Groupes symétriques

François DE MARÇAY
Département de Mathématiques d'Orsay
Université Paris-Saclay, France

1. Introduction

Ce chapitre est consacré à l'étude de certains groupes *non* commutatifs très naturels, dits *groupes symétriques*, qui interviennent partout dans la vie mathématique, ainsi que dans la vie non mathématique — y compris en physique.

Par exemple, l'adolescent blême qui au petit matin dans les frimas d'un jour brumeux d'automne, secoue le panier des noix sonores et noires qu'il vient de ramasser sous le noyer géant de son enfance, fait agir, sans le savoir, ce fameux *groupe symétrique*.

Car les mathématiques existent partout et depuis toujours, sous le ciel noir constellé d'étoiles et de galaxies, depuis l'enfance de l'univers.

2. Définitions et premières propriétés du groupe symétrique

Soit un ensemble *fini*, c'est-à-dire de cardinal $|E| < \infty$.

Définition 2.1. La collection des *bijections* de E dans lui-même :

$$\mathfrak{S}(E) := \big\{\sigma\colon\ E \longrightarrow E \text{ bijective}\big\},$$

qui est un *groupe* pour la loi de composition $* = \circ$ des applications bijectives, est appelée *groupe des permutations de* E, ou *groupe symétrique sur* E.

Un élément de $\mathfrak{S}(E)$ est appelé une *permutation* de E.

L'exemple canonique d'ensemble de cardinal fini quelconque est l'ensemble :

$$\big\{1,\, 2,\, 3,\, \ldots,\, n\big\},$$

des n premiers entiers naturels. Au lieu de $\mathfrak{S}\big(\{1,\ldots,n\}\big)$, on note alors :

$$\mathfrak{S}_n := \Big\{\sigma\colon\ \{1,\ldots,n\} \longrightarrow \{1,\ldots,n\} \text{ bijective}\Big\}.$$

Une permutation $\sigma \in \mathfrak{S}_n$ sera notée :

$$\sigma \quad \begin{array}{cccc} 1 & 2 & \cdots & n \\ \downarrow & \downarrow & \cdots & \downarrow \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{array} \qquad \text{ou} \qquad \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}.$$

Par exemple :

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

Tout au long des paragraphes qui suivront, nous continuerons à analyser ce même exemple, dont les caractéristiques heuristiques se dévoileront à nous de manière de plus en plus *séduisante*.

Proposition 2.2. *Si deux ensembles finis $E \overset{\sim}{\longleftrightarrow} E'$ sont en bijection, alors leurs groupes de permutations sont isomorphes :*

$$\mathfrak{S}(E) \;\cong\; \mathfrak{S}(E').$$

Démonstration. Supposons donc l'existence d'une bijection $f\colon E \longrightarrow E'$, de bijection inverse $E \longleftarrow E' : f^{-1}$, et dressons un diagramme de composition :

$$\begin{array}{ccc} E & \xrightarrow{\;\sigma\;} & E \\ {\scriptstyle f^{-1}}\uparrow & & \downarrow{\scriptstyle f} \\ E' & \xrightarrow[f\circ\sigma\circ f^{-1}]{} & E'. \end{array}$$

En s'aidant de ce diagramme, on vérifie alors que l'application :

$$\begin{array}{ccc} \mathfrak{S}(E) & \longrightarrow & \mathfrak{S}(E') \\ \sigma & \longmapsto & f\circ\sigma\circ f^{-1} \;=:\; \sigma', \end{array}$$

est un *isomorphisme* de groupes.

Les détails sont laissés au lecteur-étudiant [1] notamment la vérification du fait que l'isomorphisme inverse s'écrit :

$$f^{-1}\circ\sigma'\circ f \;\longleftarrow\!\shortmid\; \sigma'. \qquad \square$$

Toujours avec E de cardinal fini, considérons le cas particulier simple et concret où $E' := \{1,\dots,n\}$, avec $n := |E|$. Une bijection f^{-1} de $\{1,\dots,n\}$ à valeurs dans E s'identifie alors à une *numérotation* des n éléments de E :

$$\begin{array}{rcll} E & \longleftarrow & \{1,\dots,n\} & : f^{-1} \\ a_i \;:=\; f^{-1}(i) & \longleftarrow\!\shortmid & i, & \end{array}$$

que l'on note alors $\{a_1,\dots,a_n\} = E$.

Par conséquent, l'isomorphisme (inverse) de groupes de la Proposition 2.2 s'écrit :

$$\begin{array}{ccc} \mathfrak{S}(E) & \overset{\sim}{\longleftarrow} & \mathfrak{S}_n \\ f^{-1}\circ\tau\circ f & \longleftarrow\!\shortmid & \tau. \end{array}$$

Enfin, si $\tau \in \mathfrak{S}_n$ est une permutation quelconque, on voit que :

$$f^{-1}\big(\tau(f(a_i))\big) \;=\; f^{-1}\big(\tau(i)\big) \;=\; a_{\tau(i)},$$

ce qui signifie qu'après avoir effectué une numérotation des éléments de E, en éliminant les symboles de numérotation f^{-1} et f, la permutation considérée s'exprime tout simplement au niveau des indices, comme un changement de la place des noix dans notre panier :

$$\big(a_1,\, a_2,\, \dots,\, a_n\big) \;\longmapsto\; \big(a_{\tau(1)},\, a_{\tau(2)},\, \dots,\, a_{\tau(n)}\big).$$

1. En fait, voici « les » détails :

$$\big(f\circ\sigma_1\circ f^{-1}\big)\circ\big(f\circ\sigma_2\circ f^{-1}\big) \;=\; f\circ\sigma_1\circ\sigma_2\circ f^{-1}.$$

Ainsi, l'objectif de ce chapitre est d'étudier les groupes $\mathfrak{S}(E)$, lorsque $|E| < \infty$. Au vu de ces considérations, on peut se restreindre à l'étude du groupe $\mathfrak{S}_n$, ce que nous ferons parfois, mais pas toujours. Rappelons et re-démontrons le

Théorème 2.3. *Si E est un ensemble fini à $n \geqslant 1$ éléments, alors $\mathfrak{S}(E)$ est un groupe fini d'ordre (de cardinal) égal à la factorielle $n!$*

Démonstration. Donc on suppose $E = \{1, \ldots, n\}$. Il s'agit de compter combien de permutations de cet ensemble $\{1, \ldots, n\}$ sont possibles.

Or se donner une permutation de $\{1, \ldots, n\}$ revient à se donner n entiers $\tau(1), \ldots, \tau(n)$ distincts deux à deux et tous contenus dans $\{1, \ldots, n\}$.

Donc au début, il y a n choix possibles pour $\tau(1)$. Une fois $\tau(1)$ choisi, il n'y a plus que $n-1$ choix possibles pour $\tau(2)$, puis $n-2$ choix possibles pour $\tau(3)$, et ainsi de suite, jusqu'à ce qu'il n'y ait plus qu'un seul choix possible pour $\tau(n)$.

Au total, il y a donc précisément :

$$n\,(n-1)\,(n-2)\,\cdots\,1 \;=\; n!,$$

permutations possibles de l'ensemble $\{1, \ldots, n\}$. □

Rappelons aussi que le groupe $\mathfrak{S}_n$ n'est *jamais* commutatif dès que $n \geqslant 3$ — c'est-à-dire la plupart du temps !

En effet, dans le chapitre précédent, nous avons exhibé les deux petites babioles suivantes qui ne commutent pas entre elles :

$$\begin{array}{cccc} & 1 & 2 & 3 \\ \tau & \downarrow & \downarrow & \downarrow \\ & 1 & 3 & 2 \\ \sigma & \downarrow & \downarrow & \downarrow \\ & 2 & 3 & 1 \end{array} \qquad \text{diffère de} \qquad \begin{array}{cccc} & 1 & 2 & 3 \\ \sigma & \downarrow & \downarrow & \downarrow \\ & 2 & 1 & 3 \\ \tau & \downarrow & \downarrow & \downarrow \\ & 3 & 1 & 2 \end{array} .$$

Comme précédemment, on travaille avec un ensemble E fini.

Définition 2.4. L'ensemble des *points fixes* d'une permutation $\sigma \in \mathfrak{S}(E)$ est :

$$\mathsf{Fix}\,\sigma \;:=\; \big\{a \in E\colon\ \sigma(a) = a\big\},$$

tandis que le *support* de σ est l'ensemble des éléments de E qui sont réellement déplacés par σ :

$$\mathsf{Supp}\,\sigma \;:=\; \big\{a \in E\colon\ \sigma(a) \neq a\big\}.$$

Ainsi, l'ensemble total E se décompose comme réunion *disjointe :*

$$E \;=\; \mathsf{Fix}\,\sigma \cup \mathsf{Supp}\,\sigma.$$

Il est clair que $\sigma = \mathsf{Id}$ est l'identité si et seulement si $\mathsf{Fix}\,\sigma = E$, si et seulement si $\mathsf{Supp}\,\sigma = \emptyset$.

Pour la permutation :

$$\sigma \;:=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix},$$

on a :

$$\begin{aligned} \mathsf{Fix}\,\sigma \;&=\; \big\{2,\,6\big\}, \\ \mathsf{Supp}\,\sigma \;&=\; \big\{1,\,3,\,4,\,5,\,7,\,8,\,9\big\}. \end{aligned}$$

L'énoncé technique suivant présente quelques propriétés fondamentales qui seront souvent utilisées ultérieurement.

Proposition 2.5. *Soit E un ensemble fini.*

(1) *Pour toute permutation $\sigma \in \mathfrak{S}(E)$, on a les* égalités :

$$\begin{aligned} \sigma\big(\mathsf{Fix}\,\sigma\big) &= \mathsf{Fix}\,\sigma, \\ \sigma\big(\mathsf{Supp}\,\sigma\big) &= \mathsf{Supp}\,\sigma. \end{aligned}$$

(2) *Pour toute permutation $\sigma \in \mathfrak{S}(E)$, on a les* égalités :

$$\begin{aligned} \mathsf{Fix}\,\sigma &= \mathsf{Fix}\,\sigma^{-1}, \\ \mathsf{Supp}\,\sigma &= \mathsf{Supp}\,\sigma^{-1}. \end{aligned}$$

(3) *Pour toute $\sigma \in \mathfrak{S}(E)$ et tout entier $m \in \mathbb{Z}$, on a les* inclusions :

$$\begin{aligned} \mathsf{Fix}\,\sigma &\subset \mathsf{Fix}\,\sigma^{m}, \\ \mathsf{Supp}\,\sigma &\supset \mathsf{Supp}\,\sigma^{m}. \end{aligned}$$

(4) *Pour $\sigma, \sigma' \in \mathfrak{S}(E)$, on a les* inclusions :

$$\begin{aligned} \mathsf{Fix}\,\sigma \circ \sigma' &\supset \mathsf{Fix}\,\sigma \cap \mathsf{Fix}\,\sigma', \\ \mathsf{Supp}\,\sigma \circ \sigma' &\subset \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'. \end{aligned}$$

(5) *Si de plus σ et σ' sont à supports disjoints, on a les* égalités :

$$\begin{aligned} \mathsf{Fix}\,\sigma \circ \sigma' &= \mathsf{Fix}\,\sigma \cap \mathsf{Fix}\,\sigma', \\ \mathsf{Supp}\,\sigma \circ \sigma' &= \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'. \end{aligned}$$

Le point-clé, c'est que les inclusions de $(\mathbf{3})$ et de $(\mathbf{4})$ ne sont pas forcément des égalités. Notamment, avec $G := \mathfrak{S}(E)$, de cardinal $|G| = n!$, le théorème de Lagrange vu au chapitre précédent donne, pour toute permutation $\sigma \in \mathfrak{S}(E)$:

$$\sigma^{|\mathfrak{S}(E)|} = \sigma^{n!} = \mathsf{Id},$$

de telle sorte que :

$$\mathsf{Fix}\big(\sigma^{|E|!}\big) = \mathsf{Fix}\,\mathsf{Id} = E.$$

En première lecture, nous conseillons de « sauter » la

Démonstration. **(1)** Pour tout $a \in E$, en appliquant $\sigma^{-1}(\bullet)$ et $\sigma(\bullet)$, on constate que :

$$\begin{aligned} \sigma\big(\mathsf{Fix}\,\sigma\big) \ni a \quad &\Longleftrightarrow \quad \mathsf{Fix}\,\sigma \ni \sigma^{-1}(a) \\ &\Longleftrightarrow \quad \sigma\big(\sigma^{-1}(a)\big) = \sigma^{-1}(a) \\ &\Longleftrightarrow \quad a = \sigma^{-1}(a) \\ &\Longleftrightarrow \quad \sigma(a) = a \\ &\Longleftrightarrow \quad \mathsf{Fix}\,\sigma \ni a. \end{aligned}$$

Pareillement :

$$\begin{aligned}\sigma\big(\mathsf{Supp}\,\sigma\big)\ \ni\ a \quad &\Longleftrightarrow \quad \mathsf{Supp}\,\sigma\ \ni\ \sigma^{-1}(a)\\ &\Longleftrightarrow \quad \sigma\big(\sigma^{-1}(a)\big)\ \neq\ \sigma^{-1}(a)\\ &\Longleftrightarrow \quad a\ \neq\ \sigma^{-1}(a)\\ &\Longleftrightarrow \quad \sigma(a)\ \neq\ a\\ &\Longleftrightarrow \quad \mathsf{Supp}\,\sigma\ \ni\ a.\end{aligned}$$

(2) Pour tout $a \in E$, en appliquant aussi $\sigma^{-1}(\bullet)$ et $\sigma(\bullet)$, on constate de même que :

$$\begin{aligned}\sigma(a)\ =\ a \quad &\Longleftrightarrow \quad a\ =\ \sigma^{-1}(a),\\ \sigma(a)\ \neq\ a \quad &\Longleftrightarrow \quad a\ \neq\ \sigma^{-1}(a).\end{aligned}$$

(3) Pour tout $a \in E$, on a :

$$\sigma(a)\ =\ a \quad \Longrightarrow \quad \sigma\big(\sigma(a)\big)\ =\ \sigma(a)\ =\ a \quad \Longrightarrow \quad \sigma^3(a)\ =\ a \quad \Longrightarrow \quad \cdots,$$

puis par récurrence pour tout entier $m \geqslant 1$:

$$\sigma^m(a)\ =\ a,$$

d'où aussi $a = \sigma^{-m}(a)$ en appliquant $\sigma^{-m}(\bullet)$ à cette égalité. Ainsi, on a bien :

$$\mathsf{Fix}\,\sigma\ \subset\ \mathsf{Fix}\,\sigma^m \qquad (\forall\, m \in \mathbb{Z}).$$

En passant au complémentaire [2], nous obtenons la deuxième inclusion annoncée :

$$\mathsf{Supp}\,\sigma\ =\ E\big\backslash\mathsf{Fix}\,\sigma\ \supset\ E\big\backslash\mathsf{Fix}\sigma^m\ =\ \mathsf{Supp}\,\sigma^m,$$

(4) Soit $a \in E$ avec $\sigma(a) = a = \sigma'(a)$. Alors :

$$\sigma\circ\sigma'(a)\ =\ \sigma\big(\sigma'(a)\big)\ =\ \sigma(a)\ =\ a,$$

ce qui justifie la première inclusion. La deuxième inclusion s'obtient en passant au complémentaire [3].

(5) Supposons maintenant que $\mathsf{Supp}\,\sigma \cap \mathsf{Supp}\,\sigma' = \emptyset$. Pour un élément dans la réunion de ces deux supports disjoints $a \in \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'$, on a *ou bien* $a \in \mathsf{Supp}\,\sigma$, *ou bien* $a \in \mathsf{Supp}\,\sigma'$.

Pour fixer les idées, supposons $a \in \mathsf{Supp}\,\sigma$, c'est-à-dire $\sigma(a) \neq a$. Comme $a \notin \mathsf{Supp}\,\sigma'$, c'est-à-dire $\sigma'(a) = a$, il vient :

$$\sigma\big(\sigma'(a)\big)\ =\ \sigma(a)\ \neq\ a,$$

ce qui montre que $a \in \mathsf{Supp}\,\sigma\circ\sigma'$.

Le cas $a \in \mathsf{Supp}\,\sigma'$ est similaire. Donc on a obtenu l'inclusion :

$$\mathsf{Supp}\,\sigma\ \cup\mathsf{Supp}\,\sigma'\ \subset\ \mathsf{Supp}\,\sigma\circ\sigma',$$

qui est *inverse* de **(4)**. En conclusion, on a obtenu la deuxième inclusion **(5)**, tandis que la première s'obtient en passant au complémentaire. □

2. Rappelons que pour tous ensembles $G \subset F \subset E$, on a l'inclusion inversée $E\backslash G \supset E\backslash F$.
3. Rappelons que $F \cap G \subset H \subset E$ implique :

$$E\backslash F\ \cup\ E\backslash G\ =\ E\big\backslash(F\cap G)\ \supset\ E\backslash H.$$

Rendez-vous était donc donné ici à l'étudiant qui aura sagement décidé de sauter la lecture de la démonstration. Bien que $\mathfrak{S}(E)$ ne soit jamais commutatif dès que $|E| \geqslant 3$, on a un résultat très important de commutation entre deux permutations sous hypothèse de support (ou de territoire).

Proposition 2.6. *Deux permutations à supports disjoints commutent toujours.*

Démonstration. Soient donc $\sigma, \sigma' \in \mathfrak{S}(E)$ avec $\emptyset = \mathsf{Supp}\,\sigma \cap \mathsf{Supp}\,\sigma'$, et soit $a \in E$ quelconque. Avec la décomposition en sous-ensembles disjoints :

$$E \;=\; \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma' \cup \big(E \big\backslash \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'\big),$$

trois cas se présentent.

Si $a \in \mathsf{Supp}\,\sigma$, alors $\sigma(a) \in \mathsf{Supp}\,\sigma$ aussi grâce à la Proposition 2.5 **(1)**. Par hypothèse, $\sigma(a)$ n'est donc *pas* dans le support de σ', et donc $\sigma'\big(\sigma(a)\big) = \sigma(a) = \sigma\big(\sigma'(a)\big)$ car $a = \sigma'(a)$ puisque $a \notin \mathsf{Supp}\,\sigma'$.

Ensuite, si $a \in \mathsf{Supp}\,\sigma'$, d'où $a \notin \mathsf{Supp}\,\sigma$ par hypothèse, on raisonne de manière symétrique pour obtenir encore la commutation annoncée $\sigma'\big(\sigma(a)\big) = \sigma\big(\sigma'(a)\big)$.

Enfin, si $a \notin \mathsf{Supp}\,\sigma \cup \mathsf{Supp}\,\sigma'$, donc si a est fixé par σ *et* par σ', il vient aisément :

$$\sigma\big(\sigma'(a)\big) \;=\; \sigma(a) \;=\; a \;=\; \sigma'(a) \;=\; \sigma'\big(\sigma(a)\big). \qquad \square$$

3. Orbites d'une permutation $\sigma \in \mathfrak{S}(E)$

Soit toujours un ensemble *fini* E de cardinal $|E| =: n \geqslant 2$. Pour toute permutation $\sigma \in \mathfrak{S}(E)$, c'est-à-dire toute bijection $\sigma\colon E \longrightarrow E$ d'inverse σ^{-1}, rappelons que l'on note $\sigma^0 := \mathsf{Id}$, que l'on note $\sigma^i := \sigma \circ \cdots \circ \sigma$ composée i fois avec elle-même, et enfin, que l'on note aussi $\sigma^{-i} := \sigma^{-1} \circ \cdots \circ \sigma^{-1}$.

Proposition 3.1. *La relation binaire entre éléments $a, b \in E$ définie par :*

$$a \;\sim\; b \qquad \overset{\text{déf}}{\Longleftrightarrow} \qquad \exists\, i \in \mathbb{Z} \quad \sigma^i(a) \;=\; b,$$

est une relation d'équivalence.

Démonstration. Avec $i := 0$, on a $\sigma^0(a) = a$, d'où la réflexivité $a \sim a$.

La symétrie $b \sim a$ provient de :

$$\sigma^{-i}\big(\; \sigma^i(a) \;=\; b \;\big) \qquad \Longrightarrow \qquad a \;=\; \sigma^{-i}(b).$$

Quant à la transitivité, elle est tout aussi facile :

$$\begin{aligned} \Big(\; a \sim b \quad \text{et} \quad b \sim c \;\Big) \qquad &\Longleftrightarrow \qquad \Big(\; \sigma^i(a) = b \quad \text{et} \quad \sigma^j(b) = c \;\Big) \\ &\Longrightarrow \qquad\quad \sigma^j\big(\sigma^i(a)\big) = c \\ &\Longleftrightarrow \qquad\quad \Big(\; a \sim c \;\Big). \end{aligned} \qquad \square$$

Dans notre exemple continué :

$$\sigma \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix},$$

nous avons :

$$\begin{aligned} &1 \sim 4 \sim 5 \sim 8 \sim 1, \\ &2 \sim 2, \\ &3 \sim 7 \sim 9 \sim 3, \\ &6 \sim 6. \end{aligned}$$

D'après les propriétés générales dont jouissent les relations d'équivalence sur des ensembles arbitraires, nous savons que E se partitionne en *classes d'équivalences* associées à une permutation fixée $\sigma \in \mathfrak{S}(E)$. Traditionnellement, on donne un nom à ces classes d'équivalence.

Définition 3.2. Pour $\sigma \in \mathfrak{S}(E)$, la *$\sigma$-orbite* d'un élément quelconque $a \in E$ est la collection de tous les éléments qui sont obtenus en itérant $\sigma(\bullet)$ ainsi que $\sigma^{-1}(\bullet)$ à partir de a :

$$\begin{aligned} \mathsf{Orb}_\sigma(a) &= \big\{b \in E\colon\ b \sim a\big\} \\ &= \big\{\sigma^i(a)\colon\ i \in \mathbb{Z}\big\} \\ &= \Big\{ \ldots,\ \sigma^{-3}(a),\ \sigma^{-2}(a),\ \sigma^{-1}(a),\ a,\ \sigma(a),\ \sigma^2(a),\ \sigma^3(a),\ \ldots \Big\}. \end{aligned}$$

Il est clair qu'une σ-orbite $\mathsf{Orb}_\sigma(a)$ est réduite à un singleton (élément unique) si et seulement si $a = \sigma(a)$ est fixé par σ, car alors $\sigma\big(\sigma(a)\big) = a$, puis $\sigma^3(a) = a$, et ainsi de suite.

Proposition 3.3. *Pour un élément quelconque $a \in E$, on a :*

$$\begin{aligned} a \in \mathsf{Fix}\,\sigma \qquad &\Longleftrightarrow \qquad \big|\mathsf{Orb}_\sigma(a)\big| = 1, \\ a \in \mathsf{Supp}\,\sigma \qquad &\Longleftrightarrow \qquad \big|\mathsf{Orb}_\sigma(a)\big| \geqslant 2. \end{aligned}$$

Démonstration. La première équivalence vient d'être dite. Quant à la seconde, effectivement, elle est équivalente par contraposée à la première. Elle peut aussi être vue directement, car $a \in \mathsf{Supp}\,\sigma$ signifie $a \neq \sigma(a)$, donc $\mathsf{Orb}_\sigma(a)$ contient au moins deux éléments distincts, effectivement. □

Les propriétés générales des classes d'équivalences donnent immédiatement l'énoncé suivant.

Proposition 3.4. *Les orbites d'une permutation $\sigma \in \mathfrak{S}(E)$ satisfont les quatre propriétés suivantes.*

(1) $a \in \mathsf{Orb}_\sigma(a)$, *pour tout* $a \in E$.

(2) *Deux σ-orbites qui s'intersectent sont forcément* égales :

$$\emptyset \neq \mathsf{Orb}_\sigma(a) \cap \mathsf{Orb}_\sigma(b) \qquad \Longrightarrow \qquad \mathsf{Orb}_\sigma(a) = \mathsf{Orb}_\sigma(b).$$

(3) *Deux σ-orbites sont soit égales, soit disjointes :*

$$\mathsf{Orb}_\sigma(a) = \mathsf{Orb}_\sigma(b) \qquad \textit{ou bien} \qquad \mathsf{Orb}_\sigma(a) \cap \mathsf{Orb}_\sigma(b) = \emptyset.$$

(4) *Pour tous $a, b \in E$:*

$$\mathsf{Orb}_\sigma(a) = \mathsf{Orb}_\sigma(b) \qquad \Longleftrightarrow \qquad a \in \mathsf{Orb}_\sigma(b) \qquad \Longleftrightarrow \qquad b \in \mathsf{Orb}_\sigma(a). \qquad \square$$

Maintenant, comment « capturer » une σ-orbite ? C'est tout simple, en faisant défiler de mode tous les éléments :

$$\ldots,\ \sigma^{-5}(a),\ \sigma^{-4}(a),\ \sigma^{-3}(a),\ \sigma^{-2}(a),\ \sigma^{-1}(a),\ a,\ \sigma(a),\ \sigma^2(a),\ \sigma^3(a),\ \sigma^4(a),\ \sigma^5(a),\ \ldots$$

en nombre *infini*, mais tous contenus dans notre ensemble E *fini*.

Or comme E est de cardinal $|E| < \infty$ *fini*, tous ces éléments en nombre *infini* ne peuvent *absolument pas* être *tous* mutuellement distincts — le tapis rouge n'est pas assez long. Donc nécessairement, deux puissances distinctes de σ doivent être égales :

$$\begin{aligned} \exists\, i < j \qquad & \text{avec} \qquad & \sigma^i(a) &= \sigma^j(a), \\ & \text{d'où} \qquad & a &= \sigma^{j-i}(a), \end{aligned}$$

c'est-à-dire que a est *fixé* par une certaine *puissance* de σ.

Pour tout $a \in E$, introduisons alors l'entier :

$$n_a := \mathsf{min}\big\{m \geqslant 1 :\ \sigma^m(a) = a\big\}.$$

Clairement, $\sigma^{k\,n_a}(a) = a$ pour tout entier $k \in \mathbb{Z}$.

Proposition 3.5. *Soit E un ensemble fini, et soit une permutation quelconque $\sigma \in \mathfrak{S}(E)$. Alors pour tout $a \in E$, la σ-orbite de a est :*

$$\mathsf{Orb}_\sigma(a) = \Big\{a,\ \sigma(a),\ \sigma^2(a),\ \ldots,\ \sigma^{n_a-1}(a)\Big\},$$

où ces n_a éléments sont distincts deux à deux.

Preuve. Effectivement, ces éléments doivent être mutuellement distincts, car s'il ne l'étaient pas, à savoir s'il existait deux entiers différents $0 \leqslant i < j \leqslant n_a - 1$ avec $\sigma^i(a) = \sigma^j(a)$, et donc avec :

$$1 \leqslant j - i \leqslant n_a - 1,$$

on déduirait $a = \sigma^{j-i}(a)$, en contradiction flagrante avec la minimalité de $m = n_a$ satisfaisant $a = \sigma^m(a)$. □

L'énoncé suivant était en fait déjà contenu dans la Proposition 3.4 **(4)**, mais nous souhaitons en donner une démonstration explicite.

Proposition 3.6. *Pour tout $b \in \mathsf{Orb}_\sigma(a)$, c'est-à-dire $b = \sigma^\ell(a)$ avec un entier $0 \leqslant \ell \leqslant n_a - 1$, on a aussi :*

$$\begin{aligned} \mathsf{Orb}_\sigma(a) &= \Big\{b,\ \sigma(b),\ \sigma^2(b),\ \ldots,\ \sigma^{n_a-1}(b)\Big\} \\ &= \Big\{b,\ \sigma(b),\ \sigma^2(b),\ \ldots,\ \sigma^{n_b-1}(b)\Big\} = \mathsf{Orb}_\sigma(b). \end{aligned}$$

Autrement dit, pour tout $b \in \mathsf{Orb}_\sigma(a)$, on a :

$$n_a = n_b.$$

Démonstration. Les éléments $\sigma^i(b)$ sont mutuellement distincts, car avec $0 \leqslant i, j \leqslant n_a - 1$, on a :

$$\sigma^i(b) = \sigma^j(b) \qquad \Longleftrightarrow \qquad \sigma^{i+\ell}(a) = \sigma^{j+\ell}(a),$$

d'où en appliquant $\sigma^{-\ell}(\bullet)$:

$$\sigma^i(a) = \sigma^j(a),$$

et enfin, $i = j$ à cause de la Proposition 3.5.

Ainsi, il y a bien $n_a = |\mathsf{Orb}_\sigma(a)|$ éléments distincts parmi b, $\sigma(b)$, …, $\sigma^{n_a-1}(b)$, et donc ces éléments, tous contenus dans $\mathsf{Orb}_\sigma(a)$, « remplissent » bien cette orbite. □

Toujours avec notre exemple récréatif :

$$\sigma \;=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix},$$

puisque :

$$\begin{aligned} 8 \;&=\; \sigma(5) \;=\; \sigma\big(\sigma(4)\big) \;=\; \sigma\big(\sigma\big(\sigma(1)\big)\big), \\ 2 \;&=\; \sigma(2), \\ 9 \;&=\; \sigma(7) \;=\; \sigma\big(\sigma(3)\big), \\ 6 \;&=\; \sigma(6), \end{aligned}$$

nous voyons que :

$$\begin{aligned} \omega_1 \;&:=\; \mathsf{Orb}_\sigma(1) \;=\; \big\{1,\,4,\,5,\,8\big\}, \\ \omega_2 \;&:=\; \mathsf{Orb}_\sigma(2) \;=\; \big\{2\big\}, \\ \omega_3 \;&:=\; \mathsf{Orb}_\sigma(3) \;=\; \big\{3,\,7,\,9\big\}, \\ \omega_4 \;&:=\; \mathsf{Orb}_\sigma(6) \;=\; \big\{6\big\}. \end{aligned}$$

Ensuite, si nous notons $\omega_1, \omega_2, \omega_3, \omega_4$ ces quatre orbites, nous voyons que notre ensemble à neuf éléments en est la réunion *disjointe*, et nous voyons clairement quel est l'ensemble des points fixes de σ, ainsi que son support :

$$\begin{aligned} \big\{1, \ldots, 9\big\} \;&=\; \omega_1 \cup \omega_2 \cup \omega_3 \cup \omega_4, \\ \mathsf{Fix}\,\sigma \;&=\; \omega_2 \cup \omega_4, \\ \mathsf{Supp}\,\sigma \;&=\; \omega_1 \cup \omega_3. \end{aligned}$$

L'énoncé général, dont nous avons déjà compris la démonstration, est le suivant, dans lequel les orbites de σ — qui sont des sous-ensembles de E — sont notées ω_σ.

Proposition 3.7. *Soit E un ensemble fini, et soit une permutation $\sigma \in \mathfrak{S}(E)$. Alors on a les réunions* disjointes :

$$\begin{aligned} E \;&=\; \bigcup_{|\omega_\sigma|=1} \omega_\sigma \;\; \bigcup_{|\omega_\sigma|\geqslant 2} \omega_\sigma, \\ \mathsf{Fix}\,\sigma \;&=\; \bigcup_{|\omega_\sigma|=1} \omega_\sigma, \\ \mathsf{Supp}\,\sigma \;&=\; \bigcup_{|\omega_\sigma|\geqslant 2} \omega_\sigma. \end{aligned}$$

□

Introduisons maintenant la notion de cycle.

Définition 3.8. Une permutation $\sigma \in \mathfrak{S}(E)$ est appelée un *cycle* si σ produit une seule σ-orbite ω_σ non réduite à un singleton, c'est-à-dire avec :

$$p \;:=\; |\omega_\sigma| \;\geqslant\; 2.$$

On dit alors que σ est un *p-cycle*, en sous-entendant que $p \geqslant 2$, et dans ce cas, $\mathsf{Supp}\,\sigma$ est cette unique σ-orbite ω_σ.

Grâce à la description d'une σ-orbite quelconque donnée par la Proposition 3.5, tout p-cycle est de la forme :

$$\Big(\; a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_{p-1} \longrightarrow a_p \; \Big)$$

avec $a_1, a_2, \ldots, a_{p-1}, a_p \in E$ distincts, ce qu'on note souvent de manière abrégée sans aucune flèche :

$$\big(a_1 \;\; a_2 \;\; \cdots \;\; a_{p-1} \;\; a_p\big),$$

tandis que les autres éléments sont tous fixés.

Un *cycle*, c'est donc une succession de wagons se poussant les uns les autres sur une ligne de chemin de fer circulaire. Ou encore, un cercle mirifique de clitocybes géotropes.

Par exemple, avec $n = 7$, la permutation :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 5 & 7 & 6 & 1 \end{pmatrix},$$

est un 4-cycle. Le cas particulier $p = 2$ mérite attention.

Terminologie 3.9. Un 2-cycle est aussi appelé une *transposition*.

Par exemple, avec $n = 5$:

$$\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 4 & 3 \end{pmatrix} = \Big(\; 3 \longrightarrow 5 \; \Big) = \big(3 \;\; 5\big),$$

Une transposition échange deux éléments distincts, sans toucher aux autres.

Or si deux étudiants échangent puis ré-échangent leurs places, ils reviennent sur leur siège initial, pendant que tous les autres restent à leur place.

Observation 3.10. *Toute transposition $\tau \in \mathfrak{S}(E)$ est sa propre inverse :*

$$\tau \circ \tau = \mathsf{Id} \qquad \Longleftrightarrow \qquad \tau^{-1} = \tau. \qquad \square$$

Bientôt, nous verrons que les transpositions sont les permutations élémentaires, au sens où *toute* permutation $\sigma \in \mathfrak{S}(E)$ peut s'écrire comme composition :

$$\sigma = \tau_1 \circ \cdots \circ \tau_r,$$

de transpositions.

Pour l'instant, souvenons-nous qu'une compagnie $\sigma \in \mathfrak{S}(E)$ construit ses propres lignes de chemin de fer circulaires sans croisements :

$$\sigma \quad \rightsquigarrow \quad \sigma\text{-orbites } \omega_\sigma \text{ disjointes avec } |\omega_\sigma| \geqslant 2,$$

les orbites-fixes $|\omega_\sigma| = 1$ pouvant être vues commes de simples vaches spectatrices immobiles.

Introduisons alors :

$$\Omega_\sigma := \big\{\sigma\text{-orbites } \omega \text{ avec } |\omega| \geqslant 2\big\},$$

d'où :

$$\mathsf{Supp}\, \sigma = \bigcup_{\omega \in \Omega_\sigma} \omega,$$

cette réunion étant disjointe, et extrayons la manière dont σ agit sur une unique ligne circulaire de TGV $\omega \in \Omega_\sigma$ en introduisant la permutation :

$$\sigma_\omega(a) := \begin{cases} a & \text{si } a \notin \omega, \\ \sigma(a) & \text{si } a \in \omega. \end{cases} \tag{3.11}$$

Ainsi, σ_ω exprime l'action de σ sur une de ses orbites, ω, et fixe tous les autres points, c'est-à-dire « *met en grève* » toutes les autres lignes circulaires.

Grâce à la Proposition 3.4 **(3)** et à la Proposition 2.6, on a :

$$\omega \neq \omega' \quad \Longrightarrow \quad \omega \cap \omega' = \emptyset \quad \Longrightarrow \quad \sigma_{\omega'} \circ \sigma_\omega = \sigma_\omega \circ \sigma_{\omega'}.$$

Notons :

$$r := \big|\Omega_\sigma\big|,$$

c'est-à-dire qu'il existe r orbites de longueur $\geqslant 2$, d'où $\mathsf{Supp}\,\sigma = \omega_1 \cup \cdots \cup \omega_r$.

Théorème 3.12. [Décomposition en cycles] *Toute permutation $\sigma \in \mathfrak{S}(E)$ se décompose de manière* unique *comme produit commutatif :*

$$\sigma = \sigma_{\omega_1} \circ \cdots \circ \sigma_{\omega_r},$$

de cycles à supports disjoints.

C'est la carte complète des trajectoires des comètes. Si nous revenons à notre exemple favori :

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

il est clair que sa décomposition est :

$$\sigma = \big(\ 1 \longrightarrow 4 \longrightarrow 5 \longrightarrow 8\ \big) \circ \big(\ 3 \longrightarrow 7 \longrightarrow 9\ \big),$$

ce que l'on écrit de manière abrégée :

$$\sigma = \big(1\ 4\ 5\ 8\big)\big(3\ 7\ 9\big).$$

On pourrait même écrire :

$$\sigma = \big(1\ 4\ 5\ 8\big)\big(2\big)\big(3\ 7\ 9\big)\big(6\big),$$

mais il est préférable de ne pas faire apparaître les points fixes, en ayant en tête que les éléments *non écrits* sont fixes.

Démonstration. Montrons que σ est égale à $\sigma_{\omega_1} \circ \cdots \circ \sigma_{\omega_r}$, en faisant agir ces deux permutations sur un élément quelconque a de $E = \mathsf{Fix}\,\sigma \cup \mathsf{Supp}\,\sigma$.

Cas 1 : $a \in \mathsf{Fix}\,\sigma$. Alors $a \notin \omega_1$, …, $a \notin \omega_r$, donc :

$$\sigma_{\omega_1}(a) = a, \ \ldots\ldots\ldots, \ \sigma_{\omega_r}(a) = a,$$

puis :

$$\sigma_{\omega_1}\big(\cdots\big(\sigma_{\omega_r}(a)\big)\cdots\big) = a = \sigma(a).$$

Cas 2 : $a \in \mathsf{Supp}\,\sigma$. Comme $\mathsf{Supp}\,\sigma = \omega_1 \cup \cdots \cup \omega_r$, disjointement, il existe un unique entier $1 \leqslant i \leqslant r$ tel que $a \in \omega_i$, d'où par la définition (3.11) :

$$\begin{aligned} & & \sigma_{\omega_i}(a) &= \sigma(a), \\ j \neq i & \quad \Longrightarrow \quad & \sigma_{\omega_j}(a) &= a, \end{aligned}$$

puis grâce à la commutation :

$$\begin{aligned}\sigma_{\omega_1}\circ\cdots\circ\sigma_{\omega_i}\circ\cdots\circ\sigma_{\omega_r}(a) &= \sigma_{\omega_i}\Big(\sigma_{\omega_1}\circ\cdots\circ\sigma_{\omega_{i-1}}\circ\sigma_{\omega_{i+1}}\circ\cdots\circ\sigma_{\omega_r}(a)\Big)\\ &= \sigma_{\omega_i}(a)\\ &= \sigma(a).\end{aligned}$$

Montrons maintenant l'*unicité* de la décomposition de σ en cycles à supports disjoints. Supposons alors qu'il existe une autre décomposition :

$$\sigma_{\omega_1}\circ\cdots\circ\sigma_{\omega_r} \;=\; \sigma \;=\; \overline{\sigma}_1\circ\cdots\circ\overline{\sigma}_s,$$

en cycles $\overline{\sigma}_\ell$, pour $\ell=1,\dots,s$, à supports disjoints, donc commutant entre eux, et notons :

$$\varpi_\ell \;:=\; \mathsf{Supp}\,\overline{\sigma}_\ell \qquad (1\leqslant\ell\leqslant s),$$

de telle sorte que :

$$\omega_1\cup\cdots\cup\omega_r \;=\; \mathsf{Supp}\,\sigma \;=\; \varpi_1\cup\cdots\cup\varpi_s. \tag{3.13}$$

Comme $\overline{\sigma}_\ell$ est un cycle, son support ϖ_ℓ est la $\overline{\sigma}_\ell$-orbite d'un de ses points quelconques, d'après la Proposition 3.6.

Assertion 3.14. *Pour $1\leqslant\ell\leqslant s$, chaque $\overline{\sigma}_\ell$-orbite ϖ_ℓ coïncide en fait avec une certaine σ-orbite.*

Par conséquent, ϖ_ℓ ne dépend *que* de σ — c'est un premier pas vers l'unicité.

Preuve. Soit $a\in\varpi_\ell$ quelconque. Nous venons de dire que $\mathsf{Orb}_{\overline{\sigma}_\ell}(a)=\varpi_\ell$.

Pour $m\neq\ell$, on a $\overline{\sigma}_m(a)=a$, d'où :

$$\begin{aligned}\sigma(a) &= \overline{\sigma}_1\circ\cdots\circ\overline{\sigma}_\ell\circ\cdots\circ\overline{\sigma}_s(a)\\ &= \overline{\sigma}_\ell(a).\end{aligned} \tag{3.15}$$

Puisque $\varpi_\ell=\mathsf{Supp}\,\overline{\sigma}_\ell$ satisfait $\overline{\sigma}_\ell\big(\mathsf{Supp}\,\overline{\sigma}_\ell\big)=\mathsf{Supp}\,\overline{\sigma}_\ell$ d'après la Proposition 2.5 **(1)**, nous déduisons pour tout $m\neq\ell$ que :

$$\overline{\sigma}_\ell(a)\;\notin\;\mathsf{Supp}\,\overline{\sigma}_m \qquad\text{d'où}\qquad \overline{\sigma}_m\big(\overline{\sigma}_\ell(a)\big)\;=\;\overline{\sigma}_\ell(a) \qquad (m\neq\ell),$$

puis :

$$\begin{aligned}\sigma\big(\sigma(a)\big) &= \sigma\big(\overline{\sigma}_\ell(a)\big)\\ &= \overline{\sigma}_1\circ\cdots\circ\overline{\sigma}_\ell\circ\cdots\circ\overline{\sigma}_s\big(\overline{\sigma}_\ell(a)\big)\\ &= \overline{\sigma}_\ell\big(\overline{\sigma}_\ell(a)\big).\end{aligned}$$

Ensuite, une récurrence aisée donne :

$$\sigma^i(a) \;=\; \big(\overline{\sigma}_\ell\big)^i(a) \qquad (\forall\, i\in\mathbb{Z}),$$

et ainsi on a bien :

$$\mathsf{Orb}_\sigma(a) \;=\; \big\{\sigma^i(a)\colon\;i\in\mathbb{Z}\big\} \;=\; \big\{\big(\overline{\sigma}_\ell\big)^i(a)\colon\;i\in\mathbb{Z}\big\} \;=\; \mathsf{Orb}_{\overline{\sigma}_\ell}(a) \;=\; \varpi_\ell. \qquad\square$$

Chaque $\overline{\sigma}_\ell$-orbite $\varpi_\ell=\omega_{i(\ell)}$ s'identifie donc à une certaine σ-orbite, au moyen d'une application :

$$\{1,\dots,s\}\;\ni\;\ell\;\longmapsto\;\ell(i)\;\in\;\{1,\dots,r\}$$

qui est injective, puisque les deux collections d'orbites (disjointes) sont contenues dans notre ensemble E. De plus, cette application est aussi surjective, car d'après (3.13), les ω_i et les ϖ_ℓ remplissent $\mathsf{Supp}\,\sigma$. Ainsi :

$$r \;=\; s.$$

Assertion 3.16. *On a $\sigma_{\omega_{i(\ell)}} = \overline{\sigma}_\ell$, pour tout $\ell = 1, \ldots, r$.*

Preuve. En effet, ces deux permutations fixent tout élément $a \notin \omega_{i(\ell)} = \varpi_\ell$.

Et en tenant compte de la définition (3.11), le petit calcul (3.15) a déjà montré pour $a \in \omega_{i(\ell)} = \varpi_\ell$ que :

$$\sigma_{\omega_{i(\ell)}}(a) \;=\; \sigma(a) \;=\; \overline{\sigma}_\ell(a). \qquad \square$$

En conclusion, dans les deux décompositions en cycles qui commutent :

$$\sigma_{\omega_1} \circ \cdots \circ \sigma_{\omega_r} \;=\; \sigma \;=\; \overline{\sigma}_1 \circ \cdots \circ \overline{\sigma}_r,$$

il y a les mêmes facteurs, à un simple changement d'ordre près — c'est l'unicité ! $\square$

De manière importante, une permutation quelconque $\sigma \in \mathfrak{S}(E)$ ayant comme orbites $\omega_1, \ldots, \omega_r$ de cardinaux $p_1, \ldots, p_r \geqslant 2$ s'écrit *explicitement :*

$$\Big(a_1 \longrightarrow \sigma(a_1) \longrightarrow \cdots \longrightarrow \sigma^{p_1-1}(a_1) \Big) \circ \cdots \circ \Big(a_r \longrightarrow \sigma(a_r) \longrightarrow \cdots \longrightarrow \sigma^{p_r-1}(a_r) \Big).$$

Quant à notre exemple fétiche :

$$\sigma \;:=\; \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix},$$

montrons encore sa décomposition :

$$\sigma \;=\; \big(\; 1 \longrightarrow 4 \longrightarrow 5 \longrightarrow 8 \; \big) \circ \big(\; 3 \longrightarrow 7 \longrightarrow 9 \; \big).$$

Théorème 3.17. *Le groupe $\mathfrak{S}(E)$ des permutations d'un ensemble fini E est engendré par les cycles.* $\square$

Toutefois, si on nous donne en TD une composition de cycles dont les supports ne sont *pas* disjoints, il faut la re-travailler pour la re-décomposer en cycles à supports *disjoints*.

Exemple 3.18. Soit la permutation de l'ensemble $\{1, 2, 3, 4, 5, 6, 7, 8\}$:

$$\sigma \;:=\; \big(1 \;\; 2 \;\; 3 \;\; 5\big) \circ \big(3 \;\; 7\big) \circ \big(7 \;\; 4 \;\; 8\big),$$

dont les cycles ne sont *pas* disjoints.

Évaluons le devenir de chaque entier, en commençant les compositions par la droite comme il se doit :

$$\begin{array}{ccccccccc} & & (7\ 4\ 8) & & (2\ 7) & & (1\ 2\ 3\ 5) & & \\ 1 & \longrightarrow & 1 & \longrightarrow & 1 & \longrightarrow & 2 \\ 2 & \longrightarrow & 2 & \longrightarrow & 2 & \longrightarrow & 3 \\ 3 & \longrightarrow & 3 & \longrightarrow & 7 & \longrightarrow & 7 \\ 4 & \longrightarrow & 8 & \longrightarrow & 8 & \longrightarrow & 8 \\ 5 & \longrightarrow & 5 & \longrightarrow & 5 & \longrightarrow & 1 \\ 6 & \longrightarrow & 6 & \longrightarrow & 6 & \longrightarrow & 6 \\ 7 & \longrightarrow & 4 & \longrightarrow & 4 & \longrightarrow & 4 \\ 8 & \longrightarrow & 7 & \longrightarrow & 3 & \longrightarrow & 5 \end{array}$$

ce qui nous donne :

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

Visiblement, l'ensemble des points fixes est réduit au singleton $\{6\} = \mathsf{Fix}\,\sigma$, et on constate qu'il y a un unique cycle, de longueur 7 :

$$\big(\ 1 \longrightarrow 2 \longrightarrow 3 \longrightarrow 7 \longrightarrow 4 \longrightarrow 8 \longrightarrow 5\ \big)\,.$$

Théorème 3.19. *Le groupe des permutations $\mathfrak{S}(E)$ d'un ensemble fini E est engendré par les transpositions.*

Démonstration. Soit une permutation arbitraire $\sigma \in \mathfrak{S}(E)$. Comme σ est une composition de cycles, grâce au Théorème 3.12, il suffit de montrer que tout cycle $\big(a_1\ \cdots\ a_p\big)$ est à son tour un produit de transpositions, où les éléments $a_1, \ldots, a_p$ de E sont mutuellement distincts.

Sans difficulté, on vérifie alors que :

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

par exemple pour $p = 3$, on vérifie que :

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ \downarrow & \downarrow & \downarrow \\ a_2 & a_3 & a_1 \end{pmatrix} \overset{?}{=} \begin{pmatrix} a_1 & a_2 & a_3 \\ \downarrow & \downarrow & \downarrow \\ a_2 & a_1 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 \\ \downarrow & \downarrow & \downarrow \\ a_1 & a_3 & a_2 \end{pmatrix},$$

en calculant cette composition depuis la droite :

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ \downarrow & \downarrow & \downarrow \\ a_1 & a_3 & a_2 \\ \downarrow & \downarrow & \downarrow \\ a_2 & a_3 & a_1 \end{pmatrix} \qquad \text{OUI !},$$

le cas général étant similaire. □

Rappelons que dans un groupe abstrait fini G, l'*ordre* d'un élément $x \in G$ est l'entier :

$$\mathsf{o}(x) \,:=\, \mathsf{min}\big\{m \geqslant 1 \colon\ x^m = 1_G\big\},$$

et rappelons que pour $G := \mathfrak{S}(E)$, l'élément neutre 1_G est $\mathsf{Id} \colon E \longrightarrow E$.

Théorème 3.20. *L'ordre dans $\mathfrak{S}(E)$ d'un p-cycle :*

$$\sigma \,=\, \Big(\, a_1 \longrightarrow a_2 \longrightarrow \cdots \longrightarrow a_{p-1} \longrightarrow a_p \,\Big),$$

est égal à son nombre d'éléments, ou à sa longueur :

$$p \,=\, \mathsf{o}(\sigma) \,=\, \mathsf{min}\big\{m \geqslant 1 \colon\ \sigma^m = \mathsf{Id}\big\}.$$

Il découle alors de la théorie générale des groupes que :

$$\sigma^m \,=\, \mathsf{Id} \qquad\qquad \Longleftrightarrow \qquad\qquad p \,\big|\, m.$$

Démonstration. Comme σ est l'identité sur le complémentaire $E\backslash\{a_1, \ldots, a_p\}$, d'où :

$$\sigma^i(a) \,=\, a \qquad\qquad (\forall\, a \neq a_1, ..., a_p,\ \forall\, i \in \mathbb{Z}),$$

on peut ignorer purement et simplement tout ce qui se trouve en-dehors du cycle [4].

Tout d'abord, puisque :

$$\begin{aligned}
\sigma(a_1) \,&=\, a_2 \,\neq\, a_1,\\
\sigma^2(a_1) \,&=\, a_3 \,\neq\, a_1,\\
&\cdots\cdots\cdots\cdots\cdots\\
\sigma^{p-1}(a_1) \,&=\, a_p \,\neq\, a_1,
\end{aligned}$$

il est clair que $\sigma, \sigma^2, \ldots, \sigma^{p-1}$ ne sont *pas* l'identité, d'où $\mathsf{o}(\sigma) \geqslant p-1$.

Mais ensuite, comme :

$$\sigma^p(a_1) \,=\, \sigma\big(\sigma^{p-1}(a_1)\big) \,=\, \sigma(a_p) \,=\, a_1,$$

et comme, pour tout entier $1 \leqslant i \leqslant p$, on a :

$$\sigma^p(a_i) \,=\, \sigma^p\big(\sigma^{i-1}(a_1)\big) \,=\, \sigma^{i-1}\big(\sigma^p(a_1)\big) \,=\, \sigma^{i-1}(a_1) \,=\, a_i,$$

on constate que σ^p *est* l'identité sur son support $\big\{a_1, \ldots, a_p\big\}$, donc partout sur E, ce qui conclut. □

Théorème 3.21. *Si $\sigma_1, \ldots, \sigma_r \in \mathfrak{S}(E)$ sont des permutations à supports disjoints :*

$$\emptyset \,=\, \mathsf{Supp}\,\sigma_i \cap \mathsf{Supp}\,\sigma_j \qquad\qquad (\forall\, 1 \leqslant i \neq j \leqslant r),$$

alors :

$$\mathsf{o}\big(\sigma_1 \circ \cdots \circ \sigma_r\big) \,=\, \mathsf{ppcm}\,\big(\mathsf{o}(\sigma_1),\, \ldots,\, \mathsf{o}(\sigma_r)\big).$$

En particulier, cette formule arithmétique très élémentaire s'applique à la décompositions de :

$$\sigma \,=\, \sigma_{\omega_1} \circ \cdots \circ \sigma_{\omega_r},$$

en cycles à supports disjoints fournie par le Théorème 3.12, pour donner :

$$\begin{aligned}
\mathsf{o}(\sigma) \,&=\, \mathsf{ppcm}\,\big\{\mathsf{o}(\sigma_1),\, \ldots,\, \mathsf{o}(\sigma_r)\big\}\\
&=\, \mathsf{ppcm}\,\big\{\mathsf{longueur}(\sigma_1),\, \ldots,\, \mathsf{longueur}(\sigma_r)\big\}.
\end{aligned}$$

4. Effectivement, tout ce qui se trouve en dehors du cycle — *magnétique !* — des mathématiques pourrait, et devrait, être ignoré …

Par exemple, l'ordre de notre permutation élue décomposée de l'année 2021 :

$$\sigma \;=\; \big(1\ \ 4\ \ 5\ \ 8\big) \circ \big(3\ \ 7\ \ 9\big),$$

vaut tout simplement :

$$\boldsymbol{o}(\sigma) \;=\; \mathsf{ppcm}\,(3,4) \;=\; 12.$$

Démonstration. Le cas $r = 1$, où $\sigma = \sigma_1$, est trivial.

Supposons donc $r = 2$, c'est-à-dire $\sigma = \sigma_1 \circ \sigma_2$. Comme les supports de σ_1 et de σ_2 sont par hypothèse disjoints, il est clair que les actions de σ_1 et de σ_2 sur les éléments de E sont totalement indépendantes, et donc :

$$\begin{array}{lllll} \sigma^m \;=\; \sigma_1^m \circ \sigma_2^m & \iff & \sigma_1^m \;=\; \mathsf{Id} & \text{et} & \sigma_2^m \;=\; \mathsf{Id}, \\ & \iff & p_1 \;\big|\; m & \text{et} & p_2 \;\big|\; m, \end{array}$$

donc par définition du ppcm on a bien :

$$\boldsymbol{o}(\sigma) \;=\; \mathsf{ppcm}\,\big(\boldsymbol{o}(\sigma_1),\, \boldsymbol{o}(\sigma_2)\big).$$

Le cas $r \geqslant 3$ quelconque se déduit du cas $r = 2$ grâce à une récurrence assez immédiate. □

4. Conjugaisons comme changements de coordonnées sur E

Une permutation fixée $\rho \in \mathfrak{S}(E)$ peut être vue comme un « *changement de coordonnées* » sur E, c'est-à-dire un changement de dénomination des éléments de E. Quand on change de « coordonnées », une permutation quelconque $\sigma \in \mathfrak{S}(E)$ est transformée en sa *conjuguée par* ρ :

$$\rho \circ \sigma \circ \rho^{-1} \;=:\; \sigma',$$

comme l'exprime le diagramme suivant :

$$\begin{array}{ccc} E & \xrightarrow{\ \sigma\ } & E \\ {\scriptstyle \rho^{-1}}\uparrow & & \downarrow{\scriptstyle \rho} \\ E' & \xrightarrow[\rho\circ\sigma\circ\rho^{-1}]{\ \sigma'\ } & E'. \end{array}$$

Pour plus de mathématé-clarté, on devrait s'imaginer que l'espace d'arrivé de $\rho\colon E \longrightarrow E'$ est une « *copie* » $E' := E$ de E, que l'on décide néanmoins de considérer comme « différente », au moins au niveau des notations formelles.

$$\boxed{\textbf{\textit{Conjugaison} = \textit{Changement de coordonnées}}}$$

Dans le cas des permutations qui sont des p-cycles, on a une expression très simple de la conjugaison.

Proposition 4.1. *Le conjugué, par une une permutation fixée $\rho \in \mathfrak{S}(E)$, d'un p-cycle, est le p-cycle de même longueur :*

$$\rho \circ \big(a_1 \ \cdots \ a_p\big) \circ \rho^{-1} \;=\; \big(\rho(a_1) \ \cdots \ \rho(a_p)\big).$$

On voit bien en quoi les noms-coordonnées a_i du p-cycle à gauche se trouvent changés en les noms-coordonnées $\rho(a_i)$ à droite.

Démonstration. La permutation ρ effectue une bijection :

$$E \ni a \longmapsto \rho(a) =: b \in E.$$

Vérifions que les actions sur n'importe quel élément $b \in E$ sont égales :

$$\rho \circ \big(a_1 \ \cdots \ a_p\big) \circ \rho^{-1}(b) \overset{?}{=} \big(\rho(a_1) \ \cdots \ \rho(a_p)\big)(b).$$

Cas 1 : $b = \rho(a_i)$ avec $1 \leqslant i \leqslant p-1$. Alors on a bien :

$$\rho \circ (a_1 \ \ldots \ a_p)(a_i) \ = \ \rho(a_{i+1}) \overset{\text{OUI}}{=} \big(\rho(a_1) \cdots \rho(a_p)\big)\big(\rho(a_i)\big).$$

Cas 2 : $b = \rho(a_p)$. Le même raisonnement fonctionne, avec la convention $a_{p+1} := a_1$.

Cas 3 : $b \neq \rho(a_1), \ldots, \rho(a_p)$. Alors b reste fixé par $\big(\rho(a_1) \ \ldots, \rho(a_p)\big)$ à droite, et de même, son image inverse $a := \rho^{-1}(b)$ est fixée à gauche par $(a_1 \ \ldots \ a_p)$, donc l'égalité $\overset{?}{=}$ est encore vraie, trivialement. □

Ainsi, nous introduisons la copie $E' := E$. Alors la permutation $\rho \colon E \longrightarrow E'$ effectue une « *équivalence* » entre E et E', au sens où l'on a les deux bijections réciproques l'une de l'autre :

$$\begin{aligned} E \ni a &\longmapsto \rho(a) := a' \in E', \\ E \ni a := \rho^{-1}(a') &\longmapsfrom a' \in E'. \end{aligned}$$

Une « *équivalence* » échange les deux ensembles fondamentaux en lesquels E et E' se décomposent :

$$\begin{array}{ccccccc} & E & = & \mathsf{Fix}\,\sigma & \cup & \mathsf{Supp}\,\sigma \\ \rho & \downarrow & & \downarrow & & \downarrow \\ & E' & = & \mathsf{Fix}\,\sigma' & \cup & \mathsf{Supp}\,\sigma' \end{array}$$

Proposition 4.2. *Une conjugaison $\rho \circ \sigma \circ \rho^{-1} = \sigma'$ induit les deux transferts d'ensembles :*

$$\begin{aligned} \rho\big(\mathsf{Fix}\,\sigma\big) &= \mathsf{Fix}\,\sigma', \\ \rho\big(\mathsf{Supp}\,\sigma\big) &= \mathsf{Supp}\,\sigma'. \end{aligned}$$

Démonstration. Montrons que $\rho\big(\mathsf{Fix}\,\sigma\big) \subset \mathsf{Fix}\,\sigma'$. Soit $a \in \mathsf{Fix}\,\sigma$, c'est-à-dire $\sigma(a) = a$. Alors on a bien $\rho(a) \in \mathsf{Fix}\,\sigma'$, car :

$$\sigma'\big(\rho(a)\big) \ = \ \rho \circ \sigma \circ \rho^{-1}\big(\rho(a)\big) \ = \ \rho\big(\sigma(a)\big) \ = \ \rho(a).$$

L'inclusion inverse $\rho\big(\mathsf{Fix}\,\sigma\big) \supset \mathsf{Fix}\,\sigma'$, qui est équivalente à $\rho^{-1}\big(\mathsf{Fix}\,\sigma'\big) \subset \mathsf{Fix}\,\sigma$, se démontre pareillement en intervertissant les rôles de σ et de σ', grâce à $\sigma = \rho^{-1} \circ \sigma' \circ \rho$.

Donc $\rho\big(\mathsf{Fix}\,\sigma\big) = \mathsf{Fix}\,\sigma'$.

Enfin, les supports étant les complémentaires des ensembles de points fixes, et ρ étant une bijection, il vient automatiquement $\rho\big(\mathsf{Supp}\,\sigma\big) = \mathsf{Supp}\,\sigma'$. □

Ensuite, soit un entier $2 \leqslant p \leqslant n = |E|$, et soient deux brochettes de p éléments :

$$\begin{matrix} a_1 \\ \vdots \\ a_p \end{matrix} \quad \text{distincts} \in E \qquad\qquad \begin{matrix} a'_1 \\ \vdots \\ a'_p \end{matrix} \quad \text{distincts} \in E' = E.$$

Alors l'application bijective de morceau d'agneau à morceau de bœuf en passant par les dents de l'ogre gaulois :

$$\begin{array}{ccc} a_1 & \longmapsto & a'_1 \\ \vdots & & \vdots \\ a_p & \longmapsto & a_{p'}, \end{array}$$

peut être prolongée en une permutation $\rho \in \mathfrak{S}(E)$, simplement en numérotant les $n-p$ autres éléments $a_{p+1}, \dots, a_n$ de E ainsi que les $n-p$ autres éléments $a'_{p+1}, \dots, a'_n$ de $E' = E$, et en assignant de manière analogue :

$$\rho\big(a_{p+1}\big) := a'_{p+1}, \ \dots\dots, \ \rho\big(a_n\big) := a'_n.$$

Proposition 4.3. *Deux cycles quelconques de même longueur sont toujours conjugués dans* $\mathfrak{S}(E)$.

Démonstration. Soient donc $\big(a_1 \dots, a_p\big)$ et $\big(a'_1 \dots a'_p\big)$ deux cycles, de longueurs égales $p \geqslant 2$. Nous venons de produire $\rho \in \mathfrak{S}(E)$ satisfaisant $\rho(a_i) = a'_i$, pour $i = 1, \dots, n$. Alors la Proposition 4.1 conclut :

$$\rho \circ \big(a_1 \ \cdots \ a_p\big) \circ \rho^{-1} = \big(a'_1 \ \cdots \ a'_p\big). \qquad \square$$

Corollaire 4.4. *Deux transpositions arbitraires sont toujours conjugués dans* $\mathfrak{S}(E)$. $\square$

Exemple 4.5. Maintenant, nous affirmons que les deux éléments de $\mathfrak{S}(E)$ où $E = \{1, \dots, 7\}$:

$$\sigma := (1\ 3\ 5) \circ (2\ 4) \qquad \text{et} \qquad (1\ 2\ 3) \circ (6\ 7),$$

sont *conjugués* dans $\mathfrak{S}_7$. Notons qu'ils ont chacun *deux* cycles de mêmes longueurs $3, 2$.

Clairement :

$$\mathsf{Fix}\,\sigma = \{6, 7\} \qquad \text{et} \qquad \mathsf{Fix}\,\sigma' = \{4, 5\}.$$

D'après la Proposition 4.2, une équivalence ρ satisfaisant $\rho \circ \sigma \circ \rho^{-1} = \sigma'$ doit envoyer $\{6, 7\}$ sur $\{4, 5\}$. De plus, on devine évidemment que ρ doit envoyer les cycles de σ sur les cycles de σ' *de mêmes longueurs* :

$$\begin{array}{ccc} 6 & 7 & \\ \downarrow & \downarrow & \\ 4 & 5 & \end{array} \qquad \begin{array}{ccc} 1 & 3 & 5 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{array} \qquad \begin{array}{ccc} 2 & 4 & \\ \downarrow & \downarrow & . \\ 6 & 7 & \end{array}$$

Si on préfère, pour faciliter les calculs manuels, on peut rajouter les points fixes dans l'écriture, en étendant[5] la notation $(a_1 \cdots a_p)$ au cas $p = 1$, c'est-à-dire $(a_1) = \mathsf{Id}$. Ainsi, on pourra écrire σ et σ' en ordonnant leurs cycles respectifs (qui commutent) par longueur décroissante :

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

afin de faire apparaître des correspondances verticales qui définissent une permutation-candidate :

$$\rho := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 6 & 2 & 7 & 3 & 4 & 5 \end{pmatrix},$$

5. Mais attention ! ! ! (a_1) n'est *pas* un cycle, car dans la Définition 3.8, on demande expressément que $p \geqslant 2$! !

pour conjuguer σ à $\sigma' = \rho \circ \sigma \circ \rho^{-1}$.

Nous laissons au lecteur-étudiant le soin de vérifier que cette permutation naturelle ρ fonctionne.

Cette vérification est d'ailleurs essentiellement inutile, car nous avons déjà deviné le résultat complètement général.

Théorème 4.6. *Pour deux permutations $\sigma \in \mathfrak{S}(E)$ et $\sigma' \in \mathfrak{S}(E)$, on a équivalence entre :*
(i) *σ et σ' sont* conjuguées, i.e. *il existe une équivalence $\rho \in \mathfrak{S}(E)$ telle que $\rho \circ \sigma \circ \rho^{-1} = \sigma'$;*
(ii) *les listes (avec répétitions) des longueurs décroissantes des cycles (commutant entre eux) à supports disjoints qui les composent :*

$$\sigma \;=\; \big(a_1^1 \;\cdots\; a_{p_1}^1\big)\,\big(a_1^2 \;\cdots\; a_{p_2}^2\big)\;\cdots\;\big(a_1^i \;\cdots\; a_{p_i}^i\big)\cdots\;\big(a_1^r \;\cdots\; a_{p_r}^r\big),$$
$$\sigma' \;=\; \big(a_1'^1 \;\cdots\; a_{p'_1}'^1\big)\,\big(a_1'^2 \;\cdots\; a_{p'_2}'^2\big)\;\cdots\;\big(a_1'^i \;\cdots\; a_{p'_i}'^i\big)\cdots\;\big(a_1'^{r'} \;\cdots\; a_{p'_{r'}}'^{r'}\big),$$

avec :

$$p_1 \geqslant p_2 \geqslant \cdots \geqslant p_i \geqslant \cdots \geqslant p_r \;\geqslant\; 2,$$
$$p'_1 \geqslant p'_2 \geqslant \cdots \geqslant p'_i \geqslant \cdots \geqslant p'_{r'} \geqslant\; 2,$$

sont identiques, *c'est-à-dire que :*

$$r \;=\; r' \qquad\qquad \textit{et} \qquad\qquad p_1 \;=\; p'_1,\;\; \ldots\;\; p_r \;=\; p'_r.$$

Démonstration. **(i) $\Longrightarrow$ (ii)**. Supposons donc que $\rho \circ \sigma \circ \rho^{-1} = \sigma'$, avec une $\rho \in \mathfrak{S}(E)$. Décomposons $\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r$ en produit (commutatif) de cycles à supports disjoints, et de longueurs ordonnées de manière croissante, grâce au Théorème 3.12 — en supprimant les lettres ω —, et écrivons :

$$\begin{aligned}\sigma' \;&=\; \rho \circ \sigma \circ \rho^{-1} \\ &=\; \big(\rho \circ \sigma_1 \circ \rho^{-1}\big) \circ \big(\rho \circ \sigma_2 \circ \rho^{-1}\big) \circ \cdots \circ \big(\rho \circ \sigma_r \circ \rho^{-1}\big).\end{aligned}$$

Grâce à la Proposition 4.1, pour tout $1 \leqslant i \leqslant r$, la permutation :

$$\sigma'_i \;:=\; \rho \circ \sigma_i \circ \rho^{-1},$$

est un cycle de même longueur que σ_i, à savoir p_i.

Or d'après la Proposition 4.2, le support de σ' est l'image du support de σ par ρ. De plus, comme ρ est bijective, et comme les supports des σ_i sont disjoints, il en va de même des supports des permutations σ'_i, lesquelles commutent, donc.

Par l'*unicité* de la décomposition en cycles donnée par le Théorème 3.12, il est *nécessaire* que :

$$\sigma' \;=\; \sigma'_1 \circ \cdots \circ \sigma'_i \circ \cdots \circ \sigma'_r,$$

soit la décomposition de σ' en produit de cycles à supports disjoints. Ainsi, on a bien $r = r'$ et $p_i = p'_i$ pour $i = 1, \ldots, r$.

(ii) $\Longrightarrow$ (i). Écrivons alors, en spécifiant le parallèle vertical :

$$\sigma \;=\; \big(a_1^1 \;\cdots\; a_{p_1}^1\big)\,\big(a_1^2 \;\cdots\; a_{p_2}^2\big)\;\cdots\;\big(a_1^i \;\cdots\; a_{p_i}^i\big)\cdots\;\big(a_1^r \;\cdots\; a_{p_r}^r\big),$$
$$\sigma' \;=\; \big(a_1'^1 \;\cdots\; a_{p_1}'^1\big)\,\big(a_1'^2 \;\cdots\; a_{p_2}'^2\big)\;\cdots\;\big(a_1'^i \;\cdots\; a_{p_i}'^i\big)\cdots\;\big(a_1'^r \;\cdots\; a_{p_r}'^r\big),$$

où nous avons remplacé $r' := r$, et chaque $p'_i := p_i$ aussi. Par définition, les $p_1 + \cdots + p_r$ éléments $a_{\ell_i}^i$ sont distincts entre eux, et de même pour les $a_{\ell_i}'^i$.

Posons :

$$s \;:=\; n - \big(p_1 + \cdots + p_r\big),$$

et notons :

$$E\big\backslash\big\{a^i_{\ell_i}\big\} \;=\; \big\{b_1, b_2, \ldots, b_s\big\} \;=\; \mathsf{Fix}\,\sigma,$$
$$E'\big\backslash\big\{a'^i_{\ell_i}\big\} \;=\; \big\{b'_1, b'_2, \ldots, b'_s\big\} \;=\; \mathsf{Fix}\,\sigma'.$$

Assertion 4.7. *La bijection $\rho\colon\ E \longrightarrow E'$ définie par :*

$$\begin{array}{ccccccccccc} a^1_1 & \cdots & a^1_{p_1} & & & a^r_1 & \cdots & a^r_{p_r} & & b_1\ b_2 & \cdots\ b_s \\ \downarrow & \cdots & \downarrow & \cdots & & \downarrow & \cdots & \downarrow & & \downarrow\ \downarrow & \cdots\ \downarrow \\ a'^1_1 & \cdots & a'^1_{p_1}, & & & a'^r_1 & \cdots & a'^r_{p_r}, & & b'_1\ b'_2 & \cdots\ b'_s, \end{array}$$

conjugue $\sigma' = \rho \circ \sigma \circ \rho^{-1}$.

Preuve. Montrons en effet que $\sigma' \circ \rho\,(c) \overset{?}{=} \rho \circ \sigma\,(c)$ pour tout élément $c \in E$.

Puisqu'un cycle $\big(a^i_1 \cdots a^i_{p_i}\big)$ envoie le dernier élément $a^i_{p_i}$ sur le premier a^i_1, adoptons la convention que $a^i_{p_i+1} := a^i_1$.

Alors premièrement, on a bien :

$$\sigma' \circ \rho\,\big(a^i_{\ell_i}\big) \;=\; \sigma'\big(a'^i_{\ell_i}\big) \;=\; a'^i_{\ell_i+1} \;=\; \rho\big(a^i_{\ell_i+1}\big) \;=\; \rho \circ \sigma\,\big(a^i_{\ell_i}\big).$$

Et deuxièmement, pour $c = b_j$, on a aussi bien :

$$\sigma' \circ \rho\,(b_j) \;=\; \sigma'\big(b'_j\big) \;=\; b'_j \;=\; \rho(b_j) \;=\; \rho \circ \sigma\,(b_j).$$ □

En conclusion, cette permutation ρ convient. Elle n'est en général pas unique, car par exemple, des numérotations différentes de $\mathsf{Fix}\,\sigma$ et de $\mathsf{Fix}\,\sigma'$ conduisent à des ρ différentes. □

5. Classes de conjugaison de $\mathfrak{S}(E)$ et partitions

Eu égard au Théorème 4.6, nous sommes ramenés à lister toutes les longueurs possibles de cycles disjoints contenus dans E. Nous allons donc maintenant donner un résultat qui permet d'élaborer de telles listes. Commençons par une

Définition 5.1. Une *partition* d'un entier $n \geqslant 1$ est une suite d'entiers :

$$\boldsymbol{p} \;=\; \big\{p_1,\ \ldots,\ p_t\big\},$$

ordonnés de manière décroissante :

$$p_1 \;\geqslant\; p_2 \;\geqslant\; \cdots \;\geqslant\; p_{t-1} \;\geqslant\; p_t \;\geqslant\; 1,$$

dont la somme vaut :

$$n \;=\; p_1 + p_2 + \cdots + p_{t-1} + p_t.$$

L'entier $t \;\geqslant\; 1$ est autorisé à varier. Par exemple, voici toutes les partitions des cinq premiers entiers $n = 1, 2, 3, 4, 5$:

$1,$

$2 \;=\; 1+1,$

$3 \;=\; 2+1 \;=\; 1+1+1,$

$4 \;=\; 3+1 \;=\; 2+2 \;=\; 2+1+1 \;=\; 1+1+1+1,$

$5 \;=\; 4+1 \;=\; 3+2 \;=\; 3+1+1 \;=\; 2+2+1 \;=\; 2+1+1+1 \;=\; 1+1+1+1+1.$

Par abus de cervoise, on confondra souvent la suite finie $\boldsymbol{p} \;=\; \big\{p_1, \ldots, p_t\big\}$ à la somme explicite qui lui est associée.

Notation 5.2. L'ensemble des partitions de n sera noté $\boldsymbol{P}_n$.

Avec $n = 9$, notre exemple-Idéfix :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 7 & 5 & 8 & 6 & 9 & 1 & 3 \end{pmatrix} \;=\; \big(1\ 4\ 5\ 8\big)\,\big(3\ 7\ 9\big)\,\big(2\big)\,\big(6\big),$$

représente la partition :

$$9 \;=\; 4+3+1+1.$$

Définition 5.3. Le *type* d'une permutation $\sigma \in \mathfrak{S}(E)$ avec $|E| = n \geqslant 2$, est la partition $\boldsymbol{p}(\sigma)$ de n dont les éléments sont les cardinaux des diverses orbites de σ, rangés par ordre décroissant.

En supposant σ décomposée comme produit (commutatif) de cycles à supports disjoints :

$$\sigma \;=\; \big(a_1^1\ \cdots\ a_{p_1}^1\big)\,\big(a_1^2\ \cdots\ a_{p_2}^2\big)\ \cdots\ \big(a_1^r\ \cdots\ a_{p_r}^r\big)\,\big(b_1\big)\,\big(b_2\big)\ \cdots\ \big(b_s\big),$$

avec :

$$p_1 \;\geqslant\; p_2 \;\geqslant\; \cdots \;\geqslant\; p_r \;\geqslant\; 2,$$

et avec le nombre suivant de points fixes b_j indiqués en queue de cohorte romaine :

$$s \;:=\; n - \big(p_1 + \cdots + p_r\big),$$

il est clair que le type de σ est :

$$\boldsymbol{p}(\sigma) \;:=\; p_1 + \cdots + p_r + 1 + \cdots + 1.$$

Inversement, en partant d'une énumération quelconque des n éléments de E :

$$E \;:=\; \big\{a_1,\, a_2,\, \ldots,\, a_n\big\},$$

pour n'importe quelle partition $\boldsymbol{p}$ de :

$$n \;=\; p_1 + \cdots + p_r + 1 + \cdots + 1,$$

la permutation $\sigma_{\boldsymbol{p}} \in \mathfrak{S}(E)$ suivante :

$$\sigma_{\boldsymbol{p}} \;:=\; \big(a_1\ \cdots\ a_{p_1}\big)\,\big(a_{p_1+1}\ \cdots\ a_{p_1+p_2}\big)\ \cdots\ \big(a_{p_1+\cdots+p_{r-1}}\ \cdots\ a_{p_1+\cdots+p_{r-1}+p_r}\big),$$

dans laquelle nous n'écrivons pas à la fin les points fixes sous forme (a_ℓ), a visiblement pour type la partition $\boldsymbol{p}$ dont elle provient.

Si $\sigma \in \mathfrak{S}(E)$ est une permutation arbitraire, notons la *classe de conjugaison* de σ :

$$\mathsf{Conj}\,\sigma \;:=\; \big\{\rho \circ \sigma \circ \rho^{-1} :\ \ \rho \in \mathfrak{S}(E)\big\},$$

laquelle est une classe d'équivalence pour la relation de conjugaison.

Théorème 5.4. *L'application :*

$$\boldsymbol{p} \;\longrightarrow\; \mathsf{Conj}\,\sigma_{\boldsymbol{p}}$$

est une bijection de l'ensemble $\boldsymbol{P}_n$ des partitions de n sur l'ensemble de toutes les classes de conjugaisons de $\mathfrak{S}(E)$.

Démonstration. En effet, nous avons vu dans ce qui précède que $\sigma_{\boldsymbol{p}}$ est un *représentant* de chaque classe de conjugaison. □

6. Systèmes de générateurs

Dans cette section, nous exhibons des systèmes variés de générateurs pour le groupe symétrique $\mathfrak{S}_n$ de l'ensemble $E := \{1, \dots, n\}$.

Rappelons qu'une collection d'éléments $\gamma_1, \dots, \gamma_c \in \mathfrak{S}(E)$ est dite être un *système de générateurs* pour $\mathfrak{S}(E)$ si toute permutation $\sigma \in \mathfrak{S}(E)$ peut s'écrire comme composition finie de $\gamma_1, \dots, \gamma_c$, et de leurs inverses $\gamma_1^{-1}, \dots, \gamma_c^{-1}$. Quand $\gamma_1, \dots, \gamma_c$ sont des transpositions, donc égales à leurs inverses, il suffit de considérer $\gamma_1, \dots, \gamma_c$.

Proposition 6.1. *Le groupe $\mathfrak{S}_n$ est engendré par chacune des deux familles suivantes de transpositions :*

(1) *les transpositions $(1\ i)$ avec $2 \leqslant i \leqslant n$;*

(2) *les transpositions $\big(\ell\ \ \ell+1\big)$ avec $1 \leqslant \ell \leqslant n-1$.*

Démonstration. **(1)** Puisque toute permutation est composition de transpositions grâce au Théorème 3.19, il suffit de faire voir que toute transposition quelconque $(i\ j)$ avec $1 \leqslant i < j \leqslant n$ est une composition (finie) de transpositions de la forme $(1\ i)$ avec $1 \leqslant i \leqslant n$.

Or une vérification aisée, ou une application directe de la Proposition 4.1, montrent que :

$$\big(i\ j\big) \ = \ \big(1\ i\big) \circ \big(1\ j\big) \circ \underbrace{\big(1\ i\big)}_{= (1\ i)^{-1}} .$$

(2) De même, il suffit de montrer que toute transposition $(i\ j)$ avec $j - i \geqslant 2$ est composition finie de transpositions de la forme $(\ell\ \ \ell+1)$ avec $1 \leqslant \ell \leqslant n-1$.

Or en introduisant le « changement de coordonnées » :

$$\rho := \big(i\ \ i+1\ \cdots\ j-1\big),$$

la fameuse Proposition 4.1 nous donne :

$$\begin{aligned}\big(i\ \ i+1\ \cdots\ j-1\big) \circ \big(j-1\ \ j\big) \circ \big(i\ \ i+1\ \cdots\ j-1\big)^{-1} &= \rho \circ \big(j-1\ \ j\big) \circ \rho^{-1} \\ &= \big(\rho(j-1)\ \ \rho(j)\big) \\ &= \big(i\ j\big).\end{aligned}$$

Il reste alors seulement à faire observer — par réminiscence de la démonstration du Théorème 3.19 — que cette permutation cyclique :

$$\rho \ = \ \big(i\ \ i+1\ \cdots\ j-1\big) \ = \ \big(i\ \ i+1\big) \circ \cdots \circ \big(j-2\ \ j-1\big),$$

est composition finie de transpositions de la forme $(\ell\ \ \ell+1)$. Son inverse ρ^{-1} jouit alors de la même propriété (exercice mental).

Donc $(i\ j)$ en bas à droite est bien représentée comme composition finie en haut à gauche de transpositions de la forme $(\ell\ \ \ell+1)$. □

Par rapport au Théorème 3.19 qui disait que les $\frac{n(n-1)}{2}$ transpositions $(i\ j)$ engendrent $\mathfrak{S}_n$, cette proposition apporte un certain gain d'économie, en trouvant deux systèmes de $n-1 < \frac{n(n-1)}{2}$ transpositions génératrices. Encore mieux :

Proposition 6.2. *Le groupe $\mathfrak{S}_n$ est engendré par la transposition $(1\ 2)$ et le n-cycle $\big(1\ 2\ \cdots\ n\big)$.*

Démonstration. Grâce à la Proposition 6.1 **(2)** que nous venons d'obtenir, les transpositions $\big(\ell\ \ \ell+1\big)$ avec $1 \leqslant \ell \leqslant n-1$ engendrent $\mathfrak{S}_n$. Il suffit donc de représenter chaque $\big(\ell\ \ \ell+1\big)$ au moyen de $(1\ 2)$ et de $\big(1\ 2\ \cdots\ n\big)$.

Pour $1 \leqslant \ell \leqslant n-1$, la permutation itérée :

$$\rho_\ell\ :=\ \big(1\ 2\ \cdots\ n\big)^{\ell-1},$$

envoie 1 sur ℓ, et 2 sur $\ell+1$. Encore grâce à la Proposition-star 4.1, quand on utilise ρ_ℓ pour « changer de coordonnées » :

$$\begin{aligned}\big(\ell\ \ \ell+1\big)\ &=\ \big(\rho_\ell(1)\ \rho_\ell(2)\big)\\ &=\ \big(1\ 2\ \ldots\ n\big)^{\ell-1}\circ\big(1\ 2\big)\circ\big(1\ 2\ \ldots\ n\big)^{-\ell+1},\end{aligned}$$

on constate agréablement que $\big(\ell\ \ \ell+1\big)$ appartient effectivement au sous-groupe engendré par $(1\ 2)$ et $\big(1\ 2\ \cdots\ n\big)$. □

Deux générateurs seulement ! Pour un groupe de cardinal exponentiellement grand, égal à $n!$!

Toutefois, ce résultat devient faux en général si l'on remplace $(1\ 2)$ et $\big(1\ 2\ \cdots\ n\big)$ par une transposition et un n-cycle arbitraires, comme propose d'y réfléchir l'Exercice 1.

7. Groupe alterné

Toujours avec un ensemble fini E de cardinal $|E| = n \geqslant 2$, soit une permutation arbitraire $\sigma \in \mathfrak{S}(E)$. Grâce au Théorème 3.19, nous pouvons représenter :

$$\sigma\ =\ \tau_1\circ\cdots\circ\tau_r,$$

comme produit (composition) d'un nombre fini $r \geqslant 1$ de transpositions, *mais* une telle représentation n'a absolument rien d'unique, puisqu'on peut insérer partout des couples du type $\tau_*\circ\tau_*^{-1} = \mathsf{Id}$, où τ_* est une transposition quelconque.

Que pourrions-nous dire, alors, lorsque nous avons plusieurs représentations différentes, par exemple deux :

$$\tau_1\circ\cdots\circ\tau_r\ =\ \sigma\ =\ \tau'_1\circ\cdots\circ\tau'_{r'}\ \textbf{?}.$$

Théorème 7.1. *La parité du nombre de transpositions nécessaires pour représenter une permutation donnée est un invariant qui ne dépend que de la permutation :*

$$r\ \equiv\ r'\ \mathsf{mod}\,2.$$

Tiens, encore de l'arithmétique qui s'invite ! Pour manger du sanglier rôti !

Démonstration. Après multiplication à gauche :

$$\tau_r\circ\cdots\circ\tau_1\Big(\ \tau_1\circ\cdots\circ\tau_r\ =\ \tau'_1\circ\cdots\circ\tau'_{r'}\ \Big)$$

il vient :

$$\mathsf{Id}\ =\ \tau_1\circ\cdots\circ\tau_r\circ\tau'_1\circ\cdots\circ\tau'_{r'},$$

et avec $r+r' =: s$, tout repose sur l'énoncé crucial suivant.

Proposition 7.2. *Si l'identité est représentée comme une composition de s transpositions :*

$$\mathsf{Id}\ =\ \tau_1\circ\cdots\circ\tau_s,$$

alors $s \in 2\,\mathbb{N}$ est nécessairement pair.

Démonstration. Le cas $n = |E| = 2$ est spécial-facile, car :

$$\mathfrak{S}\big(\{1,2\}\big) \;=\; \big\{\mathsf{Id},\ (1\ 2)\big\},$$

et toute puissance impaire de la transposition $(1\ 2)$ est égale à $(1\ 2)$, tandis que toute puissance paire est égale à Id.

Nous pouvons donc supposer que $n \geqslant 3$, et admettre en raisonnant par récurrence que l'énoncé est vrai pour les permutations de l'ensemble $\{1, \ldots, n-1\}$ à $n-1$ éléments.

Par exemple dans le cas où $E = \{1,2,3,4,5,6,7\}$, c'est-à-dire avec $n = 7$, pour la composition suivante de 5 transpositions :

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

l'idée-clé consiste à déplacer vers la droite toutes les transpositions qui incorporent $n = 7$, ce que l'énoncé suivant va nous permettre de faire.

Assertion 7.3. *Pour tous indices distincts deux à deux i, j, k avec $1 \leqslant i, j, k \leqslant n-1$, on a :*

$$\begin{aligned}
(i\ n) \circ (j\ k) &\overset{1}{=} (j\ k) \circ (i\ n),\\
(i\ n) \circ (i\ j) &\overset{2}{=} (i\ j) \circ (j\ n),\\
(i\ n) \circ (j\ n) &\overset{3}{=} (i\ j) \circ (i\ n),\\
(i\ n) \circ (i\ n) &\overset{4}{=} \mathsf{Id}.
\end{aligned}$$

L'exemple en question pourra alors effectivement être soumis à ces procédés :

$$\begin{aligned}
(1\ 7) \circ (2\ 3) \circ (5\ 6) \circ (4\ 7) \circ (4\ 5) &\overset{2}{=} (1\ 7) \circ (2\ 3) \circ (5\ 6) \circ (4\ 5) \circ (5\ 7)\\
&\overset{1}{=} (2\ 3) \circ (5\ 6) \circ (4\ 5) \circ (1\ 7) \circ (5\ 7)\\
&\overset{3}{=} (2\ 3) \circ (5\ 6) \circ (4\ 5) \circ (1\ 5) \circ (1\ 7).
\end{aligned}$$

Preuve. L'égalité de commutation $\overset{1}{=}$ est connue, puisque les supports sont disjoints.

Ensuite, vérifions l'égalité $\overset{2}{=}$ comme suit, sans écrire les éléments non concernés car fixés :

$$\begin{array}{cccc}
 & i & j & n \\
(i\ j) & \downarrow & \downarrow & \downarrow \\
 & j & i & n \\
(i\ n) & \downarrow & \downarrow & \downarrow \\
 & j & n & i
\end{array}
\quad \overset{?}{=} \quad
\begin{array}{cccc}
 & i & j & n \\
 & \downarrow & \downarrow & \downarrow \\
 & i & n & j \\
 & \downarrow & \downarrow & \downarrow \\
 & j & n & i
\end{array}
\begin{array}{c}
 \\ (j\ n) \\ \\ (i\ j) \\
\end{array}
\qquad \text{OUI !}$$

Puis, vérifions l'égalité $\overset{3}{=}$ comme suit :

$$\begin{array}{cccc}
 & i & j & n \\
(j\ n) & \downarrow & \downarrow & \downarrow \\
 & i & n & j \\
(i\ n) & \downarrow & \downarrow & \downarrow \\
 & n & i & j
\end{array}
\quad \overset{?}{=} \quad
\begin{array}{cccc}
 & i & j & n \\
 & \downarrow & \downarrow & \downarrow \\
 & n & j & i \\
 & \downarrow & \downarrow & \downarrow \\
 & n & i & j
\end{array}
\begin{array}{c}
 \\ (i\ n) \\ \\ (i\ j) \\
\end{array}
\qquad \text{OUI !}$$

Enfin, l'égalité $\overset{4}{=}$ est triviale. □

Grâce aux deux relations $\overset{1}{=}$, $\overset{2}{=}$, nous pouvons « repousser » à la fin toutes les transpositions du type $(i\ n)$ avec $1 \leqslant i \leqslant n-1$, ce qui ne change pas le nombre, s, de transpositions dans l'identité $\mathsf{Id} = \tau_1 \circ \cdots \circ \tau_s$.

Ensuite, grâce aux relations $\overset{3}{=}$, $\overset{4}{=}$, nous pouvons contracter toutes les paires successives à la fin $(i\ n) \circ (j\ n)$ de manière à ne conserver qu'au plus une seule occurrence de n. Comme $\overset{3}{=}$, $\overset{4}{=}$ transforment deux transpositions en deux ou en zéro transpositions, à chaque opération $\overset{3}{=}$, $\overset{4}{=}$, la *parité* du nombre de transpositions demeure invariante. Yep !

Une fois ce travail de normalisation achevé, il ne peut rester à la fin qu'*au plus une* transposition du type $(i\ n)$, et donc il y a deux cas à considérer.

Cas 1 :

$$\mathsf{Id} \ = \ \tau'_1 \circ \cdots \circ \tau'_{s'} \circ (i\ n),$$

avec $s'+1 \equiv s \mod 2$, et avec des transpositions $\tau'_1, \ldots, \tau'_{s'}$ du *sous-ensemble* $\{1, \ldots, n-1\}$. Mais ce cas est impossible ! Car il impliquerait :

$$\tau'_1 \circ \cdots \circ \tau'_{s'} \ = \ (i\ n),$$

c'est-à-dire qu'une permutation de $\{1, \ldots, n-1\}$ serait égalée à une transformation faisant intervenir l'extraterrestre n — contradiction.

Cas 2 :

$$\mathsf{Id} \ = \ \tau'_1 \circ \cdots \circ \tau'_{s'},$$

avec de même $s' \equiv s \mod 2$, où $\tau'_1, \ldots, \tau'_{s'}$ sont à nouveau des permutations de $\{1, \ldots, n-1\}$. Par récurrence évidente sur n, nous concluons :

$$\begin{aligned} 2 \ &\equiv \ s' \mod 2 \\ &\equiv \ s \mod 2. \end{aligned}$$

□

Ainsi, $s = r + r' \in 2\,\mathbb{N}$ est pair, et il est clair que ceci garantit que $r \equiv r' \mod 2$ comme annoncé. □

Ce théorème justifie alors le fait que la définition suivante ait un sens rigoureux.

Définition 7.4. La *signature* d'une permutation arbitraire $\sigma \in \mathfrak{S}(E)$ est l'élément de $\{-1, +1\}$ noté :

$$\varepsilon(\sigma) \ := \ (-1)^r,$$

où $\tau_1 \circ \cdots \circ \tau_r = \sigma$ est une représentation quelconque de σ comme composition de transpositions.

Théorème 7.5. *Soit E un ensemble fini de cardinal $|E| = n \geqslant 2$.*

(1) *La signature de l'identité vaut $1 = \varepsilon(\mathsf{Id})$.*

(2) *La signature d'une transposition τ vaut toujours $-1 = \varepsilon(\tau)$.*

(3) *Pour toutes permutations $\sigma, \sigma' \in \mathfrak{S}(E)$, on a $\varepsilon\big(\sigma \circ \sigma'\big) = \varepsilon(\sigma) \cdot \varepsilon(\sigma')$.*

(4) *Pour toute permutation $\sigma \in \mathfrak{S}(E)$, on a $\varepsilon\big(\sigma^{-1}\big) = \frac{1}{\varepsilon(\sigma)} = \varepsilon(\sigma)$.*

Ces propriétés expriment notamment que l'application de signature :

$$\begin{aligned} \varepsilon \colon \quad \mathfrak{S}(E) \ &\longrightarrow \ \{-1, +1\} \\ \sigma \ &\longmapsto \ \varepsilon(\sigma), \end{aligned}$$

est un morphisme de groupes, où $\{-1, +1\}$ est muni de la loi de multiplication standard.

Démonstration. Nous ne détaillerons que **(3)**, puisque les autres propriétés sont évidentes. Soient deux représentations :

$$\sigma \,=\, \tau_1 \circ \cdots \circ \tau_r \qquad\qquad \text{et} \qquad\qquad \sigma' \,=\, \tau'_1 \circ \cdots \circ \tau'_{r'},$$

comme compositions de transpositions. Alors leur composition possède la représentation suivante :

$$\sigma \circ \sigma' \,=\, \tau_1 \circ \cdots \circ \tau_r \circ \tau'_1 \circ \cdots \circ \tau'_{r'}$$

et donc on a bien :

$$\varepsilon\big(\sigma \circ \sigma'\big) \,=\, (-1)^{r+r'} \,=\, (-1)^r \cdot (-1)^{r'} \,=\, \varepsilon(\sigma) \cdot \varepsilon(\sigma'). \qquad \square$$

Théorème 7.6. *Soit E un ensemble fini de cardinal $|E| = n \geqslant 2$. Alors la signature :*

$$\varepsilon\colon \quad \mathfrak{S}(E) \;\longrightarrow\; \{-1, +1\},$$

*est l'*unique *morphisme non trivial de groupes :*

$$\xi\colon \quad \mathfrak{S}(E) \;\longrightarrow\; \mathbb{C}^\times.$$

Ici, $\mathbb{C}^\times = \big\{z \in \mathbb{C}\colon\ z \neq 0\big\}$ est le groupe multiplicatif des nombres complexes non nuls, pour la multiplication standard. Évidemment, $\{-1, +1\} \subset \mathbb{C}^\times$. En particulier, ce théorème dit que les seules valeurs possibles d'un morphisme de groupes $\mathfrak{S}(E) \longrightarrow \mathbb{C}^\times$ sont -1 et $+1$.

Démonstration. Soit donc $\xi\colon \mathfrak{S}(E) \longrightarrow \mathbb{C}^\times$ un tel morphisme de groupes. À toute permutation $\sigma \in \mathfrak{S}(E)$, ce morphisme associe un nombre réel non nul $\xi(\sigma) \in \mathbb{C}^\times$. Évidemment, $\xi(\mathsf{Id}) = 1$.

Assertion 7.7. *ξ est constant sur les classes de conjugaison de $\mathfrak{S}(E)$.*

Preuve. En effet, si $\sigma' = \rho\circ\sigma\circ\rho^{-1}$ est conjugué à σ via une certaine permutation $\rho \in \mathfrak{S}(E)$, la commutativité de la multiplication dans $\mathbb{C}^\times$ donne :

$$\begin{aligned} \xi(\sigma') \,&=\, \xi\big(\rho \circ \sigma \circ \rho^{-1}\big) \\ &=\, \xi(\rho)\,\xi(\sigma)\,\xi(\rho^{-1}) \\ &=\, \xi(\rho)\,\tfrac{1}{\xi(\rho)}\,\xi(\sigma) \\ &=\, \xi(\sigma). \end{aligned}$$ $\square$

Assertion 7.8. *Pour toute transposition $\tau \in \mathfrak{S}(E)$, on a $\xi(\tau) = \pm 1$.*

Preuve. Comme $\tau^2 = \mathsf{Id}$, il vient :

$$\xi(\tau)^2 \,=\, \xi(\mathsf{Id}) \,=\, 1. \qquad \square$$

Ensuite, rappelons que d'après le Corollaire 4.4, toutes les transpositions sont conjuguées entre elles, c'est-à-dire forment *une seule* classe de conjugaison.

Assertion 7.9. *$\xi(\tau)$ prend une seule et même valeur sur toutes les transpositions :*

$$\Big(\ \xi(\tau) \,=\, 1 \quad \forall\, \tau \,\in\, \mathfrak{S}(E)\ \Big) \qquad \textit{ou} \qquad \Big(\ \xi(\tau) \,=\, -1 \quad \forall\, \tau \,\in\, \mathfrak{S}(E)\ \Big). \qquad \square$$

La première possibilité $\xi(\tau) = 1$ impliquerait, puisque toute permutation $\sigma = \tau_1 \circ \cdots \circ \tau_r$ s'écrit comme produit de transpositions, que :

$$\xi(\sigma) \,=\, \xi\big(\tau_1 \circ \cdots \circ \tau_r\big) \,=\, \xi(\tau_1) \cdots \xi(\tau_r) \,=\, 1 \cdots 1 \,=\, 1,$$

en contradiction avec l'hypothèse que le morphisme ξ est non trivial.

Donc seule la seconde possibilité est valide, à savoir $\xi(\tau) = -1$ sur toute transposition, et le même calcul conclut la démonstration d'unicité :

$$\begin{aligned} \xi(\sigma) \,&=\, \xi\big(\tau_1 \circ \cdots \circ \tau_r\big) \\ &=\, \xi(\tau_1) \cdots \xi(\tau_r) \\ &=\, (-1) \cdots (-1) \\ &=\, (-1)^r \\ &=\, \varepsilon(\sigma). \end{aligned}$$

□

Proposition 7.10. *La signature d'un p-cycle $\big(a_1 \;\cdots\; a_p\big)$ avec $p \geqslant 2$ est égale à $(-1)^{p-1}$.*

Démonstration. En effet, on sait qu'un p-cycle est composition de $p-1$ transpositions :

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

□

Proposition 7.11. *La signature d'une permutation $\sigma \in \mathfrak{S}(E)$ d'un ensemble E à n éléments vaut :*

$$\varepsilon(\sigma) \,=\, (-1)^{n - \mathrm{N}_\sigma},$$

où N_σ est le nombre total de σ-orbites, y compris celles qui sont réduites à un point.

Démonstration. Soit $\sigma_1 \circ \cdots \circ \sigma_r$ la décomposition de σ en produit de cycles à supports disjoints, gratuitement fournie par le Théorème 3.12. Pour $i = 1, \ldots, r$, notons comme d'habitude $p_i \geqslant 2$ la longueur du cycle σ_i. Ainsi, r est le nombre de σ-orbites non réduites à un point.

Alors comme $p_1 + \cdots + p_r$ est le nombre d'éléments de E qui ne sont pas fixés par σ (wagons qui circulent), il reste :

$$n - \big(p_1 + \cdots + p_r\big),$$

éléments de E qui sont fixés par σ (accompagnateurs restés sur les quais), lesquels sont *chacun* des σ-orbites — réduites à un singleton.

Le nombre total de σ-orbites distinctes est donc égal à :

$$\mathrm{N}_\sigma \,:=\, r + n - \big(p_1 + \cdots + p_r\big).$$

Enfin, une application directe de la Proposition 7.10 précédente conclut :

$$\begin{aligned} \varepsilon(\sigma) \,&=\, \varepsilon(\sigma_1) \cdots \varepsilon(\sigma_r) \\ &=\, (-1)^{p_1 - 1} \cdots (-1)^{p_r - 1} \\ &=\, (-1)^{p_1 + \cdots + p_r - r} \\ &=\, (-1)^{n - \mathrm{N}_\sigma}. \end{aligned}$$

□

Nous pouvons maintenant définir le groupe alterné en toute généralité débridée.

Définition 7.12. Le sous-groupe de $\mathfrak{S}(E)$:

$$\begin{aligned}\mathfrak{A}(E) &:= \mathsf{Ker}\,\varepsilon \\ &= \big\{\sigma \in \mathfrak{S}(E)\colon\ \varepsilon(\sigma) = 1\big\},\end{aligned}$$

est appelé *groupe alterné de* E.

Alors $\mathfrak{A}(E)$ est un sous-groupe *distingué* de $\mathfrak{S}(E)$, comme l'est tout sous-groupe $H = \mathsf{Ker}\, f$ d'un groupe G qui est noyau d'un morphisme de groupes $f\colon G \longrightarrow G'$.

Maintenant, rappelons que l'*indice* $[G\colon H]$ d'un sous-groupe $H \subset G$ d'un groupe abstrait fini G est le cardinal de l'ensemble des classes à gauche (ou à droite) de G modulo H, comme nous l'avons vu dans le chapitre consacré aux groupes abstraits.

Proposition 7.13. *$\mathfrak{A}(E)$ est un sous-groupe de $\mathfrak{S}(E)$ d'indice :*

$$2 \,=\, \big[\mathfrak{S}(E) : \mathfrak{A}(E)\big].$$

Démonstration. En effet, si τ est une transposition quelconque fixée avec $-1 = \varepsilon(\tau) = \varepsilon(\tau^{-1})$, alors pour toute permutation $\sigma \in \mathfrak{S}(E)$, on a :

$$\text{soit } \sigma \in \mathfrak{A}(E), \qquad\qquad \text{soit } \tau^{-1} \circ \sigma \in \mathfrak{A}(E),$$

et donc visiblement, $\mathfrak{A}(E)$ et $\tau\,\mathfrak{A}(E)$ sont les deux seules classes à gauche possibles de $\mathfrak{S}(E)$ modulo $\mathfrak{A}(E)$. □

Ensuite, si nous nous remémorons la formule de la Belle Grange :

$$|G| \,=\, [G : H] \cdot |H|,$$

toujours avec $|E| = n \geqslant 2$, il vient :

$$\begin{aligned}\big|\mathfrak{A}(E)\big| \,&=\, \frac{|\mathfrak{S}(E)|}{[\mathfrak{S}(E) : \mathfrak{A}(E)]} \\ &=\, \frac{n!}{2}.\end{aligned}$$

Pour $n = 2$, comme $\frac{2!}{2} = 1$, le groupe $\mathfrak{A}_2 = \{\mathsf{Id}\}$ est trivial.

Pour $n = 3$, l'Exercice 2 propose de démontrer que $\mathfrak{A}_3$ est engendré par n'importe quel 3-cycle.

Le résultat suivant est classique.

Théorème 7.14. *Soit E un ensemble de cardinal $|E| = n \geqslant 2$. Alors le groupe alterné $\mathfrak{A}(E)$ est l'unique sous-groupe d'indice 2 dans $\mathfrak{S}(E)$.*

Rappelons que dans le chapitre consacré aux groupes abstraits, nous avons démontré que tout sous-groupe $H \subset G$ d'indice $2 = [G : H]$ est nécessairement *distingué*, c'est-à-dire que — sans jamais introduire son auriculaire dans l'une de ses narines — il satisfait $g\,H\,g^{-1} = H$ pour tout élément $g \in G$.

Démonstration. Soit donc $H \subset \mathfrak{S}(E)$ un sous-groupe d'indice $2 = [\mathfrak{S}(E) : H]$. On a alors deux classes à gauche, disons H et $\sigma_0 H$, pour une certaine permutation $\sigma_0 \notin H$.

Toute permutation $\sigma \in \mathfrak{S}(E)$ s'écrit donc de manière unique sous la forme :

$$\sigma \,=\, \sigma_0^m\, h, \qquad\qquad \text{avec} \quad m \in \{0,\, 1\}, \quad \text{et avec} \quad h \in H.$$

Assertion 7.15. *L'application :*

$$f\colon \quad \mathfrak{S}(E) \ \longrightarrow \ \mathbb{C}^{\times},$$

définie par :

$$f\big(\sigma_0^m\, h\big) \ := \ (-1)^m,$$

est un morphisme de groupes.

Cette définition de f et la propriété $H \cap \sigma_0 H \ = \ \emptyset$ des classes à gauche distinctes montrent que :

$$H \ = \ \mathsf{Ker}\, f. \tag{7.16}$$

Preuve. Comme $H \subset \mathfrak{S}(E)$ aux doigts propres est *distingué*, pour tous $m, m' \in \{0,1\}$ et tous $h, h' \in H$, sans écrire les symboles $\circ$ de composition, nous pouvons faire apparaître dans le produit :

$$\begin{aligned}\big(\sigma_0^m\, h\big)\,\big(\sigma_0^{m'}\, h'\big) \ &= \ \sigma_0^{m+m'}\,\Big(\big(\underbrace{\sigma_0^{-m'}\, h\, \sigma_0^{m'}}_{\in\, H}\big)\, h'\Big)\\ &=: \ \sigma_0^{m+m'}\, h'',\end{aligned}$$

un certain élément $h'' \in H$, et par suite, f est bien un morphisme de groupes :

$$\begin{aligned} f\Big(\big(\sigma_0^m\, h\big)\,\big(\sigma_0^{m'}\, h'\big)\Big) \ &= \ f\big(\sigma_0^{m+m'}\, h''\big)\\ &= \ (-1)^{m+m'}\\ &= \ f\big(\sigma_0^m\, h\big)\cdot f\big(\sigma_0^{m'}\, h'\big). \end{aligned} \tag{7.17}$$

□

Observons que notre morphisme f est non trivial, puisque $f(\sigma_0) = -1 \neq 1 = f(\mathsf{Id})$. Donc grâce au Théorème 7.6 d'unicité, $f = \varepsilon$ est nécessairement le morphisme de signature, d'où :

$$\mathsf{Ker}\, f \ = \ \mathsf{Ker}\, \varepsilon \ = \ \mathfrak{A}(E).$$

En comparant avec (7.16), nous concluons bien que $H = \mathfrak{A}(E)$. □

Terminons ce chapitre en exhibant deux systèmes de générateurs pour le groupe alterné $\mathfrak{A}(E)$.

Théorème 7.18. *Soit E un ensemble fini à n élements. Si $n \geqslant 3$, alors le groupe alterné $\mathfrak{A}(E)$ est engendré par chacune des deux familles suivantes :*

(1) *les produits de deux transpositions (non nécessairement à supports disjoints) ;*

(2) *les 3-cycles.*

Démonstration. **(1)** D'après le Théorème 3.19, le groupe $\mathfrak{S}(E)$ est engendré par les transpositions. Pour tout $\sigma \in \mathfrak{S}(E)$, on peut donc écrire :

$$\sigma \ = \ \tau_1 \circ \cdots \circ \tau_r,$$

où chaque τ_i est une transposition.

Or on sait que que $\varepsilon(\sigma) \ = \ (-1)^r$, et donc on a $\sigma \ \in \ \mathfrak{A}(E)$ si et seulement si $r \ \in \ 2\,\mathbb{N}$ est pair. Autrement dit, les éléments de $\mathfrak{A}(E)$ sont les produits d'un nombre *pair* de transpositions. En particulier, les produits de deux transpositions engendrent $\mathfrak{A}(E)$.

(2) Grâce à **(1)**, il suffit de montrer qu'un produit de deux transpositions est un produit de 3-cycles.

Soient donc $\tau_1, \tau_2 \in \mathfrak{S}(E)$ deux transpositions quelconques. Si elles ont même support, alors $\tau_1 = \tau_2$, d'où $\tau_1 \circ \tau_2 = \mathsf{Id}$, et donc il n'y a rien à démontrer. Yep !

Si les supports de τ_1 et de τ_2 ont exactement un élément en commun, alors on peut supposer que :

$$\tau_1 \,=\, \big(a\ b\big) \qquad\qquad \text{et} \qquad\qquad \tau_2 \,=\, \big(b\ c\big),$$

avec $a, b, c \in E$ distincts deux à deux. Par le calcul, on constate alors que la composition de ces deux transpositions est un 3-cycle :

$$\begin{array}{rccc} & a & b & c \\ \tau_2 & \downarrow & \downarrow & \downarrow \\ & a & c & b \\ \tau_1 & \downarrow & \downarrow & \downarrow \\ & b & c & a \end{array} \qquad\qquad \text{montre que} \qquad\qquad \tau_1 \circ \tau_2 \,=\, \big(a\ b\ c\big).$$

Enfin, si les supports de τ_1 et τ_2 n'ont aucun élément en commun, on peut écrire :

$$\tau_1 \,=\, \big(a\ b\big) \qquad\qquad \text{et} \qquad\qquad \tau_2 \,=\, \big(c\ d\big),$$

avec $a, b, c, d \in E$ distincts deux à deux. Par le calcul, on constate alors que la composition de ces deux transpositions

$$\begin{array}{rcccc} & a & b & c & d \\ (c\ d) & \downarrow & \downarrow & \downarrow & \downarrow \\ & a & b & c & d \\ (a\ b) & \downarrow & \downarrow & \downarrow & \downarrow \\ & b & a & d & c \end{array}$$

s'identifie à la composition des deux 3-cycles suivants :

$$\begin{array}{rcccc} & a & b & c & d \\ (a\ c\ d) & \downarrow & \downarrow & \downarrow & \downarrow \\ & c & b & d & a \\ (a\ c\ b) & \downarrow & \downarrow & \downarrow & \downarrow \\ & b & a & d & c \end{array}$$

c'est-à-dire :

$$\big(a\ b\big) \circ \big(c\ d\big) \,=\, \big(a\ c\ b\big) \circ \big(a\ c\ d\big). \qquad \square$$

8. Exercices

Exercice 1. Sur l'ensemble $\{1, 2, 3, 4\}$, trouver une transposition et un 4-cycle qui n'engendrent *pas* $\mathfrak{S}_4$.

Exercice 2. Sur l'ensemble $\{1, 2, 3\}$, montrer que le groupe alterné $\mathfrak{A}_3$ est engendré par le 3-cycle $(1\ 2\ 3)$.