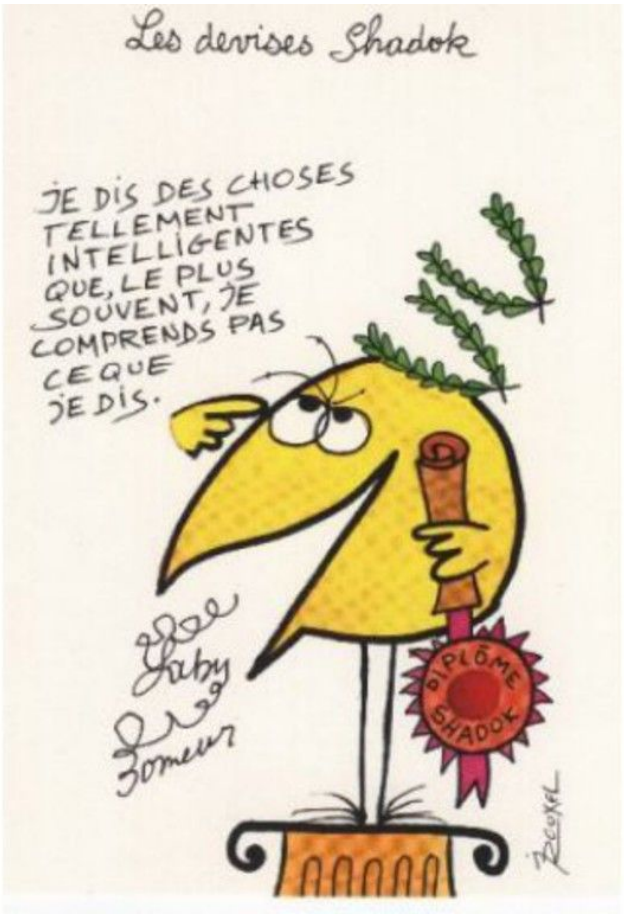
Lycée Loges

Chapitre 23
Groupe Symétrique

Simon Dauguet
simon.dauguet@gmail.com

1er avril 2025



Les ensembles finis jouent un rôle très important en mathématiques : dans toutes les sommes, on sommes les éléments d'un ensemble finis. Comprendre les ensembles finis et particulièrement les bijections sur les ensembles finis est alors indispensable. Sur les sommes, une bijection sur l'ensemble des éléments de la somme correspond à une réordonnation des éléments de la somme ; cela correspond à sommes les mêmes éléments mais dans un autre ordre. Autrement dit, c'est la généralisation des changements d'indices que nous avons vu en début d'année.

> An important thing to know is that there will always be at least as many permutations of a set as combinations, and typically many more permutations than combinations.
>
> Scott Hartshorn,
> A Beginner's Guide To Permutations And Combinations

Table des matières

1 Permutations

1.1 Généralités

Définition 1.1 (Permutations, Groupe symétrique) :
Soit E un ensemble. On appelle permutation de E toute bijection de E dans E. L'ensemble des permutations de E est noté $\mathfrak{S}(E)$.

Si $E = [\![1, n]\!]$ avec $n \in \mathbb{N}^*$, on appelle groupe symétrique d'ordre n l'ensembles des permutations de $[\![1, n]\!]$. On note $\mathfrak{S}_n$ le groupe symétrique d'ordre n.

Notation :
Soit $n \in \mathbb{N}^*$. Si $\sigma \in \mathfrak{S}_n$, on notera

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

une permutation.

Le "S" gothique ($\mathfrak{S}$) n'étant pas forcément facile à dessiner à la main, on pourra aussi noter $\mathcal{S}(E)$ et $\mathcal{S}_n$ les ensembles de permutations. Usuellement, sur les documents dactylographiés, on utilise le "S" gothique (pour des raisons de provenance historique entre autre) pour faire la distinction avec la notation $\mathcal{S}_n$ qui est plus ou moins déjà utilisé et qui peut donc porter à confusion.

Exemple 1.1 :
Si on se place dans $\mathfrak{S}_6$, la permutation

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

est une permutation dont 1 et 6 sont des points fixes.

Déterminer $\sigma^2(3)$ et $\sigma^{-3}(2)$.

Proposition 1.1 (Structure de $\mathfrak{S}_n$) :
Soit $n \in \mathbb{N}^*$. Alors $(\mathfrak{S}_n, \circ)$ est un groupe de cardinal $n!$. De plus, $(\mathfrak{S}_n, \circ)$ est non abélien si et seulement si $n \geq 3$.

Démonstration :
C'est facile. On le sait déjà. On a déjà vu dans le chapitre sur les groupes que $(S(E), \circ)$ est un

groupe non abélien. Ici, $\mathfrak{S}_n = S(\{1,\dots,n\})$. Donc $(\mathfrak{S}_n, \circ)$ est un groupe non abélien (si $n = 1$, $\mathfrak{S}_1 = \{\mathrm{Id}_{\{1\}}\}$ et $\mathfrak{S}_2$ n'est composé que de deux éléments).

Pour dénombrer le nombre d'éléments de $\mathfrak{S}_n$, on va construire une permutation σ et compter le nombre de choix à notre disposition. Pour faire une permutation à n éléments, il faut envoyer d'abord le 1 sur n'importe quel éléments de $\{1,\dots,n\}$. Nous avons donc n choix. Puis, pour 2, il faut l'envoyer également dans $\{1,\dots,n\}$. Mais σ doit être injective, donc $\sigma(1) \neq \sigma(2)$. Et donc $\sigma(2)$ est un élément de $\{1,\dots,n\} \setminus \{\sigma(1)\}$. Il reste donc $(n-1)$ choix pour $\sigma(2)$. Puis, par injectivité, on doit également avoir $\sigma(3) \in \{1,\dots,n\} \setminus \{\sigma(1), \sigma(2)\}$. Ce qui nous laisse $n-2$ choix pour $\sigma(3)$. D'une manière générale, pour $k \in \{1,\dots,n\}$, on doit avoir $\sigma(k) \in \{1,\dots,n\} \setminus \{\sigma(1),\dots,\sigma(k-1)\}$ pour conserver l'injectivité. Donc, pour $k \in \{1,\dots,n\}$, on a $n-k+1$ choix. En fabricant ainsi une injection, elle sera automatiquement surjective. En effet, l'ensemble $\{\sigma(1),\dots,\sigma(n)\}$ ne contient que des valeurs deux à deux distinctes, donc c'est un ensemble à n éléments et c'est un sous-ensemble de $\{1,\dots,n\}$ qui a également n éléments. Ils sont donc égaux et donc σ est surjective.

On vient donc de construire un éléments de $\mathfrak{S}_n$. À chaque étape, pour chacun des choix fait précédemment, on dispose de tous les $n-k+1$ choix possibles. Autrement dit, on a en tout

$$\prod_{k=1}^{n} (n-k+1) = n!$$

choix possible. Et donc $\mathfrak{S}_n$ a bien $n!$ éléments.

(Voir le chapitre sur le dénombrement en fin d'année pour plus de détails.) □

Remarque :
Si $\mathrm{Card}(E) = n$, alors $\mathfrak{S}(E)$ et $\mathfrak{S}_n$ sont équipotents (*i.e.* ont le même nombre d'éléments) (et même isomorphes comptes tenus que ce sont des groupes). En effet, en ayant une bijection $\varphi : E \to [\![1,\dots,n]\!]$, on peut alors "transporter" les permutations de l'un des ensembles sur l'autre. Il suffit de voir que $\forall \sigma \in \mathfrak{S}(E)$, $\varphi \circ \sigma \circ \varphi^{-1} \in \mathfrak{S}_n$.

On en déduit immédiatement que $\mathfrak{S}(E)$ est une groupe de cardinal $n!$.

Exemple 1.2 :
Dans $\mathfrak{S}_4$, on pose

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

Alors

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

Et

$$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \text{et} \quad \sigma'^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = \sigma'.$$

Remarque :
On se placera désormais sur $\mathfrak{S}_n$ par soucis de commodité, mais par une bijection, il est facile de transposer tous les résultats à $\mathfrak{S}(E)$ avec $\mathrm{Card}(E) = n$.

1.2 Ordres et Orbites

Définition-Propriété 1.2 (Ordre d'une permutation) :
Soit $n \in \mathbb{N}^*$. Soit $\sigma \in \mathfrak{S}_n$.
L'ordre de σ est la plus petite puissance non nulle de σ qui donne l'identité, *i.e.*

$$\omega(\sigma) = \min\{k \in \mathbb{N}^*,\ \sigma^k = 1\}.$$

Démonstration :
Soit $\sigma \in \mathfrak{S}_n$. Alors $\{\sigma, \sigma^2, \ldots, \sigma^{n!+1}\}$ est une sous-ensemble de $\mathfrak{S}_n$ de cardinal $n! + 1 > n! = \mathrm{Card}(\mathfrak{S}_n)$. Donc, par le principe des tiroirs, $\exists k, k' \in \{1, \ldots, n! + 1\}$, $k < k'$ tels que $\sigma^k = \sigma^{k'}$. Et donc $\sigma^{k-k'} = 1$. Et $k - k' \geq 1$. Donc $\{k \in \mathbb{N}^*,\ \sigma^k = 1\}$ est non vide. Et c'est un sous-ensemble de $\mathbb{N}$. Donc ... □

Exemple 1.3 :
L'ordre de la permutation du premier exemple est 4.

Proposition 1.2 (Majorant de l'ordre d'une permutation) :
Soit $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$.
Alors $\omega(\sigma) \leq n!$.

Démonstration :
On considère $\{\sigma^k,\ 1 \leq k \leq n! + 1\}$. Par structure de groupe de $\mathfrak{S}_n$, c'est un sous-ensemble de $\mathfrak{S}_n$. Mais $\mathfrak{S}_n$ ne contient que $n!$ éléments. Donc, par principe des tiroirs, $\exists k, \ell \in \{1, \ldots, n! + 1\}$ avec $k \neq \ell$ tels que $\sigma^k = \sigma^\ell$. Et donc $\sigma^{k-\ell} = \mathrm{Id}$. Donc $\omega(\sigma) \leq k - \ell \leq n!$. □

Remarque (HP) :
Le théorème Lagrange affirme qu'en fait, dans un groupe fini, l'ordre de n'importe quel élément divise le cardinal du groupe. Autrement dit, ici, $\forall \sigma \in \mathfrak{S}_n$, $\omega(\sigma) | n!$.

Définition 1.3 (Orbites) :
Soit $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$ et $x \in \{1, \dots, n\}$.
On appelle *orbite de x sous σ*, l'ensemble des images successives de x sous l'action de σ, *i.e.*

$$\mathcal{O}_\sigma(x) = \{\sigma^k(x),\ k \in \mathbb{Z}\}.$$

L'ensembles des orbites des éléments $x \in \{1, \dots, n\}$ sous l'action de σ sont les orbites de σ.

Proposition 1.3 (Orbites) :
Soit $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$. Alors

$$x \sim y \iff \exists k \in \mathbb{Z},\ y = \sigma^k(x)$$

est une relation d'équivalence sur $[\![1, n]\!]$ dont les classes d'équivalences sont les orbites de σ, *i.e.* $\forall x \in [\![1, n]\!]$, $\mathrm{Cl}(x) = \mathcal{O}_\sigma(x)$.
En particulier, les orbites ne sont jamais vides, sont finies et forment une partition de $[\![1, n]\!]$.

Démonstration :
Il suffit de vérifier que la relation est une relation d'équivalence. Et ensuite, la définition des classes d'équivalences fait le reste. □

Remarque :
Une orbite n'est jamais réduite à un point sauf si c'est un point fixe de σ. *i.e.*

$$\forall x \in \{1, \dots, n\},\ \Big(\mathrm{Card}(\mathcal{O}_\sigma(x)) = 1 \iff \sigma(x) = x\Big).$$

Exemple 1.4 :
On reprend la permutation du premier exemple. Donner les orbites de σ.

Corollaire 1.4 (Cardinal d'une orbite) :
Soit $n \in \mathbb{N}^*$, $\sigma \in \mathfrak{S}_n$ et $x \in \{1, \dots, n\}$. Alors

$$\exists \ell \in \{1, \dots, \omega(\sigma)\},\ \mathcal{O}_\sigma(x) = \{x, \sigma(x), \dots, \sigma^{\ell-1}(x)\}$$

(donc les éléments sont deux à deux distincts). En particulier, $\mathrm{Card}(\mathcal{O}_\sigma(x)) \leq \omega(\sigma)$.

Démonstration :
On considère $\{k \in \mathbb{N}^*,\ \sigma^k(x) = x\}$. C'est ensemble est non vide car $\omega(\sigma)$ est dedans. Donc il admet un minimum ℓ.

Soit $k \in \mathbb{Z}$. En effectuant la division euclidienne de k par ℓ, $\exists (q, r) \in \mathbb{Z} \times \{0, \dots, \ell - 1\}$ tel que $k = q\ell + r$. Alors

$$\sigma^k(x) = \left(\sigma^r \circ (\sigma^\ell)^q\right)(x) = \sigma^r(x)$$

Donc $\mathcal{O}_\sigma(x) \subset \{x, \sigma(x), \dots, \sigma^{\ell-1}(x)\}$. Et l'autre inclusion est évidente.

De plus, si $\exists p, q \in \{1, \dots, \ell - 1\}$ avec $p \neq q$ tel que $\sigma^p(x) = \sigma^q(x)$, alors $\sigma^{p-q}(x) = x$, ce qui contredit la minimalité de ℓ. □

1.3 Support d'une permutation

Définition 1.4 (Support d'une permutation) :
Soit $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$.

Le support de σ est l'ensemble des éléments qui ne sont pas invariants sous l'action de σ, *i.e.*

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

Remarque :
Autrement dit, $\mathrm{Supp}(\sigma)$ correspond aux éléments qui sont "déplacés" par σ, c'est donc la partie qui est intéressante, celle qui est porteuse d'informations sur σ, sur la façon dont σ fonctionne.

Exemple 1.5 :
Si on reprend $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ et $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, alors $\mathrm{Supp}(\sigma) = \{1, 2, 3, 4\}$ et $\mathrm{Supp}(\sigma') = \{1, 3\}$.

Proposition 1.5 (Support d'une permutation) :
Soit $n \in \mathbb{N}^*$ et $\sigma \in \mathfrak{S}_n$. Alors

$$\mathrm{Supp}(\sigma) = \bigcup_{\substack{x=1 \\ \sigma(x)\neq x}}^{n} \mathcal{O}_\sigma(x)$$

Donc $\mathrm{Supp}(\sigma)$ est la réunion de toutes les orbites de σ qui ne sont pas des singletons.

Démonstration :
Soit $y \in [\![1, n]\!]$ tel que $\exists x \in [\![1, n]\!]$ tel que $\sigma(x) \neq x$ et $y \in \mathcal{O}_\sigma(x)$. Alors $\exists \ell \in \{1, \dots, \omega(\sigma)\}$ tel que $\mathcal{O}_\sigma(x) = \{x, \sigma(x), \dots, \sigma^{\ell-1}(x)\}$. Et donc $\exists k \in \{0, \dots, \ell - 1\}$ tel que $y = \sigma^k(x)$. Alors $\sigma(y) = \sigma^{k+1}(x) \neq \sigma^k(x) = y$ car $\sigma(x) \neq x$. Donc $y \in \mathrm{Supp}(\sigma)$.
Si $y \in \mathrm{Supp}(\sigma)$, alors $y \in \mathcal{O}_\sigma(y)$ et $\sigma(y) \neq y$. D'où l'égalité. □

Exemple 1.6 :
Avec $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 4 & 2 & 6 & 5 \end{pmatrix}$, on a $\mathrm{Supp}(\sigma) = \{2, 3, 4, 5, 6\}$ et $\mathcal{O}_\sigma(2) = \{2, 3, 4\}$, $\mathcal{O}_\sigma(5) = \{5, 6\}$.

Proposition 1.6 (Propriétés des supports) :
Soit $n \in \mathbb{N}^*$ et $\sigma, \tau \in \mathfrak{S}_n$.

(i) $\mathrm{Supp}(\sigma)$ est stable par σ

(ii) Si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset$, alors σ et τ commutent.

Démonstration :

(i) Si $i \in \mathrm{Supp}(\sigma)$, alors $\sigma(i) \neq i$. Donc $\sigma^2(i) \neq \sigma(i)$ par injectivité. Et donc $\sigma(i) \in \mathrm{Supp}(\sigma)$.

(ii) Si $i \notin \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)$, alors $\sigma(i) = i = \tau(i)$. Et donc $\sigma \circ \tau(i) = i = \tau \circ \sigma(i)$.
Si $i \in \mathrm{Supp}(\sigma)$, alors $i \notin \mathrm{Supp}(\tau)$. Et donc $\sigma \circ \tau(i) = \sigma(i)$. Mais $\sigma(i) \in \mathrm{Supp}(\sigma)$ car le support est stable d'après le premier point. Donc $\sigma(i) \notin \mathrm{Supp}(\tau)$. Et donc $\tau \circ \sigma(i) = \sigma(i)$.
De même, par le même raisonnement en inversant σ et τ, on a $\tau \circ \sigma(i) = \sigma \circ \tau(i)$ pour $i \in \mathrm{Supp}(\tau)$.
Finalement, on a bien $\sigma \circ \tau = \tau \circ \sigma$ puisque $[\![1, n]\!] = \mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau) \cup \overline{\mathrm{Supp}(\sigma) \cup \mathrm{Supp}(\tau)}$.
□

Exemple 1.7 :
On considère les permutations

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}, \ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}, \ \gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}$$

Étudier la commutativité des trois permutations.

!!! ATTENTION !!!

⚠ Ce n'est qu'une implication ! Deux permutations dont les supports ne sont pas disjoints peuvent commuter quand même !

En revanche, si σ et τ ne commutent pas, alors $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) \neq \emptyset$.

Contre-exemple :
Prendre $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ et $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$.

Proposition 1.7 (Ordre de permutations à supports disjoints) :
Soit $\sigma, \tau \in \mathfrak{S}_n$.
Si $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset$, alors $\omega(\sigma \circ \tau) = \mathrm{ppcm}(\omega(\sigma), \omega(\tau))$.

Démonstration :
Comme les supports sont disjoints, σ et τ commutent. Donc $\forall k \in \mathbb{N}$, $(\sigma \circ \tau)^k = \sigma^k \circ \tau^k$. Si on pose $d = \omega(\sigma) \vee \omega(\tau)$. Alors $\sigma^d = \mathrm{Id} = \tau^d$.

Et si $d = \omega(\sigma \circ \tau)$, alors, par commutativité $\sigma^d \circ \tau^d = \mathrm{Id}$. Or $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset$, donc si $\sigma^d \neq \mathrm{Id}$, alors $\sigma^d \circ \tau^d \neq \mathrm{Id}$. Donc $\sigma^d = \mathrm{Id} = \tau^d$. Donc $\omega(\sigma) | d$ et $\omega(\tau) | d$. Donc $\omega(\sigma) \vee \omega(\tau) | d$. Puis, par définition de l'ordre (qui est un minimum), on en déduit $d = \omega(\sigma) \vee \omega(\tau)$. □

Remarque :
Évidemment, on peut faire une récurrence pour appliquer ce résultat sur un permutation qui serait le produit de plusieurs permutations à supports disjoints.

1.4 Transpositions et Cycles

Définition 1.5 (Transpositions) :
Soit $n \geq 2$.

Une *transposition* est une permutation qui échange deux éléments et laisse fixe tous les autres éléments, *i.e.* $\tau \in \mathfrak{S}_n$ est une transposition si $\exists i, j \in \{1, \dots, n\}$ avec $i \neq j$ tel que $\tau(i) = j$, $\tau(j) = i$ et $\forall k \in \{1, \dots, n\} \setminus \{i, j\}$, $\tau(k) = k$.

On la note $(i\ j)$ ou parfois $\tau_{i,j}$.

Proposition 1.8 (Caractérisation des transpositions) :
Soit $n \geq 2$ et $\tau \in \mathfrak{S}_n$.

τ est une transposition si, et seulement si, $\mathrm{Card}(\mathrm{Supp}(\tau)) = 2$.

Démonstration :
C'est évident. □

Proposition 1.9 (Propriétés des transpositions) :
Soit $n \geq 2$. Alors

(i) Il y a $\binom{n}{2} = \frac{n(n-1)}{2}$ transpositions dans $\mathfrak{S}_n$.

(ii) $\forall i, j \in \{1, \dots, n\}$, si $i \neq j$, alors $(i\ j) = (j\ i)$.

(iii) Toute transposition est une involution, donc d'ordre 2.

Démonstration :

(i) Une transposition est entièrement déterminer par son support. Il y a autant de transpositions que l'on peut choisir de couples de deux valeurs différentes dans $\{1, \dots, n\}$, donc autant de transpositions que de sous-ensembles de cardinal de 2 dans $[\![1, n]\!]$.

(ii) C'est évident.

(iii) La aussi, c'est évident.

□

!!! ATTENTION !!!

La réciproque du (iii) est fausse si $n \geq 4$! ! !

Contre-exemple :
Si $\sigma = (1\ 2) \circ (3\ 4)$, alors $\sigma^2 = 1$ mais pourtant σ n'est pas une transposition.

Définition 1.6 (Cycles) :
Soit $n \geq 2$ et $p \in \{2, \dots, n\}$.

On appelle *p-cycle* une permutation $c \in \mathfrak{S}_n$ qui permutent circulairement p éléments de $[\![1, n]\!]$ et laisse les autres éléments invariants, *i.e.* si il existe des entiers $1 \leq i_1 < i_2 < \cdots < i_p \leq n$ tel que $\forall j \in \{1, \dots, p-1\}$, $c(i_j) = i_{j+1}$ et $c(i_p) = i_1$ et $\forall k \in \{1, \dots, n\} \setminus \{i_1, \dots, i_p\}$, $c(k) = k$.

p est la longueur du cycle c. On note $c = (i_1\ i_2\ \dots\ i_p)$.

Donc $(i_1\ i_2\ \dots\ i_p)$ correspond à

$$i_1 \rightsquigarrow i_2 \rightsquigarrow i_3 \rightsquigarrow \cdots \rightsquigarrow i_{p-1} \rightsquigarrow i_p \rightsquigarrow i_1$$

Remarque :
L'ordre dans lequel on présente la permutation circulaire n'a pas d'importance, tant qu'on ne change pas l'ordre de la permutation.

Exemple 1.8 :
On a

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

Remarque :
On notera que l'identité n'est pas un cycle. Un cycle doit obligatoirement déplacer au moins deux éléments.

Remarque :
Les 2-cycles sont les transpositions.

!!! ATTENTION !!!

⚠ Les notations sont trompeuses ! Le cycle $(1\ 2\ 3)$ est à la fois un éléments de $\mathfrak{S}_3$, $\mathfrak{S}_4$, $\mathfrak{S}_5$ etc. De même pour les transpositions. Dans la notations d'une transposition ou d'un cycle, le nombre d'éléments sur lequel s'applique la permutation est sous-entendu et dépend du contexte. La notation développée avec les deux lignes est plus explicite de ce point de vue : tous les éléments du départ sont apparent, il n'y a pas d'ambiguïté.

Bien faire attention au contexte et donc à l'endroit où vit la transposition ou le cycle que l'on considère. $(1\ 2) \in \mathfrak{S}_2$ ou $(1\ 2) \in \mathfrak{S}_5$, ce n'est pas la même chose.

Proposition 1.10 (Propriétés des cycles) :
Soit $n \geq 2$.

(i) Un cycle de $\mathfrak{S}_n$ de longueur n est appelé une permutation circulaires sur $[\![1, n]\!]$. Il y a exactement $(n-1)!$ permutation circulaire sur $[\![1, n]\!]$.

(ii) Si $p \in \{2, \dots, n\}$, le nombre de p-cycles dans $\mathfrak{S}_n$ est $\binom{n}{p}(p-1)! = \frac{n(n+1)\dots(n-p+1)}{p}$.

(iii) Les cycles sont les permutations possédant exactement une orbite non réduite à un point.

Démonstration :

(i) Une permutation circulaire avec 1 dans le support est un cycle de la forme $(1\ \sigma(1)\ \sigma^2(1)\ \dots\ \sigma^{n-1}(1))$. Donc pour faire une permutation circulaire σ (donc qui ne peux être l'identité), on peut envoyer 1 sur n'importe quel entier autre que 1 (pour ne pas avoir de point fixe). Donc on a $n-1$ choix possible pour $\sigma(1)$. Ensuite, pour faire un cycle, il faut envoyer $\sigma(1)$ sur un entier qui ne soit pas 1 (pour avoir une permutation circulaire) ni $\sigma(1)$, donc on a $n-2$ choix. Et à chaque étape, pour choisir $\sigma^k(1)$, on a $n-k-1$ choix possible. Et σ^{n-1} est obligatoirement renvoyé sur 1, qui sera le dernier éléments qui n'aura pas d'antécédent. Donc $(n-1)!$ permutations circulaires.

(ii) Pour faire un p-cycle, on peut procéder comme précédemment en choisissant les images successives de $\sigma(i_1)$. Ou alors, pour faire un p cycle, il suffit de choisir un support à p élément

et de faire ensuite une permutation circulaire sur le support. Or on a $\binom{n}{p}$ façon de choisir un support à p éléments. Et on a ensuite $(p-1)!$ permutations circulaire sur ce support, d'après la question précédente. D'où le résultat.

(iii) Si $c \in \mathfrak{S}_n$ est un cycle, alors $\forall k \notin \mathrm{Supp}(c)$, $c(k) = k$ donc $\forall k \notin \mathrm{Supp}(c)$, $\mathcal{O}_c(k) = \{k\}$. Et $\forall i \in \mathrm{Supp}(c)$, $\mathcal{O}_c(i) = \mathrm{Supp}(c)$.

Réciproquement, supposons $\exists p \in \{2, \dots, n\}$, $\exists i_1, \dots, i_p \in \{1, \dots, n\}$ tel que $\{i_1, \cdots_p\}$ soit une orbite de c et toutes les autres orbites sont réduites à un point. Donc $\forall k \in [\![1, n]\!] \setminus \{i_1, \dots, i_p\}$, $\mathcal{O}_c(k) = \{k\}$. Alors $\forall j \in \{1, \dots, p\}$, $\mathcal{O}_c(i_j) = \{i_1, \dots, i_p\}$. Ce qui veut dire, par définition des orbites, que $\{i_1, \dots, i_p\} = \{c^r(i_1),\ r \in \mathbb{N}\}$ et donc que c est un cycle.

□

Proposition 1.11 (Décomposition en transposition d'un cycle) :
Soit $n \geq 2$, $2 \leq p \leq n$ et $i_1, \dots, i_p \in \{1, \dots, n\}$ deux à deux distincts. Alors

$$(i_1\ i_2\ \dots\ i_p) = (i_1\ i_p)(i_1\ i_{p-1}) \dots (i_1\ i_2) = (i_1\ i_2)(i_2\ i_3) \dots (i_{p-1}\ i_p)$$

Démonstration :
Il suffit de regarder les images de chaque entier : si $k \in \{1, \dots, p-1\}$, alors

$$\left(\prod_{j=1}^{p-1} (i_1\ i_{p-j+1}) \right) (i_k) = (i_1\ i_p) \dots (i_1\ i_{k+2})(i_1\ i_{k+1})(i_1\ i_k)(i_k) = i_{k+1}$$

et

$$\left(\prod_{j=1}^{p-1} (i_j\ i_{j+1}) \right) (i_k) = (i_1\ i_2) \dots (i_{k-1}\ i_k)(i_k\ i_{k+1})(i_k) = i_{k+1}$$

et de même pour i_p. □

Proposition 1.12 (Ordre d'un cycle) :
Soit $2 \leq p \leq n$.
Un p-cycle est d'ordre p

Démonstration :
On a $\mathrm{Supp}(c) = \{c^k(x),\ k \in \mathbb{N}\}$ et $\mathrm{Card}(\mathrm{Supp}(c)) = p$. □

Exemple 1.9 ([✓]) :
Montrer que si $\sigma \in \mathfrak{S}_n$, alors

$$\sigma(i_1\ i_2\ \ldots\ i_p)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \ldots\ \sigma(i_p))$$

Théorème 1.13 (Décomposition de permutations en cycles) :
Toute permutation se décompose en composée de cycles à supports disjoints. La décomposition est unique à l'ordre des cycles près.

Démonstration :
Les supports étant disjoints, les cycles vont commuter. D'où l'unicité à l'ordre près.

Soit $\sigma \in \mathfrak{S}_n$. Soit $x_1, \ldots, x_p$ des représentants de chacune des orbites des σ qui ne sont pas réduites à un point. Donc $\forall k \in \{1, \ldots, p\}$, $\mathcal{O}_\sigma(x_k) \neq \{x_k\}$ et $\forall y \in \{1, \ldots, n\}$, soit $\mathcal{O}_\sigma(y) = \{y\}$ soit $\exists k \in \{1, \ldots, p\}$, tel que $y \in \mathcal{O}_\sigma(x_k)$.

Alors, $\forall k \in \{1, \ldots, p\}$, $\exists \ell_k \in \mathbb{N}^*$ tel que $\mathcal{O}_\sigma(x_k) = \{x_k,\ \sigma(x_k),\ \ldots,\ \sigma^{\ell_k - 1}(x_k)\}$ et $\sigma^{\ell_k}(x_k) = x_k$. On pose

$$\tau = \prod_{k=1}^{p} (x_k\ \sigma(x_k)\ \ldots\ \sigma^{\ell_k - 1}(x_k))$$

Alors si $y \notin \mathrm{Supp}(\sigma)$, alors $\tau(y) = \sigma(y) = y$ et si $y \in \mathrm{Supp}(\sigma)$, alors $\tau(y) = \sigma(y)$ (si $y \in \mathrm{Supp}(\sigma)$, alors $\exists k \in \{1, \ldots, p\}$ tel que $y \in \mathcal{O}_\sigma(x_k)$ et donc $y = \sigma^r(x_k)$ puis $\tau(y) = \sigma^{r+1}(x_k) = \sigma(y)$, en prenant garde à ne pas "déborder" de l'orbite). □

Remarque :
La démonstration, comme souvent, fournit une méthode pour décomposer une permutation en produit de cycles :

- On fait la liste des toutes les orbites de σ en notant les éléments de chaque orbites par ordres croissant de composition de σ
- σ est alors le produit de toutes les permutations circulaires sur les orbites non triviales.

Exemple 1.10 :
Faire la décomposition en produit de cycles de la permutations :

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

Corollaire 1.14 :
Toute permutation est le produit de transpositions.

Démonstration :
C'est évident avec ce qui précède. On décompose σ en produit de cycles sur les orbites de σ, puis on découpe les cycles en transpositions. □

Remarque :
Une fois décomposée en produit de cycles, l'ordre d'une permutation est alors le ppcm des ordres des cycles qui le composent car ceux-ci commutent car les supports sont disjoints. Autrement dit, l'ordre d'une permutation est le ppcm des cardinaux de ses orbites.

2 Signature

2.1 Signature d'une permutation

Définition 2.1 (Inversion d'une permutation, Signature, Permutation paire/impaire) :
Soit $n \in \mathbb{N}^*$. Soit $\sigma \in \mathfrak{S}_n$.

On appelle *inversion de* σ tout couple (i, j) avec $1 \leq i < j \leq n$ tel que $\sigma(i) > \sigma(j)$. Autrement dit, une inversion est un couple d'entier ordonné par ordre croissant sur lequel la permutation σ est décroissante. On note $\mathrm{Inv}(\sigma)$ le nombre d'inversion de σ.

On appelle *signature de* σ le nombre $\varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)} \in \{-1, 1\}$.

La permutation σ est dite *paire* si $\varepsilon(\sigma) = 1$ (*i.e.* si $\mathrm{Inv}(\sigma)$ est paire) et elle est dite impaire sinon.

Remarque (Détermination pratique du nombre d'inversions) :
Pour déterminer le nombre $\mathrm{Inv}(\sigma)$ d'une permutation, on :

- On écrit σ sous forme d'un tableau explicite comme dans la première définition de tous les entiers et leurs images sur une deuxième ligne
- Pour chaque entier-image, on compte le nombre d'image plus petit *sur sa droite*
- On fait la somme.

Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 10 & 6 & 4 & 2 & 1 & 7 & 5 & 8 & 9 \end{pmatrix}$. Alors :

Images	3	10	6	4	2	1	7	5	8	9
Nombre d'images plus petites	2	8	4	2	1	0	1	0	0	0

Donc $\mathrm{Inv}(\sigma) = 2+8+4+2+1+1 = 18$. Donc $\varepsilon(\sigma) = 1$ et σ est paire.

Remarque :
Dans la littérature, on peut trouver une autre définition d'une inversion. On peut définir une inversion comme un ensemble $\{i,j\}$ avec $i \neq j$ tel que $(i-j)(\sigma(i)-\sigma(j)) < 0$. En effet, on a soit $i<j$ et $\sigma(i) > \sigma(j)$, donc (i,j) est une inversion ; ou alors $i > j$ et $\sigma(i) < \sigma(j)$ et donc (j,i) sera une inversion.

Les deux définitions sont utiles. L'avantage de la première est de permettre d'éviter facilement de faire des doublons. Mais ce n'est pas très agréable à manipuler. Ma seconde à l'avantage d'être plus facile à manipuler. Mais pas forcément plus facile à dénombrer compte tenu de la potentielle redondance (en fait non, c'est un biais cognitif).

Proposition 2.1 (Expression de la signature) :
Soit $n \in \mathbb{N}^*$. Alors

$$\forall \sigma \in \mathfrak{S}_n,\ \varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)} = \prod_{1 \leq i < j \leq n} \frac{\sigma(j)-\sigma(i)}{j-i}$$

Démonstration :
On note $\mathcal{P}_2 = \{\{i,j\},\ 1 \leq i \neq j \leq n\}$ l'ensembles des sous-parties de $\{1,\dots,n\}$ a deux éléments. Alors

$$\varphi : \begin{array}{ccc} \{(i,j),\ 1 \leq i < j \leq n\} & \to & \mathcal{P}_2 \\ (i,j) & \mapsto & \{i,j\} \end{array}$$

est évidement (bien définie et) une injection. Mais on a mieux :

$$\psi : \begin{array}{ccc} \mathcal{P}_2 & \to & \{(i,j),\ 1 \leq i < j \leq n\} \\ \{i,j\} & \mapsto & (\min(i,j), \max(i,j)) \end{array}$$

est également bien définie et l'inverse de φ (facile à vérifier). Donc φ est une bijection. De plus,

$$\mu_\sigma : \begin{array}{ccc} \mathcal{P}_2 & \to & \mathcal{P}_2 \\ \{i,j\} & \mapsto & \{\sigma(i),\sigma(j)\} \end{array}$$

est une bijection et $\mu_\sigma^{-1} = \mu_{\sigma^{-1}}$. Alors, si on note $\mathcal{C} = \{(i,j),\ 1 \leq i < j \leq n\}$,

$$\begin{aligned} \prod_{1 \leq i < j \leq n} |\sigma(j)-\sigma(i)| &= \prod_{(i,j) \in \mathcal{C}} |\sigma(j)-\sigma(i)| \\ &= \prod_{\{i,j\} \in \mathcal{P}_2} |\sigma(j)-\sigma(i)| \\ &= \prod_{\mu_{\sigma^{-1}}(\{i,j\}) \in \mathcal{P}_2} |\sigma(j)-\sigma(i)| \\ &= \prod_{\{\sigma^{-1}(i),\sigma^{-1}(j)\} \in \mathcal{P}_2} |\sigma(j)-\sigma(i)| \end{aligned}$$

$$= \prod_{\{i,j\}\in\mathcal{P}_2} |j-i|$$
$$= \prod_{(i,j)\in\mathcal{C}} |j-i|$$
$$= \prod_{1\leq i<j\leq n} |j-i|$$

D'où

$$\prod_{1\leq i<j\leq n} (\sigma(j)-\sigma(i)) = \prod_{\substack{1\leq i<j\leq n\\ \sigma(i)<\sigma(j)}} (\sigma(j)-\sigma(i)) \overbrace{\prod_{\substack{1\leq i<j\leq n\\ \sigma(i)>\sigma(j)}} (\sigma(j)-\sigma(i))}^{\mathrm{Inv}(\sigma) \text{ facteurs}}$$
$$= (-1)^{\mathrm{Inv}(\sigma)} \prod_{1\leq i<j\leq n} |\sigma(j)-\sigma(i)|$$
$$= (-1)^{\mathrm{Inv}(\sigma)} \prod_{1\leq i<j\leq n} |j-i|$$

et d'où le résultat. □

Proposition 2.2 (Imparité des transpositions) :
Toute transposition est impaire.

Démonstration :
Soit $\tau = (i\ j)$ avec $1 \leq i < j \leq n$. Alors

$$\tau = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}$$

Donc :

- $\forall k \in \{i+1, \dots, j\}$, $\tau(i) = j > \tau(k)$, donc (i,k) est une inversion.
- Si $i+1 \leq k < \ell \leq j-1$, (k,ℓ) n'est pas une inversion.
- $\forall k \in \{i+1, \dots, j-1\}$, $\tau(k) > \tau(j) = i$ donc (k,j) est une inversion.
- Tous les autres couples (donc (k,ℓ) avec $k < \ell \leq i-1$ ou $j+1 \leq k < \ell$ ou $k < i < \ell < j$ ou $i < k < j < \ell$) ne sont pas des inversions.

Donc le nombre d'inversions est

$$\mathrm{Inv}(\tau) = (j-i-1+1) + (j-1-i-1+1) = 2(j-i)-1$$

et donc τ est impaire. □

Proposition 2.3 (La signature est un morphisme de groupe) :
Soit $n \geq 1$.

$$\forall \sigma, \sigma' \in \mathfrak{S}_n,\ \varepsilon(\sigma \circ \sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$$

Démonstration (Non exigibles) *:*
Pour montrer $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$, par définition de la signature, il suffit de comparer le nombres d'inversion de $\sigma\sigma'$ et celui de σ et de σ'.

Pour ce faire, on peut classer les couples (i, j) tels que $i < j$ en quatre cas :

- $\sigma'(i) < \sigma'(j)$ et $\sigma \circ \sigma'(i) < \sigma \circ \sigma'(j)$. On note N_1 le nombres de tels couples.
- $\sigma'(i) < \sigma'(j)$ et $\sigma \circ \sigma'(i) > \sigma \circ \sigma'(j)$. On note N_2 le nombres de tels couples.
- $\sigma'(i) > \sigma'(j)$ et $\sigma \circ \sigma'(i) < \sigma \circ \sigma'(j)$. On note N_3 le nombres de tels couples.
- $\sigma'(i) > \sigma'(j)$ et $\sigma \circ \sigma'(i) > \sigma \circ \sigma'(j)$. On note N_4 le nombres de tels couples.

Par définition, $\mathrm{Inv}(\sigma')$ est le nombres de couples (i, j) avec $i < j$ tels que $\sigma'(i) > \sigma'(j)$. Donc

$$\mathrm{Inv}(\sigma') = N_3 + N_4.$$

Le nombre d'inversions de $\sigma\circ\sigma'$ est le nombres de couples (i, j) avec $i < j$ tels que $\sigma\circ\sigma'(i) > \sigma\circ\sigma'(j)$, donc

$$\mathrm{Inv}(\sigma \circ \sigma') = N_2 + N_4.$$

C'est plus délicat pour le nombres d'inversions de σ. Notons $\mathcal{P}_2(E)$ l'ensembles des sous-ensembles de cardinal 2 de E et

$$\varphi : \begin{array}{ccc} \{(i,j) \in [\![1,n]\!]^2,\ i<j\} & \to & \mathcal{P}_2(\{1,\dots,n\}) \\ (i,j) & \mapsto & \{\sigma'(i), \sigma'(j)\} \end{array}$$

Alors observons que φ est bien définie puisque σ' est une bijection (donc si $i \neq j$, alors $\sigma'(i) \neq \sigma'(j)$ et donc $\{\sigma'(i), \sigma'(j)\}$ est bien de cardinal 2). De plus, φ est une bijection. En effet,

$$\psi : \begin{array}{ccc} \mathcal{P}_2(\{1,\dots,n\}) & \to & \{(i,j) \in [\![1,n]\!]^2,\ i<j\} \\ \{k,\ell\} & \mapsto & \Big(\min(\sigma'^{-1}(k), \sigma'^{-1}(\ell)), \max(\sigma'^{-1}(k), \sigma'^{-1}(\ell))\Big) \end{array}$$

En effet, si $\{k, \ell\} \in \mathcal{P}_2(\{1, \dots, n\})$, alors $k \neq \ell$. Par bijectivité de σ' (et plus précisément injectivité de σ'^{-1}), $\sigma'^{-1}(k) \neq \sigma'^{-1}(\ell)$. Donc cette application est bien définie. Et il n'est pas très difficiles de vérifier que c'est bien l'inverse de φ.

Or, compter les couples (k, ℓ) tels que $k < \ell$ et $\sigma(k) > \sigma(\ell)$, revient à compter les ensembles $\{k, \ell\}$ distincts tels que

$$\begin{cases} k < \ell \\ \sigma(k) > \sigma(\ell) \end{cases} \quad \text{ou} \quad \begin{cases} k > \ell \\ \sigma(k) < \sigma(\ell) \end{cases}$$

(attention, l'adjectif distinct est très important pour le pas compter deux fois le même ensemble, il faut (k, ℓ) ne correspondent qu'à un seul ensemble).

Mais par la bijection φ introduite précédemment, cela revient donc à compter les coupes (i,j) avec $i<j$ tel que

$$\begin{cases}\sigma'(i)<\sigma'(j)\\ \sigma(\sigma'(i))>\sigma(\sigma'(j))\end{cases} \quad \text{ou} \quad \begin{cases}\sigma'(i)>\sigma'(j)\\ \sigma(\sigma'(i))<\sigma(\sigma'(j))\end{cases}$$

D'où

$$\mathrm{Inv}(\sigma)=N_2+N_3$$

Finalement, $\varepsilon(\sigma)\varepsilon(\sigma')=(-1)^{2N_3+N_2+N_4}=(-1)^{N_2+N_4}=\varepsilon(\sigma\sigma')$. □

Remarque :
Autrement dit, $\varepsilon:(\mathfrak{S}_n,\circ)\to(\{-1,1\},\times)$ est un morphisme de groupe.

!!! ATTENTION !!!

⚠ Il n'y a pas commutativité au niveau de $\mathfrak{S}_n$ mais il y a commutativité au niveau des signatures. Autrement dit, $\sigma\sigma'\neq\sigma'\sigma$ en général, mais $\varepsilon(\sigma\sigma')=\varepsilon(\sigma'\sigma)$.

Proposition 2.4 (Propriétés de la signature) :
Soit $n\geq 1$. Alors

(i) Si c est un p-cycle de $\mathfrak{S}_n$, alors $\varepsilon(c)=(-1)^{p-1}$

(ii) $\forall\sigma\in\mathfrak{S}_n$, $\varepsilon(\sigma^{-1})=\varepsilon(\sigma)$

Démonstration :
C'est assez évident avec la propriété multiplicative de la signature. □

Remarque :
Il n'existe que deux morphismes de groupes de $\mathfrak{S}_n$ dans $\{-1,1\}$. L'un est l'application $\sigma\mapsto 1$ qui n'a pas beaucoup d'intérêt. Et le second est le morphisme de signature.

D'ailleurs :

Théorème 2.5 (Unicité de la signature) :
La signature est l'unique application $\varepsilon : \mathfrak{S}_n \to \{-1, 1\}$ telle que :

(i) Pour toute transposition τ, $\varepsilon(\tau) = -1$

(ii) $\forall \sigma, \sigma' \in \mathfrak{S}_n$, $\varepsilon(\sigma\sigma') = \varepsilon(\sigma)\varepsilon(\sigma')$.

Démonstration :
En effet, si φ est une application telle que (ii) est vérifiée et si il existe une transposition τ telle que $\varphi(\tau) = -1$, alors si τ' est une transposition, $\exists \sigma \in \mathfrak{S}_n$ tel que $\tau' = \sigma\tau\sigma^{-1}$. Et donc $\varphi(\tau') = \varphi(\tau)$. Donc φ envoie toute transposition sur -1. Et donc par suite, $\varphi = \varepsilon$ en décomposant une permutations en produit de transpositions. □

Exemple 2.1 :
Montrer que si $\sigma \in \mathfrak{S}_n$ et p est le nombre d'orbites de σ, alors $\varepsilon(\sigma) = (-1)^{n-p}$.

2.2 Groupe alterné

Définition 2.2 (Groupe alterné) :
Soit $n \geq 1$.
L'ensemble des permutations paires de $\mathfrak{S}_n$, noté $\mathfrak{A}_n$ est appelé le *groupe alterné d'ordre* n. Donc

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

Notation :
La lettre "$\mathfrak{A}$" est "A" gothique, pour Alterné et rappeler le groupe symétrique. Il est évident qu'on pourra écrire $\mathcal{A}_n$ à la main, comme pour le groupe symétrique.

Remarque :
La signature ε est un morphisme de groupe de $(\mathfrak{S}_n, \circ)$ dans $(\{-1, 1\}, \times)$. $\mathfrak{A}_n$ est alors le noyau de ce morphisme de groupes. La propriété suivante sera alors automatique. On pourrait même aller un peu plus loin.

Proposition 2.6 (Structure de $\mathfrak{A}_n$) :
Soit $n \geq 1$.
$\mathfrak{A}_n$ est un sous-groupe de $\mathfrak{S}_n$ et

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

Démonstration :
Par multiplicativité de la signature, le produit de deux permutations paires est une permutation paire. Et donc $\mathfrak{A}_n$ est stable par le produit. De même, la réciproque d'une permutation paire est de nouveau paire. Donc $\mathfrak{A}_n$ est stable par symétrisation. Et donc $\mathfrak{A}_n$ est un sous-groupe de $\mathfrak{S}_n$ car il contient l'identité.

Notons $\mathfrak{I}_n = \{\sigma \in \mathfrak{S}_n,\ \varepsilon(\sigma) = -1\}$. Soit τ une transposition de $\mathfrak{S}_n$. On considère les applications

$$\varphi : \begin{array}{ccc} \mathfrak{A}_n & \to & \mathfrak{I}_n \\ \sigma & \mapsto & \tau \circ \sigma \end{array}$$

φ est bien définie et $\varphi^2 = \mathrm{Id}_{\mathfrak{A}_n}$. Donc φ est bijective. Donc $\mathrm{Card}(\mathfrak{A}_n) = \mathrm{Card}(\mathfrak{I}_n)$. Par ailleurs, $\mathfrak{S}_n = \mathfrak{A}_n \cup \mathfrak{I}_n$. D'où $2|\mathfrak{A}_n| = |\mathfrak{S}_n| = n!$ et donc le résultat. □

Remarque :
En particulier, il y a autant de permutations paires que de permutations impaires.

Remarque (HP) :
L'étude des groupes alternés et des groupes symétriques est, en fait, très riche. Mais pour cela, on a besoin de pouvoir "comparer" des groupes et donc d'avoir la notion de morphismes de groupes à notre disposition. Ce qui sera fait en MP.

Mais par exemple, $\mathfrak{S}_4$ contient $4! = 24$ permutations. Et $\mathfrak{A}_4$ contient 12 permutations qui sont

$$\mathfrak{A}_4 = \left\{ \begin{array}{l} 1,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3), \\ (1\ 2) \circ (3\ 4),\ (1\ 3) \circ (2\ 4),\ (1\ 4) \circ (2\ 3) \end{array} \right\}$$

On peut poser $G = \{1,\ (1\ 2) \circ (3\ 4),\ (1\ 3) \circ (2\ 4),\ (1\ 4) \circ (2\ 3)\}$. Alors G est uns sous-groupe commutatif de $\mathfrak{A}_4$ d'ordre 4, qui s'appelle le groupe de Klein. On peut montrer qu'il est isomorphe à $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, +)$. On peut également montrer que tout groupe d'ordre 4 est soit isomorphe à $(\mathbb{Z}/4\mathbb{Z}, +)$ soit au groupe de Klein (classification des groupes d'ordres 4). Il y a toute une ramification de la théorie des groupes visant à classifier les groupes finis. Une grosse partie de cette classification est due à Galois.

On peut montrer aussi que $\mathfrak{A}_4$ ne possède aucun sous-groupe d'ordre 6 (même si $\mathfrak{A}_4$ est lui même d'ordre 12). En effet, les sous-groupes de $\mathfrak{A}_4$ sont soit cycliques (donc engendré par un élément), soit isomorphes à D_6, le groupe diédral des isométries du triangle équilatéral (3 rotations, 3 symétries). Le groupe diédral D_6 est d'ailleurs isomorphe à $\mathfrak{S}_3$. Donc $\mathfrak{A}_4$ contient, à isomorphisme près, le groupe $\mathfrak{S}_3$.