Discrete Structures

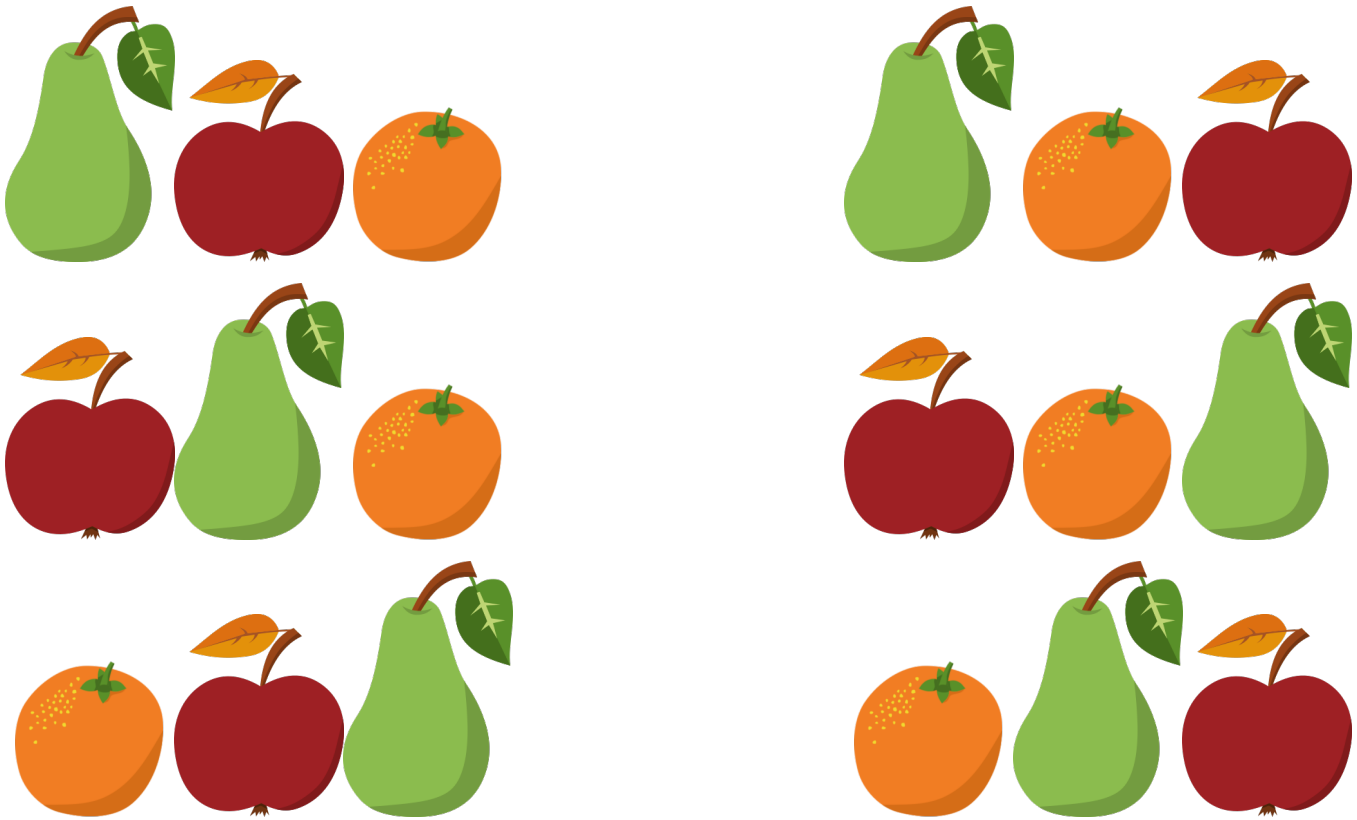
B7. Permutations

Malte Helmert, Gabriele Röger

University of Basel

October 14, 2026

Permutations



Permutation – Definition

Definition (Permutation)

Let S be a set. A bijection $\pi : S \to S$ is called a permutation of S.

Permutation – Definition

Definition (Permutation)

Let S be a set. A bijection $\pi : S \to S$ is called a permutation of S.

We will focus on permutations of finite sets.

How many permutations are there for a finite set S?

Permutations as Functions on Positions

- A permutation can be used to describe the rearrangement of objects.

Permutations as Functions on Positions

- A permutation can be used to describe the rearrangement of objects.
- Consider for example sequence o_2, o_1, o_3, o_4.

Permutations as Functions on Positions

- A permutation can be used to describe the rearrangement of objects.
- Consider for example sequence o_2, o_1, o_3, o_4.
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.

Permutations as Functions on Positions

- A permutation can be used to describe the rearrangement of objects.
- Consider for example sequence o_2, o_1, o_3, o_4.
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,

Permutations as Functions on Positions

- A permutation can be used to describe the rearrangement of objects.
- Consider for example sequence o_2, o_1, o_3, o_4.
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,
  - the one from position 3 to position 1,

Permutations as Functions on Positions

- A permutation can be used to describe the rearrangement of objects.
- Consider for example sequence o_2, o_1, o_3, o_4.
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,
  - the one from position 3 to position 1,
  - the one from position 4 to position 3 and

Permutations as Functions on Positions

- A permutation can be used to describe the rearrangement of objects.
- Consider for example sequence o_2, o_1, o_3, o_4.
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,
  - the one from position 3 to position 1,
  - the one from position 4 to position 3 and
  - the one at position 2 stayed where it was.

Permutations as Functions on Positions

- A permutation can be used to describe the rearrangement of objects.
- Consider for example sequence o_2, o_1, o_3, o_4.
- Let's rearrange the objects, e. g. to o_3, o_1, o_4, o_2.
  - The object at position 1 was moved to position 4,
  - the one from position 3 to position 1,
  - the one from position 4 to position 3 and
  - the one at position 2 stayed where it was.
- This corresponds to the permutation $\sigma = \{1 \mapsto 4, 2 \mapsto 2, 3 \mapsto 1, 4 \mapsto 3\}$.

Example I

Determine the arrangement of some objects after applying a permutation that operates on the locations.

Example I

Determine the arrangement of some objects after applying a permutation that operates on the locations.

 and π permutation of $\{1, 2, 3\}$.

Example I

Determine the arrangement of some objects after applying a permutation that operates on the locations.

 and π permutation of $\{1, 2, 3\}$.

Define $f = \{$$\mapsto 1,$$\mapsto 2,$$\mapsto 3\}$
to describe the initial configuration.

Example I

Determine the arrangement of some objects after applying a permutation that operates on the locations.

 and π permutation of $\{1, 2, 3\}$.

Define $f = \{$$\mapsto 1,$$\mapsto 2,$$\mapsto 3\}$
to describe the initial configuration.

Then $\pi \circ f$ describes the resulting configuration.

Example I

Determine the arrangement of some objects after applying a permutation that operates on the locations.

 and π permutation of $\{1, 2, 3\}$.

Define $f = \{$$\mapsto 1,$$\mapsto 2,$$\mapsto 3\}$
to describe the initial configuration.

Then $\pi \circ f$ describes the resulting configuration.

For example with $\pi = \{1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1\}$, we get
$\pi \circ f = \{$$\mapsto 2,$$\mapsto 3,$$\mapsto 1\}$, representing .

Example II

We can also consider a permutation of the fruits, describing what fruit is moved to the place of what fruit:

$\sigma = \{$🍐 $\mapsto$ 🍎, 🍎 $\mapsto$ 🍊, 🍊 $\mapsto$ 🍐$\}$

- move the pear to the position of the apple,
- the apple to the position of the orange, and
- the orange to the position of the pear.

Example II

We can also consider a permutation of the fruits, describing what fruit is moved to the place of what fruit:

$\sigma = \{$🍐 $\mapsto$ 🍎, 🍎 $\mapsto$ 🍊, 🍊 $\mapsto$ 🍐$\}$

- move the pear to the position of the apple,
- the apple to the position of the orange, and
- the orange to the position of the pear.

If g maps the locations to the initial fruits, then $\sigma^{-1} \circ g$ describes the mapping from locations to fruits after the rearrangement.

With $g = \{1 \mapsto$ 🍐, $2 \mapsto$ 🍎, $3 \mapsto$ 🍊$\}$ for arrangement 🍐🍎🍊,

we obtain $(\sigma^{-1} \circ g) = \{1 \mapsto$ 🍊, $2 \mapsto$ 🍐, $3 \mapsto$ 🍎$\}$ representing 🍊🍐🍎.

Example III

Determine the permutation of locations that leads from one configuration to the other.

Example III

Determine the permutation of locations that leads from one configuration to the other.

 $\Rightarrow$.

Example III

Determine the permutation of locations that leads from one configuration to the other.



Let $f = \{$  $\mapsto 1,$  $\mapsto 2,$  $\mapsto 3\}$ for the initial configuration

and $g = \{$  $\mapsto 2,$  $\mapsto 1,$  $\mapsto 3\}$ for the final configuration.

Example III

Determine the permutation of locations that leads from one configuration to the other.

 $\Rightarrow$.

Let $f = \{$  $\mapsto 1,$  $\mapsto 2,$  $\mapsto 3\}$ for the initial configuration

and $g = \{$  $\mapsto 2,$  $\mapsto 1,$  $\mapsto 3\}$ for the final configuration.

How can you describe the permutation of locations in terms of f and g?

Example III

Determine the permutation of locations that leads from one configuration to the other.

 $\Rightarrow$.

Let $f = \{$  $\mapsto 1,$  $\mapsto 2,$  $\mapsto 3\}$ for the initial configuration and $g = \{$  $\mapsto 2,$  $\mapsto 1,$  $\mapsto 3\}$ for the final configuration.

How can you describe the permutation of locations in terms of f and g?

$$g \circ f^{-1} = \{1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3\}$$

Two-line and One-line Notation (for Finite Sets)

Consider $\pi = \{1 \mapsto 2, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 3, 5 \mapsto 1, 6 \mapsto 6\}$.

Two-line notation lists the elements of S in the first row and the image of each element in the second row:

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

Two-line and One-line Notation (for Finite Sets)

Consider $\pi = \{1 \mapsto 2, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 3, 5 \mapsto 1, 6 \mapsto 6\}$.

Two-line notation lists the elements of S in the first row and the image of each element in the second row:

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

One-line notation only lists the second row for the natural order of the first row:

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

Composition

- Permutations of the same set can be composed with function composition.

Composition

- Permutations of the same set can be composed with function composition.
- Instead of $\sigma \circ \pi$, we write $\sigma\pi$.

Composition

- Permutations of the same set can be composed with function composition.
- Instead of $\sigma \circ \pi$, we write $\sigma\pi$.
- We call $\sigma\pi$ the product of π and σ.

Composition

- Permutations of the same set can be composed with function composition.
- Instead of $\sigma \circ \pi$, we write $\sigma\pi$.
- We call $\sigma\pi$ the product of π and σ.
- The product of permutations is a permutation. Why?

Composition

- Permutations of the same set can be composed with function composition.
- Instead of $\sigma \circ \pi$, we write $\sigma\pi$.
- We call $\sigma\pi$ the product of π and σ.
- The product of permutations is a permutation. Why?
- Example:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix} \qquad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$$

$\sigma\pi =$

$\pi\sigma =$

Inverse

Every permutation has an inverse (because it is a bijection).

- The inverse is again a permutation of the same set.
- If π is represented in two-line notation, we get π^{-1} by swapping the rows, e. g.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 2 & 4 & 1 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

- From the theorem on inverse functions in B6:

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

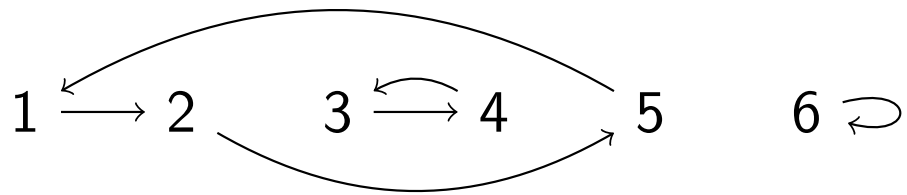
Cycle Notation – Idea

One-line notation still needs one entry per element and the effect of repeated application is hard to see.

Cycle Notation – Idea

One-line notation still needs one entry per element and the effect of repeated application is hard to see.

Consider again $\pi = \{1 \mapsto 2, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 3, 5 \mapsto 1, 6 \mapsto 6\}$.

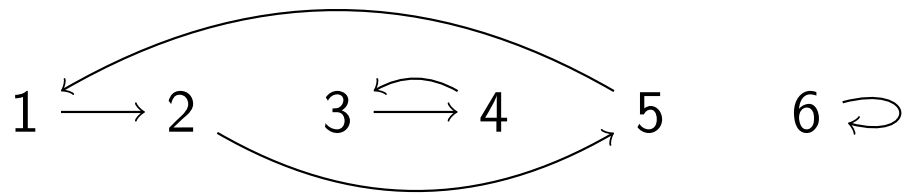


There is a cycle $(1 \quad 2 \quad 5) = (2 \quad 5 \quad 1) = (5 \quad 1 \quad 2)$ and a cycle $(3 \quad 4) = (4 \quad 3)$.

Cycle Notation – Idea

One-line notation still needs one entry per element and the effect of repeated application is hard to see.

Consider again $\pi = \{1 \mapsto 2, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 3, 5 \mapsto 1, 6 \mapsto 6\}$.



There is a cycle $(1 \quad 2 \quad 5) = (2 \quad 5 \quad 1) = (5 \quad 1 \quad 2)$ and a cycle $(3 \quad 4) = (4 \quad 3)$.

Idea: Write π as product of such cycles.

Cycles

Definition (Cycle)

A permutation σ of finite set S has a
k-cycle $(e_1 \quad e_2 \quad \ldots \quad e_k)$ if

- $e_i \in S$ for $i \in \{1, \ldots, k\}$
- $e_i \neq e_j$ for $i \neq j$
- $\sigma(e_i) = e_{i+1}$ for $i \in \{1, \ldots, k-1\}$
- $\sigma(e_k) = e_1$

- Don't confuse cycles with permutations in one-line notation.
- A 2-cycle is called a transposition.
- A 1-cycle is called a fixed point of σ.

Cyclic Permutation

Definition (Cyclic Permutation)

A permutation is cyclic if it has a single k-cycle with $k > 1$.

In cycle notation, we represent a cyclic permutation by this cycle.

Cyclic Permutation

Definition (Cyclic Permutation)

A permutation is cyclic if it has a single k-cycle with $k > 1$.

In cycle notation, we represent a cyclic permutation by this cycle.

For example:

Permutation σ of $\{1, \ldots, 5\}$ with $\sigma = (1 \quad 3 \quad 4)$ in cycle notation corresponds to

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

in two-line notation.

Cyclic Permutation

Definition (Cyclic Permutation)

A permutation is cyclic if it has a single k-cycle with $k > 1$.

In cycle notation, we represent a cyclic permutation by this cycle.

For example:
Permutation σ of $\{1, \ldots, 5\}$ with $\sigma = (1 \quad 3 \quad 4)$ in cycle notation corresponds to

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

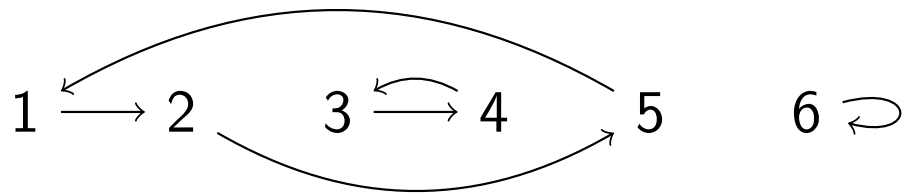
in two-line notation.

If σ is a cycle, we get σ^{-1} by reversing the order of the elements, e. g. $(1 \quad 3 \quad 4)^{-1} = (4 \quad 3 \quad 1)$.

Cycle Notation – Example

We can write every permutation of a finite set as a product of disjoint cycles.

Consider again $\pi = \{1 \mapsto 2, 2 \mapsto 5, 3 \mapsto 4, 4 \mapsto 3, 5 \mapsto 1, 6 \mapsto 6\}$.



There is a cycle $(1 \quad 2 \quad 5) = (2 \quad 5 \quad 1) = (5 \quad 1 \quad 2)$
and a cycle $(3 \quad 4) = (4 \quad 3)$.

In cycle notation:
$\pi = (1 \quad 2 \quad 5)(3 \quad 4)(6) = (1 \quad 2 \quad 5)(3 \quad 4)$

Cycle Notation – Algorithm

Let π be a permutation of finite set S.

```
 1: function ComputeCycleRepresentation(π, S)
 2:     remaining = S
 3:     cycles = ∅
 4:     while remaining is not empty do
 5:         Remove any element e from remaining.
 6:         Start a new cycle c with e.
 7:         while π(e) ∈ remaining do
 8:             remaining = remaining \ {π(e)}
 9:             Extend c with π(e).
10:             e = π(e)
11:         cycles = cycles ∪ {c}
12:     return cycles
```

The elements of *cycles* can be arranged in any order.

Cycle Notation – Algorithm

Let π be a permutation of finite set S.

1: **function** ComputeCycleRepresentation(π, S)
2: *remaining* $= S$
3: *cycles* $= \emptyset$
4: **while** *remaining* is not empty **do**
5: Remove any element e from *remaining*.
6: Start a new cycle c with e.
7: **while** $\pi(e) \in$ *remaining* **do**
8: *remaining* $=$ *remaining* $\setminus \{\pi(e)\}$
9: Extend c with $\pi(e)$.
10: $e = \pi(e)$
11: *cycles* $=$ *cycles* $\cup \{c\}$
12: **return** *cycles*

The elements of *cycles* can be arranged in any order. $\rightsquigarrow$ Why?

Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \dots \quad e_n)$ *and* $\pi' = (e'_1 \quad \dots \quad e'_m)$ *be permutations of set* S *in cycle notation and let* π *and* π' *be disjoint, i. e.* $e_i \neq e'_j$ *for* $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \dots \quad e_n)$ *and* $\pi' = (e'_1 \quad \dots \quad e'_m)$ *be permutations of set* S *in cycle notation and let* π *and* π' *be disjoint, i. e.* $e_i \neq e'_j$ *for* $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Proof.

Consider an arbitrary element $e \in S$. We distinguish three cases:



Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \dots \quad e_n)$ *and* $\pi' = (e'_1 \quad \dots \quad e'_m)$ *be permutations of set* S *in cycle notation and let* π *and* π' *be disjoint, i. e.* $e_i \neq e'_j$ *for* $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Proof.

Consider an arbitrary element $e \in S$. We distinguish three cases:

If $e = e_i$ for some $i \in \{1, \dots, n\}$ then $\pi(e) = e_j$ for some $j \in \{1, \dots, n\}$. Since the cycles are disjoint, $\pi'(e) = e$ and $\pi'(\pi(e)) = \pi(e)$. Together, this gives $\pi'(\pi(e)) = \pi(\pi'(e))$.



Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \dots \quad e_n)$ *and* $\pi' = (e'_1 \quad \dots \quad e'_m)$ *be permutations of set* S *in cycle notation and let* π *and* π' *be disjoint, i. e.* $e_i \neq e'_j$ *for* $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Proof.

Consider an arbitrary element $e \in S$. We distinguish three cases:

If $e = e_i$ for some $i \in \{1, \dots, n\}$ then $\pi(e) = e_j$ for some $j \in \{1, \dots, n\}$. Since the cycles are disjoint, $\pi'(e) = e$ and $\pi'(\pi(e)) = \pi(e)$. Together, this gives $\pi'(\pi(e)) = \pi(\pi'(e))$.

If $e = e'_i$ for some $i \in \{1, \dots, m\}$, we can use the analogous argument to show that $\pi(\pi'(e)) = \pi'(\pi(e))$.

□

Disjoint Cycles Commute

Theorem

Let $\pi = (e_1 \quad \dots \quad e_n)$ *and* $\pi' = (e'_1 \quad \dots \quad e'_m)$ *be permutations of set* S *in cycle notation and let* π *and* π' *be disjoint, i. e.* $e_i \neq e'_j$ *for* $i \in \{1, \dots, n\}, j \in \{1, \dots, m\}$.

Then $\pi\pi' = \pi'\pi$.

Proof.

Consider an arbitrary element $e \in S$. We distinguish three cases:

If $e = e_i$ for some $i \in \{1, \dots, n\}$ then $\pi(e) = e_j$ for some $j \in \{1, \dots, n\}$. Since the cycles are disjoint, $\pi'(e) = e$ and $\pi'(\pi(e)) = \pi(e)$. Together, this gives $\pi'(\pi(e)) = \pi(\pi'(e))$.

If $e = e'_i$ for some $i \in \{1, \dots, m\}$, we can use the analogous argument to show that $\pi(\pi'(e)) = \pi'(\pi(e))$.

If e occurs in neither cycle then $\pi(e) = e$ and $\pi'(e) = e$, so $\pi'(\pi(e)) = e = \pi(\pi'(e))$. □

In General, Cycles Do Not Commute

Consider cycles $(1 \quad 2)$ and $(2 \quad 3)$ and set $S = \{1, 2, 3\}$.

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

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

Example

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

$\sigma\pi^{-1} =$

Transpositions

Reminder: A 2-cycle is called a transposition.

Theorem

Every permutation of a finite set can be expressed as a finite product of transpositions, where the empty product represents the identity.

Proof idea.

Consider an arbitrary k-cycle $\sigma = (e_1 \quad \dots \quad e_k)$ with $k > 1$.
We can express σ as $(e_1 \quad e_k)(e_1 \quad e_{k-1}) \dots (e_1 \quad e_2)$.
The theorem follows because every permutation of a finite set can be written as a (finite) product of cycles and each of these cycles can be expressed as a product of transpositions. □

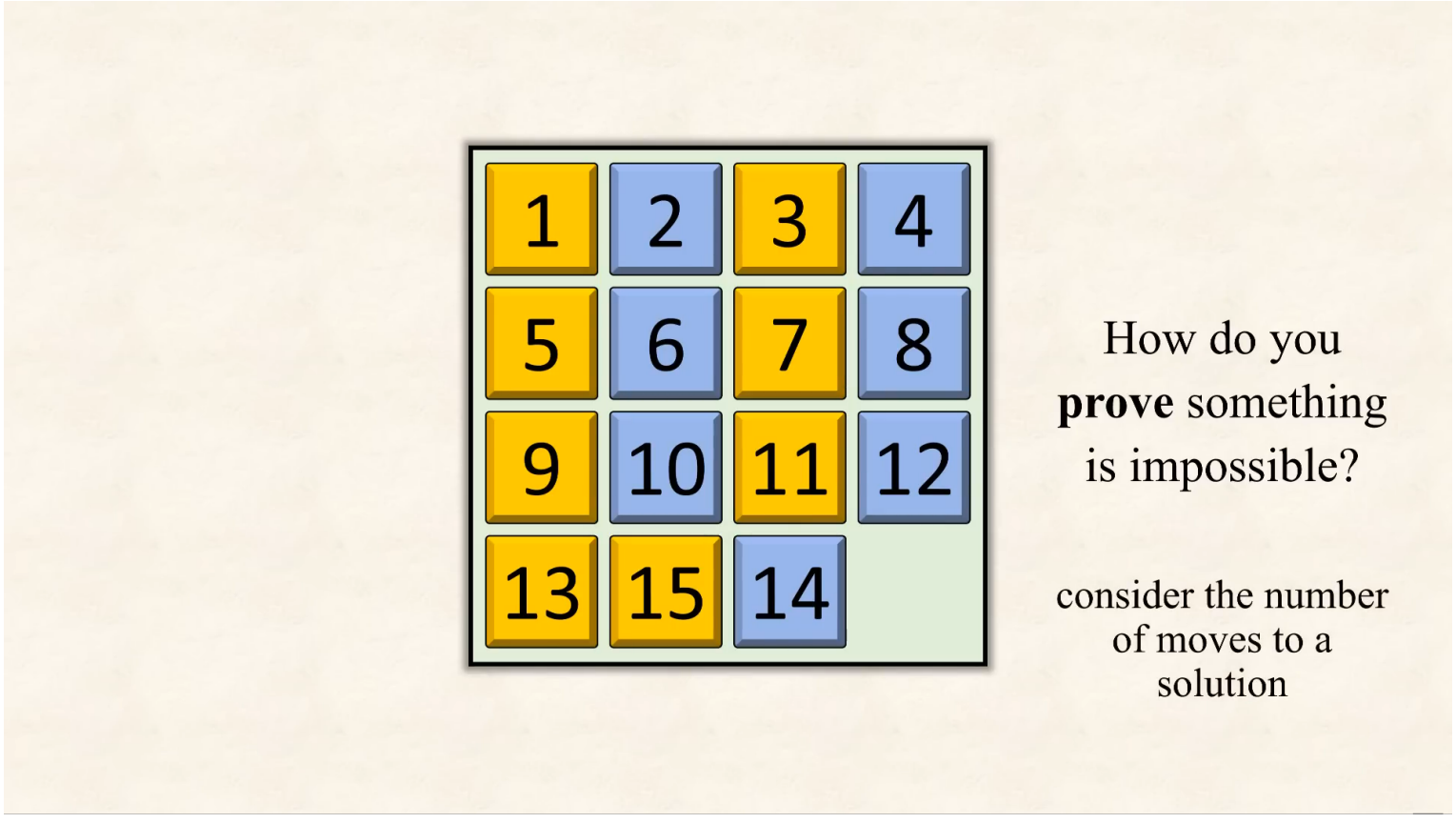
Parity of Permutations

Definition (Parity)

Let π be a permutation of a finite set.
Let $\tau_1, \ldots, \tau_k$ be transpositions so that $\pi = \tau_k \tau_{k-1} \cdots \tau_1$.
Then π is even if k is even, and odd if k is odd.

Well-defined: If a permutation has two decompositions $\sigma = \tau_k \tau_{k-1} \cdots \tau_1 = \rho_m \rho_{m-1} \cdots \rho_1$ into transpositions, then k and m are either both odd or both even.

Application: Unsolvability of 15-Puzzle Configuration



`https://www.youtube.com/watch?v=p6kCYbKIMak`

[only first 8 minutes in lecture, but the rest is also interesting]

Summary

- A permutation is a bijection from a set to itself.
- A permutation of a finite set can be written in two-line notation, one-line notation or in cycle notation.
- Disjoint cycles commute, so their order in the cycle notation does not matter.
- A cycle of length 2 is a transposition.
- Every permutation of a finite set is a finite (non-unique) product of transpositions. The permutation is even if the number of transpositions is even, otherwise it is odd.