# 105 Groupe des permutations d'un ensemble fini. Applications.

Pour toute cette leçon, on fixe un entier $n \geq 1$.

## I - Généralités

### 1. Définitions

**Définition 1.** Soit $E$ un ensemble. On appelle **groupe des permutations** de $E$ le groupe des bijections de $E$ dans lui-même. On le note $S(E)$. [ROM21] p. 37

**Notation 2.** Si $E = [\![1, n]\!]$, on note $S(E) = S_n$, le groupe symétrique à $n$ éléments.

**Notation 3.** Soit $\sigma \in S_n$. On note :

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

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

Le théorème suivant justifie que, pour un ensemble à $n$ éléments, on peut se contenter d'étudier $S_n$ en lieu et place de $S(E)$.

**Théorème 4.** (i) Soient $E$ et $F$ deux ensembles en bijection. Alors $S(E)$ et $S(F)$ sont isomorphes.

(ii)

$$|S_n| = n!$$

**Théorème 5** (Cayley)**.** Tout groupe $G$ est isomorphe à un sous-groupe de $S(G)$. p. 53

### 2. Orbites et cycles

**Définition 6.** Soit $\sigma \in [\![1, n]\!]$. On a une action naturelle de $H = \langle \sigma \rangle$ sur $[\![1, n]\!]$ définie par p. 41

$$\forall k \in \mathbb{Z}, \forall j \in [\![1, n]\!], \sigma^k \cdot j = \sigma^k(j)$$

Les orbites pour cette action sont les $H \cdot j = \{\sigma(j) \mid j \in [\![1, n]\!]\}$. On les note $\mathcal{O}_\sigma(j)$.

*Remarque* 7. — Les orbites selon $\sigma$ sont décrites par la relation

$$x \sim y \iff \exists k \in \mathbb{Z} \text{ tel que } y = \sigma^k(x)$$

— Une orbite $\mathcal{O}_\sigma(j)$ est réduite à un point si et seulement si $\sigma(j) = j$.

**Définition 8.** Soient $l \leq n$ et $i_1, \dots, i_l \in [\![1, n]\!]$ des éléments distincts. La permutation $\gamma \in S_n$ définie par p. 37

$$\gamma(j) = \begin{cases} j & \text{si } j \notin \{i_1, \dots, i_l\} \\ i_{k+1} & \text{si } j = i_k \text{ avec } k < l \\ i_1 & \text{si } j = i_l \end{cases}$$

et notée $\begin{pmatrix} i_1 & \dots & i_l \end{pmatrix}$ est appelée **cycle** de longueur $l$ et de **support** $\{i_1, \dots, i_l\}$. Un cycle de longueur 2 est une **transposition**.

**Proposition 9.** Une permutation $\sigma$ est cycle si et seulement s'il n'y a qu'une seule orbite $\mathcal{O}_\sigma(j)$ non réduite à un point. p. 42

*Remarque* 10. La composée de deux cycles n'est pas un cycle en général.

**Exemple 11.** Avec $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \in S_4$, on a $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ qui n'est pas un cycle.

**Proposition 12.** L'ordre d'un cycle est égal à sa longueur.

**Proposition 13.** Soient $\sigma$ et $\tau$ deux cycles de $S_n$ dont on note respectivement $\operatorname{Supp}(\sigma)$ et $\operatorname{Supp}(\tau)$ les supports. Si $\operatorname{Supp}(\sigma) \cap \operatorname{Supp}(\tau) = \emptyset$, alors $\operatorname{Supp}(\sigma\tau) = \operatorname{Supp}(\sigma) \cup \operatorname{Supp}(\tau)$ et dans ce cas : **[ULM21]** p. 56

(i) $\sigma\tau = \tau\sigma$.

(ii) $\sigma\tau = \mathrm{id} \implies \sigma = \tau = \mathrm{id}$.

**Théorème 14.** Toute permutation de $S_n$ s'écrit de manière unique (à l'ordre près) comme produit de cycles dont les supports sont deux à deux disjoints.

**Exemple 15.**

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

**Définition 16.** On appelle **type** d'une permutation $\sigma \in S_n$ et on note $[l_1, \dots, l_m]$ la liste des cardinaux $l_i$ des orbites dans $[\![1,n]\!]$ de l'action du groupe $\langle \sigma \rangle$ sur $[\![1,n]\!]$, rangée dans l'ordre croissant.

**Proposition 17.** Une permutation de type $[l_1, \dots, l_m]$ a pour ordre $\operatorname{ppcm}(l_1, \dots, l_m)$.

**Exemple 18.** La permutation de l'Exemple 15 est d'ordre 6.

## 3. Signature

**Définition 19.** Soit $\sigma \in S_n$. On appelle **signature** de $\sigma$, notée $\epsilon(\sigma)$ le nombre rationnel

$$\epsilon(\sigma) = \prod_{i \neq j} \frac{\sigma(i) - \sigma(j)}{i - j}$$

**Exemple 20.**

$$\epsilon\left(\begin{pmatrix}1 & 2\end{pmatrix}\right) = -1$$

**Proposition 21.** $\epsilon : S_n \to \mathbb{Q}^*$ est un morphisme de groupes. Pour une permutation $\sigma \in S_n$, on a les propriétés suivantes :

(i) Si $\sigma$ est un transposition, $\epsilon(\sigma) = -1$.

(ii) Si $l$ est le nombre de transpositions qui apparaît dans une décomposition de $\sigma$ en produit de transpositions, alors $\epsilon(\sigma) = (-1)^l$.

(iii) Si $\sigma$ est de type $[l_1, \dots, l_m]$, alors $\epsilon(\sigma) = (-1)^{l_1 + \dots + l_m - m}$.

En particulier, si $n \geq 2$, l'image de $\epsilon$ est le sous-groupe $\{\pm 1\}$ de $\mathbb{Q}^*$.

**Proposition 22.** Le seul morphisme non trivial de $S_n$ dans $\mathbb{C}^*$ est $\epsilon$. **[PEY]** p. 20

**Définition 23.**

— Soit $\sigma \in S_n$. Si $\epsilon(\sigma) = 1$, on dit que $\sigma$ est **paire**. Sinon, on dit qu'elle est **impaire**. **[ULM21]** p. 64

— Le noyau de $\epsilon$ (constitué donc des permutations paires) est un sous-groupe distingué de $S_n$ appelé **groupe alterné** et noté $A_n$.

**Proposition 24.** Pour $n \geq 2$,

$$|A_n| = \frac{n!}{2}$$

# II - Structure

## 1. Conjugaison

**Proposition 25.** Deux permutations $\sigma$ et $\tau$ de $S_n$ sont conjuguées si et seulement si elles sont du même type. En particulier, pour $\omega \in S_n$ et tout cycle $\begin{pmatrix} i_1 & \dots & i_l \end{pmatrix} \in S_n$, on a : p. 60

$$\omega \begin{pmatrix} i_1 & \dots & i_l \end{pmatrix} \omega^{-1} = \begin{pmatrix} \omega(i_1) & \dots & \omega(i_l) \end{pmatrix}$$

**Exemple 26.** Les types possibles d'une permutation de $S_4$ sont [1] (l'identité), [2] (les transpositions), [2, 2] (les doubles transpositions), [3] (les 3-cycles) et [4] (les 4-cycles) : on a 5 classes de conjugaison de tailles respectives 1, 6, 3, 8 et 6.

**Proposition 27.** Pour tout $n \geq 3$, $Z(S_n) = \{\sigma \in S_n \mid \forall \tau \in S_n, \sigma\tau = \tau\sigma\} = \{\mathrm{id}\}$. [PER] p. 13

**Lemme 28.** Les 3-cycles sont conjugués dans $A_n$ pour $n \geq 5$. p. 15

## 2. Générateurs

**Proposition 29.** [ROM21] p. 44

(i) $S_n$ est engendré par les transpositions. On peut même se limiter aux transpositions de la forme $\begin{pmatrix} 1 & k \end{pmatrix}$ ou encore $\begin{pmatrix} k & k+1 \end{pmatrix}$ (pour $k \leq n$).

(ii) $S_n$ est engendré par $\begin{pmatrix} 1 & 2 \end{pmatrix}$ et $\begin{pmatrix} 1 & \dots & n \end{pmatrix}$.

**Exemple 30.** Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix}$, on a $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix} \begin{pmatrix} 4 & 5 \end{pmatrix} \begin{pmatrix} 6 & 7 \end{pmatrix}$.

**Proposition 31.** $A_n$ est engendré par les 3-cycles pour $n \geq 3$.

## 3. Simplicité

**Lemme 32.** Les 3-cycles sont conjugués dans $A_n$ pour $n \geq 5$. [PER] p. 15

**Lemme 33.** Le produit de deux transpositions est un produit de 3-cycles. [ROM21] p. 49

[DEV]

**Théorème 34.** $A_n$ est simple pour $n \geq 5$.

[PER] p. 28

**Corollaire 35.** Le groupe dérivé de $A_n$ est $A_n$ pour $n \geq 5$, et le groupe dérivé de $S_n$ est $A_n$ pour $n \geq 2$.

**Corollaire 36.** Pour $n \geq 5$, les sous-groupes distingués de $S_n$ sont $S_n$, $A_n$ et $\{\mathrm{id}\}$.

**Corollaire 37.** Soit $H$ un sous-groupe d'indice $n$ de $S_n$. Alors, $H$ est isomorphe à $S_{n-1}$.

# III - Applications

## 1. Déterminant

Soit $\mathbb{K}$ un corps et soit $E$ un espace vectoriel de dimension $n$ sur $\mathbb{K}$.

[GOU21] p. 140

**Définition 38.** Soient $E_1, \dots, E_p$ et $F$ des espaces vectoriels sur $\mathbb{K}$ et $f : E_1, \dots, E_p \to F$.

- $f$ est dite $p$-**linéaire** si en tout point les $p$ applications partielles sont linéaires.
- Si $f$ est $p$-linéaire et si $E_1 = \dots = E_p$ ainsi que $F = \mathbb{K}$, $f$ est une **forme $p$-linéaire**. On note $\mathscr{L}_p(E, \mathbb{K})$ l'ensemble des formes $p$-linéaires sur $E$.
- Si de plus $f(x_1, \dots, x_p) = 0$ dès que deux vecteurs parmi les $x_i$ sont égaux, alors $f$ est dite **alternée**.

**Exemple 39.** En reprenant les notations précédentes, pour $p = 2$, $f$ est bilinéaire.

**Proposition 40.** $\mathscr{L}_p(E, \mathbb{K})$ est un espace vectoriel et, $\dim(\mathscr{L}_p(E, \mathbb{K})) = |\dim(E)|^p$.

**Théorème 41.** L'ensemble des formes $p$-linéaires alternées sur $E$ est un $\mathbb{K}$-espace vectoriel de dimension 1. De plus, il existe une unique forme $p$-linéaire alternée $f$ prenant la valeur 1 sur une base $\mathscr{B}$ de $E$. On note $f = \det_{\mathscr{B}}$.

**Définition 42.** $\det_{\mathscr{B}}$ est l'application **déterminant** dans la base $\mathscr{B}$. En l'absence d'ambiguïté, on s'autorise à noter $\det = \det_{\mathscr{B}}$.

**Proposition 43.** Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de $E$. Si $x_1, \dots, x_n \in E$ ($\forall i \in [\![1, n]\!]$, on peut écrire $x_i = \sum_{j=1}^{n} x_{i,j} e_j$), on a la formule $\det_{\mathscr{B}}(x_1, \dots, x_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} x_{i,\sigma(i)}$.

**Corollaire 44.** Soit $\mathscr{B}$ une base de $E$.

(i) Si $\mathscr{B}'$ est une autre base de $E$, alors $\det_{\mathscr{B}'} = \det_{\mathscr{B}'}(\mathscr{B}) \det_{\mathscr{B}}$.

(ii) Une famille de vecteurs est liée si et seulement si son déterminant est nul dans une base quelconque de $E$.

(iii) Soient $A, B \in \mathscr{M}_n(\mathbb{K})$, alors $\det_{\mathscr{B}}(AB) = \det_{\mathscr{B}}(A) \det_{\mathscr{B}}(B)$.

(iv) Soit $A \in \mathscr{M}_n(\mathbb{K})$, alors $\det_{\mathscr{B}}(A) = \det_{\mathscr{B}}({}^tA)$ et pour tout $\lambda \in \mathbb{K}$, $\det_{\mathscr{B}}(\lambda A) = \lambda^n \det_{\mathscr{B}}(A)$.

(v) Si on effectue une permutation $\sigma \in S_n$ sur les colonnes d'une matrice $A$, alors le déterminant de $A$ est multiplié par $\epsilon(\sigma)$.

**Notation 45.** Soit $a \in \mathbb{F}_p$. On note $\left(\frac{a}{p}\right)$ le symbole de Legendre de $a$ modulo $p$. **[I-P]** p. 203

**Lemme 46.** Soient $p \geq 3$ un nombre premier et $V$ un espace vectoriel sur $\mathbb{F}_p$ de dimension finie. Les dilatations engendrent $\mathrm{GL}(V)$.

**[DEV]**

**Théorème 47** (Frobenius-Zolotarev)**.** Soient $p \geq 3$ un nombre premier et $V$ un espace vectoriel sur $\mathbb{F}_p$ de dimension finie.

$$\forall u \in \mathrm{GL}(V), \epsilon(u) = \left(\frac{\det(u)}{p}\right)$$

où $u$ est vu comme une permutation des éléments de $V$.

## 2. Matrices de permutation

Soit $\mathbb{K}$ un corps et soit $E$ un espace vectoriel de dimension $n$ sur $\mathbb{K}$. **[ROM21]** p. 54

**Définition 48.** À tout $\sigma \in S_n$ on associe la matrice de passage de la base canonique $(e_i)_{i \in [\![1,n]\!]}$ à la base $(e_{\sigma}(i))_{i \in [\![1,n]\!]}$ que l'on note $P_\sigma$ : c'est la **matrice de permutation** associée à $\sigma$.

*Remarque* 49. En reprenant les notations précédentes, $\forall j \in [\![1, n]\!]$, $P_\sigma e_j = \sigma(e_j)$.

**Proposition 50.** $\sigma \mapsto P_\sigma$ est un morphisme de groupes injectif de $S_n$ dans $\mathrm{GL}_n(\mathbb{K})$. De plus, on a

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

**Corollaire 51.** Tout groupe fini d'ordre $n$ est isomorphe à un sous groupe de $\mathrm{GL}_n(\mathbb{F}_p)$ pour un premier $p \geq 2$.

## 3. Polynômes symétriques

Soit $\mathbb{K}$ un corps de caractéristique différente de 2.

[GOU21] p. 83

**Définition 52.** Soit $P \in \mathbb{K}[X_1, \dots, X_n]$. On dit que $P$ est **symétrique** si

$$\forall \sigma \in S_n, P(X_{\sigma(1)}, \dots, X_{\sigma(n)}) = P(X_1, \dots, X_n)$$

**Exemple 53.** Dans $\mathbb{R}[X]$, le polynôme $XY + YZ + ZX$ est symétrique.

**Définition 54.** On appelle **polynômes symétriques élémentaires** de $A[X_1, \dots, X_n]$ les polynômes noté $\Sigma_p$ où $p \in [\![1, n]\!]$ définis par

$$\Sigma_p = \sum_{1 \leq i_1 < \dots < i_p \leq n} X_{i_1} \dots X_{i_p}$$

**Exemple 55.**
- $\Sigma_1 = X_1 + \dots + X_n$.
- $\Sigma_2 = \sum_{1 \leq i < j \leq n} X_i X_j$.
- $\Sigma_n = X_1 \dots X_n$.

*Remarque* 56. Si $P \in A[X_1, \dots, X_n]$, alors $P(\Sigma_1(X_1, \dots, X_n), \dots, \Sigma_n(X_1, \dots, X_n))$ est symétrique. Et la réciproque est vraie.

**Théorème 57** (Théorème fondamental des polynômes symétriques)**.** Soit $P \in A[X_1, \dots, X_n]$ un polynôme symétrique. Alors,

$$\exists! \Phi \in A[X_1, \dots, X_n] \text{ tel que } \Phi(\Sigma_1, \dots, \Sigma_n)$$

**Exemple 58.** $P = X^3 + Y^3 + Z^3$ s'écrit $P = \Sigma_1^3 - 3\Sigma_1\Sigma_2 + 3\Sigma_3$.

p. 64

**Application 59** (Relations coefficients - racines)**.** Soit $P = a_0 X^n + \dots + a_n \in \mathbb{K}[X]$ avec $a_0 \neq 0$ scindé sur $\mathbb{K}$, dont les racines (comptées avec leur ordre de multiplicité) sont $x_1, \dots, x_n$. Alors

$$\forall p \in [\![1, n]\!], \Sigma_p(x_1, \dots, x_n) = (-1)^p \frac{a_p}{a_0}$$

En particulier,

— $\Sigma_1(x_1, \dots, x_n) = \sum_{i=1}^{n} x_i = -\frac{a_1}{a_0}$.

— $\Sigma_n(x_1, \dots, x_n) = \prod_{i=1}^{n} x_i = (-1)^n \frac{a_n}{a_0}$.

**Application 60** (Théorème de Kronecker)**.** Soit $P \in \mathbb{Z}[X]$ unitaire tel que toutes ses racines complexes appartiennent au disque unité épointé en l'origine (que l'on note $D$). Alors toutes ses racines sont des racines de l'unité. **[I-P]** p. 279

**Corollaire 61.** Soit $P \in \mathbb{Z}[X]$ unitaire et irréductible sur $\mathbb{Q}$ tel que toutes ses racines complexes soient de module inférieur ou égal à 1. Alors $P = X$ ou $P$ est un polynôme cyclotomique.

# Bibliographie


## Les maths en tête [GOU21]

Xavier Gourdon. *Les maths en tête. Algèbre et probabilités.* 3e éd. Ellipses, 13 juill. 2021.
https://www.editions-ellipses.fr/accueil/13722-25266-les-maths-en-tete-algebre-et-probabilites-3e-edition-9782340056763.html.

## L'oral à l'agrégation de mathématiques [I-P]

Lucas Isenmann et Timothée Pecatte. *L'oral à l'agrégation de mathématiques. Une sélection de développements.* 2e éd. Ellipses, 26 mars 2024.
https://www.editions-ellipses.fr/accueil/15218-28346-loral-a-lagregation-de-mathematiques-une-selection-de-developpements-2e-edition-9782340086487.html.

## Cours d'algèbre [PER]

Daniel Perrin. *Cours d'algèbre. pour l'agrégation.* Ellipses, 15 fév. 1996.
https://www.editions-ellipses.fr/accueil/7778-18110-cours-d-algebre-agregation-9782729855529.html.

## L'algèbre discrète de la transformée de Fourier [PEY]

Gabriel Peyré. *L'algèbre discrète de la transformée de Fourier. Niveau M1.* Ellipses, 15 jan. 2004.
https://adtf-livre.github.io.

## Mathématiques pour l'agrégation [ROM21]

Jean-Étienne Rombaldi. *Mathématiques pour l'agrégation. Algèbre et géométrie.* 2e éd. De Boeck Supérieur, 20 avr. 2021.
https://www.deboecksuperieur.com/ouvrage/9782807332201-mathematiques-pour-l-agregation-algebre-et-geometrie.

## Théorie des groupes [ULM21]

Felix Ulmer. *Théorie des groupes. Cours et exercices.* 2e éd. Ellipses, 3 août 2021.
https://www.editions-ellipses.fr/accueil/13760-25304-theorie-des-groupes-2e-edition-9782340057241.html.