GROUPE DE PERMUTATIONS
GROUPE SYMÉTRIQUE

CHAPITRE 4

Table des matières

Soit E un ensemble ayant au moins deux éléments et Id_E l'application identité sur E. On notera $\mathbf{card}(E)$ le cardinal de E.

1. Permutations, cycles et transpositions

On note $\mathcal{S}(E)$ (ou $\mathfrak{S}(E)$) l'ensemble des bijections de E sur E.

Proposition 1.1. *$\mathcal{S}(E)$ est un groupe pour la composition des applications.*

Démonstration. Evident. □

Définition 1.2. *Le groupe $\mathcal{S}(E)$ est appelé* **groupe des permutations** *de E.*

Dans le cas où E est réduit à un élément, $\mathcal{S}(E) = \{Id\}$.

Pour $E = \{1, 2, \ldots, n\}$, où $n \in \mathbb{N}^*$, on note $\mathcal{S}_n$ ou $\mathfrak{S}_n$ le groupe $\mathcal{S}(E)$ et on l'appelle **groupe symétrique** *de degré n.*

Pour toute permutation $\sigma \in \mathcal{S}_n$, on note

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

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

Avec cette notation, on calcule facilement la composée et l'inverse d'une permutation de $\mathcal{S}_n$. Par exemple, on a

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

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

Pour toute permutation $\sigma \in \mathcal{S}(E)$ et tout entier relatif r, on définit la permutation σ^r par

$$\sigma^r = \begin{cases} Id_E & \text{si } r = 0 \\ \sigma \circ \cdots \circ \sigma & (r \text{ fois}) \text{ si } r \geq 1 \\ (\sigma^{-r})^{-1} & \text{si } r \leq -1 \end{cases}$$

Définition 1.3. *Soit r un entier, $2 \leq r \leq$ **card**(E). On appelle* **cycle** *d'ordre r (ou r-cycle), toute permutation $\sigma \in \mathcal{S}(E)$ qui permute circulairement r éléments de E et laisse fixe les autres. C'est-à-dire, qu'il existe une partie $\{x_1, \ldots, x_r\}$ de E telle que*

$$\begin{cases} \sigma(x_k) = x_{k+1} & \forall k \in \{1, \ldots, r-1\} \\ \sigma(x_r) = x_1 & \\ \sigma(x) = x & \forall x \in E \setminus \{x_1, \ldots, x_r\}. \end{cases}$$

On notera alors

$$\sigma = (x_1, \ldots, x_r)$$

un tel cycle et on dit que $\{x_1, \ldots, x_r\}$ est le **support** *de σ, que l'on note* Supp(σ).

Remarque 1.4. (a) Les r permutations circulaires

$$(x_1, x_2, \ldots, x_r), (x_2, x_3, \ldots, x_r, x_1), \ldots, (x_r, x_1, \ldots, x_{r-1})$$

désignent le même cycle.

(b) L'inverse d'un r-cycle est un r-cycle de même support. Précisément, on peut vérifier facielement que

$$(x_1, x_2, \ldots, x_r)^{-1} = (x_r, x_{r-1}, \ldots, x_1).$$

(c) Si $\sigma = (x_1, x_2, \ldots, x_r)$ est un r-cycle, on a alors pour tout entier k, $1 \leq k \leq r$,

$$x_k = \sigma^{k-1}(x_1).$$

En effet, c'est vrai pour $k = 1$ et supposons le résultat acquis pour $1 \leq k-1 \leq r-1$, on a

$$x_k = \sigma(x_{k-1}) = \sigma(\sigma^{k-2}(x_1)) = \sigma^{k-1}(x_1).$$

Définition 1.5. *On appelle transposition, un cycle d'ordre 2.*

On peut remarquer qu'une transposition τ est d'ordre 2 dans le groupe $\mathcal{S}(E)$, c'est-à-dire que $\tau \neq Id_E$ et $\tau^2 = Id_E$. On a donc $\tau^{-1} = \tau$.

Proposition 1.6. *Un r-cycle est d'ordre r dans le groupe $\mathcal{S}(E)$.*

Démonstration. Soit $\sigma = (x_1, \ldots, x_r)$ un r-cycle avec $r \geq 2$. Pour tout entier k, $1 \leq k \leq r$ on a

$$\begin{aligned} \sigma^r(x_k) &= \sigma^r(\sigma^{k-1}(x_1)) = \sigma^{k-1}(\sigma^r(x_1)) \\ &= \sigma^{k-1}(\sigma(\sigma^{r-1}(x_1))) = \sigma^{k-1}(\sigma(x_r)) \\ &= \sigma^{k-1}(x_1) = x_k \end{aligned}$$

Comme $\sigma(x) = x$ pour tout $x \in E \setminus \{x_1, \ldots, x_r\}$, on en déduit que $\sigma^r = Id_E$.
Enfin puisque $\sigma^{k-1}(x_1) = x_k \neq x_1$ pour $2 \leq k \leq r$, on déduit que $\sigma^{k-1} \neq Id_E$ et σ est d'ordre r. □

Remarque 1.7. (a) On déduit du résultat précédent que l'inverse d'un r-cycle σ est un r-cycle, $\sigma^{-1} = \sigma^{r-1}$.

(b) Si σ est un r-cycle, le calcul de σ^m pour tout entier relatif m peut s'obtenir en effectuant la division euclidienne de m par r : on a $m = qr + s$ avec $0 \leq s \leq r-1$ et $\sigma^m = \sigma^s$.

(c) Si l'ensemble E a au moins 3 éléments, alors le groupe $\mathcal{S}(E)$ n'est pas commutatif. En effet, soient x_1, x_2, x_3 trois éléments distincts de E et $\tau_1 = (x_1, x_2)$, $\tau_2 = (x_2, x_3)$. On a $\tau_2\tau_1(x_1) = x_3$ et $\tau_1\tau_2(x_1) = x_2$. Donc $\tau_1\tau_2 \neq \tau_2\tau_1$.

(d) On suppose que $\mathbf{card}(E) \geq 2$. Alors on vérifie assez facilement que dans $\mathcal{S}(E)$ il y a $\binom{n}{r}(r-1)! = \frac{n!}{(n-r)!}$ cycles d'ordre r distincts.

Proposition 1.8. *Si σ et σ' sont deux cycles tels que $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma')$ est réduit à un point, alors $\sigma\sigma'$ est un cycle.*

Démonstration. En effet, supposons que $\sigma = (x_1, \ldots, x_r)$, $\sigma' = (x'_1, \ldots, x'_s)$ et $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \{x_k\}$. Soit j, $1 \leq j \leq s$ tel que $x_k = x'_j$, alors

$$\begin{aligned}\sigma\sigma' &= (x_{k+1}, \ldots, x_r, x_1, \ldots, x_k)(x_k, x'_{j+1}, \ldots, x'_s, x'_1, \ldots, x'_{j-1}) \\ &= (x_{k+1}, \ldots, x_r, x_1, \ldots, x_k, x'_{j+1}, \ldots, x'_s, x'_1, \ldots, x'_{j-1})\end{aligned}$$

□

La proposition qui suit est très souvent utilisée.

Proposition 1.9. *Soit r un entier $2 \leq r \leq \mathbf{card}(E)$.*
Le conjugué dans $\mathcal{S}(E)$ d'un r-cycle est encore un r-cycle. Précisément, pour tout r-cycle $\sigma = (x_1, \ldots, x_r)$ et toute permutation $\gamma \in \mathcal{S}(E)$, on a

$$\gamma \circ \sigma \circ \gamma^{-1} = (\gamma(x_1), \gamma(x_2), \ldots, \gamma(x_r)).$$

Réciproquement, deux cycles de même longueur sont conjugués dans $\mathcal{S}(E)$. Précisément, si σ, σ' sont deux r-cycles, il existe alors une permutation $\gamma \in \mathcal{S}(E)$ telle que $\sigma' = \gamma \circ \sigma \circ \gamma^{-1}$.

Démonstration. En notant $\sigma'' = (\gamma(x_1), \ldots, \gamma(x_r))$, il s'agit de montrer que $\gamma \circ \sigma = \sigma'' \circ \tau$.

Pour $x \in E \setminus \{x_1, \ldots, x_r\}$, on a $\sigma(x) = x$ et $\gamma(x) \in E \setminus \{\gamma(x_1), \ldots, \gamma(x_r)\}$, ce qui donne

$$\gamma \circ \sigma(x) = \gamma(x) = \sigma''(\gamma(x)) = \sigma'' \circ \gamma(x)$$

Si $x = x_k \in \{x_1, \ldots, x_r\}$, en notant $x_{r+1} = x_1$, on a

$$\gamma \circ \sigma(x) = \gamma(\sigma(x_k)) = \gamma(x_{k+1})$$

et

$$\sigma'' \circ \gamma(x) = \sigma''(\gamma(x_k)) = \gamma(x_{k+1}).$$

On a donc bien $\gamma \circ \sigma = \sigma'' \circ \gamma$, soit $\gamma \circ \sigma \circ \gamma^{-1} = \sigma''$.

Pour la réciproque, soient $\sigma = (x_1, \ldots, x_r)$ et $\sigma' = (x'_1, \ldots, x'_r)$ deux r-cycles. Soit φ une bijection de $E \setminus \{x_1, \ldots, x_r\}$ sur $E \setminus \{x'_1, \ldots, x'_r\}$ et $\gamma \in \mathcal{S}(E)$ telle que $\gamma(x_k) = x'_k$ pour $k = 1, \ldots, r$ et $\gamma(x) = \varphi(x)$ pour $x \in E \setminus \{x_1, \ldots, x_r\}$. On a alors

$$\gamma \circ \sigma \circ \gamma^{-1} = (\gamma(x_1), \ldots, \gamma(x_r)) = (x'_1, \ldots, x'_r) = \sigma'.$$

□

Le résultat précédent se traduit en disant que, pour tout entier r compris entre 2 et $\mathbf{card}(E)$, le groupe $\mathcal{S}(E)$ agit par conjugaison de façon transitive sur l'ensemble des r-cycles.

En faisant agir $\mathcal{S}(E)$ par conjugaison sur l'ensemble des cycles, l'orbite d'un r-cycle pour cette action est l'ensemble de tous les r-cycles et son cardinal est $\frac{A_r^n}{r} = (r-1)\binom{n}{r}$.

On désigne par $Z(\mathcal{S}(E))$ le centre du groupe de $\mathcal{S}(E)$, c'est-à-dire l'ensemble des éléments de $\mathcal{S}(E)$ qui commutent à tous les autres éléments de $\mathcal{S}(E)$.

Proposition 1.10. *On a*

$$Z(\mathcal{S}(E)) = \begin{cases} \mathcal{S}(E) & si\ \mathbf{card}(E) = 2 \\ \{Id_E\} & si\ \mathbf{card}(E) \geq 3 \end{cases}$$

Démonstration. Si $\mathbf{card}(E) = 2$, le groupe $\mathcal{S}(E)$ est abélien et $Z(\mathcal{S}(E)) = \mathcal{S}(E)$.
On suppose que $\mathbf{card}(E) \geq 3$. Soit $\sigma \in \mathcal{S}(E) \setminus \{Id_E\}$. Il existe donc $x \in E$ tel que $y = \sigma(x) \neq x$. Soit $z \in E \setminus \{x, y\}$ (E a aumoins trois éléments) et τ la transposition $\tau = (y, z)$. On a

$$\sigma\tau(x) = \sigma(x) = y \ \text{ et } \ \tau\sigma(x) = \tau(y) = z \neq y.$$

On en déduit que $\sigma\tau \neq \tau\sigma$ et que $\sigma \notin Z(\mathcal{S}(E))$. Par conséquent $Z(\mathcal{S}(E)) = \{Id_E\}$.
□

2. Les groupes symétriques

Théorème 2.1. *Si E et F sont deux ensembles non vides et φ une bijection de E sur F, alors les groupes $\mathcal{S}(E)$ et $\mathcal{S}(F)$ sont isomprphes.*

Démonstration. Il suffit de vérifier que l'application

$$\begin{array}{rccc} \Psi: & \mathcal{S}(E) & \to & \mathcal{S}(F) \\ & \sigma & \mapsto & \varphi \circ \sigma \circ \varphi^{-1} \end{array}$$

est un isomorphisme de groupes. □

On en déduit que tout groupe de permutations d'un ensemble à n éléments est isomorphe au groupe symétrique $\mathcal{S}_n$ des permutations de $\{1, 2, \ldots, n\}$.

Théorème 2.2. *Pour tout entier $n \geq 1$ et tout ensemble de cardinal n, le groupe $\mathcal{S}(E)$ est d'ordre $n!$.*

Démonstration. On va faire une démonstration par récurrence sur le cardinal $n \geq 1$ de E.

Si $n = 1$, $\mathcal{S}(E) = \{Id_E\}$, est de cardinal 1.

Supposons le résultat acquis pour les ensembles à $n-1$ éléments et soit $E = \{x_1, \ldots, x_n\}$ un ensemble $n \geq 2$ éléments.

On fait agir $\mathcal{S}(E)$ sur E. Cette action est transitive (il y a une seule orbite) et on désigne par $H = \mathcal{S}(E)_{x_n}$ le stabilisateur de x_n,

$$H = \{\sigma \in \mathcal{S}(E)\ ;\ \sigma(x_n) = x_n\}.$$

H est donc un sous-groupe de $\mathcal{S}(E)$ et l'application qui associe à $\sigma \in H$ sa restriction à $F = \{x_1, \ldots, x_{n-1}\}$ réalise alors un isomorphisme de groupes de H sur $\mathcal{S}(F)$, donc H est d'ordre $(n-1)!$. Soit $\mathcal{O}_{x_n}$ l'orbite de x_n. Comme l'action est transitive on a $\mathcal{O}_{x_n} = E$, donc

$$\begin{aligned} \mathbf{card}(\mathcal{S}(E)) &= \mathbf{card}(\mathcal{O}_{x_n})\,\mathbf{card}(H) \\ &= n \cdot (n-1)! = n! \end{aligned}$$

□

Exemples 2.3. (a) Le groupe symétrique $\mathcal{S}_2$ est composé de deux éléments

$$Id, \;\; \tau = (1,2)$$

C'est un groupe abélien. Il est cyclique d'ordre 2 engendré par τ et isomorphe $\mathbb{Z}_2$.

(b) Le groupe symétrique $\mathcal{S}_2$ est formé de six éléments

$$Id, \tau_1 = (1,2), \tau_2 = (1,3), \;\; \tau_3 = (2,3), \sigma_1 = (1,2,3) \text{ et } \sigma_2 = (1,3,2).$$

Ce groupe n'est pas abélien, car par exemple

$$\tau_1\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_2 \text{ et } \tau_2\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \sigma_1 \neq \sigma_2.$$

En remarquant que

$$\sigma_2 = \sigma_1^2, \tau_2 = \tau_1\sigma_2 = \tau_1\sigma_1^2, \tau_3 = \tau_1\sigma_1$$

on déduit que

$$\begin{aligned} \mathcal{S}_3 &= \{Id, \sigma_1, \sigma_1^2, \tau_1, \tau_1\sigma_1, \tau_1\sigma_1^2\} = \langle \tau_1, \sigma_1 \rangle \\ &= \{\tau_1^i \sigma_1^j \mid i = 0,1, \; j = 0,1,2\}. \end{aligned}$$

$\mathcal{S}_3$ est donc engendré par τ_1 (qui est d'ordre 2) et σ_1 (qui est d'ordre 3). On montre que $\mathcal{S}_3$ est, à isomorphisme près, le seul groupe d'ordre 6 non abélien (voir TD).

3. Support et orbites d'une permutation

Définition 3.1. *Le support d'une permutation $\sigma \in \mathcal{S}(E)$ est le complémentaire dans E de l'ensemble de ses points fixes, soit l'ensemble*

$$\mathrm{supp}(\sigma) = \{x \in E \mid \sigma(x) \neq x\}.$$

Remarque 3.2. (a) Id_E est l'unique permutation de support vide.

(b) Le support d'un cycle $\sigma = (x_1, \ldots, x_r)$ est $\{x_1, \ldots, x_r\}$.

Proposition 3.3. *Soient σ, σ' deux permutations de E.*

(a) $\sigma(\mathrm{supp}(\sigma)) = \mathrm{supp}(\sigma)$.

(b) $\mathrm{supp}(\sigma) = \mathrm{supp}(\sigma^{-1})$.

(c) Pour tout $m \in \mathbb{Z}$, $\mathrm{supp}(\sigma^m) \subset \mathrm{supp}(\sigma)$.

(d) Si $\mathrm{supp}(\sigma) \cap \mathrm{supp}(\sigma') = \emptyset$, *alors* $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Démonstration. (a) Soit $x \in \mathrm{supp}(\sigma)$. Comme σ est injective, de $\sigma(x) \neq x$ on déduit $\sigma(\sigma(x)) \neq \sigma(x)$ et $\sigma(x) \in \mathrm{supp}(\sigma)$. On a donc $\sigma(\mathrm{supp}(\sigma)) \subset \mathrm{supp}(\sigma)$. Comme σ est surjective, tout $x \in \mathrm{supp}(\sigma)$ s'ecrit $x = \sigma(x')$ et $\sigma(x) = \sigma(\sigma(x')) \neq x = \sigma(x')$ impose

$\sigma(x') \neq x'$ donc $x' \in \text{supp}(\sigma)$ et $x \in \sigma(\text{supp}(\sigma))$. On a donc $\text{supp}(\sigma) \subset \sigma(\text{supp}(\sigma))$ et $\text{supp}(\sigma) = \text{supp}(\text{supp}(\sigma))$.

(b) De $\sigma(x) = x \iff x = \sigma^{-1}(x)$, on déduit que $\text{supp}(\sigma) = \text{supp}(\sigma^{-1})$.

(c) L'égalité $\sigma(x) = x$ entraîne $\sigma^m(x) = x$, donc $\sigma^m(x) \neq x$ entraîne $\sigma(x) \neq x$ et $\text{supp}(\sigma^m) \subset \text{supp}(\sigma)$.

(d) Soient σ, σ' tel que $\text{supp}(\sigma) \cap \text{supp}(\sigma') = \emptyset$ et $x \in E$.

Si $x \notin \text{supp}(\sigma) \cup \text{supp}(\sigma')$, alors $\sigma(x) = x = \sigma'(x)$ et $\sigma' \circ \sigma(x) = \sigma'(x) = x = \sigma(x) = \sigma \circ \sigma'(x)$.

Si $x \in \text{supp}(\sigma)$ (et donc $x \notin \text{supp}(\sigma')$), alors $\sigma'(x) = x$, donc $\sigma' \circ \sigma(x) = \sigma(x) = \sigma \circ \sigma'(x)$. On montre de même que pour tout $x \in \text{supp}(\sigma')$, $\sigma' \circ \sigma(x) = \sigma'(x) = \sigma \circ \sigma'(x)$. Ainsi $\sigma \circ \sigma' = \sigma' \circ \sigma$. □

Remarque 3.4. La réciproque du point (d) de la proposition précédente est fausse. Pour le voir, il suffit de prendre $\sigma \neq Id$ et $\sigma' = \sigma^{-1}$.

Pour la suite de ce paragraphe, E est un ensemble fini de cardinal $n \geq 2$.

Soit $\sigma \in \mathcal{S}(E)$. On a une action naturelle du groupe cyclique $H := \langle \sigma \rangle = \{\sigma^k,\ k \in \mathbb{Z}\}$ sur E définie par

$$(\sigma^k, x) = \sigma^k \cdot x = \sigma^k(x).$$

Les orbites, appelées encore σ-orbites pour cette action, sont les parties de E

$$H \cdot x = \{\gamma \cdot x;\ \gamma \in H\} = \{\sigma^k(x);\ k \in \mathbb{Z}\},\ \ x \in E$$

On notera $Orb_\sigma(x)$ une telle orbite.

On rappelle que les orbites sont aussi les classes d'équivalences pour la relation d'équivalence définie sur E par

$$x \mathcal{R}_\sigma y \iff \exists k \in \mathbb{Z},\ y = \sigma^k(x)$$

et que les orbites deux à deux distinctes forment une partition de E.

Remarque 3.5. Une σ-orbite $Orb_\sigma(x)$ est réduite à un point si, et seulement si, $\sigma(x) = x$ et les orbites non réduites à un point forment une partition du support de σ.

Exemple 3.6. Soit $\sigma = (x_1, \ldots, x_r)$ un r-cycle.
Pour $x \in E \setminus \{x_1, \ldots, x_r\}$, on a $\sigma(x) = x$ et $Orb_\sigma(x) = \{x\}$.
Pour tout entier $1 \leq k \leq r$, on a $x_k = \sigma^{k-1}(x_1)$, donc $x_k \mathcal{R}_\sigma x_1$ et comme $\sigma^r(x_1) = x_1$, on a

$$\begin{aligned} Orb_\sigma(x_k) &= Orb_\sigma(x_1) = \{x_1, \sigma(x_1), \ldots, \sigma^{r-1}(x_1)\} \\ &= \{x_1, x_2, \ldots, x_r\} \end{aligned}$$

Il y a donc une seule orbite non réduite à un point. Nous verrons plus loin que cela caractérise les cycles.

Proposition 3.7. *Soient $\sigma \in \mathcal{S}(E) \setminus \{Id\}$ et O une σ-orbite de cardinal $r \geq 2$ (non réduite à un point).*
Pour tout $x \in O$, r est le plus petit entier naturel non nul tel que $\sigma^r(x) = x$ et

$$O = Orb_\sigma(x) = \{x, \sigma(x), \ldots, \sigma^{r-1}(x)\}.$$

Démonstration. Comme $\sigma \neq Id$, il existe une orbite O non réduite à un point et il existe $y \in E$ tel que $O = Orb_\sigma(y)$.
Si $x \in O$, il existe alors un entier k tel que $x = \sigma^k(y)$ et

$$\begin{aligned} Orb_\sigma(x) &= \{\sigma^j(x),\ j \in \mathbb{Z}\} = \{\sigma^{j+k}(y),\ j \in \mathbb{Z}\} \\ &= \{\sigma^i(y),\ i \in \mathbb{Z}\} \\ &= O. \end{aligned}$$

Si $\sigma^k(x) \neq x$ pour tout $k \geq 1$, on a alors $\sigma^i(x) \neq \sigma^j(x)$ pour tout $i \neq j$ dans $\mathbb{Z}$ et O est infinie, ce qui contredit l'hypothèse. Il existe donc un plus petit entier naturel non nul s tel que $\sigma^s(x) = x$. Comme $O = Orb_\sigma(x)$ est de cardinal $r \geq 2$, elle n'est pas réduite à un point et $\sigma(x) \neq x$. On a donc $s \geq 2$.
Soit $k \in \mathbb{Z}$. En effectuant la division euclidienne de k par s, on peut écrire $k = qs + j$ avec $q \in \mathbb{Z}$ et $0 \leq j \leq s-1$, ce qui donne

$$\sigma^k(x) = \sigma^j(x)$$

et $O = \{x, \sigma(x), \ldots, \sigma^{s-1}(x)\}$. Comme $\sigma^i(x) \neq \sigma^j(x)$ pour tout $i \neq j$ dans $\{0, 1, \ldots, s-1\}$ (caractère minimal de s), on déduit que $\mathbf{card}(O) = s$ et $s = r$. □

Proposition 3.8. *Une permutation $\sigma \in \mathcal{S}(E)$ est un cycle d'ordre $r \geq 2$ si, et seulement si, il n'y a qu'une seule σ-orbite non réduite à un point.*

Démonstration. On a déjà vu qu'un r-cycle a une seule orbite non réduite à un point. Réciproquement si σ a une seule orbite non réduite à un point,

$$O = \{x, \sigma(x), \ldots, \sigma^{r-1}(x)\} = \{x_1, x_2, \ldots, x_r\}$$

avec $r \geq 2$, on a alors

$$\begin{cases} \sigma(x_k) = x_{k+1} & (1 \leq k \leq r-1) \\ \sigma(x_r) = x_1 & \\ \sigma(x) = x & \text{si } x \in E \setminus \{x_1, \ldots, x_r\} \end{cases}$$

et σ est le r-cycle $(x_1, \ldots, x_r)$. □

Remarque 3.9. (a) On peut déduire de cette proposition qu'une permutation $\sigma \in \mathcal{S}(E)$ est un cycle d'ordre $r \geq 2$ si, et seulement si, il existe $x \in E$ tel que $Orb_\sigma(x) = \text{supp}(\sigma)$.

(b) La composée de deux cycles n'est pas en général un cycle. Par exemple pour $\sigma = (1, 2, 3, 4)$ dans $\mathcal{S}_4$. On a $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ avec $Orb_{\sigma^2}(1) = \{1, 3\}$, $Orb_{\sigma^2}(2) = \{2, 4\}$, et donc σ^2 n'est pas un cycle.

4. Systèmes de générateurs de $\mathcal{S}(E)$

Dans ce paragraphe E est un ensemble fini de cardinal $n \geq 2$.

Définition 4.1. *On dit que deux cycles σ et σ' dans $\mathcal{S}(E)$ sont disjoints si leurs supports sont disjoints dans E.*

En utilisant le fait que les σ-orbites forment une partition de E et que chaque σ-orbite non réduite à un point permet de définir un cycle, on obtient le résultat suivant qui nous donne un premier système de générateurs de $\mathcal{S}(E)$.

Théorème 4.2. *Toute permutation $\sigma \in \mathcal{S}(E) \setminus \{Id\}$ se décompose en produit de cycles deux à deux disjoints (le groupe $\mathcal{S}(E)$ est engendré par les cycles). Cette décomposition est unique à l'ordre près.*
Si $\sigma = \gamma_1 \cdots \gamma_p$ est une telle décomposition, on a alors la partition

$$\text{supp}(\sigma) = \cup_{k=1}^{p} \text{supp}(\gamma_k)$$

et

$$o(\sigma) = ppcm(o(\gamma_1), \ldots, o(\gamma_p))$$

Démonstration. Soit $\sigma \in \mathcal{S}(E) \setminus \{Id\}$ et soit $\mathcal{O}_1, \cdots, \mathcal{O}_p, \mathcal{O}_{p+1} \cdots, \mathcal{O}_r$ les σ-orbites deux à deux distinctes avec $r_k = \mathbf{card}\, \mathcal{O}_k \geq 2$ pour $k = 1, \cdots, p$ et $\mathbf{card}\, \mathcal{O}_k = 1$ pour $k = p+1, \cdots, r$ (s'il en existe). On a alors la partition $E = \cup_{k=1}^{r} \mathcal{O}_k$.

Pour tout entier $1 \leq k \leq r$, on désigne par γ_k la permutation de E définie par

$$\forall x \in E, \;\; \gamma_k(x) = \begin{cases} \sigma(x) & \text{si } x \in \mathcal{O}_k \\ x & \text{si } x \notin \mathcal{O}_k \end{cases}$$

(γ_k est bien une permutation de E car la restriction de σ à une orbite $\mathcal{O}_k$ est une permutation de $\mathcal{O}_k$). Si $\mathcal{O}_k$ est réduite à un point, alors $\gamma_k = Id_E$, sinon γ_k est un r_k-cycle : en effet, pour $x \notin \mathcal{O}_k$, on a $\gamma_k(x) = x$ et $Orb_{\gamma_k}(x) = \{x\}$ et pour $x \in \mathcal{O}_k$, on a

$$\begin{aligned} Orb_{\gamma_k}(x) &= \{\gamma_k^j(x) \mid j \in \mathbb{Z}\} = \{\sigma^j(x) \mid j \in \mathbb{Z}\} \\ &= Orb_\sigma(x) = \mathcal{O}_k \end{aligned}$$

donc γ_k a bien une seule orbite non réduite à un point.

On vérifie alors que $\sigma = \prod_{j=1}^{r} \gamma_j = \prod_{j=1}^{p} \gamma_j$. En effet, pour $x \in E$, il existe un unique indice k entre 1 et r tel que $x \in \mathcal{O}_k$ et on a $\gamma_k(x) = \sigma(x)$, $\gamma_j(x) = x$ pour $j \neq k$ (puisque $x \notin \mathcal{O}_j$) et tenant compte du fait que les γ_j commutent (les supports sont deux à deux disjoints), on en déduit que

$$\left(\prod_{j=1}^{r} \gamma_j\right)(x) = \left(\gamma_k \prod_{j=1, j\neq k}^{r} \gamma_j\right)(x) = \gamma_k(x) = \sigma(x)$$

il reste à montrer l'unicité, à l'ordre près, d'une telle permutation.

Soit $\sigma = \prod_{j=1}^{p'} \gamma'_j$ une autre décomposition en cycles deux à deux disjoints. En notant $\mathcal{O}'_1, \cdots, \mathcal{O}'_{p'}$ les supports de ces cycles, pour $1 \leq k \leq p'$ et $x \in \mathcal{O}'_k$, on a $\sigma(x) = \gamma'_k(x)$ ($x \notin \mathcal{O}'_j$ pour $j \neq k$ et les cycles commutent), donc $\mathcal{O}'_k = Orb_{\gamma'_k}(x) = Orb_\sigma(x)$.
Les orbites $\mathcal{O}'_k$ sont donc les orbites non réduites à un point de σ et $p' = p$. On a donc $\mathcal{O}'_k = \mathcal{O}_j$ pour un unique j entre 1 et p. Pour $x \in \mathcal{O}'_k$, on a $\gamma'_k(x) = \sigma(x) = \gamma_j(x)$ et pour $x \notin \mathcal{O}'_k$, on a $\gamma'_k(x) = \gamma_j(x)$, ce qui montre que $\gamma'_k = \gamma_j$ et l'unicité de la décomposition à l'ordre près.

La réunion $\cup_{j=1}^{\text{p}}(\gamma_k)$ est la réunion des orbites $\mathcal{O}_k$ non réduites à un point, soit le support de σ.

Notons $m = \text{ppcm}(o(\gamma_1), \cdots, o(\gamma_p))$. Comme les cycles γ_k commutent, on a $\sigma^k = \gamma_1^k \circ \cdots \circ \gamma_p^k$ pour tout entier naturel k et $\sigma^k = Id_E$ si et seulement si $\gamma_j^k = Id$ pour tout $1 \leq j \leq p$. En effet, il est claire que la condition est suffisante et si $\sigma^k = Id_E$, on a alors pour tout $x \in \mathcal{O}_j$, $\gamma_j^k(x) = \sigma^k(x) = x$ et si $x \notin \mathcal{O}_j$, on a $\sigma_j(x) = x$, donc $\gamma_j^k(x) = x$. Ainsi $\gamma_j^k = Id_E$. Il en résulte que l'ordre de σ est un multiple commun des ordres des γ_j et donc un multiple de m qui est lui même un multiple de l'ordre de σ puisque $\sigma^m = Id_E$. D'où l'égalité.

□

Remarque 4.3. (a) On conviendra que l'identité est produit de 0 cycles : $Id = \gamma^0$ pour tout cycle γ.

(b) Comme l'ordre d'un cycle est égal à sa longueur, l'ordre de σ est aussi le ppcm des longueurs des cycles γ_j.

Pour $E = \{1, 2, \cdots, n\}$, une telle décomposition s'obtient en prenant, dans le cas où il n'est pas de point fixe, les images de 1 par $\sigma, \sigma^2, \cdots$, jusqu'au moment où on retombe sur 1 (l'orbite de 1), puis on recommence avec le plus petit entier dans $E \setminus \text{Orb}_\sigma(1)$ qui n'est pas fixe et ainsi de suite.

Exemple 4.4. Soit la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$. On a $\sigma(1) = 2$, $\sigma^2(1) = 3$, $\sigma^3(1) = 4$, $\sigma^4(1) = 5$, $\sigma^5(1) = 1$, ce qui donne le premier cycle $\gamma_1 = (1, 2, 3, 4, 5)$. Puis $\sigma(6) = 7$, $\sigma^2(6) = 6$ d'où le deuxième cycle $\gamma_2 = (6, 7)$. On a donc $\sigma = \gamma_1\gamma_2 = \gamma_2\gamma_1$ et $o(\sigma) = \text{ppcm}(o(\gamma_1), o(\gamma_1)) = \text{ppcm}(5, 2) = 10$.

Proposition 4.5. *Pour $2 \leq r \leq n$, tout r-cycle dans $\mathcal{S}(E)$ s'écrit comme produit de $r - 1$ transpositions.*

Démonstration. La proposition résulte de

$$(x_1, x_2, \ldots, x_r) = (x_1, x_2)(x_2, x_3) \cdots (x_{r-1}, x_r).$$

□

Théorème 4.6. *Toute permutation $\sigma \in \mathcal{S}(E)$ se décompose en produit de transpositions (le groupe $\mathcal{S}(E)$ est engendré par les transpositions).*

Démonstration. On a $Id = \tau^2$ pour toute transposition τ.
D'après Théorème 4.2 et Proposition 4.5 toute permutation $\sigma \in \mathcal{S}(E) \setminus \{Id\}$ est produit de cycles et un cycle est produit de transpositions. □

Remarque 4.7. Dans la décomposition d'une permutation en produit de transpositions, il n'y a pas d'unicité et les transpositions ne commutent pas nécessairement. Par exemple, on a

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

et

$$(1, 2)(2, 3) = (1, 2, 3) \neq (2, 3)(1, 2) = (3, 2, 1).$$

Si $\textbf{card}(E) = n$, alors $\mathcal{S}(E)$ est isomorphe $\mathcal{S}_n$, on va se contenter maintenant de décrire des générateurs de $\mathcal{S}_n$.

Proposition 4.8. *Le groupe $\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(1,k)$ où $2 \leq k \leq n$.*

Démonstration. Soit (i,j) une transposition avec $1 \leq i \neq j \leq n$. Si $i = 1$ ou $j = 1$, il n'y a rien à faire. Pour $i \neq 1$ et $j \neq 1$ on a

$$(i,j) = (1,i)(1,j)(1,i)^{-1} = (1,i)(1,j)(1,i)$$

Le résultat se déduits alors du Théorème 4.6. □

Exemple 4.9. Soit la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1,2)(2,3)(3,4)(4,5)(6,7)$$

On a

$$\begin{aligned} \sigma &= (1,2)(1,2)(1,3)(1,2)(1,3)(1,4)(1,3)(1,4)(1,5)(1,4)(1,6)(1,7)(1,6) \\ &= (1,3)(1,2)(1,3)(1,4)(1,3)(1,4)(1,5)(1,4)(1,6)(1,7)(1,6) \end{aligned}$$

Proposition 4.10. *Le groupe $\mathcal{S}_n$ est engendré par les $n-1$ transpositions $(k,k+1)$ où $1 \leq k \leq n-1$.*

Démonstration. Comme $\mathcal{S}_n$ est engendré par les transpositions $(1,k)$ où $2 \leq k \leq n$, il suffit d'écrire chaque transposition $(1,k)$ comme produit de transposition du type $(i,i+1)$.
Pour $3 \leq k \leq n$, on a

$$(1,k) = (k-1,k)(1,k-1)(k-1,k)^{-1} = (k-1,k)(1,k-1)(k-1,k)$$

Pour $k = 3$, on a $(1,k-1) = (1,2)$ et c'est terminé, sinon on écrit

$$(1,k-1) = (k-2,k-1)(1,k-2)(k-2,k-1)$$

et on continue ainsi de suite si nécessaire.
Pour $k = 2$, la transposition $(1,k) = (1,2)$ est de la forme cherchée. □

Proposition 4.11. *Le groupe $\mathcal{S}_n$ est engendré par $(1,2)$ et $(1,2,\ldots,n)$.*

Démonstration. Comme $\mathcal{S}_n$ est engendré par les transpositions $(k,k+1)$ où $1 \leq k \leq n-1$, il suffit de montrer que chaque transposition $(k,k+1)$ est dans le sous-groupe G de $\mathcal{S}_n$ engendré par $\tau = (1,2)$ et $\gamma = (1,2,\ldots,n)$.

On a $(1,2) \in G$ et pour $n \geq 3$,

$$\begin{aligned} \gamma(1,2)\gamma^{-1} &= (\gamma(1),\gamma(2)) = (2,3) \\ \gamma(2,3)\gamma^{-1} &= (\gamma(2),\gamma(3)) = (3,4) \\ &\vdots \\ \gamma(n-2,n-1))\gamma^{-1} &= (\gamma(n-2),\gamma(n-1)) = (n-1,n) \end{aligned}$$

soit

$$(k,k+1) = \gamma^{k-1}(1,2)(\gamma^{k-1})^{-1} \text{ pour } 1 \leq k \leq n-1$$

□

5. Signature d'une permutation

Pour toute permutation $\sigma \in \mathcal{S}(E)$, on note $\mu(\sigma)$ le nombre de σ-orbites distinctes.

Si $\sigma = \sigma_1 \circ \cdots \circ \sigma_p$ est la décomposition de σ en produit de cycles deux à deux disjoints, on a vu que p est le nombre de σ-orbites non réduites à un point et donc $\mu(\sigma) = p + \varphi(\sigma)$ où $\varphi(\sigma)$ est le nombre de points fixes de σ (nombre de σ-orbites réduites à un point).

Définition 5.1. *La signature d'une permutation $\sigma \in \mathcal{S}(E)$ est l'éléments $\varepsilon(\sigma) \in \{-1, +1\}$ défini par*

$$\varepsilon(\sigma) = (-1)^{n-\mu(\sigma)}.$$

Exemple 5.2. (a) L'identité a n orbites réduites à un point $\varphi(Id) = n$ et pas d'orbites non réduite à un point $p = 0$, donc $\mu(Id) = n$ et $\varepsilon(Id) = 1$.

(b) Si σ est un r-cycle, il a une orbite non réduite à un point et $n-r$ orbites réduites à un point, donc $\mu(\sigma) = n - r + 1$ et $\varepsilon(\sigma) = (-1)^{r-1}$

(c) Une transposition (cycle d'ordre 2) est de signature $\varepsilon(\tau) = -1$.

Proposition 5.3. *Pour toute permutation $\sigma \in \mathcal{S}(E)$ et toute transposition $\tau \in \mathcal{S}(E)$, on a*

$$\varepsilon(\tau\sigma) = -\varepsilon(\sigma).$$

Démonstration. Soit $\tau = (x, y)$ une transposition dans $\mathcal{S}(E)$ avec $x \neq y$.
Si $\sigma = Id_E$, alors $\tau\sigma = \tau$ et $\varepsilon(\tau\sigma) = \varepsilon(\tau) = -1$.
Pour $\sigma \neq Id_E$, on a la décomposition en produit de cycles deux à deux disjoints, $\sigma = \sigma_1 \cdots \sigma_p$ où $\mathcal{O}_k = \text{supp}(\sigma_k)$, pour $1 \leq k \leq p$ sont toutes les orbites non réduites à un point.

Si $\{x, y\} \cap \cup_{k=1}^{p} \mathcal{O}_k = \emptyset$, le nombre de points fixes de $\sigma' = \tau\sigma$ est alors $\varphi(\sigma') = \varphi(\sigma) - 2$ et le nombre de σ'-orbites est

$$\mu(\sigma') = p + 1 + \varphi(\sigma) - 2 = \mu(\sigma) - 1$$

ce qui donne $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

Si $\{x, y\}$ est contenu dans l'une des σ-orbites $\mathcal{O}_k$, comme les cycles σ_j commutent, on a

$$\sigma' = \tau\sigma_k \prod_{j=1, j\neq k}^{p} \sigma_j$$

avec

$$y \in \mathcal{O}_k = Orb_\sigma(x) = \{x, \sigma(x), \cdots, \sigma^{r_k-1}(x)\} = \{x_1, \cdots, x_{r_k}\}.$$

Il existe alors $j \in \{2, \cdots, r_k\}$ tel que $y = x_j$ et

$$\begin{aligned} \tau\sigma_k &= (x_1, x_j)(x_1, \cdots, x_j, \cdots, x_{r_k}) \\ &= (x_1, \cdots, x_{j-1})(x_j \cdots, x_{r_k}) = \sigma'_k\sigma''_k \end{aligned}$$

(pour $k = r_k$, $\sigma''_k = Id$), ce qui donne la décomposition en produit de cycles deux à deux disjoints

$$\sigma' = \sigma'_k\sigma''_k \prod_{j=1, j\neq k}^{p} \sigma_j.$$

On a donc $\mu(\sigma') = \mu(\sigma) + 1$ (pour $j = r_k$ le nombre de cycles est inchangé, mais x_{r_k} est un point fixe de plus) et $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

Si x et y sont dans deux σ-rbites distinctes, soit $\{x, y\} \cap \mathcal{O}_k = \{x\}$ et $\{x, y\} \cap \mathcal{O}_j = \{y\}$ avec $j \neq k$, on a

$$\mathcal{O}_k = Orb_\sigma(x) = \{x, \sigma(x), \cdots, \sigma^{r_k - 1}(x)\} = \{x_1, \cdots, x_{r_k}\}, \quad \text{avec} \quad x = x_1$$

et

$$\mathcal{O}_j = Orb_\sigma(y) = \{y, \sigma(y), \cdots, \sigma^{r_j - 1}(y)\} = \{y_1, \cdots, y_{r_j}\}, \quad \text{avec} \quad y = y_j$$

donc

$$\begin{aligned} \tau\sigma_k\sigma_j &= (x_1, y_1)(x_1, \cdots, x_{r_k})(y_1, \cdots, y_{r_j}) \\ &= (y_1, x_1)(x_1, \cdots, x_{r_k})(y_1, \cdots, y_{r_j}) \\ &= (x_1, \cdots, x_{r_k}, y_1)(y_1, \cdots, y_{r_j}) \\ &= (x_1, \cdots, x_{r_k}, y_1, \cdots, y_{r_j}) = \sigma'_k \end{aligned}$$

et on a la décomposition en produit de cycles deux à deux disjoints

$$\sigma' = \tau\sigma_k\sigma_j \prod_{j=1, j \notin \{j,k\}}^{p} \sigma_i = \sigma'_k \prod_{j=1, j \notin \{j,k\}}^{p} \sigma_i$$

par suite, $\mu(\sigma') = \mu(\sigma) - 1$ et $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

Enfin, la dernière possibilité est que x (resp. y) soit dans l'une des orbites $\mathcal{O}_k$ et y (resp. x) e dehors de la réunion de toutes les orbites. On a alors $\varphi(\sigma') = \varphi(\sigma) + 1$ et

$$\mathcal{O}_k = Orb_\sigma(x) = \{x, \sigma(x), \cdots, \sigma^{r_k - 1}\} = \{x_1, \cdots, x_{r_k}\}$$

donc

$$\tau\sigma_k = (x_1, y)(x_1, \cdots, x_{r_k}) = (y, x_1, \cdots, x_{r_k})$$

d'où $\mu(\sigma') = \mu(\sigma) + 1$ et $\varepsilon(\sigma') = -\varepsilon(\sigma)$.

□

Théorème 5.4. *Si $\sigma \in \mathcal{S}(E)$ est produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$.*

Démonstration. C'est une conséquence immédiate de la proposition précédente et du fait que $\varepsilon(\tau) = -1$ pour toute transposition τ. □

Théorème 5.5. *Les seuls morphismes de groupes de $(\mathcal{S}(E), \circ)$ dans $(\mathbb{R}^*, \times)$ sont l'application constante égale à 1 et la signature ε. La signature étant un morphisme surjectif de $\mathcal{S}(E)$ sur $\{-1, +1\}$.*

Démonstration. Montrons d'abord que ε est un morphisme de groupes surjectif de $(\mathcal{S}(E), \circ)$ dans $(\{-1, +1\}, \times)$.

On sait que ε est à valeurs dans $\{-1, +1\}$ avec $\varepsilon(Id) = +1$ et $\varepsilon(\tau) = -1$ pour toute transposition τ. On en déduit que ε est surjectif.

Si σ et σ' sont deux permutations, elles s'écrivent respectivement comme produit de p et q transpositions, et donc $\sigma\sigma'$ s'écrit comme produit de $p + q$ transpositions. On a alors $\varepsilon(\sigma\sigma') = (-1)^{p+q} = (-1)^p(-1)^q = \varepsilon(\sigma)\varepsilon(\sigma')$. Donc ε est un morphisme surjectif de groupes.

Soit φ un morphisme de groupes de $\mathcal{S}(E)$ dans $\mathbb{R}^*$.

Si τ_1 et τ_2 sont deux transpositions, il existe une permutation σ telle que $\tau_2 = \sigma\tau_1\sigma^{-1}$ et comme le groupe multiplicatif $\mathbb{R}^*$ est abélien, on a

$$\varphi(\tau_2) = \varphi(\sigma\tau_1\sigma^{-1}) = \varphi(\sigma)\varphi(\tau_1)\varphi(\sigma^{-1}) = \varphi(\sigma)\varphi(\sigma^{-1})\varphi(\tau_1) = \varphi(\tau_1)$$

ce qui veut dire que φ est constant sur les transpositions, avec

$$1 = \varphi(Id) = \varphi(\tau^2) = (\varphi(\tau))^2$$

pour toute transposition τ. On déduit alors que

$$\begin{cases} \varphi(\tau) = +1, & \forall\ \tau \ \text{ transposition} \\ \text{ou} \\ \varphi(\tau) = -1, & \forall\ \tau \ \text{ transposition} \end{cases}$$

Dans le premier cas, φ est l'application constante égale à 1, puisque $\mathcal{S}(E)$ est engendré par les transpositions. Dans le second cas, comme toute permutation σ s'écrit $\sigma = \prod_{k=1}^{p} \tau_k$ où les τ_k sont des transpositions, on a

$$\varphi(\sigma) = \prod_{k=1}^{p} \varphi(\tau_k) = (-1)^p = \varepsilon(\sigma).$$

□

Exemple 5.6. On considère la permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}.$$

On a

$$\sigma = (1, 5, 4, 3, 2)(6, 7)$$

et $\varepsilon(\sigma) = (-1)^{5-1}(-1) = -1$.

On peut aussi écrire σ comme produit de transpositions

$$\sigma = (1, 2)(2, 3)(3, 4)(4, 5)(6, 7)$$

et donc $\varepsilon(\sigma) = (-1)^5 = -1$ (il y a 5 transpositions dans la décomposition de σ).

Proposition 5.7. *Pour toute permutation de $\sigma \in \mathcal{S}_n$, on a*

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

Démonstration. Soit φ l'application définie sur $\mathcal{S}_n$ par

$$\varphi(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Pour montrer que $\varphi = \varepsilon$, il suffit de montrer que φ est un morphisme de groupes non constant de $\mathcal{S}_n$ dans $\mathbb{R}^*$.

Comme σ est bijective, on a $\varphi(\sigma) \in \mathbb{R}^*$ pour tout $\sigma \in \mathcal{S}_n$.

Pour $\sigma_1, \sigma_2 \in \mathcal{S}_n$, on a

$$\begin{aligned}\varphi(\sigma_1\sigma_2) &= \prod_{1\le i<j\le n} \frac{\sigma_1(\sigma_2(j))-\sigma_1(\sigma_2(i))}{\sigma_2(j)-\sigma_2(i)} \frac{\sigma_2(j)-\sigma_2(i)}{j-i} \\ &= \prod_{1\le i<j\le n} \frac{\sigma_1(\sigma_2(j))-\sigma_1(\sigma_2(i))}{\sigma_2(j)-\sigma_2(i)} \prod_{1\le i<j\le n} \frac{\sigma_2(j)-\sigma_2(i)}{j-i} \\ &= \prod_{1\le i'<j'\le n} \frac{\sigma_1(j')-\sigma_1(i')}{j'-i'} \prod_{1\le i<j\le n} \frac{\sigma_2(j)-\sigma_2(i)}{j-i}\end{aligned}$$

puisque σ_2 est bijective de $\{1,\dots,n\}$ sur $\{1,\dots,n\}$ et

$$\frac{\sigma_1(j')-\sigma_1(i')}{j'-i'} = \frac{\sigma_1(i')-\sigma_1(j')}{i'-j'}$$

ce qui donne $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$ et donc φ est un morphisme de groupes de $\mathcal{S}_n$ dans $\mathbb{R}^*$.

De plus on a $\varphi(Id) = 1$ et pour $\tau = (1,2)$,

$$\begin{aligned}\varphi(\tau) &= \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\tau(j)-\tau(i)}{j-i} \\ &= \prod_{j=2}^{n} \frac{\tau(j)-2}{j-1} \prod_{j=3}^{n} \frac{\tau(j)-1}{j-2} \\ &= -\prod_{j=3}^{n} \frac{j-2}{j-1}\frac{j-1}{j-2} = -1\end{aligned}$$

donc φ est non constant et c'est la signature. □

Remarque 5.8. Du théorème précédent, on déduit que

$$\varepsilon(\sigma) = (-1)^{\nu(\sigma)}$$

où

$$\nu(\sigma) = \{\mathbf{card}\{(i,j) \in \mathbb{N}^2;\ \ 1 \le i < j \le n \text{ et } \sigma(j) < \sigma(i)\}\}$$

L'entier $\nu(\sigma)$ est le nombre d'**inversions** de σ.

Exemple 5.9. La permutation

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

a 5 invesions, donc $\epsilon(\sigma) = (-1)^5 = -1$

6. Le groupe alterné

Définition 6.1. *On dit d'une permutation $\sigma \in \mathcal{S}(E)$ est paire (resp. impaire) si $\varepsilon(\sigma) = +1$ (resp. $\varepsilon(\sigma) = -1$)*

Les cycles de longueur paire (resp. impaire) sont impaires (resp. paires).

Définition 6.2. *Le* **groupe alterné** *est le sous-ensemble de $\mathcal{S}(E)$ formé des permutations paires. On le note $\mathcal{A}(E)$.*
Pour $E = \{1,\dots,n\}$, on note $\mathcal{A}_n$ le groupe altérné.

Remarque 6.3. (a) $\mathcal{A}(E)$ est un sous-groupe distingué de $\mathcal{S}(E)$. Cela vient du fait que le groupe altérné $\mathcal{A}(E)$ est le noyau du morphisme ε. On a alors $\mathcal{S}(E)/\mathcal{A}(E) \simeq \{-1,+1\}$ et $\mathbf{card}(\mathcal{A}(E)) = \frac{n!}{2}$. Le sous-groupe $\mathcal{A}(E)$ est donc d'indice 2 dans $\mathcal{S}(E)$.

(b) Pour $n = 2$, $\mathcal{A}(E) = \{Id\}$.

(c) $\mathcal{A}_3$ est cyclique, engendré par $\gamma_1 = (1,2,3)$. En effet, $\mathbf{card}(\mathcal{A}_3) = \frac{3!}{2} = 3$ et le cycle γ_1 est d'ordre 3 dans $\mathcal{A}_3$.

On suppose pour la suite du paragraphe que $n \geq 3$.

Proposition 6.4. *Le produit de deux transpositions est un produit de* 3*-cycles. Précisément, pour x, y, z, t deux à deux distincts dans E, on a*

$$(x,y)(x,z) = (x,z,y) \quad \textit{et} \quad (x,y)(z,t) = (x,y,z)(y,z,t).$$

Démonstration. Soient τ_1 et τ_2 deux transpositions. Si $\tau_1 = \tau_2$, alors $\tau_1\tau_2 = \tau_1^2 = Id = \gamma^3$ pour n'importe quel 3-cycle.

Si $\tau_1 \neq \tau_2$, on a alors deux possibilités :

— soit $\mathrm{supp}(\tau_1) \cap \mathrm{supp}(\tau_2) = \{x\}$, donc $\tau_1 = (x,y)$ e, $\tau_2 = (x,z)$ avec $x, y, z \in E$ distincts et
$$\tau_1\tau_2 = (y,x)(x,z) = (y,x,z) = (x,z,y)$$

— soit $\mathrm{supp}(\tau_1) \cap \mathrm{supp}(\tau_2) = \emptyset$, donc $\tau_1 = (x,y)$ e, $\tau_2 = (z,t)$, avec $x, y, z, t \in E$ distincts et
$$\tau_1\tau_2 = (x,y)(z,t) = (x,y)(y,z)(y,z)(z,t) = (x,y,z)(y,z,t).$$

□

Théorème 6.5. *Pour $n \geq 3$, le groupe alterné $\mathcal{A}(E)$ est engendré par les 3-cycles.*

Démonstration. Comme $\mathcal{S}(E)$ est engendré par les transpositions, on déduit du Théorème 5.4 qu'une permutation paire est le produit d'un nombre pair de transpositions et la proposition précédente nous dit que ce produit s'écrit comme produit de 3-cycles. □

Théorème 6.6. *Pour $n \geq 5$, les sous-groupes distingués de $\mathcal{S}(E)$ sont $\{Id\}$, $\mathcal{A}(E)$ et $\mathcal{S}(E)$.*

Démonstration. Soit H un sous-groupe distingué de $\mathcal{S}(E)$ distinct de $\{Id\}$.

Si H contient un 3-cycle σ, et si σ' est un autre 3-cycle, alors d'après Proposition 1.9 il existe $\gamma \in \mathcal{S}(E)$ tel que $\sigma' = \gamma\sigma\gamma^{-1}$. Comme H est distingué dans $\mathcal{S}(E)$, $\sigma' \in H$. Donc si H contient un 3-cycle, il contient tous les 3-cycles. Comme les 3-cycles engendrent $\mathcal{A}(E)$ on a $\mathcal{A}(E) \subset H$. On en déduit que $H = \mathcal{A}(E)$ ou $H = \mathcal{S}(E)$. En effet, on a $\mathcal{A}(E) \subset H \subset \mathcal{S}(E)$, soit $[H : \mathcal{A}(E)] = p$ l'indice de $\mathcal{A}(E)$ dans H et $[\mathcal{S}(E) : H] = q$ l'indice de H dans $\mathcal{S}(E)$. Alors $|H| = p\frac{n!}{2} = p\frac{q|H|}{2}$, d'où $pq = 2$. Donc soit $p = 1$ donc $\mathcal{A}(E) = H$, soit $p = 2$ donc $H = \mathcal{S}(E)$.

Il reste donc à montre que H contient au moins un 3-cycle. On se donne $\sigma \in H \setminus \{Id\}$ et $\tau = (x,y)$ une transposition qui ne commute pas à σ (ceci est possible d'après Proposition 1.10). Comme H est distingué dans $\mathcal{S}(E)$, on a

$$\sigma' = \tau\sigma\tau\sigma^{-1} = (\tau\sigma\tau^{-1})\sigma^{-1} \in H$$

et en écrivant

$$\sigma' = (x,y)(\sigma(x,y)\sigma^{-1}) = (x,y)(\sigma(x),\sigma(y))$$

on voit que σ' est produit de deux transpositions.

L'égalité $\sigma' = Id$ est réalisée si, et seulement si, $\tau\sigma\tau\sigma^{-1} = Id$ ou encore $\tau\sigma = \sigma\tau$ ce qui est exclu.

Si $\{x,y\} \cap \{\sigma(x),\sigma(y)\}$ est réduit à un point, alors σ' est un 3-cycle. Sinon cette intersection est vide et en prenant $z \in E \setminus \{x,y,\sigma(x),\sigma(y)\}$ (on a $n \geq 5$), le groupe H contient $(x,y)(\sigma(x),z)$ puisque le produit de deux transpositions de supports disjoints sont conjugués dans $\mathcal{S}(E)$ et H est distingué. Il en résulte que H contient

$$(x,y)(\sigma(x),\sigma(y))(x,y)(\sigma(x),z) = (\tau(\sigma(x)),\tau(\sigma(y)))(\sigma(x),z) = (\sigma(x),\sigma(y))(\sigma(x),z)$$

qui est le 3-cycle $(\sigma(y),\sigma(x),z)$. D'où $H = \mathcal{S}(E)$.

□

Lemme 6.7. *Pour $n \geq 5$ deux 3-cycles sont conjugués dans $\mathcal{A}(E)$.*

Démonstration. Soient $\gamma = (x_1,x_2,x_3)$ et $\gamma' = (x'_1,x'_2,x'_3)$ deux 3-cycles. Puisque deux cycles de même longueur sont conjugués dans $\mathcal{S}(E)$, alors γ et γ' sont conjugués dans $\mathcal{S}(E)$. Il existe donc une permutation $\sigma \in \mathcal{S}(E)$ telle que $\gamma' = \sigma\gamma\sigma^{-1}$. On a alors $\sigma(x_k) = x'_k$ pour $k = 1,2,3$. Si $\sigma \in \mathcal{A}(E)$, c'est terminé. Sinon on choisit $x_4, x_5 \in E \setminus \{x_1,x_2,x_3\}$ (E a au moins 5 éléments distincts) et on considère la permutation $\sigma' = (x_4,x_5)\sigma$. On a $\sigma' \in \mathcal{A}(E)$ et $\sigma'(x_k) = x'_k$, donc $\gamma' = \sigma'\gamma\sigma'^{-1}$. □

Théorème 6.8. *Pour $n = 3$ ou $n \geq 5$, le groupe $\mathcal{A}(E)$ est simple (c-à-d. n'a pas de sous-groupes distingués autres que lui même et $\{Id\}$).*

Démonstration. Pour $n = 3$, $\mathcal{A}(E)$ est cyclique d'ordre 3, il est donc simple.

On suppose $n \geq 5$ et on se donne un sous-groupe distingué H de $\mathcal{A}(E)$ distinct de $\{Id\}$. Pour montrer que $H = \mathcal{A}(E)$, il suffit de montrer que H contient un 3-cycle puisque les 3-cycles sont tous conjugués dans $\mathcal{A}(E)$, d'après le lemme précédent, et que les 3-cycles engendrent le groupe alterné.

Soit $\sigma \in H \setminus \{Id\}$ et $\gamma = (x,y,z) \in \mathcal{A}(E)$ un 3-cycle avec $y = \sigma(x)$ qui ne commute pas à σ (ceci est possible puisque pour $n \geq 3$ le centre du groupe alterné est réduit à $\{Id\}$ d'après Proposition 1.10). Comme H est distingué dans $\mathcal{A}(E)$, on a

$$\sigma' = \sigma\gamma\sigma^{-1}\gamma^{-1} = \sigma(\gamma\sigma^{-1}\gamma^{-1}) \in H.$$

En écrivant

$$\begin{aligned} \sigma' &= (\sigma(x,z,y)\sigma^{-1})(y,z,x) = (\sigma(x),\sigma(z),\sigma(y))(y,z,x) \\ &= (y,\sigma(z),\sigma(y))(y,z,x) \end{aligned}$$

on voit que σ' est produit de deux 3-cycles qui agissent sur l'ensemble $F = \{x,y,z,\sigma(y),\sigma(z)\}$ formé d'au plus 5 éléments (tous les points de $E \setminus F$ sont fixes).

L'égalité $\sigma' = Id$ est réalisée si, et seulement si, $\sigma\gamma\sigma^{-1}\gamma^{-1} = Id$ soit $\gamma\sigma = \sigma\gamma$ ce qui n'est pas vraie, donc $\sigma' \neq Id$.

Dans $\mathcal{S}(F)$ la permutation σ' s'écrit donc comme produit de cycles de supports disjoints, cette décomposition étant celle de $\mathcal{S}(E)$ et comme $\sigma' \in \mathcal{A}(E)$, il n'y a que trois possibilités : σ' est soit un 3-cycle, soit σ' est un produit de deux transpositions de supports disjoints, soit σ' est un 5-cycle.

— Dans le premier cas on a le résultat voulu.

— Dans le deuxième cas, on a $\sigma' = (x_1,x_2)(x_3,x_4)$ et choisissant $x_5 \in E\setminus\{x_1,x_2,x_3,x_4\}$, on a

$$\sigma'' = (x_1,x_5)\sigma'(x_1,x_5)(\sigma')^{-1} = ((x_1,x_5)\sigma'(x_1,x_5)^{-1})(\sigma')^{-1} \in H$$

avec

$$\sigma'' = (x_1, x_5)(\sigma'(x_1), \sigma'(x_5)) = (x_1, x_5)(x_2, x_5) = (x_1, x_5, x_2)$$

d'où le résultat cherché.

— Dans le troisième cas, on a $\sigma' = (x_1, x_2, x_3, x_4, x_5)$ et

$$\sigma'' = (x_1, x_2)\sigma'(x_1, x_2)(\sigma')^{-1} = ((x_1, x_2)\sigma'(x_1, x_2)^{-1})(\sigma')^{-1} \in H$$

avec

$$\sigma'' = (x_1, x_2)(\sigma'(x_1), \sigma'(x_2)) = (x_1, x_2)(x_2, x_3) = (x_1, x_2, x_3)$$

d'où le résultat cherché.

□