105 Groupe des permutations d'un ensemble fini. Applications

E un ensemble fini, $\mathrm{card}(E) = n \geq 1$

I. Définitions, premières propriétés

1. Généralités

Def : . On appelle permutation de E une bijection de E sur lui-même. L'ensemble des permutations de E, muni de la loi de composition, est un groupe, appelé groupe symétrique et noté $\mathfrak{S}_E$

. On note $\mathfrak{S}_n$ le groupe symétrique de $\{1, \dots n\}$. On dit que $\mathfrak{S}_n$ est le groupe symétrique de degré n

Prop : $\mathrm{Card}(\mathfrak{S}_n) = n!$

Prop : Tout groupe fini G est isomorphe à un sous groupe de $\mathfrak{S}_G$

Exemple 1 : permutation de $\mathfrak{S}_4$ $s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$

2. Orbites, transpositions, cycles

Pour $x \in E$ et $s \in \mathfrak{S}_E$ on note $O_s(x) = \{s^k(x), k \in \mathbb{Z}\}$

Def : $O_s(x)$ est la s-orbite de x

Exemple 2 : les s-orbites de l'exemple 1 sont $O_s(1) = O_s(2) = O_s(3) = \{1,2,3\}$
$O_s(4) = \{4\}$

Def : . On dit que $s \in \mathfrak{S}_E$ est un cycle s'il existe une unique s-orbite O telle que $\mathrm{card}(O) > 1$

. Le cardinal de O est appellé la longueur du cycle et O son support

. Un p-cycle est un cycle de longueur p

. Un 2-cycle est appellé transposition

Prop : Soient $s \in \mathfrak{S}_E$ et O une s-orbite de cardinal p

(i) $s(O) = O$ et la restriction de s à O est une permutation de O

(ii) Si $p > 1$ $s(x) \neq x$ $\forall x \in O$

(iii) Si $p > 1$ et $a \in O$ on a $O = \{a, s(a), \dots s^{p-1}(a)\}$ et $s^p(x) = x$ $\forall x \in O$

Rq : Un p-cycle est un élément d'ordre p du groupe $\mathfrak{S}_E$

Prop : Soient $c = (i_1, \dots i_p)$ un p-cycle et $s \in \mathfrak{S}_E$, alors scs^{-1} est le cycle $c' = (s(i_1), \dots s(i_p))$. Deux p-cycles sont conjugués dans $\mathfrak{S}_E$

Exemple 3 : $c = (1\,2\,3)$ et $c' = (1\,2\,4)$ sont conjugués dans $\mathfrak{S}_4$
$[4\,3]\, c\, [4\,3]^{-1} = c'$

Prop : Deux cycles de $\mathfrak{S}_E$ à supports disjoints commutent

Rq : Si $n \geq 3$ le centre Z de $\mathfrak{S}_E$ est $\{id\}$ et $\mathfrak{S}_E$ n'est pas abélien

Thm : (i) Tout $s \in \mathfrak{S}_E \setminus \{id\}$ est produit de cycles de supports deux à deux disjoints et un tel produit est unique à l'ordre près des facteurs

(ii) Si $\mathrm{card}(E) > 1$, toute permutation est produit de transpositions

Def : On appelle transposition simple de $\mathfrak{S}_n$ toute transposition de la forme $(i, i+1)$ $1 \leq i \leq n-1$

Cor : Si $n \geq 2$, $\mathfrak{S}_n$ est engendré par l'un des ensembles suivants

(i) les transpositions $(1, i)$ $2 \leq i \leq n$

(ii) les transpositions simples

(iii) la transposition $(1\,2)$ et le n-cycle $s = (1\,2 \dots n)$

Exemple 4 : $s \in \mathfrak{S}_6$ $s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 3 & 2 & 1 \end{pmatrix}$

$s = (1\;4\;3\;6)(2\;5)$

$s = [1\,2][2\,3][3\,4][2\,3][1\,2][4\,5][5\,6][4\,5][3\,4][2\,3]$
$[3\,4][4\,5][3\,4][2\,3]$

Prop : On suppose $\mathrm{Card}(E) \geq 2$

(i) pour $2 \leq p \leq n$ le nombre de p-cycles dans $\mathfrak{S}_E$ est égal à $(p-1)!\, C_n^p$

(ii) Si n est un nombre premier, $\mathfrak{S}_n$ contient exactement $(n-1)!$ éléments d'ordre n

3. Signature, groupe alterné

Def : Soient $s \in \mathfrak{S}_E$ et $m(s)$ le nombre de s-orbite. On appelle signature de s l'élément $\varepsilon(s) \in \{-1, 1\}$ défini par
$\varepsilon(s) = (-1)^{\mathrm{card}(E) - m(s)}$

Rq : On a $\varepsilon(id) = 1$ et $\varepsilon(s) = (-1)^{p-1}$ pour un p-cycle
$\varepsilon(\tau) = -1$ pour une transposition

Thm : (i) Si $s \in \mathfrak{S}_E$ est produit de p transpositions alors $\varepsilon(s) = (-1)^p$

(ii) L'application $\varepsilon : \mathfrak{S}_E \to \{-1, 1\}$, $s \mapsto \varepsilon(s)$ est un homomorphisme surjectif de groupe pour $n \geq 2$

(iii) Pour $n \geq 2$ et $s \in \mathfrak{S}_n$ $\varepsilon(s) = \prod_{1 \leq i < j \leq n} \frac{s(i) - s(j)}{i - j}$

Def : . Le noyau de l'homomorphisme ε est appelé le groupe alterné de E et est noté $\mathcal{A}_E$

. Un élément de $\mathcal{A}_E$ (resp $\mathfrak{S}_E \setminus \mathcal{A}_E$) est appelé permutation paire (resp impaire)

II. Structure des groupes symétrique et alterné

1. Autour du groupe alterné

Prop : L'ensemble $\mathcal{A}_n$ est un sous-groupe caractéristique d'indice 2 de $\mathfrak{S}_n$. C'est le seul sous-groupe d'indice 2 de $\mathfrak{S}_n$

Rq : $\mathrm{Card}(\mathcal{A}_n) = \frac{n!}{2}$

Prop : Soit $n \geq 3$

(i) le groupe $\mathcal{A}_n$ est engendré par les permutations $(1\,i)(1\,j)$ $2 \leq i, j \leq n$

(ii) le groupe $\mathcal{A}_n$ est engendré par les 3-cycles de la forme $(1\,2\,i)$ $3 \leq i \leq n$

(iii) le groupe $\mathcal{A}_n$ est engendré par les éléments $s^2, s \in \mathcal{A}_n$

Cor : Pour $n \geq 3$ $c_i = (i, i+1, i+2)$ $1 \leq i \leq n-2$ engendrent $\mathcal{A}_n$

Prop : Pour $n \geq 5$ les 3-cycles sont conjugués dans $\mathcal{A}_n$

Rq : $\gamma = (1\,2\,3)$ et $\gamma^2 = (1\,3\,2)$ ne sont pas conjugués dans $\mathcal{A}_3$ et $\mathcal{A}_4$

Thm : Pour $n \geq 5$ $\mathcal{A}_n$ est simple

Thm : Si $n \neq 4$ les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\mathfrak{S}_n$, $\mathcal{A}_n$ et $\{id\}$

2. Resolubilité

G un groupe de cardinal fini

Def : . Si $x, y \in G$ on appelle commutateur de x et y l'élément $[x,y] = xyx^{-1}y^{-1}$ de G

. Le groupe dérivé de G noté $D(G)$ est le sous-groupe de G engendré par les commutateurs d'éléments de G

$D(G) = \{xyx^{-1}y^{-1},\ x, y \in G\}$

. On appelle suite dérivée de G la suite $(D^n(G))_{n \geq 0}$ de sous-groupes de G définie par $D^0(G) = G$ et $D^{n+1}(G) = D(D^n(G))$

Def : On dit que G est resoluble s'il existe $n \in \mathbb{N}$ tel que $D^n(G) = \{e\}$

Prop : . $D(\mathcal{A}_n) = \mathcal{A}_n$ pour $n \geq 5$

. $D(\mathfrak{S}_n) = \mathcal{A}_n$ pour $n \geq 2$

Thm : le groupe $\mathfrak{S}_n$ n'est pas résoluble ssi $n \geq 5$

III. Applications

1. A l'algèbre linéaire

* Déterminant

Soit E un $\mathbb{K}$-ev de dimension finie

Def : Soit f une application n-linéaire sur E à valeur dans $\mathbb{K}$

. f est alternée si $f(x_1, \dots x_n) = 0$ dès que deux vecteurs parmi les x_i sont égaux

. f est antisymétrique si pour tout $\sigma \in \mathfrak{S}_n$ et pour tout $(x_1, \dots x_n) \in E^n$ on a $f(x_{\sigma(1)}, \dots x_{\sigma(n)}) = \varepsilon(\sigma) f(x_1, \dots x_n)$

Soit $\mathcal{B} = (e_1, \dots e_n)$ une base de E et $x_i = \sum_{j=1}^{n} x_{ij} e_j$

Def : On appelle déterminant de $x_1, \dots x_n$, dans la base $\mathcal{B}$, la n-forme linéaire alternée définie par

$$\det_{\mathcal{B}}(x_1, \dots x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\, x_{1,\sigma(1)} \cdots x_{n,\sigma(n)}$$

Thm : (Frobenius - Zolotarev)

Soient p un nombre premier ≥ 3, $\mathbb{F}_p$ le corps fini à p éléments et V un $\mathbb{F}_p$-ev de dimension finie.

Alors pour tout $u \in GL(V)$ on a $\varepsilon(u) = \left(\frac{\det u}{p}\right)$

où $\left(\frac{\cdot}{\cdot}\right)$ est le symbole de Legendre

* Matrices de permutation

Def : On appelle matrice de permutation associée à $\sigma \in \mathfrak{S}_n$ la matrice $P_\sigma \in M_n(\mathbb{K})$ définie par $P_\sigma = (\delta_{i,\sigma(j)})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$

Thm : (Brauer)

Soient $\sigma, \tau \in \mathfrak{S}_n$. σ et τ sont conjuguées dans $\mathfrak{S}_n$ ssi P_σ et P_τ sont des matrices semblables de $M_n(\mathbb{K})$

2. Aux polynômes symétriques

Soit $\mathbb{K}$ un corps de caractéristique $\neq 2$, $\mathbb{K}[X_1, \dots X_n]$ l'anneau des polynômes à n indéterminées

Def : Soit φ l'action de $\mathfrak{S}_n$ sur $\mathbb{K}[X_1, \dots X_n]$ telle que

$$\varphi_\sigma(P(X_1, \dots X_n)) = P(X_{\sigma(1)}, \dots X_{\sigma(n)}) \quad \sigma \in \mathfrak{S}_n$$

Def : Soit $P \in \mathbb{K}[X_1, \dots X_n]$, on dit que
- P est symétrique si $\forall \sigma \in \mathfrak{S}_n \ \varphi_\sigma(P) = P$
- P est semi-symétrique si $\forall \sigma \in \mathcal{A}_n \ \varphi_\sigma(P) = P$
- P est alterné si $\forall \sigma \in \mathfrak{S}_n \ \varphi_\sigma(P) = \varepsilon(\sigma) P$

Exemple S : $P = XY + YZ + XZ$ est symétrique sous l'action de $\mathfrak{S}_3$

$P = X - Y$ est alterné sous l'action de $\mathfrak{S}_2$

Rq : P alterné $\Rightarrow$ P semi-symétrique

Prop : Soit $F \in \mathbb{K}[X_1, \dots X_n]$

F est semi-symétrique ssi il existe un unique couple $(P,Q) \in \mathbb{K}[X_1, \dots X_n]^2$ symétriques tels que

$$F(X_1, \dots X_n) = P(X_1, \dots X_n) + D(X_1, \dots X_n)\, Q(X_1, \dots X_n)$$

où $D(X_1, \dots X_n) = \det \begin{pmatrix} 1 & \cdots & 1 \\ X_1 & \cdots & X_n \\ \vdots & & \vdots \\ X_1^{n-1} & \cdots & X_n^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (X_j - X_i)$

3. A la géométrie

Prop : Soit G un sous-groupe fini de $SO(3)$ d'ordre $n \geq 2$.

Alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$, $D_{n/2}$, $\mathcal{A}_4$, $\mathfrak{S}_4$ ou $\mathcal{A}_5$

Prop :
- le groupe des isométries (resp déplacement) préservant le tétraèdre régulier est isomorphe à $\mathfrak{S}_4$ (resp $\mathcal{A}_4$)
- le groupe des isométries préservant le cube est $\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$

Références :
- Tauvel Algèbre
- Perrin Cours d'Algèbre
- Combes Algèbre et Geométrie
- Gourdon Algèbre
- Objectif Agrégation
- Goblot Algèbre commutative