Mathieu Kieffer

66 leçons pour l'agrégation de mathématiques

avec 10 fiches de synthèse

2e édition

ellipses

Chapitre 2

Permutations d'un ensemble fini, groupe symétrique. Applications

Pré-requis

1. Composition de deux applications.
2. Définition d'une bijection.
3. Notions sur les groupes.
4. Relation d'équivalence sur un ensemble.
5. Division euclidienne.
6. Isométries du plan.

2.1 Permutations d'un ensemble fini

Définition 16. Soit $n \in \mathbb{N}^*$. On appelle permutation de $[\![1;n]\!]$ toute bijection de $[\![1;n]\!]$ dans $[\![1;n]\!]$. L'ensemble des permutations de $[\![1;n]\!]$ est noté $\mathfrak{S}_n$.

Remarque. Notation matricielle d'une permutation σ :

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

Proposition 17. *Soit $n \in \mathbb{N}^*$.*

1. *$(\mathfrak{S}_n, \circ)$ est un groupe d'ordre $n!$.*
2. *$(\mathfrak{S}_n, \circ)$ est abélien si, et seulement si, $n \leqslant 2$.*

Démonstration. 1. $(\mathfrak{S}_n, \circ)$ est clairement un groupe. Soit $\sigma \in (\mathfrak{S}_n, \circ)$. Définir σ revient à définir $\sigma(i)$ pour tout $i \in [\![1; n]\!]$. Pour $\sigma(1)$ nous avons n choix possibles, pour $\sigma(2)$, nous avons alors $n-1$ choix possibles, pour $\sigma(3)$, nous avons alors $n-2$ choix possibles, etc. D'où $n!$ manières différentes de définir σ. Ainsi $|\mathfrak{S}_n| = n!$.

2. $(\mathfrak{S}_1 = \{\mathrm{id}\}, \circ)$ est clairement abélien. On vérifie aisément que $(\mathfrak{S}_2, \circ)$ est abélien.
En revanche, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$
et $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.
Donc $(\mathfrak{S}_3, \circ)$ n'est pas abélien. Pour démontrer que, pour tout $n \geqslant 3$, $(\mathfrak{S}_n, \circ)$ n'est pas abélien il suffit de considérer les deux permutations σ et σ' telles que $\sigma(1) = 1$, $\sigma(2) = 3$, $\sigma(3) = 2$, $\sigma'(1) = 3$, $\sigma'(2) = 1$, $\sigma'(3) = 2$ et pour tout $i \in [\![4; n]\!]$, $\sigma(i) = \sigma'(i) = i$, lorsque $n \geqslant 4$. □

Définition 18. Soit $n \in \mathbb{N}^*$. Soit $\sigma \in (\mathfrak{S}_n, \circ)$.

- On appelle support de σ l'ensemble des entiers $k \in [\![1; n]\!]$ tels que $\sigma(k) \neq k$. On note $\mathrm{supp}(\sigma) \coloneqq \{k \in [\![1; n]\!],\ \sigma(k) \neq k\}$.
- On appelle point fixe de σ tout élément $k \in [\![1; n]\!]$ tel que $\sigma(k) = k$. On note $\mathrm{fix}(\sigma) \coloneqq \{k \in [\![1; n]\!],\ \sigma(k) = k\}$.

Remarque. $\forall\, \sigma \in (\mathfrak{S}_n, \circ)$, $[\![1; n]\!] = \mathrm{fix}(\sigma) \bigsqcup \mathrm{supp}(\sigma)$.

Proposition 19. *Soit $n \in \mathbb{N}^*$. Soit $\sigma \in (\mathfrak{S}_n, \circ)$. La relation binaire $\Re$ définie sur $[\![1; n]\!]$ par :*

$$(x \Re y) \iff \big(\exists\, k \in \mathbb{Z},\ y = \sigma^k(x)\big)$$

est une relation d'équivalence. La classe d'équivalence de x est appelée la σ-orbite de x. Elle est notée $orb_{\langle\sigma\rangle}(x)$. On a donc $orb_{\langle\sigma\rangle}(x) = \{\sigma^k(x),\ k \in \mathbb{Z}\}$.

Démonstration. - *Réflexivité :* $x \Re x$ car $x = \sigma^0(x) = \mathrm{id}(x)$.

- *Symétrie :* $x \Re y$. Donc il existe $k \in \mathbb{Z}$, tel que $y = \sigma^k(x)$.

D'où : $x = (\sigma^k)^{-1}(y) = \sigma^{-k}(y)$Ainsi, $y \Re x$.

- *Transitivité :* $x \Re y$ et $y \Re z$. Donc il existe k, $k' \in \mathbb{Z}$, tels que $y = \sigma^k(x)$ et $z = \sigma^{k'}(y)$. Ainsi, $z = (\sigma^{k'} \circ \sigma^k)(x) = \sigma^{k+k'}(x)$ et $x \Re z$. □

Exemple. Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix} \in \mathfrak{S}_5$, on a :

$$\begin{cases} \mathrm{orb}_{\langle\sigma\rangle}(4) = \{4\} \\ \mathrm{orb}_{\langle\sigma\rangle}(3) = \{3\} \\ \mathrm{orb}_{\langle\sigma\rangle}(1) = \mathrm{orb}_{\langle\sigma\rangle}(2) = \mathrm{orb}_{\langle\sigma\rangle}(5) = \{1;2;5\} \end{cases}$$

Définition 20. Soit n un entier naturel tel que $n \geqslant 2$. On dit qu'une permutation $\sigma \in (\mathfrak{S}_n, \circ)$ est un cycle lorsqu'il existe une unique σ-orbite non réduite à un point. Autrement dit, $\sigma \in (\mathfrak{S}_n, \circ)$ est un cycle lorsqu'il existe un entier naturel p tel que $p \geqslant 2$, $a_1, \ldots, a_p \in [\![1; n]\!]$ deux à deux distincts tels que :

$$\begin{cases} \forall\, k \in \{1, \ldots, p-1\},\ \sigma(a_k) = a_{k+1} \\ \sigma(a_p) = a_1 \\ \forall\, x \notin \{a_1, \ldots, a_p\},\ \sigma(x) = x \end{cases}$$

L'entier p est alors appelé la longueur du cycle σ. On la note $l(\sigma)$.
σ est alors appelé un p-cycle et est noté $\sigma \coloneqq (a_1,\ a_2, \ldots,\ a_p)$. Un cycle de longueur 2 est appelé une transposition.

Exemples. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix} \in \mathfrak{S}_5$ est un 5-cycle car elle n'admet qu'une seule σ-orbite non réduite à un point. On écrit $\sigma = (1,\ 4,\ 5,\ 2,\ 3)$.

$\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} \in \mathfrak{S}_5$ n'est pas un cycle car elle admet deux orbites non réduites à un point. En effet, $\mathrm{orb}_{\langle\sigma\rangle}(1) = \{1;4;5\}$ et $\mathrm{orb}_{\langle\sigma\rangle}(2) = \{2;3\}$.

Remarque. On a :
$\mathrm{supp}(a_1,\ a_2, \ldots,\ a_p) = \{a_1, a_2, \ldots, a_p\}$.
$\mathrm{fix}(a_1,\ a_2, \ldots,\ a_p) = [\![1; n]\!] \setminus \{a_1, a_2, \ldots, a_p\}$.

Proposition 21. *Soient n, $p \in \mathbb{N}$ tels que $2 \leqslant p \leqslant n$. Soit $c \coloneqq (a_1,\ a_2, \ldots,\ a_p)$ un p-cycle de $(\mathfrak{S}_n, \circ)$.*

1. $\forall\, \sigma \in \mathfrak{S}_n,\ \sigma \circ c \circ \sigma^{-1} = (\sigma(a_1),\ \sigma(a_2), \ldots,\ \sigma(a_p))$.
2. $\forall\, x \in \mathrm{supp}(c),\ \mathrm{supp}(c) = \{c^k(x),\ k \in \mathbb{Z}\}$.
3. *L'ordre de c dans $(\mathfrak{S}_n, \circ)$ vaut $l(c)$.*
4. $\forall\, x \in \mathrm{supp}\ (c),\ c = \big(x,\ c(x),\ c^2(x), \ldots,\ c^{l(c)-1}(x)\big)$.

Démonstration. 1. On a :

$$\begin{aligned} & x \in \text{fix}(\sigma \circ c \circ \sigma^{-1}) \\ \Leftrightarrow \quad & (\sigma \circ c \circ \sigma^{-1})(x) = x \\ \Leftrightarrow \quad & (c \circ \sigma^{-1})(x) = \sigma^{-1}(x) \\ \Leftrightarrow \quad & \sigma^{-1}(x) = \text{fix}(c) \\ \Leftrightarrow \quad & x \in (\sigma \text{fix}(c)) \\ \Leftrightarrow \quad & x \in \text{fix}\left((\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_p))\right) \end{aligned}$$

et :

$$\begin{aligned} & x \in \text{supp}(\sigma \circ c \circ \sigma^{-1}) \\ \Leftrightarrow \quad & (\sigma \circ c \circ \sigma^{-1})(x) \neq x \\ \Leftrightarrow \quad & (c \circ \sigma^{-1})(x) \neq \sigma^{-1}(x) \\ \Leftrightarrow \quad & \sigma^{-1}(x) \in \text{supp}(c) \\ \Leftrightarrow \quad & x \in \sigma\left(\text{supp}(c)\right) \\ \Leftrightarrow \quad & x \in \text{supp}\left((\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_p))\right) \end{aligned}$$

2. Soit $x \in \text{supp}(c)$. Alors il existe $i \in [\![1; p-1]\!]$ tel que $x = c^i(a_1)$. Démontrons que $\text{supp}(c) = \{c^k(x),\, k \in \mathbb{Z}\}$.

$\subset$: Soit $y \in \text{supp}(c)$. Alors il existe $j \in [\![0; p-1]\!]$ tel que $y = c^j(a_1)$.

D'où $y = c^j\left(c^{-i}(x)\right) = c^{j-i}(x)$. Or $j - i \in \mathbb{Z}$. D'où $y \in \{c^k(x),\, k \in \mathbb{Z}\}$.

$\supset$: Soit $y \in \{c^k(x),\, k \in \mathbb{Z}\}$. Alors il existe $k \in \mathbb{Z}$ tel que $y = c^k(x)$.

D'où $y = c^k\left(c^j(a_1)\right) = c^{k+j}(a_1)$ et par conséquent $y \in \text{supp}(c)$.

3. $\forall\, i \in [\![1; p]\!]$, $c^{l(c)}(a_i) = a_i$. Donc $c^{l(c)} = \text{id}$. Donc l'ordre de c divise $l(c)$ et lui est donc inférieur. Soit $k \in [\![1; p-1]\!]$, $c^k(a_1) = a_{k+1} \neq a_1$ donc $c^k \neq \text{id}$. Donc $l(c)$ est inférieur ou égal à l'ordre de c. D'où l'égalité.

4. C'est une conséquence immédiate de 2. et 3. □

Proposition 22. *Soit n un entier naturel tel que $n \geqslant 2$. Deux cycles de $(\mathfrak{S}_n, \circ)$ dont les supports sont disjoints commutent.*

Démonstration. Soient c et c' deux cycles de $\mathfrak{S}_n$ dont les supports sont disjoints. Soit $x \in [\![1; n]\!]$.

Si $x \notin \text{supp}(c) \cup \text{supp}(c')$, alors on a :

$$(c \circ c')(x) = c\left(c'(x)\right) = c(x) = x = c'(x) = c'\left(c(x)\right) = (c' \circ c)(x)$$

Si $x \in \text{supp}(c)$ et $x \notin \text{supp}(c')$, alors d'après la proposition 21, $c(x) \notin \text{supp}(c')$. D'où :

$$(c' \circ c)(x) = c'\left(c(x)\right) = c(x) = c\left(c'(x)\right) = (c \circ c')(x)$$

De même si $x \notin \text{supp}(c)$ et $x \in \text{supp}(c')$. □

2.2 Décomposition d'une permutation

Théorème 23. *(Décomposition d'une permutation) Soit n un entier naturel tel que $n \geqslant 2$. Toute permutation de $(\mathfrak{S}_n, \circ)$ se décompose de manière unique (à l'ordre des facteurs près) en un produit de cycles à supports deux à deux disjoints.*

Démonstration. 1. *Existence :* Soit $\sigma \in \mathfrak{S}_n$. L'ensemble $[\![1; n]\!]$ étant fini, il existe un nombre fini r, avec $r \in [\![1; n]\!]$, de σ-orbite(s). Soient $O_1, \ldots, O_r$ ces orbites. On a : $[\![1; n]\!] = \bigsqcup_{i=1}^{i=r} O_i$. Pour tout $i \in [\![1; r]\!]$, définissons c_i par $c_i(x) \coloneqq \begin{cases} \sigma(x) & \text{si } x \in O_i \\ x & \text{si } x \notin O_i \end{cases}$.

Si $x \notin O_i$, $\mathrm{orb}_{\langle c_i \rangle}(x) = \{x\}$.

Si $x \in O_i$, alors $c_i(x) = \sigma(x)$ et donc $\mathrm{orb}_{\langle c_i \rangle}(x) = \mathrm{orb}_{\langle \sigma \rangle}(x) = O_i$. Ainsi, il y a au plus une c_i-orbite non réduite à un point et par conséquent, c_i est un cycle ou l'identité. Posons alors $s \coloneqq c_1 \circ c_2 \circ \ldots \circ c_r$ et démontrons que $s = \sigma$:

Soit $x \in [\![1; n]\!]$. Alors il existe un unique $i \in [\![1; r]\!]$ tel que $x \in O_i$. On a donc :

$$\begin{cases} \forall\, j \in [\![1; n]\!] \text{ tel que } j \neq i,\ c_j(x) = x \\ c_i(x) = \sigma(x). \\ \forall\, j \in [\![1; n]\!] \text{ tel que } j \neq i,\ c_j\left(\sigma(x)\right) = \sigma(x) \text{ car } \sigma(x) \in O_i \end{cases}$$

D'où $s(x) = \sigma(x)$.

2. *Unicité :* Soient $d_1, \ldots, d_q$ des cycles à supports deux à deux disjoints tels que $\sigma = d_1 \circ d_2 \circ \ldots \circ d_q$. Soit $x \in [\![1; n]\!]$. Il existe un unique $j \in [\![1; q]\!]$ tel que $x \in \mathrm{supp}(d_j)$. Comme les supports de $d_1, \ldots, d_q$ sont deux à deux disjoints, seul d_j a un effet sur x. D'où $\sigma(x) = d_j(x)$ et, par récurrence, pour tout $k \in \mathbb{Z}$, $\sigma^k(x) = d_j^k(x)$. Ainsi, $\mathrm{orb}_{\langle \sigma \rangle}(x) = \mathrm{orb}_{\langle d_j \rangle}(x) = \mathrm{supp}(d_j)$. Par conséquent, $\mathrm{supp}(d_1), \ldots, \mathrm{supp}(d_q)$ sont les σ-orbites. On en déduit que $r = q$ et que, pour tout $i \in [\![1; q]\!]$, $\mathrm{supp}(d_i) = O_i$. Donc pour tout $i \in [\![1; q]\!]$, $d_i = c_i$. D'où l'unicité. □

Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 7 & 6 & 5 & 2 \end{pmatrix} \in \mathfrak{S}_7$. Décomposons σ en produit de cycles à supports disjoints. On a : $\mathrm{orb}_{\langle \sigma \rangle}(1) = \{1; 4; 7; 2; 3\}$ et $\mathrm{orb}_{\langle \sigma \rangle}(5) = \{5; 6\}$ d'où : $\sigma = (1,\, 4,\, 7,\, 2,\, 3) \circ (5,\, 6)$.

Remarque. Cette décomposition permet de calculer σ^{2024}.

En effet, $\sigma^{2024} = (1,\, 4,\, 7,\, 2,\, 3)^{2024} \circ (5\,6)^{2024} = (1,\, 3,\, 2,\, 7,\, 4)$ d'après les propositions 21 et 22.

Corollaire 24. *Soit n un entier naturel tel que $n \geqslant 2$. $(\mathfrak{S}_n, \circ)$ est engendré par les transpositions.*

Démonstration. D'après le théorème 23, il suffit de démontrer que tout cycle se décompose en un produit de transposition(s). Soit $c := (a_1, a_2, \ldots, a_p)$ un p-cycle de $\mathfrak{S}_n$. On a alors :

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

En effet, on vérifie aisément que :

$$\begin{cases} \forall\, i \in [\![1; p-1]\!],\ (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{p-1}, a_p)(a_i) = a_{i+1} = c(a_i) \\ (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{p-1}, a_p)(a_p) = a_1 = c(a_p) \\ \forall\, x \notin \mathrm{supp}(c),\ (a_1, a_2) \circ (a_2, a_3) \circ \ldots \circ (a_{p-1}, a_p)(x) = x = c(x) \end{cases}$$

□

Remarque. Il n'y a plus unicité ici. En effet :

$$(1, 2, 3) = (1, 2) \circ (2, 3) = (1, 2) \circ (1, 2) \circ (1, 2) \circ (2, 3) = (1, 3) \circ (1, 2)$$

Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 1 & 7 & 6 & 5 & 2 \end{pmatrix} \in \mathfrak{S}_7$. Nous avons vu que : $\sigma = (1, 4, 7, 2, 3) \circ (5, 6)$. D'où $\sigma = (1, 4) \circ (4, 7) \circ (7, 2) \circ (2, 3) \circ (5, 6)$.

Corollaire 25. *(Systèmes de générateurs de $\mathfrak{S}_n$) Soit n un entier naturel tel que $n \geqslant 2$. $(\mathfrak{S}_n, \circ)$ est engendré par :*

1. $\{(i, j),\ 1 \leqslant i < j \leqslant n\}$.
2. $\{(i, i+1),\ 1 \leqslant i \leqslant n-1\}$.
3. $\{(1, i),\ 2 \leqslant i \leqslant n\}$.

Démonstration. 1. Découle directement du corollaire 24 et en remarquant que $(i, j) = (j, i)$.

2. Soient $i, j \in [\![1; n]\!]$ tels que $1 \leqslant i < j \leqslant n$. On vérifie aisément que $(i, j) = (i, i+1) \circ (i+1, i+2) \circ \ldots \circ (j-2, j-1) \circ (j-1, j) \circ (j-2, j-1) \circ \ldots \circ (i, i+1)$. Le point 1. permet alors de conclure.

3. Soient $i, j \in [\![1; n]\!]$ tels que $1 \leqslant i < j \leqslant n$. On vérifie aisément que $(i, j) = (1, i) \circ (1, j) \circ (1, i)$. Le point 1. permet alors de conclure. □

2.3 Signature

Définition 26. Soit n un entier supérieur ou égal à 2. Soit $\sigma \in (\mathfrak{S}_n, \circ)$. On appelle inversion de σ tout couple $(i, j) \in [\![1; n]\!]^2$ tel que $i < j$ et $\sigma(i) > \sigma(j)$. On note $I(\sigma)$ le nombre d'inversions de σ. On appelle signature de σ le nombre noté $\varepsilon(\sigma)$ tel que $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.

Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 3 & 4 \end{pmatrix} \in \mathfrak{S}_5$. $\sigma(1) > \sigma(2)$, $\sigma(1) > \sigma(3)$, $\sigma(1) > \sigma(4)$, $\sigma(1) > \sigma(5)$, $\sigma(2) > \sigma(3)$. σ compte 5 inversions. Sa signature est donc $\varepsilon(\sigma) = (-1)^5 = -1$.

Théorème 27. *Soit n un entier supérieur ou égal à 2. Alors :*

1. $\forall \sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j}$.
2. *L'application $\varepsilon : (\mathfrak{S}_n, \circ) \to (\{-1;1\}, \times)$ définie par $\varepsilon(\sigma) = (-1)^{I(\sigma)}$ est un morphisme de groupes. Il est le seul non trivial.*

Démonstration. 1. σ étant une permutation de $[\![1;n]\!]$, on a naturellement, pour tous $i, j \in [\![1;n]\!]$ tels que $1 \leqslant i < j \leqslant n$, $\prod_{1 \leqslant i < j \leqslant n} |\sigma(i) - \sigma(j)| = \prod_{1 \leqslant i < j \leqslant n} |i - j|$. D'où $\left| \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j} \right| = 1$. De plus, le nombre de paires $\{i;j\}$ telles que $1 \leqslant i < j \leqslant n$ et $\frac{\sigma(i)-\sigma(j)}{i-j} < 0$ est égal à $I(\sigma)$. Donc $\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j}$ est du même signe que $\varepsilon(\sigma)$. D'où le résultat.

2. Soient $\sigma, \sigma' \in \mathfrak{S}_n$. On a :

$$\begin{aligned}
\varepsilon(\sigma \circ \sigma') &= \prod_{1 \leqslant i < j \leqslant n} \frac{(\sigma \circ \sigma')(j) - (\sigma \circ \sigma')(i)}{j - i} \\
&= \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(\sigma')(j) - \sigma(\sigma')(i)}{\sigma'(j) - \sigma'(i)} \times \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma'(j) - \sigma'(i)}{j - i} \\
&= \prod_{1 \leqslant i' < j' \leqslant n} \frac{\sigma(j') - \sigma(i')}{j' - i'} \times \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma'(j) - \sigma'(i)}{j - i} \\
&= \varepsilon(\sigma) \times \varepsilon(\sigma')
\end{aligned}$$

Soit $\varphi : (\mathfrak{S}_n, \circ) \to (\{-1;+1\}, \times)$ un morphisme de groupes. Soient $i, j \in [\![1;n]\!]$ tels que $1 \leqslant i < j \leqslant n$. D'après le corollaire 25, $(i, j) = (1, i) \circ (1, j) \circ (1, i)$. Donc $\varphi((i, j)) = \varphi((1, j)) \times \varphi((1, i))^2 = \varphi((1, j))$. De même, on démontre que $\varphi((i, j)) = \varphi((1, i))$. D'où $\varphi((i, j)) = \varphi((1, i)) = \varphi((1, j))$.
Si $\varphi((1, i)) = \varphi((1, j)) = 1$, alors $\varphi((i, j)) = 1$ et φ est le morphisme trivial. Sinon, $\varphi((i, j)) = \varphi((1, i)) = \varphi((1, j)) = -1$ et alors φ et ε coïncident sur les transpositions de $\mathfrak{S}_n$ et par conséquent sur $\mathfrak{S}_n$ tout entier d'après le corollaire 24. □

Remarque. Si σ est une transposition, alors $\varepsilon(\sigma) = -1$. Si σ est un cycle, alors $\varepsilon(\sigma) = (-1)^{l(\sigma)-1}$.

Exemple. Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 1 & 6 & 3 \end{pmatrix} \in \mathfrak{S}_6$. On a $\sigma = (1, 5, 6, 3, 2, 4)$. D'où $\varepsilon(\sigma) = (-1)^5 = -1$.

Définition 28. Soit n un entier supérieur ou égal à 2. On appelle groupe alterné d'ordre n le sous-ensemble de $\mathfrak{S}_n$ noté $\mathfrak{A}_n$ des permutations de signature 1.

Théorème 29. *Soit n un entier supérieur ou égal à 2.*

1. *$(\mathfrak{A}_n, \circ)$ est un sous-groupe de $(\mathfrak{S}_n, \circ)$ d'ordre $\frac{n!}{2}$.*
2. *$(\mathfrak{A}_n, \circ)$ est engendré par les 3-cycles.*

Démonstration. 1. $\mathfrak{A}_n = \ker(\varepsilon)$ donc $(\mathfrak{A}_n, \circ)$ est un sous-groupe de $(\mathfrak{S}_n, \circ)$. Soit τ une transposition quelconque de $\mathfrak{S}_n$. L'application $\Psi : \mathfrak{A}_n \to \mathfrak{S}_n \setminus \mathfrak{A}_n$ définie par $\Psi(\sigma) = \tau \circ \sigma$ est une bijection. Donc $|\mathfrak{A}_n| = |\mathfrak{S}_n \setminus \mathfrak{A}_n|$. D'où :

$$|\mathfrak{A}_n| = \frac{|\mathfrak{S}_n|}{2} = \frac{n!}{2}$$

2. Soit $\sigma \in \mathfrak{A}_n$. Par définition de $(\mathfrak{A}_n, \circ)$, σ se décompose en un nombre pair de transpositions. Or tout produit de deux transpositions est égal à un 3-cycle :

$$\begin{aligned}(a,\, b) \circ (b,\, c) &= (a,\, b,\, c)\\ (a,\, b) \circ (a,\, c) &= (a,\, c,\, b)\\ (a,\, b) \circ (c,\, d) &= (a,\, b,\, c) \circ (b,\, c,\, d)\end{aligned}$$

D'où le résultat. □

2.4 Applications

2.4.1 Théorème de Cayley

Lemme 30. *Soit $n \in \mathbb{N}^*$. Soit E un ensemble de cardinal n. Le groupe $(\mathfrak{S}(E), \circ)$ des bijections de E dans E est isomorphe à $(\mathfrak{S}_n, \circ)$.*

Démonstration. E et $[\![1; n]\!]$ étant équipotents, il existe une bijection $f : E \to [\![1; n]\!]$. Soit $\Psi : (\mathfrak{S}(E), \circ) \to (\mathfrak{S}_n, \circ)$ l'application définie par $\Psi(\sigma) = f \circ \sigma \circ f^{-1}$. Ψ est évidemment bien définie. Ψ est bijective en tant que composée de bijections. Prouvons que Ψ est un morphisme de groupes. Soient σ_1, $\sigma_2 \in \mathfrak{S}(E)$, on a :

$$\begin{aligned}\Psi(\sigma_1 \circ \sigma_2) &= f \circ (\sigma_1 \circ \sigma_2) \circ f^{-1}\\ &= f \circ (\sigma_1 \circ (f^{-1} \circ f) \circ \sigma_2) \circ f^{-1}\\ &= (f \circ \sigma_1 \circ f^{-1}) \circ (f \circ \sigma_2 \circ f^{-1})\\ &= \Psi(\sigma_1) \circ \Psi(\sigma_2)\end{aligned}$$

□