Groupe symétrique

Cornou Jean-Louis

25 avril 2023

On fixe dans tout ce qui suit n un entier naturel non nul.

1 Groupe symétrique

Définition 1 *L'ensemble des permutations de l'ensemble $[\![1,n]\!]$ est appelé groupe symétrique, noté S_n ou $\mathfrak{S}_n$.*

Propriété 1 *Le groupe symétrique muni de la loi de composition est un groupe. Il est non commutatif dès que $n \geq 3$.*

Démonstration. On a déjà vu que les bijections d'un ensemble E forment un groupe pour la loi de composition. Si $n \geq 3$, on note $\tau : 1 \mapsto 2, 2 \mapsto 1, k \mapsto k$ si $k \notin \{1,2\}$, puis $\sigma : 1 \mapsto 3, 3 \mapsto 1, k \mapsto k$ si $k \notin \{1,3\}$. Alors $\tau \circ \sigma(1) = 3$, tandis que $\sigma \circ \tau(1) = 2$, donc $\sigma \circ \tau \neq \tau \circ \sigma$.

Notation
On change de notation pour les permutations : soit $\sigma \in S_n$. On la note sous la forme

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

Le symbole de composition entre permutations est parfois omis.

Exemple 1 *La bijection : $\sigma : 1 \mapsto 2, 2 \mapsto 1, 4 \mapsto 3, 3 \mapsto 3$ se note*

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

Définition 2 *Soit $x \in [\![1,n]\!]$ et $\sigma \in S_n$. On appelle orbite de x sous σ l'ensemble $\{\sigma^k(x) | k \in \mathbb{N}\}$, noté parfois $\mathcal{O}(x)$.*

Exemple 2 *Avec l'exemple précédent, $\mathcal{O}(1) = \{1,2\} = \mathcal{O}(2)$ tandis que $\mathcal{O}(3) = \mathcal{O}(4) = \{3,4\}$.*

Exercice 1 *Soit $\sigma \in S_n$. On définit la relation binaire $\mathcal{R}$ sur $[\![1,n]\!]$ via*

$$\forall (x,y) \in [\![1,n]\!]^2, x \mathcal{R} y \iff \exists z \in [\![1,n]\!], x \in \mathcal{O}(z) \wedge y \in \mathcal{O}(z)$$

Démontrer que la relation binaire $\mathcal{R}$ est une relation d'équivalence. En déduire que les orbites sous σ forment une partition de $[\![1,n]\!]$.

Définition 3 *Soit $\sigma \in S_n$. On appelle support de σ l'ensemble des points de $[\![1,n]\!]$ non fixes par σ i.e $\{x \in [\![1,n]\!] \,|\, \sigma(x) \neq x\}$.*

Exercice 2 *Soit $\sigma \in S_n$. Montrer que le support de σ n'est pas de cardinal $n-1$.*

Définition 4 *Soit $p \in \mathbb{N}^*$, $a_1, \dots, a_p$ des éléments distincts de $[\![1,n]\!]$. On appelle cycle de support $a_1, \dots, a_p$ la permutation γ définie par*

$$\forall j \in [\![1, p-1]\!], \gamma(a_j) = a_{j+1}, \gamma(a_p) = a_1, \forall x \in [\![1,n]\!] \backslash \{a_1, \dots, a_p\}, \gamma(x) = x$$

On la note $(a_1 \dots a_p)$. L'entier p est alors appelé la longueur de γ.

⚠ **Attention**
L'ordre des éléments a_i n'est pas unique. On a l'égalité de permutations : $(1\,3\,2\,4\,5) = (4\,5\,1\,3\,2)$.

☞ **Remarque**
Les cycles de longueur 1 *sont l'identité.*

Exemple 3 *Soit* $\gamma = (1\,2\,3)$ *et* $\tau = (1\,5)$ *dans* $\mathfrak{S}_5$. *On écrit la composée* $\gamma \circ \tau$:

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

On remarque qu'on peut l'écrire sous la forme $(1\,5\,2\,3)$. *Calculons* $\tau \circ \gamma$.

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

qui vaut également $(1\,2\,3\,5)$ *et diffère de* $\gamma \circ \tau$.

Exercice 3 *Montrer que l'inverse du cycle* $(a_1 \dots a_p)$ *est le cycle* $(a_p \dots a_1)$.

Définition 5 *On appelle transposition tout cycle de support de longueur 2.*

Exercice 4 *Démontrer que toute transposition est involutive.*

Propriété 2 *Soit* γ *et* γ' *deux cycles à supports disjoints. Alors* $\gamma\gamma' = \gamma'\gamma$.

Démonstration. Notons $\gamma = (a_1 \dots a_p)$ et $\gamma' = (b_1 \dots b_q)$. Comme ces supports sont disjoints, on sait que $\forall (i,j) \in [\![1,p]\!] \times [\![1,q]\!], a_i \neq b_j$. Soit $k \in [\![1,n]\!]$. Il a trois cas à envisager :

- $\exists i \in [\![1,p]\!], k = a_i$, alors $k \notin \{b_1, \dots, b_q\}$, donc $\gamma'(k) = k = a_i$, d'où $\gamma(\gamma'(k)) = \gamma(a_i) = a_{i+1}$ avec la convention $a_{p+1} = a_1$. D'autre part, $\gamma(k) = a_{i+1}$ et $a_{i+1} \notin \{b_1, \dots, b_q\}$, donc $\gamma'(\gamma(k)) = \gamma'(a_{i+1}) = a_{i+1}$.
- $\exists j \in [\![1,q]\!], k = b_j$, alors $j \notin \{a_1, \dots, a_p\}$, donc $\gamma(k) = k = b_j$, d'où $\gamma'(\gamma(k)) = \gamma(b_j) = b_{j+1}$ avec la convention $b_{q+1} = b_1$. D'autre part, $\gamma'(k) = b_{j+1}$ et $b_{j+1} \notin \{a_1, \dots, a_p\}$, donc $\gamma(\gamma'(k)) = \gamma(b_{j+1}) = b_{j+1}$.
- $k \notin \{a_1, \dots, a_p\} \cup \{b_1, \dots, b_q\}$, alors $\gamma(k) = k$ non plus, ni $\gamma'(k) = k$. Dans ce cas, $\gamma'(\gamma(k)) = k = \gamma(\gamma'(k))$.

Dans tous les cas, $\gamma(\gamma'(k)) = \gamma'(\gamma(k))$. D'où l'égalité des premutations.

Définition 6 *Soit* σ *et* σ' *deux permutations. On dit que que* σ *et* σ' *sont conjugées lorsqu'il existe une permutation* ξ *telle que*

$$\sigma = \xi \sigma' \xi^{-1}$$

Propriété 3 *Soit* $(a\,b)$ *et* $(c\,d)$ *deux transpositions. Alors elles sont conjugées.*

Démonstration. Montrons que $(a\,b)$ est conjuguée à $(1\,2)$. Si $a = 1$ et $b = 2$, c'est gagné. Sinon, comme $(a\,b) = (b\,a)$ on peut supposer $b \neq 1$ et $i \neq 2$. On calcule alors les produits

$$(1\,b)(1\,2)(1\,b) = (b\,2) \quad \text{et} \quad (2\,a)(b\,2)(2\,a) = (a\,b)$$

On en déduit

$$(a\,b) = (2\,a)(1\,b)(1\,2)(1\,b)(2\,a)$$

Ceci est bien une conjugaison puisque $[(2\,a)(1\,b)]^{-1} = (1\,b)(2\,a)$. De même, $(c\,d)$ est conjugée à $(1\,2)$. Par conséquent, $(c\,d)$ est conjugée à $(a\,b)$

Exercice 5 *Soit* $\sigma \in \mathfrak{S}_n$ *et* $a_1, \dots, a_p$ *des éléments distincts de* $[\![1,n]\!]$. *Montrer que*

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

2 Décomposition de permutations

Lemme 1 *Soit $\sigma \in S_n$ et O une orbite de σ. Alors σ induit un cycle sur O.*

Démonstration. Le cas où O est de cardinal 1 est trivial. Supposons $|O| \geq 2$. Notons $x \in$. On sait que $O = \{\sigma^k(x) | k \in \mathbb{N}\}$ est finie, donc qu'il existe un entier p non nul minimal tel que $\sigma^p(x) = x$. Montrons alors que $\{x, \sigma(x), \dots, \sigma^{p-1}(x)\} = O$. L'inclusion $\{x, \sigma(x), \dots, \sigma^{p-1}(x)\} \subset O$ est claire. Réciproquement, soit $k \in \mathbb{N}$, on effectue la division euclidienne de k par p sous la forme $k = pq + r$, ce qui entraîne $\sigma^k(x) = \sigma^r(\sigma^{pq}(x)) = \sigma^r(x)$. Comme $r \in [\![0, p-1]\!]$, on a bien $O \subset \{x, \sigma(x), \dots, \sigma^{p-1}(x)\}$.
Notons à présent $s : O \to [\![1, n]\!], i \mapsto \sigma(i)$. Il est clair que $s(O) \subset O$, on continue de noter s la corestriction de s à O. En notant $a_0 = x, \dots, a_{p-1} = \sigma^{p-1}(x)$. Il est clair que pour tout entier j dans $[\![0, p-2]\!]$, $s(a_j) = a_{j+1}$ et $s(a_{p-1}) = \sigma(\sigma^{p-1}(x)) = \sigma^p(x) = x = a_0$. Ainsi, s est bien un cycle.

Théorème 1 *Toute permutation se décompose de manière unique à l'ordre près en produit de cycles à supports disjoints.*

☞ **Remarque**
Si cette permutation est l'identité, on convient qu'elle vaut le produit vide.

Démonstration. Existence : On procède par récurrence forte sur n. Pour $n = 1$, il n'y a qu'une possibilité, le produit vide. Pour $n = 2$, la seule permutation différente de l'identité est un cycle de longueur de 2. Soit $n \in \mathbb{N}^*$. Supposons le théorème vrai pour tout $k \in [\![1, n]\!]$, et démontrons le pour $n+1$. Soit $\sigma \in S_{n+1}$, si σ est l'identité, c'est un produit vide. Sinon, il existe i dans $[\![1, n+1]\!]$ tel que $\sigma(i) \neq i$. On considère alors l'orbite $O = \mathcal{O}(i)$, celle-ci est de cardinal au moins 2. On définit alors

$$s : k \mapsto \begin{cases} k & \text{si } k \notin O \\ \sigma(k) & \text{si } k \in O \end{cases}$$

On a vu que cette permutation est un cycle. Elle vérifie $\forall x \in O, s^{-1}(x) \in O$. Donc la permutation $\sigma \circ s^{-1}$ vérifie

$$\forall x \in O, \sigma(s^{-1}(x)) = \sigma(\sigma^{-1}(x)) = x$$

Par conséquent, le support de $\sigma \circ s^{-1}$ est inclus dans $[\![1, n+1]\!] \backslash O$. Elle induit donc une permutation sur $[\![1, n+1]\!] \backslash O$ qui est de cardinal inférieur ou égal à n. D'après l'hypothèse de récurrence, $\sigma \circ s^{-1}$ s'écrit sous la forme $\gamma_1 \circ \gamma_m$ avec $(\gamma_i)_{1 \leq i \leq m}$ des cycles à supports disjoints. Leurs supports sont donc disjoints de O, donc $\sigma = s \circ \gamma_1 \circ \gamma_m$ est bien un produit de cycles à supports disjoints.
Unicité à l'ordre près : admise. L'idée serait de montrer que dans une telle décomposition, les cycles sont déterminés de manière unique par les orbites de la permutation considérée.

Exemple 4 *On considère la permutation σ définie par*

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 3 & 1 & 4 & 6 & 7 & 10 & 2 & 9 & 8 \end{pmatrix}$$

On commencer par étudier l'orbite de 1, ce qui donne le cycle (156710823). Il nous reste à étudier l'effet de σ sur $[\![1, 10]\!]$ privé de cette orbite. 4 et 9 sont fixes sous σ. Donc σ est le cycle (156710823). Considérons la permutation σ' définie par

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 3 & 4 & 8 & 5 & 7 & 1 & 2 & 9 & 10 \end{pmatrix}$$

L'orbite de 1 donne le cycle (167). L'orbite de 2 donne le cycle (2348). σ' fixe 5, 9 et 10, donc $\sigma' = (167)(2348)$.

Théorème 2 *Toute permutation se décompose en produit de transpositions.*

Démonstration. D'après le théorème précédent, il suffit de décomposer chaque cycle en produit de transpositions. Soit $\gamma = (a_1 \dots a_p)$ un cycle. Montrons

$$\gamma = (a_1\, a_2) \circ (a_2\, a_3) \circ \dots \circ (a_{p-1}\, a_p)$$

Soit $k \in [\![1, n]\!]$.

— Si $k \notin \{a_1, \dots, a_p\}$, alors $\gamma(k) = k$. De même, toutes les transpositions ci-dessus fixent k, donc leur composée également.

— Si $k \in \{a_2 \dots a_{p-1}\}$. Notons $j \in [\![2, p-1]\!]$ tel que $k = a_j$. Seules les transpositions $(a_{j-1}\ a_j)$ et $(a_j a_{j+1})$ comportent a_j dans leur support. Mais alors $(a_{j-1}\ a_j)[(a_j a_{j+1})(a_j)] = (a_{j-1}\ a_j)(a_{j+1}) = a_{j+1}$

— Si $k = a_1$, seule la transposition $(a_1\ a_2)$ ne fixe pas a_1 et $(a_1\ a_2)(a_1) = a_2$.

— Si $k = a_p$,

$$(a_1\ a_2) \circ (a_2\ a_3) \circ \cdots \circ (a_{p-1}\ a_p)(a_p) = (a_1\ a_2) \circ (a_2\ a_3) \circ \cdots \circ (a_{p-2}\ a_{p-1})(a_{p-1}) = \cdots = (a_1\ a_2)(a_2) = a_1$$

Dans tous les cas, $(a_1\ a_2) \circ (a_2\ a_3) \circ \cdots \circ (a_{p-1}\ a_p)(k) = \gamma(k)$, d'où l'égalité d'applications.

Exercice 6 *Montrer que la famille* $\{(1\ k) | k \in [\![2, n]\!]\}$ *engendre le groupe* S_n.

3 Signature

Définition 7 *Soit* $\sigma \in \mathrm{S}_n$. *Soit* $(i, j) \in [\![1, n]\!]^2$ *tels que* $i \neq j$. *On dit que* $\{i, j\}$ *est une inversion pour* σ *si* $(i-j)(\sigma(i)-\sigma(j)) < 0$. *On note* $Inv(\sigma)$ *le nombre d'inversions de* σ.

☞ **Remarque**
On dit bien que la paire $\{i, j\}$ *est une inversion, et non le couple* (i, j) *car* $(i-j)(\sigma(i)-\sigma(j)) = (j-i)(\sigma(j)-\sigma(i))$.

Définition 8 *Soit* $\sigma \in \mathrm{S}_n$. *On appelle signature de* σ, *la quantité* $(-1)^{Inv(\sigma)}$, *notée* $\varepsilon(\sigma)$.

Exemple 5 *Soit* $\tau = (1\ 2)$ *une transposition. Alors* $(\tau(1) - \tau(2))(1-2) = (2-1)(1-2) = -1 < 0$. *C'est la seule inversion puisque* $\forall k \geq 3, (1-k)(2-k) > 0$ *et* $\forall (k, l) \geq 3 (k-l)(k-l) > 0$. *Ainsi,* $\varepsilon(\tau) = (-1)^1 = -1$.

Propriété 4 *Soit* $\sigma \in \mathrm{S}_n$. *Alors*

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

Démonstration. Soit $(i, j) \in [\![1, n]\!]^2$ tel que $i < j$. Si c'est une inversion, $\sigma(i) - \sigma(j)$ est du signe de $j - i$, donc $\frac{\sigma(i)-\sigma(j)}{i-j} = -\frac{|\sigma(i)-\sigma(j)|}{|i-j|}$. Si ce n'est pas un inversion, numérateur et dénominateur ont même signe et $\frac{\sigma(i)-\sigma(j)}{i-j} = \frac{|\sigma(i)-\sigma(j)|}{|i-j|}$. Ainsi,

$$\prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j} = (-1)^{\mathrm{Inv}(\sigma)} \prod_{1 \leq i < j \leq n} \frac{|\sigma(i) - \sigma(j)|}{|i - j|}$$

Or σ induit une bijection sur les paires de $[\![1, n]\!]$, donc

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

Par conséquent, $\varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)}$.

Théorème 3 *La signature est un morphisme de groupes entre* $(\mathrm{S}_n, \circ)$ *et* $(\{-1, 1\}, \times)$.

Démonstration. Soit σ_1, σ_2 deux permutations, alors

$$\varepsilon(\sigma_1 \circ \sigma_2) = \prod_{1 \leq i < j \leq n} \frac{\sigma_1 \circ \sigma_2(i) - \sigma_1 \circ \sigma_2(j)}{i - j} = \prod_{1 \leq i < j \leq n} \frac{\sigma_1 \circ \sigma_2(i) - \sigma_1 \circ \sigma_2(j)}{\sigma_2(i) - \sigma_2(j)} \prod_{1 \leq i < j \leq n} \frac{\sigma_2(i) - \sigma_2(j)}{i - j}$$

Comme σ_2 est une bijection,

$$\prod_{1 \leq i < j \leq n} \frac{\sigma_1 \circ \sigma_2(i) - \sigma_1 \circ \sigma_2(j)}{\sigma_2(i) - \sigma_2(j)} = \prod_{1 \leq i < j \leq n} \frac{\sigma_1(i) - \sigma_1(j)}{i - j} = \varepsilon(\sigma_1)$$

On reconnaît alors

$$\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$$

Exemple 6 *Soit $\tau = (a\,b)$ une transposition, alors τ est conjuguée à $(1\,2)$. Par commutativité du produit dans $\{-1,1\}$, $\varepsilon(\tau) = \varepsilon((1\,2)) = -1$. Soit γ un cycle de longueur p, alors γ est produit de $p-1$ transpositions donc $\varepsilon(\gamma) = (-1)^{p-1}$. Soit σ une permutation, on la décompose sous la forme $\gamma_1 \dots \gamma_q$ en notant pour tout k dans $[\![1,q]\!]$, p_k la longueur de γ_k, on obtient*

$$\varepsilon(\sigma) = \prod_{k=1}^{q} (-1)^{p_k - 1} = (-1)^{\sum_{k=1}^{q} p_k - q} = (-1)^{S-q}$$

avec S le cardinal du support de σ.

Propriété 5 *Soit $\varphi : S_n \to \mathbb{C}^*$ un morphisme de groupes non trivial. Alors c'est la signature.*

Démonstration. Soit τ une transposition. Comme $\tau^2 = \mathrm{id}$, et φ est un morphisme de groupes, $\varphi(\tau)^2 = \varphi(\tau^2) = \varphi(\mathrm{id}) = 1$. Par conséquent, $\varphi(\tau) = \pm 1$. Si $\varphi(\tau) = 1$, alors pour toute transposition τ', $\varphi(\tau') = \varphi(\tau)$ car τ et τ' sont conjuguées. Mais alors comme toute permutation est produit de transpositions, φ est constante égale à 1. Par conséquent, $\varphi(\tau) = -1$, et de même que précédemment, pour toute transposition τ', $\varphi(\tau') = \varphi(\tau) = -1$. Par conséquent, φ coïncide avec la signature sur une partie génératrice de S_n, donc est égale à la signature.

Définition 9 *On appelle permutation paire toute permutation de signature 1. Leur ensemble est appelé groupe alterné noté $\mathcal{A}_n$.*

Propriété 6 *Le groupe alterné est un groupe.*

Démonstration. C'est le noyau du morphisme signature, donc un sous-groupe de S_n.

Exemple 7 *Le groupe $\mathcal{A}_4$ ne comporte que les permutations paires du groupe S_4. Faisons une liste rapide. Dans S_4, il y a l'identité, 6 transpositions, 8 cycles de longueur 3, 6 cycles de longueur 4 et 3 produits de deux transpositions (ou doubles transpositions). Dans $\mathfrak{A}_4$, il n'y a que l'identité, 8 cycles de longueur 3 et 3 doubles transpositions. On peut continuer le dévissage et constater que l'ensemble formé de l'identité et des doubles transpositions fournit un sous-groupe strict de $\mathfrak{A}_4$.*

Exercice 7 *On suppose $n \geq 3$. Démontrer que la famille $\{(1\,2\,k) | k \in [\![3,n]\!]\}$ engendre $\mathcal{A}_n$.*