Chapitre 2
Groupes de permutations

Ce court chapitre a pour but de rappeler les notions de base sur les groupes de permutations et, en particulier, d'établir les propriétés de la signature (la signature d'une permutation est un signe ± 1 décrivant sa parité).

1. Définitions et premières propriétés

1.1. Groupe des permutations d'un ensemble

1.1.1. Définition. *Soit A un ensemble. On note $\mathfrak{S}_A$ l'ensemble des applications bijectives $\sigma : A \to A$ (qu'on appelle aussi permutations de A). Pour la composition des applications $\circ$, on a une structure de groupe $(\mathfrak{S}_A, \circ)$, non commutatif si* $\operatorname{card} A \geqslant 3$.

L'élément neutre du groupe est Id_A et le symétrique d'un élément $\sigma \in \mathfrak{S}_A$ est la bijection inverse σ^{-1} (l'associativité étant toujours vraie pour la composition des applications). On s'intéressera ici surtout au cas où A est un ensemble fini, noté $A = \{a_1, \ldots, a_n\}$.

1.1.2. Notation. *Une permutation $\sigma \in \mathfrak{S}_A$ pourra être définie en donnant la liste des images successives $\sigma(a_i)$ des éléments $a_i \in A$. On notera ainsi*

$$\sigma = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \\ b_1 & b_2 & \ldots & b_n \end{bmatrix}$$

la permutation σ telle que $\sigma(a_i) = b_i$.

1.1.3. Définition. *Le support d'une paermutation $\sigma \in \mathfrak{S}_A$ est par définition la partie*

$$\operatorname{Supp} \sigma = \{x \in A \,/\, \sigma(x) \neq x\}.$$

C'est donc le complémentaire dans A de l'ensemble des éléments invariants, soit

$$\operatorname{Inv} \sigma = \{x \in A \,/\, \sigma(x) = x\}.$$

1.1.4. Définition. *On désigne par $\mathfrak{S}_n$ l'ensemble des permutations de $\{1, 2, ..., n\}$. On a* $\operatorname{card} \mathfrak{S}_n = n!$.

En effet, une telle permutation est obtenue en choisissant $\sigma(1)$ dans $\{1,\dots,n\}$ (n choix possibles), puis $\sigma(2)$ dans $\{1,\dots,n\}\setminus\{\sigma(1)\}$ ($n-1$ choix possibles), puis $\sigma(3)$ dans $\{1,\dots,n\}\setminus\{\sigma(1),\sigma(2)\}$ ($n-2$ choix possibles), etc, ce qui donne

$$\operatorname{card}\mathfrak{S}_n = n\times(n-1)\times(n-2)\times\cdots\times 2\times 1 = n!$$

(il ne reste plus qu'un choix pour le dernier élément $\sigma(n)$, les autres ayant déjà été choisis). □

1.2. Transpositions et cycles

Les exemples fondamentaux de permutations sont les transpositions et les cycles :

1.2.1. Transpositions. Si a,b sont des éléments distincts de A, on note $\tau_{a,b}\in\mathfrak{S}_A$ la permutation définie par

$$\tau_{a,b}(a)=b,\quad \tau_{a,b}(b)=a,\quad \tau_{a,b}(x)=x,\quad \text{si } x\in A\setminus\{a,b\}.$$

La permutation $\tau_{a,b}$ correspond donc à faire l'échange des éléments a,b sans "toucher" aux autres éléments, par suite $\operatorname{Supp}\tau_{a,b}=\{a,b\}$. Il est clair que $\tau_{a,b}$ est une involution, c'est-à-dire que $\tau_{a,b}^2=\mathrm{Id}_A$ (ou encore que c'est un élément d'ordre 2 du groupe $\mathfrak{S}_A$).

1.2.2. Rappel. *Dans un groupe $(G,*)$, un élément x est dit d'ordre fini s'il existe un entier $k\in\mathbb{N}^*$ tel que $x^k=x*x*\cdots*x=1_G$, et on appelle ordre de x, noté* $\operatorname{ordre}(x)$*, le plus petit entier $k\in\mathbb{N}^*$ tel que $x^k=1_G$.*

1.2.3. Cycle de longueur ℓ. Soit $a_1,a_2,\dots,a_\ell$ des éléments 2 à 2 distincts de l'ensemble A. on considère la permutation c définie par

$$c=\begin{bmatrix} a_1 & a_2 & \dots & a_{\ell-1} & a_\ell & b_1 & b_2 & \dots & b_{n-\ell}\\ a_2 & a_3 & \dots & a_\ell & a_1 & b_1 & b_2 & \dots & b_{n-\ell}\end{bmatrix}$$

où $A\setminus\{a_1,\dots,a_\ell\}=\{b_1,\dots,b_{n-\ell}\}$, en d'autres termes c est telle que

$$c: a_1\mapsto a_2\mapsto a_3\mapsto\cdots\mapsto a_{\ell-2}\mapsto a_{\ell-1}\mapsto a_\ell\mapsto a_1$$

et $c(x)=x$ pour $x\notin\{a_1,\dots,a_\ell\}$. Un tel cycle est noté en abrégé

$$c=(a_1\ a_2\ \dots\ a_\ell).$$

Le support du cycle c est donc la partie $\operatorname{Supp}c=\{a_1,\dots,a_\ell\}$, et une transposition $\tau_{a,b}$ n'est pas autre chose qu'un cycle $(a\,b)$ de longueur 2. En général, il est facile de voir que $c^k(a_i)=a_{k+i \bmod \ell}$, c'est-à-dire

$$c^k=\begin{bmatrix} a_1 & a_2 & \dots & a_{\ell-k} & a_{\ell-k+1} & \dots & a_{\ell-1} & a_\ell & b_1 & b_2 & \dots & b_{n-\ell}\\ a_{k+1} & a_{k+2} & \dots & a_\ell & a_1 & \dots & a_{k-1} & a_k & b_1 & b_2 & \dots & b_{n-\ell}\end{bmatrix}$$

pour $k \leqslant \ell - 1$ et $c^\ell = \mathrm{Id}_A$, par conséquent ordre$(c) = \ell$. Il est facile de voir que l'on a pour tout $i = 0, 1, \ldots, \ell - 1$ l'égalité

$$c = (a_1\ a_2\ \ldots\ a_\ell) = (a_{i+1}\ a_{i+2}\ \ldots\ a_\ell\ a_1\ a_2\ \ldots\ a_i),$$

par exemple (1 2 3 4 5) = (4 5 1 2 3), c'est-à-dire que le cycle ne dépend pas de son point de départ, si "l'ordre cyclique" des éléments est préservé. En revanche, le cycle (1 2 3 4 5) n'est pas égal au cycle (1 3 2 4 5).

1.2.4. Exemple. Le groupe $\mathfrak{S}_3$ est constitué des 6 éléments

$$\mathfrak{S}_3 = \{\mathrm{Id}, c, c^2, \tau_{1,2}, \tau_{2,3}, \tau_{1,3}\} \quad \text{où} \quad c = (1\ 2\ 3),\quad c^2 = (1\ 3\ 2),\quad c^3 = \mathrm{Id}\,.$$

On calcule aisément la table de Pythagore du groupe $\mathfrak{S}_3$:

$(u, v) \mapsto u \circ v$

$u \backslash v$	Id	c	c^2	$\tau_{1,2}$	$\tau_{2,3}$	$\tau_{1,3}$
Id	Id	c	c^2	$\tau_{1,2}$	$\tau_{2,3}$	$\tau_{2,3}$
c	c	c^2	Id	$\tau_{1,3}$	$\tau_{1,2}$	$\tau_{2,3}$
c^2	c^2	Id	c	$\tau_{2,3}$	$\tau_{1,3}$	$\tau_{1,2}$
$\tau_{1,2}$	$\tau_{1,2}$	$\tau_{2,3}$	$\tau_{1,3}$	Id	c	c^2
$\tau_{2,3}$	$\tau_{2,3}$	$\tau_{1,3}$	$\tau_{1,2}$	c^2	Id	c
$\tau_{1,3}$	$\tau_{1,3}$	$\tau_{1,2}$	$\tau_{2,3}$	c	c^2	Id

On voit en particulier que le groupe $(\mathfrak{S}_3, \circ)$ est non commutatif, et donc $\mathfrak{S}_n$ est non commutatif pour $n \geqslant 3$ (mais $\mathfrak{S}_1 = \{\mathrm{Id}\}$ et $\mathfrak{S}_2 = \{\mathrm{Id}, \tau_{1,2}\}$ sont commutatifs).

1.3. Décomposition en cycles à supports disjoints

Prenons d'abord l'exemple de la permutation $\sigma \in \mathfrak{S}_8$ telle que

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

On a $\mathrm{Inv}\,\sigma = \{5\}$ et $\mathrm{Supp}\,\sigma = \{1, 2, 3, 4, 6, 7, 8\}$. Considérons les images des éléments successifs du support :

$$1 \mapsto 6 \mapsto 2 \mapsto 1$$
$$3 \mapsto 7 \mapsto 3$$
$$4 \mapsto 8 \mapsto 4$$

Pour chaque ligne, on prend les images successives et on s'arrête lorsqu'on retombe sur l'élément de départ. On considère ensuite à chaque ligne le premier élément du

support qui n'a pas encore été pris en compte. On voit alors que σ est la composée d'un cycle de longueur 3 et de deux cycles de longueur 2 (transpositions) :

$$\sigma = (1\ 6\ 2) \circ (3\ 7) \circ (4\ 8),$$

avec l'élément 5 qui n'intervient pas (car invariant). L'ordre des composées importe peu, car on a le résultat évident suivant.

1.3.1. Lemme. *Si c et c' sont des cycles dont les supports* $\operatorname{Supp} c$ *et* $\operatorname{Supp} c'$ *sont disjoints* ($\operatorname{Supp} c \cap \operatorname{Supp} c' = \emptyset$), *alors $c' \circ c = c \circ c'$.*

Quel que soit l'ordre de composition, l'image $\sigma(x)$ de la composée σ coïncide en effet avec $c(x)$ si $x \in \operatorname{Supp} c$, avec $c'(x)$ si $x \in \operatorname{Supp} c'$, tandis que $\sigma(x) = x$ si $x \notin \operatorname{Supp} c \cup \operatorname{Supp} c'$. □

En considérant les itérés successifs $\sigma^k(x)$ des éléments du support d'une permutation σ quelconque, on obtient de même le résultat général suivant.

1.3.2. Théorème. *Toute permuation $\sigma \in \mathfrak{S}_A$ d'un ensemble fini A se décompose en un produit commutatif de cycles, c'est-à-dire que*

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_p$$

avec des cycles c_j dont les supports $\operatorname{Supp} c_j$ *sont 2 à 2 disjoints. Une telle décomposition est unique à l'ordre près des c_j et on a*

$$\operatorname{Supp} \sigma = \operatorname{Supp} c_1 \cup \ldots \cup \operatorname{Supp} c_p.$$

Démonstration. Il faut d'abord voir que si on prend les itérés d'un élément $x_0 \in \operatorname{Supp} \sigma$ quelconque, soit

$$x_0, \quad x_1 = \sigma(x_0), \quad \ldots \quad , \quad x_i = \sigma(x_{i-1}) = \sigma^i(x_0),$$

il y nécessairement un indice $m \in [2, \operatorname{card} A]$ minimal tel que $x_m \in \{x_0, \ldots, x_{m-1}\}$ (sinon on aurait $\operatorname{card}\{x_0, \ldots, x_{i-1}\} \geqslant i$ pour tout i, ce qui contredit la finitude de A). D'autre part, on a nécessairement $x_m = \sigma^m(x_0) = x_0$, sinon on "retomberait" sur $x_m = \sigma^m(x_0) = x_i = \sigma^i(x_0)$ avec $i > 0$, et ceci impliquerait $x_{m-i} = \sigma^{m-i}(x_0) = x_0$, contredisant la minimalité de m. Enfin , si on prend $y_0 \in \operatorname{Supp} \sigma$ en dehors de "l'orbite" $\{x_0, \ldots, x_{m-1}\}$ de x_0, alors tous les itérés $y_i = \sigma^i(y_0)$ sont également en dehors de cette orbite (vérification évidente : $\sigma^i(y_0) = \sigma^j(x_0)$ impliquerait $y_0 = \sigma^{j-i}(x_0)$ ou $y_0 = \sigma^{j+m-i}(x_0)$ suivant que $j \geqslant i$ ou $j < i$). Les orbites qui constituent les supports des cycles sont donc disjointes. □

1.4. Ordre d'une permutation

Soit $\sigma \in \mathfrak{S}_A$ une permutation d'un ensemble fini A, et écrivons

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_p$$

avec les cycles de longueurs respectives $\ell_1, \ell_2, \ldots, \ell_p$. Comme les cycles commutent, on trouve pour tout $k \in \mathbb{N}^*$

$$\sigma^k = c_1^k \circ c_2^k \circ \cdots \circ c_p^k$$

(on remarquera que dans un groupe non commutatif $(G, \cdot)$, on a en général $(xy)^2 = xyxy$, ce qui ne coïncide avec $x^2y^2 = xxyy$ que si x et y commutent). On a $c_j^k = \mathrm{Id}$ si et seulement si k est multiple de la longeur ℓ_j du cycle c_j. Or, pour $x \in \operatorname{Supp} c_j$, on a $\sigma^k(x) = c_j^k(x)$, donc on voit que $\sigma^k = \mathrm{Id}$ si et seulement si k est simultanément multiple de $\ell_1, \ell_2, \ldots, \ell_p$. Le plus petit entier $k \in \mathbb{N}^*$ tel que $\sigma^k = \mathrm{Id}$ est donc le plus petit commun multiple des ℓ_j. On peut énoncer :

1.4.1. Théorème. *Pour trouver l'ordre d'une permutation σ, on cherche une décomposition en cycles, et alors l'ordre*

$$\operatorname{ordre}(\sigma) = \operatorname{ppcm}(\ell_1, \ell_2, \ldots, \ell_p)$$

est le ppcm des longueurs des cycles $c_1, c_2, \ldots, c_p$ à supports disjoints qui composent σ.

On trouve ainsi par exemple

$$\operatorname{ordre}((1\ 6\ 2) \circ (3\ 7) \circ (4\ 8)) = \operatorname{ppcm}(3, 2, 2) = 6.$$

2. Signature d'une permutation

2.1. Nombre d'inversions et signature

On désigne par P_n l'ensembles des paires $\{i, j\}$ (non ordonnées, $i \neq j$) d'éléments de $\{1, 2, \ldots, n\}$. On a

$$\operatorname{card} P_n = \binom{n}{2} = \frac{n(n-1)}{2}.$$

Si $\sigma \in \mathfrak{S}_n$, alors σ induit une application $\widehat{\sigma} : P_n \to P_n$ définie par

$$\widehat{\sigma}(\{i, j\}) = \{\sigma(i), \sigma(j)\},$$

et il est clair que c'est une bijection de P_n dans P_n, d'inverse $\widehat{\sigma^{-1}}$. On dit que la paire $\{i, j\}$ est inversée par σ (resp. non inversée) si

$$\frac{\sigma(j) - \sigma(i)}{j - 1} < 0, \quad \text{resp.} \quad \frac{\sigma(j) - \sigma(i)}{j - 1} > 0,$$

autrement dit, si $\sigma(i), \sigma(j)$ sont en ordre inverse (ou non) de i, j.

2.1.1. Définition. *Le nombre d'inversions d'une permutation $\sigma \in \mathfrak{S}_n$ est, comme son nom l'indique, le nombre de paires $\{i,j\}$ inversées par σ :*

$$N(\sigma) = \mathrm{card}\Big\{\{i,j\} \in P_n \,/\, \frac{\sigma(j)-\sigma(i)}{j-i} < 0\Big\}.$$

On a donc $N(\sigma) \in \{0, 1, \ldots, \frac{n(n-1)}{2}\}$. La signature $\varepsilon(\sigma)$ de la permutation σ est la valeur ± 1 définie par

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

2.1.2. Examples.

(a) L'application identique $\sigma = \mathrm{Id}$ n'a pas d'inversions, par conséquent $N(\mathrm{Id}) = 0$, $\varepsilon(\mathrm{Id}) = +1$.

(b) La transposition $\tau_{a,b}$ (avec disons $a < b$) s'écrit

$$\tau_{a,b} = \begin{bmatrix} 1 & 2 & \ldots & a-1 & a & a+1 & \ldots & b-1 & b & b+1 & \ldots n \\ 1 & 2 & \ldots & a-1 & b & a+1 & \ldots & b-1 & a & b+1 & \ldots n \end{bmatrix}$$

donne lieu aux paires inversées $\{a,b\}$ et

$$\{a,i\} \mapsto \{b,i\}, \quad a+1 \leqslant i \leqslant b-1,$$
$$\{i,b\} \mapsto \{i,a\}, \quad a+1 \leqslant i \leqslant b-1,$$

soit $2p+1$ paires inversées avec $p = (b-1)-(a+1)+1 = b-a-1$. On a donc $\varepsilon(\tau_{a,b}) = -1$.

(c) Le cycle $c = (1\ 2\ \cdots\ \ell)$ de longueur ℓ

$$c = \begin{bmatrix} 1 & 2 & \ldots & \ell-1 & \ell & \ell+1 & \ldots & n \\ 2 & 3 & \ldots & \ell & 1 & \ell+1 & \ldots & n \end{bmatrix}$$

donne lieu aux paires inversées $\{i,\ell\} \mapsto \{i+1, 1\}$ pour $1 \leqslant i \leqslant \ell-1$. On obtient par conséquent

$$N(c) = \ell - 1, \quad \varepsilon(c) = (-1)^{\ell-1}.$$

(d) La permutation σ correspondant au renversement de l'ordre

$$c = \begin{bmatrix} 1 & 2 & \ldots & n-1 & n \\ n & n-1 & \ldots & 2 & 1 \end{bmatrix}$$

admet le nombre maximum $N(\sigma) = \frac{n(n-1)}{2}$ d'inversions, et on a par conséquent $\varepsilon(\sigma) = (-1)^{n(n-1)/2}$.

On a la formule importante suivante

2.1.3. Formule de la signature. *Pour tout $\sigma \in \mathfrak{S}_n$, on a*

$$\varepsilon(\sigma) = \prod_{\{i,j\}\in P_n} \frac{\sigma(j)-\sigma(i)}{j-i}.$$

Démonstration. Posons

$$\widetilde{\varepsilon}(\sigma) = \prod_{\{i,j\}\in P_n} \frac{\sigma(j)-\sigma(i)}{j-i} \in \mathbb{Q}^*.$$

Il est clair que le signe de $\widetilde{\varepsilon}(\sigma)$ est $(-1)^{N(\sigma)}$. Mais si on fait le changement de variable bijectif $\{u,v\} = \widehat{\sigma}(\{i,j\}) = \{\sigma(i),\sigma(j)\}$, on voit que le numérateur et le démoninateur de $\widetilde{\varepsilon}(\sigma)$ sont tous les deux égaux en valeur absolue à

$$\prod_{\{u,v\}\in P_n} |v-u| = \prod_{2\leqslant v\leqslant n} \prod_{1\leqslant u\leqslant v-1} (v-u) = \prod_{2\leqslant v\leqslant n} (v-1)! = \prod_{1\leqslant i\leqslant n-1} i! = \prod_{i=1}^{n-1} i^{n-i}.$$

Il en résulte que $|\widetilde{\varepsilon}(\sigma)| = 1$ et donc $\widetilde{\varepsilon}(\sigma) = \varepsilon(\sigma)$. □

2.2. Propriété d'homomorphisme de la signature

On va voir que $\varepsilon : \mathfrak{S}_n \to \{+1,-1\}$ est un homomorphisme du groupe $(\mathfrak{S}_n, \circ)$ dans le groupe multiplicatif $(\{+1,-1\}, \times)$, autrement dit :

2.2.1. Théorème. *Pour toutes permutations $\sigma, \tau \in \mathfrak{S}_n$, on a*

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

Rappelons qu'un homomorphisme $\varphi : G \to H$ entre deux groupes $(G,*)$, $(H,*')$ est une application telle que, pour tous $x, y \in G$, on ait $\varphi(x*y) = \varphi(x) *' \varphi(y)$. Dans ce cas

$$\operatorname{Ker}\varphi = \{x\in G \,/\, \varphi(x) = 1_H\}, \quad \operatorname{Im}\varphi = \{u = \varphi(x) \in H \,/\, x\in G\}$$

sont des sous-groupes de G et H respectivement.

Démonstration. Pour toutes permutations $\sigma, \tau \in \mathfrak{S}_n$, il vient

$$\varepsilon(\sigma\circ\tau) = \prod_{\{i,j\}\in P_n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} = \prod_{\{i,j\}\in P_n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \prod_{\{i,j\}\in P_n} \frac{\tau(j)-\tau(i)}{j-i}.$$

Dans le premier produit du membre de droite, faisons le changement de variable bijectif $\{u,v\} = \widehat{\tau}(\{i,j\}) = \{\tau(i),\tau(j)\}$. Ceci donne

$$\prod_{\{i,j\}\in P_n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} = \prod_{\{u,v\}\in P_n} \frac{\sigma(v)-\sigma(u)}{v-u}.$$

Par conséquent

$$\varepsilon(\sigma\circ\tau)=\prod_{\{u,v\}\in P_n}\frac{\sigma(v)-\sigma(u)}{v-u}\prod_{\{i,j\}\in P_n}\frac{\tau(j)-\tau(i)}{j-i}=\varepsilon(\sigma)\varepsilon(\tau).\qquad\square$$

2.2.2. Corollaire. *Soit $A=\{a_1,\ldots,a_n\}$ un ensemble fini. Une permutation $\sigma\in\mathfrak{S}_A$ est définie à l'aide d'une permutation $\alpha\in\mathfrak{S}_n$ par la correspondance bijective*

$$\alpha\in\mathfrak{S}_n\longmapsto\sigma\in\mathfrak{S}_A,\quad \sigma(a_i)=a_{\alpha(i)}.$$

Alors la signature de σ définie par $\varepsilon(\sigma):=\varepsilon(\alpha)$ ne dépend pas de la numérotation des éléments de A, autrement dit, si $A=\{a'_1,\ldots,a'_n\}$ avec une autre numérotation des éléments, et si $\beta\in\mathfrak{S}_n$ est telle que $\sigma(a'_i)=a'_{\beta(i)}$, on a bien $\varepsilon(\alpha)=\varepsilon(\beta)$.

Démonstration. Le changement de numérotation est donné par $a'_i=a_{\gamma(i)}$ avec une certaine permutation $\gamma\in\mathfrak{S}_n$. Posant $j=\gamma(i)$ et $i=\gamma^{-1}(j)$, il vient $a'_{\gamma^{-1}(j)}=a_j$, donc

$$\sigma(a'_i)=\sigma(a_{\gamma(i)})=a_{\alpha(\gamma(i)}=a'_{\gamma^{-1}(\alpha(\gamma(i)))}=a'_{\beta(i)},$$

ce qui montre que les permutations $\alpha,\beta\in\mathfrak{S}_n$ sont liées par $\beta=\gamma^{-1}\circ\alpha\circ\gamma$. Mais on a alors

$$\varepsilon(\beta)=\varepsilon(\gamma)^{-1}\varepsilon(\alpha)\varepsilon(\gamma)=\varepsilon(\alpha).\qquad\square$$

2.2.3. Corollaire. *Pour tout ensemble fini A, il existe un homomorphisme signature $\varepsilon:\mathfrak{S}_A\to\{+1,-1\}$ défini indépendamment de la numérotation des éléments.*

2.3. Calcul de la signature d'une permutation quelconque

2.3.1. Proposition. *Si $c=(a_1\,a_2\ldots a_\ell)$ est un cycle de longueur ℓ dans un ensemble fini A, alors $\varepsilon(c)=(-1)^{\ell-1}$.*

Démonstration. Il suffit de numéroter les éléments en sorte que $a_1,a_2,\ldots,a_\ell$ soient précisément les ℓ premiers éléments de A, et d'observer que le nombre d'inversions de $(1\ 2\ \ldots\ \ell)$ est alors exactement $\ell-1$ (on applique ici le corollaire 2.2.3). $\square$

2.3.2. Corollaire. *Pour une permutation $\sigma\in\mathfrak{S}_A$ décomposée comme*

$$\sigma=c_1\circ c_2\circ\ldots\circ c_p$$

avec des cycles c_j à supports disjoints de longueurs respectives $\ell_1,\ell_2,\ldots,\ell_p$, on a

$$\varepsilon(\sigma)=(-1)^{(\ell_1-1)+(\ell_2-1)+\cdots+(\ell_p-1)}.$$

On observera qu'il est algorithmiquement beaucoup plus efficace de calculer la signature à l'aide d'une décomposition en cycles qu'en examinant les inversions

de toutes les paires $\{i,j\} \in P_n$. En effet, dans le premier cas, on fait un nombre d'opérations d'un ordre de grandeur égal à n, alors que dans le deuxième cas, c'est de l'ordre de $\frac{n(n-1)}{2} \sim \frac{1}{2}n^2$.

2.3.3. Remarque. Pour $\{a_1, a_2, \dots, a_\ell\} \subset \{1, 2, , \dots, n\}$, une façon équivalente de démontrer la proposition 2.3.1 est d'observer que le cycle $c = (a_1\, a_2 \dots a_\ell)$ est le conjugué du cycle $c_\ell = (1\ 2\ \dots\ \ell)$ par la permutation

$$\gamma = \begin{bmatrix} 1 & 2 & \dots & \ell & \ell+1 & \dots & n \\ a_1 & a_2 & \dots & a_\ell & b_1 & \dots & b_{n-\ell} \end{bmatrix}$$

où $\{b_1, \dots, b_{n-\ell}\}$ est le complémentaire de $\{a_1\, a_2 \dots a_\ell\}$ dans $\{1, 2, \dots, n\}$, c'est-à-dire que $c = \gamma \circ c_\ell \circ \gamma^{-1}$ (exercice !)
Plus généralement, on voit facilement que deux permutations $\sigma, \sigma' \in \mathfrak{S}_n$ sont conjuguées, i.e. $\sigma' = \gamma \circ \sigma \circ \gamma^{-1}$ pour un certain élément $\gamma \in \mathfrak{S}_n$, si et seulement si elles ont des décompositions en cycles disjoints

$$\sigma = c_1 \circ c_2 \circ \dots \circ c_p, \quad \sigma' = c'_1 \circ c'_2 \circ \dots \circ c'_p$$

formées du même nombre p de cycles, avec des longueurs identiques $\ell'_j = \ell_j$ (après avoir éventuellement réordonné les composées). Il suffit pour cela de prendre γ qui envoie $\operatorname{Supp} c_j$ sur $\operatorname{Supp} c'_j$ en respectant l'ordre cyclique des éléments dans ces cycles, et qui envoie $\{1, 2, \dots, n\} \smallsetminus \bigcup \operatorname{Supp} c_j$ bijectivement sur $\{1, 2, \dots, n\} \smallsetminus \bigcup \operatorname{Supp} c'_j$.

2.4. Le sous-groupe alterné $\mathcal{A}_n$

2.4.1. Définition. *On pose*

$$\mathcal{A}_n = \ker \varepsilon = \{\sigma \in \mathfrak{S}_n \,/\, \varepsilon(\sigma) = +1\}.$$

C'est un sous-groupe de $\mathfrak{S}_n$.

2.4.2. Proposition. *On a* $\mathcal{A}_1 = \mathfrak{S}_1 = \{\mathrm{Id}\}$, *et pour* $n \geqslant 2$, $\operatorname{card} \mathcal{A}_n = \frac{1}{2}n!$.

Démonstration. Posons

$$\mathfrak{S}_n^+ = \{\sigma \in \mathfrak{S}_n \,/\, \varepsilon(\sigma) = +1\} = \mathcal{A}_n, \quad \mathfrak{S}_n^- = \{\sigma \in \mathfrak{S}_n \,/\, \varepsilon(\sigma) = -1\}.$$

Alors on a la réunion disjointe $\mathfrak{S}_n = \mathfrak{S}_n^+ \cup \mathfrak{S}_n^-$, et pour $n \geqslant 2$, on a une bijection

$$\mathfrak{S}_n^+ \longrightarrow \mathfrak{S}_n^-, \quad \sigma \longmapsto \sigma \circ \tau_{1,2}.$$

Par conséquent $\operatorname{card} \mathfrak{S}_n^+ = \operatorname{card} \mathfrak{S}_n^- = \operatorname{card} \mathcal{A}_n = \frac{1}{2}n!$. □

2.4.3. Complément historique. Pour $n \geqslant 5$, on peut démontrer que $\mathcal{A}_n$ est un groupe simple, c'est-à-dire que $\mathcal{A}_n$ n'a aucun sous-groupe distingué H autre

que $H = \{\mathrm{Id}\}$ et $H = \mathcal{A}_n$ (un sous-groupe distingué H d'un groupe G est un sous-groupe invariant par conjugaison : $\forall \gamma \in G$, $\gamma H \gamma^{-1} = H$) ; d'autre part, $\mathcal{A}_n$ est non commutatif si $n \geqslant 5$. Vers 1830, Évariste Galois a déduit de ce résultat que les racines complexes $z_1, \ldots, z_n$ d'un polynôme général $P \in \mathbb{Q}[X]$ de degré n ne peuvent s'exprimer par radicaux à partir de $\mathbb{Q}$, à savoir comme combinaisons de racines p-ièmes "enchevêtrées" en partant des rationnels – c'était une question ouverte depuis la découverte des formules de résolution des équations de degré 3 et 4 par Tartaglia et Ferrari au 16$^{\mathrm{e}}$ siècle. On vérifie en effet que le corps $\mathbb{K} = \mathbb{Q}[z_1, \ldots, z_n]$ engendré par les racines de P admet un groupe d'automorphismes $\mathrm{Aut}(\mathbb{K})$ de permutation des racines égal à $\mathfrak{S}_n$ si P est général. Or, $\mathfrak{S}_n$ ne peut se "dévisser" à l'aide de groupes abéliens, alors que ce serait le cas pour $\mathrm{Aut}(\mathbb{K})$ si les racines étaient résolubles par radicaux. É. Galois a découvert ces résultats alors qu'il avait à peine 20 ans, et les a consignés fébrilement dans un testament écrit à la veille de son duel. Ils sont restés incompris de la communauté mathématique pendant au moins 20 ans. C'est d'ailleurs à cette occasion qu'il a introduit la notion fondamentale de groupe !

3. Générateurs du groupe des permutations

3.1. Génération par transpositions

3.1.1. Théorème. *Toute permutation $\sigma \in \mathfrak{S}_n$ s'écrit comme un produit d'au plus $\frac{n(n-1)}{2}$ transpositions $\tau_{i,i+1}$ portant sur des éléments consécutifs, $1 \leqslant i \leqslant n-1$, c'est-à-dire*

$$\sigma = \tau_{i_1,i_1+1} \circ \tau_{i_2,i_2+1} \circ \cdots \circ \tau_{i_k,i_k+1}, \quad k \leqslant \frac{n(n-1)}{2}.$$

Démonstration. On raisonne par récurrence sur $N(\sigma)$. Pour $N(\sigma) = 0$, on a $\sigma = \mathrm{Id}$, et le résutat est vrai avec $k = 0$ (produit vide, égal à Id par convention).

Supposons maintenant que $N = N(\sigma) \geqslant 1$ et que le résultat ait déjà été démontré pour les permutations σ' telles que $N(\sigma') = N - 1$. Il existe alors $j \in \{1, 2, \ldots, n-1\}$ tel que $\sigma(j) > \sigma(j+1)$, sinon σ serait strictement croissante (donc $\sigma = \mathrm{Id}$ et $N(\sigma) = 0$ contrairement à notre hypothèse). Posons

$$\begin{aligned}\sigma' &= \sigma \circ \tau_{j,j+1} \\ &= \begin{bmatrix} 1 & 2 & \ldots & j-1 & j & j+1 & j+2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(j-1) & \sigma(j+1) & \sigma(j) & \sigma(j+2) & \ldots & \sigma(n) \end{bmatrix}.\end{aligned}$$

Alors l'inversion $\sigma(j+1) < \sigma(j)$ n'est plus une inversion pour σ'. On a donc $N(\sigma') = N(\sigma) - 1 = N - 1$, et par hypothèse de récurrence, il existe une décomposition

$$\sigma' = \tau_{i_1,i_1+1} \circ \tau_{i_2,i_2+1} \circ \cdots \circ \tau_{i_\ell,i_\ell+1},$$

d'où

$$\sigma = \sigma' \circ \tau_{j,j+1} = \tau_{i_1,i_1+1} \circ \tau_{i_2,i_2+1} \circ \cdots \circ \tau_{i_\ell,i_\ell+1} \circ \tau_{j,j+1}.$$

Par récurrence, ce raisonnement fournit une décomposition ayant exactement $k = N(\sigma)$ transpositions $\tau_{i,i+1}$, de sorte que $k \leqslant \frac{N(N-1)}{2}$. □

3.1.2. Corollaire. *En particulier, toute permutation $\sigma \in \mathfrak{S}_n$ est une composée*

$$\sigma = \tau_{a_1,b_1} \circ \tau_{a_2,b_2} \circ \cdots \circ \tau_{a_k,b_k}$$

de transpositions, et la signature $\varepsilon(\sigma) = (-1)^k$ est déterminée par la parité du nombre de transpositions nécessaires (et inversement).

3.2. Génération par une transposition et un cycle

Si $c = (1\ 2\ \ldots\ n)$ est le cycle $1 \mapsto 2 \mapsto \cdots \mapsto (n-1) \mapsto n \mapsto 1$ de longueur n, on a $c^{j-1}(i) = i + j - 1$ modulo n, et on voit facilement que

$$\tau_{j,j+1} = c^{j-1} \circ \tau_{1,2} \circ c^{-(j-1)}$$

puisque $c^{-(j-1)}$ "ramène" $\{j, j+1\}$ sur $\{1, 2\}$, tandis que c^{j-1} "renvoie" $\{2, 1\}$ sur $\{j+1, j\}$. Ceci montre que les transpositions $\tau_{j,j+1}$ sont toutes conjuguées de $\tau_{1,2}$ par des puissances de c. Le théorème 3.1.1 implique alors

3.2.1. Théorème. *Le groupe $\mathfrak{S}_n$ est engendré par le cycle $c = (1\ 2\ \ldots\ n)$ et la permutation $\tau = \tau_{1,2}$, c'est-à-dire que toute permutation σ peut s'écrire comme une composée (non commutative) de τ et de puissances c^i entremêlées :*

$$\sigma = c^{j_0} \circ \tau \circ c^{j_1} \circ \tau \circ \cdots \circ c^{j_{k-1}} \circ \tau \circ c^{j_k}, \qquad 0 \leqslant j_\ell \leqslant n-1.$$

3.2.2. Exercice. On peut démontrer que pour $n \geqslant 3$ le groupe alterné $\mathcal{A}_n$ est engendré par les cycles $(a_1\ a_2\ a_3)$ de longueur 3. Exercice pour le lecteur !