Les groupes symétriques

AJARCIF ELHASSANE

23 juin 2016

Remerciements

Je tiens à remercier le professeur Najib Mahdou, qui a proposé ce sujet, et qui a bien voulu encadrer ce travail. Je lui exprime aussi ma gratitude pour son dévouement et le temps qu'il m'a consacré.

Je remercie les membres du jury pour avoir daigné assister à ma soutenance.

Je n'oublie pas de remercier ma famille et surtout mes parents, qui m'ont toujours soutenus durant mes études.

Table des matières

Chapitre 1

Structure du groupe symétrique

soit E un ensemble ayant au moins deux éléments et Id_E est l'application identité sur E. On note $card(E)$ le cardinal de E.

1.1 Les permutations

Définition :
Soit E un ensemble. Une permutation de E est une bijection de E dans E.
On note $S(E)$ l'ensemble des permutations de E. Si $E = \{1, ..., n\}$ on le note simplement S_n. Une permutation est souvent notée σ.

Représentation d'une permutation :
Si $\sigma \in S_n$, on peut représenter σ soit :
$i)$ sous la forme d'application

$$\begin{aligned} \sigma : & E \longrightarrow E \\ & k \longrightarrow \sigma(k) \end{aligned}$$

$ii)$ par une matrice :

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

où la première ligne représente l'ensemble de départ, et la seconde ligne l'ensemble d'arrivée, les éléments de la seconde ligne étant les images des éléments de la première ligne par σ.
L'élément neutre I_d est représenté par

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

et l'inverse σ^{-1} de σ par

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

Pour toute permutation $\sigma \in S(E)$ et tout entier relatif r, σ^r est la permutation de E définie par :

$$\sigma^r = \begin{cases} Id_E \, si \, r = 0 \\ \sigma \circ ... \circ \sigma (r fois) \, si \, r \geq 1 \\ (\sigma^{-r})^{-1} \, si \, r \leq -1 \end{cases}$$

Opérations entre permutations :

- Pour alléger les écritures, on notera, pour tout couple (σ, ψ) d'éléments de S_n, $\sigma\psi$ à la place de $\sigma \circ \psi$. On parlera de produit de deux permutations plutôt que de composition de deux permutations.
- Puisque la loi est la composition, les cycles sont lus de droite à gauche

Exemple :

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

et :

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix}$$

1.2 Propriétés du groupe symétrique

On démontre le théorème suivant :

Théorème :

$(S_n, \circ)$ est appelé le groupe symétrique ou groupe des permutations.

Démonstration :

Soient $f, g \in S_n$. Alors la composée $g \circ f$ est une application de E dans lui-même, et est une bijection en tant que composée de deux applications bijectives.

Donc $g \circ f$ est une permutation de E.

Par conséquent, la loi

$$\begin{aligned} S_n \times S_n &\longrightarrow S_n \\ (f, g) &\longrightarrow f \circ g \end{aligned}$$

est une loi de composition interne dans S_n.
- la composition est clairement associative.
- L'identité est l'élément neutre pour la composition.
- Enfin, tout élément σ de S_n étant une bijection possède un symétrique σ^{-1} qui est sa fonction réciproque tel que :

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

donc S_n est bien un groupe appelé groupe symétrique.

Remarque :

- Dans le cas où E est réduit à un élément, on peut quand même définir $S(E)$ et il est réduit à Id_E.
- À isomorphisme près, $S(E)$ ne dépend que de $Card(E)$.

Théorème :

Si E, F sont deux ensembles non vides et φ une bijection de E sur F, alors les groupes $S(E)$ et $S(F)$ sont isomorphes.

Démonstration :

L'application :

$$\psi : S(E) \longrightarrow S(F)$$
$$\sigma \longrightarrow \phi \circ \sigma \circ \phi^{-1}$$

est un isomorphisme de groupes.

En effet, pour $\sigma \in S(E)$, $\psi(\sigma) \in S(F)$ comme composée de bijections et pour σ_1, σ_2 dans $S(E)$, on a :

$$\psi(\sigma_1 \circ \sigma_2) = \phi \circ \sigma_1 \circ \sigma_2 \circ \phi^{-1} = (\phi \circ \sigma_1 \circ \phi^{-1}) \circ (\phi \circ \sigma_2 \circ \phi^{-1}) = \psi(\sigma_1) \circ \psi(\sigma_2)$$

c'est-à-dire que ψ est un morphisme de groupes de $S(E)$ dans $S(F)$. Si $\sigma \in ker(\psi)$, on a alors $\phi \circ \sigma \circ \phi^{-1} = Id_F$ et $\sigma = \phi^{-1} \circ Id_F \circ \phi = Id_E$, donc ψ est injective. Pour $\sigma' \in S(F)$, l'application $\sigma = \phi^{-1} \circ \sigma' \circ \phi$ est dans $S(E)$ et on a $\psi(\sigma) = \sigma'$,donc ψ est surjective.

Donc tout groupe de permutations d'un ensemble E à n éléments est isomorphe au groupe symétrique S_n des permutations de $\{1, 2, ..., n\}$. On rappelle que deux ensembles finis qui sont en bijection ont le même nombre d'éléments.

Propriété :

Soit $n \in \mathbb{N}^*$, Alors $(S_n, \circ)$ est un groupe fini d'ordre $n!$.

Démonstration :

Par récurrence sur $n \geq 1$.

Pour $n = 1$ c'est clair puisque $S(E) = Id_E$.

Supposons le résultat acquis pour les ensembles à $n - 1 \geq 1$ éléments et soit $E = \{x_1, ..., x_n\}$ un ensemble à $n \geq 2$ éléments.

On désigne par H le sous-ensemble de $S(E)$ formé des permutations de E qui laissent stable x_n.

On vérifie facilement H est un sous-groupe de $S(E)$. En effet, on a $Id \in H$ et pour σ_1, σ_2 dans H, $\sigma_1\sigma_2^{-1}(x_n) = \sigma_1(x_n) = x_n$, donc $\sigma_1\sigma_2^{-1} \in H$ et H est un sous-groupe de $S(E)$.

L'application qui associe à $\sigma \in H$ sa restriction à $F = \{x_1, ..., x_{n-1}\}$ réalise alors un isomorphisme de H sur $S(F)$.

En désignant, pour tout entier k compris entre 1 et $n-1$, par τ_k la permutation $\tau_k = (x_k, x_n)$, on a $S(E)/H = \{\tau_1 H, ..., \tau_{n-1}H, H\}$.

En effet, pour tout $\sigma \in S(E)$, il existe $k \in \{1, ..., n\}$ tel que $\sigma(x_n) = x_k$ et en notant $\tau_n = Id$, on a $\tau^{-1}\sigma(x_n) = \tau^{-1}(x_k) = x_n$, donc $\tau_k^{-1}\sigma \in H$ et $\sigma H = \tau_k H$. On a donc $S(E)/H = \{\tau_1 H, ..., \tau_n H\}$ avec $\tau_j H \neq \tau_k H$ pour $k \neq j$

(pour $1 \leq k < j \leq n$, on a $\tau_k^{-1}\tau_j(x_n) = \tau_k(x_j) \neq x_n$, donc $\tau_k^{-1}\tau_j \notin H$).
En utilisant l'hypothèse de récurrence, on en déduit que :

$$\begin{aligned} card(S(E)) &= card(S(E)/H)card(H) \\ &= card(S(E)/H)card(S(F)) \\ &= n.(n-1)! \\ &= n!. \end{aligned}$$

propriété :
1) S_1 et S_2 sont abéliens.
2) Pour $n \geq 3$, S_n n'est pas abélien.

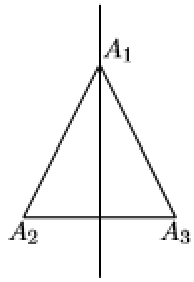
Démonstration :
1)$S_1 = Id$ donc S_1 est abélien. S_2 est composé de l'identité et de la permutation échangeant 1 et 2 donc S_2 est abélien.
2)Soient i, j et k trois éléments distincts de $\{1, ..., n\}$.
Soit σ une application bijective qui à i associe j, à j associe i et qui fixe k.
Soit ψ une application bijective qui à i associe k, à k associe i et qui fixe j.
Alors, $(\sigma \circ \psi)(i) = k$ et $(\psi \circ \sigma)(i) = j$ et donc $\sigma \circ \psi \neq \psi \circ \sigma$ et par conséquent S_n n'est pas abélien.

Exercice :
Montrer que si l'ensemble E a au moins 3 éléments, alors le groupe $S(E)$ n'est pas commutatif

Solution :
Soient x_1, x_2, x_3 distincts dans E et $\tau_1 = (x_1, x_2), \tau_2 = (x_2, x_3)$. On a $\tau_2 \circ \tau_1(x_1) = x_3$ et $\tau_1 \circ \tau_2(x_1) = x_2 \neq x_3$.
Donc $\tau_2 \circ \tau_1 \neq \tau_1 \circ \tau_2$ et S (E) n'est pas commutatif.

Exercice :
Montrer que le groupe des isométries du plan affine euclidien qui conservent les sommets d'un vrai triangle isocèle non équilatéral est isomorphe à S_2.

Solution :
On note P le plan affine euclidien et on se donne un vrai triangle isocèle non équilatéral T de sommets A_1,A_2,A_3 avec $A_1A_2 = A_1A_3$ (voir le figure).



On note $Is(T)$ le groupe des isométries de P qui conservent $E = \{A_1, A_2, A_3\}$.
Soit $\varphi \in Is(T)$. Par conservation des barycentres, on a $\varphi(O) = O$, en désignant par O le centre de gravité du triangle (l'isobarycentre de E) et $\varphi([A_2A_3])$ est un coté du triangle de même longueur que $[A_2A_3]$, c'est donc $[A_2A_3]$ puisque le triangle est non équilatéral et isocèle en A_1.

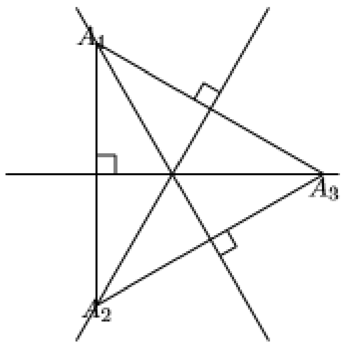
On a donc $\varphi(\{A_2A_3\}) = \{A_2, A_3\}$ et nécessairement $\varphi(A_1) = A_1$. Si $\varphi(A_2) = A_2$, alors $\varphi = Id$ puisque ces deux applications coïncident sur le repère affine (O, A_1, A_2). Si $\varphi(A_2) = A_3$, alors φ est la réflexion σ d'axe (OA_1), la médiatrice de $[A_2A_3]$, puisque ces deux applications coïncident sur le repère affine (O, A_1, A_2). On a donc $Is(T) = \{Id, \sigma\} = S(\{A2, A3\})$ qui est isomorphe à S_2.

Exercice :

Montrer que le groupe des isométries du plan affine euclidien qui conservent les sommets d'un vrai triangle équilatéral est isomorphe à S_3.

Solution :

On note P le plan affine euclidien, on se donne un vrai triangle équilatéral T de sommets A_1, A_2, A_3, et $Is(T)$ est le groupe des isométries de P qui conservent



les sommets de ce triangle (figure).

En désignant par O l'isobarycentre de $E = \{A_1, A_2, A_3\}$, on a $A_k = \rho(A_{k-1})$ pour $k = 2, 3$ où ρ est la rotation de centre 0 et de mesure d'angle égale à $\frac{2\pi}{3}$. Donc $Is(T)$ contient $\langle\rho\rangle$ qui est d'ordre 3.

L'application Ψ qui associe à $\varphi \in Is(T)$ associe la permutation

$$\sigma = \begin{pmatrix} A_1 & A_2 & A_3 \\ \varphi(A_1) & \varphi(A_2) & \varphi(A_3) \end{pmatrix}$$

réalise un morphisme de groupes de $Is(T)$ dans $S(E)$.

En effet, pour φ, ψ dans $Is(T)$ et $k = 1, 2, 3$, on a :

$$\Phi(\varphi \circ \psi)(A_k) = (\varphi \circ \psi)(A_k) = \varphi(\psi(A_k)) = \Phi(\varphi) \circ \Phi(\psi)(A_k)$$

et comme (A_1, A_2, A_3) est un repère affine de E, ce morphisme est injectif (deux applications affines qui coïncident sur un repère affine sont identiques). Il en résulte que $Is(T)$ est isomorphe à un sous-groupe de S_3 et il est d'ordre 3 ou 6. La réflexion σ d'axe la médiatrice de l'un des cotés étant aussi dans $Is(T)$, on a au moins 4 éléments dans $Is(T)$ et ce groupe est nécessairement d'ordre 6. Il est donc isomorphe à S_3.

On a en fait, $Is(T) = \langle \rho, \sigma \rangle$.

On peut aussi dire que le groupe $Is(T)$ contient les trois réflexions par rapport aux médiatrices et comme ces réflexions ont pour image par Φ les trois transpositions $(A_1, A_2), (A_1, A_3) et (A_2, A_3)$ qui engendrent $S(E)$ (voir plus loin), on en déduit que $s(T)$ est isomorphe à $S(E)$, donc à S_3.

1.3 Cycles et transpositions

Définition :

Soit σ un élément de S_n.

On appelle support de σ et on note $Supp(\sigma)$, l'ensemble :

$$Supp(\sigma) = \{1 \leq i \leq n / \sigma(i) \neq i\}.$$

Exemple :

1- Le support de l'identité est l'ensemble vide.

2- Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 4 & 2 & 5 \end{pmatrix}$

alors on a :

$$supp(\sigma) = \{2, 3, 5, 6\}.$$

Propriété :

Si deux éléments de S_n ont leurs supports disjoints alors ils commutent.

Démonstration :

Soient σ et ψ deux éléments de S_n. Soit i compris entre 1 et n. Si i appartient au support de σ alors $\sigma(i)$ appartient au support de σ car si $\sigma(\sigma(i)) = \sigma(i)$ alors $\sigma(i) = i$.

D'où, puisque les supports de σ et ψ sont disjoints, $\sigma(i)$ n'appartient pas au support de ψ et par conséquent $\sigma\psi(i) = \sigma(i) = \psi\sigma(i)$. On a de même $\sigma\psi(i) = \psi(i) = \psi\sigma(i)$ si i appartient au support de ψ.

Si i n'appartient ni au support de σ ni au support de ψ alors $\sigma\psi(i) = i = \psi\sigma(i)$.

Remarque :

La réciproque est fausse. Par exemple, les permutations $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ commutent et elles ont le même support : l'ensemble $\{1, 2, 3\}$.

Théorème :

Soient σ, $\sigma^{'}$ dans $S(E)$. alors :
1. $\sigma(Supp(\sigma)) = Supp(\sigma)$.
2. $Supp(\sigma) = Supp(\sigma^{-1})$.
3. Pour tout $r \in \mathbb{Z}$, on a $Supp(\sigma^r) \subset Supp(\sigma)$.
4. Si $Supp(\sigma) \cap Supp(\sigma^{'}) = 0$, alors $\sigma \circ \sigma^{'} = \sigma^{'} \circ \sigma$.

Démonstration :

1. Soit $x \in Supp(\sigma)$. Comme σ est injective, de $\sigma(x) \neq x$ on déduit que $\sigma(\sigma(x)) \neq \sigma(x)$ et $\sigma(x) \in Supp(\sigma)$. On a donc $\sigma(Supp(\sigma)) \subset Supp(\sigma)$ (dans le cas où E est fini, on a l'égalité puisque ces ensembles ont le même nombre d'éléments). Comme σ est surjective, tout $x \in Supp(\sigma)$ s'écrit $x = \sigma(x')$ et $\sigma(x) = \sigma(\sigma(x')) \neq x = \sigma(x')$ impose $\sigma(x') \neq x'$, donc $x' \in Supp(\sigma)$ et $x \in \sigma(Supp(\sigma))$. On a donc $Supp(\sigma) \subset \sigma(Supp(\sigma))$ et $\sigma(Supp(\sigma)) = Supp(\sigma)$.

2. De $\sigma(x) = x$ équivalent à $x = \sigma^{-1}(x)$, on déduit que $x \in Supp(\sigma)$ si, et seulement si, $x \in Supp(\sigma^{-1})$ et donc $Supp(\sigma) = Supp(\sigma^{-1})$.

3. L'égalité $\sigma(x) = x$ entraîne $\sigma^r(x) = x$ pour tout $r \in \mathbb{Z}$, donc $\sigma^r(x) \neq x$ entraîne $\sigma(x) \neq x$ et $Supp(\sigma^r) \subset Supp(\sigma)$.

4. Soient σ, σ' telles que $Supp(\sigma) \cap Supp(\sigma') = \emptyset$ et $x \in E$.
Si $\sigma(x) = x = \sigma'(x)$, on a alors $\sigma' \circ \sigma(x) = \sigma'(x) = x = \sigma(x) = \sigma \circ \sigma'(x)$.
Si $x \in Supp(\sigma)$, alors $x \notin Supp(\sigma')$ et $\sigma(x') = x$, donc $\sigma \circ \sigma'(x) = \sigma(x)$. Mais on a aussi $\sigma(x) \in Supp(\sigma)$, donc $\sigma(x) \notin Supp(\sigma')$ et $\sigma' \circ \sigma(x) = \sigma(x) = \sigma \circ \sigma'(x)$.
De manière analogue, on vérifie que $\sigma' \circ \sigma(x) = \sigma(x) = \sigma \circ \sigma'(x)$ pour tout $x \in Supp(\sigma')$(on permute les rôles de σ et σ'). On a donc $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Remarque :

La réciproque du point 4. du théorème précédent est fausse. Pour le voir, on prend $\sigma \neq Id_E$ et $\sigma' = \sigma^{-1}$.

Définition :

Soit $\sigma \in S_n$.
On appelle $\sigma - orbite$ de i $\in \{1, ..., n\}$ ou bien orbite de i suivant σ l'ensemble

$$\Omega_\sigma(i) = \{\sigma^k(i) | k \in \mathbb{N}\}.$$

Exemple :

Soit $\sigma \in S_7$ définie par :

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

alors on a :

$$\Omega_\sigma\{1\} = \{1, 2, 4, 7\}, \Omega_\sigma\{3\} = \{3, 5\}, \Omega_\sigma\{6\} = \{6\}.$$

Remarque (Action de groupe) :

1- On a une action naturelle du groupe cyclique $H = \langle \sigma \rangle$ sur E définie par :

$$(\sigma^k, x) \longrightarrow \sigma^k.x = \sigma^k(x)$$

Les orbites (ou $\sigma - orbites$) pour cette action , sont les parties de E :

$$H.x = \{\gamma.x | \gamma \in H\} = \{\sigma^k(x) | k \in \mathbb{Z}\}$$

où x décrit E.
On notera $\Omega_\sigma(x)$ une telle orbite.

2- Une $\sigma - orbite$ $\Omega_\sigma(x)$ est réduite à un point si, et seulement si, $\sigma(x) = x$ et on dit que c'est une orbite ponctuelle. Les orbites non réduites à un point forment une partition du support de σ.

3-Dans la pratique, $\Omega_\sigma(i)$ est l'ensemble des j de $\{1, ..., n\}$ qu'on rencontre en partant de i et en faisant agir σ jusqu'à retrouver i.

Par exemple, dans S_6, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 4 & 2 & 3 \end{pmatrix}$, on a les $\sigma - orbites$ sont : $\Omega(1) = \Omega(3) = \Omega(6) = \{1, 3, 6\}$, $\Omega(2) = \Omega(5) = \{2, 5\}$, $\Omega(4) = \{4\}$.

Elles sont simplement déterminées en regardant l'image d'un élément (par exemple 1), et en itérant la permutation (on obtient ainsi 3, puis 6, etc) jusqu'à retomber sur l'élément de départ (ici, 1).

Définition :

Soit r un entier compris entre 2 et $card(E)$.

On appelle cycle d'ordre r (ou r-cycle), toute permutation $\sigma \in S(E)$ qui permute circulairement r éléments de E et laisse fixe les autres, c'est-à-dire qu'il existe une partie $\{x_1, ..., x_r\}$ de E telle que :

$$\begin{cases} \forall k \in \{1, ..., r-1\}, \sigma(x_k) = x_{k+1}, \\ \sigma(x_r) = x_1, \\ \forall x \in E \backslash \{x_1, ..., x_r\}, \sigma(x) = x, \end{cases}$$

On notera :

$$\sigma = (x_1, ..., x_r)$$

un tel cycle et on dit que $\{x_1, ..., x_r\}$ est le support de σ et on le note $Supp(\sigma)$.

Notation :

Pour noter le $r - cycle$ défini par $x_1, x_2, ..., x_r$ on utilise la notation suivante : $(x_1 x_2 ... x_r)$ qui se lit : x_1 donne x_2, ... ,x_{r-1} donne x_r et x_r donne x_1. Il est d'usage de ne pas noter les éléments fixés par un cycle.

Exemples :

(a)- Dans S_6, la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 2 & 4 & 2 & 6 \end{pmatrix}$ est un $3 - cycle$. On le note (2, 5, 3) (ou (5, 3, 2) ou (3, 2, 5)).

(b)- Dans S_6, la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ n'est pas un cycle.

(c)- Dans S_8 le $5-cycle$ $(1, 8, 5, 3, 7)$ correspond à la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 2 & 7 & 4 & 3 & 6 & 1 & 5 \end{pmatrix}$
(d)- Dans S_6, les cycles (1, 3) et (2, 4, 5) sont disjoints.
(e)- Dans S_7, les cycles (2, 6, 8, 5) et (4, 5) ne sont pas disjoints.

Remarque :
1- Le support d'un cycle $\sigma = (x_1, x_2, ..., x_r)$ est $\{x_1, x_2, ..., x_r\}$.
2- Les r permutations circulaires :

$$(x_1, x_2, ..., x_r), (x_2, x_3, ..., x_r, x_1), , (x_r, x_1, ..., x_{r-1})$$

définissent le même $r-cycle$ car ils se déduisent l'un de l'autre par permutation circulaire.
3- L'inverse d'un r-cycle est un r-cycle de même support. Précisément, on a :

$$(x_1, x_2, ..., x_r)^{-1} = (x_r, x_{r-1}, ..., x_1)$$

En effet, en notant $x_0 = x_r$, on a :

$$\begin{cases} \sigma(x_{k-1}) = x_k (1 \le k \le r) \\ \sigma(x) = x \, si \, x \in E \backslash \{x_1, ..., x_r\} \end{cases} \Leftrightarrow \begin{cases} \sigma^{-1}(x_k) = x_{k-1} (1 \le k \le r), \\ \sigma^{-1}(x) = x \, si \, x \in E \backslash \{x_1, ..., x_r\}, \end{cases}$$

4- Si $\sigma = (x_1, ..., x_r)$ est un $r - cycle$, on a alors pour tout entier k compris entre 1 et r :

$$x_k = \sigma^{k-1}(x_1)$$

En effet, c'est vrai pour $k = 1$ et supposant le résultat acquis pour $1 \le k \le r - 1$, on a :

$$x_k = \sigma(x_{k-1}) = \sigma(\sigma^{k-2}(x_1)) = \sigma^{k-1}(x_1).$$

Définition :
On appelle transposition, un cycle d'ordre 2.
On peut remarquer qu'une transposition τ est d'ordre 2 dans le groupe $S(E)$, c'est-à-dire que $\tau \ne Id_E$ et $\tau^2 = Id_E$. On a donc $\tau^{-1} = \tau$.
Plus généralement, on a le résultat suivant.

Lemme :
Un r-cycle est d'ordre r dans le groupe $(S(E), \circ)$.

Démonstration :
Soit $\sigma = (x_1, ..., x_r)$ un r-cycle avec $r \ge 2$.
Pour tout entier k compris entre 1 et r, on a :

$$\begin{aligned} \sigma^r(x_k) &= \sigma^r(\sigma^{k-1}(x_1)) = \sigma^{k-1}(\sigma^r(x_1)) \\ &= \sigma^{k-1}(\sigma(\sigma^{r-1}(x1))) \\ &= \sigma^{k-1}(\sigma(x_r)) \\ &= \sigma^{k-1}(x_1) \\ &= x_k. \end{aligned}$$

Comme $\sigma(x) = x$, pour $x \in E\backslash\{x_1, ..., x_r\}$, on en déduit que $\sigma^r = Id_E$.
Enfin avec $\sigma(x_1) = x_k \neq x_1$, pour $1 \leq k \leq r$, on déduit que $\sigma^{k-1} \neq Id_E$ et σ est d'ordre r.
On déduit du résultat précédent que l'inverse d'un $r - cycle$ σ est le $r - cycle$ $\sigma^{-1} = \sigma^{r-1}$.

Remarque :
La réciproque est fausse en général.
Par exemple, la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ est d'ordre 2 mais ce n'est pas une transposition puisqu'il y a deux orbites non réduites à un élément : $\{1, 2\}$ et $\{3, 4\}$.

Théorème :
Une permutation $\sigma \in S(E)$ est un cycle d'ordre $r \geq 2$ si, et seulement si, il n'y a qu'une seule $\sigma - orbite$ non réduite à un point.

Démonstration :
Soit $\sigma = (x_1, ..., x_r)$ un r-cycle. Pour $x \in E\backslash\{x_1, ..., x_r\}$, on a $\sigma(x) = x$ et $\Omega_\sigma(x) = \{x\}$.
Pour k compris entre 2 et r, on a $x_k = \sigma^{k-1}(x_1)$, donc $x_k \sim x_1$ modulo $\langle\sigma\rangle$ et comme $\sigma^r(x_1) = x_1$, on a :

$$\begin{aligned} \Omega_\sigma(x_k) = \Omega_\sigma(x_1) &= \{x_1, \sigma(x_1), ..., \sigma^{r-1}(x_1)\} \\ &= \{x_1, x_2, ..., x_r\} \end{aligned}$$

Il y a donc une seule orbite non réduite à un point.
Réciproquement si σ a une seule orbite non réduite a un point :

$$O = \{x, \sigma(x), ..., \sigma^{r-1}(x)\} = \{x_1, x_2, ..., x_r\}$$

avec $r \geq 2$, on a alors :

$$\begin{cases} \sigma(x_k) = \sigma(x_{k+1}) \\ \sigma(x_r) = x_1 \\ \sigma(x) = x \, si \, x \in E\backslash\{x_1, ..., x_r\} \end{cases}$$

et σ est le r-cycle $(x_1, x_2, ..., x_r)$.

Lemme :
Soient $\sigma \in S(E)\backslash\{Id_E\}$ et O une $\sigma - orbite$ de cardinal $r \geq 2$.
Pour tout $x \in O$, r est le plus petit entier naturel non nul tel que $\sigma^r(x) = x$ et :

$$O = Orb_\sigma(x) = \{x, \sigma(x), ..., \sigma^{r-1}(x)\}.$$

Démonstration. :
Comme $\sigma \neq Id_E$, il existe une orbite O non réduite à un point.
Il existe $y \in E$ tel que $O = Orb_\sigma(y) = \{\sigma(y) | k \in \mathbb{Z}\}$. Si $x \in O$, il existe alors un entier k tel que $x = \sigma^k(y)$ et :

$$Orb_\sigma(x) = \sigma^j(x) | j \in \mathbb{Z} = \{\sigma^{j+k}(y) | j \in \mathbb{Z}\}$$

$$= \{\sigma^i(y) | i \in \mathbb{Z}\} = O.$$

Si $\sigma^k(x) \neq x$ pour tout $k \geq 1$, on a alors $\sigma^i(x) \neq \sigma^j(x)$ pour tous $i \neq j$ dans $\mathbb{Z}$ et O est infini, ce qui n'est pas. Il existe donc un plus petit entier naturel non nul s tel que $\sigma^s(x) = x$.

Comme $O = Orb_\sigma(x)$ est de cardinal $r \geq 2$, elle n'est pas réduite à un point et $\sigma(x) \neq x$. On a donc $s \geq 2$.

En utilisant le théorème de division euclidienne, tout entier $k \in \mathbb{Z}$ s'écrit $k = qs + j$ avec $q \in \mathbb{Z}$ et $0 \leq j \leq s - 1$, ce qui donne :

$$\sigma^k(x) = \sigma^j(x)$$

et $O = \{x, \sigma(x), ..., \sigma^{s-1}(x)\}$.

Avec $\sigma^i(x) \neq \sigma^j(x)$ pour tous $i \neq j$ dans $\{0, 1, ..., s - 1\}$ (caractère minimal de s), on déduit que $card(O) = s$ et $s = r$.

Remarque :

1- On déduit du résultat précédent qu'une permutation $\sigma \in S(E)$ est un cycle d'ordre $r \geq 2$ si, et seulement si, il existe $x \in E$ tel que $Supp(\sigma) = \Omega_\sigma(x)$.

2- Si σ est un r-cycle, le calcul de σ^m pour tout entier relatif m peut alors s'obtenir en effectuant la division euclidienne de m par r : on a $m = qr + i$ avec $0 \leq i \leq r - 1$ et $\sigma^m = \sigma^i$.

3- La composée de deux cycles n'est pas un cycle en général. Par exemple pour $\sigma = (1, 2, 3, 4)$ dans S_4, on a

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

avec $\Omega_{\sigma^2}(1) = \{1, 3\}$ et $\Omega_{\sigma^2} = \{2, 4\}$, donc σ^2 n'est pas un cycle.

4- Une $\sigma - orbite$ $\Omega_\sigma(x)$ est réduite à un point si, et seulement si, $\sigma(x) = x$ et les orbites non réduites à un point forment une partition du support de σ.

Exercice :

On suppose que $card(E) = n \geq 2$. Montrer que, pour $2 \leq r \leq n$, dans $S(E)$ il y a $C_n^r = \dfrac{n!}{r(n-r)!}$ cycles d'ordre r distincts.

Solution :

Pour définir un r-cycle, on choisit d'abord une liste $(x_1, ..., x_r)$ dans E, il y a $A_n^r = r!C_n^r = \dfrac{n!}{(n-r)!}$ possibilités. Pour un tel choix de la partie $\{x_1, ..., x_r\}$ de E, les r permutations circulaires :

$$(x_1, ..., x_r), (x_2, x_3, ..., x_r, x_1), , (x_r, x_1, ..., x_r - 1)$$

donnent le même cycle, les autres permutations donnant des cycles différents, il y a donc $\frac{A_n^r}{r} = (r-1)!C_n^r$ possibilités.

Exercice :

Montrer que si σ et σ' sont deux cycles tels l'intersection $Supp(\sigma) \cap Supp(\sigma')$ est réduite à un point, alors le produit $\sigma\sigma'$ est un cycle.

Solution :

Soient $\sigma = (x_1, x_2, ..., x_r)$ et $\sigma' = (x'_1, ..., x'_s)$ deux cycles tels que $Supp(\sigma) \cap Supp(\sigma') = \{x_k\}$. Si j est l'entier compris entre 1 et s tel que $x_k = x'_j$, on a alors :

$$\begin{aligned}\sigma\sigma' &= (x_{k+1}, ..., x_r, x_1, ..., x_k)(x_k, x'_{j+1}, ..., x'_s, x'_1, ..., x'_{j-1}) \\ &= (x_{k+1}, ..., x_r, x_1, ..., x_k, x'_{j+1}, ..., x'_s, x'_1, ..., x'_{j-1})\end{aligned}$$

Exercice :

Soit $\sigma = (x_1, x_2, ..., x_r)$ un cycle de longueur paire.
Montrer que σ^2 n'est pas un cycle.

Solution :

Soit $r = 2p$ la longueur de σ avec $p - 1$. Pour p = 1, $\sigma^2 = Id_E$ n'est pas un cycle et pour $p \geq 2$, on a :

$$Orb_{\sigma^2}(x_1) = \{x_1, x_3, ..., x_{2p-1}\} \, et \, Orb_{\sigma^2}(x_2) = \{x_2, x_4, , x_{2p}\}$$

et σ^2 n'est pas un cycle.

1.4 Centre de S(E)

Définition :

On désigne par $Z(S(E))$ le centre du groupe de $S(E)$, c'est-à-dire l'ensemble des éléments de $S(E)$ qui commutent à tous les autres éléments de $S(E)$.

Lemme :

On a :

$$Z(S(E)) = \begin{cases} S(E) \, si \, card(E) = 2 \\ \{Id_E\} \, si \, card(E) \geq 3 \end{cases}$$

Démonstration :

Si $card(E) = 2$, le groupe $S(E)$ est commutatif et $Z(S(E)) = S(E)$.

On suppose que $card(E) \geq 3$ et on se donne σ dans $Z(S(E))$. Pour $x \neq y$ dans E, on a :

$$(\sigma(x), \sigma(y)) = \sigma(x, y)\sigma^{-1} = (x, y)\sigma\sigma^{-1} = (x, y)$$

et donc $\sigma\{x, y\} = \{x, y\}$. Pour $card(E) \geq 3$, on peut trouver, pour tout $x \in E$ deux éléments $y \neq z$ distincts de x et avec $\{x\} = \{x, y\} \cap \{y, z\}$, on déduit que :

$$\begin{aligned}\{\sigma(x)\} &= \sigma(\{x\}) = \sigma(\{x, y\} \cap \{y, z\}) \\ &= \sigma(\{x, y\}) \cap \{x, z\}) = \{x, y\} \cap \{y, z\} = \{x\}\end{aligned}$$

ce qui donne $\sigma(x) = x$. On a donc $\sigma = Id_E$.
Le centre de $S(E)$ est donc réduit à $\{Id\}$.
On retrouve ainsi le fait que $S(E)$ n'est pas commutatif pour $n \geq 3$.

Exercice :

On suppose que $card(E) \geq 3$. Montrer que pour toute permutation $\sigma \in S(E) \backslash \{IdE\}$, il existe une transposition qui ne commute pas à σ. On a donc $\sigma \neq Z(S(E))$ et on retrouve ainsi le fait que $Z(S(E)) = \{Id_E\}$.

Solution :

Si $\sigma \in S(E) \backslash \{Id\}$, il existe $x \in E$ tel que $y = \sigma(x) \neq x$. On se donne $z \in E \backslash \{x, y\}$ (E a au moins 3 éléments) et τ est la transposition $\tau = (y, z)$. Avec :

$$\sigma\tau(x) = \tau(x) = y \, et \, \tau\sigma(x) = \tau(y) = z \neq y$$

on déduit que $\sigma\tau \neq \tau\sigma$ et $\sigma \notin Z(S(E))$.

1.5 Décomposition d'une permutation

Comme précisé au paragraphe précédent, E est un ensemble fini de cardinal $n \geq 2$.

Pour toute permutation $\sigma \in S(E)$, on note $\theta(\sigma)$ son ordre dans le groupe $S(E)$.

Définition :

On dit que deux cycles σ et σ' dans $S(E)$ sont disjoints si leurs supports sont disjoints dans E.

En utilisant le fait que les $\sigma - orbites$ forment une partition de E et que chaque $\sigma - orbite$ non réduite à un point permet de définir un cycle, on obtient le résultat suivant qui nous donne un premier système de générateurs de $S(E)$.

Théorème :

Toute permutation $\sigma \in S(E) \backslash \{Id_E\}$ se décompose en produit de cycles deux à deux disjoints. Cette décomposition est unique à l'ordre près.

Si $\sigma = \gamma_1 ... \gamma_p$ est une telle décomposition, on a alors la partition :

$$Supp(\sigma) = \bigcup_{k=1}^{p} Supp(\gamma_k)$$

et :

$$\theta(\sigma) = ppcm(\theta(\gamma_1), ..., \theta(\gamma)).$$

Ici il faut bien sûr faire abstraction des 1-cycles, sinon il n'y a pas d'unicité, car on peut toujours composer par Id_E un nombre arbitraire de fois. L'identité elle-même s'écrit comme un produit vide, par définition égal à l'élément neutre du groupe. Cependant, il arrive qu'on rajoute dans cette écriture les points fixes sous forme de 1-cycles à la fin du produit, pour mettre en évidence ces points fixes et en même temps l'ensemble de toutes les orbites.

Démonstration. :

Soient $\sigma \in S(E) \backslash \{Id_E\}$ et $O_1, ..., O_p, ..., O_r$ les $\sigma - orbites$ deux à deux distinctes avec $r_k = card(O_k) \geq 2$ pour $k = 1, ..., p$ et $card(O_k) = 1$ pour $k = p + 1, ..., r$ (s'il en existe). On a alors la partition $E = \bigcup_{k=1}^{r} O_k$

Pour tout entier k compris entre 1 et r, on désigne par γ la permutation de E définie par :

$$\forall x \in E, \gamma(x) = \begin{cases} \sigma(x)\, si\, x \in O_k \\ x\, si\, x \notin O_k \end{cases}$$

(γ_k est bien une permutation de E car la restriction de σ à une orbite O_k est une permutation de O_k). Si O_k est réduite à un point, alors $\gamma_k = Id_E$, sinon γ_k est un $r_k - cycle$: en effet, pour $x \notin O_k$, on a $\gamma_k(x) = x$ et $Orb_{\gamma_k}(x) = \{x\}$ et pour $x \in O_k$, on a :

$$\begin{aligned} Orb_{\gamma_k}(x) &= \{\gamma_k^j(x) | j \in \mathbb{Z}\} = \{\sigma^j(x) | j \in \mathbb{Z}\} \\ &= Orb_\sigma(x) = O_k \end{aligned}$$

donc γ_k a bien une seule orbite non réduite à un point.

On vérifie alors que $\sigma = \prod_{j=1}^r \gamma_j = \prod_{j=1}^p \gamma_j$. En effet, pour $x \in E$ il existe un unique indice k compris entre 1 et r tel que $x \in O_k$ et on a $\gamma_k(x) = \sigma(x), \gamma_j(x) = x$ pour $j \neq k$ (puisque $x \notin O_j$) et tenant compte du fait que les γ_j commutent (leurs supports sont deux à deux disjoints), on en déduit que :

$$\left(\prod_{j=1}^r \gamma_j\right)(x) = \left(\gamma_k \prod_{j=1 j\neq k}^r \gamma_j\right)(x) = \gamma_k(x) = \sigma(x)$$

Il reste à montrer l'unicité, à l'ordre près, d'une telle décomposition.

Soit $\sigma = \prod_{j=1}^{p'} \gamma'_k$ est une autre décomposition en cycles deux à deux disjoints.

En notant $O'_1, ..., O'_p$ les supports de ces cycles, pour $k \in \{1, ..., p'\}$ et $x \in O'_k$, on a $\sigma(x) = \gamma'_k(x)(x \neq O'_j$ pour $j \neq k$ et les cycles commutent), donc $O'_k = Orb_{\gamma'_k}(x) = Orb_\sigma(x)$.

Les orbites O'_k sont donc les orbites non réduites à un point de σ et $p' = p$. On a donc $O'_k = O_j$ pour un unique j compris entre 1 et p. Pour $x \in O'_k$, on a $\gamma'_k(x) = \sigma(x) = \gamma_j(x)$ et pour $x \neq O'_k, \gamma'_k(x) = x = \gamma_j(x)$, ce qui donne $\gamma_k = \gamma_j$ et l'unicité de la décomposition à l'ordre près.

La réunion $\bigcup_{k=1}^p Supp(\gamma_k)$ est la réunion des orbites O_k non réduites à un point, soit le support de σ.

Notons $\mu = ppcm(\theta(\gamma_1), ..., \theta(\gamma_p))$.

Comme les cycles γ_k commutent, on a $\sigma^k = \gamma_1^k ... \gamma_p^k$ pour tout entier naturel k et $\sigma_k = Id_E$ si, et seulement si $\gamma_j^k = Id_E$ pour tout j compris entre 1 et p. En effet, il est clair que la condition est suffisante et si $\sigma^k = Id_E$, on a alors pour tout $x \in O_j(O_1, ..., O_p$ sont toutes les $\sigma - orbites)\gamma_j^k(x) = \sigma^k(x) = x$ et aussi $\gamma_j^k(x) = x$ pour $x \neq O_j$, donc $\gamma_j^k = Id_E$. Il en résulte que l'ordre de σ est un multiple commun des ordres des σ_j et c'est un multiple de μ qui lui même est multiple de l'ordre de σ puisque $\sigma^\mu = Id_E$. D'où l'égalité.

Remarque :

1- On conviendra que l'identité est produit de 0 cycle : $Id_E = \gamma^0$ pour tout cycle γ.

2- Comme l'ordre d'un cycle est égal à sa longueur, l'ordre de σ est aussi le ppcm des longueurs des cycles γ_j.

Pour $E = \{1, 2, ..., n\}$, une telle décomposition s'obtient en prenant, dans le cas où il n'est pas fixe, les images de 1 par σ, σ^2, ... , jusqu'au moment où on retombe sur 1 (l'orbite de 1), puis on recommence avec le plus petit entier dans

$E \backslash Orb_\sigma(1)$ qui n'est pas fixe et ainsi de suite. Par exemple, pour :

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

on a $\sigma(1) = 2$, $\sigma^2(1) = 3$, $\sigma^3(1) = 4$, $\sigma^4(1) = 5$, $\sigma^5(1) = 1$, ce qui donne le premier cycle $(1, 2, 3, 4, 5)$, puis $\sigma(6) = 7$, $\sigma^2(6) = 6$ et $\sigma(8) = 8$, donc $\sigma = (1, 2, 3, 4, 5)(6, 7)$.

Exemple :
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 8 & 7 & 3 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\ 4\ 3\ 7)(2\ 8) = (2\ 8)(1\ 4\ 3\ 7)$
L'ordre de σ est

$$\theta(\sigma) = ppcm(2, 4) = 4$$

Remarques :
1. Cette preuve fournit une méthode pratique de décomposition en produit de cycles : on cherche le cycle correspondant à l'orbite de 1, qui est fourni par les images itérées de 1 par σ, puis on recommence avec le plus petit entier qui n'est pas dans cette orbite, etc...
2. La décomposition en produit de cycles permet par exemple de calculer facilement l'ordre d'une permutation puisque l'ordre d'un cycle est sa longueur et l'ordre d'un produit d'éléments commutant dans un groupe divise le ppcm de leurs ordres.

Exercice :
Soit $\sigma \in S_n$ définie par :

$$\forall k \in \{1, 2, ..., n\}, \sigma(k) = n + 1 - k$$

(elle inverse l'ordre des entiers 1, 2, ... , n). Donner la décomposition de σ en produit de cycles deux à deux disjoints.

Solution :
On a :

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

Si n est pair, soit $n = 2p$ avec $p \geq 1$, on a :

$$\sigma(k) = 2p + 1 - k, \sigma^2(k) = \sigma(2p + 1 - k) = k$$

pour $k = 1, ..., p$ (et $2p + 1 - k = 2p, ..., p + 1$), ce qui donne :

$$\sigma = (1, 2p)(2, 2p - 1)...(p, p + 1)$$

Si n est impair, soit $n = 2p + 1$ avec $p \geq 1$, on a :

$$\sigma(k) = 2p + 2 - k, \sigma^2(k) = \sigma(2p + 2 - k) = k$$

pour $k = 1, ..., p$ $(2p+2-k = 2p+1, ..., p+2)$ et $\sigma(p+1) = p+1$ ce qui donne :

$$\sigma = (1, 2p + 1)(2, 2p)...(p, p + 2)$$

Donc σ est produit de transpositions deux a deux disjointes et est d'ordre 2 (ce qui se voit directement sur sa définition).

Exercice :
Quel est l'ordre maximal d'un élément de S_5.

Solution :
La décomposition en cycles disjoints d'un élément de $S_5 \backslash \{Id\}$(Id est d'ordre 1) est formée soit d'un r-cycle avec $2 \leq r \leq 5$, soit d'un 2-cycle et d'un cycle d'ordre 2 ou 3 et cet ordre est au maximum 6, qui est atteint pour (1, 2) (3, 4, 5) .

Exercice :
soit σ et γ deux permutations dans $S(E) \backslash \{Id_E\}$.
Exprimer la décomposition de $\sigma\gamma\sigma^{-1}$ en fonction de celle de γ.

Solution :
Si $\gamma = \prod_{j=1}^{p} \gamma_j$ est la décomposition en cycles disjoints de γ, alors :
$\sigma\gamma\sigma^{-1} = \prod_{j=1}^{p}(\sigma\gamma_j\sigma^{-1})$ est celle de $\sigma\gamma\sigma^{-1}$ puisque pour $\gamma_j = (x_1, ..., x_r)$ on a $\sigma\gamma_j\sigma^{-1} = (\sigma(x_1), ..., \sigma(x_r))$ et les supports de ces cycles sont 2 à 2 disjoints du fait que σ est bijective

Exercice :
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 3 & 3 & 1 & 7 & 6 & 8 \end{pmatrix}$
calculer σ^{2009}.

Solution :
La permutation $\sigma = (1, 2, 3, 4, 5)(6, 7) = \gamma\tau$ est d'ordre ppcm (5, 2) = 10.
En effectuant la division euclidienne, on a pour tout entier relatif $m = 10q + r$ où $0 \leq r \leq 9$, $\sigma^m = \sigma^r$. Ce qui donne

$$\begin{aligned} \sigma^{2009} &= \sigma^9 = \gamma^9\tau^9 = \gamma^{-1}\tau \\ &= (5, 4, 3, 2, 1)(6, 7) \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 2 & 3 & 4 & 7 & 6 & 8 \end{pmatrix}. \end{aligned}$$

1.6 Classes de conjugaison

Lemme :
Soit r un entier compris entre 2 et $card(E)$.
Le conjugué dans $S(E)$ d'un r-cycle est encore un r-cycle. Précisément, pour tout r-cycle $\sigma = (x_1, x_2, ..., x_r)$ et toute permutation τ, on a :$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \tau(x_2), ..., \tau(x_r))$.
Réciproquement, deux cycles de même longueur sont conjugués dans $S(E)$, c'est-à-dire que si σ et σ' sont deux cycles de même longueur r-cycles, il existe alors une permutation τ telle que $\sigma' = \tau \circ \sigma \circ \tau^{-1}$.

Démonstration :
En notant $\sigma'' = (\tau(x_1), \tau(x_2), ..., \tau(x_r))$, il s'agit de montrer que $\tau \circ \sigma = \sigma'' \circ \tau$.
Pour $x \in E \backslash \{x_1, ., x_r\}$, on a $\sigma(x) = x$ et $\tau(x) \in E \backslash (\tau(x_1), ..., \tau(x_r)$, ce qui

donne :

$$\tau \circ \sigma(x) = \tau(x) = \sigma''(\tau(x)) = \sigma'' \circ \tau(x)$$

Si x est l'un des x_k, on a alors :

$$\tau \circ \sigma(x) = \tau(\sigma(x_k)) = \tau(x)$$

en notant $x_{r+1} = x_1$ et :

$$\sigma'' \circ \tau(x) = \sigma''(\tau(x_k)) = \tau(x_k).$$

On a donc bien $\tau \circ \sigma = \sigma \circ \tau$, soit $\tau \circ \sigma \circ \tau^{-1} = \sigma$.

Soient $\sigma = (x_1, x_2, ..., x_r)$ et $\sigma' = (x'_1, x'_2, ..., x'_r)$ deux r-cycles. En se donnant une bijection φ de $E \backslash \{x, ..., x\}$ sur $E \backslash \{x'_1, ..., x'_r\}$, on définit une permutation τ de E en posant $\tau(x_k) = x'_k$ pour $k = 1, ..., r$ et $\tau(x) = \varphi(x)$ pour $x \in E \backslash \{x_1, ..., x_r\}$ et on a :

$$\tau \circ \sigma \circ \tau^{-1} = (\tau(x_1), \tau(x_2), ..., \tau(x_r)) = (x'_1, x'_2, ..., x'_r) = \sigma'.$$

Le résultat précédent se traduit en disant que, pour tout entier r compris entre 2 et $card(E)$, le groupe $S(E)$ agit par conjugaison de façon transitive sur l'ensemble des r-cycles.

En faisant agir $S(E)$ par conjugaison sur l'ensemble des cycles, l'orbite d'un r-cycle pour cette action est l'ensemble de tous les r-cycles et son cardinal est $\frac{A_n^r}{r} = (r-1)! C_n^r$.

Exemple :

Pour $n = 6$, $\sigma = (1\ 3\ 4)$ et $\alpha = (1\ 2)(3\ 5\ 6)$,
on a :

$$\alpha \sigma \alpha^{-1} = (2\ 5\ 4).$$

Corollaire :

La classe de conjugaison d'un $k_1 \times ... \times k_r - cycle$ est l'ensemble des $k_1 \times ... \times k_r - cycle$.

démonstration :

Soit $\sigma = \sigma_1 ... \sigma_r$ un $k_1 \times ... \times k_r - cycle$.

Pour tout élément α de S_n, $\alpha \sigma \alpha^{-1} = \alpha \sigma_1 \alpha^{-1} ... \alpha \sigma_r \alpha^{-1}$ donc, d'après la Proposition précédente, $\alpha \sigma \alpha^{-1}$ est un $k_1 \times ... \times k_r - cycle$.

Soit φ un $k_1 \times ... \times k_r - cycle$.

Posons $\sigma = (i_1^1 ... i_{k_1}^1) ... (i_1^r ... i_{k_r}^r)$ et $\varphi = (j_1^1 ... j_{k_1}^1) ... (j_1^r ... j_{k_r}^r)$.

Définissons α par $\alpha(i_s^t) = j_s^t$ pour tout t compris entre 1 et r et pour tout s compris entre 1 et k_t, et α bijective de $\{1, ..., n\} \backslash \{i_1^1, ..., i_{k_r}^r\}$ vers $\{1, ..., n\} \backslash \{j_1^1, ..., j_{k_r}^r\}$ (ce qui est possible car ces deux derniers ensembles ont le même cardinal).

Puisque les supports des cycles sont deux à deux disjoints, α est une application injective.

De plus, α est surjective par construction donc α appartient à S_n. D'après la Proposition précédente, $\alpha \sigma \alpha^{-1} = \varphi$ donc φ et σ sont conjugués.

D'où, la classe de conjugaison du $k_1 \times ... \times k_r - cycle$ σ est l'ensemble des $k_1 \times ... \times k_r - cycles$.

Corollaire :
Deux permutations sont conjuguées si et seulement si les ensembles des longueurs des cycles apparaissant dans leurs décompositions en cycles à supports disjoints sont égaux.

Proposition :
Pour tout $\sigma \in S_n$, et $1 \leq j \leq n$, soit $a_j(\sigma)$ le nombre de cycles de longueur j de σ, on a donc $n = \sum_{j=1}^{n} j a_j(\sigma)$.
Alors σ est conjugué à σ' si et seulement si $a_j(\sigma) = a_j(\sigma')$, pour tout $1 \leq j \leq n$.

Démonstration :
Soient H et H' les sous-groupes de S_n engendrés par σ et σ' respectivement.
Si $\tau \in S_n$ est tel que $\tau\sigma\tau^{-1} = \sigma'$, il est clair que $\tau H \tau^{-1} = H'$, et si $C = Hx$ est une $H-orbite$ (i.e. un cycle de σ), $C' = \tau(C) = H'\tau(x)$ est un cycle de σ'. Donc τ définit une bijection de l'ensemble des cycles de σ sur l'ensemble des cycles de σ', qui respecte évidemment les longueurs, ce qui prouve que $a_j(\sigma) = a_j(\sigma')$ pour $1 \leq j \leq n$
Réciproquement, supposons que $a_j(\sigma) = a_j(\sigma')$ pour $1 \leq j \leq n$. Rangeons les cycles $C_1, \dots, C_s$ de σ par ordre de longueurs décroissantes, et faisons de même pour les cycles $C'_1, \dots, C'_s$ de σ' (remarquons que l'hypothèse dit que σ et σ' ont même nombre de cycles en chaque longueur, donc aussi même nombre total de cycles).
Alors on a $|C_j| = |C'_j|$ pour $1 \leq j \leq s$.
Choisissons un élément x_j dans chaque C_j , et de même un x'_j dans chaque C'_j, et soit $d_j = |C_j| = |C'_j|$. on a alors $C_j = \{\sigma^i(x_j)\}_{0 \leq i \leq d_j}$, et $C'_i = \{\sigma'^i(x'_j)\}_{0 \leq i \leq d_j}$.
Définissons maintenant une permutation τ de $S(E)$ en posant $\tau(\sigma^i(x_j)) = (\sigma'^i(x_j)$.
On a alors clairement $\tau\sigma(x) = \sigma'\tau(x)$ pour tout $x \in E$, donc $\tau\sigma\tau^{-1} = \sigma'$.

1.7 Systèmes de générateurs de S(E)

On sait que le groupe S_n est engendré par les cycles. Il est souvent utile, pour montrer certaines propriétés des permutations, de pouvoir se restreindre à un ensemble plus petit de générateurs.

Lemme :
Pour $2 \leq r \leq n$, tout r-cycle dans $S(E)$ s'écrit comme produit de $r-1$ transpositions.

Démonstration. :
Résulte de : $(x_1, x_2, ..., x_r) = (x_1, x_2)(x_2, x_3)...(x_{r-1}, , x_r)$

Théorème :
Toute permutation $\sigma \in S(E)$ se décompose en produit de transpositions (le groupe $S(E)$ est engendré par les transpositions).

Démonstration :

On a $Id_E = \tau^2$ pour toute transposition.
Toute permutation $\sigma \in S(E)\backslash\{Id_E\}$ est produit de cycles et un cycle est produit de transpositions.

Remarque :

Dans la décomposition d'une permutation en produit de transpositions, il n'y a pas unicité et les transpositions ne commutent pas nécessairement.
Par exemple, on a : $(2,3) = (1,2)(1,3)(1,2)$ et : $(1,2)(2,3) = (1,2,3) \neq (2,3)(1,2) = (3,2)(2,1) = (3,2,1)$.

Exemple :

Pour : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} \in S_8$
On écrit d'abord σ sous forme de produit de cycles à supports disjoints :

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

On applique ensuite le Lemme pour décomposer chacun des cycles en produit de transpositions :

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

Lemme :

S_n est engendré par les $n-1$ transpositions $(1,k)$ où $2 \leq k \leq n$.

Démonstration :

Soit (i,j) une transposition avec $1 \leq i \neq j \leq n$. Si $i = 1$ ou $j = 1$, il n'y a rien à faire ($(i,j) = (j,i)$) et pour $i \neq 1$, $j \neq 1$, on a : $(i,j) = (1,i)(1,j)(1,i)^{-1} = (1,i)(1,j)(1,i)$(par conjugaison).
Le résultat se déduit alors du fait que S_n est engendré par les transpositions.

Remarque :

Il n'est pas possible d'enlever une de ces transpositions $(1,k)$ du fait que pour $2 \leq k \leq n$ et $2 \leq j \neq k \leq n$, toutes les transposition $(1,j)$ laissent fixe k.

Exemple :

Pour $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1,2)(2,3)(3,4)(4,5)(6,7)$ on a :

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

Lemme :

S_n est engendré par les $n-1$ transpositions $(k, k+1)$ où $1 \leq k \leq n-1$.

Démonstration. :

Comme S_n est engendré par les transpositions $(1,k)$ où $2 \leq k \leq n$, il suffit d'écrire chaque transposition $(1,k)$ comme produit de transpositions du type $(i,i+1)$.

Pour $3 \leq k \leq n$, on a :

$$(1,k) = (k-1,k)(1,k-1)(k-1,k)^{-1} = (k-1,k)(1,k-1)(k-1,k)$$

Pour $k=3$, on a $(1,k-1) = (1,2)$ et c'est terminé, sinon on écrit :

$$(1,k-1) = (k-2,k-1)(1,k-2)(k-2,k-1)$$

et on continue ainsi de suite si nécessaire.

Pour $k=2$, la transposition $(1,k) = (1,2)$ est de la forme souhaitée.

Remarque :

Il n'est pas possible d'enlever une de ces transpositions $(k,k+1)$ du fait que pour $1 \leq k \leq n-1$ et $1 \leq j \neq k \leq n-1$, toutes les transposition $(j,j+1)$ laissent globalement invariant la partie $\{1,...,k\}$.

Lemme :

S_n est engendré par $(1,2)$ et $(1,2,...,n)$ (Sn est $di-cyclique$).

Démonstration. :

Comme S_n est engendré par les transpositions $(k,k+1)$ où $1 \leq k \leq n-1$, il suffit de montrer que chaque transposition $(k,k+1)$ est dans le sous-groupe G de S_n engendré par $\tau = (1,2)$ et $\gamma = (1,2,...,n)$.

On a déjà $(1,2) \in G$ et, pour $n \geq 3$:

$$\begin{cases} \gamma(1,2)\gamma^{-1} = (\gamma(1),\gamma(2)) = (2,3) \\ \gamma(2,3)\gamma^{-1} = (\gamma(2),\gamma(3)) = (3,4) \\ . \\ . \\ . \\ \gamma(n-2,n-1)\gamma^{-1} = (\gamma(n-2),\gamma(n-1)) = (n-1,n) \end{cases}$$

soit $(k,k+1) = \gamma^{k-1}(1,2)(\gamma^{k-1})^{-1}$ pour $1 \leq k \leq n-1$.

Exercice :

Montrer directement par récurrence sur $n \geq 2$, que $S(E)$ est engendré par les transpositions.

Solution :

Pour $E = \{x_1, x_2\}$, on a $S(E) = \{Id_E, (x_1,x_2)\}$.

Supposons le résultat acquis pour les ensembles de cardinal $n-1 \geq 2$ et soit E de cardinal n. Soient $\sigma \in S(E)$. Si $\sigma = Id_E$, on a $\sigma = \tau^2$ pour toute transposition τ. Sinon il existe $x \in E$ tel que $y = \sigma(x) \neq x$.

En désignant par τ la transposition $\tau = (x, y)$, on a $\tau\sigma(x) = x$ et la restriction de $\tau\sigma$ à $F = E\backslash\{x\}$ est une permutation de F, elle s'écrit donc comme produit de transpositions et $\tau\sigma = \tau_1 ... \tau_r$ où les τ_k sont des transpositions de E qui laissent fixe x. Il en résulte que $\sigma = \tau\tau_1 ... \tau_r$ est produit de transpositions.

Cette démonstration montre aussi que si $\{1\tau_1, ..., \tau_r\}$ est une famille de transpositions qui engendre $S(E)$, on a nécessairement $r \geq n - 1$.

Exercice :

Montrer que, pour $n \geq 3$, S_n est engendré par (1, 2) et (2, 3, ... , n).

Solution :

Comme S_n est engendré par les transpositions (1, k) où $2 \leq k \leq n$, il suffit de montrer que chaque transposition (1, k) est dans le sous-groupe G de S_n engendré par (1, 2) et (2, 3, ... , n).

On a déjà $(1, 2) \in G$. En notant $\sigma_k = (2, 3, ..., n)^{k-2}$ pour $3 \leq k \leq n$, on a $\sigma_k(1) = 1$, $\sigma_k(2) = k$, et :

$(1, k) = \sigma_k(1, 2)\sigma^{-}1\ k \in H$.

Chapitre 2

Signature et groupe alterné

2.1 Signature d'une permutation

Pour toute permutation $\sigma \in S(E)$, on note $\mu(\sigma)$ le nombre de $\sigma - orbites$ distinctes.
Si $\sigma = \prod_{k=1}^{p} \sigma_k$ est la décomposition de σ en produit de cycles deux à deux disjoints, on a vu que p est le nombre de $\sigma - orbites$ non réduites à un point et $\mu(\sigma) = p + \varphi(\sigma)$ où $\varphi(\sigma)$ est le nombre de points fixes de σ.

Définition :
La signature d'une permutation $\sigma \in S(E)$ est l'élément $\epsilon(\sigma)$ de $\{1, -1\}$ défini par : $\epsilon(\sigma) = (-1)^{n-\mu(\sigma)}$

Exemple :
L'identité a n orbites réduites à un point et $\epsilon(Id_E) = 1$.

proposition :
Si σ est un r-cycle, il a une orbite non réduite à un point et $n - r$ orbites réduites à un point, donc $\mu(\sigma) = n - r + 1$ et $\epsilon(\sigma) = (-1)^{r-1}$.

Démonstration :
Un r-cycle σ a une seule orbite non ponctuelle et celle-ci est de cardinal r.
On a donc $1 + (n - r)$ orbites et par conséquent $\epsilon(\sigma) = (-1)^{r-1}$.

Proposition :
Un r-cycle est une permutation impaire si r est pair et une permutation paire si r est impaire.

Exemple :
Si τ est une transposition, on $\epsilon(\sigma) = -1$.

Lemme :
Pour toute permutation $\sigma \in S(E)$ et toute transposition $\tau \in S(E)$, on a :

$$\epsilon(\tau\sigma) = -\epsilon(\sigma).$$

Démonstration :

Soit $\tau = (x, y)$ une transposition dans $S(E)$ avec $x \neq y$.

Si $\sigma = Id_E$, on a alors $\tau\sigma = \tau$ et $\epsilon(\tau\sigma) = -1$.

Pour $\sigma \neq Id_E$, on a la décomposition en produit de cycles deux à deux disjoints, $\sigma = \sigma_1 ... \sigma_p$, où les $O_k = Supp(\sigma_k)$, pour k compris entre 1 et p, sont toutes les orbites non réduites à un point.

Si $\{x, y\} \cap \bigcup_{k=1}^{p} O_k = \emptyset$, le nombre de points fixes de $\sigma' = \tau\sigma$ est alors $\varphi(\sigma') = \varphi(\sigma) - 2$ et le nombre de $\sigma' - orbites$ est :

$$\mu(\sigma') = p + 1 + \varphi(\sigma) - 2 = \mu(\sigma) - 1$$

ce qui donne $\epsilon(\sigma') = -\epsilon(\sigma)$.

Si $\{x, y\}$ est contenu dans l'une des $\sigma - orbites O_k$, comme les cycles σ_j commutent, on a :

$$\sigma' = \tau\sigma_k \prod_{j=1 j\neq k} \sigma_j$$

avec :

$$y \in O_k = Orb_\sigma(x) = \{x, \sigma(x), ..., \sigma_{r_k - 1}(x)\} = \{1x_1, ..., x_{r_k}\}$$

Il existe donc $j \in \{2, ..., r_k\}$ tel que $y = x_j$ et :

$$\begin{aligned} \tau\sigma_k &= (x_1, x_j)(x_1, ..., x_j, ..., x_{r_k}) = (x_1, ..., x_{j-1})(x_j, ..., x_{r_k}) \\ &= \sigma'_k \sigma''_k \end{aligned}$$

(pour $j = r_k, \sigma''_k = Id_E$), ce qui donne la décomposition en produit de cycles deux à deux disjoints :

$$\sigma' = \sigma'_k \sigma''_k \prod_{j=1 j\neq k} \sigma_j$$

On a donc,$\mu(\sigma') = \mu(\sigma) + 1$ (pour $j = r_k$, le nombre de cycles est inchangé, mais x_{r_k} est un point fixe de plus) et $\epsilon(\sigma') = -\epsilon(\sigma)$.

Si x et y sont dans deux $\sigma - orbites$ distinctes, soit $\{x, y\} \cap O_k = \{x\}$ et $\{x, y\} \cap O_j = \{y\}$ avec $j \neq k$, on a alors :

$$O_k = Orb_\sigma(x) = \{x, \sigma(x), ..., \sigma^{r_k - 1}(x)\} = \{x_1, ..., x_{r_k}\}$$

et :

$$O_j = Orb_\sigma(y) = \{y, \sigma(y), ..., \sigma^{r_j - 1}(y)\} = \{y_1, ..., y_{r_j}\}$$

donc :

$$\begin{aligned} \tau\sigma_k\sigma_j &= (x_1, y_1)(x_1, ..., x_{r_k})(y_1, ..., y_{r_j}) \\ &= (y_1, x_1)(x_1, ..., x_{r_k})(y_1, ..., y_{r_j}) \\ &= (y_1, x_1, ..., x_{r_k})(y_1, ..., y_{r_j}) \\ &= (x_1, ..., x_{r_k}, y_1)(y_1, ..., y_{r_j}) \\ &= (x_1, ..., x_{r_k}, y_1, ..., y_{r_j}) = \sigma'_k \end{aligned}$$

et la décomposition en produit de cycles deux à deux disjoints :

$$\sigma' = \tau\sigma_k\sigma_j \prod_{i=1 i\notin\{j,k\}} \sigma_i = \sigma'_k \prod_{i=1 i\notin\{j,k\}} \sigma_i$$

On a donc, $\mu(\sigma') = \mu(\sigma)^1$ et $\epsilon(\sigma') = -\epsilon(\sigma)$.

Enfin, la dernière possibilité est que x [*resp.* y] soit dans l'une des orbites O_k et y [*resp.* x] en dehors de la réunion de toutes les orbites. On a alors $\varphi(\sigma') = \varphi(\sigma) + 1$ et $O_k = Orb_\sigma(x) = \{x, \sigma(x), ..., \sigma^{r_k-1}(x)\} = \{x_1, ..., x_{r_k}\}$, donc :

$$\tau\sigma_k = (x_1, y)(x_1, ..., x_{r_k}) = (y, x_1, ..., x_{r_k})$$

et $\mu(\sigma') = \mu(\sigma) + 1$, ce qui donne $\epsilon(\sigma') = -\epsilon(\sigma)$.

On en déduit le théorème qui suit qui nous donne une définition équivalente de la signature d'une permutation.

Théorème :

Si $\sigma \in S(E)$ est produit de p transpositions, on a alors $\epsilon(\sigma) = (-1)^p$ (la parité de p est donc uniquement déterminée par σ).

Démonstration :

C'est une conséquence immédiate du lemme précédent et du fait que $\epsilon(\tau) = -1$ pour toute transposition τ.

corollaire :

La signature

$$\begin{aligned} \epsilon : S_n &\longrightarrow \{1, -1\} \\ \sigma &\longrightarrow \epsilon(\sigma) \end{aligned}$$

est un morphisme du groupe $(S_n; \circ)$ dans le groupe $(\{1, -1\}; \times)$.

Remarque :

on peut définir la signature comme l'unique morphisme non-trivial de S_n dans $\{1, -1\}$.

Théorème :

Les seuls morphismes de groupes de $(S(E), \circ)$ dans $(\mathbb{R}^*, .)$ sont l'application constante égale à 1 et la signature ϵ. La signature étant surjective de $S(E)$ sur $\{-1, 1\}$.

Démonstration. :

Montrons tout d'abord que ϵ est un morphisme de groupes surjectif de $(S(E), \circ)$ sur $\{-1, 1\}$.

On a vu que ϵ est à valeurs dans $\{-1, 1\}$ et avec $\epsilon(Id_E) = 1$, $\epsilon(\tau) = -1$ pour toute transposition τ (E a au moins deux éléments), on déduit que σ est surjectif.

Si σ, σ' sont deux permutations elles s'écrivent respectivement comme produit de p et q transpositions, ce qui permet d'écrire $\sigma\sigma'$ comme produit de p+q transpositions et on a $\epsilon(\sigma\sigma') = (-1)^{p+q} = \epsilon(\sigma)\epsilon(\sigma')$. Donc ϵ est un morphisme de groupes.

Soit φ un morphisme de groupe de $S(E)$ dans $\mathbb{R}^*$.

Si τ_1 et τ_2 sont deux transpositions, il existe une permutation σ telle que $\tau_2 = \sigma\tau_1\sigma^{-1}$ et comme le groupe multiplicatif $\mathbb{R}^*$ est commutatif, on a :

$$\varphi(\tau_2) = \varphi(\sigma)\varphi(\tau_1)\varphi(\sigma^{-1}) = \varphi(\sigma)\varphi(\sigma^{-1})\varphi(\tau_1) = \varphi(\tau_1)$$

c'est-à-dire que φ est constant sur les transpositions. Avec :

$$\varphi(Id_E) = \varphi(\tau_2) = (\varphi(\tau))^2$$

pour toute transposition τ, on déduit que $\varphi(\tau) = 1$ pour toute transposition τ ou $\varphi(\tau) = -1$ pour toute transposition τ. Dans le premier cas, on a $\varphi(\sigma) = 1$ pour toute permutation σ puisque les transpositions engendrent $S(E)$ et dans le second cas, comme toute permutation $\sigma \in S(E)$ s'écrit $\sigma = \prod_{k=1}^{p} \tau_k$ où les τ_k sont des transpositions, on a $\varphi(\sigma) = \prod_{k=1}^{p} \varphi(\tau_k) = (-1)^p = \epsilon(\sigma)$.

Exercice :

Déterminer la signature de :

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

Solution :

on a :

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

et $\epsilon(\sigma) = (-1)^{5-1}(-1) = -1$. on peut aussi écrire σ comme produit de transposition :

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

et $\epsilon(\sigma) = (-1)^5 = -1$.

Le résultat qui suit nous donne une autre définition de la signature d'une permutation $\sigma \in S_n$ (on peut toujours se ramener à ce cas).

Théorème :

Pour toute permutation $\sigma \in S_n$, on a : $\epsilon(\sigma) = \prod \frac{\sigma(j)-\sigma(i)}{j-i}$.

Démonstration. :

Soit φ l'application définie sur S_n par $\varphi(\sigma) = \prod \frac{\sigma(j)-\sigma(i)}{j-i}$. Pour montrer que $\varphi = \epsilon$, il suffit de montrer que φ est un morphisme de groupes non constant de S_n dans $\mathbb{R}^*$.

Comme σ est bijective, on a $\varphi(\sigma) \in \mathbb{R}^*$ pour tout $\sigma \in S_n$.

Pour σ_1, σ_2 dans S_n, on a :

$$\begin{aligned}
\varphi(\sigma_1\sigma_2) &= \prod_{1\le i<j\le n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(j)} \frac{\sigma_2(j) - \sigma_2(i)}{j-i} \\
&= \prod_{1\le i<j\le n} \frac{\sigma_1(\sigma_2(j)) - \sigma_1(\sigma_2(i))}{\sigma_2(j) - \sigma_2(j)} \prod \frac{\sigma_2(j) - \sigma_2(i)}{j-i} \\
&= \prod_{1\le i'<j'\le n} \frac{\sigma_2(j) - \sigma_2(i)}{j-i} \prod \frac{\sigma_2(j) - \sigma_2(i)}{j-i}
\end{aligned}$$

puisque σ_2 est bijective de $\{1,...,n\}$ sur $\{1,...,n\}$ et $\frac{\sigma_1(j')-\sigma_1(i')}{j'-i'} = \frac{\sigma_1(i')-\sigma_1(j')}{i-j'}$ ce qui donne $\varphi(\sigma_1\sigma_2) = \varphi(\sigma_1)\varphi(\sigma_2)$.

On a $\varphi(Id_E) = 1$ et pour $\tau = (1,2)$:

$$\begin{aligned}
\varphi(\tau) &= \prod_{i=1}^{n-1} \prod_{j=i+1}^{n} \frac{\tau(j) - \tau(i)}{j-i} \\
&= \prod_{j=2}^{n} \frac{\tau(j) - 2}{j-1} \prod_{j=3}^{n} \frac{j-1}{j-2} \\
&= -\prod_{j=3}^{n} \frac{j-2}{j-1}\frac{j-1}{j-2} = -1
\end{aligned}$$

donc φ est non constant et c'est la signature.

Du théorème précédent, on déduit que $\epsilon(\sigma) = ((-1)^{\nu(\sigma)}$, où :

$$\nu(\sigma) = card\{(i,j) \in \mathbb{N}^2 | 1 \le i < j \le net\sigma(j) < \sigma(i)\}$$

est le nombre d'inversions de σ. Ce qui nous donne une définition supplémentaire de la signature.

définition :

On appelle nombre d'inversions de $\sigma \in S_n$, et note $I(\sigma)$, le nombre de couples $(i;j)$ tels que $i < j$ et $\sigma(i) > \sigma(j)$.

Proposition :

En utilisant la définition, pour $\sigma \in S_n$ on a :
$\epsilon(\sigma) = (-1)^{I(\sigma)}$.

Exemple :

Pour :

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

on a 5 inversions, donc $\epsilon(\sigma) = (-1)^5 = -1$.

2.2 Le groupe alterné

Définition :

On dit qu'une permutation $\sigma \in S(E)$ est paire [*resp.* impaire] si $\epsilon(\sigma) = 1$ [*resp.* $\epsilon(\sigma) = -1$].

Exemple :
Les cycles de longueur paire [*resp.* impaire] sont impaires [*resp.* paires].

Définition :
Le groupe alterné est le sous-ensemble de S (E) formé des permutations paires. On le note A(E).
Pour $E = \{1, 2, ..., n\}$, on noteA_n le groupe alterné.

Remarque :
A_n est un sous-groupe distingué de S_n puisque c'est le noyau du morphisme ϵ.

Proposition
1- A_n est un sous-groupe normal propre de S_n, d'ordre $\frac{n!}{2}$.
2- A_3 est abélien.
3- Pour $n \geq 3$, A_n n'est pas abélien.

Démonstration :
1- Puisque A_n est le noyau d'un homomorphisme partant de S_n, A_n est un sous-groupe normal de S_n. Puisque la signature d'une transposition est -1 et la signature d'un 3-cycle est 1, A_n est un sous-groupe normal propre de S_n.
D'après le premier théorème d'isomorphisme, S_n/A_n est isomorphe à $Im(\epsilon)$ Mais ϵ est un homomorphisme surjectif d'après la remarque donc $Im(\epsilon) = \{1, -1\}$. D'où, $|S_n/A_n| = \frac{|S_n|}{|An|} = 2$ et donc $|A_n| = \frac{n!}{2}$.
2- A_3 étant d'ordre 3, A_3 est isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et est donc abélien.
3- On a (1 2 3)(1 2 4) = (1 3)(2 4) et (1 2 4)(1 2 3) = (1 4)(2 3) donc A_n n'est pas abélien.

Exercice :
Donner la liste de tous les éléments de A_4 en précisant leur ordre.

Solution :
On note τ_{ij} la transposition (i, j) dans S_4 pour $1 \leq i \neq j \leq 4$. On a dans le groupe A_4 les 12 éléments distincts suivants :
- l'identité ;
- les 3 éléments d'ordre 2 : $\tau_{12} \circ \tau_{34}$, $\tau_{13} \circ \tau_{24}$, $\tau_{23} \circ \tau_{14}$ (le produit de deux transpositions de supports disjoints est d'ordre 2 puisque ces transpositions commutent).
- les 8 éléments d'ordre 3 : (2, 3, 4), (2, 4, 3), (1, 3, 4), (1, 4, 3), (1, 2, 4), (1, 4, 2), (1, 2, 3), (1, 3, 2) (un 3-cycle fixe un élément de $\{1, 2, 3, 4\}$ et il y en a deux qui fixent k, pour k= 1, 2, 3, 4).

et on a ainsi tous les éléments puisque A_4 est de cardinal $\frac{4!}{2} = 12$.

Exercice :
1- Soient G un groupe d'ordre $2n$ et H un sous-groupe de G d'ordre n (donc

d'indice 2).
Montrer que :

$$\forall g \in G, g^2 \in H$$

2- Montrer que A_4 (qui est d'ordre 12) n'a pas de sous-groupe d'ordre 6.

Solution :

1- Soit $g \in G$. Si $g \in H$, on a alors $g^2 \in H$ puisque H est un groupe.

Si $g \notin H$, on a alors $gH \neq H$ et $G/H = \{H, gH\}$, ce qui nous donne la partition $G = H \cap gH$.

Si $g^2 \notin H$, il est alors dans gH et s'écrit $g^2 = gk$ avec $k \in H$, ce qui entraîne $g = k \in H$ qui est en contradiction avec $g \notin H$.

2- Si H est un sous-groupe de A_4 d'ordre 6, on a alors $\sigma^2 \in H$ pour tout $\sigma \in A_4$.

Si $\sigma \in A_n$ est un 3-cycle, il est alors d'ordre 3 et $\sigma^4 = \sigma$, c'est-à-dire que $\sigma = \gamma^2$ avec $\gamma = \sigma^2 = \sigma^{-1} \in A_n$.
Donc H va contenir tous les 3-cycles, soit 8 éléments, ce qui n'est pas possible.

Exercice :

Le groupe $S(E)$ est-il isomorphe au produit direct $A(E) \times \{-1, 1\}$?

Solution :

Pour $n = 2$, on a $S(E) \cong \{-1, 1\}$ et $A(E) = \{Id_E\}$, donc $S(E)$ est isomorphe au produit direct $A(E) \times \{-1, 1\}$.

Pour $n = 3$, $A(E)$ est d'ordre 3, donc cyclique et $A(E) \times \{-1, 1\}$ qui est commutatif ne peut être isomorphe a $S(E)$.

Pour $n \geq 4$, $\gamma = (Id, -1)$ est dans le centre de $A(E) \times .1, 1$, il est d'ordre 2, donc si φ est un isomorphisme de $A(E) \times \{-1, 1\}$ sur $S(E)$, l'élément $\varphi(\gamma)$ serait d'ordre 2 dans le centre de $S(E)$, ce qui contredit le fait que $Z(S(E)) = \{Id\}$. Donc $S(E)$ n'est pas isomorphe au produit direct $A(E) \times \{-1, 1\}$.

2.3 Générateurs de A(E)

Pour $n = 2$, on a $A(E) = \{Id_E\}$.

Dans ce qui suit, on suppose que $n \geq 3$.

Lemme :

Le produit de deux transpositions est un produit de 3-cycles. Précisément, pour x, y, z, t deux à distincts dans E, on a :

$$(x, y)(x, z) = (x, z, y) \, et \, (x, y)(z, t) = (x, y, z)(y, z, t).$$

Démonstration :

Soient τ_1 et τ_2 deux transpositions. Si $\tau_1 = \tau_2$, on a alors $\tau_1\tau_2 = \tau_1^2 = Id_E = \gamma_3$ pour n'importe quel 3-cycle.

Si $\tau_1 \neq \tau_2$, on a alors deux possibilités. Soit $Supp(\tau_1) \cap Supp(\tau_2) = \{x\}$, donc $tau_1 = (x, y)$, $\tau_2 = (x, z)$ avec x, y, z distincts et :

$$\tau_1\tau_2 = (y, x)(x, z) = (y, x, z) = (x, z, y)$$

soit $Supp(\tau_1) \cap Supp(\tau_2) = \emptyset$, donc $\tau_1 = (x, y)$, $\tau_2 = (z, t)$ avec x, y, z, t distincts et :

$$\tau_1\tau_2 = (x, y)(z, t) = (x, y)(y, z)(y, z)(z, t) = (x, y, z)(y, z, t).$$

proposition :
Pour $n \geq 3$ A_n est engendré par les 3-cycles.

Démonstration :
Comme S_n est engendré par les transpositions, on déduit qu'une permutation paire est le produit d'un nombre pair de transpositions et le lemme qui précède nous dit que ce produit s'écrit comme produit de 3-cycles.

Exercice :
Décomposer en produit de 3-cycles dans A_7 la permutation :

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

Solution :
On a la décomposition en produit de transpositions :

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

donc $\epsilon(\sigma) = 1$ et $\sigma \in A_7$. Puis :

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

Exercice :
Montrer que A(E) est stable par tout automorphisme de S (E).

Solution :
Si φ est un automorphisme de S (E), alors pour tout 3-cycle $\sigma \in A(E)$, $\varphi(\sigma)$ est d'ordre 3 dans S (E). Comme $\varphi(\sigma)$ est produit de cycles et l'ordre de $\varphi(\sigma)$ est le ppcm des longueurs de ces cycles, ils sont nécessairement tous d'ordre 3 et $\varphi(\sigma) \in A(E)$.
En fait, de manière plus générale si E, F sont deux ensembles de même cardinal et φ une bijection de E sur F, on lui associe naturellement l'application $\Phi : \sigma \in S(E) \longrightarrow \varphi \circ \sigma \circ \varphi^{-1}$ qui réalise un isomorphisme de groupes de S (E) sur S (F). Le raisonnement fait avec l'exercice précédent nous montrer que la restriction de Φ à A(E) réalise un isomorphisme de groupes de A(E) sur A(F).

Exercice :
Montrer que, pour $n \geq 3$, A_n est engendré par les 3-cycles $\gamma = (1, 2, k)$ où $3 \leq k \leq n$ (en particulier A_4 est *di*-cyclique engendre par (1, 2, 3) et (1, 2, 4)).

Solution :

Il suffit de montrer que tout 3-cycle peut s'écrire comme produit de cycles du type (1, 2, k) . Pouri, j, k distincts de 1, 2, on a :

$$(i, j, k) = (1, 2, i)(2, j, k)(1, 2, i)^{-1}$$

et :

$$(2, j, k) = (1, 2, j)(1, 2, k)(1, 2, j)^{-1}$$

On peut aussi procéder par récurrence. Pour n = 3, c'est vrai ($A_3 = \langle(1, 2, 3)\rangle$). Supposons le résultat acquis pour $n \geq 3$ et soit $\sigma \in A_{n+1}$. Si $\sigma(n+1) = n+1$, alors la restriction de σ à $\{1, ..., n\}$ est dans A_n, donc elle s'écrit comme produit de γ_k avec $3 \leq k \leq n$ et il en est de même de σ. Sinon, $\sigma(n+1) = j \leq n$ et avec

$$(\gamma_{n+1}^{-1} \circ \gamma_j \circ \sigma)(n+1) = (\gamma_{n+1}^{-1} \circ \gamma_j)(j) = (\gamma_{n+1}^{-1})(1) = n+1$$

on déduit $\sigma' = \gamma_{n+1}^{-1} \circ \gamma_j \circ \sigma \in A_{n+1}$ est produit de γ_k avec $3 \leq k \leq n$ et $\sigma = \gamma_j^{-1} \circ \gamma_{n+1} \circ \sigma' = \gamma_j^2 \circ \gamma_{n+1} \circ \sigma'$ est produit de γ_k avec $3 \leq k \leq n+1$.

Exercice :

Montrer que, pour $n \geq 3$, A_n est engendré par les 3-cycles (k, k + 1, k + 2) où $1 \leq k \leq n-2$.

Solution :

Comme A_n est engendré par les 3-cycles $\gamma_k = (1, 2, k)$ où $3 \leq k \leq n$, il suffit d'écrire chaque γ_k comme produit 3-cycles du type (j, j + 1, j + 2) et $(i, i+1, i+2)^{-1} = (i+2, i+1, i)$ ou $1 \leq i,\ j \leq n-2$.

Pour $4 \leq k \leq n$, on a :

$$(1, 2, k) = (k-1, k, k+1)(1, 2, k-1)(k-1, k, k+1)^{-1}$$

Pour $k = 4$, on a $(1, 2, k-1) = (1, 2, 3)$ et c'est terminé, sinon on écrit $(1, 2, k-1) = (k-2, k-1, k)(1, 2, k-2)(k-2, k-1, k)^{-1}$ et on continue ainsi de suite si nécessaire.

Pour $k = 3$, le cycle (1, 2, 3) est de la forme souhaitée.

2.4 Classes de conjugaison

Le lemme des classes de conjugaison dans S_n reste valable dans A_n, Cependant le corollaire tombe en défaut car les permutations construites pour rendre conjugués deux $k_1 \times ... \times k_r - cycles$, n'appartiennent pas forcément à A_n.

Par exemple, la classe de conjugaison de (1 2 3) dans A_4 est $\{(1\ 2\ 3), (1\ 3\ 4), (1\ 4\ 2), (2\ 4\ 3)\}$ qui n'est pas l'ensemble des 3-cycles.

Les 3-cycles manquants forment la classe de conjugaison de (1 3 2).

Toutefois, on a le résultat suivant qui nous sera utile dans la section suivante :

Proposition :

Si $n \geq 5$ alors la classe de conjugaison d'un 3-cycle est l'ensemble des 3-cycles.

Démonstration :

Soit $\sigma = (i_1\ i_2\ i_3)$ un 3-cycle.

D'après ce qui procède, les conjugués de σ sont des trois cycles. Soit $\varphi = (j_1\ j_2\ j_3)$ un autre 3-cycle.

On définit α par $\alpha(i_s) = j_s$ pour tout i compris entre 1 et 3 et α bijective de $\{1, ..., n\}\backslash\{i_1, i_2, i_3\}$ vers $\{1, ..., n\}\backslash\{j_1, j_2, j_3\}$ (ce qui est possible car ces deux derniers ensembles ont le même cardinal). On vérifie que α appartient à S_n et $\alpha\sigma\alpha^{-1} = \varphi$.

Si α appartient à A_n alors σ et φ sont conjugués dans A_n.

Sinon, soit s et t deux éléments distincts de $\{1, ..., n\}\backslash\{j_1, j_2, j_3\}$ (possible car $n \geq 5$).

Posons $\tau = (s\ t)$. (D'après le lemme et le corollaire, $\tau\alpha$ appartient à A_n. Puisque φ et τ ont leurs supports disjoints, φ et τ commutent. donc $\tau\varphi\tau^{-1} = \varphi$. D'où, $\varphi = (\tau\alpha)\sigma(\tau\alpha)^{-1}$ et σ et φ sont conjugués dans A_n.

La classe de conjugaison de σ dans A_n est l'ensemble des 3-cycles.

Exercice :

Montrer que, pour $n \geq 4$, les produits de deux transpositions disjointes sont conjugués dans $A(E)$.

Solution :

Soient $\sigma = (x_1, x_2)(x_3, x_4)$ et $\sigma' = (x'_1, x'_2)(x'_3, x'_4)$ deux produits de deux transpositions disjointes. En désignant par τ une permutation dans S (E) telle que $\tau(x_k) = x'_k$ pour $1 \leq k \leq 4$, on a :

$$\begin{aligned}\tau\sigma\tau^{-1} &= \tau(x_1, x_2)\tau^{-1}\tau(x_3, x_4)\tau^{-1} = (\tau(x_1), \tau(x_2))(\tau(x_3), \tau(x_4)) \\ &= (x'_1, x'_2)(x'_4, x'_3) = \sigma'\end{aligned}$$

(ce qui prouve que σ et σ' sont conjuguées dans S (E)). Si $\tau_i n A(E)$ c'est terminé, sinon $\gamma = (x'_3, x'_4)\tau$ est dans $A(E)$ et :

$$\begin{aligned}\gamma\sigma\gamma^{-1} &= (\gamma(x_1), \gamma(x_2))(\gamma(x_3), \gamma(x_4)) \\ &= (x'_1, x'_2)(x'_4, x'_3) = \sigma'.\end{aligned}$$

Exercice :

1. Montrer que, pour $n \geq 5$, deux 3-cycles sont conjugués dans $A(E)$.
2. Vérifier que ce résultat n'est pas vrai pour A_4.
3. En déduire que, pour $n \geq 5$, le groupe dérivé $D(A(E))$ de $A(E)$ (i.e. le groupe engendré par les commutateurs $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1}$où σ et τ sont dans $A(E)$) est $A(E)$.

Solution :

1. On sait déjà que deux 3-cycles sont conjugués dans $S(E)$.

Soient $\gamma = (x_1, x_2, x_3)$ et $\gamma' = (x'_1, x'_2, x'_3)$ deux 3-cycles. On se donne une permutation $\sigma \in S(E)$ telle que $\sigma(x_k) = x'_k$ pour $k = 1, 2, 3$ et on a alors $\gamma' = \sigma\gamma\sigma^{-1}$. Si $\sigma \in A(E)$, c'est terminé, sinon en prenant x_4, x_5 dans $E\backslash\{x_1, x_2, x_3\}$ (E a au moins 5 éléments), la permutation $\sigma' = (x_4, x_5)\sigma$ est dans $A(E)$ avec $\sigma'(x_k) = x'_k$ pour $k = 1, 2, 3$ et on est ramené au cas précédent.

2. Ce résultat n'est pas valable pour $n = 4$. Si $\gamma = (1, 2, 3)$ et $\gamma' = (2, 3, 4)$ sont

conjugués dans A_4, il existe $\sigma \in A_4$ telle que $(2,3,4) = \sigma\gamma\sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3))$ et on a nécessairement $\sigma(4) = 1$. On parcourant la liste des éléments de A_4, on voit que $\sigma = \tau_{23} \circ \tau_{14}$, ou $\sigma = (1,3,4)$, ou $\sigma = (1,2,4)$ et $\sigma\gamma\sigma^{-1} = (4,3,2) \neq \gamma'$, ou $\sigma\gamma\sigma^{-1} = (3,2,4) \neq \gamma'$, ou $\sigma\gamma\sigma^{-1} = (2,4,3) \neq \gamma'$. Les cycles γ et γ' ne sont pas conjugues dans A_4.

3. Comme $A(E)$ est engendré par les 3-cycles, il suffit de montrer que tout 3-cycle est dans $D(A(E))$. Si γ est un 3-cycle, il en est de même de $\gamma^{-1} = \gamma^2$, donc γ^2 est conjugué à γ dans $A(E)$, c'est-à-dire qu'il existe $\sigma \in A(E)$ tel que $\gamma^2 = \sigma^{-1}\gamma\sigma$ et $\gamma = \gamma^{-1}\sigma^{-1}\gamma\sigma \in D(A(E))$.

2.5 Simplicité

Proposition :

A_3 est un groupe simple.

Démonstration :

A_3 est d'ordre 3 donc A_3 est isomorphe au groupe simple $\mathbb{Z}/3\mathbb{Z}$.

Théorème de Lagrange :

Pour un groupe G fini et pour tout sous-groupe H de G, le cardinal(ou l'ordre) de H divise le cardinal de G.

Corollaire :

Les sous-groupes normaux de S_3 sont $\{Id\}$, A_3 et S_3.

Démonstration :

Soit N un sous-groupe normal de S_3. D'après le Théorème de Lagrange, N est d'ordre 1, 3 ou 6.

Si N est d'ordre 1 alors $N = \{Id\}$ et si N est d'ordre 6 alors $N = S_3$.

Supposons N d'ordre 3.

Si N contient une transposition alors N contient toutes les transpositions D'où, $N = S_3$ Contradiction.

D'où, N est constitué par l'identité et les 3-cycles c'est à dire $N = A_3$

Proposition :

L'ensemble formé de l'identité et des $2 \times 2 - cycles$ est un sous-groupe normal abélien de A_4, d'ordre 4.

Démonstration :

Pour la structure de sous-groupe abélien, la vérification est immédiate à partir des éléments (1 2)(3 4), (1 3)(2 4) et (1 4)(2 3).

Définition :

Le groupe défini dans la Proposition précédente est noté V_2.

Proposition :

Les sous-groupes normaux de A_4 sont $\{Id\}$, V_2 et A_4.

Démonstration :

Soit N un sous-groupe normal de A_4 non réduit à $\{d\}$.

On vérifie facilement qu'il y a 8 3-cycles dans A_4.

D'où, puisque l'ordre de N doit diviser l'ordre de $A_4 = 12$ d'après le Théorème de Lagrange, N contient au moins un $2 \times 2 - cycle$. Les conjugués (dans A_n) de (1 2)(3 4) sont des $2 \times 2 - cycles$. Comme (1 2 3)(1 2)(3 4)(1 3 2)=(1 4)(2 3) et (2 3 4)(1 2)(3 4)(2 4 3)=(1 3)(2 4), la classe de conjugaison d'un $2 \times 2 - cycle$ est l'ensemble des $2 \times 2 - cycles$.

D'où, N contient l'ensemble des $2 \times 2 - cycles$.

Si N n'a pas d'autre élément que les $2 \times 2 - cycles$ et l'identité alors $N = V_2$.

Sinon, N contient un 3-cycle $(i\ j\ k)$.

Soit s l'entier compris entre 1 et 4, différent de i, j et k.

On a $(i\ j\ s)(i\ j\ k)(i\ s\ j) = (j\ s\ k)$ et $(i\ s\ j)(i\ j\ k)(i\ j\ s) = (i\ k\ s)$ donc N contient au moins 3 3-cycles. D'où, puisque N possède 3 $2 \times 2 - cycles$ et l'identité, N a un ordre au moins égal à 7. La seule possibilité est $|N| = 24$ c'est à dire $N = A_4$.

Corollaire :

Les sous-groupes normaux de S_4 sont $\{Id\}$, V_2, A_4 et S_4.

Démonstration :

Soit N un sous-groupe normal de S_4 non réduit à $\{Id\}$.

Si N contient une transposition alors $N = S_4$.

Si N contient un 3-cycle alors A_n est inclus dans S_n.

Mais $|N|$ divise $|G|$ par le Théorème de Lagrange donc $|N| \leq \frac{|S_n|}{2} = |A_n|$. D'où, $N = A_n$.

Supposons que N ne contient aucune transposition et aucun 3-cycle.

Si N contient un $2 \times 2 - cycle$ alors N contient tous les $2 \times 2 - cycles$ et V_2 est donc inclus dans N.

Si N contient un 4-cycle alors N contient tous les 4-cycles.

Dans S_4, il y a 6 4-cycles donc si N n'est constitué que de l'identité et des 4-cycles, N est d'ordre 7 ce qui contredit le Théorème de Lagrange.

D'où, N contient un $2 \times 2 - cycle$ et donc N contient V_2.

On a alors N d'ordre 10 ce qui contredit encore le Théorème de Lagrange.

D'où, les sous-groupes normaux de S_4 sont $\{Id\}$, V_2, A_4 et S_4.

Le résultat le plus important de cette section est le suivant :

Théorème :

Pour $n \geq 5$, les sous-groupes distingués de $S(E)$ sont $\{Id\}$, $A(E)$ et $S(E)$.

Démonstration :

Soit H un sous-groupe distingué non trivial de $S(E)$ (i.e. distinct de $\{Id\}$ et de $S(E)$).

Pour montrer que $H = A(E)$, il suffit de montrer que H contient un 3-cycle(il les contient alors tous puisqu'ils sont conjugués dans $S(E)$, donc $A(E) \subset H$ et $H = A(E)$ puisque les 3-cycles engendrent $A(E)$ et $H \neq S(E)$: en effet, on a $A(E) \subset H \subset S(E)$, donc $card(H) = p\frac{n!}{2} = p\frac{q\ card(H)}{2}$et $pq = 2$, soit $p = 1$ et $H = A(E)$ ou $p = 2$ et $H = S(E)$).

On se donne $\sigma \in H \backslash \{Id\}$ et $\tau = (x, y)$ une transposition qui ne commute pas

à τ.
Comme H est distingué dans S (E), on a

$$\sigma' = \tau\sigma\tau\sigma^{-1} = (\tau\sigma\tau^{-1})\sigma^{-1} \in H$$

et en écrivant que :

$$\sigma' = (x, y)(\sigma(x, y)\sigma^{-1}) = (x, y)(\sigma(x), \sigma(y))$$

on voit que σ' est produit de deux transpositions.

L'égalité $\sigma' = Id$ est réalisée si, et seulement si, $\tau\sigma\tau\sigma^{-1} = Id$, soit $\tau\sigma = \sigma\tau^{-1} = \sigma\tau$, ce qui n'est pas.

Si $\{x, y\} \cap \{\sigma(x), \sigma(y)\}$ est réduit a un point, alors σ' est un 3-cycle et dans ce cas $H = A(E)$, sinon cette intersection est vide et en prenant z dans $E \backslash \{x, y, \sigma(x), \sigma(y)\}$ (on a $n \geq 5$), le groupe H contient $(x, y)(\sigma(x), z)$ puisque le produit de deux transpositions de supports disjoints sont conjugués dans $S(E)$ et H est distingué. Il en résulte que H contient

$$(x, y)(\sigma(x), \sigma(y))(x, y)(\sigma(x), z) = (\sigma(x), \sigma(y))(\sigma(x), z)$$

qui est le 3-cycle $(\sigma(y), \sigma(x), z)$.

Exercice :

On se propose de montrer que, pour n = 5, $A(E)$ est simple (i.e. n'a pas de sous-groupes distingués autres que lui même et $\{Id\}$). Ici E est un ensemble à 5 éléments.

1. Donner une description de $A(E)$ en classant ses élément en fonction de leur ordre.
2. Montrer que $A(E)$ est simple.

Solution :

1. Pour n = 5, notons $E = \{x_1, x_2, x_3, x_4, x_5\}$ et pour $1 \leq i \neq j \leq 5$, τ_{ij} la transposition (x_i, x_j) dans $S(E)$. On décrit d'abord le groupe A(E). Dans ce groupe, on a les 60 éléments distincts suivants :
- l'identité ;
- $\frac{C_5^2 C_3^2}{2} = 15$ éléments d'ordre 2 donnes par le produit de deux transpositions de supports disjoints : $\tau_{12} \circ \tau_{34}$, $\tau_{12} \circ \tau_{35}$, $\tau_{12} \circ \tau_{45}$, ... (deux transpositions de supports disjoints commutent et leur produit est d'ordre 2) ;
- $2C_5^2 = 20$ cycles d'ordre 3 distincts (un même support à 3 éléments donne 2 cycles) ;
- $4! = 24$ cycles d'ordre 5 : $(x_1, x_2, x_3, x_4, x_5)$, $(x_1, x_3, x_4, x_5, x_2)$, ... (si $\gamma^5 = 1$, alors $\gamma^{-1} = \gamma^4 \in A(E)$ et $\gamma \in A(E)$)

et on a ainsi tous les éléments puisque A(E) est de cardinal $\frac{5!}{2} = 60$.

2. Soit H un sous-groupe distingué de $A(E)$ non réduit à $\{Id\}$.

Si H contient un 3-cycle, il les contient alors tous puisqu'ils sont conjugués et $H = A(E)$ puisque les 3-cycles engendrent A(E).

Si H contient un produit $\sigma = (x, y)(z, t)$ de deux transpositions de supports disjoints, il contient alors, pour $u \in E \backslash \{x, y, z, t\}$, le commutateur :

$$\begin{aligned}\sigma(x, y, u)\sigma^{-1}(x, y, u)^{-1} &= (\sigma(x), \sigma(y), \sigma(u))(u, y, x) \\ &= (y, x, u)(u, y, x) = (x, y, u)\end{aligned}$$

($\sigma \in H$, donc $\sigma^{-1} \in H$ puisque H est un groupe et $(x,y,u)\sigma^{-1}(x,y,u)^{-1} \in H$ puisque H est distingué) qui est un 3-cycle, donc $H = A(E)$.
Si H contient un 5-cycle $\sigma = (x,y,z,t,u)$, il contient alors le commutateur :

$$\begin{aligned}(x,y,z)\sigma(x,y,z)^{-1}\sigma^{-1} &= (x,y,z)\sigma(z,y,x)^{-1}\sigma^{-1} = (x,y,z)(\sigma(z),\sigma(y),\sigma(x)) \\ &= (x,y,z)(t,z,y) = (y,t,x)\end{aligned}$$

qui est un 3-cycle, donc $H = A(E)$.
Plus généralement, on a le résultat suivant.

Théorème :
Pour $n = 3$ ou $n \geq 5$ le groupe A_n est simple (i.e. n'a pas de sous-groupes distingués autres que lui même et $\{Id\}$).

Démonstration :
Pour n = 3, A_n est cyclique d'ordre 3 et n'a pas de sous-groupe trivial.
On suppose $n \geq 5$ et on se donne un sous-groupe distingué H de A_n distinct de $\{Id\}$.
Pour montrer que $H = A_n$, il suffit de montrer que H contient un 3-cycle puisqu'ils sont tous conjugués dans A_n et l'engendrent.
On se donne $\sigma \in H \backslash \{Id\}$ et $\gamma = (x,z,y) \in A_n$ un 3-cycle avec $y = \sigma(x)$ qui ne commute pas à σ. Comme H est distingué dans A_n, on a :

$$\sigma' = \sigma\gamma\sigma^{-1}\gamma^{-1} = \sigma(\gamma\sigma^{-1}\gamma^{-1} \in H$$

et en écrivant que :

$$\begin{aligned}\sigma' &= (\sigma(x,z,y)\sigma^{-1})(y,z,x) = (\sigma(x),\sigma(z),\sigma(y))(y,z,x) \\ &= (y,\sigma(z),\sigma(y))(y,z,x)\end{aligned}$$

on voit que σ' est produit de deux 3-cycles qui agissent sur l'ensemble $F = \{x,y,z,\sigma(y),\sigma(z)\}$ formé d'au plus 5 éléments (tous les points de E/F sont fixes).
L'égalité $\sigma' = Id$ est réalisée si, et seulement si, $\sigma\gamma\sigma^{-1}\gamma^{-1} = Id$, soit $\tau\sigma = \gamma\sigma$, ce qui n'est pas, donc $\sigma' \neq Id$.
Dans $S(F)$ la permutation σ' s'écrit comme produit de cycles de supports disjoints, cette décomposition étant celle de $S(E)$ et comme $\sigma' \in A(E)$, il n'y a que trois possibilités : σ' est soit un 3-cycle, soit un produit de deux transpositions de supports disjoints, soit un 5-cycle.
Dans le premier cas c'est termine.
Dans le deuxième cas, on a $\sigma' = (x_1,x_2)(x_3,x_4)$ et choisissant $x_5 \in E \backslash \{x_1,x_2,x_3,x_4\}$, on a :

$$\sigma'' = (x_1,x_5)\sigma'(x_1,x_5)(\sigma')^{-1} = ((x_1,x_5)\sigma(x_1,x_5)^{-1})(\sigma')^{-1} \in H$$

avec :

$$\sigma'' = (x_1,x_5)(\sigma'(x_1),\sigma'(x_5)) = (x_1,x_5)(x_2,x_5) = (x_1,x_5,x_2)$$

et c'est terminé.
Dans le troisième cas, on a $\sigma' = (x_1, x_2, x_3, x_4, x_5)$ et :

$$\sigma'' = (x_1, x_2)\sigma'(x_1, x_2)(\sigma')^{-1} = ((x_1, x_2)\sigma(x_1, x_2)^{-1})(\sigma')^{-1} \in H$$

avec :

$$\sigma'' = (x_1, x_2)(\sigma'(x_1), \sigma'(x_2)) = (x_1, x_2)(x_2, x_3) = (x_1, x_2, x_3)$$

et c'est terminé.

2.6 Centres

Proposition :
1) $Z(A_3) = A_3$ et $Z(S_3) = \{Id\}$.
2) $Z(A_4) = \{Id\}$ et $Z(S_4) = \{Id\}$.
3) Pour $n \geq 5$, $Z(A_n) = \{Id\}$ et $Z(S_n) = \{Id\}$.

Démonstration :
$Z(A_n)$ est un sous-groupe normal de A_n et $Z(S_n)$ est un sous-groupe normal de S_n.
1)A_3 est abélien donc $Z(A_3) = S_3$.
D'après ce qui précède, $Z(S_3) = \{Id\}$, A_3 ou S_3.
S_3 n'est pas abélien donc $Z(S_3) \neq \{S_3\}$.
On a (1 2)(1 2 3)(1 2) = (1 3 2) donc (1 2 3) n'appartient pas à $Z(S_3)$ et par conséquent, A_3 n'est pas inclus dans $Z(S_3)$. D'où, $Z(S_3) = \{Id\}$ A_3 n'est pas inclus dans $Z(S_3)$. D'où, $Z(S_3) = \{Id\}$.
2) On a $Z(A_4) = \{Id\}$, V_2 ou A_4 et $Z(S_4) = \{Id\}$, V_2, A_4 ou S_4.
A_4 et S_4 n'étant pas abéliens, $Z(A_4) \neq A_4$ et $Z(S_4) \neq S_4$.
On a (1 2 3)(1 2)(3 4)(1 3 2) = (2 3)(1 4) donc (1 2)(3 4) n'appartient ni à A_4 ni à S_4. D'où, V_2 n'est inclus ni dans $Z(A_4)$ ni dans $Z(S_4)$.
Par conséquent, $Z(A_4) = \{Id\}$ et $Z(S_4) = \{Id\}$.
3)On a, $Z(A_n) = \{Id\}$ ou A_4 et $Z(S_n) = \{Id\}$, A_n ou S_n.
A_n n'est pas abélien donc $Z(A_n) \neq A_n$ et par conséquent, $Z(A_n) = \{Id\}$.
S_n n'est pas abélien donc $Z(S_n) \neq S_n$.
On a (1 2 4)(1 2 3)(1 4 2) = (2 4 3) donc (1 2 3) n'appartient pas à $Z(S_n)$.
D'où, A_n n'est pas inclus dans $Z(S_n)$ et donc $Z(S_n) = \{Id\}$.

Exercice :
Déterminer, pour $n \geq 4$, le centre $Z(A(E))$ de $A(E)$ (c'est-à-dire l'ensemble des éléments de $A(E)$ qui commutent à tous les autres éléments de $A(E)$).

Solution :
Si $\sigma \in A(E) \backslash \{Id\}$, il existe $x \in E$ tel que $y = \sigma(x) \neq x$.
On se donne $z \in E \backslash \{x, y, \sigma(y)\}$ (E a au moins 4 éléments) et γ est le 3-cycle $\gamma = (x, y, z) \in A(E)$. On a alors :$\sigma\gamma(x) = \sigma(y)$ et $\gamma\sigma(x) = \gamma(y) = z \neq \sigma(y)$ donc $\sigma\gamma \neq \gamma\sigma$ et $\sigma \notin Z(A(E))$. Le centre de A(E) est donc réduit à $\{Id\}$.
Pour $n = 3$, $A(E)$ est cyclique, donc commutatif et $Z(A(E)) = A(E)$.

Chapitre 3

Applications

3.1 Formes multilinéaires

$\mathbb{K}$ est un corps commutatif de caractéristique différente de 2 et E un $\mathbb{K}$-espace vectoriel de dimension $n \geq 2$.

Définition :
Une application φ k-fois multilinéaire de E^k dans F est dite symétrique si pour toute permutation τ des entiers $\{1,...,k\}$ *i.e.* $\tau \in S_k$, et pour tout $\{h_1,...,h_k\} \in E^k$ on a

$$\varphi(h_{\tau(1)},...,h_{\tau(k)} = \varphi(h_1,...,h_k)$$

On dit qu'une forme n-linéaire φ sur E est alternée si $\varphi(x_1,...,x_n) = 0$ pour toute liste $(x_1,...,x_n)$ de vecteurs non tous distincts (i.e. il existe $i \neq j$ tels que $x_i = x_j$).

Théorème :
Une forme n-linéaire φ sur E est alternée (ou antisymétrique) si, et seulement si, $\varphi(x_{\sigma(1)},...,x_\sigma(n)) = \epsilon(\sigma)\varphi(x_1,...,x_n)$ pour tout $(x_1,...,x_n) \in E^n$ et toute permutation $\sigma \in S_n$.

Démonstration :
Il suffit de montrer que $\varphi(x_{\tau(1)},...,x\tau(n)) = -\varphi(x_1,...,x_n)$ pour toute transposition τ, puisque S_n est engendre par les transpositions.
Supposons φ alternée et soit $\tau = (j,k)$ une transposition avec $1 \leq j < k \leq n$. En écrivant que :

$$\begin{aligned}
0 &= \varphi(x_1,...,x_j + x_k,...,x_j + x_k,...,x_n) \\
&= \varphi(x_1,...,x_j,...,x_j,...,x_n) + \varphi(x_1,...,x_n) \\
&+ \varphi(x_{\tau(1)},...,x_{\tau(n)}) + \varphi(x_1,...,x_k,...,x_k,...,x_n) \\
&= \varphi(x_1,...,x_n) + \varphi(x_{\tau(1)},...,x_{\tau(n)})
\end{aligned}$$

on déduit que $\varphi(x_{\tau(1)},...,x_{\tau(n)}) = -\varphi(x_1,...,x_n)$.
Réciproquement, supposons cette condition vérifiée.

Si $x_j = x_k$ pour $1 \leq j < k \leq n$, on a alors, pour $\tau = (j,k)$:

$$\varphi(x_1, ..., x_n) = \varphi(x_{\tau(1)}, ..., x_{\tau(n)}) = -\varphi(x_1, ..., x_n)$$

et $\varphi(x_1, ..., x_n) = 0$ pour $\mathbb{K}$ de caractéristique différente de 2.

Exemple :
- Soient $E = K$, $F = K$ et $n \in \mathbb{N}^*$.
L'application $\varphi : K^n \longrightarrow K$ définie par $\varphi(x_1, \ldots, x_n) = x_1 \ldots x_n$ est une forme n linéaire symétrique.
En effet par commutativité de la multiplication, on vérifie $x_{\sigma(1)} \ldots x_{\sigma(n)} = x_1 \ldots x_n$ pour tout $\sigma \in S_n$.
- Le produit scalaire du plan ou de l'espace est une forme bilinéaire symétrique. En effet, pour tout $\sigma \in S_2 = \{Id, \tau\}$ avec $\tau = (1,2)$, on a
Si $\sigma = Id$, $\overrightarrow{u}.\overrightarrow{v} = \overrightarrow{v}.\overrightarrow{u}$.
Si $\sigma = (12)$, $\overrightarrow{v}.\overrightarrow{u} = \overrightarrow{u}.\overrightarrow{v}$.
- Le produit vectoriel dans l'espace est une application bilinéaire antisymétrique. En effet, pour tout $\sigma \in S_2 = \{Id, \tau\}$ avec $\tau = (12)$, on a
Si $\sigma = Id$, $\overrightarrow{u} \wedge \overrightarrow{v} = \epsilon(\sigma)\overrightarrow{u} \wedge \overrightarrow{v}$.
Si $\sigma = (1;2)$, $\overrightarrow{v} \wedge \overrightarrow{u} = -\overrightarrow{u} \wedge \overrightarrow{v} = \epsilon(\sigma)\overrightarrow{u} \wedge \overrightarrow{v}$.

3.2 Déterminant

Théorème :
$B = (e_i)_{1 \leq i \leq n}$ une base de E.
L'espace vectoriel $\wedge^{*n}(E)$ des formes n-linéaires alternées est de dimension 1 engendré par l'application $det : E^n \longleftrightarrow K$ définie par :

$$det(x_1, ..., x_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} x_{\sigma(i),i}$$

où $x_j = \sum_{i=1}^{n} x_{ij} e_i$ pour tout j compris entre 1 et n.

Démonstration :
Vérifions tout d'abord que l'application det est n-linéaire alternée.
En désignant, pour tout j compris entre 1 et n, par :

$$\pi : x = \sum_{i=1}^{n} x_i e_i \longmapsto x_j$$

la j-ème projection, on a :

$$det(x_1, ..., x_n) = \sum_{\sigma \in S_n} \epsilon(\sigma) \prod_{i=1}^{n} \pi_{\sigma(i)}(x_i)$$

Chaque application $\pi_{\sigma(i)}$ étant linéaire, l'application $(x_1, ..., x_n) \longmapsto \prod_{i=1}^{n} \pi_{\sigma(i)}(x_i)$ est n-linéaire et il en est de même de det comme combinaison linéaire d'applications n-linéaires.

Pour tout permutation τ, en effectuant le changement d'indice $k=\tau(i)$, on a :

$$\begin{aligned} det(x_{\tau(1)},...,x_{\tau(n)}) &= \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n}\pi_{\sigma(i)}(x_{\tau(i)}) \\ &= \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{k=1}^{n}\pi_{\sigma(\tau^{-1}(k))}(x_k) \\ &= \sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{k=1}^{n}\pi_{\sigma\circ\tau^{-1}(k)}(x_k) \end{aligned}$$

et en utilisant le fait que l'application $\sigma' \longrightarrow \sigma = \sigma'\circ\tau$ est une bijection de S_n sur lui même, on en déduit que :

$$\begin{aligned} det(x_{\tau(1)},...,x_{\tau(n)}) &= \sum_{\sigma'\in S_n}\epsilon(\sigma'\circ\tau)\prod_{k=1}^{n}\pi_{\sigma'(k)}(x_k) \\ &= \epsilon(\tau)\sum_{\sigma'\in S_n}\epsilon(\sigma')\prod_{k=1}^{n}\pi_{\sigma'(k)}(x_k) \\ &= \epsilon(\tau)det(x_1,...,x_n) \end{aligned}$$

ce qui signifie que det est alternée.
En utilisant le caractère n-linéaire de $\varphi\in\wedge^{*n}(E)$, on a :

$$\begin{aligned} \varphi(x_1,...,x_n) &= \varphi(\sum_{i_1=1}^{n}x_{i_1,1}e_{i_1},...,x_n) = \sum_{i_1=1}^{n}x_{i_1,1}\varphi(e_{i_1},x_2...,x_n) \\ &= \sum_{i_1=1}^{n}\sum_{i_2=1}^{n}x_{i_1,1}x_{i_2,2}\varphi(e_{i_1},e_{i_2},x_3,...,x_n) \\ &= \sum_{i_1=1}^{n}...\sum_{i_n=1}^{n}x_{i_1,1}...x_{i_n,n}\varphi(e_{i_1},...,e_{i_n}) = \sum_{\gamma\in F_n}\prod_{i=1}^{n}x_{\gamma(i),i}\varphi(e_{\gamma(1)},...,e_{\gamma(n)}) \end{aligned}$$

où F_n est l'ensemble des applications de $\{1,...,n\}$ dans $\{1,...,n\}$.
Comme φ est alternée, on a $\varphi(x_{\gamma(1)},...,x_{\gamma(n)})=0$ pour γ non bijective et :

$$\begin{aligned} \varphi(x_1,...,x_n) &= \sum_{\sigma\in S_n}\prod_{i=1}^{n}x_{\sigma(i),i}\varphi(e_{\sigma(1)},...,e_{\sigma(n)}) \\ &= (\sum_{\sigma\in S_n}\epsilon(\sigma)\prod_{i=1}^{n}x_{\sigma(i),i})\varphi(e_1,...,e_n) \end{aligned}$$

et $\varphi=\lambda det$ avec $\lambda=\varphi(e_1,...,e_n)\in\mathbb{K}$ et $det\in\wedge^{*n}(E)\backslash\{0\}$.
Donc$\wedge^{*n}(E)$ est de dimension 1 engendré par det.