Le groupe des permutations d'un ensemble fini

1 Introduction

1.1 Rappels

Théorème 1.1 . *Soit E un ensemble. On appelle permutation de E, une bijection de E dans E. L'ensemble des permutations de E, muni de la composition classique des applications est un groupe, appelé groupe des permutations de E (ou groupe symétrique de E), noté $(S_E, \circ)$ ou encore S_E.*

Preuve. La composée de deux bijections de E dans E est une bijection de E dans E, donc $\circ$ est bien une opération interne sur S_E. L'application réciproque d'une bijection de E dans E est une bijection une bijection de E dans E, qui est l'élément symétrique pour l'opération $\circ$. □

Remarque 1.2 *Le groupe symétrique est en général un groupe non commutatif (la composition des applications n'est pas une opération commutative). Dans la suite, on omettra souvent $\circ$: la composée de deux permutations α et β sera notée $\alpha\beta$ plutôt que $\alpha \circ \beta$.*

Dans la suite, nous allons nous intéresser au cas où E est un ensemble fini. Dans ce cas, on peut toujours renommer (ou coder) les éléments de E par les entiers de 1 à n. Nous allons nous intéresser au cas où $E = \{1, 2, \ldots, n\}$. Dans ce cas, le groupe symétrique S_E est noté S_n.

Remarque 1.3 *S_n est un groupe fini d'ordre $n!$ et pour $n > 2$, S_n est non-abélien*[1].

1.2 Première notation pour un élément σ de S_n.

Une première notation classique est un tableau à 2 lignes et n colonnes. La première ligne contient les éléments $1, 2 \ldots, n$ dans l'ordre croissant. En dessous de chaque élément i de la première ligne, apparaît son image $\sigma(i)$. Par exemple,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

[1]Les groupes S_n sont des exemples très important de groupes finis. On peut montrer (théorème de Cayley) que tout groupe fini est isomorphe à un groupe de permutation, (i.e. à un renommage de ses éléments près, est un groupe de permutation).

désigne la permutation de $\{1,2,3\}$, telle que $\sigma(1)=3$, $\sigma(2)=2$ et $\sigma(3)=1$.

1.3 Un premier exemple: S_3

Comme déjà évoqué, ce groupe a $3!=6$ éléments. On peut les évoquer tous en notation tableau à deux lignes:

$$Id=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}\quad \tau_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\quad \tau_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\quad \tau_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$

$$\sigma_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\quad \sigma_1=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

Dressons la table de multiplication du groupe. Pour cela, il faut effectuer le calcul des composés deux à deux des six permutations précédentes. Calculons par exemple $\tau_1\tau_2$:

$$\tau_1\tau_2(1)=\tau_1(\tau_2(1))=\tau_1(3)=2,\quad \tau_1\tau_2(2)=\tau_1(\tau_2(2))=\tau_1(2)=3,$$

$$\tau_1\tau_2(3)=\tau_1(\tau_2(3))=\tau_1(1)=1,\quad \text{donc}\quad \tau_1\tau_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\sigma_1.$$

En ayant effectué tous les calculs de produits deux à deux, on obtient la table suivante où sur la ligne s et la colonne s', on lit $s\circ s'$:

	Id	τ_1	τ_2	τ_3	σ_1	σ_2
Id	Id	τ_1	τ_2	τ_3	σ_1	σ_2
τ_1	τ_1	Id	σ_1	σ_2	τ_2	τ_3
τ_2	τ_2	σ_2	Id	σ_1	τ_3	τ_1
τ_3	τ_3	σ_1	σ_2	Id	τ_1	τ_2
σ_1	σ_1	τ_3	τ_1	τ_2	σ_2	Id
σ_2	σ_2	τ_2	τ_3	τ_1	Id	σ_1

On vérifiera en exercice que τ_1,τ_2,τ_3 sont des éléments d'ordre 2, et que σ_1 et σ_2 sont des éléments d'ordre 3. On peut remarquer que S_3 n'est pas un groupe cyclique (sinon il serait en particulier abélien). D'après le théorème de Lagrange, les sous-groupes de S_3, ne peuvent être que d'ordres $1,2,3$ ou 6. En dehors des sous-groupes triviaux, il ne peut exister que des sous-groupes d'ordres 2 ou 3. On montrera en exercice qu'un groupe d'ordre un nombre premier est cyclique. Comme 2 et 3 sont nombres premiers, les sous-groupes d'ordre 2 ou 3 sont donc des sous-groupes cycliques. Il existe trois sous-groupes d'ordre 2, $\{Id,\tau_1\},\{Id,\tau_2\}$ et $\{Id,\tau_3\}$ et un sous–groupe d'ordre 3, $\{Id,\sigma_1,\sigma_2\}$.

2 Décomposition d'une permutation en produit de cycles à supports disjoints

Nous allons présenter plusieurs factorisations d'une permutation de S_n comme produits de permutations plus simples appelées des *cycles*.

Définition 2.1 *Soit $\sigma \in S_n$. On appelle un* point fixe *d'une permutation $\sigma \in S_n$, un élément i de $\{1,\dots,n\}$, qui reste fixe sous l'action de σ, i.e. tel que $\sigma(i) = i$. On appelle support de σ et on note* $\mathrm{supp}(\sigma)$*, l'ensemble des éléments i de $\{1,\dots,n\}$, qui ne sont pas des points fixes de la permutation, i.e. tels que $\sigma(i) \neq i$:*

$$\mathrm{supp}(\sigma) = \{i : \quad 1 \leq i \leq n \ et \ \ \sigma(i) \neq i\}.$$

Définition 2.2 *Soit $i_1, i_2, \dots, i_r$, des éléments deux à deux distincts de $\{1,\dots,n\}$. On appelle cycle de longueur r, la permutation $\sigma \in S_n$, ayant comme support l'ensemble $\{i_1, i_2, \dots, i_r\}$ et telle que*

$$\sigma(i_1) = i_2, \quad \sigma(i_2) = i_3, \quad \dots \quad , \sigma(i_{r-1}) = i_r \quad et \quad \sigma(i_r) = i_1.$$

La permutation σ est alors notée $(i_1 \ i_2 \ \ \dots \ i_r)$.

Voici quelques exemples,

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

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

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

Un cycle de longueur 1 est l'identité. Un cycle de longueur 2 est appelé *transposition*.

Remarque 2.3 *Dans un cycle σ de longueur r, $(i_1 \ i_2 \ \ \dots \ i_r)$, les éléments $i_2, \dots, i_r$ sont les itérés de i_1 sous l'action de σ.*

$$\sigma(i_1) = i_2, \quad i_3 = \sigma(i_2) = \sigma(\sigma(i_1)) = \sigma \circ \sigma(i_1) = \sigma^2(i_1), \quad \dots \quad , i_r = \sigma^{r-1}(i_1).$$

Remarque 2.4 *On peut noter un cycle de longueur r en commençant par un élément de son support et continuant avec les itérés de cet élément. Ainsi tout cycle de longueur r peut se noter de r façons:*

$$(i_1 \ i_2 \ \ \dots \ i_r) = (i_2 \ i_3 \ \dots \ i_r \ i_1) = \cdots = (i_r \ i_1 \ \dots \ i_{r-1}).$$

EXERCICE 1 Soit $\sigma \in S_n$, un cycle de longueur r. Montrer que $ordre(\sigma) = r$.

Théorème 2.5 *Toute permutation de S_n est un cycle ou un produit de cycles à supports deux à deux disjoints.*

Le théorème précédent se démontre de plusieurs façons. Pour montrer l'existence de la décomposition, une manière utile et élégante est de donner un algorithme qui fournit une décomposition. Ci-dessous, une fonction en python qui réalise cela. L'entrée de la fonction `decompose()` est ici une liste `l` qui représente une permutation σ de l'ensemble $\{0, \ldots, n-1\}$, donnée par $\sigma(0) = l[0], \sigma(1) = l[1] \ldots, \sigma(n-1) = l[n-1]$. La liste `l` représente la deuxième ligne, dans la notation d'une permutation en un tableau de deux lignes et la permutation d'entrée est donc:

$$\sigma = \begin{pmatrix} 0 & 1 & \ldots & n-1 \\ l[0] & l[1] & \ldots & l[n-1] \end{pmatrix}.$$

```
def decompose(l):
        n=len(l)
        i=0
        visite=[False]*n
        res=[]
        while True:
                c=[i]
                visite[i]=True
                j=i
                while l[j]!=i:  # On complete c par les iteres de i
                        c+=[l[j]]
                        j=l[j]
                        visite[j]=True
                if len(c)>1 :
                        res+=[c]
                k=(j+1) %n
                while visite[k] and k!=j: # on recherche le prochain
                        k= (k+1)% n       # element non encore visite
                if k==j:
                        return res
                i=k
```

La boucle principale de la fonction précédente (celle qui commence par `while True`) s'exécute au plus n fois car à chaque exécution au moins un élément supplémentaire de la liste l sera visitée. Plus précisément, les sommes des itérations de la boucle principale et de la boucle secondaire commençant par `while l[j]!=i` est exactement n. L'algorithme précédent finit et retourne une décomposition souhaitée.

Il faut impérativement savoir exécuter cet algorithme à la main et calculer une décomposition d'une permutation en produit de cycles à supports deux à deux disjoints.

On peut aussi prouver le théorème par récurrence sur le cardinal k du support de la permutation σ:

Si $k = 0$, σ est l'identité qui est un cycle de longueur 1.

Si $k > 0$, soit i_1 un élément du support de σ. On définit $i_2, \dots i_r$, par $i_2 = \sigma(i_1)$, $i_3 = \sigma(i_2), \dots, i_{r+1} = \sigma(i_r)$, où r est le plus petit entier tel que $i_{r+1} \in \{i_1, i_2, \dots, i_r\}$ (un tel r existe, car la séquence $i_1, i_2, i3, \dots, i_k, \dots$ prend ses valeurs dans l'ensemble $\{1, \dots, n\}$ et donc a nécessairement des répétitions et $r \leq n$). On a alors nécessairement $\sigma(i_r) = i_1$. Sinon $\sigma(i_r) = i_j$ pour un certain $j \geq 2$. Or on a déjà $\sigma(i_{j-1}) = i_j$, et cela contredirait l'injectivité de σ. Soit α le cycle de longueur r $(i_1\ i_2\ i_3\ \dots\ i_r)$.

Si $r = n$, alors $\sigma = \alpha$.

Si $r < n$, en appelant $Y = \{1, \dots, n\} \backslash \{i_1, i_2, \dots, i_r\}$, l'ensemble des points fixes de α, on a par construction, $\sigma(Y) = Y$. Soit σ' la permutation définie par $\sigma'(i) = \sigma(i)$ pour tout $i \in Y$ et $\sigma'(i) = i$, pour tout $i \notin Y$. Toujours par construction, $\sigma = \alpha \circ \sigma'$ et par hypothèse de récurrence, on a $\sigma' = \beta_1 \circ \dots \circ \beta_t$, où les β_i sont des cycles à supports deux à deux disjoints. Comme α et σ' ont des supports disjoints, $\sigma = \alpha \circ \beta_1 \circ \dots \circ \beta_t$ est bien un produit de cycles à supports deux à deux disjoints[2].

Définition 2.6 *On appelle décomposition complète d'une permutation σ en cycles à supports disjoints, une décomposition qui contient exactement un cycle de longueur 1, pour chaque point fixe de σ. Deux décompositions en cycles disjoints sont de même type si et seulement si elles contiennent le même nombre de cycles de longueur r, pour tout $r > 0$.*

Proposition 2.7 *Deux permutations αet β de S_n à supports disjoints commutent, i.e. $\alpha\beta = \beta\alpha$.*

Preuve. Nous allons prouver que pour $i \in \{1, \dots, n\}, \alpha\beta(i) = \beta\alpha(i)$.

Si $i \notin \text{supp}(\alpha)$, alors $i \in \text{supp}(\beta)$, donc $\beta(i) = j \neq i$. On a alors aussi $j \in \text{supp}(\beta)$ (sinon $\beta(i) = i$ serait en contradiction avec $\beta(i) = j \neq i$ et l'injectivité de β.). Comme α et β sont à supports disjoints, $\alpha(i) = i$ et $\alpha(j) = j$. Donc $\alpha(\beta(i)) = \alpha(j) = j$ et $\beta(\alpha(i)) = \beta(i) = j$.

De même, si Si $i \in \text{supp}(\alpha)$, $\alpha(i) = j \neq i$ et on a aussi $j \in \text{supp}(\alpha)$, puis $\beta(i) = i$ et $\beta(j) = j$. Donc, $\alpha(\beta(i)) = \alpha(i) = j$ et $\beta(\alpha(i)) = \beta(j) = j$.

□

Théorème 2.8 *La décomposition complète d'une permutation σ en produit de cycles à supports disjoints d'une permutation est unique à l'ordre près.*

Preuve. L'unicité sera admise. Voici une idée d'une preuve (par récurrence). Comme la décomposition complète a exactement un cycle de longueur 1 par point fixe, il suffit de

[2]On peut supprimer les cycles de longueur 1 (ils correspondent à l'identité) ou garder exactement un cycle de longueur 1 pour tout point fixe de σ.

montrer le théorème sans les cycles de longueur 1 (on rappelle qu'un cycle de longueur 1 est l'identité). Supposons que σ a deux décompositions $\alpha_1 \dots \alpha_s$ et $\beta_1 \dots \beta_t$. Le théorème peut se montrer par récurrence sur le $\max(s,t)$. Soit i_1 un élément du support de σ. Il apparait dans exactement un des cycles α_i et exactement un des cycles β_j. En changeant l'ordre des cycles à supports disjoints, on peut toujours poser que $i_1 \in \text{supp}(\alpha_s)$ et $i_1 \in \text{supp}(\beta_t)$. Comme pour tout $r \geq 1$, on a $\sigma^r(i_1) = \alpha_s^r(i_1) = \beta_t^r(i_1)$, on en déduit que $\alpha_s = \beta_t$. On applique ensuite l'hypothèse de récurrence aux deux décompositions $\alpha_1 \dots \alpha_{s-1}$ et $\beta_1 \dots \beta_{t-1}$ de la permutation $\sigma\alpha_s^{-1}$. □

2.1 Quelques applications de la décomposition produit de cycles à supports disjoints

Proposition 2.9 *L'élément symétrique (appelé inverse en notation multiplicatif) d'un cycle de longueur r, $\alpha = (i_1\ i_2\ i_3\ \dots\ i_{r-1}\ i_r)$ est le cycle de longueur r, $(i_r\ i_{r-1}\ i_{r-2}\ \dots\ i_2\ i_1)$. En particulier, une transposition est sa propre inverse. Si $\sigma \in S_n$ est un produit de cycles $\sigma = \beta_1\beta_2 \dots \beta_k$. Alors, $\sigma^{-1} = \beta_k^{-1}\beta_{k-1}^{-1} \dots \beta_1^{-1}$.*

Preuve. La vérification (très aisée) de la première et deuxième assertions est laissée au lecteur. La dernière assertion est un résultat déjà connu pour le calcul de l'inverse d'un produit dans tout groupe, appliqué ici au cas d'un produit de cycles dans le groupe S_n. □

Proposition 2.10 *Soient $\alpha, \gamma \in S_n$. La permutation $\alpha\gamma\alpha^{-1}$ a le même type de décomposition complète en cycles à supports disjoints que γ. Plus précisément la décomposition complète de $\alpha\gamma\alpha^{-1}$ s'obtient à partir de celle de γ en y remplaçant chaque valeur i, par $\alpha(i)$.*

Preuve. Appelons σ la permutation de S_n obtenue en remplaçant chaque valeur i, par $\alpha(i)$, dans la décomposition complète de γ. Nous allons montrer que pour tout $j \in \{1, \dots, n\}$, on a $\alpha\gamma\alpha^{-1}(j) = \sigma(j)$.

Considérons d'abord le cas où $\alpha^{-1}(j) \notin \text{supp}(\gamma)$. On alors $\alpha\gamma\alpha^{-1}(j) = \alpha\alpha^{-1}(j) = j$. Comme point fixe de γ, $\alpha^{-1}(j)$ est dans un cycle de longueur 1 dans la décomposition complète de γ. D'après la définition de σ, $\alpha(\alpha^{-1}(j)) = j$ est dans un cycle de longueur 1 dans la décomposition complète de σ, i.e. j est bien un point fixe de σ.

Considérons maintenant le cas où $i_1 = \alpha^{-1}(j) \in \text{supp}(\gamma)$. i_1 est donc dans un cycle de longueur au moins 2 dans la décomposition complète de γ et $\gamma(i_1) = i_2 \neq i_1$. Mais d'après la définition de σ, $\alpha(i_1)$ et $\alpha(i_2)$ se succèdent dans un même cycle, dans la décomposition complète de σ.

On alors $\alpha\gamma\alpha^{-1}(j) = \alpha\gamma(i_1) = \alpha(i_2)$. Mais on a aussi $\sigma(j) = \sigma(\alpha(i_1)) = \alpha(i_2)$.

Or α étant une permutation, elles est donc surjective. $\alpha^{-1}(j)$ existe donc bien toujours et tout élément $j \in \{1, \dots, n\}$ est bien dans un des deux cas envisagés par la preuve. □

Voici deux exemples:

Si $\gamma = (1\ 3)(2\ 4\ 7)(5)(6)$ et $\alpha = (2\ 5\ 6)(1\ 4\ 3)$, alors

$$\alpha\gamma\alpha^{-1} = (\alpha(1)\ \alpha(3))\ (\alpha(2)\alpha(4)\alpha(7))\ (\alpha(5))\ (\alpha(6)) = (4\ 1)\ (5\ 3\ 7)\ (6)\ (2).$$

Soient $\beta, \gamma, \alpha \in S_5$, définies par:

$$\begin{array}{rcl} \beta & = & (1\ 2\ 3)\ (4)\ (5) \\ \gamma & = & (5\ 2\ 4)\ (1)\ (3) \end{array} . \tag{1}$$

et

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

On a alors $\gamma = \alpha\beta\alpha^{-1}$.

Définition 2.11 *Soit $(G, .)$ un groupe. Deux éléments $x, y \in G$ sont dits conjugués si et seulement si il existe $z \in G$ tel que $y = zxz^{-1}$.*

On vérifie aisément que la relation de conjugaison définie sur les éléments d'un groupe est une relation d'équivalence. Dans un groupe donné, le problème de décider si deux éléments du groupe sont conjugués peut être un problème algorithmiquement difficile. Lorsque c'est le cas, ce problème peut être à la base de protocoles cryptographiques de chiffrement ou d'échange de clé. La proposition suivante montre que le problème de conjugaison, dans les groupes de permutations, est un problème algorithmiquement facile.

Proposition 2.12 *Deux permutations γ et β de S_n sont conjuguées si et seulement si elles ont le même type de décomposition complète en cycles à supports disjoints.*

Preuve. D'après la proposition précédente, si γ et β sont conjuguées, alors elles ont le même type de décomposition en cycles à supports disjoints. Réciproquement, si deux permutations γ et β ont le même type de décomposition, on determine $\alpha \in S_n$, telle que $\beta = \alpha\gamma\alpha^{-1}$, en identifient la décomposition de β avec celle de γ où chaque i est remplacé par $\alpha(i)$. □

On peut remarquer que lorsque deux permutations γ et σ de S_n sont conjuguées, alors le choix de α telle que $\sigma = \alpha\gamma\alpha^{-1}$ n'est pas unique: dans l'exemple précédent (1), on peut également par choisir α différemment, en "alignant" les décompositions de β et γ d'une autre manière que celle suggérée, par l a relation (1):

$$\begin{array}{rcl} \beta & = & (1\ 2\ 3)\ (4)\ (5) \\ \gamma & = & (2\ 4\ 5)\ (3)\ (1) \end{array} .$$

et choisir α:

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

On a alors encore bien $\gamma = \alpha\beta\alpha^{-1}$, d'après la proposition 2.10.

3 La décomposition d'une permutation en produit de transpositions

Théorème 3.1 *Pour $n > 1$, toute permutation se décompose en produit de transpositions. Il n'y a pas d'unicité d'une telle décomposition.*

Preuve. Comme toute permutation se décompose en produit de cycles, il suffit de montrer la propriété pour les cycles. On vérifie aisément que

$$(i_1\ i_2\ \ldots\ i_r) = (i_1\ i_r)\ (i_1\ i_{r-1})\ \ldots\ (i_1\ i_3)\ (i_1\ i_2).$$

On vérifie de même que:

$$(i_1\ i_2\ \ldots\ i_r) = (i_1\ i_2)\ (i_2\ i_3)\ \ldots\ (i_{r-2}\ i_{r-1})\ (i_{r-1}\ i_r).$$

□

Comme déjà indiqué, il n'y a ni unicité des transpositions qui forment le produit, ni même unicité du nombre de facteurs. Par exemple, dans S_4 on a:

$$\begin{array}{rcl} (1\ 2\ 3) & = & (1\ 3)\ (1\ 2) \\ & = & (2\ 3)\ (1\ 3) \\ & = & (1\ 3)\ (4\ 2)\ (1\ 2)\ (1\ 4) \\ & = & (1\ 3)\ (4\ 2)\ (1\ 2)\ (1\ 4)\ (1\ 3)\ (1\ 3) \end{array} .$$

Nous allons voir dans la suite que la parité du nombre de transpositions dans toute les décompositions d'une même permutation en produit de transpositions reste constante.

4 Signature d'une permutation

Définition 4.1 *Soit $\sigma \in S_n$. On appelle signature de σ et on note $\varepsilon(\sigma)$, l'entier $(-1)^{n-m}$, où m est le nombre de cycles dans la décomposition* **complète** *de σ en produit de cycles disjoints.*

L'identité a pour signature 1 ($n = m$). Une transposition a pour signature -1 ($m = n-1$). Un cycle de longueur r a pour signature $r-1$ ($m = n-r+1$).

Théorème 4.2 *Soient σ une permutation et τ une transposition. Alors $\varepsilon(\tau\sigma) = -\varepsilon(\sigma)$.*

Preuve. Posons $\tau = (a\ b)$ et $\sigma' = (a\ b)\sigma$. Les décompositions complètes en cycles à supports disjoints de σ et de σ' ne diffèrent que sur les cycles contenant a et/ou b. (Pour les autres cycles, tout se passe comme si ils étaient composés avec l'identité). Deux cas peuvent alors se produire:

Premier cas : a et b apparaissent dans un même cycle dans la décomposition complète de σ. Il existe alors $k, l \geq 0$ et des entiers c_i et d_j tels que:

$$(a\ b)\ (a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_l) = (a\ c_1\ \ldots\ c_k)\ (b\ d_1\ \ldots\ d_l).$$

Deuxième cas: a et b apparaissent dans deux cycles distincts dans la décomposition complète de σ. En multipliant (composant) la relation précédente à gauche par la transposition $(a\ b)$, on obtient:

$$(a\ b)\ (a\ c_1\ \ldots\ c_k)\ (b\ d_1\ \ldots\ d_l) = (a\ c_1\ \ldots\ c_k\ b\ d_1\ \ldots\ d_l).$$

Dans les deux cas, les nombres de cycles dans les décompositions complètes de σ' et de σ diffèrent donc de 1. □

Corollaire 4.3 *Si $\sigma \in S_n$ est produit de r transpositions, alors $\varepsilon(\sigma) = (-1)^r$.*

Preuve. récurrence immédiate sur r. □

Corollaire 4.4 *La parité du nombre de transpositions dans toute décomposition d'une permutation en produit de transpositions est invariante.*

Corollaire 4.5 *L'application $\varepsilon : S_n \to \{-1, 1\}$, qui à une permutation, associe sa signature est un morphisme du groupe $(Sn, \circ)$ dans le groupe $(\{-1, 1\}, \times)$.*

Preuve. Soient deux permutations $\alpha, \beta \in S_n$. Elles se décomposent respectivement en produits de a et b transpositions. La permutation $\alpha\beta$ se décompose alors en un produit de $a + b$ transpositions. Ainsi $\varepsilon(\alpha\beta) = (-1)^{a+b} = (-1)^a(-1)^b = \varepsilon(\alpha)\varepsilon(\beta)$. □

Définition 4.6 *Le noyau du morphisme ε est un sous-groupe de S_n, composé des permutation de signature 1, appelé le groupe alterné et noté A_n. Les éléments de A_n. sont également appelées permutations paires. Les autre permutations (de signature -1) sont appelées permutations impaires.*

EXERCICE 2 Quel est l'indice (noté $[S_n : A_n]$) de A_n dans S_n? Quel est l'ordre de A_n?