Permutations and the Symmetric Group

Let X be a set. A *permutation* of X is a bijection ($\iff$ one-to-one and onto mapping)

$$\alpha : X \longrightarrow X.$$

We will focus on the case $\boxed{X = \{1, 2, 3, \ldots, n\}}$.

Let S_n be the set of all permutations of X.

This set has a binary operation given by *composition*:

$$\alpha\beta := \alpha \circ \beta$$

$$\begin{tikzcd} X \arrow[r, "\beta"] \arrow[rr, bend right, "\alpha\circ\beta"'] & X \arrow[r, "\alpha"] & X \end{tikzcd}$$

where $(\alpha\circ\beta)(x) = \alpha(\beta(x))$

- Associative:

$$\begin{aligned} ((\alpha\beta)\gamma)(x) &= ((\alpha\beta)\circ\gamma)(x) \\ &= (\alpha\beta)(\gamma(x)) \\ &= (\alpha\circ\beta)(\gamma(x)) \\ &= \alpha(\beta(\gamma(x))) \\ &= \alpha((\beta\circ\gamma)(x)) \\ &= (\alpha\circ(\beta\gamma))(x) \\ &= (\alpha(\beta\gamma))(x) \end{aligned}$$

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

- Identity element

$$e : X \longrightarrow X, \quad k \longmapsto k$$

- Inverses: $\alpha : X \longrightarrow X$ bijective

$$\Rightarrow \exists\ \alpha^{-1} : X \to X \text{ s.t. } \alpha\alpha^{-1} = e, \ \alpha^{-1}\alpha = e.$$

So S_n is a group, called the **symmetric group**

Remark: Number of elements in S_n is

$$|S_n| = n \cdot (n-1) \cdot \cdots \cdot 3 \cdot 2 \cdot 1 = n!$$

Grows very fast with n:

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n \qquad \text{(Stirling's Formula)}$$

Examples: $|S_2| = 2$, $|S_3| = 6$, $|S_4| = 24$, $|S_5| = 120$,

$$|S_{230}| \sim 10^{400}.$$

Two-Row Notation $\qquad X = \{1, 2, \ldots, n\}$

We write $\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$

to mean: $\alpha : X \longrightarrow X$ is the map sending 1 to i_1, 2 to i_2, etc., n to i_n

In this notation, the identity is

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Example Let $n = 3$.

Let $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\quad \beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$.

Then $\alpha^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $\quad \beta^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ $(= \beta)$.

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

[do β first, then α!]

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

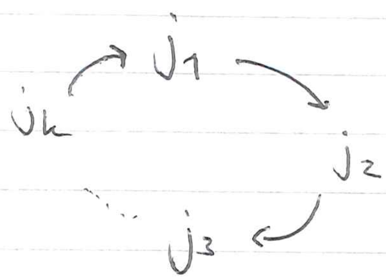
So in S_n, order matters when multiplying permutations!

"S_n is not commutative".

Cycle Notation

We write $\alpha = (j_1 \, j_2 \cdots j_k)$ to mean:

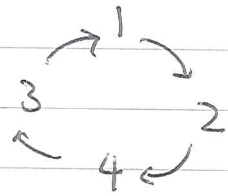
α sends j_1 to j_2
j_2 to j_3
$\vdots$
j_{k-1} to j_k
j_k to j_1



k-cycle

Example: $(1\ 2\ 4\ 3)$ ← cycle notation

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$ ← two-row notation.



4-cycle

Note: $(1\ 2\ 4\ 3) = (2\ 4\ 3\ 1) = (4\ 3\ 1\ 2) = (3\ 1\ 2\ 4)$.

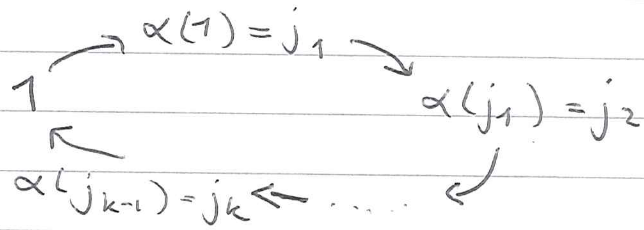
Usually write with smallest entry first, so $(1\ 2\ 4\ 3)$.

Proposition (Examinable)

Any permutation can be written as a product of disjoint cycles. ← Disjoint: no number appears in more than 1 cycle.

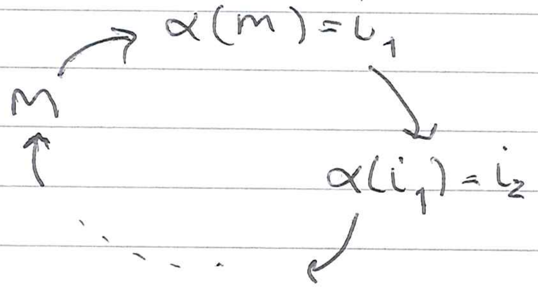
Proof: Let $\alpha \in S_n$ be a permutation.

Consider the cycle



So we get a cycle $(1\ j_1\ \cdots\ j_k)$

Now take the smallest number $m \in \{1, \ldots, n\}$ which is not in this cycle, and repeat:



$\Rightarrow$ Get another cycle $(m\ i_1\ \cdots\ i_\ell)$.

Repeat this process until each number in $\{1, \ldots, n\}$ has appeared in a cycle.

Then $\alpha = (1\ j_1 \cdots j_k)(m\ i_1 \cdots i_l) \cdots$ ∎

Example: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 7 & 1 & 2 & 6 & 3 \end{pmatrix}$

$$= (1\ 5\ 2\ 4)(3\ 7)(6)$$

Remarks: 1) Disjoint cycles commute, so can swap order! we could write this as $(3\ 7)(1\ 5\ 2\ 4)(6)$ also.

2) Usually we "drop" 1-cycles (and use convention that any number not appearing is sent to itself by our permutation. So could write the above as $(1\ 5\ 2\ 4)(3\ 7)$.

or $(3\ 7)(1\ 5\ 2\ 4)$.

Transpositions and Sign

A Transposition just means a 2-cycle $(i\ j)$ – swaps 2 elements i and j, leaves others fixed.

Proposition (Examinable)

Any permutation can be written as a product of transpositions.

Proof: Since any transposition is a product of cycles, it's enough to show any cycle is a product of transpositions. Now:

$$\underbrace{(i_1 \cdots i_k)}_{\text{cycle of length } k} = \underbrace{(i_1\ i_k)(i_1\ i_{k-1}) \cdots (i_1\ i_2)}_{\text{product of } k-1 \text{ transpositions.}} \leftarrow \text{Check!}$$

$(i_1\ i_3)$

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

$$= (2\ 4\ 3\ 5)$$

$$= (2\ 5)(2\ 3)(2\ 4)$$

Remark: Can do this in multiple ways: e.g.

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

Now let $\alpha \in S_n$ and write α as a product of transpositions:

$$(*) \quad \alpha = \tau_1 \cdots \tau_k \qquad (\underbrace{\tau_i = (k_i j_i)}_{\text{transposition}})$$

Then we define the sign of α to be

$$\operatorname{sign}(\alpha) = (-1)^k$$

where k is the number of transpositions in $(*)$

Proposition: The sign of α depends only on α, not on its representation as a product of transpositions.

Example:

a) $\underbrace{(12)}_{1 \text{ transposition}} = \underbrace{(12)(13)(13)}_{3 \text{ transpositions}}$

So $\operatorname{sign}(12) = (-1)^1 = (-1)^3 = -1$.

b) $(i_1 \cdots i_k) = \underbrace{(i_1 i_k) \cdots (i_1 i_2)}_{k-1}$

so $\operatorname{sign}(i_1 \cdots i_k) = (-1)^{k-1}$.

If $\operatorname{sign}(\alpha) = 1$ we say α is even;
if $\operatorname{sign}(\alpha) = -1$ we say α is odd.