105 - Groupe des permutations d'un ensemble fini. Applications.

1 Définitions et généralités

Définition 1. L'ensemble des bijections d'un ensemble dans lui-même forme un groupe pour la composition, appelé *groupe des permutations* de E, et noté $\mathfrak{S}(E)$. Le groupe des permutations de $[|1,n|]$ est noté $\mathfrak{S}_n$.

Proposition 1. $|\mathfrak{S}_n| = n!$

Proposition 2. *Si $f : E \to F$ est une bijection, alors on a la bijection $\mathfrak{S}(E) \to \mathfrak{S}(F); \sigma \mapsto f \circ \sigma \circ f^{-1}$. En particulier $\mathfrak{S}(E) \approx \mathfrak{S}_{|E|}$.*

Proposition 3. *Deux permutations à supports disjoints commutent.*

Remarque. Toute action de groupe d'un groupe G vers un ensemble E est donnée par le morphisme $\varphi : G \to \mathfrak{S}(E)$ défini par $\varphi(g) = (x \mapsto g.x)$.

Théorème 1 (Cayley)**.** *Tout groupe d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$*

2 Cycles et décompositions

Définition 2. Une permutation de la forme $(a_1 \dots a_k)$, avec $a_1, \dots, a_k$ une famille d'éléments de $[|1,n|]$ deux à deux distincts, est appelée un k-cycle. Un 2-cycle est appelé une transposition.

Remarque. Un l-cycle est d'ordre l.

Remarque. Le groupe $\mathfrak{S}_n$ agit naturellement sur l'ensemble $[|1,n|]$ (par spécialisation). Cette action est transitive.

Proposition 4. *Toute permutation se décompose de manière unique en produit de cycles à supports disjoints (à l'ordre près des cycles).*
Toute permutation se décompose en produit de transpositions.

Exemple. Nombre de dérangements.

Proposition 5. *Soit $\sigma = \sigma_1 \dots \sigma_k$ la décomposition de σ en produit de cycles à supports disjoints. Alors l'ordre de σ est le ppcm des ordres des σ_i.*

Application. $\mathfrak{S}_5$ ne possède pas d'élément d'ordre 15.

Proposition 6. *Soient $(a_1 \dots a_k)$ un k-cycle, et $\sigma \in \mathfrak{S}_n$. Alors $\sigma(a_1 \dots a_k)\sigma^{-1} = (\sigma(a_1) \dots \sigma(a_k))$.*

Corollaire 1. *Deux permutations sont conjuguées ssi les ensembles des longueurs des cycles apparaissant dans leurs décompositions en cycles à supports disjoints sont égaux.*

Application. Le nomrbre de classes de conjugaison dans $\mathfrak{S}_n$ est égal au mombre de manières d'écrire n sous la forme $n = 1k_1 + 2k_2 + ... + nk_n$.

Exemple. Les classes de conjugaison dans $\mathfrak{S}_5$ sont données par les représentants $Id, (1,2), (123), (1234), (12345), (12)(34), (123)(45)$.

Exemple (Parties génératrices). Les parties suivantes génèrent $\mathfrak{S}_n$: $\{(1\ i) \mid 2 \leq i \leq n\}$, $\{(i-1\ i) \mid 2 \leq i \leq n\}$, $\{(1\ 2), (2 \dots n)\}$. Elles sont de plus minimales. Une partie génératrice formée de transpositions est de cardinal au moins $n-1$.

Proposition 7. *Si $n \geq 3$, alors $Z(\mathfrak{S}_n) = \{1\}$.*

Théorème 2. *Si $n \neq 6$, alors $Aut(\mathfrak{S}_n) = Int(\mathfrak{S}_n)$. D'autre part, $Aut(\mathfrak{S}_6)/Int(\mathfrak{S}_6) \approx \mathbf{Z}/2\mathbf{Z}$.*

3 Signature et groupe alterné

Théorème 3. *Il existe un unique morphisme non trivial de $\mathfrak{S}_n$ dans $\mathbf{C}^*$, appelé* signature *et noté ε. Il est à valeurs dans $\{-1, 1\}$ et on a :*

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

Définition 3. On appelle *nombre d'inversions* de $\sigma \in \mathfrak{S}_n$, et note $I(\sigma)$, le nombre de couples (i, j) tels que $i < j$ et $\sigma(i) > \sigma(j)$.

Proposition 8. $\varepsilon(\sigma) = (-1)^{I(\sigma)}$

Remarque. La signature d'une transposition est -1, celle d'un l-cycle est $(-1)^{l-1}$.

Définition 4. Si $\varepsilon(\sigma) = 1$, on dit que σ est *paire*, et si $\varepsilon(\sigma) = -1$, on dit que σ est *impaire*. L'ensemble des permutations paires est appelé *groupe alterné* et est noté $\mathfrak{A}_n$.

Remarque. $\mathfrak{A}_n$ est un sous-groupe distingué d'indice 2 de $\mathfrak{S}_n$.

Proposition 9. *Si $n \geq 3$, alors $Z(\mathfrak{A}_n) = \{1\}$.*
$\mathfrak{A}_n$ est le seul groupe d'indice 2 de $\mathfrak{S}_n$.
Si $n \geq 3$, alors $\mathfrak{A}_n$ est engendré par les 3-cycles.
$\mathfrak{A}_n$ est $n-2$ fois transitif sur $[|1, n|]$. Ainsi pour tout $n \geq 5$, tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$.
On peut plonger $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+2}$ [FGN p.68].

Théorème 4. *Si $n \geq 5$, alors $\mathfrak{A}_n$ est simple.*

Proposition 10. *Pour $n \geq 5$, $D(\mathfrak{A}_n) = D(\mathfrak{S}_n) = \mathfrak{A}_n$.*

Application ([Per p.30]). Tout groupe d'indice n de $\mathfrak{S}_n$ est isomorphe à $\mathfrak{S}_{n-1}$. On ne peut pas plonger $\mathfrak{S}_n$ dans $\mathfrak{A}_{n+1}$.

Corollaire 2. *Si $n \geq 5$, alors $\mathfrak{S}_n$ n'est pas résoluble.*

Application. Il existe des équations polynomiales non résolubles par radicaux.

4 Applications

4.1 Déterminant

On considère un anneau commutatif et unitaire $\mathcal{A}$ ainsi qu'un $\mathcal{A}$-module libre M de rang $n \in \mathbf{N}$.

Définition 5. Soit $e = (e_1, ..., e_n)$ une base de M et $x = (x_1, ..., x_n) = (\sum_{i=1}^n a_{ij} e_i)_{j=1...n} \in M^n$. On appelle *déterminant* de x dans la base e la quantité $\det_e(x) = \sum_{\sigma \in \mathfrak{S}_n} \epsilon(\sigma) \prod_{i=1}^n a_{i,\sigma(i)}$.

Proposition 11. *Unique forme n-linéaire alternée.*

Proposition 12. *Déterminant d'un endomorphisme.*

Proposition 13. *Commutativité...*

Théorème 5 (Frobénius-Zolotarev)**.** *Soit p un nombre premier impair et V un $\mathbf{F}_p$-e.v. de dimension finie. Alors pour tout $u \in Gl(V)$, on peut considérer u comme un élément de $\mathfrak{S}(V)$, si bien qu'on peut lui associer sa signature. On a alors $\varepsilon(u) = \left(\frac{det(u)}{p}\right)$.*

4.2 Matrices de permutation

Définition 6. Matrice de permutation par changement de base.

Remarque. D'où action de $\mathfrak{S}_n$ sur M_n.

Proposition 14. *$\mathfrak{S} \to Gl_n$, $\sigma \mapsto P_\sigma$ est un morphisme de groupes vérifiant $\det P_\sigma = \varepsilon\sigma$.*

Application (théorème de Sylow). On pose $|G| = p^\alpha m$, avec $p \wedge m = 1$ et $\alpha \in \mathbf{N}^*$. On note $S_p(G)$ l'ensemble des p-sous-groupes de Sylow de G. Alors

1. $S_p(G) \neq \emptyset$.
2. Si H est un p-sous-groupe de G, alors il est inclus dans un p-Sylow.
3. Les p-Sylow sont tous deux à deux conjugués.
4. $|S_p(G)| \mid m$ et $|S_p(G)| \equiv 1\ [p]$.

Théorème 6 (Décomposition de Bruhat)**.** *[Fgn1 p. 34 7].*

Théorème 7 (Brauer)**.** *Cf Beck.*

4.3 Polynômes symétriques

A intègre.

Définition 7. Action du groupe symétrique, polynôme symétrique, antisymétrique. $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$, $A[X_1, \ldots, X_n]^{\mathfrak{A}_n}$.

Définition 8. Polynômes symétriques élémentaires.

Proposition 15. *Relations coefficients-racines dans $A[X_1, \ldots, X_n][T]$. Applications aux polynômes.*

Application. Kronecker.

Application. Calcul de $\zeta(2)$ [FGN].

Application. D'Alembert-Gauss par Samuel.

Théorème 8. *$\varphi : A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_n]$; $P \mapsto P(\sigma_1, \ldots, \sigma_n)$ est un morph de A-alg injectif d'image $A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$.*

Avec l'algorithme !

Proposition 16 (Formules de Newton)**.**

Remarque. Inversion des sommes en carac nulle.

Application. χ_u déterminé par les ${}^t u^i$. En particulier pour les mat nilpotentes. Ths p.6 et 94 Mneimné.

Proposition 17. *Si $car(K) \neq 2$, $A[X_1, \ldots, X_n]^{\mathfrak{A}_n} = A[X_1, \ldots, X_n]^{\mathfrak{S}_n} + D(X_1, \ldots, X_n)A[X_1, \ldots, X_n]^{\mathfrak{S}_n}$.*

4.4 Groupe diédral [Cal]

Définition 9. Comme un groupe d'isométries de polygone.

Proposition 18. *Cardinal, générateurs, semi direct...*

Proposition 19. *Injection dans $\mathfrak{S}_n$. $D_3 \simeq \mathfrak{S}_3$. Image : cycle et produit de transpositions.*