28 | Le groupe symétrique

L'étude algébrique des groupes de permutations s'avère féconde et aboutit à des résultats aussi importants que la non résolubilité par radicaux des équations algébriques de degré supérieur ou égal à 5. Cette étude va toutefois bien au-delà des objectifs du programme qui se limite à introduire des outils commodes pour la définition des déterminants, en l'occurence la notion de signature d'une permutation.

Dans l'ensemble de ce chapitre, n désigne un entier naturel non nul.

1 Permutation, cycle, transposition

Définition-théorème 1 – Permutation, support, groupe des permutations

- On appelle *permutation de* $[\![1\,,n]\!]$ toute bijection de $[\![1\,,n]\!]$ sur $[\![1\,,n]\!]$ et on note $\mathfrak{S}_n$ (ou plus simplement S_n) l'ensemble des permutations de $[\![1\,,n]\!]$.
- On appelle *support* d'une permutation σ de $\mathfrak{S}_n$ le complémentaire dans $[\![1\,,n]\!]$ de l'ensemble des points fixes de σ, *i.e.*
$$\mathrm{supp}(\sigma) = \{k \in [\![1\,,n]\!] \mid \sigma(k) \neq k\}.$$
- Deux permutations de $[\![1\,,n]\!]$ sont dites *disjointes* lorsque leurs supports respectifs le sont.
- Le magma $(\mathfrak{S}_n, \circ)$ est un groupe fini de cardinal $n!$, appelé le *groupe symétrique de degré* n.

Démonstration. Simple vérification des axiomes définissant la structure de groupe : la loi de composition est associative, admet l'identité $\mathrm{Id}_{[\![1,n]\!]}$ pour élément neutre, et la réciproque d'une permutation de $[\![1\,,n]\!]$ en est également une. ■

Notation 2 Pour représenter une permutation σ de $\mathfrak{S}_n$, le plus simple consiste à donner le tableau de ses valeurs

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

Il est alors aisé de calculer le produit de deux permutations et l'inverse d'une permutation via cette représentation.

Exemple 3 Dans $\mathfrak{S}_5$,

$$\underbrace{\begin{pmatrix} 1&2&3&4&5 \\ 1&4&2&5&3 \end{pmatrix}}_{\sigma} \circ \underbrace{\begin{pmatrix} 1&2&3&4&5 \\ 2&1&4&5&3 \end{pmatrix}}_{\tau} = \begin{pmatrix} 1&2&3&4&5 \\ 4&1&5&3&2 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1&2&3&4&5 \\ 1&4&2&5&3 \end{pmatrix}^{-1} = \begin{pmatrix} 1&2&3&4&5 \\ 1&3&5&2&4 \end{pmatrix}.$$

Par ailleurs, $\mathrm{supp}(\sigma) = \{2,3,4,5\}$ et $\mathrm{supp}(\tau) = \{1,2,3,4,5\}$. Pour le calcul de l'inverse, il suffit de lire du bas vers le haut la matrice représentant la permutation à inverser.

Exemple 4 Les 2 (= 2!) éléments de $\mathfrak{S}_2$ sont $\begin{pmatrix} 1&2 \\ 1&2 \end{pmatrix}$ et $\begin{pmatrix} 1&2 \\ 2&1 \end{pmatrix}$. Les 6 (= 3!) éléments de $\mathfrak{S}_3$ sont

$$\begin{pmatrix} 1&2&3 \\ 1&2&3 \end{pmatrix}, \quad \begin{pmatrix} 1&2&3 \\ 2&1&3 \end{pmatrix}, \quad \begin{pmatrix} 1&2&3 \\ 3&2&1 \end{pmatrix}, \quad \begin{pmatrix} 1&2&3 \\ 1&3&2 \end{pmatrix}, \quad \begin{pmatrix} 1&2&3 \\ 2&3&1 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1&2&3 \\ 3&1&2 \end{pmatrix}.$$

Lemme 5 – Stabilité du support d'une permutation

Soit $\sigma \in \mathfrak{S}_n$. Le support $\mathrm{supp}(\sigma)$ de σ est une partie σ-stable de $[\![1\,,n]\!]$.

Démonstration. ... ■

Théorème 6 – Une condition suffisante pour commuter

Deux permutations disjointes commutent.

Démonstration. ... ■

La définition suivante introduit une classe particulière et importante d'éléments de $\mathfrak{S}_n$ qui permutent circulairement certains éléments de $[\![1\,,n]\!]$ et laissent fixes les autres.

Définition 7 – Cycle, transposition

- **Cycle.** Soit $p \in [\![2\,,n]\!]$. On appelle *p-cycle de $[\![1\,,n]\!]$*, ou *cycle de longueur p de $[\![1\,,n]\!]$*, toute permutation σ de $[\![1\,,n]\!]$ telle qu'il existe p éléments distincts $i_1,\dots,i_p$ de $[\![1\,,n]\!]$ vérifiant

  (i) $\forall j \in [\![1\,,p-1]\!],\quad \sigma(i_j) = i_{j+1}\quad$ et $\quad\sigma(i_p) = i_1\,;\qquad$ **(ii)** $\forall k \in [\![1\,,n]\!]\backslash\{i_1,\dots,i_p\},\quad \sigma(k) = k.$

  On préférera alors noter $(i_1\ i_2\ \cdots\ i_p)$ cette permutation, dont le support est l'ensemble $\{i_1,\dots,i_p\}$.
- **Transposition.** On appelle *transposition* de $[\![1\,,n]\!]$ tout 2-cycle de $[\![1\,,n]\!]$.

Exemple 8

- La permutation $\begin{pmatrix}1&2&3&4&5&6\\1&4&5&3&2&6\end{pmatrix}$ est le cycle $(2\ 4\ 3\ 5)$ de longueur 4. En revanche, la permutation $\begin{pmatrix}1&2&3&4&5&6\\3&4&5&2&6&1\end{pmatrix}$ n'est pas un cycle, mais un produit de cycles, en l'occurence $(1\ 3\ 5\ 6)(2\ 4)$.
- Le cycle $(1\ 5\ 8\ 2\ 9\ 7\ 3)$ de $\mathfrak{S}_9$ correspond à la permutation $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\5&9&1&4&8&6&3&2&7\end{pmatrix}$.
- La transposition $(2\ 5)$ de $\mathfrak{S}_6$ correspond à la permutation $\begin{pmatrix}1&2&3&4&5&6\\1&5&3&4&2&6\end{pmatrix}$.

Exemple 9 Avec cette nouvelle notation pour les cycles,

$$\mathfrak{S}_2 = \{\mathrm{Id}_{[\![1,2]\!]}, (1\ 2)\} \qquad \text{et} \qquad \mathfrak{S}_3 = \{\mathrm{Id}_{[\![1,3]\!]}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

Remarque 10

- La notation $(i_1\ i_2\ \cdots\ i_p)$ pour un p-cycle suggère que tout élément i_j de la liste est envoyé sur l'élément suivant, à l'exception du dernier envoyé sur le premier.
- La représentation d'un cycle sous la forme $(i_1\ i_2\ \cdots\ i_p)$ n'est pas unique, dans la mesure où l'on peut commencer cette représentation par n'importe quel élément de son support.
  Par exemple dans $\mathfrak{S}_3$, $(1\ 2\ 3)$, $(2\ 3\ 1)$ et $(3\ 1\ 2)$ sont trois écritures du même cycle $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ de longueur 3.
  En revanche, $(1\ 2\ 3) \neq (1\ 3\ 2)$! Puisque $(1\ 3\ 2)$ est la permutation $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$.
- L'inverse du p-cycle $(i_1\ i_2\ \cdots\ i_p)$ est le p-cycle $(i_1\ i_2\ \cdots\ i_p)^{-1} = (i_p\ i_{p-1}\ \cdots\ i_1)$.
- Si c est un cycle de longueur p de $[\![1\,,n]\!]$, alors $c^p = \mathrm{Id}_{[\![1,n]\!]}$ et p est le plus petit entier strictement positif k tel que $c^k = \mathrm{Id}_{[\![1,n]\!]}$. On dit que c est d'*ordre p* dans le groupe $\mathfrak{S}_n$.

2 Décomposition d'une permutation en produit de cycles disjoints

Théorème 11 – Décomposition d'une permutation en produit de cycles disjoints

Toute permutation de $[\![1\,,n]\!]$ se décompose d'une et d'une seule manière, à l'ordre près des facteurs, comme un produit de cycles disjoints.

Démonstration. Admis conformément au programme (cf. annexe A). ■

✎ **En pratique** ✎ Pour déterminer la décomposition d'une permutation σ de $[\![1\,,n]\!]$ en produit de cycles disjoints, on peut procéder de la façon suivante :

- Partir de 1 et suivre ses images successives par σ jusqu'à retomber sur 1, ce qui donne le premier cycle.
- Recommencer en partant du plus petit élément de $[\![1\,,n]\!]$ n'appartenant pas au support du cycle déterminé précédemment.
- Poursuivre ainsi jusqu'à épuisement des éléments de $[\![1\,,n]\!]$.

Exemple 12

- La décomposition en cycles disjoints de $\begin{pmatrix}1&2&3&4&5&6&7&8&9&10\\5&2&8&10&7&9&1&3&4&6\end{pmatrix}$ est $(1\ 5\ 7)(3\ 8)(4\ 10\ 6\ 9)$.
- La décomposition en cycles disjoints de $(1\ 2\ 3\ 4\ 5\ 6)(1\ 2\ 4\ 6)(1\ 3\ 5)$ est $(1\ 4)(2\ 5\ 3\ 6)$.

Théorème 13 – Le groupe symétrique est engendré par ses transpositons

Toute permutation de $[\![1\,,n]\!]$ se décompose en un produit de transposition.

Démonstration. Via le théorème 11, il suffit de le vérifier pour un cycle quelconque. Or, pour tous $i_1,\dots,i_p\in[\![1\,,n]\!]$ distincts,

$$(i_1\ \dots\ i_p)=(i_1\ i_2)(i_2\ i_3)\cdots(i_{p-1}\ i_p).$$

■

Ainsi quelque soit la complexité apparente d'une permutation de n objets, celle-ci peut toujours s'effectuer progressivement par des échanges successifs de deux éléments.

✖ **Attention !** ✖ Contrairement à la décomposition en cycles disjoints, il n'y a pas d'unicité pour la décomposition d'une permutation en produit de transpositions, *e.g.* $(1\ 2\ 3)=(1\ 2)(2\ 3)=(1\ 3)(1\ 2)$.

✎ **En pratique** ✎ Pour décomposer une permutation en un produit de transpositions, on peut commencer par en donner la décomposition en produit de cycles disjoints, puis écrire chacun de ces cycles comme un produit de transpositions, comme le suggère la démonstration du théorème 13.

Exemple 14 – Conjugaison d'une transposition/d'un cycle (résultat à connaître) Soit $\sigma\in\mathfrak{S}_n$ une permutation.

- Pour toute transposition $(a\ b)$ de $\mathfrak{S}_n$, $\sigma(a\ b)\sigma^{-1}=(\sigma(a)\ \sigma(b))$.
- Plus généralement, pour tout p-cycle $(i_1\ i_2\ \cdots\ i_p)$ de $\mathfrak{S}_n$, $\sigma(i_1\ i_2\ \cdots\ i_p)\sigma^{-1}=(\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_p))$.

3 Signature d'une permutation

Définition-théorème 15 – Signature

On appelle *signature* d'une permutation σ de $[\![1\,,n]\!]$, notée $\varepsilon(\sigma)$, l'élément de $\{\pm1\}$ défini par

$$\varepsilon(\sigma)=\prod_{1\leqslant i<j\leqslant n}\frac{\sigma(j)-\sigma(i)}{j-i}=\prod_{\{i,j\}\in\mathscr{P}}\frac{\sigma(j)-\sigma(i)}{j-i},$$

où $\mathscr{P}$ désigne l'ensemble des paires (parties de cardinal 2) de $[\![1\,,n]\!]$.

Démonstration. ... ■

Le théorème suivant est le résultat central de ce chapitre.

Théorème 16 – Propriétés de la signature

La signature ε est l'unique morphisme de groupes de $(\mathfrak{S}_n,\circ)$ sur $(\{\pm1\},\times)$ qui attribue à toute transposition la valeur -1.

Démonstration. ... ■

Définition 17 – Permutation paire/impaire, groupe alterné

- Une permutation $\sigma\in\mathfrak{S}_n$ est dite *paire* lorsque $\varepsilon(\sigma)=1$ et *impaire* lorsque $\varepsilon(\sigma)=-1$.
- On appelle *groupe alterné (de degré n)*, noté $\mathfrak{A}_n$, le noyau de la signature ε, *i.e.* le sous-groupe de $\mathfrak{S}_n$ formé de l'ensemble des permutations paires.

Remarque 18 Soit $n\geqslant2$. Si τ est une permutation impaire de $\mathfrak{S}_n$, alors $\mathfrak{S}_n\backslash\mathfrak{A}_n=\tau\mathfrak{A}_n=\mathfrak{A}_n\tau$. Précisément, les applications $\sigma\longmapsto\tau\sigma$ et $\sigma\longmapsto\sigma\tau$ sont des bijections de l'ensemble $\mathfrak{A}_n$ des permutations paires sur l'ensemble $\mathfrak{S}_n\backslash\mathfrak{A}_n$ des permutations impaires. En particulier, ces deux ensembles finis ont le même cardinal, à savoir $n!/2$.

Il découle immédiatement des propriétés du morphisme de signature ε les deux corollaires suivants.

Corollaire 19

Si $\sigma = \tau_1\tau_2\cdots\tau_p$ est une décomposition en produit de transpositions de la permutation σ, alors $\varepsilon(\sigma) = (-1)^p$.

Ainsi, bien qu'il n'y ait pas unicité de la décomposition en produit de transposition d'une permutation, la parité du nombre de transpositions intervenant dans un tel produit est elle invariante.

Corollaire 20 – Signature d'un cycle

Pour tout $p \in [\![2\,,n]\!]$, la signature d'un p-cycle de $[\![1\,,n]\!]$ vaut $(-1)^{p-1}$.

Démonstration. Tout p-cycle se décompose en un produit de $p-1$ transpositions (cf. démonstration du théorème 13). ■

✎ **En pratique** ✎ Pour calculer la signature d'une permutation, une stratégie efficace consiste à en déterminer une décomposition en cycles (par forcément disjoints dans ce cas).

Exemple 21

- La permutation $(1\ 5\ 3)(2\ 4\ 6\ 1)(3\ 4)$ est paire.

  En effet, $\varepsilon\big((1\ 5\ 3)(2\ 4\ 6\ 1)(3\ 4)\big) = \varepsilon\big((1\ 5\ 3)\big)\varepsilon\big((2\ 4\ 6\ 1)\big)\varepsilon\big((3\ 4)\big) = (-1)^{3-1}(-1)^{4-1}(-1)^{2-1} = 1.$
- La permutation $\begin{pmatrix}1&2&3&4&5&6\\5&2&6&1&4&3\end{pmatrix}$ est impaire.

  En effet, la décomposition en cycles disjoints de cette permutation est $(1\ 5\ 4)(3\ 6)$ et

$$\varepsilon\big((1\ 5\ 4)(3\ 6)\big) = \varepsilon\big((1\ 5\ 4)\big)\varepsilon\big((3\ 6)\big) = (-1)^{3-1}(-1)^{2-1} = -1.$$

Compétences à acquérir

- Calculer dans le groupe $\mathfrak{S}_n$: exercices 1 à 3, 8, 9 et 11 à 13.
- Décomposer une permutation en produit de cycles disjoints/de transpositions : exercices 1, 2 et 11.
- Calculer la signature d'une permutation : exercices 1, 2 et 4.
- Énumérer/dénombrer des éléments de $\mathfrak{S}_n$: exercices 3 et 6.

Quelques résultats classiques :

- Conjugaison d'un cycle (exemple 14).
- Nombre de k-cycles dans $\mathfrak{S}_n$ (exercice 6).
- Exemples de parties génératrices de $\mathfrak{S}_n$ (exercice 11).
- Les 3-cycles engendrent $\mathfrak{A}_n$ (exercice 12).
- Centre du groupe symétrique (exercice 9).
- Éléments conjugués dans $\mathfrak{S}_n$ et $\mathfrak{A}_n$ (exercice 13).
- Matrices de permutation (exercice 14).

A Annexe

Démonstration du théorème 11 Soit $\sigma \in \mathfrak{S}_n$.

Existence. Définissons une relation binaire sur $[\![1\,,n]\!]$ par

$$x \sim_\sigma y \quad \Longleftrightarrow \quad \exists k \in \mathbb{Z}, \quad y = \sigma^k(x),$$

pour tous $x, y \in [\![1\,,n]\!]$. On vérifie sans difficulté qu'il s'agit d'une relation d'équivalence puisque, pour tous $x, y, z \in [\![1\,,n]\!]$,

- *Réflexivité.* Puisque $\sigma^0 = \mathrm{Id}_{[\![1,n]\!]}$, $x = \sigma^0(x)$ et $x \sim_\sigma x$.
- *Symétrie.* Si $x \sim_\sigma y$, alors il existe $k \in \mathbb{Z}$ tel que $y = \sigma^k(x)$, d'où $x = \sigma^{-k}(y)$ avec $-k \in \mathbb{Z}$, soit $y \sim_\sigma x$.
- *Transitivité.* Si $x \sim_\sigma y$ et $y \sim_\sigma z$, alors il existe $k, l \in \mathbb{Z}$ tels que $y = \sigma^k(x)$ et $z = \sigma^l(y)$, ainsi

$$z = \sigma^l\Big(\sigma^k(x)\Big) = \sigma^{l+k}(x)$$

avec $k + l \in \mathbb{Z}$, d'où $z \sim_\sigma x$.

Notons alors $X_1, \ldots, X_r$ les classes d'équivalence de $[\![1\,,n]\!]$ pour la relation $\sim_\sigma$ et x_i un représentant de X_i, pour tout $i \in [\![1\,,r]\!]$.

Soit $i \in [\![1\,,r]\!]$, on a alors $X_i = \big\{\sigma^k(x_i) \;\big|\; k \in \mathbb{Z}\big\}$, pour tout $i \in [\![1\,,r]\!]$, par définition. Or X_i est un ensemble fini, il existe donc $k, l \in \mathbb{Z}$ avec $k < l$ tels que $\sigma^k(x_i) = \sigma^l(x_i)$, soit $\sigma^{l-k}(x_i) = x_i$ avec $l - k \in \mathbb{N}^*$, ce qui nous autorise à considérer

$$p_i = \min\Big\{k \in \mathbb{N}^* \;\Big|\; \sigma^k(x_i) = x_i\Big\}.$$

Une division euclidienne par p_i permet alors d'établir que $X_i = \big\{x_i, \sigma(x_i), \ldots, \sigma^{p_i-1}(x_i)\big\}$ avec $|X_i| = p_i$.

Pour tout $i \in [\![1\,,r]\!]$, notons finalement σ_i le p_i-cycle $\big(x_i \;\; \sigma(x_i) \;\; \ldots \;\; \sigma^{p_i-1}(x_i)\big)$ de support X_i (*on s'autorise ici à considérer des cycles de longueur* 1). Par construction, ces r cycles sont disjoints et, pour tout $i \in [\![1\,,r]\!]$, $\sigma_i|_{X_i} = \sigma|_{X_i}$. En somme, $\sigma = \sigma_1 \cdots \sigma_r$, ce qui correspond à la décomposition souhaitée.

Unicité. Montrons l'unicité de la décomposition $\sigma = \sigma_1 \cdots \sigma_r$ par récurrence sur r.

Si $r = 1$, alors σ est un n-cycle et l'unicité est claire.

Soit $r \geqslant 2$ et supposons l'unicité acquise pour les permutations pouvant s'exprimer comme produit de strictement moins de r-cycles disjoints. Considérons le cas où $\sigma = \sigma_1 \cdots \sigma_r$ est le produit de r cycles disjoints et donnons-nous $\sigma = \sigma'_1 \cdots \sigma'_q$ une seconde écriture de σ en produit de cycles à supports disjoints. En reprenant les notations précédentes, l'élément x_1 du support X_1 du cycle σ_1 appartient au support d'un des cycles σ'_j et à un seul et, quitte à les renuméroter, on peut supposer que $j = 1$. Ayant $\sigma^k(x_1) = \sigma_1^k(x_1) = {\sigma'_1}^k(x_1)$, pour tout $k \in \mathbb{Z}$, il vient $\sigma_1 = \sigma'_1$ et, après simplification, $\sigma_2 \cdots \sigma_r = \sigma'_2 \cdots \sigma'_q$. D'après l'hypothèse de récurrence, on a donc $q = r$ et $\{\sigma_2, \ldots, \sigma_r\} = \{\sigma'_2, \ldots, \sigma'_r\}$, d'où l'unicité de la décomposition de σ.

Remarque : l'existence et l'unicité de la décomposition en cycles à supports disjoints d'une permutation σ s'établissent également par récurrence forte décroissante sur le nombre d'éléments de $[\![1\,,n]\!]$ fixés par σ.