

dev: Générateurs de $\mathcal{O}_n$

Leçons: 101, 104, 105

ex: Rambaldi 43-45.

Théorème: Toute permutation $\sigma \in \mathcal{O}(E) \setminus \{Id_E\}$ se décompose en produit de cycles deux à deux disjoints. (i.e. $\mathcal{O}(E)$ est engendré par des cycles).
De plus, cette décomposition est unique à l'ordre près.

dem:

(E) Soient $\sigma \in \mathcal{O}(E) \setminus \{Id_E\}$ et $O_1, \dots, O_p, \dots, O_n$ les orbites deux à deux distinctes avec $n_1 = \text{card}(O_1) \geq 2 \quad \forall k \in \{1, \dots, p\}$ et $\text{card}(O_k) = 1 \quad \forall k \in \{p+1, \dots, n\}$.
On a alors la partition $E = \bigcup_{k=1}^n O_k$.

Pour $k \in \{1, \dots, p\}$, on définit $\gamma_k \in \mathcal{O}(E)$ par $\gamma_k(x) = \begin{cases} \sigma(x) & \text{si } x \in O_k \\ x & \text{si } x \notin O_k \end{cases} \quad \forall x \in E$.
(c'est bien une permutation car $\sigma|_{O_k}$ est une permutation de O_k)
⚡: tous les points sont atteints.

Si O_k est réduite à un point, alors $\gamma_k = Id_E$ ($\sigma(a) = a$, si on note a ce pt).
Sinon γ_k est un n_k -cycle:

en effet, pour $x \in O_k$. On a $\gamma_k(x) = \sigma(x)$ et $\text{Orb}_{\gamma_k}(x) = \text{Orb}_{\sigma}(x) = O_k$
et pour $x \notin O_k$: $\text{Orb}_{\gamma_k}(x) = \{x\} \quad \gamma_k^j(x) = x \quad \forall j \in \mathbb{Z} \quad \sigma(x) = x \quad \forall x \notin O_k$

Donc γ_k a bien une seule orbite non réduite à un point: c'est donc un cycle.

Décrivons que $\sigma = \prod_{j=1}^n \gamma_j = \prod_{j=1}^p \gamma_j$

Soit $x \in E$. Il existe un unique indice $k \in \{1, \dots, p\}$ tq $x \in O_k$ et on a
 $\gamma_k(x) = \sigma(x) \quad ; \quad \gamma_j(x) = x \quad \text{si } j \neq k$.

Comme les γ_j commutent (car ils sont à support disjoint), on en déduit:

$$\left(\prod_{j=1}^n \gamma_j \right)(x) = \left(\gamma_k \prod_{\substack{j=1 \\ j \neq k}}^n \gamma_j \right)(x) = \gamma_k(x) = \sigma(x), \quad (*)$$

(U) Montrons l'unicité:

Soit $\sigma = \prod_{k=1}^{p'} \gamma'_k$ une autre décomposition en cycles deux à deux disjoints.

Notons $O'_1, \dots, O'_{p'}$ les supports de ces cycles.

Soient $k \in \{1, \dots, p'\}$ et $x \in O'_k$: $\sigma(x) = \gamma'_k(x)$ car $x \notin O'_j \quad \forall j \neq k$, cf (*).
donc $O'_k = \text{Orb}_{\gamma'_k}(x) = \text{Orb}_{\sigma}(x)$.

Les orbites O'_k sont donc les orbites non réduites à un point de σ et $p' = p$.
car $\sigma \neq Id$ par hyp (c'est des cycles)

On a donc $O'_k = O_k$ pour un unique $j \in \{1, \dots, p\}$. car O_j aussi orb de σ

Pour $x \in O'_k$: $\gamma'_k(x) = \sigma(x) = \gamma_j(x)$

$x \notin O'_k$: $\gamma'_k(x) = x = \gamma_j(x)$

Donc $\gamma'_k = \gamma_j$

Ceci donne l'unicité à l'ordre près.

→ Ex: plus σ (sans cycle de longueur 1) → + cycle

→ Ex: $(1, 2, 3, 4, 5) = (1, 2, 3)(4, 5)$ et $(1, 2, 3, 4, 5) = (1, 2, 3, 4)(5)$

exer: i) les cycles sont des générateurs de $\mathcal{O}(E)$

ii) transposition

iii) $(1, k), 2 \leq k \leq n$

iv) $(k, k+1), 1 \leq k \leq n-1$

v) $(1, 2), (1, 2, \dots, n)$

$\mathcal{O}_n$

i) pour l'un précédent.

ii) tout cycle s'écrit comme produit de transposition:

$$(x_1 \ x_2 \ \dots \ x_n) = (x_1 \ x_2)(x_2 \ x_3) \dots (x_{n-1} \ x_n)$$

expliquer dans le sens.

iii) Soit $(i \ j)$ une transposition.

Si i ou $j = 1$, c'est ok.

$$\text{Sinon: } (i \ j) = (1, i)(1, j)(1, i)^{-1}$$

$$= (1, i)(1, j)(1, i)$$

(car $\sigma \sigma^{-1} = \text{id}$)

$$\sigma \tau \sigma^{-1} = (\sigma(\tau) \dots)$$

donc $(1, k)$ engendre les transpositions qui engendrent $\mathcal{O}_n$.

iv) $k \in \mathbb{Z} : \text{ok}$
 $k \in \{3, \dots, n\}$

$$(1, k) = (k-1, k)(1, k-1)(k-1, k)^{-1} = (k-1, k)(1, k-1)(k-1, k)$$

$k=3$ $(1, k-1) = (1, 2)$ c'est ok.

sinon on recommence avec $(1, k-1)$ jusqu'à $(1, 2)$

$$e) \ G = \langle \underbrace{(1, 2)}_T, \underbrace{(1, 2, \dots, n)}_T \rangle \quad \text{où } (1, k) \in G \ \forall k.$$

$$(1, 2) \in G.$$

Pour $n \geq 3$:

$$\begin{cases} \gamma(1, 2)\gamma^{-1} = (\gamma(1), \gamma(2)) = (2, 3) \\ \gamma(2, 3)\gamma^{-1} = (\gamma(2), \gamma(3)) = (3, 4) \end{cases}$$

$$\gamma(n-2, n-1)\gamma^{-1} = (\gamma(n-2), \gamma(n-1)) = (n-1, n)$$

$$\text{r. e. } (k, k+1) = \gamma^{k-1}(1, 2)(\gamma^{k-1})^{-1} \quad \forall k \in \{n, n-1\}.$$