Leçon 105 : Groupe des permutations d'un ensemble fini. Applications

RM
2022-2023

Soit $n \in \mathbb{N}^*$ tel que $n \geq 2$.

1 Définitions et propriétés du groupe symétrique

1.1 Définitions

Définition 1 : Soit E un ensemble de cardinal n. On appelle groupe des permutations de E notée $\mathcal{S}(E)$ le groupe des bijections de E sur lui même. Si $E = \{1, ..., n\}$, on l'appelle alors groupe symétrique notée $\mathcal{S}_n$.

Théorème 2 : Si E,F sont deux ensembles non vides de même cardinal, alors $\mathcal{S}(E)$ est isomorphe à $\mathcal{S}(F)$.

Remarque 3 : Cela nous permet de ramener l'étude des permutations d'un ensemble fini à l'étude de $\mathcal{S}_n$.

Notation 4 : Si $\sigma \in \mathcal{S}_n$, on le note de la façon suivante :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Proposition 5 : Le groupe symétrique $\mathcal{S}_n$ agit naturellement sur l'ensemble $\{1, ..., n\}$ par permutation. Cette action naturelle est donnée par $\sigma.i = \sigma(i)$ pour tout $\sigma \in \mathcal{S}_n$ et $i \in \{1, ..., n\}$.

Définition 6 : Soit $2 \leq r \leq n$. On appelle cycle d'ordre r(ou r-cycle), toute permutation $\sigma \in \mathcal{S}_n$, qui permute circulairement r éléments de $\{1, ..., n\}$ et laisse fixe les autres, i.e il existe $x_1, ..., x_r$ de $\{1, ..., n\}$ telle que :

$$\begin{cases} \forall k \in \{1, ..., r-1\}, \sigma(x_k) = x_{k+1} \\ \sigma(x_r) = x_1 \\ \forall x \in \{1, ..., n\} \setminus \{x_1, ..., x_r\}, \sigma(x) = x \end{cases}$$

On appelle transposition un cycle de longueur 2.

Proposition 7 : Un r-cycle est d'ordre r dans $\mathcal{S}_n$.

Théorème 8 : On a $|\mathcal{S}_n| = n!$.

1.2 Support et orbites d'une permutation

Définition 9 : Le support d'une permutation $\sigma \in \mathcal{S}_n$ est le complémentaire dans E de l'ensemble de ses points fixes, soit l'ensemble :

$$Supp(\sigma) = \{x \in E | \sigma(x) \neq x\}$$

Exemple 10 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$ est un cycle de support $\{1, 3, 5\}$.

Théorème 11 : Si $\sigma, \sigma' \in \mathcal{S}_n$, alors on a $\sigma(Supp(\sigma)) = Supp(\sigma)$ et si $Supp(\sigma) \cap Supp(\sigma') = \emptyset$, on a que σ et σ' commute.

Définition 12 : On appelle orbite de $x \in \{1, ..., n\}$ par rapport à $\sigma \in \mathcal{S}_n$ l'ensemble $\mathcal{O}_\sigma(x) = \{\sigma^k(x), k \in \mathbb{Z}\}$.

Remarque 13 : $\mathcal{O}_\sigma(x)$ est réduite à un point si et seulement si $\sigma(x) = x$ et les orbites non réduites à un point forment une partition du support de σ.

Proposition 14 : Si $|\mathcal{O}_\sigma(x)| = r$, alors r est le plus petit entier tel que $\sigma^r(x) = x$ et $\mathcal{O}_\sigma(x) = \{x, \sigma(x), ..., \sigma^{r-1}(x)\}$.

Théorème 15 : Soit $\sigma \in \mathcal{S}_n$. Alors σ est un r-cycle si et seulement si il n'y a qu'une seule orbite de σ non réduit à un point.

Théorème 16 : Toute permutation $\sigma \in \mathcal{S}_n$ non trivial se décompose en produit de cycles deux à deux disjoints. Cette décomposition est unique à l'ordre près. Si $\sigma = \gamma_1 ... \gamma_p$ une telle décomposition, on a alors $Supp(\sigma) = \bigcup_{k=1}^{p} Supp(\gamma_k)$ et $o(\sigma) = ppcm(o(\gamma_1), ..., o(\gamma_p))$.

Exemple 17 : On a $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 5 & 1 & 3 & 4 & 7 \end{pmatrix} = (1, 2, 6, 4).(3, 5).(7)$.

Remarque 18 : Les cycles sont des générateurs de $\mathcal{S}_n$.

Théorème 19 : Le groupe $\mathcal{S}_n$ est engendré par les transpositions

1.3 Conjugaison dans $\mathcal{S}_n$

Lemme 20 : Soit r tel que $2 \leq r \leq n$. Le conjugué dans $\mathcal{S}_n$ d'un r-cycle est encore un r-cycle. Plus précisément, pour tout r-cycle $\sigma = (x_1, x_2, ..., x_r)$ et toute permutation τ, on a :

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), ..., \tau(x_r))$$

Corollaire 21 : Réciproquement, deux cycles de même longueur sont conjugués dans $\mathcal{S}_n(E)$, i.e que si σ et σ' sont deux cycles de même longueur r, il existe alors une

permutation τ telle que $\sigma' = \tau \circ \sigma \circ \tau^{-1}$.

Remarque 22 : Le résultat précédent signifie que pour tout $r \in [\![2\,;n]\!]$, le groupe $\mathcal{S}_n$ agit par conjugaison de façon transitive sur l'ensemble des r-cycles.

2 Signature et groupe alternée

2.1 Signature d'une permutation

Définition 23 : Soit $\sigma \in \mathcal{S}_n$. On appelle signature de σ le produit

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

On a $\varepsilon(\sigma) \in \{-1, 1\}$. Si $\varepsilon(\sigma) = 1$, alors σ est dite paire et impaire dans le cas contraire.

Exemple 24 : Soit $\sigma = (i, j)$ avec $i < j$ une transposition de $\mathcal{S}_n$. Alors $\varepsilon(\sigma) = \frac{i-j}{j-i} = -1$.

Proposition 25 : Si $\sigma, \tau \in \mathcal{S}_n$, alors $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

Remarque 26 : La proposition précédente exprime le fait que la signature est un morphisme de groupe. De plus, on en déduit que la signature d'un produit de r transpositions est $(-1)^r$.

Proposition 27 : La signature d'un cycle de longueur p est $(-1)^p$.

Exemple 28 : La signature de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 6 & 5 & 1 & 3 & 4 & 7 \end{pmatrix} = (1, 2, 6, 4).(3, 5).(7)$ est donc $\varepsilon(\sigma) = (-1)^3(-1)(-1)^0 = 1$.

2.2 Le groupe alterné

Définition 29 : Le groupe alterné notée $\mathcal{A}_n$ est le sous-ensemble de $\mathcal{S}_n$ formé des permutations paires. C'est le noyau du morphisme signature.

Proposition 30 : On a $|\mathcal{A}_n| = n!/2$.

Théorème 31 : Pour $n \geq 3$, $\mathcal{A}_n$ est engendré par les 3-cycles.

Théorème 32 : $\mathcal{A}_n$ est simple pour $n \geq 5$.

Dev 1

3 Applications du groupe symétrique

3.1 En théorie des groupes

Théorème (de Cayley) 33 : Tout groupe G tel que $|G| = n$ est isomorphe à un sous groupe de $\mathcal{S}_n$.

Définition 34 : Soit G un groupe et φ un endomorphisme de G. On dit que φ est un automorphisme intérieur de G s'il existe $a \in G$ tel que $\varphi(x) = axa^{-1}$ pour tout $x \in G$, et qu'il est extérieur sinon. On note $Int(G)$ l'ensemble des automorphismes intérieurs de G.

Théorème 35 : Pour $n \neq 6$, tout automorphisme de $\mathcal{S}_n$ est intérieur. **Dev 2**

3.2 En algèbre multilinéaires

On se place dans E un $\mathbb{K}$-e.v de dimension fini $n \in \mathbb{N}^*$.

Définition 36 : Une application $f : E^p \to \mathbb{K}$ est appelé une forme $p-$linéaire sur E, appartenant à l'espace vectoriel noté $\mathcal{L}_p(E, \mathbb{K})$, si en tout point les p applications partielles de f sont linéaires.
Si $f \in \mathcal{L}_p(E, \mathbb{K})$:

- f est dite alternée si $f(x_1, ..., x_p) = 0$ dès que deux vecteurs parmi les x_i sont égaux.
- f est dite antisymétrique si l'échange de deux vecteurs dans la suite $(x_1, ..., x_p)$ donne à f des valeurs opposées.

Théorème 37 : L'ensemble des formes n-linéaires alternées sur E est de dimension. De plus, il existe une et une seule forme linéaire alternée prenant la valeur 1 sur une base donnée de E, appelé déterminant dans la $B = (e_1, ..., e_n)$. Pour $x_1, ..., x_n \in E$ $(x_i = \sum_{j=1}^{n} x_{i,j} e_j)$, on a

$$det_B(x_1, ..., x_n) = \sum_{\sigma \in \mathcal{S}_n} \varepsilon\sigma x_{1,\sigma(1)} ... x_{n,\sigma(n)}$$

Définition 38 : Soit $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{K})$. On a

$$detA = \sum_{\sigma \in \mathcal{S}_n} \varepsilon(\sigma) a_{1,\sigma(1)} ... a_{n,\sigma(n)}.$$

3.3 Polynômes symétriques

On se place sur $\mathbb{A}$ un anneau commutatif unitaire.

Définition 39 : Un polynôme $P \in \mathbb{A}[X_1, ..., X_n]$ est dit symétrique si pour tous $\sigma \in \mathcal{S}_n$, $P(X_{\sigma(1)}, ..., X_{\sigma(n)}) = P(X_1, ..., X_n)$.

Exemple 40 : Dans $\mathbb{R}[X, Y, Z], P = XY + YZ + ZX$ est symétrique.

Définition 41 : Pour $n \in \mathbb{N}$ et $k \in [\![0\,;n]\!]$, on définit le polynôme symétrique élémentaire e_k de $\mathbb{A}[X_1, ..., X_n]$ par

$$e_k = \sum_{I \in \mathcal{P}_k([\![1\,;n]\!])} \prod_{i \in I} X_i$$

où $\mathcal{P}_k([\![1\,;n]\!])$ désigne l'ensemble des parties à k éléments de $\{1, ..., n\}$.

Théorème 42 : Pour tout $P \in \mathbb{A}[X_1, ..., X_n]$ symétrique, il existe un unique polynôme $Q \in \mathbb{A}[X_1, .., X_n]$ tel que $P(X_1, ..., X_n) = Q(e_1, ..., e_n)$.

Références :

1. Algèbre et géométrie - Rombaldi
2. Algèbre - Gourdon
3. Théorie des groupes - Ulmer
4. Cours d'algèbre - Perrin
5. L'oral à l'agrégation - Pecate