Groupe des permutations d'un ensemble fini. Applications.

Mohamed NASSIRI

En considérant un ensemble fini E de cardinal n (dont on peut toujours indexer les éléments de 1 à n), on souhaite étudier le groupe des permutations de cet ensemble : ordre des éléments, classes de conjugaisons, générateurs, sous-groupes, etc. Bref de la botanique !

L'intérêt de l'étude de ce groupe vient en particulier du théorème de Cayley qui dit que tout groupe de cardinal n s'injecte dans $\mathcal{S}_n$. Néanmoins, petit bémol, pour étudier un groupe de cardinal 5, il faut étudier $\mathcal{S}_5$ qui est de cardinal 120 ...

Les applications très sont variées. Par exemple, on a une formule explicite pour le déterminant avec une somme portant sur $\sigma \in \mathcal{S}_n$. Même si cette formule nous permet de démontrer que $\det(AB) = \det(BA)$ ou encore $\det({}^tA) = \det(A)$, elle n'est pas "top" dans la pratique. En effet, pour calculer un déterminant d'une matrice de taille 5×5, on aura $|\mathcal{S}_5| = 120$ termes dans la somme ...

Encore plus fort, encore plus loin ! On peut définir les matrices de permutations. La magie de la chose est que cette fois-ci, c'est le déterminant (des matrices de permutations) qui va nous donner un lien avec (la signature) des permutations ($\det P_\sigma = \epsilon(\sigma)$).

En géométrie, avec les groupes des isométries $Is(X)$ d'un objet $X \subset \mathbb{R}^3$, on peut montrer des isomorphismes très intéressants : par exemple, si Δ_4 est le tétraèdre régulier, on $Is(\Delta_4) \approx \mathcal{S}_4$.

Pour finir, chez les polynômes, on peut définir une action du groupe $\mathcal{S}_n$ sur les polynômes $P \in A[X_1, ..., X_n]$. On dira qu'un polynôme est "symétrique" s'il est invariant par cette action (*i.e.*) si pour tout $\sigma \in \mathcal{S}_n$, $P(X_{\sigma(1)}, ..., X_{\sigma(n)}) = P(X_1, ..., X_n)$. Ils jouent notamment un rôle dans les relations entre coefficients et racines du polynôme.

Références

[GRI] Algèbre linéaire 5e Edition, Joseph Grifone
[GOUag] Les maths en tête : Algèbre, Xavier Gourdon
[TAU] Algèbre pour l'agrégation interne, Patrice Tauvel
[OBJ] Objectif Agrégation, Vincent Beck, Jérôme Malick et Gabriel Peyré
[H2G2t1] Histoires hédonistes de groupes et de géométries - T1, Philippe Caldero et Jérôme Germoni ♠
[PER] Cours d'Algèbre, Daniel Perrin ♠
[DEL] Théorie des groupes 2e édition, Jean Delcourt

Développements

Table des caractères de $\mathcal{S}_4$
Générateurs de $\mathcal{S}_n$

1 Groupe symétrique

1.1 Définitions et premières propriétés [TAU] p.45→47

Définition 1 *Soit E un ensemble. Une bijection de E sur lui-même est appelée une permutation de E. On note l'ensemble des permutations de E $\mathcal{S}(E)$. Lorsque $E = [\![1, ..., n]\!]$, on note $\mathcal{S}_n = \mathcal{S}(E)$. Un permutation σ sera notée :*

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n-1 & n \\ \sigma(1) & \sigma(2) & ... & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

Remarque 2 *On se place dans le cadre $\mathcal{S}_n$.*

Proposition 3 *Muni de la composition des applications, $\mathcal{S}_n$ est un groupe, appelé groupe symétrique, et on a $|\mathcal{S}_n| = n!$.*

Proposition 4 *Théorème de Cayley : Tout groupe fini G de cardinal est isomorphe à un sous-groupe de $\mathcal{S}_n$.*

Définition 5 *Pour $x \in [\![1, ..., n]\!]$, $\sigma \in \mathcal{S}_n$, on note $\mathcal{O}_\sigma(x) = \{\sigma^k(x); k \in \mathbb{Z}\}$ et on dit que $\mathcal{O}_\sigma(x)$ est une σ-orbite de x.*

Exemple 6 *Soit $\sigma \in \mathcal{S}_7$ définie par :*

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

On a $\mathcal{O}_\sigma(1) = \{1, 2, 3\}$, $\mathcal{O}_\sigma(4) = \{4\}$ et $\mathcal{O}_\sigma(5) = \{5.6.7\}$.

Définition 7 *On dit que $\sigma \in \mathcal{S}_n$ est un cycle s'il existe une unique orbite $\mathcal{O}$ tel que $\text{card}(\mathcal{O}) > 1$.*

Alors, le cardinal de $\mathcal{O}$ est appelé la longueur du cycle et $\mathcal{O}$ son support.
Un q-cycle est un cycle de longueur q et un 2-cycle est une transposition.

Exemple 8 *Soient $\sigma, \tau \in \mathcal{S}_5$ définies par :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$$

Alors σ est un 3-cycle et τ une transposition.

Proposition 9 *Soit $\sigma, \tau \in \mathcal{S}_n$, $\mathcal{O}$ une σ-orbite de cardinal $p > 1$. Si $a \in \mathcal{O}$, on a $\mathcal{O} = \{a, \sigma(a), ...\sigma^{p-1}(a)\}$, et $\sigma^p(x) = x$ pour tout $x \in \mathcal{O}$. Si σ est un cycle, il est donc d'ordre p.*

Remarque 10 *Un p-cycle dont l'unique orbite non trivial est $\{a_1, ..., a_p\}$ avec $a_i = s^{i-1}(a_1)$ pour $1 \leq i \leq p$ sera noté $(a_1...a_p)$*

Proposition 11 • *Soient s, t des p-cycles. Il existe $u \in \mathcal{S}_n$ telle que $t = usu^{-1}$*
• *Deux cycles à support disjoints commutent.*

Proposition 12 *Principe de conjugaison : Si $\sigma = (a_1...a_p) \in \mathcal{S}_n$ est un cycle d'ordre p et $\tau \in \mathcal{S}_n$, on a*

$$\tau\sigma\tau^{-1} = (\tau(a_1)...\tau(a_p))$$

[PER] p.15

Corollaire 13 *Classes de conjugaisons de Sn*

1.2 Décompositions et parties génératrices [TAU] p.47

Théorème 14 *Tout $\sigma \in \mathcal{S}_n$ différent de l'identité est produit de cycles à supports deux à deux disjoints, et un tel produit est unique à l'ordre près des facteurs.*

le ppcm des longueurs de ces derniers est égal à l'ordre de la permutation

Exemple 15

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$

Théorème 16 ♠ *Générateurs de $\mathcal{S}_n$* ♠
Soit $n \geq 2$.
(i) Les transpositions engendrent $\mathcal{S}_n$.
(ii) L'ensemble $\{(1\ i), 2 \leq i \leq n\}$ engendre $\mathcal{S}_n$.
(iii) Le nombre minimal de transpositions engendrant $\mathcal{S}_n$ est $n-1$.

Corollaire 17 *(i) L'ensemble $\{(i\ i+1), 1 \leq i \leq n-1\}$ engendre $\mathcal{S}_n$.*
(ii) La transposition $(1\ 2)$ et le n-cycle $(1\ 2...n)$ engendrent $\mathcal{S}_n$.

2 Groupe alterné

2.1 Le morphisme signature ϵ [GOUag] p.21

Définition 18 *Soit $\sigma \in \mathcal{S}_n$. On appelle signature de σ le produit*

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

Proposition 19 *Soient $\sigma, \tau \in \mathcal{S}_n$. Alors*
(i) $\epsilon(\sigma) \in \{-1, 1\}$,
(ii) $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau)$.

Proposition 20 *ϵ est l'unique morphisme de groupe non trivial de $\mathcal{S}_n$ dans $\mathbb{R}^*$.*

2.2 Le groupe alterné

Définition 21 *On définit le groupe alterné $\mathcal{A}_n = \text{Ker}\epsilon$.* **[GOUag] p.21**

Proposition 22 *$\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ et on a $|\mathcal{A}_n| = n!/2$.* **[GOUag] p.21**

Proposition 23 *Pour $n \geq 3$,*
(i) $Z(\mathcal{S}_n) = \{Id\}$, et $\mathcal{S}_n$ n'est pas abélien.
(ii) $\mathcal{A}_n$ est engendré par les permutations $(1\ i)(1\ j)$, où $2 \leq i, j \leq n$.
(ii) $\mathcal{A}_n$ est engendré par les 3-cycles de la forme $(1\ 2\ i)$, où $3 \leq i \leq n$.
$\mathcal{A}_n$ est engendré par les éléments σ^2, $\sigma \in \mathcal{S}_n$. **[TAU] p.49**

Théorème 24 *$\mathcal{A}_n$ est simple pour $n \geq 5$*

3 Applications

3.1 Déterminant [GRI] p.113 → 115

Proposition 25 *Soit $A = (a_{ij}) \in \mathcal{M}_n(K)$. Alors*

$$\det(A) = \sum_{\sigma \in \mathcal{S}_n} \epsilon(\sigma) a_{\sigma(1)1}...a_{\sigma(n)n}$$

Exemple 26 *Pour $n = 3$, on a $\mathcal{S}_3 = \{\sigma_1 = Id, \sigma_2 = (1\ 2\ 3), \sigma_3 = (1\ 3\ 2), \tau_1 = (2\ 3), \tau_2 = (1\ 3), \tau_3 = (1\ 2)\}$ avec $\epsilon(\sigma_i) = 1$ et $\epsilon(\tau_i) = -1$ $(i = 1, 2, 3)$.*

$$\begin{aligned} \det(A) &= \sum_{\sigma \in \mathcal{S}_3} \epsilon(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} a_{\sigma(3)3} \\ &= a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} \\ &+ a_{31}a_{12}a_{23} - a_{11}a_{32}a_{23} \\ &- a_{31}a_{22}a_{13} - a_{21}a_{12}a_{33} \end{aligned}$$

Théorème 27 *Soit $A = (a_{ij}) \in \mathcal{M}_n(K)$. Alors*

$$\det({}^tA) = \det(A)$$

3.2 Matrices de permutations [DEL] p.61→68

Définition 28 *Soit $\sigma \in \mathcal{S}_n$, on appelle matrice de permutation une matrice de la forme $P_\sigma = (p_{ij})$ où $p_{ij} = \delta_{i\sigma(j)}$ pour $1 \leq i, j \leq n$ (où δ_{ij} est le symbole de Kronecker).*

Proposition 29 *(i) L'ensemble $\mathcal{P}$ des matrices de permutation est un groupe isomorphe à $\mathcal{S}_n$.*
(ii) $\mathcal{P}$ agit par translation sur $\mathcal{M}_n(\mathbb{K})$ ($\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$).

Exemple 30 *Soit $M \in \mathcal{M}_n(\mathbb{R})$ que l'on note $M = (C_1\ C_2\ C_3) = \begin{pmatrix} L_1 \\ L_2 \\ L_3 \end{pmatrix}$ et en considérant $\sigma = (123)$. Alors :*

$$P_\sigma M = \begin{pmatrix} L_3 \\ L_1 \\ L_2 \end{pmatrix} \text{ et } MP_\sigma = (C_2\ C_3\ C_1)$$

Proposition 31 *Soit $\sigma \in \mathcal{S}_n$. Alors $\det P_\sigma = \epsilon(\sigma)$. En d'autres termes, le diagramme suivant est commutatif*

$$\begin{array}{ccc} \mathcal{S}_n & \xrightarrow{\varphi} & \mathrm{GL}_n(\mathbb{K}) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\det} \\ \{-1,1\} & \longrightarrow & \mathbb{K}^* \end{array}$$

[OBJ] p.188

3.3 Polyèdres [H2G2t1] p.361→364

Définition 32 *Le groupe Is(X) des isométries d'un objet $X \subset \mathbb{R}^3$ est le sous-groupe des isométries de l'espace affine euclidien $\mathbb{R}^3$ qui stabilisent X.*

Proposition 33 ♠ *Soit Δ_4 le tétraèdre régulier. Alors $Is(\Delta_4) \approx \mathcal{S}_4$.*

Application 34 *Table des caractères de $\mathcal{S}_4$.* ♠

3.4 Polynômes symétriques [GOUag] p.78

Définition 35 *Soit A un anneau commutatif unitaire. Un polynôme $P \in A[X_1, ..., X_n]$ est dit symétrique si pour tout $\sigma \in \mathcal{S}_n$, $P(X_{\sigma(1)}, ..., X_{\sigma(n)}) = P(X_1, ..., X_n)$.*

Exemple 36 *Dans $\mathbb{R}[X, Y, Z]$, P=XY+YZ+ZX est symétrique.*

Définition 37 *On appelle polynômes symétriques élémentaires de $A[X_1, ..., X_n]$ les polynômes notés Σ_p $(1 \leq p \leq n)$ et définis par*

$$\Sigma_p = \Sigma X_1 ... X_p = \Sigma_{i_1 < ... < i_p} X_{i_1} ... X_{i_p}$$

Exemple 38 $\Sigma_1 = \Sigma X_1 = X_1 + ... + X_n$
$\Sigma_2 = \Sigma X_1 X_2 = \Sigma_{i<j} X_i X_j$
$\Sigma_n = X_1 ... X_n$

Proposition 39 *Relation coefficients/racines : Si $P(X) = (X - a_1)...(X - a_n)$, alors*

$$P(X) = X^n + \sum_{i=1}^{n} (-1)^i \Sigma_i(a_1, ...a_n) X^{n-i}$$

Théorème 40 (admis) *Soit $P \in A[X_1, ..., X_n]$ un polynôme symétrique. Alors il existe un unique polynôme $\Phi \in A[X_1, ..., X_n]$ tel que $P = \Phi(\Sigma_1, ..., \Sigma_n)$.*

Exemple 41 *Dans $A[X_1, ..., X_n]$, $\Sigma X_1^2 = \Sigma_1^2 - 2\Sigma_2^2$.*

Questions

Exercice : Montrer que, pour $n \geq 3$, les 3-cycles engendrent $\mathcal{A}_n$.

Solution : Soit $\sigma \in \mathcal{A}_n$, a fortiori $\sigma \in \mathcal{S}_n$ donc il se décompose comme un produit de transpositions (car les transpositions engendrent $\mathcal{S}_n$), mais comme $\sigma \in \mathcal{A}_n$, le nombre de transpositions est pair ($i.e$) $\sigma = \tau_1 ... \tau_{2k}$ avec $k \in \mathbb{N}$. Regardons les produits de deux transpositions :
- si $\tau_i = \tau_j$ pour $i, j \in 1, ...2k$, alors $\tau_i \tau_j = id$ donc c'est en particulier un 3-cycle.
- si τ_i et τ_j ont élément en commun, alors on peut écrire $(\alpha\beta)(\beta\gamma) = (\alpha\beta\gamma)$ donc c'est un 3-cycle.
- si τ_i et τ_j n'ont pas d'élément en commun, alors on peut écrire $(\alpha\beta)(\gamma\delta) = (\alpha\beta)(\beta\gamma)(\beta\gamma)(\gamma\delta) = (\alpha\beta\gamma)(\beta\gamma\delta)$ et donc c'est produit de 3-cycles.

Exercice : Montre que $\mathcal{A}_4$ n'est pas simple.

Solution : Regardons les éléments de $\mathcal{A}_4$. $|\mathcal{A}_4| = 12 = 2^2.3$
Dans $\mathcal{A}_4$, il y a l'identité Id, $\binom{4}{2}/2 = 3$ éléments d'ordre 2 et $\binom{4}{3} \times 2 = 8$ éléments d'ordre 3.

Arrêtons nous un peu sur le décompte des éléments !
- Eléments d'ordre 2 : Ce sont les doubles transpositions et pour créer une double transposition, on procède de la sorte : pour

$$(ab)(cd)$$

on a 2 choix parmi 4 pour le choix de a et b et par suite c et d sont fixés. Mais attention, comme, par exemple, la double transposition $(12)(34)$ est la même que $(34)(12)$, il faut donc diviser par deux ce nombre de choix. Ainsi, on a bien $\binom{4}{2}/2 = 3$ doubles transpositions.
- Eléments d'ordre 3 : Ce sont les 3-cycles et pour créer un 3-cycles, on procède de la sorte : pour

$$(abc)(d)$$

on a 3 choix parmi 4 pour le choix de a, b et c et par suite d sont fixés. Mais attention, comme, par exemple, le 3-cycle $(123)(4)$ n'est pas le même que $(132)(4)$, il faut donc multiplier par deux ce nombre de choix. Ainsi, on a bien $\binom{4}{3} \times 2 = 8$ 3-cycles.

S'il existe un sous-groupe distingué H de $\mathcal{A}_4$, celui-ci vérifie, par le théorème de Lagrange, que $|H| = \{1, 2, 3, 4, 6, 12\}$. Pour démontrer la non-simplicité de $\mathcal{A}_4$, on exclut les cas triviaux $|H| = 1$ et $|H| = 12$ (qui correspondent respectivement à $H = Id$ et $H = \mathcal{A}_4$).

- Si $|H| = 2$: Alors H contient une double transposition (car c'est un élément d'ordre 2) et comme H est distingué dans $\mathcal{A}_4$, il les contient toutes. Or il y a 3 doubles transpositions. Contradiction (avec $|H| = 2$) !

- Si $|H| = 3$: Même argument : H contient un 3-cycle et comme H est distingué dans $\mathcal{A}_4$, il les contient tous. Or il y a 8 3-cycles. Contradiction (avec $|H| = 3$) !

- Si $|H| = 6 = 2 \times 3$: Alors H contient au moins un élément d'ordre 2 (une double transposition) et 3 (un 3-cycle) mais comme H est distingué dans $\mathcal{A}_4$, il contient toutes les doubles transpositions et tous les 3-cycles. Or il y a 3 doubles transpositions et 8 3-cycles (donc 11 éléments). Contradiction (avec $|H| = 6$) !

- Si $|H| = 4$: On remarque $H = \{Id; (12)(34); (13)(24); (14)(23)\}$ est distingué dans $\mathcal{A}_4$.

Exercice : Soit

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix} \in \mathcal{S}_5$$

On définit la matrice M_σ définit par $m_{ij} = \delta_{i\sigma(j)}$. Calculer $\det M_\sigma$.

Solution : On a

$$M_\sigma = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

On peut montrer, dans le cas général, que

$$\det(M_\sigma) = \sum_{\rho \in \mathcal{S}_n} \epsilon(\rho) \prod_{i=1}^{n} m_{\rho(i)i} = \sum_{\rho \in \mathcal{S}_n} \epsilon(\rho) \prod_{i=1}^{n} \delta_{\rho(i)\sigma(i)}$$

Or, pour tout $1 \leq i \leq n$, si $\rho(i) \neq \sigma(i)$, on a $\delta_{\rho(i)\sigma(i)} = 0$ et $\rho(i) = \sigma(i)$ implique $\delta_{\rho(i)\sigma(i)} = 1$ et ceci n'arrive que si $\sigma = \rho$. Donc dans la somme portant sur $\rho \in \mathcal{S}_n$, il ne reste que σ. Par suite,

$$\det(M_\sigma) = \epsilon(\sigma) = \epsilon((23)(45)) = 1$$
