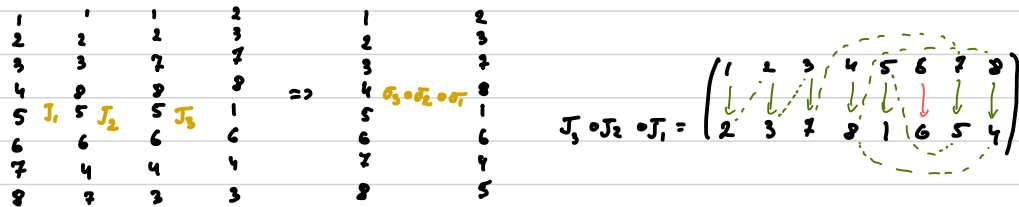




Thm: Toute $\sigma \in S(E)$ se décompose en ^{produit} fini de cycles à support disjoints.

Ex: $\sigma = \overbrace{(1\ 3\ 5\ 7)}^{J_3} \circ \overbrace{(3\ 7)}^{J_2} \circ \overbrace{(7\ 4\ 8)}^{J_1}$ à support non disjoints $f \circ g(x) = f(g(x))$



CCL: $J_3 \circ J_2 \circ J_1 = (1\ 2\ 3\ 7\ 4\ 8\ 5) \circ (6)$
un seul cycle

Thm: ^{Cor:} $S(E)$ le groupe des permutations de E est engendré par les cycles

Thm: $S(E)$ est engendré par les transpositions = les 2-cycles

pr: Suffit de mq chaque p -cycle est un produit (composition) de 2-cycles.

$p=2$: $(a_1\ a_2)$ 2-cycle = transpo

$p=3$: $(a_1\ a_2\ a_3) = (a_1\ a_2) \circ (a_2\ a_3)$

$a_1 \rightarrow a_2$
 $a_2 \xrightarrow{(a_2\ a_3)} a_3$
 $a_3 \rightarrow a_1$
 $(a_1\ a_2)$
 $a_1 \rightarrow a_2$
 $a_2 \rightarrow a_1$
 $(a_1\ a_2\ a_3)$

p -qlec: $(a_1\ a_2\ \dots\ a_p) = (a_1\ a_2) \circ (a_2\ a_3) \circ \dots \circ (a_{p-1}\ a_p)$

Thm: L'ordre d'un p -cycle $(a_1\ \dots\ a_p)$ dans $S(E)$ est égal à p = sa longueur

pr: $G = 1$ tour de cadran $\sigma^2 = 2$ tours; $\sigma^{p-1} = p-1$; $\sigma^p = p$ tours. $\square$

Thm: L'ordre de $\sigma = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_r$ décomposée en cycles à supp disj.
 $o(\sigma) = \text{ppcm}(o(\sigma_1), o(\sigma_2), \dots, o(\sigma_r)) = \text{ppcm}(\text{long}(\sigma_1), \dots, \text{long}(\sigma_r))$

pr: Comme les supp sont disj. $\sigma_1, \dots, \sigma_r$ commutent, donc
 $\sigma^m = \sigma_1^m \circ \dots \circ \sigma_r^m$ donc $\sigma^m = \text{Id} \Leftrightarrow \sigma_1^m = \text{Id}, \dots, \sigma_r^m = \text{Id}$

$I_{S(E)} = \text{Id}$

$E \rightarrow E$

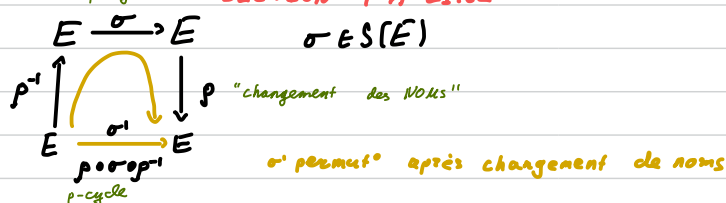
$x \mapsto x$

donc le m minimal est bien le $\text{ppcm}(o(\sigma_1), \dots, o(\sigma_r))$

Chargements de "coordonnées" sur E

p -cycle

SECTION 4 À LIRE



Prop: $p \circ (a_1 \dots a_p) \circ p^{-1} = (p(a_1) \dots p(a_p))$

pv: p bijection $\exists \exists a \mapsto p(a) = b \in E$

Vérifions que $\forall b \in E \quad p \circ (a_1 \dots a_p) \circ p^{-1}(b) = (p(a_1) \dots p(a_p))(b)$

si oui, on a:

Cas 1: $b = p(a_i)$ avec $1 \leq i \leq p-1$ Alors

$$p(a_1 \dots a_p) \circ p^{-1}(p(a_i)) = p(a_1 \dots a_p)(a_i) = p(a_{i+1}) = (p(a_1) \dots p(a_p))(p(a_i))$$

$p(a_i) \rightarrow p(a_{i+1})$ OUI

Cas 2: $b = p(a_p)$ $i=p$ possible avec convention $p+1 = 1 \bmod p$

Cas 3: $b \neq p(a_1), \dots, p(a_p)$ Alors b est fixé par $(p(a_1) \dots p(a_p))$

$p^{-1}(b) \neq a_1, \dots, a_p$ de $\hat{m}$ $a := p^{-1}(b)$ est fixé par $(a_1 \dots a_p)$

car $a \neq a_1, \dots, a_p$

donc évident $p \circ (a_1 \dots a_p) \circ p^{-1}(b) = b = (p(a_1) \dots p(a_p))(b)$

i.e b reste fixé $\square$

Prop: Avec $\sigma \in S(E)$ avec $\frac{E}{E}$ p changement de noms, avec $\sigma' = p \circ \sigma \circ p^{-1}$

$p(\text{Fix } \sigma') = \text{Fix } \sigma'$

$p(\text{Supp } \sigma) = \text{Supp } \sigma'$

$E = \text{Fix } \sigma \sqcup \text{Supp } \sigma$

EXO-LECT

C'est unique? démontrer

Groupe Alterné

$$E, |E| \text{ pair}$$

Thm: $\sigma \in S(E)$ représentée $\sigma = J_1 \circ J_2 \circ \dots \circ J_k$ produit de transpositions 2-cycles

$$J = (i \rightarrow j) \quad 1 \leq i < j \leq n \quad \begin{matrix} i \mapsto j \\ j \mapsto i \end{matrix}$$

pas unique!

$J^2 = Id$ Ajouter J^2 ne change rien

$$\sigma = J_1 \circ \dots \circ J_k \circ \underline{J_i \circ J_i}$$

Thm: $z \bmod 2$ ne dépend pas de la représentation de $\sigma = J_1 \circ \dots \circ J_k$ comme produit de transposition

pv: $(J_1 \circ \dots \circ J_k = \sigma = J'_1 \circ \dots \circ J'_l) \quad \text{But } z \equiv z' \bmod 2$
 $\underline{J_1 \circ \dots \circ J_k}$

$$\underline{J_1 \circ \dots \circ J_k \circ J_i \circ J_i \circ \dots \circ J_l = J_1 \circ \dots \circ J_k \circ J_i \circ J_i \circ \dots \circ J_l}$$

$$Id = \text{-----} \quad S := z + z'$$

Lm: $J_i \quad Id = J_i \circ \dots \circ J_i$ produit de s transp

alors $S \equiv 0 \bmod 2 \Rightarrow$ Fin thm $0 \equiv z + z' \bmod 2 \Leftrightarrow z \equiv z' \bmod 2$

pv Lm: Cas $n=2 \quad S(\{1, 2\}) = (Id, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}) = (Id, (1 \ 2))$

$$J_1 \circ \dots \circ J_k = (1 \ 2)^s \quad (1 \ 2)^s = Id \Leftrightarrow s \text{ pair} \\ \Leftrightarrow S \equiv 0 \bmod 2$$

Rec sur $n = \text{Card } E$: HYP-REC Lm vrai pour $E = \{1, 2, \dots, n-1\}$

Passer à $\{1, \dots, n-1\} \cup \{n\}$ Ex: $n=7 \quad E = \{1 \ 2 \ 3 \ 4 \ 5 \ 6\} \cup \{7\}$
 $J := (1 \ 7) \circ (2 \ 3) \circ (5 \ 6) \circ (4 \ 7) \circ (4 \ 5)$ compos. de transpos.
HR HR

Manipulⁿ nécessaire

Assertion: Pour trois indices distincts $1 \leq i, j, k \leq n-1$
cycles à supp. disjoints
 $(i \ n) \circ (j \ k) \stackrel{1}{=} (j \ k) \circ (i \ n)$ n poussé à droite
 $(i \ n) \circ (i \ j) \stackrel{2}{=} (i \ j) \circ (j \ n)$
 $(i \ n) \circ (j \ n) \stackrel{3}{=} (i \ j) \circ (i \ n)$
 $(i \ n) \circ (i \ n) \stackrel{4}{=} Id$

Ex: $(1 \ 7)(2 \ 3)(5 \ 6)(4 \ 7)(4 \ 5) \stackrel{2}{=} (1 \ 7)(2 \ 3)(5 \ 6)(4 \ 5)(5 \ 7)$
 $\stackrel{1}{=} (1 \ 7)(2 \ 3)(5 \ 6)(4 \ 5)(1 \ 7)(5 \ 7)$
 $\stackrel{3}{=} (1 \ 7)(2 \ 3)(5 \ 6)(4 \ 5)(1 \ 5)(1 \ 7)$

pv 2: $\begin{matrix} i & j & j \\ j & i & i \\ n & n & i \end{matrix} \stackrel{1}{=} \begin{matrix} i & i & j \\ j & j & n \\ n & j & i \end{matrix}$ oui!

pv 3: EXO

Retour: $Id = T_1 \circ \dots \circ T_s$ Opérations 1, 2, 4 on repousse à droite
toutes les transpositions $(i \ n)$ avec $1 \leq i \leq n-1$

Alors $T_1 \circ \dots \circ T_s = \dots$ produit de $(i \ n)$ plusieurs
pos de n
La parité du nombre de transp ne change pas, parce que les opérations 1, 2, 3, 4 respectent mod 2

Enfin, Op 3, 4 permettent de n'avoir qu'une seule $(i \ n)$ à la fin (un plus)

Fin: Cas 1: $Id = T'_1 \circ \dots \circ T'_s \circ (i \ n)$

Cas 2: $Id = T'_1 \circ \dots \circ T'_s$ avec $T'_1, \dots, T'_s$ transpositions de $(1, \dots, n-1)$
HYP REC $\Rightarrow s' \equiv 0 \pmod 2$

A11°: Cas 1 impossible

$\Leftrightarrow (i \ n) = T'_1 \circ \dots \circ T'_s$

dans $(1 \dots n-1 \ n)$ dans $(1 \dots n-1)$

□

Déf: Signature de $\sigma = J_1 \circ \dots \circ J_s$