

Permutations d'un ensemble fini

Notations

E est un ensemble non vide et Id_E est l'application identité sur E .

On note $\mathcal{S}(E)$ le groupe des bijections de E sur lui-même.

Pour toute permutation $\sigma \in \mathcal{S}_n$, on note :

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

pour signifier que σ est la bijection $\sigma : k \in E \mapsto \sigma(k)$.

Pour $E = \{1, 2, \dots, n\} \subset \mathbb{N}$, on note \mathcal{S}_n le groupe $\mathcal{S}(E)$.

- I - Généralités

1. Montrer que si l'ensemble E a au moins 3 éléments, alors le groupe $\mathcal{S}(E)$ n'est pas commutatif.
2. Montrer que si E, F sont deux ensembles non vides et φ une bijection de E sur F , alors les groupes $\mathcal{S}(E)$ et $\mathcal{S}(F)$ sont isomorphes.
3. Soit $E = \{x_1, \dots, x_n\}$ un ensemble à $n \geq 2$ éléments et H le sous-ensemble de $\mathcal{S}(E)$ formé des permutations de E qui laissent stable x_n .
 - (a) Montrer que H est un sous-groupe de $\mathcal{S}(E)$ isomorphe à $\mathcal{S}(F)$, où $F = \{x_1, \dots, x_{n-1}\}$.
 - (b) En désignant, pour tout entier k compris entre 1 et n , par τ_k la permutation définie par $\tau_k(x_k) = x_n$, $\tau_k(x_n) = x_k$ et $\tau_k(x) = x$ pour tout $x \in E \setminus \{x_k, x_n\}$ ($\tau_n = Id$), montrer que $\mathcal{S}(E)/H = \{\tau_1 H, \dots, \tau_n H\}$.
 - (c) En déduire que $\text{card}(\mathcal{S}(E)) = n!$
4. On appelle dérangement de l'ensemble $I_n = \{1, 2, \dots, n\}$ toute permutation σ de cet ensemble n'ayant aucun point fixe (i. e. telle que $\sigma(i) \neq i$ pour tout $i \in I_n$). Pour tout entier naturel non nul p , on note δ_p le nombre de dérangements de I_p . On a $\delta_1 = 0$ et, par convention, on pose $\delta_0 = 1$.
 - (a) Soient $(f_n)_{n \in \mathbb{N}}$ et $(g_n)_{n \in \mathbb{N}}$ deux suites de réels telles que :

$$\forall n \in \mathbb{N}, f_n = \sum_{k=0}^n C_n^k g_k.$$

Montrer que :

$$\forall n \in \mathbb{N}, g_n = \sum_{k=0}^n (-1)^{n-k} C_n^k f_k.$$

(Formule d'inversion de Pascal).

- (b) Montrer que :

$$\forall n \in \mathbb{N}, n! = \sum_{k=0}^n C_n^k \delta_k. \quad (1)$$

- (c) En déduire, en utilisant la formule d'inversion de Pascal, que :

$$\forall n \in \mathbb{N}, \delta_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

- (d) Montrer ce résultat directement, sans utiliser la formule d'inversion de Pascal.

- (e) On se propose de montrer le résultat précédent en utilisant la série entière $\sum \frac{\delta_n}{n!} z^n$.

- (f) Montrer que la série entière $\sum \frac{\delta_n}{n!} z^n$ est convergente pour $|z| < 1$. On note $f(z)$ sa somme.

(g) En utilisant (1), montrer que, pour $|z| < 1$, on a :

$$f(z) = \frac{e^{-z}}{1-z}$$

(h) En déduire que $\delta_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$.

(i) Montrer que $\delta_n = E\left(\frac{n!}{e} + \frac{1}{2}\right)$ pour tout $n \geq 1$, où E est la fonction partie entière.

(j) On considère n couples qui se présentent à un concours de danse, chaque danseur choisissant une partenaire au hasard.

- i. Quelle est la probabilité p_n pour que personne ne danse avec son conjoint ?
- ii. Calculer la limite de p_n quand n tend vers l'infini.

5. Montrer que l'inverse d'un r -cycle est un r -cycle de même support.

6. Montrer que \mathcal{S}_3 est, à isomorphisme près, le seul groupe d'ordre 6 non commutatif.

7. Montrer que le groupe des isométries du plan affine euclidien qui conservent les sommets d'un vrai triangle équilatéral est isomorphe à \mathcal{S}_3 .

8. Montrer que le groupe des isométries du plan affine euclidien qui conservent les sommets d'un vrai triangle isocèle non équilatéral est isomorphe à \mathcal{S}_2 .

9.

(a) Montrer que si $\sigma = (x_1, x_2, \dots, x_r)$ est un r -cycle et τ une permutation, alors :

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \tau(x_2), \dots, \tau(x_r))$$

(le conjugué dans $\mathcal{S}(E)$ d'un r -cycle est encore un r -cycle de même longueur).

(b) Montrer que si σ et σ' sont deux cycles de même longueur r , il existe alors une permutation τ telle que $\sigma' = \tau \circ \sigma \circ \tau^{-1}$ (deux cycles de même longueur sont conjugués dans $\mathcal{S}(E)$).

10. Déterminer, pour $n \geq 3$, le centre $Z(\mathcal{S}(E))$ de $\mathcal{S}(E)$ (c'est-à-dire l'ensemble des éléments de $\mathcal{S}(E)$ qui commutent à tous les autres éléments de $\mathcal{S}(E)$).

– II – Générateurs de $\mathcal{S}(E)$

1. Montrer que toute permutation $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ se décompose en produit de cycles de supports deux à deux disjoints (le groupe $\mathcal{S}(E)$ est engendré par les cycles) et que cette décomposition est unique à l'ordre près.

2. Soit $\sigma \in \mathcal{S}_n$ définie par :

$$\forall k \in \{1, 2, \dots, n\}, \sigma(k) = n + 1 - k$$

(elle inverse l'ordre des entiers $1, 2, \dots, n$). Donner la décomposition de σ en produit de cycles de supports deux à deux disjoints.

3. Montrer que si $\sigma = \sigma_1 \cdots \sigma_p$ est « la » décomposition de $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$ en produit de cycles de supports deux à deux disjoints, on a alors :

$$\text{ordre}(\sigma) = \text{ppcm}(\text{ordre}(\sigma_1), \dots, \text{ordre}(\sigma_r))$$

4. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$. Calculer σ^{2009} .

5. Montrer que pour $r \geq 2$, tout r -cycle dans $\mathcal{S}(E)$ s'écrit comme produit de $r - 1$ transpositions.

6. Montrer que toute permutation $\sigma \in \mathcal{S}(E)$ se décompose en produit de transpositions (le groupe $\mathcal{S}(E)$ est engendré par les transpositions).

7. Montrer que \mathcal{S}_n est engendré par les $n - 1$ transpositions $(1, k)$ où $2 \leq k \leq n$.
8. Montrer que \mathcal{S}_n est engendré par les $n - 1$ transpositions $(k, k + 1)$ où $1 \leq k \leq n - 1$.
9. Montrer que \mathcal{S}_n est engendré par $(1, 2)$ et $(1, 2, \dots, n)$ (on dit que \mathcal{S}_n est dicyclique).
10. Montrer que, pour $n \geq 3$, \mathcal{S}_n est engendré par $(1, 2)$ et $(2, 3, \dots, n)$.

– III – Signature et groupe alterné

Pour toute permutation $\sigma \in \mathcal{S}(E)$, on note $\mu(\sigma)$ le nombre de σ -orbites distinctes.

Si $\sigma = \prod_{k=1}^p \sigma_k$ est la décomposition de σ en produit de cycles de supports deux à deux disjoints, p est le nombre de σ -orbites non réduites à un point et $\mu(\sigma) = p + \varphi(\sigma)$ où $\varphi(\sigma)$ est le nombre de points fixes de σ .

La signature d'une permutation $\sigma \in \mathcal{S}(E)$ est l'élément $\varepsilon(\sigma)$ de $\{-1, 1\}$ défini par :

$$\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}$$

Le groupe alterné est le sous-ensemble de $\mathcal{S}(E)$ formé des permutations paires. On le note $\mathcal{A}(E)$.

Pour $E = \{1, 2, \dots, n\}$, on note \mathcal{A}_n le groupe alterné.

1. Montrer que si $x, y, x_1, \dots, x_j, y_1, \dots, y_k$ sont des éléments distincts de E , on a :

$$(x, y)(x, x_1, \dots, x_j, y, y_1, \dots, y_k) = (x, x_1, \dots, x_j)(y, y_1, \dots, y_k) \quad (2)$$

et :

$$(x, y)(x, x_1, \dots, x_j)(y, y_1, \dots, y_k) = (x, x_1, \dots, x_j, y, y_1, \dots, y_k) \quad (3)$$

2. Montrer que pour toute permutation $\sigma \in \mathcal{S}(E)$ et toute transposition $\tau \in \mathcal{S}(E)$, on a :

$$\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$$

3. Montrer que si $\sigma \in \mathcal{S}(E)$ est produit de p transpositions, on a alors $\varepsilon(\sigma) = (-1)^p$.
4. Montrer que la signature ε réalise un morphisme de groupes surjectif de $\mathcal{S}(E)$ sur $\{-1, 1\}$.
5. Déterminer la signature de :

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

6. Montrer que pour toute permutation $\sigma \in \mathcal{S}_n$, on a :

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

7. Montrer que les seuls morphismes de groupes de $\mathcal{S}(E)$ dans $\{-1, 1\}$ sont l'application constante égale à 1 et la signature ε .
8. Montrer que $\mathcal{A}(E)$ est un sous-groupe distingué de $\mathcal{S}(E)$ d'indice 2.
9. Montrer que \mathcal{A}_3 est cyclique engendré par $(1, 2, 3)$.
10. Soient G un groupe d'ordre $2n$ et H un sous-groupe de G d'ordre n .
 - (a) Montrer que, pour tout $g \in G \setminus H$, on a la partition $G = H \cup gH$.
 - (b) En déduire que $g^2 \in H$ pour tout $g \in G$.
 - (c) Montrer que tout 3-cycle $\sigma \in \mathcal{A}_n$ est le carré d'un élément de \mathcal{A}_n .
 - (d) Donner la liste de tous les éléments de \mathcal{A}_4 en précisant leur ordre.
 - (e) Montrer que \mathcal{A}_4 (qui est d'ordre 12) n'a pas de sous-groupe d'ordre 6.
11. Montrer qu'un produit de deux transpositions est un produit de 3-cycles.

12. Montrer que, pour $n \geq 5$, le produit de deux transpositions de supports disjoints sont conjugués dans $\mathcal{A}(E)$.
13. Montrer que pour $n \geq 3$, $\mathcal{A}(E)$ est engendré par les 3-cycles.
14. Montrer que pour $n \geq 5$, les sous-groupes distingués de $\mathcal{S}(E)$ sont $\{Id\}$, $\mathcal{A}(E)$ et $\mathcal{S}(E)$.
15. Montrer que $\mathcal{A}(E)$ est stable par tout automorphisme de $\mathcal{S}(E)$.
16. Décomposer en produit de 3-cycles dans \mathcal{A}_7 la permutation :

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

17. Montrer que, pour $n \geq 3$, \mathcal{A}_n est engendré par les 3-cycles $\gamma_k = (1, 2, k)$ où $3 \leq k \leq n$ (en particulier \mathcal{A}_4 est dicyclique engendré par $(1, 2, 3)$ et $(1, 2, 4)$).
18. Montrer que, pour $n \geq 3$, \mathcal{A}_n est engendré par les 3-cycles $(k, k+1, k+2)$ où $1 \leq k \leq n-2$.
19. Déterminer, pour $n \geq 4$, le centre de $\mathcal{A}(E)$ (c'est-à-dire l'ensemble des éléments de $\mathcal{A}(E)$ qui commutent à tous les autres éléments de $\mathcal{A}(E)$).
20. Le groupe $\mathcal{S}(E)$ est-il isomorphe au produit direct $\mathcal{A}(E) \times \{-1, 1\}$?
21.
 - (a) Montrer que, pour $n \geq 5$, deux 3-cycles sont conjugués dans $\mathcal{A}(E)$.
 - (b) En déduire que le groupe dérivé $D(\mathcal{A}(E))$ de $\mathcal{A}(E)$ (i. e. le groupe engendré par les commutateurs $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$ où σ et τ sont dans $\mathcal{A}(E)$) est $\mathcal{A}(E)$.
22. On se propose de montrer que, pour $n = 5$, $\mathcal{A}(E)$ est simple (i. e. n'a pas de sous groupes distingués autres que lui même et $\{Id\}$). Ici E est un ensemble à 5 éléments.
 - (a) Donner une description de $\mathcal{A}(E)$ en classant ses éléments en fonction de leur ordre.
 - (b) Montrer que $\mathcal{A}(E)$ est simple.
23. Montrer que pour $n = 3$ ou $n \geq 5$ le groupe $\mathcal{A}(E)$ est simple (i. e. n'a pas de sous groupes distingués autres que lui même et $\{Id\}$).
24. On se propose de montrer ici que pour $n \geq 2$, il n'existe pas de morphisme de groupes injectif de \mathcal{S}_n dans \mathcal{A}_{n+1} .
 - (a) Montrer le résultat pour $n = 2$ et $n = 3$.
 - (b) Montrer le résultat pour n pair.
 - (c) On suppose que $n = 2p+1$ est impair avec $p \geq 2$ et qu'il existe un morphisme de groupes injectif φ de \mathcal{S}_{2p+1} dans \mathcal{A}_{2p+2} . On note $H = \varphi(\mathcal{S}_{2p+1})$ et $E = \mathcal{A}_{2p+2}/H$ est l'ensemble quotient des classes à gauche modulo H .

i. Montrer que l'application :

$$\psi : \begin{array}{ccc} \mathcal{A}_{2p+2} & \rightarrow & \mathcal{S}(E) \\ \sigma & \mapsto & (\gamma H \mapsto \sigma\gamma H) \end{array}$$

est un morphisme de groupes.

ii. Conclure en utilisant le fait que \mathcal{A}_{2p+2} est simple.

– IV – Utilisations du groupe symétrique

1. Montrer que tout groupe G est isomorphe à un sous-groupe de $\mathcal{S}(G)$.
2. Soient G un groupe d'ordre $n \geq 2$ et $\varphi : g \mapsto (\varphi(g) : h \mapsto g \cdot h)$ l'injection de G dans $\mathcal{S}(G)$.
 - (a) Montrer que, pour tout $g \in G \setminus \{1\}$, la permutation $\varphi(g)$ se décompose en produit de cycles tous de longueur égale à l'ordre $\theta(g)$ de g dans G .

(b) En déduire la signature de $\varphi(g)$ pour tout $g \in G$.

(c) En déduire que, si G est un groupe d'ordre impair, il est alors isomorphe à un sous-groupe du groupe alterné $\mathcal{A}(G)$.

3. On désigne par \mathbb{K} un corps commutatif.

À toute permutation $\sigma \in \mathcal{S}_n$, on associe la matrice de passage P_σ de la base canonique $\mathcal{B} = (e_j)_{1 \leq j \leq n}$ de \mathbb{K}^n à la base $\mathcal{B}_\sigma = (e_{\sigma(j)})_{1 \leq j \leq n}$. On dit que P_σ est la matrice de permutation associée à σ .

(a) Montrer que l'application $P : \sigma \mapsto P_\sigma$ est un morphisme de groupes injectif de \mathcal{S}_n dans $GL_n(\mathbb{K})$ et pour toute permutation $\sigma \in \mathcal{S}_n$, on a :

$$\det(P_\sigma) = \varepsilon(\sigma)$$

(b) Montrer que tout groupe fini d'ordre $n \geq 1$ est isomorphe à un sous-groupe de $GL_n(\mathbb{Z}_p)$ où $\mathbb{Z}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$ et $p \geq 2$ est un nombre premier.

4. On désigne par E un espace affine euclidien de dimension $n \geq 2$.

On note $Is(E)$ le groupe des isométries de E , $Is^+(E)$ le sous-groupe des déplacements de E et $Is^-(E)$ l'ensemble des antidéplacements de E .

Pour toute partie non vide \mathcal{P} de E , on note $Is(\mathcal{P})$ [resp. $Is^+(\mathcal{P})$, $Is^-(\mathcal{P})$] l'ensemble des isométries [resp. des déplacements, antidéplacements] φ de E qui conservent \mathcal{P} , c'est-à-dire telles [resp. tels] que $\varphi(\mathcal{P}) = \mathcal{P}$.

(a) Montrer que si \mathcal{P} est une partie non vide de E , alors :

- i. $Is(\mathcal{P})$ est un sous-groupe de $Is(E)$ et $Is^+(\mathcal{P})$ est un sous-groupe distingué de $Is(\mathcal{P})$;
- ii. l'application qui associe à $\varphi \in Is(\mathcal{P})$ sa restriction à \mathcal{P} est un morphisme de groupes de $Is(\mathcal{P})$ dans $\mathcal{S}(\mathcal{P})$; dans le cas où \mathcal{P} est un repère affine de E , cette application est injective et $Is(\mathcal{P})$ est isomorphe à un sous-groupe de \mathcal{S}_{n+1} ;
- iii. si $Is^-(\mathcal{P}) \neq \emptyset$, alors pour toute isométrie $\sigma \in Is^-(\mathcal{P})$, l'application $\rho \mapsto \sigma \circ \rho$ réalise une bijection de $Is^+(\mathcal{P})$ sur $Is^-(\mathcal{P})$; dans le cas où \mathcal{P} est fini, on a $\text{card}(Is(\mathcal{P})) = 2 \text{card}(Is^+(\mathcal{P}))$;
- iv. si \mathcal{P} est fini, alors toute isométrie $\varphi \in Is(\mathcal{P})$ laisse fixe l'isobarycentre de \mathcal{P} .

5. On se fixe un entier $n \geq 2$.

On dit qu'un groupe G est diédral de type \mathcal{D}_{2n} , s'il est dicyclique engendré par un élément ρ d'ordre n et un élément $\sigma \neq \rho$ d'ordre 2 tels que $\rho\sigma\rho\sigma = 1$.

On se place dans le plan complexe muni de sa structure euclidienne canonique et on définit les applications ρ et σ par :

$$\forall z \in \mathbb{C}, \rho(z) = e^{\frac{2i\pi}{n}}z, \sigma(z) = \bar{z}$$

(ρ est la rotation d'angle $\frac{2\pi}{n}$ et σ est la réflexion d'axe Ox).

(a) Montrer que le sous-groupe $G = \langle \rho, \sigma \rangle$ de $\mathcal{S}(\mathbb{C})$ est diédral de type \mathcal{D}_{2n} .

(b) On vérifiera que G est le groupe des isométries du plan complexe qui conservent l'ensemble $\Gamma_n = \left\{ e^{\frac{2ik\pi}{n}} \mid 0 \leq k \leq n-1 \right\}$ des sommets d'un polygone régulier à n cotés.

(c) Soit $G = \langle \rho, \sigma \rangle$ un groupe diédral de type \mathcal{D}_{2n} .

i. Montrer que :

$$G = \{Id, \rho, \dots, \rho^{n-1}\} \cup \{\sigma, \sigma\rho, \dots, \sigma\rho^{n-1}\}$$

et que G est d'ordre $2n$.

ii. Montrer que deux groupes diédraux de type \mathcal{D}_{2n} sont isomorphe.

(d) Montrer que \mathcal{S}_3 est diédral de type \mathcal{D}_6 (le groupe du triangle équilatéral).

6. Montrer que le groupe des isométries positives du tétraèdre est isomorphe à \mathcal{A}_4 .

7. Montrer que le groupe des isométries positives du cube (resp. de l'octaèdre) est isomorphe à \mathcal{S}_4 .
8. Montrer que le groupe des isométries positives du dodécaèdre est isomorphe à \mathcal{A}_5 .
9. Montrer que le groupe des isométries du tétraèdre est isomorphe à \mathcal{S}_4 .
10. Montrer que le groupe des isométries du cube (resp. de l'octaèdre) est isomorphe à $\mathcal{S}_4 \times \{-Id, Id\}$.
11. Montrer que le groupe des isométries du dodécaèdre est isomorphe à $\mathcal{A}_5 \times \{-Id, Id\}$.