Group of permutations

Definition: A *permutation* on the set $\{1, 2, \ldots, n\}$ is a bijective mapping $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

A permutation can be described by a table,

i	1	2	3
$p(i)$	1	3	2

shortly by its 2nd row $(1, 3, 2)$

by a bipartite graph

$$\begin{tikzcd} 1 \arrow[d] & 2 \arrow[dr] & 3 \arrow[dl] \\ 1 & 2 & 3 \end{tikzcd}$$

by the graph of its cycles $1 \circlearrowleft \; 2 \rightleftarrows 3$ or their list $(1)(2, 3)$

by the so called *permutation matrix* $\boldsymbol{P}$

where $(\boldsymbol{P})_{i,j} = \begin{cases} 1 & \text{when } p(i) = j \\ 0 & \text{otherwise} \end{cases}$ $\qquad \boldsymbol{P} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$

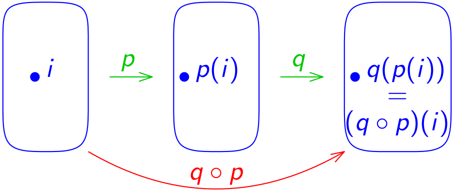
Observation: For any $\boldsymbol{A}$ and $\boldsymbol{P}$ of matching orders,
$\boldsymbol{PA}$ shuffles the rows of $\boldsymbol{A}$ according to p, while $\boldsymbol{AP}$ the columns:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 7 & 8 & 9 \\ 4 & 5 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 4 & 6 & 5 \\ 7 & 9 & 8 \end{pmatrix}$$

Group of permutations

Definition: A *permutation* on the set $\{1, 2, \dots, n\}$ is a bijective mapping $p : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$.

Observation: The set S_n of all permutations on n elements with the composition operation $\circ$ form the *symmetric group* $(S_n, \circ)$.
Notation for the composition: $(q \circ p)(i) = q(p(i))$.

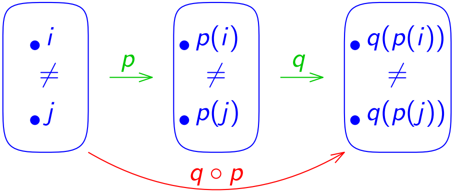


Group of permutations

Definition: A *permutation* on the set $\{1, 2, \dots, n\}$ is a bijective mapping $p : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$.

Observation: The set S_n of all permutations on n elements with the composition operation $\circ$ form the *symmetric group* $(S_n, \circ)$. Notation for the composition: $(q \circ p)(i) = q(p(i))$.

Proof: A composition of two permutations is a permutation:
$i \neq j \implies p(i) \neq p(j) \implies q(p(i)) \neq q(p(j))$ ... $q \circ p$ is injective.



Group of permutations

Definition: A *permutation* on the set $\{1, 2, \ldots, n\}$ is a bijective mapping $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Observation: The set S_n of all permutations on n elements with the composition operation $\circ$ form the *symmetric group* $(S_n, \circ)$.
Notation for the composition: $(q \circ p)(i) = q(p(i))$.

Proof: A composition of two permutations is a permutation:
$i \neq j \Longrightarrow p(i) \neq p(j) \Longrightarrow q(p(i)) \neq q(p(j))$ ... $q \circ p$ is injective.
$(\forall i\ \exists j : q(j) = i) \wedge (\forall j\ \exists k : p(k) = j) \Rightarrow (\forall i\ \exists k : q(p(k)) = i)$
... $q \circ p$ is surjective.

$$\begin{tikzcd} \bullet\, k \arrow[r, "p"] \arrow[rr, bend right, "q \circ p"'] & \bullet\, j = p(k) \arrow[r, "q"] & \bullet\, i = q(j) \end{tikzcd}$$

$$(q \circ p)(k) = q(p(k)) = q(j) = i$$

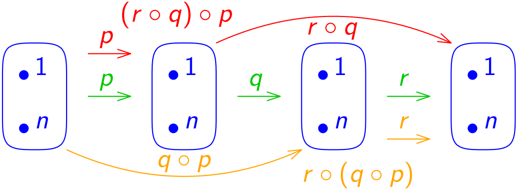
Group of permutations

Definition: A *permutation* on the set $\{1, 2, \ldots, n\}$ is a bijective mapping $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Observation: The set S_n of all permutations on n elements with the composition operation $\circ$ form the *symmetric group* $(S_n, \circ)$.
Notation for the composition: $(q \circ p)(i) = q(p(i))$.

Proof: A composition of two permutations is a permutation:
$i \neq j \implies p(i) \neq p(j) \implies q(p(i)) \neq q(p(j))$ $\quad\ldots\; q \circ p$ is injective.
$(\forall i\ \exists j : q(j) = i) \wedge (\forall j\ \exists k : p(k) = j) \Rightarrow (\forall i\ \exists k : q(p(k)) = i)$
$\ldots\; q \circ p$ is surjective.

The composition is associative: $(r \circ q) \circ p = r \circ (q \circ p)$.



$((r \circ q) \circ p)(i)$

$= r(q(p(i))) =$

$(r \circ (q \circ p))(i)$

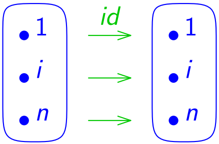
Group of permutations

Definition: A *permutation* on the set $\{1, 2, \ldots, n\}$ is a bijective mapping $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Observation: The set S_n of all permutations on n elements with the composition operation $\circ$ form the *symmetric group* $(S_n, \circ)$.
Notation for the composition: $(q \circ p)(i) = q(p(i))$.

Proof: A composition of two permutations is a permutation:
$i \neq j \Longrightarrow p(i) \neq p(j) \Longrightarrow q(p(i)) \neq q(p(j)) \quad \ldots \; q \circ p$ is injective.
$(\forall i \; \exists j : q(j) = i) \land (\forall j \; \exists k : p(k) = j) \Rightarrow (\forall i \; \exists k : q(p(k)) = i)$
$\ldots \; q \circ p$ is surjective.
The composition is associative: $(r \circ q) \circ p = r \circ (q \circ p)$.

The *identity* $id \in S_n$ given by $\forall i : id(i) = i$ is the neutral element.



Group of permutations

Definition: A *permutation* on the set $\{1, 2, \ldots, n\}$ is a bijective mapping $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

Observation: The set S_n of all permutations on n elements with the composition operation $\circ$ form the *symmetric group* $(S_n, \circ)$.
Notation for the composition: $(q \circ p)(i) = q(p(i))$.

Proof: A composition of two permutations is a permutation:
$i \neq j \Longrightarrow p(i) \neq p(j) \Longrightarrow q(p(i)) \neq q(p(j))$ ... $q \circ p$ is injective.
$(\forall i\ \exists j : q(j) = i) \wedge (\forall j\ \exists k : p(k) = j) \Rightarrow (\forall i\ \exists k : q(p(k)) = i)$
... $q \circ p$ is surjective.

The composition is associative: $(r \circ q) \circ p = r \circ (q \circ p)$.

The *identity* $id \in S_n$ given by $\forall i : id(i) = i$ is the neutral element.

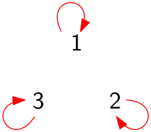
The inverse permutation is obtained by arrow reversal:
$p(i) = j \iff p^{-1}(j) = i$.

$$\bullet\, i \;\underset{p^{-1}}{\overset{p}{\rightleftarrows}}\; \bullet\, j$$

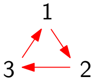
The group S_3

The ground set:

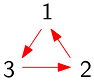
$$\{(1,2,3),(1,3,2),(3,2,1),(2,1,3),(2,3,1),(3,1,2)\} = \\ \{ \quad id \quad , \quad p_1 \quad , \quad p_2 \quad , \quad p_3 \quad , \quad r_+ \quad , \quad r_- \quad \}$$



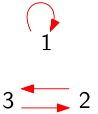
$id = (1,2,3)$



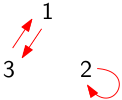
$r_+ = (2,3,1)$



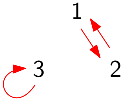
$r_- = (3,1,2)$



$p_1 = (1,3,2)$



$p_2 = (3,2,1)$



$p_3 = (2,1,3)$

The group S_3

The ground set:

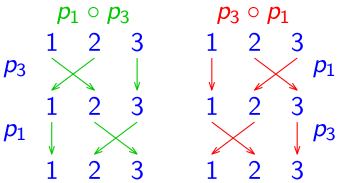
$$\{(1,2,3),(1,3,2),(3,2,1),(2,1,3),(2,3,1),(3,1,2)\} =$$
$$\{\ id,\ p_1,\ p_2,\ p_3,\ r_+,\ r_-\ \}$$

The composition operation:

$\circ$	id	p_1	p_2	p_3	r_+	r_-
id	id	p_1	p_2	p_3	r_+	r_-
p_1	p_1	id	r_+	r_-	p_2	p_3
p_2	p_2	r_-	id	r_+	p_3	p_1
p_3	p_3	r_+	r_-	id	p_1	p_2
r_+	r_+	p_3	p_1	p_2	r_-	id
r_-	r_-	p_2	p_3	p_1	id	r_+

Inverse elements:

p	id	p_1	p_2	p_3	r_+	r_-
p^{-1}	id	p_1	p_2	p_3	r_-	r_+



The composition *is not* commutative: $p_1 \circ p_3 = r_- \neq r_+ = p_3 \circ p_1$
$(1,3,2) \circ (2,1,3) = (3,1,2) \neq (2,3,1) = (2,1,3) \circ (1,3,2)$.

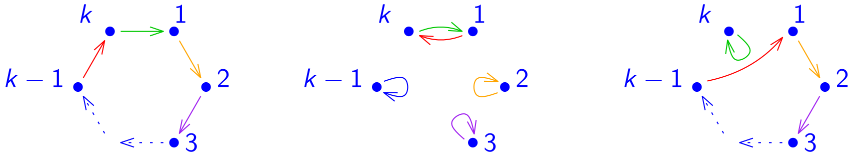
Permutation properties

Definition: A *fixed point* is $i : p(i) = i$, a trivial cycle of length 1.

Definition: A *transposition* has only one nontrivial cycle of length 2.

Observation: Any permutation can be factorized to transpositions.

Proof: A cycle $(1, \ldots, k)$ can be factorized e.g. by:
$(1, 2, \ldots, k) = (1, k) \circ (1, 2, \ldots, k-1) = (1, k) \circ (1, k-1) \circ \cdots \circ (1, 2)$



$(1, 2, \ldots, k) \quad = \quad (1, k) \quad \circ \quad (1, 2, \ldots, k-1)$

Permutation properties

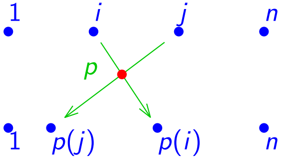
Definition: A *fixed point* is $i : p(i) = i$, a trivial cycle of length 1.

Definition: A *transposition* has only one nontrivial cycle of length 2.

Observation: Any permutation can be factorized to transpositions.

Proof: A cycle $(1, \ldots, k)$ can be factorized e.g. by:
$(1, 2, \ldots, k) = (1, k) \circ (1, 2, \ldots, k-1) = (1, k) \circ (1, k-1) \circ \cdots \circ (1, 2)$

Definition: An *inversion* of p is a pair $(i, j) : i < j$ and $p(i) > p(j)$.



Permutation properties

Definition: A *fixed point* is $i : p(i) = i$, a trivial cycle of length 1.

Definition: A *transposition* has only one nontrivial cycle of length 2.

Observation: Any permutation can be factorized to transpositions.

Proof: A cycle $(1, \ldots, k)$ can be factorized e.g. by:
$(1, 2, \ldots, k) = (1, k) \circ (1, 2, \ldots, k-1) = (1, k) \circ (1, k-1) \circ \cdots \circ (1, 2)$

Definition: An *inversion* of p is a pair $(i, j) : i < j$ and $p(i) > p(j)$.

Definition: The *sign* of a permutation p is $\mathrm{sgn}(p) = (-1)^{\#\text{inver. of } p}$.
Permutations with positive sign are *even*; with negative are *odd*.

Observation: Every transposition (i, j) has negative sign.

Permutation properties

Definition: A *fixed point* is $i : p(i) = i$, a trivial cycle of length 1.

Definition: A *transposition* has only one nontrivial cycle of length 2.

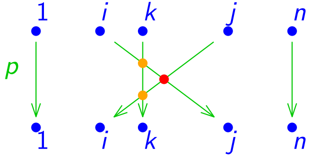
Observation: Any permutation can be factorized to transpositions.

Proof: A cycle $(1, \ldots, k)$ can be factorized e.g. by:
$(1, 2, \ldots, k) = (1, k) \circ (1, 2, \ldots, k-1) = (1, k) \circ (1, k-1) \circ \cdots \circ (1, 2)$

Definition: An *inversion* of p is a pair $(i, j) : i < j$ and $p(i) > p(j)$.

Definition: The *sign* of a permutation p is $\mathrm{sgn}(p) = (-1)^{\#\text{inver. of } p}$.
Permutations with positive sign are *even*; with negative are *odd*.

Observation: Every transposition (i, j) has negative sign.

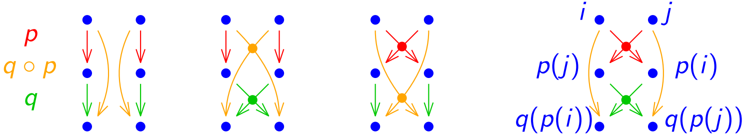


$\#$ inversions $= 2(j - i - 1) + 1$

Sign of composed permutation

Theorem: For any $p, q \in S_n : \operatorname{sgn}(q \circ p) = \operatorname{sgn}(p)\operatorname{sgn}(q)$.

Proof: #inversions of $(q \circ p) =$ #inver. of p $+$ #inver. of q $-$
$- 2|\{(i,j) : i < j \wedge p(i) > p(j) \wedge q(p(i)) < q(p(j))\}|$



an inversion of $q \circ p$ corresponds to an inversion of p or of q

inversions of p and q cancel each other

Consequences:

$\operatorname{sgn}(p^{-1}) = \operatorname{sgn}(p)$

... because $\operatorname{sgn}(p)\operatorname{sgn}(p^{-1}) = \operatorname{sgn}(p^{-1} \circ p) = \operatorname{sgn}(id) = 1$

$\operatorname{sgn}(p) = (-1)^{\#\text{transpositions of any factorization of } p \text{ into transpositions}}$

$\operatorname{sgn}(p) = (-1)^{\#\text{even cycles of } p}$

... *even* cycles decompose into *odd* number of transpositions.