Lycée Henri IV
MPSI

Cours
Durée : 4 h 15

GROUPE SYMÉTRIQUE

Les énoncés et parties suivis du symbole [✠] ne seront pas traités en cours.

Prérequis

Revoir les chapitre sur :

- la théorie des applications ;
- les structures algébriques.

Dans tout ce chapitre, les lettres $n, m, p, q, r, i, j, k, \ell$ désignent des entiers naturels (dont on suppose parfois implicitement qu'ils sont non nuls).

Les trois lettres AQT signifient « Âne Qui Trotte » et sont utilisées pour désigner une démonstration facile laissée au lecteur.

A. Compléments sur les groupes

A.1. Groupes finis

Le langage des structures algébriques a son vocabulaire propre. La définition suivante introduit la notion d'ordre d'un groupe qui est redondante avec celle de cardinal dans la théorie des ensembles.

Définition 1

Si $(G,*)$ est un groupe fini, on appelle ordre de G le cardinal de G.

Un sous-groupe étant un groupe, on peut parler de son ordre.

Voici le très joli théorème de Lagrange sur l'ordre des sous-groupes d'un groupe fini.

Théorème 1

Soient $(G,*)$ un groupe fini et H un sous-groupe de G. Alors l'ordre de H divise l'ordre de G.

■ Sur G, on considère la relation définie par $\forall g_1, g_2 \in G,\ (g_1 \sim g_2) \iff (g_1 {g_2}^{-1} \in H)$. Vérifions que $\sim$ est une relation d'équivalence.

- ▷ Pour tout $g \in G$, on a $g \sim g$ car $g g^{-1} = e_G \in H$. Donc $\sim$ est réflexive.
- ▷ Soient $g_1, g_2, g_3 \in G$ tels que $g_1 \sim g_2$ et $g_2 \sim g_3$ de sorte que $g_1 {g_2}^{-1} \in H$ et $g_2 {g_3}^{-1} \in H$. Alors $g_1 {g_2}^{-1} g_2 {g_3}^{-1} \in H$, c'est-à-dire $g_1 {g_3}^{-1} \in H$ ou encore $g_1 \sim g_3$. Donc $\sim$ est transitive.
- ▷ Soient $g_1, g_2 \in G$ tels que $g_1 \sim g_2$ de sorte que $g_1 {g_2}^{-1} \in H$. Alors $(g_1 {g_2}^{-1})^{-1} \in H$, c'est-à-dire $g_2 {g_1}^{-1} \in H$ ou encore $g_2 \sim g_1$. Donc $\sim$ est symétrique.

On sait que les classes d'équivalence de la relation $\sim$ forment une partition de G. De plus, si g désigne un élément de G, sa classe d'équivalence est $Hg = \{hg : h \in H\}$. En particulier, H est la classe d'équivalence de e_G.

Or, pour tout $g \in G$, l'application δ_g de H dans Hg définie par $h \longmapsto hg$ est une bijection (sa réciproque est $\delta_{g^{-1}}$), donc $\operatorname{card} Hg = \operatorname{card} H$ pour tout g. Cela signifie que toutes les classes d'équivalence ont le même cardinal, à savoir $\operatorname{card} H$.

Dès lors, si m désigne le nombre de classes d'équivalence, on a $\operatorname{card} G = m \operatorname{card} H$, ce qui démontre notre résultat. ■

Exemples :

- Il n'existe pas de sous-groupe à 10 éléments dans $(\mathbb{Z}/24\mathbb{Z}, +)$.

Le théorème de Lagrange ne dit pas qu'il existe un sous-groupe d'ordre d pour chaque diviseur d de n. Le résultat est d'ailleurs faux. Les énoncés dans ce sens sont nettement plus difficiles (théorèmes de Sylow).

A.2. Sous-groupes engendrés

a) Sous-groupe engendré par une partie

Définition 2

Soient $(G,*)$ un groupe et A une partie de G. L'intersection de tous les sous-groupes de $(G,*)$ qui contiennent A est un sous-groupe de $(G,*)$, appelé sous-groupe engendré par A dans G. On le note $\langle A\rangle$. C'est (au sens de l'inclusion) le plus petit sous-groupe de G qui contient A.

■ On a vu qu'une intersection quelconque de sous-groupes est un sous-groupe, donc $\langle A\rangle$ est bien un sous-groupe de $(G,*)$. C'est aussi clairement le plus petit au sens de l'inclusion. ■

La minimalité de $\langle A\rangle$ parmi les sous-groupes contenant A se traduit en disant que si un sous-groupe H contient la partie A, alors H contient nécessairement $\langle A\rangle$.

Exemples :

- $\langle\varnothing\rangle = \{e_G\}$.
- Si H est un sous-groupe de G, alors $\langle H\rangle = H$. En particulier, $\langle e_G\rangle = \{e_G\}$ et $\langle G\rangle = G$.
- Dans $(\mathbb{Z},+)$, le sous groupe engendré par $\{3\}$ est $3\mathbb{Z}$ et le sous-groupe engendré par $\{6,10\}$ est $6\mathbb{Z}+10\mathbb{Z} = (6\wedge 10)\mathbb{Z} = 2\mathbb{Z}$.

On peut donner la description suivante d'un sous-groupe engendré par une partie.

Proposition 1

Soient $(G,*)$ un groupe et A une partie de G. Alors

$$\langle A\rangle = \left\{g\in G : \exists n\in\mathbb{N},\ \exists(a_1,\dots,a_n)\in A^n,\ \exists(\varepsilon_1,\dots,\varepsilon_n)\in\{-1;1\}^n,\ g = {a_1}^{\varepsilon_1}{a_2}^{\varepsilon_2}\dots{a_n}^{\varepsilon_n}\right\}.$$

■ Posons $H = \left\{g\in G : \exists n\in\mathbb{N},\ \exists(a_1,\dots,a_n)\in A^n,\ \exists(\varepsilon_1,\dots,\varepsilon_n)\in\{-1;1\}^n,\ g = {a_1}^{\varepsilon_1}{a_2}^{\varepsilon_2}\dots{a_n}^{\varepsilon_n}\right\}$.

Comme $\langle A\rangle$ doit nécessairement contenir tous les produits d'éléments de A ou de leurs inverses, on a nécessairement $H\subset\langle A\rangle$.

Pour conclure, il suffit de démontrer que H est un sous-groupe de G. Il est clair que $e_G\in H$ (en prenant $n=0$, on voit que le produit vide appartient à H, c'est-à-dire $e_G\in H$). Si g_1,g_2 sont dans H, alors d'une part il existe $n\in\mathbb{N}$, $(a_1,\dots,a_n)\in A^n$ et $(\varepsilon_1,\dots,\varepsilon_n)\in\{-1;1\}^n$ tels que $g_1 = {a_1}^{\varepsilon_1}{a_2}^{\varepsilon_2}\dots{a_n}^{\varepsilon_n}$ et, d'autre part, il existe $m\in\mathbb{N}$, $(b_1,\dots,b_m)\in A^m$ et $(\delta_1,\dots,\delta_m)\in\{-1;1\}^m$ tels que $g_2 = {b_1}^{\delta_1}{b_2}^{\delta_2}\dots{b_n}^{\delta_n}$, donc $g_1{g_2}^{-1} = {a_1}^{\varepsilon_1}{a_2}^{\varepsilon_2}\dots{a_n}^{\varepsilon_n}{b_1}^{-\delta_1}{b_2}^{-\delta_2}\dots{b_n}^{-\delta_n}$, ce qui démontre que $g_1{g_2}^{-1}\in H$. Donc H est bien un sous-groupe de G. ■

b) Groupes monogènes et cycliques

Lorsqu'un groupe est engendré par une partie finie, on dit que ce groupe est de type fini. Nous nous intéressons dans ce paragraphe au cas particulier où il suffit d'un seul élément pour engendrer le groupe.

Définition 3

Un groupe $(G, *)$ est dit monogène s'il existe un élément $g \in G$ tel que $G = \langle g \rangle$. Un tel élément g est alors appelé un générateur du groupe G.

Notons que les groupes monogènes sont nécessairement abéliens. En effet, dans un groupe monogène de générateur g, tout élément s'écrit g^n où $n \in \mathbb{Z}$ donc tous les éléments commutent.

Si g est un générateur d'un groupe, alors g^{-1} en est un autre.

Un sous-groupe étant un groupe, on peut s'intéresser au caractère monogène d'un sous-groupe.

Exemples :

- $(\mathbb{Z}, +)$ est un groupe monogène engendré par -1 ou $+1$.
  Tout sous-groupe non trivial de $\mathbb{Z}$ est monogène et engendré par son plus petit élément strictement positif.
- $(\mathbb{R}, +)$ n'est pas un groupe monogène.
  Nous avons vu que les sous-groupes de $(\mathbb{R}, +)$ sont ou bien monogènes ou bien denses dans $\mathbb{R}$.

On a $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ mais cette écriture est trompeuse : elle ne signifie pas que $\langle g \rangle$ est infini car les puissances de g peuvent être égales. Un groupe monogène peut donc n'avoir qu'un nombre fini d'éléments, ce qui nous conduit à introduire la notion suivante.

Définition 4

Un groupe monogène et fini est dit cyclique.

Un sous-groupe étant un groupe, on peut s'intéresser au caractère cyclique d'un sous-groupe.

Exemples :

- Pour tout $n \in \mathbb{N}^*$, on a $\mathbb{Z}/n\mathbb{Z} = \{1, 1+1, \ldots, 1+\cdots+1 \ (n \text{ fois})\}$, ce qui signifie que $\mathbb{Z}/n\mathbb{Z}$ est un groupe additif cyclique d'ordre n engendré par 1.
- Pour tout $n \in \mathbb{N}^*$, le groupe $(\mathbb{U}_n, \times)$ des racines n-ème de l'unité est cyclique. Il est engendré par $e^{2i\pi/n}$.

A.3. Ordre d'un élément

Définition 5

Soient $(G,*)$ un groupe et g un élément de G.

S'il existe un entier $n \in \mathbb{N}^*$ tel que $g^n = e_G$, on dit que g est d'ordre fini dans G. Le plus petit entier $n_0 \in \mathbb{N}^*$ tel que $g^{n_0} = e_G$ est alors appelé l'ordre de g et il est noté $\omega(g)$.

Si, pour tout entier $n \in \mathbb{N}^*$, on a $g^n \neq e_G$, on dit que g est d'ordre infini dans G et on pose $\omega(g) = +\infty$.

L'ordre de g est donc défini par $\omega(g) = \inf\{n \in \mathbb{N}^* : g^n = e_G\}$ où la borne inférieure est déterminée dans $\mathbb{N}^* \cup \{+\infty\}$

Lorsque le groupe est additif, on a $\omega(g) = \inf\{n \in \mathbb{N}^* : ng = 0\}$.

Exemples :

- On a $\omega(e_G) = 1$. En fait, e_G est même le seul élément d'ordre 1.
- Un élément d'ordre 2 est un élément qui est égal à son symétrique (et distinct de l'élément neutre).
- Un groupe d'ordre infini peut avoir des éléments d'ordre fini. Par exemple, dans $(\mathbb{R}^*, \times)$, l'élément -1 est d'ordre 2.

Il est possible de définir l'ordre d'un élément g de manière plus algébrique. L'application φ_g de $\mathbb{Z}$ dans G définie par $n \longmapsto g^n$ est un morphisme de groupe dont le noyau est un sous-groupe de $(\mathbb{Z},+)$. Ce noyau est donc de la forme $m\mathbb{Z}$. Si $m = 0$, φ_g est injectif et g est d'ordre infini et si $m \neq 0$, alors m est l'ordre de g.

Cette façon de définir l'ordre d'un élément g permet de caractériser les entiers n tel que $g^n = e_G$.

Proposition 2

Soient $(G,*)$ un groupe, g un élément de G et $m \in \mathbb{N}^*$. On a $g^m = e_G$ si, et seulement si, $\omega(g)$ divise m.

■ Considérons φ_g le morphisme de $(\mathbb{Z},+)$ dans $(G,*)$ tel que $\varphi_g(m) = g^m$ pour tout $m \in \mathbb{Z}$. On a alors $(g^m = e_G) \iff (m \in \operatorname{Ker}\varphi) \iff (m \in \omega(g)\mathbb{Z})$, ce qui correspond au résultat attendu. ■

On peut relier l'ordre d'un élément à l'ordre du sous-groupe qu'il engendre (ce qui explique la terminologie commune).

Proposition 3

Soient $(G,*)$ un groupe et g un élément de G. Alors g est d'ordre fini si, et seulement si, $\langle g\rangle$ est un groupe cyclique d'ordre $\omega(g)$. Dans ce cas, on a $\langle g\rangle = \{e_G, g, g^2, \ldots, g^{\omega(g)-1}\}$.

■ $\Rightarrow$ Supposons que $\omega(g)$ est fini. On vérifie alors sans difficulté que $\{e_G, g, g^2, \ldots, g^{\omega(g)-1}\}$ est un sous-groupe de G, que c'est le plus petit qui contient g et que tous ses éléments sont distincts. Donc $\langle g\rangle = \{e_G, g, g^2, \ldots, g^{\omega(g)-1}\}$ et l'ordre de $\langle g\rangle$ est $\omega(g)$.

$\Leftarrow$ Si l'on suppose que $\omega(g) = +\infty$, alors le morphisme de groupes de $\mathbb{Z}$ dans G défini par $n \longmapsto g^n$ est injectif (si $n \in \mathbb{N} \cap \operatorname{Ker}\varphi$, on a $g^n = e_G$ ce qui est impossible et si $n \in \mathbb{Z}_- \cap \operatorname{Ker}\varphi$, on a $g^{-n} = {e_G}^{-1} = e_G$ ce qui est également impossible). Il s'ensuit que $\langle g\rangle$ est infini (et même isomorphe à $\mathbb{Z}$). ■

On peut alors donner une description des groupes monogènes.

Corollaire 1

Si $(G, *)$ est un groupe monogène infini, alors G est isomorphe à $\mathbb{Z}$. Plus précisément, si g est un générateur de G (d'ordre infini nécessairement), alors $G = \{g^n : n \in \mathbb{Z}\}$ et l'application $g^n \longmapsto n$ est alors un isomorphisme de groupes entre G et $\mathbb{Z}$.

Si $(G, *)$ est un groupe cyclique, alors G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Plus précisément, si g est un générateur de G (d'ordre fini nécessairement), alors $G = \{e_G, g, g^2, \ldots, g^{\omega(g)-1}\}$ et l'application $g^n \longmapsto n \ [\text{mod } \omega(g)]$ est alors un isomorphisme de groupes entre G et $\mathbb{Z}/n\mathbb{Z}$.

■ AQT ■

En associant le théorème de Lagrange et la proposition 3, on obtient le résultat suivant.

Proposition 4

L'ordre d'un groupe fini est un multiple de l'ordre de n'importe lequel de ses éléments.

■ Soit $(G, *)$ un groupe d'ordre $n \in \mathbb{N}^*$. Soit $g \in G$. Le sous-groupe $\langle g \rangle$ est alors d'ordre $\omega(g)$. Le théorème de Lagrange nous dit alors que $\omega(g)$ divise n. ■

Ce résultat nous dit, en particulier, que tout élément g d'un groupe fini G d'ordre n est d'ordre fini et $g^n = e_G$.

Exemples :

- Un groupe dont l'ordre est un nombre premier est cyclique.
  En effet, si G est un groupe d'ordre p premier et si g est un élément de G tel que $g \neq e_G$, alors l'ordre de g divise p et n'est pas égal à 1, donc g est d'ordre p, ce qui donne $G = \langle g \rangle$.

B. Groupe symétrique

L'objectif de ce cours est d'étudier l'ensemble $\mathfrak{S}_E$ des permutations d'un ensemble fini E, c'est-à-dire l'ensemble des bijections de E dans E. Comme E est en bijection avec $[\![1;n]\!]$, il est équivalent d'étudier les permutations de $[\![1;n]\!]$, où $n \in \mathbb{N}^*$.

B.1. Permutations d'un ensemble fini

a) Définitions et notations

Définition 6

On note $\mathfrak{S}_n$ l'ensemble des permutations de l'ensemble $[\![1;n]\!]$, c'est-à-dire l'ensemble des bijections de $[\![1;n]\!]$ dans lui-même.

On représente un élément σ de $\mathfrak{S}_n$ par la liste des éléments de $[\![1;n]\!]$ en dessous de laquelle on indique l'image de chaque élément :

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

La lettre $\mathfrak{S}$ est un S majuscule gothique.

L'identité $\mathrm{Id}_{[\![1;n]\!]}$ est une permutation de $[\![1;n]\!]$ que nous noterons Id.

Remarquons que $\mathfrak{S}_1 = \{\mathrm{Id}\}$. Par conséquent, nous supposerons souvent que $n \geqslant 2$.

Exemples :

- La notation
$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix}$$
désigne la permutation σ de $[\![1;n]\!]$ telle que $\sigma_0(1) = 2$, $\sigma_0(2) = 6$, $\sigma_0(3) = 3$, $\sigma_0(4) = 4$, $\sigma_0(5) = 4$ et $\sigma_0(6) = 1$.

Les éléments de $[\![1;n]\!]$ qui restent invariants par une permutation jouent un rôle important dans l'étude de cette permutation.

Définition 7

Soit $\sigma \in \mathfrak{S}_n$. Un point fixe de σ est un élément i de $[\![1;n]\!]$ tel que $\sigma(i) = i$.

Le support d'une permutation est l'ensemble $[\![1;n]\!]$ privé des points fixes de σ. On le note $\mathrm{supp}(\sigma)$.

Exemples :

- La permutation σ_0 de l'exemple précédent admet un unique point fixe : 3. Son support est $\{1, 2, 4, 5, 6\}$.

b) Structure de $\mathfrak{S}_n$

Définition 8

La composée de deux permutations σ et ρ de $[\![1;n]\!]$ est une permutation de $[\![1;n]\!]$ que l'on note $\sigma\rho$ plutôt que $\sigma \circ \rho$ et que l'on appelle produit des deux permutations.

■ Le fait que la composée de deux bijections de $[\![1;n]\!]$ dans lui-même soit une bijection de $[\![1;n]\!]$ dans lui-même est un résultat général sur la composition des applications bijectives. ■

La notation adoptée pour représenter les permutations rend très facile le calcul du produit de deux permutations. Il faut juste faire attention à l'ordre d'action dans le produit $\sigma\rho$: comme toujours avec la loi $\circ$, on commence par faire agir ρ puis σ.

Exemples :

- Si
$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix} \quad \text{et} \quad \rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$
on a
$$\sigma_0\rho_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 2 & 3 & 6 \end{pmatrix}$$
et
$$\rho_0\sigma_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 4 & 3 & 1 & 6 \end{pmatrix}.$$
On constate au passage qu'en général deux permutations ne commutent pas.

La proposition suivante donne la structure de $\mathfrak{S}_n$.

Proposition 5

$\mathfrak{S}_n$ est un groupe pour la loi $\circ$, appelé groupe symétrique d'indice n. C'est un groupe fini d'ordre $n!$ qui n'est pas abélien dès que $n \geqslant 3$.

■ Nous savons déjà tout cela. ■

Remarquons que deux permutations de $[\![1;n]\!]$ dont les supports sont disjoints commutent. Mais attention, ce n'est qu'une condition suffisante pour que deux permutations commutent. La réciproque est évidemment fausse puisqu'une permutation commute toujours avec elle-même.

On dispose de toutes les définitions et tous les résultats sur les groupes finis pour étudier $\mathfrak{S}_n$. On peut, en particulier, parler de l'ordre d'une permutation.

Définition 9

L'ordre d'une permutation $\sigma \in \mathfrak{S}_n$ est le plus petit entier naturel non nul k tel que $\sigma^k = \mathrm{Id}$.

Exemples :

- Si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$, on a $\sigma \neq \mathrm{Id}$, $\sigma^2 \neq \mathrm{Id}$ et $\sigma^3 = \mathrm{Id}$ donc $\omega(\sigma) = 3$.

L'ordre d'une permutation est un diviseur de $n!$ (puisque c'est l'ordre de $\mathfrak{S}_n$).

c) Conjugaison

Définition 10

Soient σ_1 et σ_2 deux permutations de $\mathfrak{S}_n$. On dit que σ_1 et σ_2 sont conjuguées s'il existe une permutation ρ telle que $\sigma_1 = \rho\sigma_2\rho^{-1}$. On définit ainsi la relation de conjugaison sur $\mathfrak{S}_n$.

Exemples :

- Id n'est conjuguée qu'avec elle-même.

La proposition suivante donne les propriétés de la conjugaison.

Proposition 6

La conjugaison est une relation d'équivalence sur $\mathfrak{S}_n$.

De plus, l'application de conjugaison par une permutation fixée ρ de $\mathfrak{S}_n$, définie par

$$\left\{ \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathfrak{S}_n \\ \sigma & \longmapsto & \rho\sigma\rho^{-1} \end{array} \right.$$

est un automorphisme de groupes, appelé automorphisme intérieur de $\mathfrak{S}_n$.

■ AQT ■

B. 2. Décomposition d'une permutation

a) Décomposition en produit de transpositions

Définition 11

On appelle transposition de $[\![1;n]\!]$ une permutation τ de $\mathfrak{S}_n$ qui échange deux éléments distincts en laissant fixes tous les autres.

On note $\tau = (i,j)_n$, ou (i,j) s'il n'y a pas d'ambiguïté, la transposition de $[\![1;n]\!]$ qui échange i et j (avec $i \neq j$).

$\mathfrak{S}_n$ contient $\binom{n}{2}$ transpositions. En particulier, $\mathfrak{S}_1$ ne contient pas de transposition.

Exemples :

- $(2,5)_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$.

On peut immédiatement donner l'ordre d'une transposition dans le groupe $\mathfrak{S}_n$.

Proposition 7

Une transposition de $[\![1;n]\!]$ est d'ordre 2. Autrement dit, elle est sa propre inverse : c'est une involution.

■ On vérifie sans difficulté que $(i,j)(i,j) = \mathrm{Id}$ pour tous $i,j \in [\![1;n]\!]$ tels que $i \neq j$. ■

Attention, un élément de $\mathfrak{S}_n$ qui est d'ordre 2 n'est pas nécessairement une transposition, comme le montre le produit $(1,2)(3,4)$ de deux transpositions de $[\![1;4]\!]$.

On peut alors énoncer le théorème de décomposition en produit de transpositions.

Théorème 2

Les transpositions de $[\![1;n]\!]$ engendrent le groupe $\mathfrak{S}_n$. Autrement dit, toute permutation de $[\![1;n]\!]$ est décomposable en un produit de transpositions.

Il n'y a pas du tout unicité de la décomposition. De plus, les transpositions qui interviennent dans la décomposition ne commutent pas nécessairement.

■ Pour $n \in \mathbb{N}^*$, on note $\mathscr{P}(n)$: « tout élément de $\mathfrak{S}_n$ se décompose en un produit de transpositions ».

Initialisation :
Si $n = 1$, l'ensemble des transpositions de $\mathfrak{S}_1$ est vide et l'on a bien $\mathfrak{S}_1 = \{\mathrm{Id}\} = \langle \varnothing \rangle$.
Si $n = 2$, $\mathfrak{S}_2$ contient une seule transposition $\tau = (1,2)$ qui l'engendre car $\mathfrak{S}_2 = \{\mathrm{Id}, \tau\}$ et $\tau^2 = \mathrm{Id}$.

Hérédité :
Soit $n \geqslant 2$ tel que $\mathfrak{S}_n$ soit engendré par les transpositions de $[\![1;n]\!]$. Il faut montrer que tout élément de $\mathfrak{S}_{n+1}$ est un produit de transpositions de $[\![1;n+1]\!]$. Soit $\sigma \in \mathfrak{S}_{n+1}$. Distinguons deux cas :

- Si $\sigma(n+1) = n+1$, la restriction σ'de σ à $[\![1;n]\!]$ est un élément de $\mathfrak{S}_n$. C'est donc un produit de k transpositions de $[\![1;n]\!]$: $\sigma' = (i_k,j_k)_n \cdots (i_2,j_2)_n (i_1,j_1)_n$. Chacune de ces transpositions se prolonge à $[\![1;n+1]\!]$ en fixant $n+1$. On a alors $\sigma = (i_k,j_k)_{n+1} \cdots (i_2,j_2)_{n+1}(i_1,j_1)_{n+1}$.
- Si $\sigma(n+1) = p \neq n+1$, la permutation $\rho = (p,n+1)_{n+1}\sigma$ laisse $n+1$ invariant. D'après ce qui précède, ρ est donc un produit de k transpositions de $[\![1;n+1]\!]$. Alors $\tau = (p,n+1)_{n+1}\rho$ est un produit de $k+1$ transpositions de $[\![1;n+1]\!]$.

Conclusion :
D'après le principe de récurrence, la propriété est vraie pour tout $n \geqslant 1$. ■

Concrètement, cela signifie que, pour remettre en ordre un jeu de cartes mélangées, on peut le faire en permutant les cartes deux par deux.

L'encadré ci-dessous explique comment décomposer en pratique une permutation en un produit de transpositions.

Décomposition en produit de transpositions

La démonstration précédente fournit un algorithme pour décomposer une permutation quelconque en un produit de transpositions : on remet les éléments $1, \ldots, n$ dans l'ordre, en en mettant au moins un à sa place à chaque étape. Cela permet de décomposer n'importe quelle permutation en un produit d'au plus n transpositions (au moins d'une façon).

Exemples :

- On a

$$\begin{aligned}
\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 4 & 1 & 2 \end{pmatrix} &= (2,5) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix} \\
&= (2,5)(1,4) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \\
&= (2,5)(1,4)(1,3) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \\
&= (2,5)(1,4)(1,3)(1,2).
\end{aligned}$$

Le procédé de décomposition en produit de transpositions permet de se convaincre que cette décomposition n'est pas unique. Même le nombre de transpositions nécessaires n'est pas fixé ! Nous verrons cependant que la parité de ce nombre de transpositions est une caractéristique de la permutation. Ainsi, la permutation ci-dessus a été décomposée en un produit de 4 transpositions et il aurait été possible de le faire en 6 ou 8 transpositions ; par contre, elle ne pourra jamais l'être en 5 ou 7 transpositions.

b) Décomposition en cycles

Définition 12

On appelle cycle de $[\![1;n]\!]$ une permutation c de $\mathfrak{S}_n$ pour laquelle il existe un entier $2 \leqslant p \leqslant n$ et une suite $(a_1, \dots, a_p)$ d'éléments de $[\![1;n]\!]$ distincts deux à deux tels que

(i) $\forall i \in [\![1; p-1]\!]\,, \quad c(a_i) = a_{i+1}\,;$

(ii) $c(a_p) = a_1\,;$

(iii) $\forall \ell \in [\![1;n]\!] \setminus \{a_1, \dots, a_p\}, \quad c(\ell) = \ell.$

On adopte la notation $c = (a_1, a_2, \dots, a_p)_n$, ou $c = (a_1, a_2, \dots, a_p)$ s'il n'y a pas ambiguïté, pour désigner ce cycle. On dit que c est un cycle de longueur p ou encore que c'est un p-cycle.

La notation $c = (a_1, a_2, \dots, a_p)$ signifie que tout élément (sauf le dernier) est envoyé sur l'élément suivant et que le dernier est envoyé sur le premier. C'est une écriture Pac-Man :-)

Par conséquent, on a $(a_1, a_2, \dots, a_{p-1}, a_p) = (a_2, a_3 \dots, a_p, a_1) = (a_3, a_4, \dots, a_1, a_2) = \cdots$

Un cycle de longueur n est parfois appelé une permutation circulaire.

Les cycles de longueur 1 n'existent pas !

Exemples :

- Une transposition est un 2-cycle.
- $(1,3,4)_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 4 & 1 & 5 \end{pmatrix}$.
- Id n'est pas un cycle (dès que $n \geqslant 2$).
- Si $\sigma = (1,2,3,4,5,6)$ alors $\sigma^2 = (1,3,5)(2,4,6)$. On constate ainsi que les puissances d'un cycle ne sont pas toujours des cycles !

La proposition suivante rassemble les propriétés élémentaires des cycles.

Proposition 8

Soit $(a_1, a_2, \dots, a_p)$ un p-cycle de $[\![1;n]\!]$. Alors

(i) $\operatorname{supp}\big((a_1, a_2, \dots, a_p)\big) = \{a_1, a_2, \dots, a_p\}\,;$

(ii) $\omega\big((a_1, a_2, \dots, a_p)\big) = p\,;$

(iii) $(a_1, a_2, \dots, a_{p-1}, a_p)^{-1} = (a_p, a_{p-1}, \dots, a_2, a_1)\,;$

(iv) $\forall \sigma \in \mathfrak{S}_n, \quad \sigma(a_1, a_2, \dots, a_p)\sigma^{-1} = \big(\sigma(a_1), \sigma(a_2), \dots, \sigma(a_p)\big).$

■ AQT ■

La propriété (iv) est généralement appelée la formule de conjugaison. Nous allons voir, dans l'énoncé qui suit, qu'elle permet de démontrer que, pour un entier $p \geqslant 2$ fixé, tous les p-cycles sont dans la même classe de conjugaison.

Corollaire 2

Soit $p \geqslant 2$. Deux p-cycles de $\mathfrak{S}_n$ sont toujours conjugués.

■ Soit $c = (a_1, a_2, \dots, a_p)$ un p-cycle de $[\![1;n]\!]$. Si l'on considère une permutation $\rho \in \mathfrak{S}_n$ telle que $\forall i \in [\![1;p]\!]\,,\ \rho(a_i) = i$ (peu importe comment agit ρ en dehors du support de c), on a $c = \rho^{-1}\gamma\rho$. On démontre ainsi que tout p-cycle est conjugué avec γ et donc, par transitivité de la conjugaison, que tous les p-cycles sont conjugués. ■

On peut alors énoncer le théorème de décomposition en produit de cycles.

Théorème 3

Toute permutation de $[\![1;n]\!]$ est décomposable en un produit de cycles à supports deux à deux disjoints (Id se décompose en un produit vide de cycles). Cette décomposition est unique, à l'ordre près des cycles (les cycles commutent deux à deux puisqu'ils sont à supports disjoints).

■ Cf annexe. ■

En abrégé, on dit souvent « cycles disjoints » pour « cycles à supports deux à deux disjoints ».

L'encadré ci-dessous explique comment décomposer en pratique une permutation en un produit de cycles à supports disjoints.

Décomposition en produit de cycles

Pour décomposer une permutation σ en un produit de cycles à support disjoints, on part d'un élément a du support de σ et l'on écrit la suite $\sigma^k(a)$ pour $k = 1, 2, \ldots, \omega(a) - 1$, ce qui donne le cycle $c_1 = \big(a, \sigma(a), \ldots, \sigma^{\omega(a)-1}(a)\big)$. S'il reste un élément b du support de σ qui n'appartient pas au cycle c_1, on réitère ce processus avec b. Et ainsi de suite jusqu'à l'épuisement du support de σ.

On notera que les points fixes de σ n'apparaissent pas dans les cycles de la décomposition.

Exemples :

- On a

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

B.3. Signature

a) Définitions et premières propriétés

Définition 13

Soit $\sigma \in \mathfrak{S}_n$. On appelle inversion de σ tout paire $\{i,j\}$ d'éléments de $[\![1;n]\!]$ telle que

$$\frac{\sigma(i)-\sigma(j)}{i-j} < 0,$$

c'est-à-dire telle que $\sigma(i)$ et $\sigma(j)$ soient classés dans l'ordre inverse de i et j.

On note $I(\sigma)$ le nombre d'inversions de σ.

Exemples :

- Les inversions de $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ sont $\{1;4\}$, $\{2;4\}$ et $\{3;4\}$, d'où $I(\sigma_1) = 3$.

Le nombre d'inversions d'une permutation permet de définir sa signature.

Définition 14

On appelle signature d'une permutation σ de $\mathfrak{S}_n$, le nombre réel $(-1)^{I(\sigma)}$.

Une permutation paire est une permutation de signature 1, c'est-à-dire une permutation dont le nombre d'inversions est pair.

Une permutation impaire est une permutation de signature -1, c'est-à-dire une permutation dont le nombre d'inversions est impair.

Exemples :

- $\varepsilon(\mathrm{Id}) = 1$.
- Pour la permutation σ_1 de l'exemple précédent, on a $\varepsilon(\sigma_1) = -1$.

L'intérêt de la notion de signature réside dans la proposition suivante.

Proposition 9

L'application

$$\varepsilon \left\{ \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \{-1;+1\} \\ \sigma & \longmapsto & \varepsilon(\sigma) = (-1)^{I(\sigma)} \end{array} \right.$$

est un morphisme de groupes de $(\mathfrak{S}_n, \circ)$ dans $(\{-1;+1\}, \times)$. Autrement dit, la signature d'un produit de permutations est le produit des signatures.

■ Soient σ et ρ deux permutations de $[\![1;n]\!]$. Les inversions du produit $\rho\sigma$ sont :

▷ les inversions $\{i;j\}$ de σ telles que $\{\sigma(i);\sigma(j)\}$ ne soit pas une inversion de ρ ;

▷ les paires $\{i;j\}$ qui ne sont pas des inversions de σ telles que $\{\sigma(i);\sigma(j)\}$ soit une inversion de ρ.

Si l'on ajoute les nombres d'inversions de σ et ρ, on compte deux fois le nombre N d'inversions $\{i;j\}$ de σ telles que $\{\sigma(i);\sigma(j)\}$ soit une inversion de ρ. Donc $I(\rho\sigma) = I(\rho) + I(\sigma) - 2N$, ce qui donne

$$\varepsilon(\rho\sigma) = (-1)^{I(\rho)+I(\sigma)-2N} = (-1)^{I(\rho)}(-1)^{I(\sigma)} = \varepsilon(\rho)\varepsilon(\sigma).$$

Donc ε est bien un morphisme de groupes de $(\mathfrak{S}_n, \circ)$ dans $(\{-1;+1\}, \times)$. ■

La signature vérifie donc une « règle des signes » : le produit de deux permutations de même parité est paire et le produit de deux permutations de parités différentes est impaire.

Les propriétés générales des morphismes de groupes impliquent les résultats de l'énoncé suivant.

Corollaire 3

On a

(i) une permutation et son inverse ont la même signature :
$$\forall \sigma \in \mathfrak{S}_n, \quad \varepsilon(\sigma^{-1}) = \varepsilon(\sigma)\,;$$

(ii) deux permutations conjuguées ont la même signature :
$$\forall \sigma, \rho \in \mathfrak{S}_n, \quad \varepsilon(\rho^{-1}\sigma\rho) = \varepsilon(\sigma).$$

■ (i) Les propriétés des morphismes de groupes impliquent que, pour toute permutation $\sigma \in \mathfrak{S}_n$, on a $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)^{-1}$. Mais $\varepsilon(\sigma)^{-1} = \varepsilon(\sigma)$ car $\varepsilon(\sigma) \in \{-1; +1\}$. D'où le résultat.

(ii) On a $\varepsilon(\rho^{-1}\sigma\rho) = \varepsilon(\rho^{-1})\varepsilon(\sigma)\varepsilon(\rho) = \varepsilon(\sigma)\varepsilon(\rho)^2 = \varepsilon(\sigma)$. ■

La signature est donc un invariant de conjugaison.

b) Signature d'un cycle

Proposition 10

Un p-cycle a pour signature $(-1)^{p-1}$.

En particulier, une transposition a pour signature -1.

■ On sait que tout p-cycle de $\mathfrak{S}_n$ est conjugué au cycle $\gamma = (1, 2, \dots, p)$ d'après le corollaire 2. Tous les p-cycles ont donc la même signature que γ. Les inversions de $(1, 2, \dots, p)$ sont $\{1; p\}$, $\{2; p\}$, $\{3; p\}$, $\dots$, $\{p-1; p\}$. Il y en a $p-1$ donc la signature de γ est $(-1)^{p-1}$. Youpi ! ■

Attention !! Un cycle de longueur paire est une permutation impaire et vice versa.

La décomposition en produit de transpositions ou en produit de cycles à supports disjoints, combinée au fait que l'on connait la signature des transpositions et des cycles, permet d'envisager le calcul pratique de la signature d'une permutation (n'utilisant pas une énumération de toutes les inversions de cette permutation).

Calcul de la signature

Pour déterminer la signature d'une permutation σ, on a le choix entre :

- décomposer σ en un produit de k transpositions, ce qui donne $\varepsilon(\sigma) = (-1)^k$;
- décomposer σ en produit de cycles à supports disjoints $\sigma = c_k \dots c_2 c_1$, ce qui donne $\varepsilon(\sigma) = \varepsilon(c_k) \dots \varepsilon(c_2)\varepsilon(c_1)$ où $\varepsilon(c_i) = (-1)^{\omega(c_i)-1}$ pour tout $i \in [\![1; k]\!]$.

Avant de donner un exemple, notons que le premier point de cet encadré a deux conséquences :

▷ D'une part, il justifie l'invariance de la parité du nombre de transpositions dans la décomposition d'une permutation : une permutation paire ne peut être le produit que d'un nombre pair de transpositions et une permutation impaire ne peut être le produit que d'un nombre impair de transpositions.

▷ D'autre part, il implique que la signature est l'unique morphisme de groupe non constant entre $\mathfrak{S}_n$ et $\{-1; 1\}$. En effet, un tel morphisme, pour ne pas être le morphisme trivial valant toujours 1, doit prendre la valeur -1 sur au moins une transposition. Comme toutes les transpositions sont conjuguées (y réfléchir), le morphisme prend la valeur -1 sur toutes les transpositions. C'est donc la signature !

Exemples :

- Pour déterminer la signature de la permutation

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 6 & 4 & 3 & 7 & 5 \end{pmatrix},$$

Avec la décomposition en produit de transpositions, on a

$$\sigma_2 = (5, 7)(5, 6)(3, 5)(1, 2) \qquad \text{d'où} \qquad \varepsilon(\sigma_2) = (-1)^4 = 1.$$

Avec la décomposition en produit de cycles, on a

$$\sigma_2 = (1, 2)(3, 6, 7, 5) \qquad \text{d'où} \qquad \varepsilon(\sigma_2) = (-1) \times (-1) = 1.$$

B.4. Groupe alterné

Définition 15

L'ensemble des permutations paires est le noyau de la signature. C'est donc un sous-groupe de $\mathfrak{S}_n$ appelé groupe alterné d'indice n et noté $\mathfrak{A}_n$.

L'ensemble des permutations impaires n'est pas un sous-groupe de $\mathfrak{S}_n$ puisqu'il ne contient pas l'identité et qu'il n'est pas stable par produit.

Exemples :

- On a $\mathfrak{S}_1 = \mathfrak{A}_1 = \{\mathrm{Id}\}$.
- On a $\mathfrak{S}_2 = \{\mathrm{Id}, (1,2)\}$ donc $\mathfrak{A}_2 = \{\mathrm{Id}\}$.
- Le groupe $\mathfrak{S}_3$ est constitué de l'identité qui est paire, des transpositions $(1,2)$, $(2,3)$ et $(1,3)$ qui sont impaires et des 3-cycles $(1,2,3)$ et $(3,2,1)$ qui sont paires. On a donc $\mathfrak{A}_3 = \{\mathrm{Id}, (1,2,3), (3,2,1)\}$.

L'énoncé suivant justifie qu'il existe autant de permutations paires que de permutations impaires.

Proposition 11

Si $n \geqslant 2$, le groupe $\mathfrak{A}_n$ est d'ordre $n!/2$.

■ Soit τ une transposition de $\mathfrak{S}_n$ (qui existe puisque $n \geqslant 2$). On pose $\mathfrak{A}_n\tau = \{\rho\tau : \rho \in \mathfrak{A}_n\}$.

▷ Démontrons que $\mathfrak{S}_n \setminus \mathfrak{A}_n = \mathfrak{A}_n\tau$.
Soit $\rho \in \mathfrak{A}_n$, alors $\varepsilon(\rho\tau) = \varepsilon(\rho)\varepsilon(\tau) = 1 \times (-1) = -1$ donc $\rho\tau \in \mathfrak{S}_n \setminus \mathfrak{A}_n$.
Si $\sigma \in \mathfrak{S}_n \setminus \mathfrak{A}_n$, alors $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau) = (-1) \times (-1) = 1$ donc $\sigma\tau \in \mathfrak{A}_n$, ce qui justifie que $\sigma \in \mathfrak{A}_n\tau$.

▷ L'application $\rho \longmapsto \rho\tau$ est une involution (car $\rho\tau\tau = \rho$ lol) de $\mathfrak{A}_n$ sur $\mathfrak{A}_n\tau$, ce qui implique que $\mathrm{card}(\mathfrak{A}_n\tau) = \mathrm{card}(\mathfrak{A}_n)$.

▷ Comme $\mathfrak{A}_n$ et $\mathfrak{S}_n \setminus \mathfrak{A}_n$ forment une partition de $\mathfrak{S}_n$, on a $\mathrm{card}(\mathfrak{A}_n) + \mathrm{card}(\mathfrak{S}_n \setminus \mathfrak{A}_n) = n!$, ce qui donne $2\,\mathrm{card}\,\mathfrak{A}_n = n!$. Le résultat en découle. ■

4 h 15