Algèbre 06 – Groupes des permutations d'un ensemble fini. Applications.

On considère un ensemble E de cardinal fini $n \geq 2$ et on note $\mathbb{N}_n = \{1, \dots, n\}$.

1. Définition et généralités

Définition. On note $\mathcal{S}(E)$ l'ensemble des *permutations de E i.e.* des bijections de E dans E.

Si $E = \mathbb{N}_n$, on note $\mathcal{S}(E) = \mathcal{S}_n$ et pour $\sigma \in \mathcal{S}_n$:

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

Proposition. *$\mathcal{S}(E)$ et $\mathcal{S}_n$ sont des groupes (pour la loi $\circ$ de composition) isomorphes, d'ordre $n!$.*

On dit que $\mathcal{S}_n$ est le *groupe symétrique* d'ordre n.

Exemple. $\mathcal{S}_3$ n'est pas abélien et c'est le seul (à isomorphisme près) groupe non abélien d'ordre 6.

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

Définition. Le *support* d'une permutation $\sigma \in \mathcal{S}_n$ est l'ensemble $\{k \in \mathbb{N}_n ; \sigma(k) \neq k\}$.

Proposition. *Deux permutations à supports disjoints commutent.*

Définition. Si $\sigma \in \mathcal{S}_n$ et $i \in \mathbb{N}_n$, on appelle *σ-orbite* de i, l'ensemble $\Omega_{\sigma(i)} = \{\sigma^r(i), r \in \mathbb{Z}\}$.

Définition. On dit que $\gamma \in \mathcal{S}_n$ est un *p-cycle* s'il existe une unique σ-orbite non ponctuelle et que celle-ci est de cardinal p ; il s'agit du support de γ.
Les 2-cycles sont appelés *transpositions*.

Si γ est un p-cycle dont l'unique orbite non triviale est $\{j_1, \dots, j_p\}$, on note $\gamma = (j_1 \ \cdots \ j_p)$.

Proposition. *Un p-cycle est d'ordre p.*

Proposition. *Soit $\gamma = (j_1 \ \cdots \ j_p)$ et $\sigma \in \mathcal{S}_n$ alors*

$$\sigma\gamma\sigma^{-1} = (\sigma(j_1) \ \cdots \ \sigma(j_p)).$$

Si γ' est un autre p-cycle alors il existe $\psi \in \mathcal{S}_n$ tel que $\gamma' = \psi\gamma\psi^{-1}$.

2. Étude algébrique du groupe symétrique

2.1. Générateurs de $\mathcal{S}_n$.

Proposition. *Toute permutation $\sigma \neq \mathrm{id}$ se décompose de façon unique sous la forme d'un produit de cycles à supports disjoints.*

Exemple. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} = (1\ 3\ 4)(2\ 5)$

Proposition. *Si $\sigma = \gamma_1 \cdots \gamma_r$ est une permutation décomposée sous la forme d'un produit de cycles à supports disjoints alors l'ordre de σ est le ppcm des ordres des γ_i.*

Remarque. $\mathcal{S}_n$ est engendré par $(1\ 2)$ et $(1\ 2\ \cdots\ n)$.

Proposition. *Les transpositions engendrent $\mathcal{S}_n$.*

Remarque. On peut même se limiter aux transpositions de la forme $(i\ i+1)$ ou aux transpositions de la forme $(1\ i)$.

Remarque. Si $\tau_1, \dots, \tau_k$ sont des transpositions qui engendrent $\mathcal{S}_n$ alors $k \geq n-1$.

Exemple. $(1\ 2\ 3) = (1\ 3)(1\ 2) = (2\ 3)(1\ 2)(2\ 3)(1\ 2)$

2.2. Signature et groupe alterné.

Définition et proposition. Il existe un unique morphisme surjectif de $\mathcal{S}_n$ sur $\{-1, +1\}$ appelé *signature* et noté ε. On appelle
- *groupe alterné* d'ordre n le noyau $\mathcal{A}_n = \ker \varepsilon$
- *permutation paire* tout $\sigma \in \mathcal{S}_n$ avec $\varepsilon(\sigma) = 1$
- *permutation impaire* tout $\sigma \in \mathcal{S}_n$ avec $\varepsilon(\sigma) = -1$

Remarque. $\mathcal{A}_n$ est le seul sous-groupe d'indice 2 de $\mathcal{S}_n$.

Exemple. $\varepsilon((j_1 \ \cdots \ j_p)) = (-1)^{p-1}$

Proposition. *Si $\sigma \in \mathcal{S}_n$ alors* $\varepsilon(\sigma) = \prod_{i<j} \dfrac{\sigma(j) - \sigma(i)}{j - i}$

i.e. $\varepsilon(\sigma)$ est le nombre d'inversions présentées par σ.

Proposition. *$\mathcal{A}_n$ est un groupe d'ordre $\frac{n!}{2}$ engendré par les 3-cycles.*

Remarque. On peut même se limiter aux 3-cycles de la forme $(i\ i+1\ i+2)$.

Remarque. $\mathcal{A}_4$ est un groupe d'ordre 12 qui n'a pas de sous-groupe d'ordre 6.

Proposition. *Si $n \geq 5$ et si γ et γ' sont des 3-cycles alors il existe $\sigma \in \mathcal{A}_n$ tel que $\gamma' = \sigma\gamma\sigma^{-1}$.*

2.3. Sous-groupes de $\mathcal{S}_n$.

Proposition. *Si $n \geq 3$ alors $Z(\mathcal{S}_n) = \{\mathrm{id}\}$ i.e. $\mathcal{S}_n$ n'est pas abélien.*

Proposition. *$\mathcal{A}_5$ est le seul (à isomorphisme près) groupe simple d'ordre 60.*

Proposition. *Si $n \geq 5$ alors $\mathcal{A}_n$ est simple.*

Corollaire. *Si $n \geq 5$ alors $D(\mathcal{A}_n) = \mathcal{A}_n$ et $\mathcal{A}_n$ est le seul sous-groupe distingué non trivial de $\mathcal{S}_n$.*

Remarque. $D(\mathcal{A}_4) = \{\mathrm{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ et $D(\mathcal{A}_3) = \{\mathrm{id}\}$.

3. Quelques actions du groupe symétrique

3.1. Polynômes symétriques.

On considère l'action de $\mathcal{S}_n$ sur $\mathbb{K}[T_1, \dots, T_n]$ définie par $\sigma \cdot f(T_1, \dots, T_n) = f(T_{\sigma(1)}, \dots, T_{\sigma(n)})$.

Définition. On dit que $f \in \mathbb{K}[T_1, \dots, T_n]$ est

(*i*) *symétrique* si $\sigma \cdot f = f$ pour tout $\sigma \in \mathcal{S}_n$,

(*ii*) *alterné* si $\sigma \cdot f = \varepsilon(\sigma) f$ pour tout $\sigma \in \mathcal{S}_n$,

(*iii*) *semi-symétrique* si $\sigma \cdot f = f$ pour tout $\sigma \in \mathcal{A}_n$.

Exemple. Le k-è polynôme symétrique élémentaire est $\Sigma_k = \sum_{i_1 < \cdots < i_k} T_{i_1} \cdots T_{i_k}$.

Exemple. $V(T_1,\dots,T_n)=\prod_{i<j}(T_j-T_i)$ est alterné.

Proposition. *Si f est symétrique alors il existe g unique tel que $f(T_1,\dots,T_n)=g(\Sigma_1,\dots,\Sigma_n)$.*

Exemple. $X^3+Y^3+Z^3=\Sigma_1^3-3\Sigma_1\Sigma_2+3\Sigma_3$

Application. Un sous-groupe G de $GL_n(\mathbb{C})$ est fini si et seulement s'il est de torsion et de type fini.

Proposition. *Si f est semi-symétrique alors il existe g,h symétriques uniques tels que $f=g+Vh$.*

3.2. **Matrices de permutations.**
On considère l'action de $\mathcal{S}_n$ sur les bases $(e_1,\dots,e_n)$ de $\mathbb{R}^n$ définie par $\sigma\cdot(e_1,\dots,e_n)=(e_{\sigma(1)},\dots,e_{\sigma(n)})$.
On dit que la matrice de passage correspondante est une *matrice de permutation* et est notée P_σ.
Notons que $P_{\sigma_1\sigma_2}=P_{\sigma_2}P_{\sigma_1}$ pour tous $\sigma_1,\sigma_2\in\mathcal{S}_n$, d'où

Proposition. $P_\sigma^{-1}=P_{\sigma^{-1}}$ *et* $\det P_\sigma=\varepsilon(\sigma)$.

Théorème de Brauer. *P_σ et P_ψ sont conjuguées dans $GL_n(\mathbb{R})$ si et seulement si σ et ψ sont conjuguées dans $\mathcal{S}_n$.*

Proposition (décomposition de Bruhat)**.** *Toute matrice $A\in GL_n(\mathbb{R})$ s'écrit de façon unique $A=T_1P_\sigma T_2$ avec $\sigma\in\mathcal{S}_n$ et T_1,T_2 triangulaires supérieures inversibles.*

Définition. On dit que $A=(a_{i,j})_{1\le i,j\le n}\in\mathcal{M}_n(\mathbb{R})$ est *bistochastique* si, pour tous i,j, on a $a_{i,j}\ge 0$ et

$$\sum_{k=1}^n a_{k,j}=\sum_{\ell=1}^n a_{i,\ell}=1\ .$$

Exemple. Soit X et Y deux v.a.r. à valeurs dans $\{1,\dots,n\}$ alors la matrice $(a_{i,j})_{1\le i,j\le n}$, où $a_{i,j}=P(Y=j|X=i)$, est bistochastique.

Théorème de Birkhoff. *L'ensemble des matrices bistochastiques est compact convexe et ses points extrémaux sont les matrices de permutation.*

Donc l'ensemble des matrices bistochastiques est l'enveloppe convexe de l'ensemble des matrices de permutation.

Proposition. *Si A est bistochastique alors il n'existe pas de sous-matrice nulle de A de taille $(r,n+1-r)$.*

4. Quelques applications

4.1. **Déterminant et permanent.**
Soit E un $\mathbb{K}$-espace vectoriel de dimension n.

Proposition. *L'ensemble des formes n-linéaires alternées sur E est un $\mathbb{K}$-e.v. de dimension* 1.

Définition et proposition. Soit $\mathcal{B}=(e_1,\dots,e_n)$ une base de E.

(*i*) Il existe une unique forme n-linéaire alternée φ telle que $\varphi(e_1,\dots,e_n)=1$, on l'appelle le *déterminant* dans la base $\mathcal{B}$ et on note $\det_{\mathcal{B}}$.

(*ii*) Soit $x^{(1)},\dots,x^{(n)}\in E$, on note $x^{(i)}=\sum_{j=1}^n x_j^{(i)}e_j$, alors $\det_{\mathcal{B}}(x_1,\dots,x_n)=\sum_{\sigma\in\mathcal{S}_n}\varepsilon(\sigma)x_{\sigma(1)}^{(1)}\cdots x_{\sigma(n)}^{(n)}$.

Définition. Soit $A=(a_{i,j})\mathcal{M}_n(\mathbb{K})$. On appelle

(*i*) *déterminant* de A le déterminant des vecteurs colonnes de A *i.e.*

$$\det A=\sum_{\sigma\in\mathcal{S}_n}\varepsilon(\sigma)a_{\sigma(1),1}\cdots a_{n,\sigma(n),n}$$

(*ii*) *permanent* de A le scalaire

$$\mathrm{per}A=\sum_{\sigma\in\mathcal{S}_n}a_{\sigma(1),1}\cdots a_{n,\sigma(n),n}\ .$$

Proposition. *Soit $A=(a_{i,j})\mathcal{M}_n(\mathbb{K})$ alors :*

(*i*) $\det A=\det\ {}^tA$ *et* $\mathrm{per}A=\mathrm{per}\ {}^tA$

(*ii*) *en notant $A_{i,j}$ la matrice obtenue en supprimant la i-è ligne et j-è colonne, on a pour tous $1\le i,j\le n$:*

$$\det A=\sum_{i=1}^n(-1)^{i+j}a_{i,j}\det A_{i,j}=\sum_{j=1}^n(-1)^{i+j}a_{i,j}\det A_{i,j}$$

$$\mathrm{per}A=\sum_{i=1}^n a_{i,j}\mathrm{per}A_{i,j}=\sum_{j=1}^n a_{i,j}\mathrm{per}A_{i,j}.$$

(*iii*) *Soit $\sigma,\rho\in\mathcal{S}_n$ et $B=P_\sigma AP_\rho$, alors* $\mathrm{per}A=\mathrm{per}B$.

Théorème de Frobenius-König. *Soit $A=(a_{i,j})\mathcal{M}_n(\mathbb{R})$ à coefficients positifs alors* $\mathrm{per}A=0$ *si et seulement si il existe une sous-matrice nulle de A de taille $(r,n+1-r)$.*

Corollaire. *Si $A=(a_{i,j})\in\mathcal{M}_n(\mathbb{R})$ est bistochastique alors* $\mathrm{per}A>0$. *Il s'ensuit qu'il existe $\sigma\in\mathcal{S}_n$ tel que $a_{\sigma(j),j}>0$ pour tout $1\le j\le n$.*

Application (lemme des mariages)**.** Soit F,G deux ensembles finis et $f:G\to\mathcal{P}(F)$, on a équivalence entre

(*i*) il existe une injection $\varphi:G\to F$ avec $\varphi(x)\in f(x)$ pour tout $x\in G$,

(*ii*) pour tout $G'\subset G$, $\mathrm{card}\bigcup_{x\in G'}f(x)\ge\mathrm{card}G'$.

4.2. **Sous-groupes finis de $\mathcal{SO}(3)$.**

Proposition. *Les sous-groupes finis de $\mathcal{SO}(3)$ sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$, $D_{n/2}$, $\mathcal{A}_4$, $\mathcal{S}_4$ ou $\mathcal{A}_5$.*

Remarque. $\mathcal{A}_4$ est le groupe des isométries du tétraèdre, $\mathcal{S}_4$ celui du cube et de l'octaèdre et $\mathcal{A}_5$ celui de l'icosaèdre et du dodécaèdre.

Développements

$\mathcal{A}_5$ est le seul groupe simple d'ordre 60**.**

Action de $\mathcal{A}_n$ sur $\mathbb{K}[T_1,\dots,T_n]$.

Sous-groupes finis de $\mathcal{SO}(3)$.

Groupe des isométries du cube.

Références

[1] M. Alessandri, *Thèmes de géométrie. Groupes en situation géométrique*, Dunod, 1999.
[2] J. Calais, *Éléments de théorie des groupes*, P.U.F., 1996.
[3] F. Combes, *Algèbre et géométrie*, Bréal, 1998.
[4] S. Francinou, H. Gianella et S. Nicolas, *Oraux X-ENS, algèbre 1*, Cassini, 2001.
[5] R. Goblot, *Algèbre commutative*, Masson, 1996.
[6] J.-M. Monier, *Algèbre, tome 2*, Dunod, 1991.
[7] D. Perrin, *Cours d'algèbre*, Ellipses, 1996.
[8] D. Serre, *Les matrices*, Dunod, 2001.