

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

Dans cette leçon on considère E un ensemble fini ayant au moins 2 éléments.

1 Généralités

1.1 Permutations et groupe symétrique

Définition 1. Le groupe $\mathcal{S}(E)$ des bijections de E sur lui même est appelé groupe des permutations de E .

Remarque 2. Pour $E = \{1, \dots, n\}$ on note $\mathcal{S}_n = \mathcal{S}(E)$ appelé groupe symétrique à n éléments.

Définition 3. Soit $2 \leq r \leq |E|$. On appelle r -cycle toute permutation $\sigma \in \mathcal{S}(E)$ qui permute circulairement r éléments et laisse fixe les autres. C'est-à-dire qu'il existe $\{x_1, \dots, x_r\} \subset E$ telle que : $\forall k \in \{1, \dots, r-1\}, \sigma(x_k) = x_{k+1}$; $\sigma(x_r) = x_1$; $\forall x \in E \setminus \{x_1, \dots, x_r\}, \sigma(x) = x$. On notera un tel cycle $(x_1, \dots, x_r)$.

Proposition 4. L'inverse d'un r -cycle est un r -cycle, précisément $(x_1, \dots, x_r)^{-1} = (x_r, \dots, x_1)$.

Définition 5. Un 2-cycle est appelé transposition.

Proposition 6. Soit $2 \leq r \leq |E|$. Le conjugué dans $\mathcal{S}(E)$ d'un r -cycle est encore un r -cycle. Plus précisément pour tout $\sigma = (x_1, \dots, x_r)$ et toute permutation τ on a $\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \dots, \tau(x_r))$. Réciproquement deux cycles de même longueur sont conjugués dans $\mathcal{S}(E)$.

Proposition 7. Le centre du groupe de $\mathcal{S}(E)$ est $Z(\mathcal{S}(E)) = \mathcal{S}(E)$ si $|E| = 2$ et $Z(\mathcal{S}(E)) = \{Id\}$ sinon.

Théorème 8. Si E et F sont deux ensembles non vides et $\varphi : E \rightarrow F$ une bijection, alors $\mathcal{S}(E)$ et $\mathcal{S}(F)$ sont isomorphes.

Théorème 9. Pour E de cardinal $n \geq 1$ on a $|\mathcal{S}(E)| = n!$.

1.2 Supports, orbites et générateurs

Définition 10. Le support de $\sigma \in \mathcal{S}(E)$ est l'ensemble $Supp(\sigma) = \{x \in E | \sigma(x) \neq x\}$.

Théorème 11. Soient $\sigma, \sigma' \in \mathcal{S}(E)$ alors :

1. $\sigma(Supp(\sigma)) = Supp(\sigma)$,
2. $Supp(\sigma^{-1}) = Supp(\sigma)$,
3. Pour tout $r \in \mathbb{Z}$ on a $Supp(\sigma^r) \subset Supp(\sigma)$,
4. Si $Supp(\sigma) \cap Supp(\sigma') = \emptyset$ (on dit qu'ils sont à support disjoints), alors $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Théorème 12. Toute permutation $\sigma \in \mathcal{S}(E) \setminus \{Id\}$ se décompose en produit de cycles à support disjoints. Cette décomposition est unique à l'ordre près.

Définition 13. On appelle type d'une permutation $\sigma \in \mathcal{S}_n$ noté $[l_1, \dots, l_m]$ la liste des longueurs dans l'ordre croissant des cycles de sa décomposition en cycle à support disjoint.

Proposition 14. Une permutation de type $[l_1, \dots, l_m]$ a pour ordre le ppcm($l_1, \dots, l_m$).

Lemme 15. Pour $2 \leq r \leq n$, tout r -cycle s'écrit comme produit $r-1$ transpositions.

Théorème 16. Toute permutation $\sigma \in \mathcal{S}(E)$ se décompose en produit de transpositions.

Lemme 17. $\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(1\ k)$ où $2 \leq k \leq n$.

Lemme 18. $\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(k\ k+1)$ où $1 \leq k \leq n-1$.

Lemme 19. $\mathcal{S}_n$ est engendré par $(1\ 2)$ et $(1\ 2\ \dots\ n)$.

2 Signature et groupe alterné

2.1 Signature

On note $\mu(\sigma)$ le nombre d'orbites distinctes de $\sigma \in \mathcal{S}_n$.

Définition 20. La signature d'une permutation $\sigma \in \mathcal{S}(E)$ est l'élément $\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)} \in \{-1, 1\}$.

Exemple 21. On a $\varepsilon(\text{Id}) = 1$, pour un r -cycle σ on a $\varepsilon(\sigma) = (-1)^{r-1}$

Lemme 22. Pour tout $\sigma \in \mathcal{S}(E)$ et toute transposition $\tau \in \mathcal{S}(E)$, on a $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.

Théorème 23. Si $\sigma \in \mathcal{S}(E)$ est produit de p transpositions, on a alors $\varepsilon(\sigma) = (-1)^p$.

Théorème 24. Les seuls morphismes de groupes de $(\mathcal{S}(E), \circ)$ vers $(\mathbb{R}^*, \cdot)$ sont l'application égale à 1 et la signature qui est surjective sur $\{-1, 1\}$.

Théorème 25. Pour toute permutation $\sigma \in \mathcal{S}(E)$ on a :

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

Exemple 26. METTRE UN EXEMPLE

2.2 Groupe alterné

Définition 27. On dit qu'une permutation $\sigma \in \mathcal{S}(E)$ est paire (resp impaire) lorsque $\varepsilon(\sigma) = 1$ (resp $\varepsilon(\sigma) = -1$).

Définition 28. Le groupe alterné $\mathcal{A}(E)$ est le sous ensemble de $\mathcal{S}(E)$ formé des permutations paires.

Théorème 29. Le sous groupe $\mathcal{A}(E)$ est un sous groupe normal du groupe $\mathcal{S}(E)$.

Proposition 30. Pour tout $n \in \mathbb{N}^*$, $\mathcal{A}_n$ est un sous groupe d'indice 2 de $\mathcal{S}_n$ et on a $|\mathcal{A}_n| = \frac{n!}{2}$.

Lemme 31. Le produit de 2 transpositions est un produit de 3-cycles. Précisément pour $x, y, z, t \in E$ distincts on a : $(x y)(x z) = (x z y)$ et $(x y)(z t) = (x y z)(y z t)$.

Théorème 32. Pour $n \geq 3$, $\mathcal{A}(E)$ est engendré par les 3-cycles.

Théorème 33. Pour $n \geq 5$ les sous groupes normaux de $\mathcal{S}(E)$ sont $\{\text{Id}\}$, $\mathcal{A}(E)$ et $\mathcal{S}(E)$.

Théorème 34. Pour $n = 3$ ou $n \geq 5$ le groupe $\mathcal{A}(E)$ est simple.

3 Applications

3.1 Dérangements[GOU21]

Définition 35. Soit $I_n = \{1, \dots, n\}$ on appelle dérangement de I_n toute permutation σ n'ayant aucun point fixe.

Théorème 36. Pour tout $p \in \mathbb{N}^*$ on note D_p l'ensemble des dérangements de I_p , c'est-à-dire les permutations sans point fixe. On pose $\delta_p = |D_p|$ et on a $\delta_1 = 0$ et par convention $\delta_0 = 1$. La formule générale est $\delta_n = \lfloor \frac{n!}{e} + 1/2 \rfloor$.

3.2 Théorie des groupes

Théorème 37. (Cayley) Tout groupe de G est isomorphe à un sous groupe de $\mathcal{S}(G)$.

Définition 38. Pour toute permutation $\sigma \in \mathcal{S}_n$ on associe la matrice P_σ la matrice de passage de la base $\mathcal{B} = (e_j)_{1 \leq j \leq n}$ vers la base $\mathcal{B}_\sigma = (e_{\sigma(j)})_{1 \leq j \leq n}$. Cette matrice vérifie $P_\sigma e_j = e_{\sigma(j)}$ pour tout $j \in \{1, \dots, n\}$ et pour tout $x = (x_j)_{1 \leq j \leq n} \in \mathbb{K}^n$ on a $P_\sigma x = (x_{\sigma^{-1}(j)})_{1 \leq j \leq n}$.

Théorème 39. L'application $p : \mathcal{S}_n \rightarrow GL_n(\mathbb{K}) ; \sigma \mapsto P_\sigma$ est un morphisme de groupe injectif et on a $\det(P_\sigma) = \varepsilon(\sigma)$.

Corollaire 40. Tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous groupe de $GL_n(\mathbb{F}_p)$.

Dev 1 : An est simple 31,32 et 34
Dev 2 : Nombre de dérangements de $\mathcal{S}_n$ 36

Références

- [GOU21] Xavier GOURDON : Les maths en tête. Algèbre et probabilités. Editions Ellipses, 2021.
- [ROM17] JeanÉtienne ROMBALDI : Mathématiques pour l'Agrégation : Algèbre géométrie. De Boeck Supérieur, 2017.
- [ULM12] Félix ULMER : Théorie des groupes. Ellipses, 2012.

RAPPORT DU JURY :

Parmi les attendus, il faut savoir relier la leçon avec les notions d'orbites et d'actions de groupes. Il faut aussi savoir décomposer une permutation en cycles à supports disjoints, tant sur le plan théorique (preuve du théorème de décomposition), que pratique (sur un exemple) et savoir l'utiliser pour déterminer les classes de conjugaison du groupe symétrique et pour donner des systèmes de générateurs. L'existence du morphisme signature est un résultat non trivial mais ne peut pas constituer, à elle seule, l'objet d'un développement. Il est bon d'avoir en tête que tout groupe fini se plonge dans un groupe symétrique et de savoir calculer la signature des permutations ainsi obtenues dans des cas concrets. Les applications sont nombreuses, il est très naturel de parler du déterminant, des polynômes symétriques ou des fonctions symétriques des racines d'un polynôme. On peut également parler du lien avec les groupes d'isométries des solides.

Pour aller plus loin, les candidates et candidats peuvent s'intéresser par exemple aux automorphismes du groupe symétrique, à des problèmes de dénombrement, aux représentations des groupes des permutations ou encore aux permutations aléatoires.