{-1} = \text{id}$$
$$(\pi \circ \sigma)^{-1} = \sigma^{-1} \circ \pi^{-1}$$

Example

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5

x	1	3	2	6	4	5
$\pi^{-1}(x)$	1	2	3	4	5	6

$$\pi^{-1} = [(23)(465)]^{-1} = (32)(564) = (23)(456)$$

Example

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5

x	1	2	3	4	5	6
$\pi^{-1}(x)$	1	3	2	5	6	4

$$\pi^{-1} = [(23)(465)]^{-1} = (32)(564) = (23)(456)$$

Example

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5

x	1	2	3	4	5	6
$\pi^{-1}(x)$	1	3	2	5	6	4

$$\pi^{-1} = [(23)(465)]^{-1} = (32)(564) = (23)(456)$$

Example

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5

x	1	2	3	4	5	6
$\pi^{-1}(x)$	1	3	2	5	6	4

$$\pi^{-1} = [(23)(465)]^{-1} = (32)(564) = (23)(456)$$

Example

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5

x	1	2	3	4	5	6
$\pi^{-1}(x)$	1	3	2	5	6	4

$$\pi^{-1} = [(23)(465)]^{-1} = (32)(564) = (23)(456)$$

Example

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5
x	1	2	3	4	5	6
$\pi^{-1}(x)$	1	3	2	5	6	4

$$\pi^{-1} = [(23)(465)]^{-1} = (32)(564) = (23)(456)$$

Example

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5

x	1	2	3	4	5	6
$\pi^{-1}(x)$	1	3	2	5	6	4

$$\pi^{-1} = [(23)(465)]^{-1} = (32)(564) = (23)(456)$$

Permutation matrices

Definition

For a permutation $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$, the permutation matrix P_π is the $n \times n$ matrix satisfying

$$P_\pi \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{\pi(1)} \\ x_{\pi(2)} \\ \cdots \\ x_{\pi(n)} \end{pmatrix} \qquad \text{i.e. } P_\pi e_k = e_{\pi^{-1}(k)}.$$

- $P_\pi = (e_{\pi(1)}|e_{\pi(2)}| \ldots |e_{\pi(n)})^T = (e_{\pi^{-1}(1)}|e_{\pi^{-1}(2)}| \ldots |e_{\pi^{-1}(n)})$
- Product and composition (note the reversed order!)

$$P_{\pi \circ \sigma} = P_\sigma P_\pi$$

- $P_{\pi^{-1}} = P_\pi^{-1} = P_\pi^T$

Example

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5

$$P_\pi = (e_1|e_3|e_2|e_6|e_4|e_5)^T$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 1 \\ 3 \\ 2 \\ 6 \\ 4 \\ 5 \end{pmatrix}$$

Sign of a permutation

Definition

For a permutation $\pi : X \to X$,

$$\operatorname{sgn}(\pi) = (-1)^{|X| - \text{number of cycles of } \pi}$$

The permutation π is even if $\operatorname{sgn}(\pi) = 1$ and odd if $\operatorname{sgn}(\pi) = -1$.

Example:

x	1	2	3	4	5	6
$\pi(x)$	1	3	2	6	4	5

$$\operatorname{sgn}((23)(465)) = \operatorname{sgn}((1)(23)(465)) = (-1)^{6-3} = -1$$

Transposition

Definition

For distinct $a, b \in X$, let $\tau_{a,b} : X \to X$ be defined by

$$\tau_{a,b}(x) = \begin{cases} \text{a} & \text{if } x = b \\ \text{b} & \text{if } x = a \\ \text{x} & \text{otherwise} \end{cases}.$$

We call such a permutation a transposition.

$$\tau_{a,b} = (ab)$$

has one cycle of length 2 and $|X| - 2$ cycles of length 1, and thus

$$\text{sgn}(\tau_{a,b}) = (-1)^{|X|-(|X|-1)} = -1.$$

Expressing permutations by transpositions

Lemma

Every permutation can be expressed as a composition of transpositions.

Proof.

Every permutation is the composition of its cycles. For a cycle, we have

$$\begin{aligned}(a_1\,a_2\ldots a_n) &= (a_1\,a_n)\circ(a_1\,a_{n-1})\circ\ldots\circ(a_1\,a_3)\circ(a_1\,a_2)\\ &= \tau_{a_1,a_n}\circ\ldots\circ\tau_{a_1,a_3}\circ\tau_{a_1 a_2}\end{aligned}$$

$\square$

Sign and transpositions

Lemma

For any permutation π and transposition $\tau_{a,b}$, the permutations π and $\pi \circ \tau_{a,b}$ have opposite signs.

Proof.

$$(ac_1c_2 \dots c_n bd_1 \dots d_m) \circ (ab) = (ad_1 \dots d_m)(bc_1c_2 \dots c_n)$$

$$(ac_1c_2 \dots c_n)(bd_1 \dots d_m) \circ (ab) = (ad_1 \dots d_m bc_1c_2 \dots c_n)$$

Hence, the number of cycles of π and $\pi \circ \tau_{a,b}$ differs by 1. $\square$

Corollary

A permutation π is even if and only if it can be expressed as a product of even number of transpositions.

Sign and operations with permutations

- $\text{sgn}(\text{id}) = 1$
- $\text{sgn}(\pi^{-1}) = \text{sgn}(\pi)$
- $\text{sgn}(\pi \circ \sigma) = \text{sgn}(\pi)\text{sgn}(\sigma)$

Application: Puzzle solvability

$\pi_0 = \mathrm{id}$

$\pi_1 = (5, 6)$

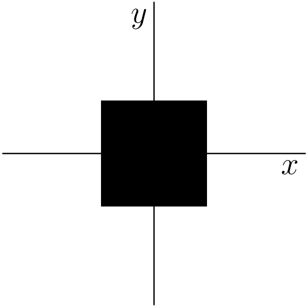
Rotation of the middle piece: $\pi \mapsto \pi \circ (1,4)(2,3)$
Shifting the numbers: $\pi \mapsto \pi \circ (1,2,3,4,\dots,18,19)$

$$\mathrm{sgn}((1,4)(2,3)) = 1 \qquad \mathrm{sgn}((1,2,3,4,\dots,18,19)) = 1$$

But $\mathrm{sgn}(\pi_0) \neq \mathrm{sgn}(\pi_1) \Rightarrow$ no solution.

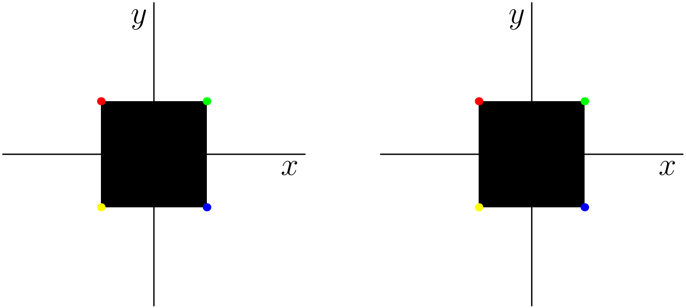
Symmetries

Consider the plane $\mathbf{R}^2$. An isometry is a function $f : \mathbf{R}^2 \to \mathbf{R}^2$ that preserves distances (rotations, translations, reflections, and their combinations). A symmetry of a set S is an isometry f such that $f(S) = S$.



Symmetries

Consider the plane $\mathbf{R}^2$. An isometry is a function $f : \mathbf{R}^2 \to \mathbf{R}^2$ that preserves distances (rotations, translations, reflections, and their combinations). A symmetry of a set S is an isometry f such that $f(S) = S$.

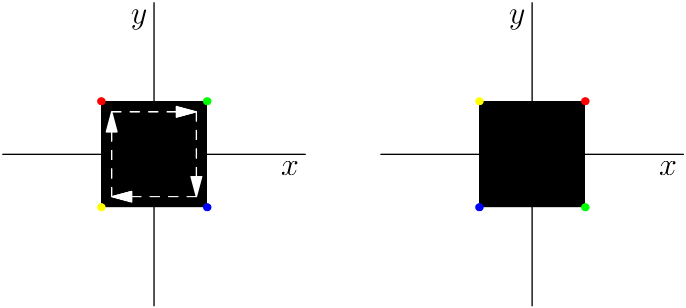


identity

$$\mathrm{id}(x, y) = (x, y)$$

Symmetries

Consider the plane $\mathbf{R}^2$. An isometry is a function $f : \mathbf{R}^2 \to \mathbf{R}^2$ that preserves distances (rotations, translations, reflections, and their combinations). A symmetry of a set S is an isometry f such that $f(S) = S$.

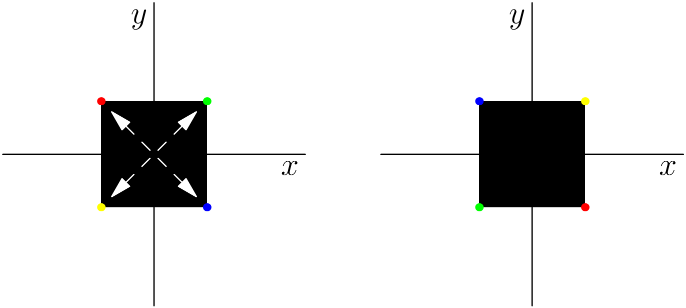


rotation by 90°

$$\mathrm{rot}_{90}(x, y) = (y, -x)$$

Symmetries

Consider the plane $\mathbf{R}^2$. An isometry is a function $f : \mathbf{R}^2 \to \mathbf{R}^2$ that preserves distances (rotations, translations, reflections, and their combinations). A symmetry of a set S is an isometry f such that $f(S) = S$.

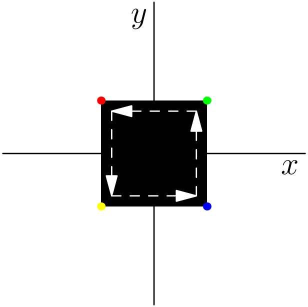


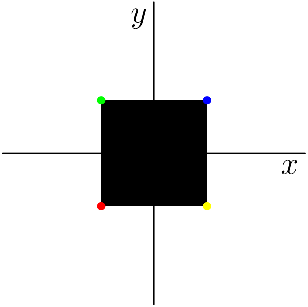
rotation by 180°

$$\mathrm{rot}_{180}(x, y) = (-x, -y)$$

Symmetries

Consider the plane $\mathbf{R}^2$. An isometry is a function $f : \mathbf{R}^2 \to \mathbf{R}^2$ that preserves distances (rotations, translations, reflections, and their combinations). A symmetry of a set S is an isometry f such that $f(S) = S$.



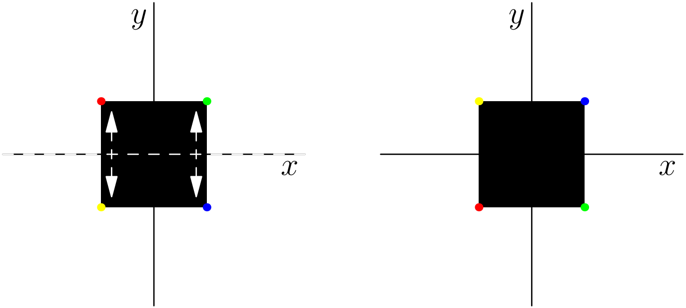


rotation by 270°

$$\mathrm{rot}_{270}(x, y) = (-y, x)$$

Symmetries

Consider the plane $\mathbf{R}^2$. An isometry is a function $f : \mathbf{R}^2 \to \mathbf{R}^2$ that preserves distances (rotations, translations, reflections, and their combinations). A symmetry of a set S is an isometry f such that $f(S) = S$.

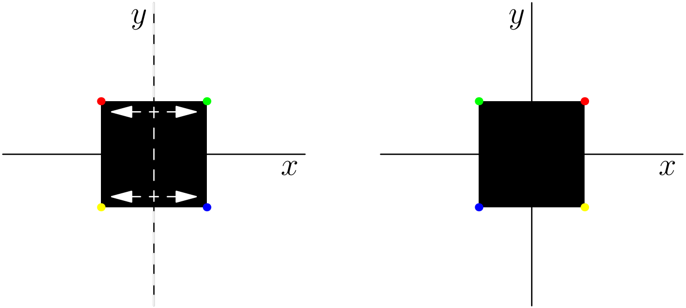


reflection by x axis

$$\mathrm{ref}_x(x, y) = (x, -y)$$

Symmetries

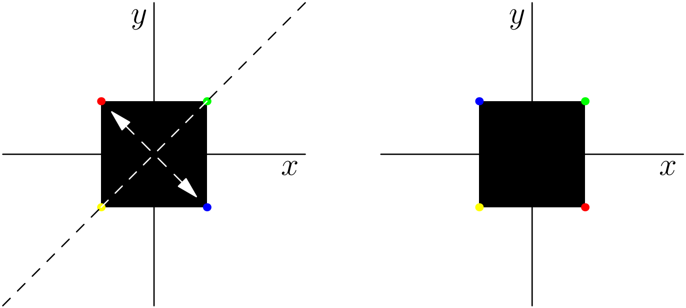
Consider the plane $\mathbf{R}^2$. An isometry is a function $f : \mathbf{R}^2 \to \mathbf{R}^2$ that preserves distances (rotations, translations, reflections, and their combinations). A symmetry of a set S is an isometry f such that $f(S) = S$.



reflection by y axis

$$\mathrm{ref}_y(x, y) = (-x, y)$$

Consider the plane $\mathbf{R}^2$. An isometry is a function $f : \mathbf{R}^2 \to \mathbf{R}^2$ that preserves distances (rotations, translations, reflections, and their combinations). A symmetry of a set S is an isometry f such that $f(S) = S$.

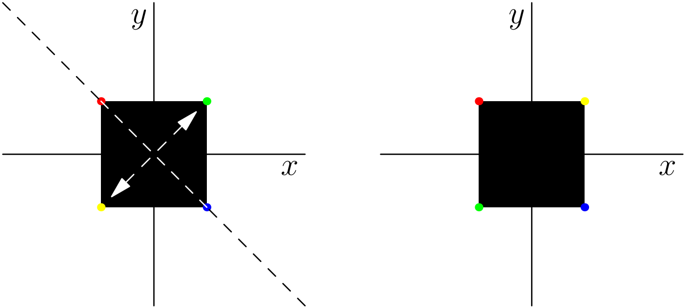


reflection by a diagonal

$$\mathrm{ref}_d(x, y) = (y, x)$$

Symmetries

Consider the plane $\mathbf{R}^2$. An isometry is a function $f : \mathbf{R}^2 \to \mathbf{R}^2$ that preserves distances (rotations, translations, reflections, and their combinations). A symmetry of a set S is an isometry f such that $f(S) = S$.



reflection by the other diagonal

$$\mathrm{ref}_o(x, y) = (-y, -x)$$

Properties of symmetries

Let f, g be symmetries of S.

- Composition of symmetries is a symmetry: $(f \circ g)(S) = f(g(S)) = f(S) = S$.
  - $\mathrm{rot}_{90} \circ \mathrm{rot}_{90} = \mathrm{rot}_{180}$, $\mathrm{rot}_{90} \circ \mathrm{ref}_x = \mathrm{ref}_o$, $\ldots$
- The inverse of a symmetry is a symmetry: $f^{-1}(S) = S$.
  - $\mathrm{rot}_{90}^{-1} = \mathrm{rot}_{270}$, $\mathrm{ref}_x^{-1} = \mathrm{ref}_x$, $\ldots$

Motivation for group theory

- What other things can we say about symmetries?
- What sets of isometries may be symmetries of a set in $\mathbf{R}^2$?
- What other mathematical objects behave in a similar way?

Definition of a monoid

Definition

A monoid is a pair $(X, \circ)$, where

- X is a set and $\circ : X \times X \to X$ is a total function,

satisfying the following axioms:

associativity	$(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in X$.
neutral element	There exists $e \in X$ s.t. $a \circ e = e \circ a = a$ for every $a \in X$.

Lemma

There exists only one neutral element.

Proof.

If $e_1 \circ a = a$ and $a \circ e_2 = a$ for all $a \in X$, then
$e_1 = e_1 \circ e_2 = e_2$. $\square$

Definition of a group

Definition

A group is a monoid $(X, \circ)$ such that

inverse for every $a \in X$ there exists $b \in X$ such that $a \circ b = b \circ a = e$.

The group is abelian if additionally

commutativity $a \circ b = b \circ a$ for all $a, b \in X$.

Lemma

For every $a \in X$, there exists only one inverse element.

Proof.

If $b_1 \circ a = e$ and $a \circ b_2 = e$, then
$b_1 = b_1 \circ e = b_1 \circ (a \circ b_2) = (b_1 \circ a) \circ b_2 = e \circ b_2 = b_2$. $\square$

Examples

Groups:

- $\mathbf{Z}$ with addition (inverse$\equiv$negation, neutral element 0)
- $\mathbf{Q}$ with addition (inverse$\equiv$negation, neutral element 0)
- $\mathbf{R}$ with addition (inverse$\equiv$negation, neutral element 0)
- $\mathbf{R} \setminus \{0\}$ with multiplication (inverse to a is $1/a$, neutral element 1)
- permutations on $\{1, \ldots, n\}$ with composition (inverse, id): non-abelian
- even permutations on $\{1, \ldots, n\}$ with composition (inverse, id): non-abelian
- regular $n \times n$ matrices with multiplication (matrix inverse, I): non-abelian
- symmetries of a set in $\mathbf{R}^2$ with composition (function inverse, id): non-abelian

Examples

The following objects are not groups:

- Set $\{-1, 0, 1\}$ with addition.
  - $1 + 1$ is not in the set.
- **Z** with subtraction
  - not associative: $(1 - 1) - 1 \neq 1 - (1 - 1)$
- positive integers with addition
  - no neutral element
- $n \times n$ matrices with multiplication
  - not all have inverse

Notation

- The binary operation: $\circ$, $+$ (for abelian groups).
- The neutral element: e, 0 (for abelian groups), 1 (for non-abelian groups).
- The inverse element to a: a^{-1}, $-a$ (for abelian groups).

Basic properties of groups

- $a \circ x = b$ has exactly one solution $x = a^{-1} \circ b$
- $x \circ a = b$ has exactly one solution $x = b \circ a^{-1}$
- $\left(a^{-1}\right)^{-1} = a$
- $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Subgroups

Definition

Let $(X, \circ)$ be a group and let Y be a subset of X. If $(Y, \circ)$ is a group, we say it is a subgroup of $(X, \circ)$.

Examples:

- $(\mathbf{Z}, +)$ is a subgroup of $(\mathbf{R}, +)$.
- even permutations form a subgroup of all permutations (with composition).
- odd permutations do not form a subgroup of all permutations (with composition).
  - composition of two odd permutations is even

Needed:

- $a \circ b \in Y$ for all $a, b \in Y$, and
- $a^{-1} \in Y$ for all $a \in Y$.

Group isomorphism

Two groups are isomorphic if they differ only by “renaming” their elements.

Definition

Let $(X, \circ)$ and $(Y, \bullet)$ be groups. A bijection $f : X \to Y$ is an isomorphism if

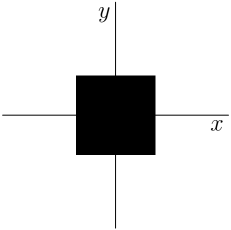
$$f(a \circ b) = f(a) \bullet f(b)$$

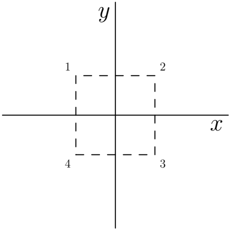
for all $a, b \in X$.

Example

Let $\mathcal{G}_1 = (\{\text{id}, \text{rot}_{90}, \text{rot}_{180}, \text{rot}_{270}, \text{ref}_x, \text{ref}_y, \text{ref}_d, \text{ref}_o\}, \circ)$ be the group of symmetries of the square.

Let
$\mathcal{G}_2 = (\{\text{id}, (1234), (13)(24), (1432), (14)(23), (12)(34), (13), (24)\}, \circ)$
be a group of permutations.





Then the following function f is an isomorphism.

x	id	rot_{90}	rot_{180}	rot_{270}
$f(x)$	id	(1234)	(13)(24)	(1432)

x	ref_x	ref_y	ref_d	ref_o
$f(x)$	(14)(23)	(12)(34)	(13)	(24)

Isomorphism properties

Let $(X, \circ)$ and $(Y, \bullet)$ be groups with neutral elements e_X and e_Y.

- If $f : X \to Y$ is an isomorphism, then $f^{-1} : Y \to X$ is an isomorphism.

$$\begin{aligned} f^{-1}[c \bullet d] &= f^{-1}\left[f(f^{-1}(c)) \bullet f(f^{-1}(d)] \right) \\ &= f^{-1}\left[f\left(f^{-1}(c) \circ f^{-1}(d) \right) \right] \\ &= f^{-1}(c) \circ f^{-1}(d) \end{aligned}$$

- $\mathrm{id} : X \to X$ is an isomorphism of $(X, \circ)$ with itself.
- If $f : X \to Y$ is an isomorphism, then
  - $f(e_X) = e_Y$
  - $f(a^{-1}) = (f(a))^{-1}$ for every $a \in X$.