Aide à la compréhension sur le cours sur les permutations

Les premières notions sur les permutations

Si E est un ensemble fini de cardinal n que l'on note :

$$E = \{a_1, \cdots, a_n\},$$

l'ensemble $\mathfrak{S}(E)$ de toutes les bijections de E vers E forme un groupe pour la composition. On remarque que si $\sigma \in \mathfrak{S}(E)$, alors l'inverse de σ pour cette loi $\circ$ est exactement la fonction réciproque de la bijection σ ce qui amène à cette très belle formule :

$$\sigma^{-1} = \sigma^{-1},$$

où la notation σ^{-1} désigne a priori deux concepts différents, ici égaux.
On appelle **permutation** toute bijection $\sigma : E \longrightarrow E$ sur l'ensemble E. Il y a autant d'informations dans $\sigma : E \longrightarrow E$ que dans la liste :

$$\sigma(a_1), \sigma(a_2), \cdots, \sigma(a_n).$$

car connaître σ revient à connaître les images par σ des éléments $a_1, a_2, \cdots, a_n$.
Il y a $n!$ factorielles permutations sur l'ensemble E car choisir une permutation $\sigma \in \mathfrak{S}(E)$ revient à choisir l'image $\sigma(a_1)$ [n choix possibles], puis $\sigma(a_2)$ [$(n-1)$ choix possibles car σ doit être injective donc $\sigma(a_2) \neq \sigma(a_1)$], ainsi de suite jusqu'à l'image de $\sigma(a_{n-1})$ [2 choix possibles] puis finalement l'image de $\sigma(a_n)$ [un seul choix, le seul élément restant dans $E \setminus \{\sigma(a_1), \cdots, \sigma(a_{n-1})\}$.]

La propriété 2 nous dit qu'étudier le groupe $(\mathfrak{S}(E), \circ)$ ou le groupe $(\mathfrak{S}(\llbracket 1, n \rrbracket), \circ)$, c'est pareil !!
Dans toute la suite, on notera :

$$\mathfrak{S}_n = \mathfrak{S}(\llbracket 1, n \rrbracket).$$

En effet, l'application Φ proposée est bien un isomorphisme de groupes car :

- déjà l'application Φ est bien définie, puisque si $\sigma \in \mathfrak{S}_n$, alors en notant :

$$\rho : \left| \begin{array}{ccc} E & \longrightarrow & E \\ a_i & \longmapsto & a_{\sigma(i)} \end{array} \right. ,$$

  si l'on se donne deux indices i et j différents entre 1 et n, alors les indices $\sigma(i)$ et $\sigma(j)$ seront encore différents : les éléments $a_{\sigma(i)}$ et $a_{\sigma(j)}$ restent différents dans E. Autrement dit, les éléments $\rho(i)$ et $\rho(j)$ sont différents. L'application ρ est injective. Comme l'application ρ va d'un ensemble fini dans un ensemble fini de même cardinal (en l'occurrence le même ensemble...), alors l'application ρ est bijective (se référer au cours du chapitre 1, qui date un peu...). Résultat des courses, la fonction $\rho = \Phi(\sigma)$ appartient bien à $\mathfrak{S}(E)$.

- si σ_1 et σ_2 sont dans $\mathfrak{S}_n$, si i est un entier entre 1 et n, on dispose des égalités suivantes :

$$\begin{aligned}\Phi(\sigma_1 \circ \sigma_2)(a_i) &= a_{\sigma_1 \circ \sigma_2(i)} \\ &= a_{\sigma_1(\sigma_2(i))} \\ &= \Phi(\sigma_1)(a_{\sigma_2(i)}) \\ &= \Phi(\sigma_1)(\Phi(\sigma_2)(a_i)) \\ &= \Big(\Phi(\sigma_1) \circ \Phi(\sigma_2)\Big)(a_i)\end{aligned}$$

  Les applications $\Phi(\sigma_1 \circ \sigma_2)$ et $\Phi(\sigma_1) \circ \Phi(\sigma_2)$ sont identiques : l'application Φ est bien un morphisme de groupes ! !
- pour montrer que Φ est une bijection, on peut expliciter la fonction qui sera sa bijection réciproque, à savoir :

$$\sigma \longmapsto \Big(a_i \longmapsto a_{\sigma^{-1}(i)}\Big).$$

  On peut aussi montrer que Φ est injective (en regardant ce qui se passe dans $\mathrm{Ker}(\Phi)$ [attention, on est bien loin des matrices et des applications linéaires...] et comme Φ va d'un ensemble fini, dans un ensemble fini de même cardinal $n!$, alors Φ sera bijective.
  Si l'on veut détailler $\mathrm{Ker}(\Phi)$, voici ce qui se passe : soit $\sigma \in \mathrm{Ker}(\Phi)$. Alors, $\Phi(\sigma) = \mathrm{id}$. Soit i un entier entre 1 et n. Alors,

$$a_i = \Phi(\sigma)(a_i) = a_{\sigma(i)},$$

  imposant aux indices i et $\sigma(i)$ d'être égaux : $\sigma(i) = i$, pour tout i, donc $\sigma = \mathrm{id}$ et :

$$\mathrm{Ker}(\Phi) = \{\mathrm{id}\},$$

  le neutre du groupe $\mathfrak{S}_n$.

Dorénavant, on n'étudie uniquement que les permutations $\sigma \in \mathfrak{S}_n$ qui opèrent sur l'ensemble $[\![1, n]\!]$.
Lorsque l'on considère une permutation $\sigma : [\![1, n]\!] \longrightarrow [\![1, n]\!]$, il y a plusieurs notions qui interviendront dans la suite. Par exemple interviendront les points fixes de σ (les éléments k entre 1 et n tels que $\sigma(k) = k$) et les points non fixes qui constitueront le support de la permutation σ, noté $\mathrm{supp}(\sigma)$.

Mettons tout cela en image en démontrant au passage la propriété 3.

Fixons dans la suite une permutation $\sigma \in \mathfrak{S}_n$.
On va définir une relation $\mathscr{R}$ sur l'ensemble $[\![1, n]\!]$ de la manière suivante :

$$\forall (i, j) \in [\![1, n]\!]^2,\ i \mathscr{R}\ j \iff \exists k \in \mathbb{Z},\ j = \sigma^k(i),$$

où rappelons-le, $\sigma^k = \sigma \circ \cdots \circ \sigma$ avec k symboles σ si $k \geqslant 1$, $\sigma^0 = \mathrm{id}$ et $\sigma^k = (\sigma^{-1} \circ \cdots \circ \sigma^{-1})$, avec $-k \geqslant 1$ symboles σ^{-1} lorsque $k \leqslant -1$.
On va montrer que la relation $\mathscr{R}$ est une relation d'équivalence...
Cette relation est réflexive car pour tout $i \in [\![1, n]\!]$,

$$i = \sigma^0(i),$$

donc $i \mathscr{R} i$.
Cette relation est symétrique car si $i \mathscr{R} j$, on peut écrire :

$$j = \sigma^k(i), \text{ donc } i = \sigma^{-k}(j),$$

avec k et donc $(-k)$ dans $\mathbb{Z}$.
Cette relation est transitive car si $i_1 \mathscr{R} i_2$ et $i_2 \mathscr{R} i_3$, on écrit :

$$i_2 = \sigma^k(i_1) \text{ et } i_3 = \sigma^\ell(i_2),$$

donc :

$$i_3 = \sigma^{k+\ell}(i_1),$$

avec k et ℓ deux entiers, ainsi que $k + \ell$.

On peut donc partitionner l'ensemble $[\![1, n]\!]$ en classes d'équivalence, qui sont les trajectoires des points i en itérant plusieurs fois σ et en évaluant ces itérés au point i. Nécessairement, on reviendra au point de départ i après un nombre fini d'étapes. En effet, si i est fixé entre 1 et n, la permutation σ étant elle aussi fixée dès le début, l'application :

$$\Phi : \left| \begin{array}{ccc} \mathbb{Z} & \longrightarrow & [\![1, n]\!] \\ k & \longmapsto & \sigma^k(i) \end{array} \right.$$

prend ses valeurs dans la classe d'équivalence de i pour la relation $\mathscr{R}$. Par les cardinaux et le principe des tiroirs, l'application Φ ne peut être injective, puisque l'ensemble de départ $\mathbb{Z}$ est infini alors que l'ensemble d'arrivée est fini.
On peut donc trouver deux entiers $k < \ell$ tels que $\sigma^k(i) = \sigma^\ell(i)$, alors :

$$i = \sigma^{\ell-k}(i),$$

ce qui signifie que lorsque l'on calcule i, $\sigma(i)$, $\sigma^2(i)$, etc., on retombe sur i au bout d'un moment !! Et ce moment arrive au maximum à l'instant $\ell - k$.
On voit alors que dans la définition 2, l'orbite $\mathscr{O}(i)$ est exactement la classe d'équivalence de l'entier i et que l'ensemble des points fixes d'une permutation σ est exactement l'ensemble des indices i entre 1 et n pour lesquelles l'orbite $\mathscr{O}(i)$ est réduite au singleton $\{i\}$.

Passons maintenant à la propriété 3.
• On vient de voir que si k est un entier entre 1 et n, alors il existait un entier $p > 0$ tel que :

$$\sigma^p(k) = k.$$

Parmi tous les entiers qui marchent on choisit l'entier $p > 0$ minimal.
D'une part, il est clair que :

$$\left\{k, \sigma(k), \cdots, \sigma^{p-1}(k)\right\} \subset \mathscr{O}(k).$$

Pour l'autre inclusion, donnons-nous un élément $x = \sigma^q(k)$, pour un certain $q \in \mathbb{Z}$. On effectue la division euclidienne de q par p, ce qui donne :

$$q = ap + r, \text{ avec } 0 \leqslant r \leqslant p - 1.$$

On en déduit :

$$x = \sigma^r\left(\left(\sigma^p \circ \cdots \circ \sigma^p\right)(k)\right).$$

Or, $\sigma^p(k) = k$, donc en calculant successivement les images de k par les σ^p, on obtient :

$$\left(\sigma^p \circ \cdots \circ \sigma^p\right)(k) = k,$$

puis :

$$x = \sigma^r(k) \in \left\{k, \sigma(k), \cdots, \sigma^{p-1}(k)\right\}.$$

On a l'autre inclusion.
Tout se passe comme si on avait fait $|a|$ « tours » de trajectoires circulaires complètes, si on faisait un dessin. Les dessins viendront après ... Patience...
On peut juste terminer sur ceci en disant que l'ensemble :

$$\mathscr{O}(k) = \left\{k, \sigma(k), \cdots, \sigma^{p-1}(k)\right\},$$

est de cardinal p.
En effet, les éléments $k, \sigma(k), \cdots, \sigma^{p-1}(k)$ sont tous différents car si tel n'était pas le cas, on trouverait deux indices $0 \leqslant m_1 < m_2 < p$ tels que :

$$\sigma^{m_1}(k) = \sigma^{m_2}(k).$$

Par conséquent, en composant à gauche par σ^{-m_1}, on aurait :

$$\sigma^{m_2 - m_1}(k) = k,$$

et l'entier $m_2 - m_1 = m$ vérifierait :

$$0 < m < p \text{ et } \sigma^m(k) = k,$$

contredisant ainsi la minimalité de l'entier p pour cette propriété.

- Le deuxième point est clair.
- Le troisième point a déjà été montré.

Je vous propose de traiter un exemple, pour voir comment s'articulent les différentes notions et les différentes notations possibles pour une même permutation.

Prenons par exemple $n = 25$. Pourquoi ? Et ... pourquoi pas !

Prenons alors la permutation choisie au hasard (le hasard existe-t-il ? vaste question ...) $\sigma \in \mathfrak{S}_{25}$ définie sur $[\![1, 25]\!]$ par :

$$\sigma : \left|\begin{array}{ccc|ccc|ccc|ccc|ccc} 1 & \longmapsto & 6 & 6 & \longmapsto & 7 & 11 & \longmapsto & 21 & 16 & \longmapsto & 22 & 21 & \longmapsto & 24 \\ 2 & \longmapsto & 10 & 7 & \longmapsto & 16 & 12 & \longmapsto & 12 & 17 & \longmapsto & 2 & 22 & \longmapsto & 25 \\ 3 & \longmapsto & 5 & 8 & \longmapsto & 23 & 13 & \longmapsto & 20 & 18 & \longmapsto & 17 & 23 & \longmapsto & 8 \\ 4 & \longmapsto & 4 & 9 & \longmapsto & 9 & 14 & \longmapsto & 19 & 19 & \longmapsto & 13 & 24 & \longmapsto & 11 \\ 5 & \longmapsto & 15 & 10 & \longmapsto & 18 & 15 & \longmapsto & 3 & 20 & \longmapsto & 14 & 25 & \longmapsto & 1 \end{array}\right.$$

Les choses sont un peu volumineuses à retranscrire ...

Essayons une autre notation plus compacte, pour cette même permutation. On met en première ligne les nombres entiers entre 1 et 25 et en deuxième ligne, les images par σ de ces éléments. Voici ce que cela donne :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \\ 6 & 10 & 5 & 4 & 15 & 7 & 16 & 23 & 9 & 18 & 21 & 12 & 20 & 19 & 3 & 22 & 2 & 17 & 13 & 14 & 24 & 25 & 8 & 11 & 1 \end{pmatrix}.$$

On va maintenant colorer en différentes teintes les orbites différentes des éléments. Il suffit de commencer par l'orbite de 1 en comptabilisant les images successives par σ de 1, etc. jusqu'à revenir sur 1, ce qui arrive fatalement, on l'a déjà démontré.

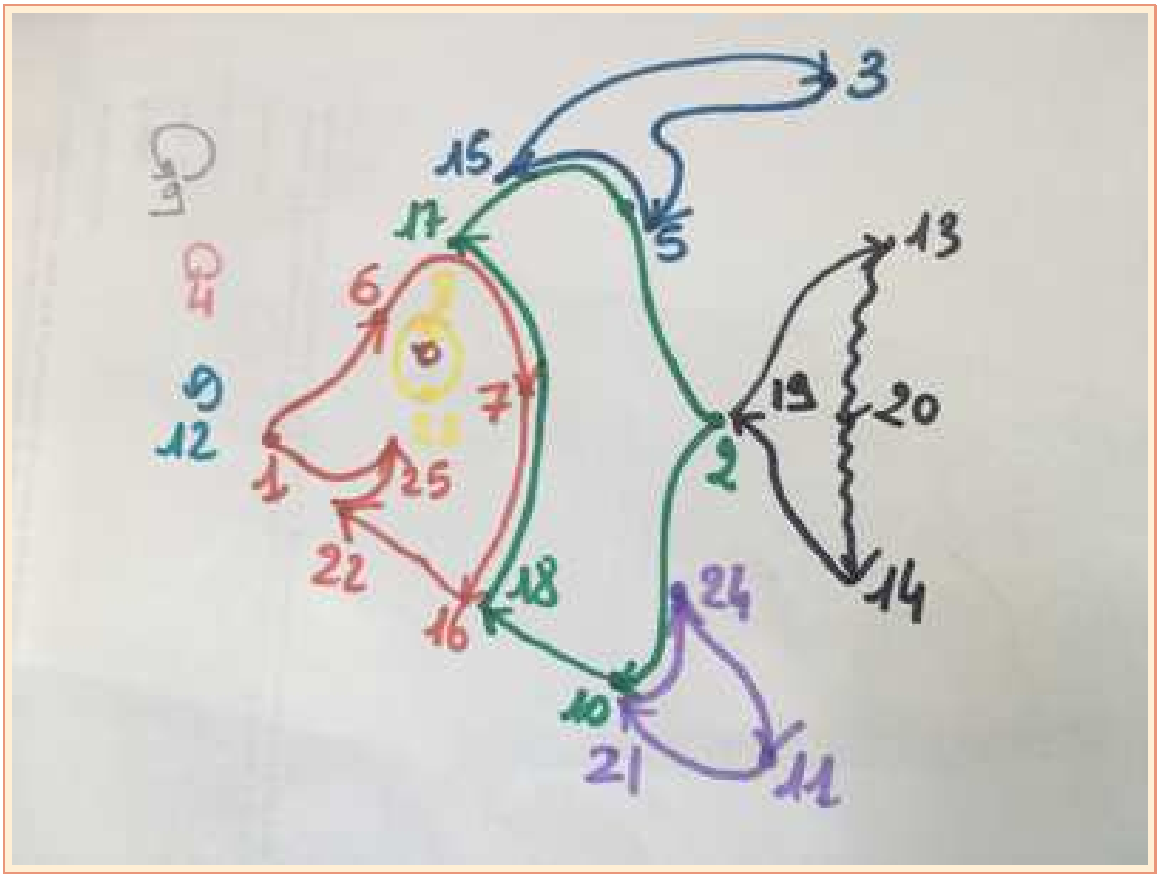
Voici ce que cela donne avec les couleurs :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 \\ 6 & 10 & 5 & 4 & 15 & 7 & 16 & 23 & 9 & 18 & 21 & 12 & 20 & 19 & 3 & 22 & 2 & 17 & 13 & 14 & 24 & 25 & 8 & 11 & 1 \end{pmatrix}.$$

On a donc les différentes orbites :

$\mathscr{O}(1) = \{1, 6, 7, 16, 22, 25\}$ $\mathscr{O}(2) = \{2, 10, 18, 17\}$ $\mathscr{O}(3) = \{3, 5, 15\}$ $\mathscr{O}(4) = \{4\}$	$\mathscr{O}(8) = \{8, 23\}$ $\mathscr{O}(9) = \{9\}$ $\mathscr{O}(11) = \{11, 21, 24\}$ $\mathscr{O}(12) = \{12\}$ $\mathscr{O}(13) = \{13, 20, 14, 19\}$

Voici un schéma possible pour représenter ces orbites :



C'est un poisson d'avril avant l'heure!!!

On voit sur le dessin les différentes trajectoires des éléments via la permutation σ.

On démontre la propriété 4, pour se familiariser avec les supports des permutations et leur importance vis-à-vis de la composition.
On considère σ et σ' deux permutations à support disjoints.
Soit $k \in [\![1, n]\!]$.
On distingue plusieurs cas sur l'entier k :

- si l'entier k est un point fixe de σ, alors $\sigma(k) = k$, puis :

$$\sigma' \circ \sigma(k) = \sigma'(k).$$

  Il y a deux sous-cas possibles.
  ▷ soit k est un point fixe de σ' auquel cas, $\sigma'(k) = k$ et donc $\sigma \circ \sigma'(k) = k = \sigma' \circ \sigma(k)$;
  ▷ soit k n'est pas un point fixe de σ', auquel cas, l'entier k fait partie d'une (seule) orbite de σ' et cette orbite $\mathscr{O}'(k)$ est de cardinal au moins 2. Il se trouve que $\sigma'(k)$ fait aussi partie de cette orbite, ce qui signifie que :

$$\mathscr{O}'(k) = \mathscr{O}'(\sigma'(k)),$$

  et donc que $\sigma'(k)$ appartient au support de σ'. Nécessairement, $\sigma'(k)$ ne fait pas partie du support de σ, donc est un point fixe de σ. Par conséquent,

$$\sigma(\sigma'(k)) = \sigma'(k),$$

et dans ce cas, :

$$\sigma \circ \sigma'(k) = \sigma'(k) = \sigma' \circ \sigma(k).$$

- si l'entier k n'est pas un point fixe de σ, alors k et $\sigma(k)$ font partie de la même orbite $\mathscr{O}(k)$ pour σ, orbite de cardinal supérieur ou égal à 2 : k et $\sigma(k)$ appartenant au support de σ ne peuvent appartenir au support de σ'. Ces deux entiers sont fixes par σ' et donc :

$$\sigma \circ \sigma'(k) = \sigma(k) = \sigma' \circ \sigma(k).$$

Quoiqu'il arrive, $\sigma \circ \sigma'(k) = \sigma' \circ \sigma(k)$ et les deux permutations commutent.

Les cycles et les transpositions

Un cycle est une permutation c n'ayant qu'une seule orbite de cardinal supérieur ou égale à 2. Si $\mathscr{O}(k) = \{k, c(k), \cdots, c^{r-1}(k)\}$ est cette seule orbite de cardinal $r \geqslant 2$, on notera alors :

$$c = (k, c(k), \cdots, c^{r-1}(k)).$$

On saura alors que tous les points de la liste $k, c(k), \cdots, c^{r-1}(k)$ sont transformés par c en le point suivant, sauf le dernier qui revient au début : $c(c^{r-1}(k)) = c^r(k) = k$ et que si i ne fait pas partie de la liste des entiers figurant dans l'orbite $\mathscr{O}(k)$, alors i est un point fixe pour c. On connaît donc le cycle c en tous les entiers entre 1 et n.

On voit donc qu'en posant les cycles :

- $c_1 = (1, 6, 7, 16, 22, 25)$
- $c_2 = (2, 10, 18, 17)$
- $c_3 = (3, 5, 15)$
- $c_4 = (8, 23)$
- $c_5 = (11, 21, 24)$
- $c_6 = (13, 20, 14, 19)$

alors les cycles c_i commutent deux à deux car leurs supports sont disjoints et :

$$\sigma = c_1 \circ c_2 \circ c_3 \circ c_4 \circ c_5 \circ c_6,$$

les cycles affectés aux orbites $\{4\}$ ou $\{9\}$ ou $\{12\}$ n'apparaissant pas car les cycles de longueur 1 associés valent id, donc peuvent être supprimés de la composition.

Le théorème 1 nous indique qu'il y a une unique décomposition de cycles à supports disjoints, dont la composition sera alors commutative. Bien entendu, l'unicité est garantie seulement à ordre près. Pour établir cette décomposition, il suffit pour cela de ne considérer que les orbites de σ de cardinal supérieur ou égal à 2. Pour chaque telle orbite, on crée un cycle c dont les éléments successifs sont les images successives par σ de n'importe quel élément de cette orbite. Il s'agit alors de composer tous ces cycles pour obtenir la permutation σ, à l'image de l'exemple ci-dessus.

En ce qui concerne l'unicité à ordre près, voici la démarche dans les grandes lignes :

- considérer une permutation $\sigma \in \mathfrak{S}_n$ quelconque
- partitionner $[\![1, n]\!]$ en les orbites $\mathscr{O}_1, \cdots, \mathscr{O}_r$ de σ

- considérer pour chaque orbite $\mathscr{O}_k = \{k, \sigma(k), \cdots, \sigma^{\ell_k - 1}(k)\}$ le cycle :

$$c_k = (k, \sigma(k), \cdots, \sigma^{\ell_k - 1}(k)).$$

On voit alors qu'on a déjà l'égalité :

$$\sigma = c_1 \circ c_2 \circ \cdots \circ c_r = c_1 c_2 \cdots c_r,$$

qui est une décomposition de σ en cycles à supports disjoints. On remarque dans l'écriture précédente que l'on peut mettre ou non les compositions $\circ$ dans les produits de composition. Parfois dans ce qui suivra, on omettra de les mettre par souci de notation...
Reste à voir que c'est la seule à ordre près. À remarquer que dans la décomposition précédente, si k est un point fixe, alors $\mathscr{O}(k) = \{k\}$, puis $c_k = (k) = \mathrm{id}$ et donc c_k peut ne pas apparaître dans le produit de composition pour σ.
- on veut maintenant démontrer par récurrence sur r la propriété suivante :
$\mathscr{P}(r)$: « si $\sigma \in \mathfrak{S}_n$ possède r orbites de cardinal $\geqslant 2$, alors il y a unicité à ordre près de sa décomposition de cycles à supports disjoints. »
- lorsque $r = 0$, on considère une permutation σ ne possédant aucun orbite qui n'est pas un singleton : $\sigma = \mathrm{id}$ et si $\sigma = d_1 \cdots d_s$ est un produit de cycles à supports disjoints, si $d_1 \neq \mathrm{id}$, alors d_1 possède une seule orbite de cardinal $\ell(d_1) = p_1$ et si k est dans cette orbite que l'on note $\mathscr{O}$, l'élément k est donc fixe par les autres cycles d_j, pour $j \geqslant 2$. Ainsi, $\sigma(k) = d_1(k)$. Cependant, $k \neq d_1(k)$ car $\mathscr{O}$ contient au moins deux éléments mais $\sigma(k) = k$. Résultat des courses, il n'y a aucun cycle d_j de longueur supérieure ou égale à 2 et chaque d_j vaut id. On a l'unicité dans ce cas.
- Supposons la propriété $\mathscr{P}(r)$.
- Donnons-nous une permutation σ possédant $(r+1)$ orbites de cardinal supérieur ou égal à 2. On peut donc écrire :

$$\sigma = c_1 \cdots c_{r+1},$$

où les c_k sont construits selon les orbites disjointes.
Considérons une autre décomposition :

$$\sigma = d_1 \cdots d_s,$$

avec chaque d_j qui est un cycle de longueur $\geqslant 2$.
On note $\mathscr{O}$ la seule orbite de d_s de cardinal $\geqslant 2$.
Soit $k \in \mathscr{O}$. Alors, $d_s(k) \neq k$ reste dans $\mathscr{O}$ et en considérant les images successives de k par les itérés de d_s, on obtient complètement l'orbite $\mathscr{O}$ pour avoir :

$$d_s = (k, d_s(k), \cdots, d_s^{\ell_s - 1}(k)),$$

de sorte que la longueur ℓ_s du cycle d_s est le plus petit entier strictement positif tel que :

$$d_s^{\ell_s}(k) = k.$$

Tous les éléments $d_s^p(k)$ – pour p décrivant $\mathbb{Z}$ – sont dans $\mathscr{O}$, donc sont fixes par les cycles $d_1, \cdots, d_{s-1}$.
On en déduit :

$$\sigma(k) = \Big(d_1 \cdots d_{s-1}\Big)(d_s(k)) = d_s(k).$$

Conclusion, le cycle d_s est exactement l'un des cycles c_j, avec j l'indice de l'orbite $\mathscr{O}_j$ de σ tel que :

$$\mathscr{O}_j = \mathscr{O}.$$

On a l'égalité :

$$\sigma = c_1 \cdots c_{r+1} = d_1 \cdots d_s,$$

ou encore l'égalité :

$$\rho = \sigma \circ c_j^{-1} = \prod_{q \neq j} c_q = d_1 \cdots d_{s-1}.$$

On peut appliquer l'hypothèse de récurrence à la permutation ρ qui admet r orbites de cardinal $\geqslant 2$. On a unicité de la décomposition pour ρ, puis en rajoutant c_j qui vaut d_s, alors on a unicité à ordre près de la décomposition pour σ.

Remarquons que si $c = (a_1, \cdots, a_r)$ est un cycle, alors le cycle c est aussi égal à $c = (a_2, a_3, \cdots, a_r, a_1)$ et la permutation c^{-1} est encore un cycle de même support que celui de c et où les éléments sont parcourus dans le sens inverse :

$$c^{-1} = (a_r, a_{r-1}, \cdots, a_1) = (a_1, a_r, a_{r-1}, \cdots, a_2),$$

par exemple.

Pour la permutation du poisson d'avril σ, cette permutation σ est composée de neuf orbites, dont six orbites de cardinal supérieur ou égal à 2 et l'égalité :

$$\sigma = c_1 \circ c_2 \circ c_3 \circ c_4 \circ c_5 \circ c_6,$$

est la décomposition en cycles à supports disjoints.

Pour l'exemple 1, voici la décomposition en cycles :

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

Bien évidemment, on peut permuter les cycles entre eux, ce qui donnera globalement la même composition σ et on peut permuter circulairement la représentation de chaque cycle. Par exemple,

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

alors que $(1, 7, 2) = (1, 2, 7)^{-1} \neq (1, 2, 7)$.
On peut aussi noter sans les symboles $\circ$ de composition :

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

Pour l'exemple 2, avant de calculer σ^{1001}, on décompose σ en cycles à supports disjoints. Faisons déjà le calcul. On trouve :

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

Comme les cycles commutent, alors :

$$\sigma^{1001} = (1, 10, 6)^{1001}\ (3, 7)^{1001}\ (4, 5, 11, 9, 8)^{1001}.$$

On remarque que si c est un cycle de longueur ℓ, alors on a toujours :

$$c^\ell = \mathrm{id}.$$

On en déduit qu'il suffit non pas de calculer c^{1001}, mais de faire la division euclidienne de 1001 par la longueur ℓ, puis de calculer en fait le reste r et donc :

$$c^{1001} = c^r,$$

avec r beaucoup plus petit que 1001 en général.
Ici, on obtient :

$$\begin{aligned}\sigma^{1001} = (1,10,6)^2\ (3,7)\ (4,5,11,9,8) &= (1,6,10)\ (3,7)\ (4,5,11,9,8) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 6 & 2 & 7 & 5 & 11 & 10 & 3 & 4 & 8 & 1 & 9 \end{pmatrix}.\end{aligned}$$

Parmi les cycles les plus simples figurent les cycles de longueur 2 appelés **transpositions**. Une transposition est une permutation (i,j) qui échangent deux éléments $i \neq j$, l'un avec l'autre. Ce sont des permutations utiles, notamment lors de l'algorithme du pivot de Gauss, avec l'opération $L_i \longleftrightarrow L_j$.

Si τ est une transposition (i,j), alors :

$$\tau^2 = \mathrm{id},\ \tau^{-1} = \tau \text{ et } \forall k \in \mathbb{Z},\ \tau^k = \begin{cases} \mathrm{id}, \text{ si } k \text{ est pair} \\ \tau, \text{ si } k \text{ est impair} \end{cases}.$$

Le théorème 2 s'obtient alors rapidement à l'aide du théorème 1. En effet, si σ est n'importe quelle permutation, on peut la décomposer en cycles à supports disjoints. Il suffit de pouvoir décomposer chaque cycle c en produit de transpositions pour obtenir σ comme un produit d'un produit de transpositions, et donc comme un (gros) produit de composition de transpositions. Or, on remarque que si $c = (a_1, \cdots, a_r)$ est un cycle, alors :

$$c = (a_1, a_2)(a_2, a_3) \cdots (a_{r-1}, a_r).$$

Vous pouvez vous amuser à tester cette égalité évaluée en n'importe quel entier : ça marche ! ! Il vous faudra distinguer trois cas, selon l'entier k choisi : soit $k \notin \mathrm{supp}(c)$, soit k est égal à a_i avec $1 \leqslant i < r$, soit $k = a_r$. Pour le premier k, k est fixe pour tout le monde. Dans le deuxième cas, k est successivement transformé en k, k, $\cdots$, k puis est transformé en a_{i+1} par la transposition (a_i, a_{i+1}), puis n'est plus modifié par les transpositions ultérieures (celles plutôt à gauche dans la composition). Dans le troisième cas, l'entier k est tranquillement transformé en a_{r-1}, puis a_{r-2}, etc. jusqu'à inexorablement terminer sa course en a_1 par la dernière transposition (a_1, a_2).

On remarque plusieurs choses quant à ces compositions de transpositions. Premièrement, la décomposition n'est pas du tout unique. Par exemple, on a :

$$\mathrm{id} = (1,2)(1,2),$$

ou encore :

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

ou encore :

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

Deuxièmement, les transpositions ne sont pas forcément à support disjoints. Imaginons qu'une permutation σ soit un produit de composition de transpositions à support disjoints :

$$\sigma = \tau_1\tau_2\cdots\tau_s.$$

Alors, $\sigma^2 = \tau_1^2\tau_2^2\cdots\tau_s^2 = \mathrm{id}\circ\mathrm{id}\circ\cdots\circ\mathrm{id} = \mathrm{id}$. Il n'est pas très difficile de montrer que si σ est permutation telle que :

$$\sigma^2 = \mathrm{id},$$

alors toutes les orbites de σ sont de cardinal 1 ou 2 et donc que l'on peut décomposer σ est un produit (éventuellement vide si $\sigma = \mathrm{id}$) d'autant de transpositions τ_k à supports disjoints que σ admet d'orbites de cardinal supérieur ou égal à 2.
Tout cycle de longueur $\ell \geqslant 3$ ne peut donc pas se décomposer en produit de transpositions à supports disjoints par exemple.

Le premier point de l'exemple 3 a donc déjà été traité, y compris dans la méthode du cours.
Une décomposition de la permutation $\sigma \in \mathfrak{S}_{2n}$ du second point de l'exemple 3 est :

$$\sigma = \prod_{k=1}^{n}(2k-1, 2k),$$

le produit étant bien entendu le produit de composition qui est ici commutatif car les transpositions mises en jeu sont à support disjoints.

La signature

La signature $\varepsilon(\sigma)$ d'une permutation σ est toujours un nombre valant ± 1. On le calcule de la manière suivante pour l'instant : on décompose σ en produit de cycles à supports disjoints et on applique la formule :

$$\varepsilon(\sigma) = (-1)^{\text{somme des longueurs des cycles - nombre de cycles}}.$$

On remarque dans cette formule que le résultat reste le même si l'on considère dans la décomposition de σ en cycles à supports disjoints, les cycles (a) à un seul élément (qui valent donc id) ou non.

Par exemple, dans l'exemple 4, comme id est un produit vide de cycles, alors :

$$\varepsilon(\sigma) = (-1)^{0-0} = 1.$$

Si c est un cycle de longueur ℓ, alors $c = c$ est la décomposition du cycle c en cycles à supports disjoints, donc la formule de la signature donne directement :

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

En particulier, pour les transpositions (cycles de longueurs 2), on obtient :

$$\varepsilon(\tau) = -1.$$

La signature de la permutation associée au poisson d'avril vaut :

$$\varepsilon(\sigma) = (-1)^{(6+4+3+2+3+4)-6} = 1.$$

Le théorème 3 est très étonnant. Démontrons-le.

Il s'agit de montrer que pour toutes permutations σ_1 et σ_2 dans $\mathfrak{S}_n$, alors :

$$\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1) \times \varepsilon(\sigma_2). \qquad \bigstar$$

On va décomposer la démonstration en plusieurs étapes.

- premièrement, on va montrer l'égalité $\bigstar$ lorsque σ est quelconque et lorsque σ' est une transposition (i, j).
  On pose $\sigma = c_1 \cdots c_r$ la décomposition de σ en produit de cycles à supports disjoints. On sait que les orbites des c_k sont exactement les orbites de la permutation σ. On note $\mathscr{O}_1, \cdots, \mathscr{O}_r$ les orbites respectives des cycles $c_1, \cdots, c_r$. On note $\ell_1, \cdots, \ell_r$ les longueurs respectives de ces cycles, de sorte que :

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

  On distingue alors quatre cas, selon les dispositions des entiers i et j vis-à-vis des orbites de σ.

  ▷ premier cas : les entiers i et j ne font partie d'aucune orbite $\mathscr{O}_k$. Dans ce cas, les points i et j sont fixes par σ et on peut écrire :

  $$\sigma \circ (i, j) = c_1 \cdots c_r \circ (i, j)$$

  qui est la décomposition de σ en produit de cycles à supports disjoints. Par conséquent, en appliquant la définition de la signature :

  $$\varepsilon(\sigma \circ (i, j)) = (-1)^{\ell_1 + \cdots + \ell_r + 2 - (r+1)} = -\varepsilon(\sigma).$$

  ▷ deuxième cas : un seul des deux entiers i et j fait partie d'une (seule) orbite $\mathscr{O}_k$. Mettons que i appartienne à $\mathscr{O}_k$ et que j ne soit dans aucune orbite.
  On peut alors écrire :

  $$c_k = (i, a_1, \cdots, a_s)$$

  et la décomposition de $c_k \circ (i, j)$ en cycles à supports disjoints est :

  $$c_k \circ (i, j) = (i, j, a_1, \cdots, a_s).$$

  Comme la décomposition de $\sigma \circ (i, j)$ en cycles à supports disjoints est donc :

  $$\sigma \circ (i, j) = \left(\prod_{q \neq k} c_q \right) \circ (i, j, a_1, \cdots, a_s)$$

alors il y a autant de cycles dans σ que dans $\sigma \circ (i,j)$, mais la somme des longueurs des cycles dans $\sigma \circ (i,j)$ est supérieure d'une unité à la somme des longueurs des cycles dans σ :

$$\varepsilon(\sigma) \circ (i,j)) = -\varepsilon(\sigma).$$

▷ troisième cas : les deux entiers i et j font partie de la même orbite $\mathscr{O}_k$. Par exemple, on peut écrire :

$$c_k = (i, a_1, \cdots, a_s, j, b_1, \cdots, b_m),$$

avec éventuellement $s = 0$ ou $m = 0$, si $c_k(i) = j$ ou $c_k(j) = i$.
On en déduit la décomposition de cycles à supports disjoints pour : $c_k \circ (i,j)$, qui est :

$$c_k \circ (i,j) = (i, b_1, \cdots, b_m) \circ (j, a_1, \cdots, a_s).$$

La décomposition de $\sigma \circ (i,j)$ en cycles à supports disjoints est donc :

$$\sigma \circ (i,j) = \left(\prod_{q \neq k} c_q \right) \circ (i, b_1, \cdots, b_m) \circ (j, a_1, \cdots, a_s).$$

La somme des longueurs des cycles pour $\sigma \circ (i,j)$ est égale à celle pour σ et $\sigma \circ (i,j)$ compte une orbite de plus que pour σ. Là encore :

$$\varepsilon(\sigma \circ (i,j)) = -\varepsilon(\sigma).$$

▷ quatrième cas : les deux entiers i et j font partie de deux orbites $\mathscr{O}_k$ et $\mathscr{O}_{k'}$ différentes. Par exemple, on peut poser :

$$c_k = (i, a_1, \cdots, a_s) \text{ et } c_{k'} = (j, b_1, \cdots, b_m).$$

La décomposition en cycles à supports disjoints pour $c_k \circ c_{k'} \circ (i,j)$ est donc :

$$c_k \circ c_{k'} \circ (i,j) = (i, b_1, \cdots, b_m, j, a_1, \cdots, a_s).$$

La décomposition de $\sigma \circ (i,j)$ en cycles à supports disjoints est donc :

$$\sigma \circ (i,j) = \left(\prod_{q \notin \{k,k'\}} c_q \right) \circ (i, b_1, \cdots, b_m, j, a_1, \cdots, a_s).$$

La somme des longueurs des cycles dans $\sigma \circ (i,j)$ est égale à celle pour σ alors que le nombre d'orbites dans $\sigma \circ (i,j)$ est inférieur d'une unité à celui pour σ. Une fois de plus,

$$\varepsilon(\sigma \circ (i,j)) = -\varepsilon(\sigma).$$

Quoiqu'il arrive, si $\sigma' = (i,j)$, alors :

$$\varepsilon(\sigma \circ \sigma') = -\varepsilon(\sigma) = \varepsilon(\sigma) \times \varepsilon(\sigma').$$

- deuxièmement, on montre que si σ est un produit de m transpositions, alors :

$$\varepsilon(\sigma) = (-1)^m.$$

En effet, on peut faire une récurrence sur l'entier m.
$\longrightarrow$ Si σ est un produit de 0 transpositions, alors σ est un produit vide, donc $\varepsilon(\sigma) = 1 = (-1)^m$ et la formule marche.
$\longrightarrow$ Supposons la formule vraie dès que σ est un produit de m transpositions.
$\longrightarrow$ Soit σ une permutation obtenue comme produit de $(m+1)$ transpositions :

$$\sigma = \tau_1\tau_2\cdots\tau_{m+1}.$$

On pose $\rho = \tau_1\tau_2\cdots\tau_m$ et $\rho' = \tau_{m+1}$. Par le début de la démonstration, puis par hypothèse de récurrence sur ρ, on sait que :

$$\varepsilon(\rho\circ\rho') = -\varepsilon(\rho) = -(-1)^m = (-1)^{m+1},$$

et de plus, $\rho\circ\rho' = \sigma$. La formule est juste au rang suivant.
- finalement, on revient au cas général où σ et σ' sont deux permutations quelconques. On écrit (décompositions non uniques) :

$$\sigma = \tau_1\cdots\tau_m \text{ et } \sigma' = \chi_1\cdots\chi_{m'},$$

des décompositions en transpositions. Par le deuxième point, on sait que :

$$\varepsilon(\sigma) = (-1)^m \text{ et } \varepsilon(\sigma') = (-1)^{m'}.$$

Or,

$$\sigma\circ\sigma' = \tau_1\cdots\tau_m\circ\chi_1\cdots\chi_{m'},$$

est un produit de composition de $m+m'$ transpositions. Toujours par le deuxième point de la démonstration,

$$\varepsilon(\sigma\circ\sigma') = (-1)^{m+m'}.$$

En conclusion,

$$\varepsilon(\sigma\circ\sigma') = (-1)^{m+m'} = (-1)^m\times(-1)^{m'} = \varepsilon(\sigma)\times\varepsilon(\sigma').$$

On dispose alors de deux moyens de calculer une signature $\varepsilon(\sigma)$: premièrement décomposer σ en produit de cycles à supports disjoints et on utilise la définition [c'est le mode de calcul le plus efficace] ; deuxièmement décomposer σ en un produit de s transpositions et donc :

$$\varepsilon(\sigma) = (-1)^s.$$

On remarque qu'il n'y a pas unicité de ces décompositions mais la parité du nombre de transpositions dans n'importe quelle décomposition de σ en transpositions est toujours la même.

Il y a une autre méthode pour calculer $\varepsilon(\sigma)$ en faisant intervenir le nombre d'inversions. Une inversion est un couple (i,j) avec $i<j$ tel que $\sigma(i)>\sigma(j)$.

On va démontrer la formule :

$$\forall \sigma \in \mathfrak{S}_n,\ \varepsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

La démonstration va nous faire réviser pas mal de choses ... Allons-y !!

On pose la fonction :

$$\Psi : \left| \begin{array}{ccc} \mathfrak{S}_n & \longrightarrow & \mathbb{R}^* \\ \sigma & \longmapsto & \displaystyle\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i} \end{array} \right. .$$

L'application Ψ est déjà bien à valeurs dans $\mathbb{R}^*$ car si $i < j$, alors $\sigma(i) \neq \sigma(j)$.
Ensuite, on va montrer que Ψ est un morphisme de groupes entre $(\mathfrak{S}_n, \circ)$ et $(\mathbb{R}^*, \times)$.

Soient σ_1 et σ_2 deux permutations. On écrit :

$$\begin{aligned} \Psi(\sigma_1 \circ \sigma_2) &= \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{j - i} \\ &= \left(\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(i)} \right) \times \left(\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma_2(j) - \sigma_2(i)}{j - i} \right) \\ &= \left(\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(i)} \right) \times \Psi(\sigma_2). \end{aligned}$$

Pour tout $\sigma \in \mathfrak{S}_n$, si $i < j$ sont deux entiers, on remarque que :

$$\frac{\sigma(j) - \sigma(i)}{j - i} = \frac{\sigma(i) - \sigma(j)}{i - j}.$$

On pose dans la suite :

$$\mathscr{P}_2 = \Big\{ A \subset [\![1, n]\!] \mid \mathrm{card}(A) = 2 \Big\}.$$

Pour tout $A = \{a, b\} \in \mathscr{P}_2$, on note :

$$\xi_\sigma(A) = \frac{\sigma(b) - \sigma(a)}{b - a},$$

car ce quotient ne dépend pas de l'ordre d'énumération de l'ensemble A selon $\{a, b\}$ ou $\{b, a\}$.
D'autre part, l'application $F_\sigma : A \longmapsto \sigma(A)$ est une bijection de $\mathscr{P}_2$ vers $\mathscr{P}_2$, en notant au passage que si $A = \{a, b\}$ est de cardinal 2, alors $\sigma(A) = \{\sigma(a), \sigma(b)\}$ aussi.
On en déduit :

$$\begin{aligned} \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(i)} &= \prod_{\{i,j\} \in \mathscr{P}_2} \xi_{\sigma_1}(\sigma_2(\{i, j\})) \\ &= \prod_{\{i,j\} \in \mathscr{P}_2} \xi_{\sigma_1}(F_{\sigma_2}(\{i, j\}) \\ &= \prod_{\{k,\ell\} \in \mathscr{P}_2} \xi_{\sigma_1}(\{k, \ell\}) \\ &= \Psi(\sigma_1). \end{aligned}$$

Conclusion,

$$\Psi(\sigma_1 \circ \sigma_2) = \Psi(\sigma_1) \times \Psi(\sigma_2).$$

L'application Ψ est bien un morphisme de groupes.

Ensuite, si $\sigma \in \mathfrak{S}_n$, le corollaire du théorème de Lagrange sur les groupes finis donne :

$$\sigma^{n!} = \mathrm{id}, \text{ donc } 1 = \Psi(\mathrm{id}) = \Psi(\sigma^{n!}) = \Psi(\sigma)^{n!}.$$

Le nombre $\Psi(\sigma) = a$ est donc un réel qui est une racine $(n!)^{ème}$ de l'unité : $a \in \{-1, 1\}$ et Ψ prend en fait ses valeurs dans le groupe $\{-1, 1\}$ muni de la multiplication $\times$.

$\triangleright$ Lorsque $n = 1$, on a directement que la seule permutation possible est $\sigma = \mathrm{id}$ et donc l'application Ψ est constante sur $\mathfrak{S}_1 = \{\mathrm{id}\}$ égale à 1, tout comme la signature ε :

$$\Psi = \varepsilon$$

dans ce cas.

$\triangleright$ Plaçons-nous maintenant dans le cas $n \geqslant 2$.

On va calculer $\Psi(\tau)$, avec τ la transposition :

$$\tau = (1, 2).$$

On fixe $1 \leqslant i < j \leqslant n$ deux entiers.

$\longrightarrow$ si $i \geqslant 3$, alors :

$$\frac{\tau(j) - \tau(i)}{j - i} = \frac{j - i}{j - i} = 1.$$

$\longrightarrow$ si $i = 2$ et $j \geqslant 3$, alors :

$$\frac{\tau(j) - \tau(i)}{j - i} = \frac{j - 1}{j - 2}.$$

$\longrightarrow$ si $i = 1$ et $j \geqslant 3$, alors :

$$\frac{\tau(j) - \tau(i)}{j - i} = \frac{j - 2}{j - 1}.$$

$\longrightarrow$ si $i = 1$ et $j = 2$, alors :

$$\frac{\tau(j) - \tau(i)}{j - i} = \frac{1 - 2}{2 - 1} = -1.$$

On voit alors que pas mal de simplifications s'opérent dans le produit $\displaystyle\prod_{1 \leqslant i < j \leqslant n} \frac{\tau(j) - \tau(i)}{j - i}$. Il ne reste que (-1) et donc :

$$\Psi((1, 2)) = -1.$$

On montre maintenant que si ρ est n'importe quelle transposition (i, j) alors :

$$\Psi(\tau) = -1.$$

En effet, si $\tau = (i,j)$ est une transposition, avec donc nécessairement $i \neq j$, les deux ensembles $[\![3,n]\!]$ et $[\![1,n]\!] \setminus \{i,j\}$ comptent le même nombre d'éléments à savoir $n-2$ éléments. On peut donc avoir une bijection χ entre les deux ensembles.
On définit alors la permutation $\sigma \in \mathfrak{S}_n$ de la façon suivante :

$$\sigma : \left| \begin{array}{ccc} [\![1,n]\!] & \longrightarrow & [\![1,n]\!] \\ k & \longmapsto & \left\{ \begin{array}{l} i, \text{ si } k = 1 \\ j, \text{ si } k = 2 \\ \chi(k), \text{ si } k \notin \{1,2\} \end{array} \right. \end{array} \right. .$$

Ainsi, $\sigma(1) = i$ et $\sigma(2) = j$.
On va maintenant montrer une formule qui peut s'avérer utile en pratique pour la résolution d'exercices sur les permutations :

$$\sigma \circ (1,2) \circ \sigma^{-1} = (i,j).$$

Prenons un entier k entre 1 et n. On distingue trois cas :

$\longrightarrow$ si $k \notin \{i,j\}$, alors $(i,j)(k) = k$ et $\sigma^{-1}(k) \notin \{1,2\}$, donc :

$$\sigma \circ (1,2) \circ \sigma^{-1}(k) = \sigma \circ (1,2)\Big(\sigma^{-1}(k)\Big) = \sigma\Big(\sigma^{-1}(k)\Big) = k.$$

$\longrightarrow$ si $k = i$, alors $(i,j)(k) = j$ et $\sigma^{-1}(k) = 1$, donc :

$$\sigma \circ (1,2) \circ \sigma^{-1}(k) = \sigma \circ (1,2)\Big(\sigma^{-1}(k)\Big) = \sigma \circ (1,2)\Big(1\Big) = \sigma(2) = j.$$

$\longrightarrow$ si $k = j$, alors $(i,j)(k) = i$ et $\sigma^{-1}(k) = 2$, donc :

$$\sigma \circ (1,2) \circ \sigma^{-1}(k) = \sigma \circ (1,2)\Big(\sigma^{-1}(k)\Big) = \sigma \circ (1,2)\Big(2\Big) = \sigma(1) = i.$$

On a bien ce qu'il faut.

On applique maintenant le morphisme de groupes Ψ :

$$\begin{array}{rcl} \Psi((i,j)) & = & \Psi\Big(\sigma \circ (1,2) \circ \sigma^{-1}\Big) \\ & = & \Psi(\sigma) \times \Psi((1,2)) \times \Psi(\sigma^{-1}) \\ & = & \Psi(\sigma) \times \Psi((1,2)) \times \Psi(\sigma)^{-1} \\ & = & \Psi((1,2)) = -1. \end{array}$$

En conclusion, si σ est une permutation quelconque, on écrit σ comme un produit de transpositions :

$$\sigma = \tau_1 \tau_2 \cdots \tau_s,$$

de façon à avoir :

$$\Psi(\sigma) = \Psi(\tau_1) \times \Psi(\tau_2) \times \cdots \times \Psi(\tau_s) = (-1)^s = \varepsilon(\sigma).$$

Ainsi,

$$\Psi = \varepsilon,$$

et l'application Ψ est bien la signature.

Remarque : le résultat est peu utile car cette formule donne des calculs très peu exploitables en pratique ; la démonstration est intéressante. C'est bien de la comprendre, sans que ce soit primordial.

Je ne détaille l'exemple 5, qui a partiellement été traité.

Démontrons le corollaire 1 pour conclure cette section sur les permutations...

Si $n \geqslant 2$ est en entier, on sait que la signature $\varepsilon(\cdot)$ est un morphisme de groupes. On découvre alors que l'ensemble $\mathscr{A}_n$ des permutations paires est le noyau de la signature :

$$\mathscr{A}_n = \mathrm{Ker}(\varepsilon).$$

En tant que noyau d'un morphisme de groupes, l'ensemble $\mathscr{A}_n$ est bien un sous-groupe de $\mathfrak{S}_n$. De plus, en posant τ la transposition $(1,2)$, on remarque que si σ est une permutation paire, alors $\sigma \circ \tau$ est une permutation impaire, l'application $\sigma \longmapsto \sigma \circ (1,2)$ étant bijective, car il s'agit d'une involution sur $\mathfrak{S}_n$.
L'application :

$$\Lambda : \left| \begin{array}{ccc} \mathscr{A}_n & \longmapsto & \mathfrak{S}_n \setminus \mathscr{A}_n \\ \sigma & \longmapsto & \sigma \circ \tau \end{array} \right.$$

est donc déjà bien définie, est bijective (ce n'est pas une involution car la composée de Λ avec elle-même est interdite pour cause d'ensembles de départ et d'arrivée disjoints). Les ensembles $\mathscr{A}_n$ et $\mathfrak{S}_n \setminus \mathscr{A}_n$ ont le même cardinal fini, qui vaut la moitié du cardinal de $\mathfrak{S}_n$:

$$\mathrm{Card}(\mathscr{A}_n) = \mathrm{Card}(\mathfrak{S}_n \setminus \mathscr{A}_n) = \frac{n!}{2}.$$

Pour être tout à fait complet, lorsque $n = 1$, alors :

$$\mathscr{A}_1 = \mathfrak{S}_1 = \{\mathrm{id}\}.$$