Chapitre 36

Groupe symétrique

Dans ce chapitre, n désigne un entier naturel supérieur ou égal à 2. On note id_n l'application identité de $[\![1\,;n]\!]$.

L'objectif de ce chapitre est d'étudier quelques propriétés du groupe symétrique S_n, introduit brièvement dans le chapitre 17, principalement dans le but de définir la notion de déterminant dans le prochain chapitre (même si ce groupe est intéressant en soi).

Le groupe S_1 est réduit à id_1 (l'application identité sur $\{1\}$, qui est constante) et n'a donc pas beaucoup d'intérêt.

I Structure de groupe

1) Définition et notation

Proposition/Définition. *On note S_n l'ensemble des permutations de $[\![1\,;n]\!]$, c'est-à-dire des bijections de $[\![1\,;n]\!]$ dans lui même. Il s'agit d'un groupe (pour la composition) appelé groupe symétrique d'ordre n.*

Ce groupe est parfois noté $\mathfrak{S}_n$ mais ce n'est pas la notation retenue par le programme.

Démonstration. Déjà montré dans le chapitre 17. □

Proposition. *On a $\mathrm{card}(S_n) = n!$.*

Démonstration. On a vu dans le chapitre 33 qu'il y a $n!$ permutations d'un ensemble à n éléments, ce qui est le cas de $[\![1\,;n]\!]$. □

Notation. Une permutation σ de S_n consiste à se donner la liste des images des éléments de $[\![1\,;n]\!]$ par σ. La première façon usuelle de noter σ est sous forme d'un tableau à 2 lignes et n colonnes, les entiers de 1 à n sur la première ligne, et leurs images respectives sur la deuxième ligne :

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

Une permutation étant, par définition, une bijection, tous les entiers de 1 à n doivent apparaître exactement une fois sur la deuxième ligne.

Exemples :

- *La permutation*
$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \ldots & n \end{pmatrix}$$
est simplement id_n.
- *Lorsque $n = 2$, ce groupe est constitué de deux éléments : id_2 et l'application*
$$\begin{cases} [\![1\,;2]\!] & \longrightarrow & [\![1\,;2]\!] \\ 1 & \longmapsto & 2 \\ 2 & \longmapsto & 1 \end{cases}$$
Cette dernière est donc notée plus simplement :
- *Lorsque $n = 3$, ce groupe est constitué de six éléments :*
- *L'application $\sigma : k \longmapsto n + 1 - k$ est une permutation de $[\![1\,;n]\!]$ (je vous laisse le montrer) qui consiste à parcourir $[\![1\,;n]\!]$ en sens inverse. Elle s'écrit :*
$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ n & n-1 & \ldots & 1 \end{pmatrix}$$

- *Si* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix}$, *alors* σ *est la bijection de* $[\![1\,;6]\!]$ *sur lui-même qui à* 1 *associe* 2, *à* 2 *associe* 5, *à* 3 *associe* 6, *à* 4 *associe* 4, *à* 5 *associe* 1 *et à* 6 *associe* 3.

On calcule facilement la réciproque d'une permutation écrite sous cette forme en inversant les deux lignes et en remettant les termes dans le bon ordre.

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

On écrit souvent la composée de deux permutations multiplicativement (sans symbole) au lieu d'utiliser $\circ$. Pour obtenir la permutation produit, on passe en revue chaque élément de $[\![1\,;n]\!]$ et on lui fait subir les différentes permutations « de droite à gauche » bien entendu. Comme dans tout groupe multiplicatif, pour tous $\sigma \in S_n$ et $k \in \mathbb{N}^*$, on définit $\sigma^k = \underbrace{\sigma \circ \sigma \circ \cdots \circ \sigma}_{k \text{ fois}}$. On pose aussi $\sigma^0 = \mathrm{Id}_n$ et $\sigma^k = (\sigma^{-1})^{-k}$ lorsque $k \in \mathbb{Z}\backslash\mathbb{N}$.

Bien que la notation ressemble à une notation matricielle, le produit de permutations n'est en aucun cas un produit matriciel (qui n'aurait de toute façon aucun sens dès que $n \neq 2$). De même la notation « puissance -1 » n'a rien à voir avec un inverse matriciel.

Exemples : *Notons* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ *et* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$. *On a :*

- $\sigma \circ \tau =$
- $\tau \circ \sigma =$
- $\sigma^2 =$
- $\sigma^3 =$
- $\sigma^4 =$

Le groupe S_n est non abélien (c'est-à-dire que deux permutations ne commutent pas en général) dès que $n \geqslant 3$.

Par exemple

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

mais

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

Remarques :

- Quel que soit l'ensemble E à n éléments, l'ensemble S_E des permutations de E est en bijection avec S_n. En effet, si on note $E = \{x_1; \ldots; x_n\}$, l'application

$$\left\{ \begin{array}{ccc} S_n & \longrightarrow & S_E \\ \sigma & \longmapsto & \left\{ \begin{array}{ccc} E & \longrightarrow & E \\ x_i & \longmapsto & x_{\sigma(i)} \end{array} \right. \end{array} \right.$$

est une bijection. ⇝ Démonstration laissée en exercice.

On pourrait donc « identifier » S_n et S_E en identifiant une permutation de E avec son antécédent par cette application.

Par exemple, lorsque $n=3$, il est naturel d'identifier les permutations

$$\sigma : \begin{cases} [\![1\,;3]\!] & \longrightarrow & [\![1\,;3]\!] \\ 1 & \longmapsto & 3 \\ 2 & \longmapsto & 1 \\ 3 & \longmapsto & 2 \end{cases} \quad \text{et} \quad \widetilde{\sigma} : \begin{cases} \{x_1;x_2;x_3\} & \longrightarrow & \{x_1;x_2;x_3\} \\ x_1 & \longmapsto & x_3 \\ x_2 & \longmapsto & x_1 \\ x_3 & \longmapsto & x_2 \end{cases}$$

- Considérons une permutation σ de S_n et définissons

$$\widetilde{\sigma} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n & n+1 \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) & n+1 \end{pmatrix}$$

qui est une permutation de S_{n+1} qui fixe $n+1$. Les permutations σ et $\widetilde{\sigma}$ ne sont pas des éléments du même ensemble pourtant, il arrive qu'on les confonde par abus de notation. Cette identification peut être rendue rigoureuse en montrant (ce qui est immédiat) que l'application qui à σ associe $\widetilde{\sigma}$ est injective de S_n dans S_{n+1}. Ou encore qu'elle est bijective de S_n sur l'ensemble des permutations de S_{n+1} qui laissent fixe $n+1$.

Surtout quand on aura vu la notation en produit de cycles où la notation des deux est totalement confondues, cf. paragraphe II.1.

2) Support d'une permutation

Définition. *Soit $\sigma \in S_n$. On appelle support de σ, et on note $\mathrm{Supp}(\sigma)$ l'ensemble des éléments de $[\![1\,;n]\!]$ qui ne sont pas invariants par σ , c'est-à-dire*

$$\mathrm{Supp}(\sigma) = \{x \in [\![1\,;n]\!] \,|\, \sigma(x) \neq x\}.$$

En d'autres termes, le support de σ est le complémentaire de l'ensemble de ses points fixes.

Exemples :

- *Une permutation de S_n a un support vide si et seulement si elle est égale à l'identité.*
- *Le support de* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$ *est*
- *Le support de* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix}$ *est*

Proposition. *Soient σ et τ deux éléments de S_n. Alors*

$$\mathrm{Supp}(\sigma \circ \tau) \subset \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau).$$

On généralise aisément à un nombre quelconque de permutations : le support d'une composition est inclus dans l'union des supports. En particulier, si $k \geqslant 2$,

$$\mathrm{Supp}(\sigma^k) \subset \mathrm{Supp}(\sigma).$$

Démonstration.

□

Corollaire. *Si σ et τ sont à supports disjoints alors, pour tout $k \in \mathbb{N}^*$, σ^k et τ^k sont à supports disjoints.*

Démonstration. Découle du fait que $\mathrm{Supp}(\sigma^k) \subset \mathrm{Supp}(\sigma)$ et $\mathrm{Supp}(\tau^k) \subset \mathrm{Supp}(\tau)$.□

⚠ En général, il n'y a pas égalité dans l'inclusion de la proposition : une des deux permutations peut remettre à sa place un élément dérangé par l'autre, si bien que cet élément sera laissé stable par la composition des deux, et donc ne sera pas dans le support de $\sigma \circ \tau$ alors qu'il sera dans l'union des deux supports.

Par exemple, si $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ *et* $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$*, alors :*

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \quad \text{et} \quad \tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

donc

$$\mathrm{Supp}(\sigma \circ \tau) = \{2;3;4\} \neq \{1;2;3;4\} = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau).$$

Si on veut l'égalité, il faut une condition supplémentaire.

Lemme. *Soit $\sigma \in S_n$. On a $x \in \mathrm{Supp}(\sigma)$ si et seulement si $\sigma(x) \in \mathrm{Supp}(\sigma)$.*

Et donc une permutation stabilise son support.

Démonstration.

□

Proposition. *Soient σ et τ deux éléments de S_n à supports disjoints. Alors σ et τ commutent, et $\mathrm{Supp}(\sigma \circ \tau) = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$, cette union étant disjointe.*

Quand on dit qu'ils commutent, c'est évidemment pour la loi $\circ$, c'est-à-dire que $\sigma \circ \tau = \tau \circ \sigma$.

Démonstration.

Ce résulat est intuitif : σ et τ ne vont « pas toucher aux mêmes éléments » donc peuvent agir chacune de leur côté dans l'ordre qu'elles veulent, cela ne changera rien.

□

Ce résultat se généralise à un nombre quelconque de permutations : le support d'une composée de permutations à supports **deux à deux** disjoints est l'union des supports.

Remarques :

- La réciproque est fausse : il est tout à fait possible que deux permutations à support non disjoints commutent.

  Par exemple une permutation qui n'est pas l'identité commute avec elle-même.
- Ainsi, si σ et τ sont à supports disjoints, alors pour tous $k \in \mathbb{N}$, $(\sigma \circ \tau)^k = \sigma^k \circ \tau^k$.

3) Orbite d'un élément suivant une permutation

Les résultats de ce paragraphe (y compris la notion d'orbite) ne sont pas officiellement au programme. Nous l'introduisons uniquement dans le but de faciliter la preuve du théorème de décomposition en produit de cycles disjoints (cf. paragraphe II.1).

Définition. *Soit $\sigma \in S_n$. Soit $x \in [\![1\,;n]\!]$. On appelle orbite de x suivant σ l'ensemble $\mathscr{O}_\sigma(x) = \{\sigma^k(x) \mid k \in \mathbb{Z}\}$.*

$\mathscr{O}_\sigma(x)$ est l'ensemble de toutes les éléments de $[\![1\,;n]\!]$ que l'on peut atteindre « à partir de x » en lui appliquant plusieurs fois σ et σ^{-1}. Il s'agit bien sûr d'un ensemble fini puisque c'est une partie de $[\![1\,;n]\!]$.

Exemple : *Si* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix}$, *alors*

Remarque : Pour tout $x \in [\![1\,;n]\!]$, on a

$$\sigma(\mathscr{O}_\sigma(x)) = \{\sigma^{k+1}(x) \,|\, k \in \mathbb{Z}\} = \{\sigma^k(x) \,|\, k \in \mathbb{Z}\} = \mathscr{O}_\sigma(x).$$

En particulier, les orbites suivant σ sont stables par σ.

Proposition/Définition. *Soit $\sigma \in S_n$. On définit une relation binaire $\mathcal{R}_\sigma$ sur $[\![1\,;n]\!]$ par*

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

Il s'agit d'une relation d'équivalence sur $[\![1\,;n]\!]$ dont les classes d'équivalences sont les orbites suivant σ.

Démonstration.

□

Corollaire. *Les orbites suivant σ forment une partition de $[\![1\,;n]\!]$.*

Remarque : Pour tout $x \in [\![1\,;n]\!]$, $\mathscr{O}_\sigma(x) = \{x\}$ si et seulement si $\sigma(x) = x$ si et seulement si $x \notin \mathrm{Supp}(\sigma)$. On en déduit que $\mathrm{Supp}(\sigma)$ est l'union disjointe des orbites non réduites à un point.

Proposition. *Soient $x \in [\![1\,;n]\!]$ et $\sigma \in S_n$. L'ensemble $\{k \in \mathbb{N}^* \,|\, \sigma^k(x) = x\}$ admet un plus petit élément p. On a $p = \mathrm{card}(\mathscr{O}_\sigma(x))$ et $\mathscr{O}_\sigma(x) = \{\sigma^k(x) \,|\, k \in [\![0\,;p-1]\!]\}$.*

Démonstration.

□

Remarque : Puisqu'une orbite est une classe d'équivalence, pour tous $\sigma \in S_n$, $x \in [\![1\,;n]\!]$ et $y \in \mathscr{O}_\sigma(x)$, on a l'égalité $\mathscr{O}_\sigma(x) = \mathscr{O}_\sigma(y)$. En notant p le cardinal de cette orbite, on a

$$\{x; \sigma(x); \sigma^2(x); \dots; \sigma^{p-1}(x)\} = \{y; \sigma(y); \sigma^2(y); \dots; \sigma^{p-1}(y)\}.$$

Pour décrire une orbite de cette façon, on peut donc prendre le « point de départ » que l'on veut dans l'orbite.

4) Transpositions et cycles

Définition (transposition). *On appelle transposition de S_n toute permutation de S_n qui laisse fixe tous les éléments de $[\![1\,;n]\!]$ sauf deux (qui sont échangés). Autrement dit, $\sigma \in S_n$ est une transposition s'il existe i et j distincts dans $[\![1\,;n]\!]$ tels que*

$$\sigma(i) = j, \qquad \sigma(j) = i \qquad \text{et} \qquad \forall x \in [\![1\,;n]\!]\backslash\{i;j\}, \quad \sigma(x) = x.$$

On la note alors plus simplement $\begin{pmatrix} i & j \end{pmatrix}$.

Exemple : *La permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$ de S_5 est une transposition. On la note donc plus simplement $\begin{pmatrix} 2 & 5 \end{pmatrix}$ ou $\begin{pmatrix} 5 & 2 \end{pmatrix}$.*

ou $\begin{pmatrix} j & i \end{pmatrix}$, cela revient au même. Cette notation indique que j est changé en i, i est changé en j et les autres éléments sont invariants. On en reparlera ci-dessous en généralisant cette notation aux cycles.
⚠ Ne pas confondre cette notation avec un vecteur de $\mathbb{R}^2$.

Proposition. *Soit σ une transposition de S_n. Alors $\sigma^2 = \mathrm{id}_n$. Autrement dit $\sigma^{-1} = \sigma$.*

Démonstration. On a $\sigma^2(i) = \sigma(\sigma(i)) = \sigma(j) = i$, $\sigma^2(j) = \sigma(\sigma(j)) = \sigma(i) = j$ et, pour tout $x \in [\![1\,;n]\!]\backslash\{i;j\}$, $\sigma^2(x) = \sigma(\sigma(x)) = \sigma(x) = x$. □

Définition (cycle). *Soit $p \in [\![2\,;n]\!]$. Soit $\sigma \in S_n$. On dit que σ est un p-cycle de S_n s'il existe $(x_1, \dots, x_p) \in [\![1\,;n]\!]^p$ deux à deux distincts tels que :*

- $\mathrm{Supp}(\sigma) = \{x_1; \dots; x_p\}$.
- $\forall i \in [\![1\,;p-1]\!]$, $\sigma(x_i) = x_{i+1}$.
- $\sigma(x_p) = x_1$.

On la note plus simplement $\begin{pmatrix} x_1 & x_2 & \cdots & x_p \end{pmatrix}$. L'entier p est aussi appelé la longueur du cycle.

Autrement dit σ transforme x_1 en x_2, x_2 en x_3, etc. x_{p-1} en x_p et enfin x_p en x_1... et laisse tous les autres invariants.

Exemples :

- *La permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 2 & 7 & 4 & 5 & 3 & 1 \end{pmatrix}$ de S_7 est un 4-cycle. En effet :*

  On la note donc plus simplement
- *Avec cette écriture, on a*

  $S_3 =$

Remarques :

- Une transposition est un 2-cycle.
- Si un élément n'est pas listé dans le cycle, c'est qu'il est fixe.

- Le cycle $\begin{pmatrix} x_1 & x_2 & \cdots & x_p \end{pmatrix}$ peut encore s'écrire $\begin{pmatrix} x_1 & \sigma(x_1) & \sigma^2(x_1) & \cdots & \sigma^{p-1}(x_1) \end{pmatrix}$. Son support est

$$\{x_1; x_2; \ldots; x_n\} = \{x_1; \sigma(x_1); \sigma^2(x_1); \ldots; \sigma^{p-1}(x_1)\}.$$

  Autrement dit le support de ce cycle consiste en l'orbite de x_1... mais aussi en l'orbite de n'importe quel élément du support compte tenu de la dernière remarque du paragraphe précédent.

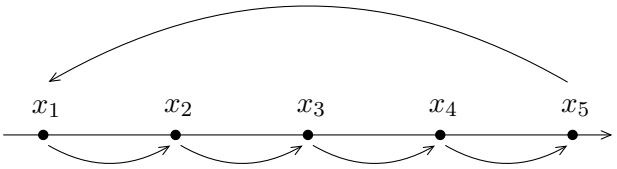
Réciproquement, si le support d'une permutation consiste en une seule orbite de cardinal $p \geqslant 2$, alors il s'agit d'un p-cycle.

- La notation $\begin{pmatrix} x_1 & x_2 & \cdots & x_p \end{pmatrix}$ n'est donc pas unique. On peut prendre pour « point de départ » n'importe quel élément de $\{x_1; \ldots; x_p\}$. Tout ce qui importe est qu'à partir de cet élément, on écrit de gauche à droite tous les images successives par σ (en revenant au début pour l'image du dernier élément et ensuite « ça boucle »).

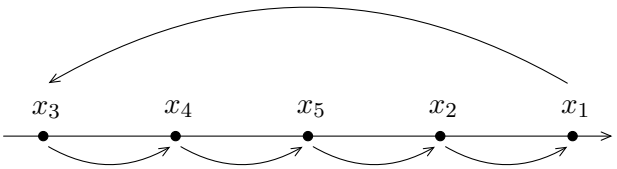
  Par exemple, le 4-cycle ci-dessus peut aussi s'écrire $\begin{pmatrix} 6 & 3 & 7 & 1 \end{pmatrix}$ ou $\begin{pmatrix} 3 & 7 & 1 & 6 \end{pmatrix}$ ou $\begin{pmatrix} 3 & 7 & 6 & 1 \end{pmatrix}$

  Pour bien comprendre cela, il suffit d'avoir en tête les dessins suivantes :

On comprend bien le terme « cycle ».



  est la même chose que



  ⚠ Il faut bien juste respecter l'ordre des images successives et donc l'ordre relatif des éléments du cycle.

  Par exemple, le 4-cycle ci-dessus ne peut pas s'écrire $\begin{pmatrix} 1 & 3 & 6 & 7 \end{pmatrix}$. Ce dernier a le même support mais il envoie 1 sur 3 et non sur 6 !

- Dans cette notation d'un cycle, le n de S_n est sous-entendu : on note par exemple de la même manière un cycle de S_5 qu'un cycle de S_n ne faisant apparaître que 1, 2, 3, 4 ou 5 lorsque $n \geqslant 6$.
- Il existe des éléments de S_n qui ne sont pas des cycles.

  Par exemple $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ n'est pas un cycle. En effet son support est $\{1; 2; 3; 4\}$ mais l'orbite de 1 est $\{1; 4\}$ tandis que l'orbite de 2 est $\{2; 3\}$. Il s'agit en fait de la composée des transpositions $\begin{pmatrix} 1 & 4 \end{pmatrix}$ et $\begin{pmatrix} 2 & 3 \end{pmatrix}$ (dans l'ordre voulu puisque, ayant des supports disjoints, elles commutent).
- ⚠ Une composée de cycles (ou une puissance d'un cycle) n'est pas forcément un cycle.

  Par exemple, si on note $\sigma = \begin{pmatrix} 2 & 5 & 3 & 1 & 7 & 9 \end{pmatrix}$ un 6-cycle de S_9, alors :

$$\sigma^2 = \quad \boxed{\phantom{\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 7 & 9 \end{pmatrix}}}$$

  Alors σ^2 n'est pas un 6-cycle. En effet :

  Plus précisément, σ est la composée de deux 3-cycles à supports disjoints :

- La réciproque d'un cycle s'obtient en listant les éléments dans le sens inverse.

  Par exemple $\begin{pmatrix} 2 & 7 & 5 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 3 & 5 & 7 & 2 \end{pmatrix}$.

Proposition. *Soit σ un p-cycle de S_n. Alors $\sigma^p = \mathrm{id}_n$. En particulier, l'inverse de σ est σ^{p-1}.*

Il découle même de la démonstration que p est le plus petit indice $k \geqslant 1$ tel que $\sigma^k = \mathrm{Id}$: on dit que σ est d'ordre p, si bien que l'ordre d'un cycle est égal à sa longueur (nous le verrons en exercices).

Démonstration.

II Décomposition d'une permutation

L'idée (comme pour les polynômes ou les entiers) consiste à écrire une permutation comme « produit » de permutations plus simples : on va s'intéresser à l'écriture comme produit de cycles ou comme produit de transpositions, chacune ayant ses avantages et ses inconvénients.

Le produit est en fait la composition de bijections.

1) Décomposition en produit de cycles à supports disjoints

Théorème. *Toute permutation de S_n peut s'écrire comme produit de cycles à supports disjoints. De plus, cette écriture est unique à l'ordre près des termes.*

Remarques :

- Les cycles étant à supports disjoints, ils commutent deux à deux donc on peut écrire ces cycles dans l'ordre que l'on veut sans changer la permutation.
- Si $\sigma = \mathrm{id}_n$, alors il faut voir cette décomposition comme un produit vide de cycles.

Démonstration. **Existence.**

Une orbite est réduit à un point si ce point est fixe par la permutation.

Unicité. Supposons que σ s'écrive aussi $\tau_1 \cdots \tau_q$ avec $\tau_1, \dots, \tau_q$ des cycles à supports disjoints. D'après le paragraphe I.2, $\mathrm{Supp}(\sigma) = \bigcup_{i=1}^{q} \mathrm{Supp}(\tau_i)$ (cette union étant disjointe).

Soit $j \in [\![1\,;q]\!]$. Soit $x \in \mathrm{Supp}(\tau_j)$. Comme x et $\tau_j(x)$ sont laissés fixes par les τ_k lorsque $k \neq j$, on a

$$\sigma(x) = \tau_1 \cdots \tau_q(x) = \tau_j(x)$$

et donc $\sigma(x) \in \mathrm{Supp}(\tau_j)$. En appliquant ce même raisonnement à $\sigma(x)$, on trouve que $\sigma^2(x) = \tau_j(\sigma(x)) = \tau_j^2(x)$. Par récurrence immédiate, pour tout $k \in \mathbb{N}$, $\sigma^k(x) = \tau_j^k(x)$ et donc $\sigma^k(x) \in \mathrm{Supp}(\tau_j)$.

Soit $i \in [\![1\,;p]\!]$. On a $\mathrm{Supp}(c_i) = \{x_i; \sigma(x_i); \dots; \sigma^{k_i-1}(x_i)\}$. Il existe aussi un unique $j \in [\![1\,;q]\!]$ tel que $x_i \in \mathrm{Supp}(\tau_j)$ et donc $\mathrm{Supp}(c_i) \subset \mathrm{Supp}(\tau_j)$ d'après ce qui précède.

... en reprenant les notations de la preuve de l'existence.

On vient de montrer chaque c_i a un support inclus dans le support de l'un des τ_j. Il s'ensuit que $p \leqslant q$. Mais, si $p < q$ ou bien si $p = q$ et que l'une de ces inclusions est stricte, l'union disjointe $\bigcup_{i=1}^{p} \mathrm{Supp}(c_i)$ serait strictement incluse dans l'union disjointe $\bigcup_{i=1}^{q} \mathrm{Supp}(\tau_i)$, ce qui est absurde puisqu'elles sont toutes les deux égales à $\mathrm{Supp}(\sigma)$. Dès lors $p = q$ et chaque c_i a un support égal à celui d'un τ_j.

Quitte à échanger l'ordre des τ_j, supposons que $\mathrm{Supp}(c_i) = \mathrm{Supp}(\tau_i)$ pour tout $i \in [\![1\,;p]\!]$. On a vu qu'alors τ_i et c_i coïncident (avec σ) sur leur support commun et, comme ce sont des cycles, $\tau_i = c_i$. D'où l'unicité. □

Remarque : La technicité de cette démonstration ne doit pas cacher l'idée générale qui est très simple : les différents cycles de cette écriture sont obtenus en prenant des éléments non équivalents, c'est-à-dire qu'on ne peut pas passer de l'un à l'autre en appliquant σ, et les cycles sont simplement obtenus en prenant leurs images successives par σ. Cela nous donne un algorithme constructif assez simple :

- On prend le premier élément x du support de σ (1 si 1 est dans le support, sinon 2 etc.).
- On prend ses images successives par σ. On finit par retomber sur x lui-même : les images distinctes forment une classe d'équivalence, et cela nous donne un premier cycle.
- Si on a obtenu le support de σ, on arrête là, sinon on recommence avec le plus petit élément du support que nous n'avons pas encore « visité », cela donnera une autre classe d'équivalence, et donc un autre cycle.
- On recommence jusqu'à obtenir le support de σ en entier. Cet algorithme termine puisque le support est un ensemble fini, et on retire au moins un élément à chaque fois, donc le cardinal des éléments restants diminue strictement donc il finit par être nul.

Exemple : *Décomposons en produit de cycles à supports disjoints la permutation de S_{15} :*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 2 & 8 & 12 & 1 & 7 & 6 & 10 & 11 & 9 & 13 & 5 & 3 & 14 & 15 \end{pmatrix}$$

Commençons par 1 qui est dans le support : ses images successives par σ sont $4, 12$ et 5 si bien qu'on a un premier cycle : $(1 \quad 4 \quad 12 \quad 5)$. Le prochain élément du support que nous n'avons pas visité est 3 : ses images successives par σ sont $8, 10, 9, 11, 13$ et on retombe sur 3 si bien qu'on a un deuxième cycle : $(3 \quad 8 \quad 10 \quad 9 \quad 11 \quad 13)$. Ensuite, au tour de 6 : son image est 7 et on revient ensuite sur 6, cela donne un cycle (en fait une transposition) : $(6 \quad 7)$. On a pris tous les éléments du support, donc finalement :

$$\sigma =$$

Remarque : Si $(k, p) \in (\mathbb{N}^*)^2$ et $\sigma = c_1 \circ c_2 \circ \cdots \circ c_k$ est un produit de cycles à supports disjoints alors, comme ceux-ci commutent, on a

$$\sigma^p = c_1^p \circ c_2^p \circ \cdots \circ c_k^p.$$

Ce résultat est l'un des grands intérêt de cette décomposition.

Par exemple, considérons $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 4 & 5 & 3 & 1 & 6 & 7 \end{pmatrix}$ et calculons σ^{2025}.

2) Décomposition en produit de transpositions

Théorème. *Toute permutation de S_n peut s'écrire comme produit de transpositions.*

Remarques :

- Cette écriture n'est pas forcément unique, même à l'ordre près des termes.

  Par exemple :

  $$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (2 \quad 4) = (1 \quad 2)(1 \quad 4)(1 \quad 2)$$

  De plus, les supports ne sont pas disjoints : les transpositions ne commutent pas !
- Là aussi, pour l'identité, ce résultat est toujours valable : soit on prend un produit vide, soit on remarque que $\mathrm{id}_n = \sigma \circ \sigma$ avec σ une transposition quelconque.

Démonstration. Soit $\sigma \in S_n$. Puisque σ est produit de cycles (à supports disjoints), alors il suffit de prouver le résultat pour un cycle : en effet, si $\sigma = \sigma_1 \circ \cdots \circ \sigma_m$ avec les σ_i des cycles, s'ils sont produits de transpositions, σ l'est aussi.

Il suffit ensuite de voir que, pour tous éléments $a_1, \ldots, a_m$ deux à deux distincts dans $[\![1\,;n]\!]$,

$$(a_1 \quad a_2 \quad \ldots \quad a_m) = (a_1 \quad a_2)(a_2 \quad a_3) \cdots (a_{m-1} \quad a_m)$$

Notons en effet τ le produit de droite. Alors $\tau(a_1) = a_2$ puisque a_1 se trouve uniquement dans le support de la dernière transposition, donc est laissé invariant par les autres, et la dernière transposition l'envoie sur a_2. De plus, $\tau(a_2) = a_3$: a_2 est laissé stable par toutes sauf les deux dernières, l'avant-dernière l'envoie sur a_3, et la dernière laisse a_3 invariant, et ainsi de suite : pour tout $k \leqslant m-1$, a_k est laissé invariant par toutes les transpositions avant $(a_k \quad a_{k+1})$ qui l'envoie sur a_{k+1} mais a_{k+1} n'apparaît pas dans le support des transpositions qui suivent donc est laissé stable si bien que $\tau(a_k) = a_{k+1}$. Enfin, la dernière transposition envoie a_m sur a_{m-1}, celle d'avant envoie a_{m-1} sur a_{m-2} etc. et la dernière envoie a_2 sur a_1 si bien que $\tau(a_m) = a_1$.

En conclusion, $\sigma = \tau$: tout cycle est produit de transpositions ce qui permet de conclure. □

Remarques :

- Un des avantages de ces deux types de décomposition (comme produit de cycles ou comme produit de transpositions) est que si on veut prouver un résultat pour toutes les permutations, il suffit de le prouver pour les transpositions ou les cycles, et c'est souvent plus facile.
- La démonstration ci-dessus est à connaître car elle permet d'obtenir une décomposition de σ en produit de transpositions quand on connaît sa décomposition sous forme d'un produit de cycles à supports disjoints, on écrit chaque cycle comme produit de transpositions en prenant chaque élément de chaque cycle et son successeur.

  Par exemple, si on reprend σ la permutation de $[\![1\,;15]\!]$ du paragraphe précédent :

  $\sigma = (1 \quad 4 \quad 12 \quad 5)\,(3 \quad 8 \quad 10 \quad 9 \quad 11 \quad 13)\,(6 \quad 7)$

  $=$

- La méthode que l'on vient de décrire est assez simple mais nécessite de connaître la décomposition de σ en produit de cycles à supports disjoints. Certes, celle-ci n'est pas très difficile à obtenir, mais on peut envisager une méthode directe.
  - ⋆ Si $\sigma(n) \neq n$, alors on pose $\tau_1 = (n \quad \sigma(n))$ puis $\sigma_1 = \tau_1 \circ \sigma$. Si $\sigma(n) = n$, on pose $\sigma_1 = \sigma$. Dans les deux cas, la permutation σ_1 laisse n invariant donc on peut la voir comme une permutation de S_{n-1}.
  - ⋆ Si $\sigma_1(n-1) \neq n-1$, alors on pose $\tau_2 = (n-1 \quad \sigma(n-1))$ puis $\sigma_2 = \tau_2 \circ \sigma_1$. Si $\sigma_1(n-1) = n-1$, on pose $\sigma_2 = \sigma_1$. Dans les deux cas, la permutation σ_2 laisse $n-2$ invariant donc on peut la voir comme une permutation de S_{n-2}.
  - ⋆ etc.

  On construit $\tau_3, \tau_4, \ldots, \tau_k$ par récurrence descendante jusqu'à ce qu'on obtienne l'identité. La décomposition de σ en produit de transpositions est alors $\tau_1\tau_2\ldots\tau_k$.

  Reprenons l'exemple de

  $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 2 & 8 & 12 & 1 & 7 & 6 & 10 & 11 & 9 & 13 & 5 & 3 & 14 & 15 \end{pmatrix}$$

  que l'on a déjà décomposé en produits de cycles puis de transpositions. Utilisons cette deuxième méthode :

  $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 2 & 8 & 12 & 1 & 7 & 6 & 10 & 11 & 9 & 13 & 5 & 3 & 14 & 15 \end{pmatrix}$$

La méthode décrite ci-contre fournit en fait une démonstration alternative et constructive de l'existence d'une décomposition en produit de transpositions.

σ_1 s'obtient à partir de σ en invertissant dans la ligne du bas $\sigma(n)$ et son image, σ_2 s'obtient à partir de σ_1 en invertissant dans la ligne du bas $\sigma(n-1)$ et son image, etc.

Enlevons au fur et à mesure les éléments de $\sigma_1, \sigma_2, \ldots$ qui sont fixes (ceux de la fin).

- On peut même envisager une troisième méthode en partant du début plutôt que de la fin.

  Reprenons une dernière fois la permutation σ ci-dessus. On a

$$\begin{aligned}\sigma &= \begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12&13&14&15\\4&2&8&12&1&7&6&10&11&9&13&5&3&14&15\end{pmatrix}\\ &= (1\quad 4)\begin{pmatrix}1&2&3&4&5&6&7&8&9&10&11&12&13&14&15\\1&2&8&12&4&7&6&10&11&9&13&5&3&14&15\end{pmatrix}\\ &= \cdots\\ &= (1\quad 4)\,(3\quad 8)\,(4\quad 12)\,(5\quad 12)\,(6\quad 7)\,(8\quad 10)\,(9\quad 11)\,(10\quad 11)\,(11\quad 13)\,.\end{aligned}$$

Notons que l'on trouve une décomposition différente.

On va encore trouver une décomposition différente. Remarquons que les trois décompositions trouvées comportent le même nombre de transpositions. Cela pourrait ne pas être le cas (en ajoutant par exemple n'importe quelle transposition au carrée à la fin).

III Signature

On a vu que toute permutation s'écrit comme produit de transpositions. Cependant cette décomposition n'est pas unique, y compris le nombre de transposition intervenant (il suffit de multiplier par le carré d'une transposition quelconque pour en changer le nombre). Mais nous allons montrer qu'il y a unicité de la parité du nombre de transpositions. Pour cela intéressons-nous à la notion de signature d'une permutation (celle-ci trouvera surtout son intérêt dans le prochain chapitre).

Proposition/Définition. *Il existe un unique morphisme de groupe de S_n dans $\{-1;1\}$ qui envoie toutes les transpositions sur -1. Ce morphisme est noté ε, il est appelé signature et il est défini par :*

$$\varepsilon : \left\{\begin{array}{ccc} S_n & \longrightarrow & \{-1;1\} \\ \sigma & \longmapsto & \displaystyle\prod_{1\leqslant i<j\leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j}\end{array}\right.$$

Rappelons que $\{-1;1\}$ est un groupe à deux éléments quand on le munit de la multiplication.

Démonstration. Commençons par l'unicité.

On voit que la valeur de f et g en les transpositions ne joue aucun rôle dans l'unicité. On verra en exercices que la signature est même l'unique morphisme non trivial (c'est-à-dire non constant égal à 1) de S_n dans $\mathbb{C}^*$.

Montrons maintenant l'existence. Pour cela, prouvons que

$$\varepsilon : \left\{\begin{array}{ccc} S_n & \longrightarrow & \{-1;1\} \\ \sigma & \longmapsto & \displaystyle\prod_{1\leqslant i<j\leqslant n} \frac{\sigma(i)-\sigma(j)}{i-j}\end{array}\right.$$

convient.

□

Corollaire. *Soit $p \in \mathbb{N}^*$. Soit $\sigma \in S_n$. Si σ est le produit de p transpositions, alors $\varepsilon(\sigma) = (-1)^p$.*

Exemples :

- *Calculons la signature de la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ de deux façons différentes.*

On ne fera plus jamais cela à l'avenir : c'est ultra fastidieux (et on a pris $n = 4$ seulement...).

- *Considérons*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 4 & 2 & 8 & 12 & 1 & 7 & 6 & 10 & 11 & 9 & 13 & 5 & 3 & 14 & 15 \end{pmatrix}$$

Si on a plutôt écrit une permutation en produit de cycles à supports disjoints, on utilise le résultat suivant :

Proposition. *Soit $p \in \mathbb{N}\backslash\{0;1\}$. Soit σ un p-cycle. Alors $\varepsilon(\sigma) = (-1)^{p-1}$.*

Démonstration. On a vu dans le paragraphe II.2 (dans la démonstration) qu'un p-cycle est produit de $p-1$ transpositions, ce qui permet de conclure. □