Leçon 105 : Groupes de permutations d'un ensemble fini. Applications.

Pré-requis : la notion d'action de groupe ainsi que les théorèmes de Sylow.

1 Le groupe symétrique

Définition 1. Soit X un ensemble fini de cardinal n, on appelle *permutations* de X les bijections de X dans lui-même. L'ensemble des permutations de X muni de la composition est un groupe noté $\mathfrak{S}(X)$. Si $X = \{1,\dots,n\}$, on notera $\mathfrak{S}_n$.

Proposition 2. *Si X est de cardinal $n \in \mathbf{N}^*$, alors $\mathfrak{S}(X)$ et $\mathfrak{S}_n$ sont isomorphes.*

Proposition 3. *Le groupe $\mathfrak{S}_n$ est de cardinal $n!$.*

Définition 4. Soit $\sigma \in \mathfrak{S}_n$, on appelle support de σ l'ensemble $\operatorname{supp}(\sigma) = \{k \in [\![1,n]\!] \mid \sigma(k) \neq k\}$.

Définition 5. On dit que $\sigma \in \mathfrak{S}_n$ est un k–cycle s'il existe $i_1,\dots,i_k$ distincts dans $\{1,\dots,n\}$ tels que $\sigma(i_1) = i_2$, ..., $\sigma(i_{k-1}) = i_k$, $\sigma(i_k) = i_1$ et si σ fixe les autres éléments. On note $\sigma = (i_1 \cdots i_k)$. On appelle transposition un cycle de longueur 2.

Proposition 6. *Deux cycles dont les supports sont disjoints commutent.*

Proposition 7. *Les k–cycles sont d'ordre k.*

Proposition 8. *Soit $\sigma \in \mathfrak{S}_n$. Alors l'action de $\mathfrak{S}_n$ sur $[\![1;n]\!]$ induit une action de $\langle\sigma\rangle$ sur $[\![1;n]\!]$. Notons $F_1,\dots,F_r$ les orbites pour cette action et définissons :*

$$\sigma_i(x) = \begin{cases} x & \text{si } x \notin F_i \\ \sigma(x) & \text{si } x \in F_i \end{cases}$$

Alors les σ_i sont des cycles d'ordre $|F_i|$, disjoints, et $\sigma = \sigma_1 \cdots \sigma_r$. Ainsi, toute permutation se décompose en produit de cycles à supports disjoints. De plus, la décomposition est unique à l'ordre des facteurs près.

Corollaire 9. *Soit $\sigma \in \mathfrak{S}_n$, que l'on décompose en $\sigma = c_1 \cdots c_k$ produit de cycles à supports disjoints. Alors l'ordre de σ est le PPCM des ordres des c_i.*

Exemple 10.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 1 & 9 & 4 & 6 & 3 & 8 & 2 \end{pmatrix}$$

Sa décomposition en cycles disjoints est $\sigma = (1\ 7\ 3) \circ (2\ 5\ 4\ 9)$ et σ est d'ordre 12.

Proposition 11. *Pour $n \geqslant 3$, le centre de $\mathfrak{S}_n$ est trivial.*

Proposition 12.

1. *Soit $\sigma = (a_1 \cdots a_k)$ un cycle et $\tau \in \mathfrak{S}_n$. Alors le conjugué de σ par τ est : $\tau\sigma\tau^{-1} = \big(\tau(a_1) \cdots \tau(a_k)\big)$.*
2. *Dans $\mathfrak{S}_n$, les k–cycles sont conjugués.*

Proposition 13 (générateurs de $\mathfrak{S}_n$)**.** *Le groupe $\mathfrak{S}_n$ est engendrés par les familles suivantes :*

1. *l'ensemble de toutes les transpositions ;*
2. *l'ensemble des transpositions de la forme $(1\ i)$ pour i de 2 à n ;*
3. *l'ensemble des transpositions de la forme $(i\ i+1)$ pour i de 1 à n.*

2 Le groupe alterné

Théorème 14. *Il existe un unique morphisme non trivial de $\mathfrak{S}_n$ dans $\mathbf{C}^*$. On l'appelle la signature et on la note ε.*

Remarque 15. La signature est donnée par $\varepsilon(\sigma) = \prod_{i<j} \frac{\sigma(i)-\sigma(j)}{i-j}$.

Proposition 16.

1. *Les transpositions sont de signature* -1.
2. *Si* σ *est un k–cycle, alors* $\varepsilon(\sigma) = (-1)^{k+1}$.
3. *Si* $\sigma = c_1 \cdots c_k$ *avec les* c_i *des cycles de longueur* ℓ_i*, alors :*

$$\varepsilon(\sigma) = \prod_{i=1}^{k} (-1)^{\ell_i}$$

Exemple 17.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 5 & 1 & 9 & 4 & 6 & 3 & 8 & 2 \end{pmatrix}$$

Alors $\varepsilon(\sigma) = 1$.

Définition 18. On appelle groupe alterné le noyau de la signature. On le note $\mathfrak{A}_n$.

Proposition 19. *Si* $n \geqslant 2$*, le cardinal de* $\mathfrak{A}_n$ *est* $\frac{n!}{2}$.

Proposition 20 (générateurs de $\mathfrak{A}_n$)**.**

1. $\mathfrak{A}_n$ *est engendré par les produits de deux transpositions.*
2. *Pour* $n \geqslant 3$, $\mathfrak{A}_n$ *est engendré par les* 3*–cycles.*
3. *Pour* $n \geqslant 3$, $\mathfrak{A}_n$ *est engendré par les* $(1\ 2\ i)$ *pour* i *de* 3 *à* n.

Lemme 21. *Soient* $a_1, \ldots, a_{n-2}$ *et* $b_1, \ldots, b_{n-2}$ *deux listes d'éléments distincts de* $\{1, \ldots n\}$*. Alors il existe* $\sigma \in \mathfrak{A}_n$ *tel que* $\sigma(a_i) = b_i$.

Théorème 22. *Pour* $n \geqslant 5$, $\mathfrak{A}_n$ *est un groupe simple.*

Exemple 23 (Structure de $\mathfrak{A}_4$)**.** $\mathfrak{A}_4$ possède 12 éléments :
- le neutre ;
- les doubles transpositions (éléments d'ordre 2) : $(1\ 2)(3\ 4)$, $(1\ 3)(2\ 4)$ et $(1\ 4)(2\ 3)$;
- les 3–cycles : $(1\ 2\ 3)$, $(1\ 3\ 2)$, $(1\ 2\ 4)$, $(1\ 4\ 2)$, $(1\ 3\ 4)$, $(1\ 4\ 3)$, $(2\ 3\ 4)$ et $(2\ 4\ 3)$.

Faisons la liste de ses sous-groupes :
- $\{\mathrm{id}\}$ et $\mathfrak{A}_4$;
- il n'y a pas de sous-groupes d'ordre 6 ;
- il y a un sous-groupe d'ordre 4 (les doubles transpositions + le neutre) noté V_4 qui est distingué ;
- il y a 4 sous-groupes d'ordre 3 qui sont engendrés par les 3–cycles et qui sont conjugués (les 3–Sylow) ;
- il y 3 sous-groupes d'ordre 2 engendrés par chacune des doubles transpositions et qui sont conjugués.

3 Sous-groupes et automorphismes de $\mathfrak{S}_n$

Proposition 24. *Le seul sous-groupe de* $\mathfrak{S}_n$ *d'indice 2 est* $\mathfrak{A}_n$.

Théorème 25 (Cayley)**.** *Tout groupe fini de cardinal n est isomorphe à un sous-groupe de* $\mathfrak{S}_n$.

Remarque 26. Ce théorème est la première étape d'une démonstrations des théorèmes de Sylow.

Théorème 27. *Pour* $n \geqslant 5$*, le sous-groupe dérivé de* $\mathfrak{A}_n$ *est* $\mathfrak{A}_n$ *et pour* $n \geqslant 2$*, le sous-groupe dérivé de* $\mathfrak{S}_n$ *est* $\mathfrak{A}_n$.

Théorème 28. *Pour* $n \geqslant 5$*, les sous-groupes distingués de* $\mathfrak{S}_n$ *sont* $\{\mathrm{id}\}$, $\mathfrak{A}_n$ *et* $\mathfrak{S}_n$.

Corollaire 29. *Tout sous-groupe de* $\mathfrak{S}_n$ *d'indice n est isomorphe à* $\mathfrak{S}_{n-1}$.

Lemme 30. *Si un automorphisme de* $\mathfrak{S}_n$ *transforme toute transposition en transposition, alors il est intérieur.*

Théorème 31. *Pour* $n \neq 6$*, les automorphismes de* $\mathfrak{S}_n$ *sont tous intérieurs.*

4 Polynômes symétriques

définition, polynômes symétriques élémentaires, exemples pour $n = 3$, relations coefficients/racines, théorème de structure, sommes de Newton.

Développements

1. $\mathfrak{A}_n$ est simple pour $n \geqslant 5$. **[22]**
2. Pour $n \neq 6$, $\mathrm{Aut}(\mathfrak{S}_n) = \mathrm{Int}(\mathfrak{S}_n)$. **[31]**

Références

- Combes, *Algèbre et géométrie.*
- Cortella, *Théorie des groupes.*
- Perrin, *Cours d'algèbre.*
- Ramis, Deschamps et Odoux, *Cours de mathématiques spéciales tome 1 : algèbre.*
- Zavidovique, *Un Max de Math.*