Permutations : Preliminary Definition

A permutation of a list of objects is a rearrangement of these objects.

Ex:

Ex:

1	2	3	4	5	6	7	8

In general, the number of permutations of n distinct objects is $n(n-1)(n-2)\cdots 2\cdot 1 = n!$

Ex: How many ways can the tiles on the 15 puzzle be arranged?

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Permutations : Mathematical Definition

Definition 3.2.3 A **permutation** of a set A is a function $\alpha : A \to A$ that is bijective (i.e. both one-to-one and onto).

Function refresher :

Definition 3.2.1 A **function**, or **mapping**, f from a (nonempty) set A to a (nonempty) set B is a rule that associates each element $a \in A$ to exactly one element $b \in B$.

Definition 3.2.2 A function $f : A \to B$ is called **one-to-one**, or **injective**, if no two elements of A have the same image in B.

A function $f : A \to B$ is called **onto**, or **surjective**, if $f(A) = B$. That is, if each element of B is the image of at least one element of A.

A function that is both injective and surjective is called **bijective** .

We will focus on permutations of the set

$$[n] = \{1, 2, \dots, n\}$$

for various n.

To represent a permutation $\alpha : [n] \to [n]$ we just need to list where each number gets mapped to.

Ex:

Array form: $\alpha = \begin{pmatrix} & \end{pmatrix} = \begin{pmatrix} & \\ & \end{pmatrix}$ ← input ← output

$\beta = \begin{pmatrix} & \end{pmatrix} = \begin{pmatrix} & \\ & \end{pmatrix}$ ← input ← output

Arrow form:

α: 1 2 3 ← input; 1 2 3 ← output

β: 1 2 3 4 5 ← input; 1 2 3 4 5 ← output cycle-arrow form & cycle form : We'll see this in chapter 4.

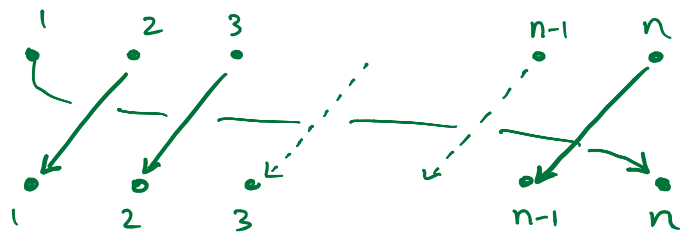
Ex : (a) the identity or "do nothing" permutation is denoted by $\varepsilon : [n] \to [n]$ and it maps every element to itself

$$\varepsilon = \left(\qquad\qquad\qquad \right)$$

(b) An n-cycle cyclically permutes the values. For example,

$$\left(\qquad\qquad\qquad \right)$$

or we could use the arrow diagram



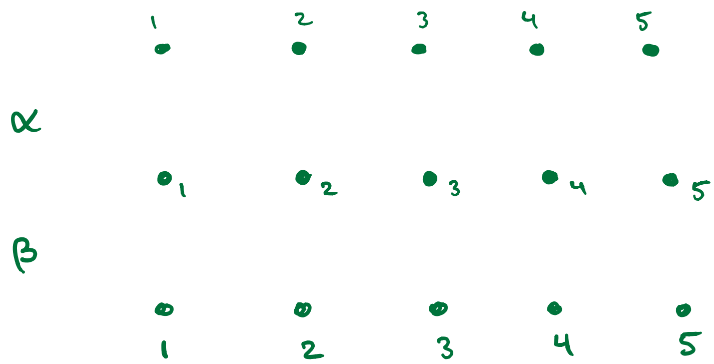
Composition :

Since permutations are functions we can combine two or more together using function composition.

Ex : Consider $\alpha, \beta : [5] \to [5]$ given by

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$$

Stack the arrow diagram for α on top of β :



This gives a new permutation $\alpha\beta$ which is the function obtained by first applying α then applying β.

We can compute this directly from array form:

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

Notice we are moving from left to right.

Definition 3.3.1 Let $\alpha, \beta : [n] \to [n]$ be two permutations. The **permutation composition**, or **product**, of α and β is denoted by $\alpha\beta : [n] \to [n]$ is the permutation defined by:

$$\begin{array}{rccccc} \alpha\beta : & [n] & \to & [n] & \to & [n] \\ & k & \longmapsto & \alpha(k) & \longmapsto & \beta(\alpha(k)) \end{array}$$

This means $(\alpha\beta)(k) =$

Important: Composition is done left-to-right which is opposite the usual convention.

Ex: Let $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix}$, $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$

(a) Compute $\alpha(\beta\gamma)$

$\alpha(\beta\gamma) =$

$=$

$=$

(b) Compute $(\alpha\beta)\gamma$

$$(\alpha\beta)\gamma =$$

In general, $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ for permutations. This is called the associative property of permutation composition. It means we can unambiguously write

$$\alpha\beta\gamma$$

For example, cube move sequence

$$RUL^{-1}URD$$

doesn't need grouping brackets.

(c) Compute $\alpha\gamma$

$$\alpha\gamma =$$

(d) The product of α with itself n times is

$$\alpha^n = \underbrace{\alpha \cdot \alpha \cdot \ \cdots \cdot \alpha}_{n \text{ times}}$$

$\alpha^2 =$

$\alpha^3 =$

$\alpha^4 =$

$\alpha^5 =$

$\alpha^6 =$

(e) Find $\alpha\beta$ and $\beta\alpha$. What do you notice?

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

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

If $\sigma\gamma = \gamma\sigma$ for permutations we say σ and γ <u>commute</u>. In general permutation composition is not necessarily commutative.

Inverses:

Given a permutation α can we find a permutation β such that

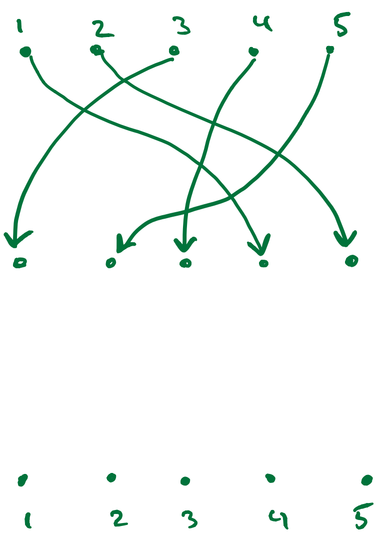
$$\alpha\beta = \beta\alpha = \varepsilon \ ?$$

Answer :

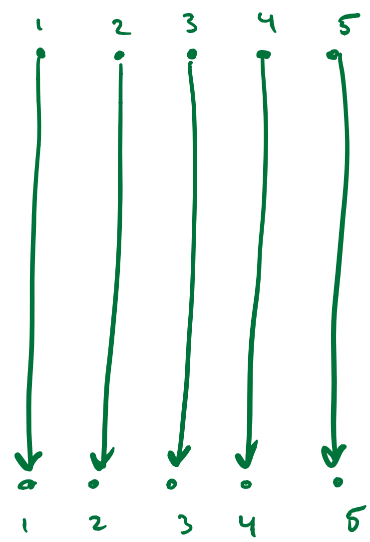
Ex: Consider $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}$

$$\underset{\alpha}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix}}\underset{\beta}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ & & & & \end{pmatrix}} = \underset{\varepsilon}{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}}$$

Visually:



$\Rightarrow \varepsilon$



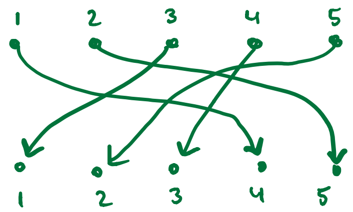
Theorem 3.5.1 For any permutation $\alpha : [n] \to [n]$, there exists a unique permutation $\beta : [n] \to [n]$ such that $\alpha\beta = \beta\alpha = \varepsilon$.

We call β the inverse of α and write $\beta = \alpha^{-1}$

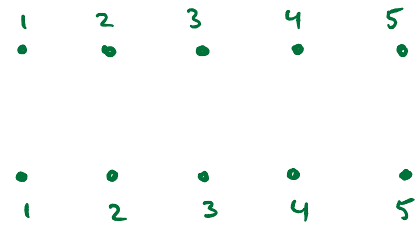
To find an inverse we can either

(1) in arrow form, reverse the arrows (flip the diagram)

α



α^{-1}



(2) in array form, flip the array upside down

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

Ex: Find the inverse of $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 2 & 8 & 1 & 4 & 6 & 5 \end{pmatrix}$

$$\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ & & & & & & & \end{pmatrix}$$

check: $\beta\beta^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 2 & 8 & 1 & 4 & 6 & 5 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ & & & & & & & \end{pmatrix}$

Inverse of products: $(\alpha\beta)^{-1} = \beta^{-1}\alpha^{-1}$ (notice order is reversed)

Check:

In general, $(\alpha_1\alpha_2\cdots\alpha_k)^{-1} = \alpha_k^{-1}\alpha_{k-1}^{-1}\cdots\alpha_2^{-1}\alpha_1^{-1}$

Cancellation property :

(left cancellation) $\alpha\beta = \alpha\gamma \Rightarrow \beta = \gamma$

(right cancellation) $\beta\alpha = \gamma\alpha \Rightarrow \beta = \gamma$

Proof (of left) :

Ex: Are the two move sequences of Rubik's cube equivalent (i.e. they put the cube in the same position)?

RUF^{-1}, R^3F^3

Symmetric Group :

$S_n = \{\alpha \mid \alpha$ is a permutation of $[n]\}$ is called the Symmetric Group

Let's summarize what we know so far about S_n.

- S_n, the symmetric group of degree n, is the set of all permutation of $[n] = \{1, 2, \dots, n\}$.
- $|S_n| = n!$
- Two elements $\alpha, \beta \in S_n$ can be composed (multiplied) to give another element $\alpha\beta \in S_n$.[2]
- The *identity* permutation is $\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$. It has the property that $\varepsilon\alpha = \varepsilon\alpha = \alpha$ for all $\alpha \in S_n$.
- Every $\alpha \in S_n$ has an inverse denoted by α^{-1}. The defining property of an inverse is $\alpha\alpha^{-1} = \alpha^{-1}\alpha = \varepsilon$.
- $(\alpha_1\alpha_2\cdots\alpha_k)^{-1} = \alpha_k^{-1}\cdots\alpha_2^{-1}\alpha_1^{-1}$.
- Permutation composition (multiplication) is associative: $\alpha(\beta\gamma) = (\alpha\beta)\gamma$.
- Permutation composition (multiplication) is not necessarily commutative.
- Cancellation Property: $\alpha\beta = \alpha\gamma$ implies $\beta = \gamma$, and $\beta\alpha = \gamma\alpha$ implies $\beta = \gamma$.

Example: Show that $\alpha\beta\alpha^{-1} = \beta$ if and only if α and β commute.

Proof:

Order of a permutation:

The smallest number m for which $\alpha^m = \varepsilon$ is called the order of α, which we denote by $\text{ord}(\alpha)$.

Ex: Find the order of $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$

Must such a number exist?

Theorem 3.8.1 For any $\alpha \in S_n$ there exists a positive number m for which $\alpha^m = \varepsilon$. The smallest such m is the **order** of α, denoted $\text{ord}(\alpha)$.

Ex: If α has order 7, what is α^{35} ?

Ex: For $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, does $\beta^{62} = \varepsilon$?

Theorem 3.8.2 Let α be a permutation. If $\alpha^m = \varepsilon$ then $\text{ord}(\alpha)$ divides m.