Permutations - Théorème

Prop Deux cycles à support disjoints commutent

preuve : Soit c_1 et c_2 deux cycles à support respectifs A_1 et A_2

avec $A_1 \cap A_2 = \emptyset$. Soit $x \in [\![1,n]\!]$

1er cas . $x \notin A_1 \cup A_2$, x est invariant par c_1 et c_2

donc $c_1 \circ c_2(x) = c_2 \circ c_1(x) = x$

2nd cas : $x \in A_1 \cup A_2$ et $x \in A_1$ par exemple et $x \notin A_2$

alors $c_2(x) = x$ et $c_1 \circ c_2(x) = c_1(x)$

or $c_1(x) \neq x$ et $c_1 \circ c_1(x) \neq c_1(x)$ par injectivité de c_1

donc $c_1(x) \in A_1$ et donc $c_1(x) \notin A_2$

d'où $c_1 \circ c_2(x) = c_1(x) = c_2 \circ c_1(x)$

D'où $c_1 \circ c_2 = c_2 \circ c_1$

Prop : Soit σ une permutation de $[\![1,n]\!]$. On définit sur $[\![1,n]\!]$ la relation $x \mathcal{R}_\sigma y \Leftrightarrow \exists k \in \mathbb{Z} \quad y = \sigma^k(x)$

C'est une relation d'équivalence sur $[\![1,n]\!]$

preuve. réflexif : $\forall x \in [\![1,n]\!]$ $x \mathcal{R}_\sigma x$ puisque $x = \sigma^0(x)$

symétrique : $\forall (x,y) \in [\![1,n]\!]^2$ tq $x \mathcal{R}_\sigma y$ alors $\exists k \in \mathbb{Z}$ tq

$y = \sigma^k(x)$ or σ est bijective d'où $x = \sigma^{-k}(y)$

donc $-k \in \mathbb{Z}$ et $y \mathcal{R}_\sigma x$

transitive : $\forall x, y, z \in [\![1,n]\!]$ tq $y = \sigma^k(x)$ et $z = \sigma^{k'}(y)$

$z = \sigma^{k'+k}(x)$ avec $k'+k \in \mathbb{Z}$ d'où $x \mathcal{R}_\sigma z$.

Prop 3 : Soit σ une permutation de $[\![1,n]\!]$ et $x \in [\![1,n]\!]$

il existe un entier naturel non nul p tq :

$x, \sigma(x), \dots, \sigma^{p-1}(x)$ soient 2 à 2 distincts et $\sigma^p(x) = x$

La classe d'équivalence de x pour la relation d'équivalence R_σ

est alors l'ensemble $\{x, \sigma(x), \dots, \sigma^{p-1}(x)\}$ appelée orbite de x

preuve : l'application $\mathbb{N} \to [\![1,n]\!]$ est une application non injective
$k \mapsto \sigma^k(x)$

car $\mathbb{N}$ est un ensemble de cardinal infini.

$\exists\, k, \ell$ tq $k \neq \ell$ $\sigma^k(x) = \sigma^\ell(x)$, on peut supposer $k < \ell$

$\sigma^{k-\ell}(x) = x$ avec $\ell - k \in \mathbb{N}^*$

Soit $A = \{ q \in \mathbb{N} \mid \sigma^q(x) = x \}$ est une partie de $\mathbb{N}^*$ non vide.

il admet un plus petit élément noté p

p vérifie les propriétés suivantes :

. comme $p \in A$ $\sigma^p(x) = x$

. $x, \sigma(x), \dots \sigma^{p-1}(x)$ sont 2 à 2 distincts.

En effet s'il existe i et j tq $1 \leq i < j \leq p-1$

avec $\sigma^i(x) = \sigma^j(x)$ alors $\sigma^{j-i}(x) = x$

et $0 < j-i < p$ contradiction avec minimum de p.

Les éléments de l'orbite de x sont dans la classe d'équivalence de x pour la relation R_σ.

Réciproquement, si $y \in$ à la classe d'équivalence de x, il existe $k \in \mathbb{Z}$ tq $y = \sigma^k(x)$. Soit r le reste de la division euclidienne de k par p

$$y = \sigma^{pq+r}(x) = \sigma^r \sigma^{pq}(x) = \sigma^r(x) \quad \text{et } r \in [\![0,p-1]\!]$$

donc $y \in$ l'orbite de x.

Donc l'orbite de x est bien la classe d'équivalence de x pour R_σ

Théorème : Décomposition en produit de cycles à support disjoints

Toute permutation différente de l'identité se décompose, de manière unique à l'ordre près des facteurs, en produit de cycles à supports deux à deux disjoints.

Preuve. Soit σ une permutation de $[\![1,n]\!]$ autre que Id.

unicité - Soit $c_1, c_2, \dots c_r$ cycles à supports disjoints 2 à 2 d'ordre respectifs $p_1, \dots, p_r$ tq $\sigma = \prod_{i=1}^{r} c_i$

Soit $j \in [\![1,r]\!]$. Considérons un élément $x \in [\![1,n]\!]$ tel que $c_j(x) \neq x$. On a alors $c_i(x) = x \ \forall i \neq j$

donc $\sigma(x) = \left(\prod_{i=1}^{r} c_i\right)(x) = c_j\left(\prod_{i \neq j} c_i(x)\right) = c_j(x)$

Ainsi x a la même image par σ et c_j, l'orbite de x pour ces deux applications est la même et c_j est le cycle $(x, \sigma(x), \dots \sigma^{p_j-1}(x))$

On en déduit l'unicité de r (nombre d'orbites de σ) et l'unicité des cycles $(c_j)_{1\leq j\leq r}$ (restriction de σ à ses orbites non réduites en un point)

les cycles sont 2 à 2 disjoints, ils commutent, ce qui justifie l'unicité de la décomposition.

Existence - Considérons les orbites de σ de cardinal ≥ 2. Il y en a au moins une car $\sigma \neq Id$.

Soit r le nombre d'orbites.

On définit alors la restriction de σ à chacune de ces orbites -

On définit alors r cycles $(c_i)_{1 \leq i \leq r}$ dont les supports sont les orbites de σ.

Par définition des orbites (cō classes d'équivalence), les supports de ces cycles sont 2 à 2 disjoints.

Notons $\sigma' = \prod_{i=1}^{r} c_i$

Soit $x \in [\![1,n]\!]$ invariant par σ. Alors l'orbite de x est réduite à $\{x\}$, et $x \notin supp(c_i)$ $\forall i$ donc x est invariant par

$$\sigma' = \prod_{i=1}^{r} c_i$$

alors $\sigma(x) = x = \sigma'(x)$

Soit $x \in [\![1,n]\!]$ non invariant par x. Alors $x \in supp(c_{i_0})$

(un seul car classes d'éq. sont disjointes)

$$\sigma'(x) = c_{i_0} \left(\prod_{\substack{i=1 \\ i \neq i_0}}^{r} c_i \right)(x) = c_{i_0}(x) = \sigma(x)$$

d'où $\sigma = \sigma' = \prod_{i=1}^{r} c_i$

Prop. Toute permutation de $[\![1,n]\!]$ est un produit de transpositions

preuve : $\sigma \in S_n$ $n \geq 2$

- $\sigma = Id$, $Id = (1,2)(1,2)$
- σ cycle de longueur p, $\sigma = (a_1, \dots, a_p)$ se décompose en

$$\sigma = (a_1\, a_2)(a_2\, a_3) \dots (a_{p-1}\, a_p)$$

donc produit de transpo.

- cas général, on décompose σ en produit de cycles en utilisant le th précédent. Chaque cycle s'écrit comme le produit de transpositions d'où le résultat