Groupe des permutations d'un ensemble fini. Applications.

105

I - Permutations d'un ensemble fini

A - Introduction

[R] 37 **Def 1** : Soit E un ensemble. On note $\mathfrak{S}(E)$ l'ensemble des bijections de E dans E. On l'appelle *groupe symétrique* de E.
On notera plus simplement $\mathfrak{S}_n = \mathfrak{S}(\llbracket 1,n \rrbracket)$. On appelle *permutation* de E un élément de $\mathfrak{S}(E)$.

Prop 2 : $\mathfrak{S}(E)$ est un groupe pour la composition, de neutre l'identité de E.

[R] 39 **Prop 3** : Si E et F sont deux ensembles équipotents, alors $\mathfrak{S}(E)$ et $\mathfrak{S}(F)$ sont isomorphes (en tant que groupes).

[R] 39 **Prop 4** : Pour $n \geq 3$, $\mathfrak{S}_3$ n'est pas commutatif.

Dans toute la suite, on étudiera $\mathfrak{S}_n$ pour $n \geq 3$.

[R] 40 **Prop 5** : $\#\mathfrak{S}_n = n!$

[U] 41 **Notation** : Soit $\sigma \in \mathfrak{S}_n$. On représentera σ par la matrice $2 \times n$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

B - Action naturelle de $\mathfrak{S}_n$ sur $\llbracket 1,n \rrbracket$, conséquences

[U] 41 **Prop 6** : $\mathfrak{S}_n$ agit naturellement sur $\llbracket 1,n \rrbracket$ par $\sigma \cdot i = \sigma(i)$. Le morphisme associé est l'identité de $\mathfrak{S}_n$.

[U] 42 **Def 7** : On note $\mathrm{Fix}(\sigma)$ l'ensemble des points fixes de $\sigma \in \mathfrak{S}_n$. Son complémentaire dans $\llbracket 1,n \rrbracket$ est appelé *support* de σ, et est noté $\mathrm{Supp}(\sigma)$.

[U] 43 **Def/Prop 8** : Soit $\sigma \in \mathfrak{S}_n$. Le sous-groupe $\langle \sigma \rangle$ agit sur $\llbracket 1,n \rrbracket$ par restriction de l'action de $\mathfrak{S}_n$. Les orbites de cette action sont appelées *σ-orbites*. La réunion des σ-orbites ponctuelles est $\mathrm{Fix}(\sigma)$. Les σ-orbites non ponctuelles partitionnent $\mathrm{Supp}(\sigma)$.

Ex 9 : Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix}$. On a $\mathrm{Supp}(\sigma) = \{1,2\} \sqcup \{4,5\} = \langle \sigma \rangle \cdot \{1\} \sqcup \langle \sigma \rangle \cdot \{4\}$.

[U] 43 **Def 10** : ▸ Un k-cycle $(2 \leq k \leq n)$ est une permutation σ n'ayant qu'une seule σ-orbite non ponctuelle $\{i_1, \dots, i_k\}$. On la note $\sigma = (i_1, \dots, i_k)$ pour signifier que $\forall j \notin \{i_1, \dots, i_k\}$, $\sigma(j) = j$, et $\sigma(i_j) = i_{j+1}$ en regardant les indices modulo k.
▸ Un 2-cycle est appelé *transposition*.

[U] 43 **Prop 11** : $(i_1, i_2, \dots, i_k) = (i_2, i_3, \dots, i_k, i_1) = \dots = (i_k, i_1, i_2, \dots, i_{k-1})$

Prop 12 : Un k-cycle est d'ordre k.

C - Décomposition d'une permutation, conséquences

[U] 42 **Prop 13** : Deux permutations à supports disjoints commutent.

[U] 43 **Thm 14** : Toute permutation se décompose de manière unique (à l'ordre des facteurs près) comme produit de cycles à supports disjoints.

[U] 43 **Algorithme 15** : Pour trouver une telle décomposition, il suffit de trouver les σ-orbites
▸ On calcule $\sigma(1), \sigma^2(1), \dots$ jusqu'à trouver $\sigma^{k_1}(1) = 1$ (NB : $k_1 \leq n$).
▸ On pose $i_2 = \min \llbracket 1,n \rrbracket \setminus (\langle \sigma \rangle \cdot \{1\})$, et de même on calcule $\sigma(i_2), \sigma^2(i_2), \dots$ jusqu'à trouver $\sigma^{k_2}(i_2) = i_2$.
▸ On itère jusqu'à épuiser $\llbracket 1,n \rrbracket$.
On a alors $\sigma = (1, \sigma(1), \dots, \sigma^{k_1-1}(1)) \circ (i_2, \sigma(i_2), \dots, \sigma^{k_2-1}(i_2)) \circ \dots \circ (i_j, \sigma(i_j), \dots, \sigma^{k_j-1}(i_j))$

Ex 16 : $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 4 & 1 & 6 & 5 \end{pmatrix} = (1,3,4)(5,6)$

[R] 94 **Prop 17** : $(i_1, \dots, i_k) = (i_1, i_2)(i_2, i_3) \cdots (i_{k-1}, i_k)$

[R] 44 45 **Cor 18** : Les transpositions engendrent $\mathfrak{S}_n$.

Prop 19 : $\mathfrak{S}_n = \langle (i, i+1),\ 1 \leq i < n \rangle = \langle (1,i),\ 2 \leq i \leq n \rangle = \langle (1,2), (1,2,\dots,n) \rangle$

[U] 45 **Def 20** : On appelle *type* de $\sigma \in \mathfrak{S}_n$ la liste croissante des cardinaux des σ-orbites.

Ex 21 : Le type de $(1,2,5)(3,4)(7,8) \in \mathfrak{S}_8$ est la liste $[1,2,2,3]$.

[U] 46 **Prop 22** : Deux permutations sont conjuguées dans $\mathfrak{S}_n$ si, et seulement si elles ont le même type. Cela décrit donc les classes de conjugaison de $\mathfrak{S}_n$.

[U] 45 **Prop 23** : Si σ est du type $[l_1, \dots, l_k]$, alors $\mathrm{ord}(\sigma) = l_1 \vee \dots \vee l_k$.

D - Signature d'une permutation, groupe alterné

[R] 47 **Def Prop 24** : Il existe un unique morphisme $\varepsilon : \mathfrak{S}_n \longrightarrow \{\pm 1\}$ qui envoie les transpositions sur -1. On appelle signature de σ la quantité $\varepsilon(\sigma)$.

Cor 25 : La signature d'un k-cycle est $(-1)^{k+1}$.

[R] 48 **Prop 26** : $\forall \sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$. En particulier, la signature mesure le nombre d'inversions.

[R] 49 **Def 27** : On appelle n^e groupe alterné le sous-groupe $\mathcal{A}_n = \ker(\varepsilon)$. C'est l'ensemble des permutations dites paires.

Ex 28 : $\mathcal{A}_3 = \{\mathrm{id}, (1,2,3), (1,3,2)\}$

Prop 29 : $\#\mathcal{A}_n = \frac{n!}{2}$

[R] 49 **Thm 30** : Pour $n \geq 3$, les 3-cycles engendrent $\mathcal{A}_n$, et y sont conjugués.

[R] 50 **Thm 31** : Pour $n \geq 5$, $\mathcal{A}_n$ n'admet pas de sous-groupe distingué non trivial.

II - Quelques applications du groupe symétrique

A - En géométrie : les isométries des polytopes

[R] 94 **Thm 32** : L'ensemble des isométries du plan conservant un triangle équilatéral est un groupe isomorphe à $\mathfrak{S}_3$.

[R] 82 **Prop 33** : Soit $\mathcal{C}$ un cube. L'ensemble des isométries de l'espace conservant $\mathcal{C}$ est un groupe, noté $\mathrm{Is}(\mathcal{C})$. On note $\mathrm{Is}^+(\mathcal{C})$ le sous-groupe de $\mathcal{C}$ formé de rotations.

[R] 85 **Thm 34** : $\mathrm{Is}^+(\mathcal{C}) \simeq \mathfrak{S}_4$ et $\mathrm{Is}(\mathcal{C}) \simeq \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$ — DEV 1

[R] 95 **Thm 35** : En notant $\mathcal{T}$ le tétraèdre régulier, on a :

$$\mathrm{Is}(\mathcal{T}) \simeq \mathfrak{S}_4 \quad \text{et} \quad \mathrm{Is}^+(\mathcal{T}) \simeq \mathcal{A}_4$$

B - Chez les (actions de) groupes

[R] 53 **Thm 36** (Cayley) : Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Rq 37 : Comme pour tout corps (commutatif) K, $\mathfrak{S}_n \hookrightarrow GL_n(K)$, tout groupe de cardinal n est isomorphe à un sous-groupe de $GL_n(K)$.

Ex 38 : Soit $D_{2\times 4}$ le groupe des isométries du carré. Comme $\#D_{2\times 4} = 8$, $D_{2\times 4}$ est isomorphe à un sous-groupe de $\mathfrak{S}_8$ — notons φ un isomorphisme. Comme $D_{2\times 4} = \langle r, s \rangle$ où $\mathrm{ord}(r) = 4$, $\mathrm{ord}(s) = 2$ et $\mathrm{ord}(rs) = 2$, on a $\varepsilon \circ \varphi(s) = \varepsilon \circ \varphi(rs) = -1$, donc $\varepsilon \circ \varphi(r) = 1$.

C - Polynômes symétriques

[R] 55 **Def 39** : Un *polynôme symétrique* est un polynôme $P \in K[X_1, \dots, X_n]$ tel que $\forall \sigma \in \mathfrak{S}_n$, $P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$.

[R] 55 **Def 40** : Les *polynômes symétriques élémentaires* sont les :

$$\Sigma_{k,n} = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \cdots X_{i_k} \in K[X_1, \dots, X_n] \quad (n \in \mathbb{N}^*, 1 \leq k \leq n).$$

[R] 55 **Thm 41** [admis] : Pour tout polynôme symétrique $P \in K[X_1, \dots, X_n]$, il existe un unique polynôme $Q \in K[X_1, \dots, X_n]$ tel que $P(X_1, \dots, X_n) = Q(\Sigma_{1,n}, \dots, \Sigma_{n,n})$

D – En algèbre (multi-)linéaire

Dans ce paragraphe, E est un $\mathbb{K}$-espace vectoriel de dimension finie n.
On fixe une base $\mathcal{B} = (e_1, \dots, e_n)$ de E.

[R] 545 **Def 42** : Une forme k-linéaire sur E est une application $\varphi : E^k \to \mathbb{K}$ telle que pour tout $i \in [\![1,k]\!]$, pour tout $(x_1, \dots, x_k) \in E^k$, $\varphi(x_1, \dots, x_{i-1}, \cdot, x_{i+1}, \dots, x_k)$ est linéaire.
On note $\bigotimes^k E^*$ l'ensemble des formes k-linéaires sur E.

[R] 546 **Prop 43** : $(e_{i_1}^* \otimes \dots \otimes e_{i_k}^*)_{1 \leq i_1 < \dots < i_k \leq n}$ est une base de $\bigotimes^k E^*$, où pour $(x_1, \dots, x_k) \in E^k$,
$e_{i_1}^* \otimes \dots \otimes e_{i_k}^* (x_1, \dots, x_k) = e_{i_1}^*(x_1) \cdots e_{i_k}^*(x_k)$.

[R] 546 **Def 44** : Une forme k-linéaire *alternée* est une forme k-linéaire $\varphi \in \bigotimes^k E^*$ telle que $\forall \sigma \in \mathfrak{S}_k$, $\forall (x_1, \dots, x_k) \in E^k$, $\varphi(x_{\sigma(1)}, \dots, x_{\sigma(k)}) = \varepsilon(\sigma)\, \varphi(x_1, \dots, x_k)$.
On note $\Lambda^k E^*$ l'espaces des formes k-linéaires alternées sur E.

Prop 45 : $(e_{i_1}^* \wedge \dots \wedge e_{i_k}^*)_{1 \leq i_1 < \dots < i_k \leq n}$ est une base de $\Lambda^k E^*$, où pour $(x_1, \dots, x_k) \in E^k$,
$e_{i_1}^* \wedge \dots \wedge e_{i_k}^* (x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_k} \varepsilon(\sigma)\, e_{i_1}^*(x_{\sigma(1)}) \cdots e_{i_k}^*(x_{\sigma(k)})$.

Cor 46 : $\dim(\Lambda^k E^*) = \binom{n}{k}$.

Def 47 : On appelle *déterminant dans la base $\mathcal{B}$* l'unique forme n-linéaire alternée $\det_{\mathcal{B}}$ sur E vérifiant $\det_{\mathcal{B}}(\mathcal{B}) = 1$. (La famille $(\det_{\mathcal{B}})$ est une base de $\Lambda^n E^*$.)

[R] 547 **Prop 48** : $\forall (x_1, \dots, x_n) \in E^n$, $\det_{\mathcal{B}}(x_1, \dots, x_n) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma)\, e_1^*(x_{\sigma(1)}) \cdots e_n^*(x_{\sigma(n)})$.

E – Résultats en probabilités

[R] 51 **Def 49** : On appelle *dérangement* une permutation sans point fixes.

[S] 60 **Prop 50** : Notons d_n le nombre de dérangements de $[\![1,n]\!]$. Alors $d_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$ et en particulier, la probabilité de choisir un dérangement en tirant au hasard une permutation de $[\![1,n]\!]$ tend vers $\frac{1}{e}$ quand $n \to +\infty$.

[C] **Prop 51** : Soit X la variable aléatoire qui compte le nombre de points fixes d'une permutation aléatoirement choisie dans $\mathfrak{S}_n$.
Alors $\mathbb{E}[X] = \mathbb{V}[X] = 1$.

F – Groupes simples d'ordre 60

Dans ce paragraphe, on se donne p premier, et on note $\#G = p^\alpha m$, $m \wedge p = 1$.

[U] 85 **Def 52** : Un p-Sylow de G est un sous-groupe de G de cardinal p^α.
Notation : $\mathrm{Syl}_p(G)$ désigne l'ensemble des p-Sylow de G, et $n_p = \#\mathrm{Syl}_p(G)$.

[U] 87 **Thm 53** (de Sylow) : 1▸ $\mathrm{Syl}_p(G) \neq \emptyset$
2▸ G agit transitivement sur $\mathrm{Syl}_p(G)$ par conjugaison
3▸ $n_p \equiv 1 \ [p]$ (donc $n_p \mid m$).

Def 54 : On dit que G est *simple* si les seuls sous-groupes de G distingués (i.e. fixe par l'action par conjugaison de G) sont $\{1\}$ et G.

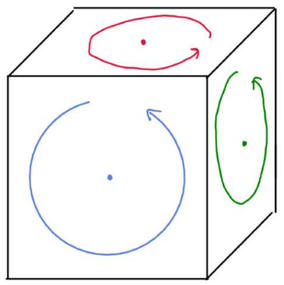
[S] 277 **Thm 55** : Si G est simple et d'ordre 60, alors $G \simeq \mathcal{A}_5$. DEV 2

RÉFÉRENCES :

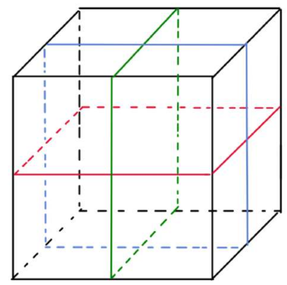
[U] : Théorie des groupes (Félix Ulmer)
[R] : Mathématiques pour l'agrégation – Algèbre et géométrie (Jean-Étienne Rombaldi) [2e édition]
[S] : Algèbre pour la licence 3 (Szpirglas).
[C] : Carnets de voyage en Algébrie (Caldero)

FIGURE : Isométries du cube

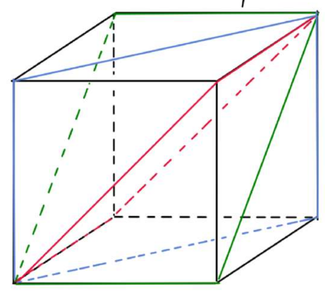
Rotations passant par les faces



Symétries coupant les faces

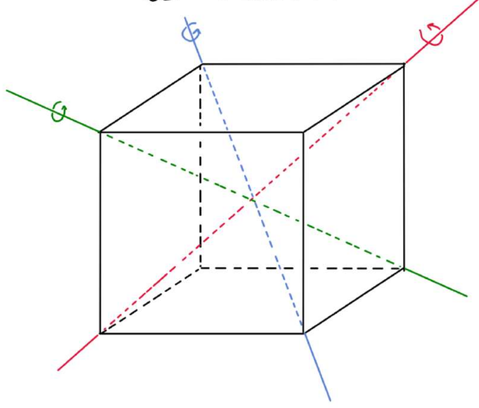


Symétries passant par une arête



(pas toutes représentées)

Rotations passant par les sommets



Rotations passant par les arêtes