$S_3 \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \quad (1\ 2)$

$S_5 \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 4 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 5 \\ 5 & 1 \end{pmatrix} \quad (1\ 5)$

$(1\ 2)$

$$\tau : \begin{aligned} 1 &\longmapsto 2 \\ 2 &\longmapsto 1 \\ x &\longmapsto x \quad \text{si } x \neq 1, 2. \end{aligned}$$

$$\tau^{-1} : \begin{aligned} 2 &\longmapsto 1 \\ 1 &\longmapsto 2 \\ x &\longmapsto x \quad \text{si } x \neq 1, 2 \end{aligned}$$

$\tau^{-1} = (2\ 1) = (1\ 2) \qquad \tau^{-1} = \tau$ <u>idempotente</u>

preuve : récurrence sur n.

Si $n=2$: $S_2=\{id, (1,2)\}$

$(1,2)$ est une transposition : elle est la composée de $\underline{1}$ transposition.

$id=(1\ 2)\circ(1\ 2)$

Donc la propriété est vraie au rang 2.

Hérédité : On suppose la propriété vraie au rang n.

$[\![1, n+1]\!]$ Soit $\gamma \in S_{n+1}$

si $\gamma(n+1) = n+1$

$$\gamma = \begin{pmatrix} 1 & 2 & \cdots & n & n+1 \\ a_1 & a_2 & & a_n & n+1 \end{pmatrix} = \begin{pmatrix} 1 & & n \\ a_1 & & a_n \end{pmatrix}$$

On peut considérer que $\gamma \in S_n$

Par hypothèse de récurrence :

$\gamma = \tau_1 \circ \quad \circ \tau_r$ $\quad \tau_i \in S_n$

τ_i transposition

On peut considérer que $\tau_i \in S_{n+1}$

et donc γ se décompose en un

produit de transpositions.

Si $\gamma(n+1) = p \leq n$

On pose $\tau = (p \;\; n+1)$

$\tau \circ \gamma(n+1) = \tau(p) = n+1$

et $\tau \circ \gamma \in S_{n+1}$:
D'après le cas $\gamma(n+1) = n+1$, on en déduit qu'il existe des transpositions $\tau_1 \dots \tau_r$ telles que $\tau \circ \tau \circ \gamma = \tau \circ \tau_1 \circ \dots \circ \tau_r$.

On compose à gauche par τ:

$$\gamma = id \circ \gamma = \tau \circ \tau_1 \circ \dots \circ \tau_r$$

La récurrence est terminée.

$$(1\ 5) \circ (3\ 5) \circ (1\ 2) \circ (4\ 6) \circ (1\ 2)$$

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

$$= (1\ 5) \circ (3\ 5) \circ id \circ (4\ 6)$$

$$= (1\ 5) \circ (3\ 5) \circ (4\ 6) = \underline{\sigma_3}$$

$$= (1\ 6) \circ (1\ 6) \circ (1\ 5) \circ (3\ 5) \circ (4\ 6)$$

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

$$\sigma_3 = (4\ 6) \circ (1\ 3) \circ (1\ 5)$$

$$\sigma_3^{-1} = (1\ 5) \circ (1\ 3) \circ (4\ 6)$$

$$\underbrace{(4\ 6) \circ \underbrace{(1\ 3) \circ \underbrace{(1\ 5) \circ (1\ 5)}_{id} \circ (1\ 3)}_{id} \circ (4\ 6)}_{id}$$

$$= id$$

$$\sigma_3^{-1} = (1\ 5) \circ (1\ 3) \circ (4\ 6)$$

$$
\begin{tikzcd}
a_1 \arrow[r, mapsto] & a_2 \arrow[r, mapsto] & a_3 \arrow[r, mapsto] & \cdots \arrow[r, mapsto] & a_p \arrow[llll, bend left, mapsto]
\end{tikzcd}
$$

$$
\begin{pmatrix} a_1 & a_2 & & a_{p-1} & a_p \\ a_2 & a_3 & & a_p & a_1 \end{pmatrix} \quad p\text{-cycle.}
$$

$$
(a_1 \ \ a_2) \qquad
\begin{tikzcd}
a_1 \arrow[r, mapsto] & a_2 \arrow[l, bend left, mapsto]
\end{tikzcd}
$$

une transposition est un 2-cycle.

un cycle

$$\gamma^{k} \circ \gamma^{k'} = \underbrace{\gamma \circ \quad \circ \gamma}_{k} \circ \underbrace{\gamma \circ \quad \circ \gamma}_{k'} \quad k \in \mathbb{N}$$

$$= \gamma^{k+k'}$$

$$\gamma^{k} \circ \gamma^{-k} = \underbrace{\gamma \circ \quad \circ \gamma}_{k} \circ \underbrace{\gamma^{-1} \circ \quad \circ \gamma^{-1}}_{k} = id.$$

$$= \gamma^{k-k} = \gamma^{0}$$

$$\forall k, k' \in \mathbb{Z} \quad \gamma^{k} \circ \gamma^{k'} = \gamma^{(k+k')}.$$

$(a_1 \quad a_2 \qquad\qquad a_p)$

$\forall k \in [\![\overset{1}{\cancel{2}}, p]\!] \qquad a_k = \gamma^{k-1}(a_1)$.

<u>Initialisation</u>

$k = 1$ vrai $\qquad a_1 = id(a_1)$.

$k = 2 \qquad a_2 = \gamma(a_1)$.

<u>Hérédité</u>

Si $a_k = \gamma^{k-1}(a_1) \qquad k \le p-1$

$$a_{k+1} = \gamma(a_k) = \gamma(\gamma^{k-1}(a_1))$$
$$= \gamma^{k}(a_1).$$

Donc par récurrence, la proposition est vraie.

x tq $\sigma(x) \neq x$.

$\{x, \sigma(x), \sigma^2(x), \sigma^3(x), \dots, \sigma^h(x), \dots, h \in \mathbb{N}\}$

$\sigma : [\![1, n]\!] \longrightarrow [\![1, n]\!]$.

cet ensemble a au plus n éléments.

car inclus dans $[\![1, n]\!]$.

$\Longrightarrow \exists\, i, j \in \mathbb{N}$ tq $\sigma^i(x) = \sigma^j(x)$.

$i < j$

$\sigma^{-i} \circ \sigma^i(x) = \underline{x} = \sigma^{-i}(\sigma^j(x)) = \underline{\sigma^{j-i}(x)}$

$j - i > 0$.

Donc il existe p tel que $\gamma^p(x) = x$.

??? ⚠ $\Longrightarrow$ $(x \quad \gamma(x) \quad \gamma^2(x) \quad \gamma^{p-1}(x))$

est p-cycle.

Danger : on ne sait pas si

$x, \gamma(x), \dots, \gamma^{p-1}(x)$ sont deux à

deux distincts

Exemple $\gamma = (1\,2)$ $\quad \gamma^4(x) = x \quad \forall x \in [\![1,2]\!]$.

2 cycles.

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

$= (1, \gamma(1), \gamma^2(1), \gamma^3(1)) \quad \gamma^4(1) = 1$.

On sait que :

$\{p \in \mathbb{N}^* \text{ tq } \gamma^p(x) = x\} \neq \emptyset$.

$\subset \mathbb{N}^*$.

On va prendre le plus petit p dans l'ensemble :

$\{x, \gamma^1(x), \dots, \gamma^{p-1}(x)\}$ possède p éléments : supposons $\gamma^i(x) = \gamma^j(x)$

avec $i, j \leq p-1$ et $i < j \Rightarrow \gamma^{j-i}(x) = x$

$j \leq p-1$ et $i \geq 0$ $\quad$ $j - i \leq p-1$ IMPOSSIBLE

CONTRADICTION

Donc $x, \gamma(x), \dots, \gamma^{p-1}(x)$ sont deux à deux distincts.

et alors $\gamma = (x, \quad , \gamma^{p-1}(x))$ est un p-cycles.

$A_\gamma = \{a_1, a_2\}$: $\forall x \neq a_1, a_2 \quad \gamma(x) = x$

$\gamma(a_1) = a_2$

$\gamma(a_2) = a_1$

Initialisation :

$\gamma = (a_1 \; a_2)$ 2 cycles.

Récurrence forte : Hérédité :

$\forall i \leq k \quad \mathcal{P}(i)$ est vrai :

On montre que $\mathcal{P}(k+1)$ est vrai

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix} = (1\ 3) \circ (2\ 4\ 5)$$

$$\Big((1\ \gamma(1)\ \dots\ \gamma^{p-1}(1))\ (2\ \gamma(2)\ \dots\ \ )$$