Cours d'Algèbre 6

Chapitre 2

Filière SMA

Année 2020-2021

Mme F. ERRAJI, Pr.

16 avril 2021

Table des matières

Chapitre 2

Groupes Symétriques

I Notion de Groupe Symétrique

Soit n un entier strictement positif. Soit X un ensemble fini à n éléments. L'ensemble $S(X)$ des bijections de X sur X muni de la composition des applications est alors un groupe fini. Si Y est un autre ensemble de même cardinal n ; il existe une bijection f de X sur Y et l'on construit de façon évidente un isomorphisme de groupes φ de $S(X)$ sur $S(Y)$ en posant $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$ pour tout $\sigma \in S(X)$. Le groupe $S(X)$ est donc, à un isomorphisme près, indépendant du choix de l'ensemble X et ne dépend donc que de son cardinal.

Notation : On note dans toute la suite $I_n = \{1, 2, \cdots, n\}$ et S_n l'ensemble des bijections de I_n sur lui-même.

Définition I.0.1. *$(S_n, \circ)$ s'appelle le groupe symétrique sur n éléments ou n-ième groupe symétrique.*

Remarques. — *(a) Les éléments de S_n sont appelés les permutations sur n éléments. On choisit de noter une telle permutation en écrivant l'un au dessous de l'autre les éléments de I_n et leurs images, ce qui conduit à l'écriture :*

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

— *(b) On note e_n l'élément neutre de S_n, qui est l'identité sur I_n le composé $\sigma \circ \tau$ de deux permutations de S_n sera désigné par $\sigma \cdot \tau$ ou tout simplement par $\sigma\tau$.*

Exemples : $n = 1 \quad S_1 = \{e_1\}, |S_1| = 1$

$n = 2$, $I_2 = \{1, 2\}$; $e_2 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$; $\tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$; $S_2 = \{e_2, \tau\}$; $\quad |S_2| = 2$, $\tau \circ \tau = e_2$

$n = 3, \quad I_3 = \{1, 2, 3\}$, *les permutations de* S_3 *sont*

$$e_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad ; \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad ; \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad ; \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad ; \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

La table de S_3 *est la suivante :*

$\circ$	e_3	σ_1	σ_2	τ_1	τ_2	τ_3
e_3	e_3	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e_3	τ_3	τ_1	τ_2
σ_2	σ_2	e_3	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e_3	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	e_3	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	e_3

S_3 *est un groupe non commutatif :* $(\sigma_1\tau_1 = \tau_3, \quad \tau_1\sigma_1 = \tau_2, \quad \tau_2 \neq \tau_3)$ *; C'est le plus petit groupe fini non commutatif !*

S_3 *contient trois sous-groupes d'ordre* 2 *:* $\{e_3, \tau_1\}$, $\{e_3, \tau_2\}$ $\{e_3, \tau_3\}$ *et un sous-groupe d'ordre* 3 *:* $\{e_3, \sigma_1, \sigma_2\}$

— *(c) Soit* $n > m$*. L'application :*

$$\begin{array}{rcl} j_{n,m} : S_m & \to & S_n \\ \sigma & \mapsto & \sigma' = \begin{cases} \sigma'(i) = \sigma(i), & \forall i \in I_m \\ \sigma'(i) = i, & \text{sinon.} \end{cases} \end{array}$$

est un homomorphisme injectif dont l'image est le sous-groupe de S_n *formé des permutations laissant fixes* $m+1, m+2, \cdots, n$*. En particulier,* $j_{n,m}(e_m) = e_n$*.*

Donc, on peut considérer, par identification, S_m *comme un sous-groupe de* S_n*.*

Théorème I.1. *Pour* $n \geq 1$*, le groupe symétrique est d'ordre* $n!$*.*

Preuve. Par récurrence sur $n \in \mathbb{N}^*$. L'assertion est vraie pour $n = 1$.

Soit $n \in \mathbb{N}^*$, on suppose l'assertion vraie pour n. Soit I_{n+1}, $k_0 \in I_{n+1}$ et $Y = I_{n+1} \backslash \{k_0\}$. D'après l'hypothèse de récurrence, $|S(Y)| = n!$.

On considère maintenant l'application

$$\begin{array}{rcl} f : S_{n+1} & \to & I_{n+1} \\ \sigma & \mapsto & \sigma(k_0) \end{array}$$

f étant surjective par construction, par ailleurs, si $\sigma, \sigma' \in S_{n+1}$,

$$f(\sigma) = f(\sigma') \Longleftrightarrow \sigma(k_0) = \sigma'(k_0) \Longleftrightarrow \sigma^{-1}\sigma'(k_0) = k_0$$

$\sigma^{-1}\sigma'$ appartient au sous-groupe de S_{n+1} formé des permutations laissant fixe k_0 et qu'on identifie avec $S(Y)$, $(S(Y) \cong S_n)$.

$$f(\sigma) = f(\sigma') \Longleftrightarrow \sigma^{-1}\sigma' \in S(Y)$$

Ainsi, on peut conclure, d'après la factorisation de l'application f, qu'il existe une bijection $\overline{f} : (S_{n+1}/S(Y))_g \quad \to \quad I_{n+1}$, unique, tel que $\overline{f} \circ p = f$.

D'où $card(S_{n+1}/S(Y))_g = card(I_{n+1}) = n+1$, et d'après le théorème de Lagrange,

$$card(S_{n+1}/S(Y))_g = [S_{n+1} : S(Y)] = \frac{|S_{n+1}|}{|S(Y)|}$$

Par conséquent, $|S_{n+1}| = (n+1)|S(Y)| = (n+1)n! = (n+1)!$ □

Théorème I.2. *Pour $n \geq 3$, S_n n'est pas abélien.*

Preuve. On a S_3 n'est pas abélien et d'après la remarque (c), pour tout $n \geq 3$, S_3 est un sous-groupe de S_n, donc S_n n'est pas abélien. □

II Support d'une Permutation

Définition II.0.1. *On appelle support d'une permutation σ de S_n, noté $supp(\sigma)$, l'ensemble $\{k \in I_n \quad / \quad \sigma(k) \neq k\}$.*

Deux permutations σ et σ' de S_n tel que $supp(\sigma) \cap supp(\sigma') = \emptyset$ sont dites disjointes.

Lemme 1. *Pour toute permutation σ non triviale de S_n, la restriction de σ à $supp(\sigma)$ est une permutation de $supp(\sigma)$.*

Preuve. Soit $i \in supp(\sigma)$ et notons $j = \sigma(i)$. Par absurde, supposons que $j \notin supp(\sigma)$, on a alors $\sigma(j) = j$, et par suite $\sigma(i) = \sigma(j)$ donc $i = j$ d'où $\sigma(i) = i$ ce qui est contradictoire avec $i \in supp(\sigma)$. Donc, $supp(\sigma)$ est stable par σ, et par conséquent, la restriction de σ à $supp(\sigma)$ qui est une application injective est donc bijective de $supp(\sigma)$ dans lui-même. □

Proposition II.0.1. *Deux permutations de S_n disjointes commutent.*

Preuve. On suppose $n \geq 2$. Soit $\sigma, \eta \in S_n$ tel que $supp(\sigma) \cap supp(\eta) = \emptyset$. Soit $i \in I_n$. Si $i \notin supp(\sigma) \cup supp(\eta)$ alors $\sigma(i) = i = \eta(i)$, donc, $\sigma\eta(i) = \eta\sigma(i)$.

Supposons maintenant $i \in supp(\sigma)$, on a alors d'une part, $i \notin supp(\eta)$ donc $\eta(i) = i$ et par suite $\sigma\eta(i) = \sigma(i)$. D'autre part, puisque $i \in supp(\sigma)$ d'après le lemme précédent, on a alors $\sigma(i) \in supp(\sigma)$ et par suite $\sigma(i) \notin supp(\eta)$ donc $\eta\sigma(i) = \sigma(i)$. On conclut que $\sigma\eta(i) = \eta\sigma(i)$. D'une façon analogue on montre que si $i \in supp(\eta), \sigma\eta(i) = \eta\sigma(i)$. □

III Décomposition d'une Permutation en Produit de Transpositions

Définition III.0.1. *Soit $n \geq 2$. On appelle transposition toute permutation τ de S_n qui échange deux éléments distincts i et j de I_n en laissant fixes les $n-2$ autres.*

$$\Big(\tau(i) = j, \quad \tau(j) = i \quad et \quad \forall k \in I_n - \{i,j\},\ \tau(k) = k\Big)$$

τ est alors noté (i,j) ou bien τ_{ij}. Il est évident que $\tau_{ij}^2 = e_n$, i.e. $\tau_{ij}^{-1} = \tau_{ij}$.

Théorème III.1. *Pour tout $n \geq 2$, toute permutation de S_n est un produit fini de transpositions. En d'autres termes, le groupe S_n est engendré par ses transpositions.*

Preuve. On raisonne par récurrence sur n. Pour $n = 2$, $S_2 = \{e_2, (1,2)\}$ on a $e_2 = (1,2)^2$. Supposons le résultat vrai pour S_{n-1} où $n \geq 3$. Soit $\sigma \in S_n$. Distinguons deux cas :

1er Cas, $\sigma(n) = n$. Par suite $\sigma' = \sigma/I_{n-1}$, la restriction de σ à I_{n-1} est un élément de S_{n-1}. Donc, par hypothèse de récurrence : $\sigma' = \tau'_1\tau'_2\cdots\tau'_r$ où τ'_k est une transposition de S_{n-1} pour tout $1 \leq k \leq r$. Chaque τ'_k se prolonge en une transposition τ_k de S_n, en posant $\tau_k(i) = \tau'_k(i)$ pour tout $1 \leq i \leq n-1$ et $\tau_k(n) = n$ et on alors $\sigma = \tau_1\tau_2\cdots\tau_r$.

2eme Cas, $\sigma(n) = p < n$. Soit alors $\tau = (p,n)$ et $\sigma_1 = \tau\cdot\sigma$. On a $\sigma_1(n) = n$. En appliquant le 1^{er} cas, σ_1 se décompose en produit fini de transpositions, i.e. $\sigma_1 = \tau_1\tau_2\cdots\tau_r$, par conséquent, $\sigma = \tau\tau_1\tau_2\cdots\tau_r$.

□

Remarque. *Cette décomposition n'est pas unique, par exemple, dans S_4,*

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

IV Décomposition d'une Permutation en Cycles

Définition IV.0.1. *Soit $i_1, i_2, \cdots, i_k$ avec $1 < k \leq n$ des éléments deux à deux distincts de I_n. On désigne par $(i_1, i_2, \cdots, i_k)$ la permutation c de S_n telle que $c(i_l) = i_{l+1}$ $(1 \leq l \leq k-1), c(i_k) = i_1$ et $c(i_s) = i_s$ pour $i_s \notin \{i_1, i_2, \cdots, i_k\}$. Une telle permutation est appelée un cycle. L'entier k est la longueur du cycle, et on écrit c est un $k-$cycle.*

Remarques. — *Un cycle de longueur 2 est une transposition.*

— *$supp(c) = \{i_1, i_2, \cdots, i_k\}$ où c est le k-cycle $(i_1, i_2, \cdots, i_k)$.*

— *La notation* $c = (i_1, i_2, \cdots, i_k)$ *n'est pas unique. En effet, les cycles*

$$(i_1, i_2, \cdots, i_k), (i_2, \cdots, i_k, i_1), \cdots, (i_k, i_1, i_2, \cdots, i_{k-1}) \quad \textit{sont identiques.}$$

Propriétés IV.0.1. *Soit* $c = (i_1, i_2, \cdots, i_k)$ *un* k*-cycle, on a alors :*

— $o(c) = k$. *Car* k *est le plus petit entier strictement positif tel que* $c^k = e_n = Id_{I_n}$.

— $c = (i_1, i_2, \cdots, i_k) = (i_1, i_2)(i_2, i_3)\cdots(i_{k-1}, i_k)$.

— *L'inverse de* c, c^{-1} *est un* k*-cycle :* $c^{-1} = (i_k, i_{k-1})\cdots(i_2, i_1) = (i_k, i_{k-1}, \cdots i_2, i_1)$.

Attention ! *Si* c *est un* $k-$*cycle et si* $2 \leq l \leq k-2$, *alors* c^l *n'est pas nécessairement un cycle. En effet : soit* $c = (1, 2, 3, 4)$ *de* S_4, $c^2 = (1, 3)(2, 4)$ *n'est pas un cycle.*

Proposition IV.0.1. *Tout élément* σ *de* S_n *est un produit de cycles disjoints et cela d'une manière unique, à l'ordre des cycles près.*

Preuve. Soit $n \geq 2$. Soit $\sigma \in S_n$ avec $\sigma \neq Id_{I_n}$. On considère la relation binaire R_σ définie sur I_n par :

$$iR_\sigma j \Longleftrightarrow \exists k \in \mathbb{Z}/j = \sigma^k(i)$$

R_σ est une relation d'équivalence et la classe d'équivalence de tout élément de I_n fixe par σ est un singleton. Soit $O_1, O_2, \cdots, O_p$ les classes distinctes qui ne sont pas réduites à un singleton (il en existe au moins une car $\sigma \neq Id_{I_n}$), on a alors $\bigcup_{1\leq m\leq p} O_m = supp(\sigma)$. Soit $i \in O_1$ donc $\sigma(i) \neq i$, soit l_1 le plus petit entier strictement positif tel que $\sigma^{l_1}(i) = i$, ainsi $O_1 = \{i, \sigma(i), \sigma^2(i), \cdots, \sigma^{l_1-1}(i)\}$. O_1 définit un cycle c_1 de longueur l_1 de la manière suivante : $c_1(j) = \sigma(j)$ si $j \in O_1$ et $c_1(j) = j$ sinon. Autrement dit, $c_1 = (i, \sigma(i), \sigma^2(i), \cdots, \sigma^{l_1-1}(i))$. Comme les classes $O_1, O_2, \cdots, O_p$ sont distinctes deux à deux, alors elles sont disjointes deux à deux, par suite, les cycles associés respectivement sont disjoints deux à deux et commutent entre-eux, et $\sigma(j) = c_1c_2\cdots c_p(j)$ pour tout $j \in supp(\sigma)$. Les autres éléments de I_n sont fixes par σ et par le produit $c_1c_2\cdots c_p$. Donc, $\sigma = c_1c_2\cdots c_p$. □

Exemple. *On montre sur un exemple comment cette décomposition s'obtient facilement. On considère la permutation* σ *dans* S_8 *définie par :*

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

On a $\sigma(1) = 3 \neq 1$ *(*1 *n'est pas fixe par* σ*). On va calculer l'image de* 1 *par les puissances de* σ *jusqu'à obtenir* 1.

$$\sigma(1) = 3, \quad \sigma^2(1) = \sigma(3) = 4, \quad \sigma^3(1) = \sigma(4) = 5, \quad \sigma^4(1) = \sigma(5) = 1$$

On obtient ainsi le cycle $c = (1, \sigma(1), \sigma^2(1), \sigma^3(1)) = (1, 3, 4, 5)$.

Comme il existe encore des éléments de $I_8 \setminus supp(c)$ *que* σ *ne laisse pas invariants, on en prend un, par exemple* 2, *et de même, on va calculer l'image de* 2 *par les puissances de* σ *jusqu'à l'obtention de* 2 *:*

$$\sigma(2) = 6, \quad \sigma^2(2) = \sigma(6) = 8, \quad \sigma^3(2) = \sigma(8) = 2$$

Ce qui donne le cycle $c' = (2, 6, 8)$.

On a $I_8 \setminus supp(c) \cup supp(c') = \{7\}$ *et* 7 *est fixe par* σ, *donc* $\sigma = cc' = c'c$.

Remarques. — *Soit* $\sigma \in S_n$, *si* $\sigma = c_1 c_2 \cdots c_p$ *est la décomposition de* σ *en cycles disjoints, alors* $o(\sigma) = ppcm(o(c_1), o(c_2), \cdots, o(c_p))$.

— *On a montré que toute permutation est un produit de transpositions et la démonstration du résultat donne une méthode pour obtenir une telle décomposition.*

Une seconde méthode, qui est très commode, est la suivante :

on commence d'abord par décomposer la permutation en produit de cycles disjoints, ensuite on applique la propriété (2) IV.0.1 donnée auparavant, on obtient la décomposition de σ *en produit de transpositions. Comme illustration, on reprend l'exemple précédent dans* S_8 *: la décomposition de* σ *en produit de cycles disjoints* $\sigma = (1, 3, 4, 5)(2, 6, 8)$.
D'après la propriété (2) IV.0.1,
$(1, 3, 4, 5) = (1, 3)(3, 4)(4, 5)$ *et* $(2, 6, 8) = (2, 6)(6, 8)$ *d'où*
$\sigma = (1, 3)(3, 4)(4, 5)(2, 6)(6, 8)$

Proposition IV.0.2. — *(i) Si* $c = (i_1, i_2, \cdots, i_p)$ *est un cycle de longueur* p *et* $\sigma \in S_n$, *alors* $\sigma c \sigma_{-1}$ *est le cycle* $c' = (\sigma(i_1), \sigma(i_2), \cdots, \sigma(i_p))$.

— *(ii) Deux cycles de même longueur sont conjugués (i.e. si* c_1 *et* c_2 *sont deux* p*-cycles alors il existe* $\sigma \in S_n$ *tel que* $c_2 = \sigma c_1 \sigma^{-1}$*).*

Preuve. — (i) Soit $A = \{i_1, i_2, \cdots, i_p\}$ le support de c, $\sigma(A) = \{\sigma(i_1), \sigma(i_2), \sigma(i_p)\} = supp(c')$. On montre que $\sigma c \sigma^{-1} = c'$: soit $k \in I_n$
si $k \in \sigma(A)$, $\exists 1 \leq j \leq p$, tel que $k = \sigma(i_j)$. On a $\sigma c \sigma^{-1}(k) = \sigma c \sigma^{-1}(\sigma(i_j)) = \sigma c(i_j) = \sigma(i_{j+1}) = c'(\sigma(i_j)) = c'(k)$.
si $k \notin \sigma(A)$ alors d'une part $c'(k) = k$, d'autre part $\sigma^{-1}(k) \notin A$ et donc $c(\sigma^{-1}(k)) = \sigma^{-1}(k)$, par suite $\sigma c \sigma^{-1}(k) = \sigma\sigma^{-1}(k) = k = c'(k)$,
donc $\sigma c \sigma^{-1}(k) = c'(k)$ pour tout $k \in I_n$.

— (ii) Soit $c = (i_1, i_2, \cdots, i_p), c' = (j_1, j_2, \cdots, j_p)$ deux p-cycles. Soit $A = \{i_1, i_2, \cdots, i_p\} = supp(c)$ et $B = \{j_1, j_2, \cdots, j_p\} = supp(c')$. On a $card(\complement_{I_n} A) = card(\complement_{I_n} B) = n - p$, donc il existe une bijection f de $\complement_{I_n} A$ sur $\complement_{I_n} B$. Soit $\sigma : I_n \to I_n$ définie par :

$\sigma(k) = f(k)$, si $k \in \complement A$
$\sigma(i_r) = j_r$, $\forall 1 \leq r \leq p$
et d'après (1) $\sigma c \sigma^{-1} = c'$.

σ est alors une bijection de I_n sur I_n, donc on a $\sigma \in S_n$

□

Remarque. *Plus généralement, deux permutations de S_n sont conjuguées si et seulement si dans leur décomposition canonique en cycles disjoints apparaît le même nombre de p-cycles pour tout $2 \leq p \leq n$.*

Corollaire IV.1. *Toute transposition (i, j) où $i < j$ est conjuguée d'une transposition simple. En particulier, $(i, j) = c(j-1, j)c^{-1}$ où $c = (i, i+1, i+2, \cdots, j-1)$.*

Exercice 1. *Montrer que les transpositions simples $\tau_{i,i+1}$, notées aussi $(i, i+1)$, où $1 \leq i \leq n-1$ engendrent S_n.*

Montrer que les deux permutations $\tau_{1,2}$ et $c = (1, 2, \cdots, n)$ engendrent S_n.

V Signature d'une Permutation

Définition V.0.1. *Soit $n \geq 2$. Soit $\sigma \in S_n$. On dit que le couple (i, j) où $1 \leq i < j \leq n$ est une inversion pour σ si $\sigma(i) > \sigma(j)$. Notons $I(\sigma)$ le nombre d'inversions de σ, l'entier $(-1)^{I(\sigma)}$ est appelé signature de σ et noté $\epsilon(\sigma)$.*

$\begin{cases} Si\ \epsilon(\sigma) = 1, & on\ dit\ que\ la\ permutation\ est\ paire. \\ Si\ \epsilon(\sigma) = -1, & la\ permutation\ est\ dite\ impaire. \end{cases}$

Exemples.

1. *Si $\tau = (i, i+1) = \tau_{i,i+1}$ est une transposition simple de S_n alors le couple $(i, i+1)$ est le seul couple de I_n qui présente une inversion, donc $\epsilon(\tau) = (-1)^1 = -1$.*
2. *Dans S_3, considérons la transposition*

$$\sigma = (1, 3) = \tau_{1,3} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

les couples (i, j) qui présentent une inversion pour $\tau_{1,3}$ sont $(1, 2), (1, 3)$ et $(2, 3)$. Donc, $I(\sigma) = 3$ et, par suite, $\epsilon(\tau_{1,3}) = (-1)^3 = -1$.

Proposition V.0.1. *L'application $\epsilon : \sigma \mapsto \epsilon(\sigma)$ est un homomorphisme surjectif du groupe $(S_n, \circ)$ sur le groupe multiplicatif $(\{-1, 1\}, \times)$, et c'est le seul homomorphisme surjectif de S_n sur $\{-1, 1\}$. Si $\sigma = \tau_1 \tau_2 \cdots \tau_k$ est un produit de k transpositions, on a $\epsilon(\sigma) = (-1)^k$.*

Preuve. Soit $\sigma, \eta \in S_n$. On montre que $\epsilon(\sigma\eta) = \epsilon(\sigma)\epsilon(\eta)$. On pose :

$$N_1 = card(\{1 \leq i < j \leq n, \ / \ \eta(i) < \eta(j) \quad \text{et} \quad \sigma(\eta(i)) < \sigma(\eta(j))\})$$
$$N_2 = card(\{1 \leq i < j \leq n, \ / \ \eta(i) < \eta(j) \quad \text{et} \quad \sigma(\eta(i)) > \sigma(\eta(j))\})$$
$$N_3 = card(\{1 \leq i < j \leq n, \ / \ \eta(i) > \eta(j) \quad \text{et} \quad \sigma(\eta(i)) < \sigma(\eta(j))\})$$
$$\text{et} \quad N_4 = card(\{1 \leq i < j \leq n, \ / \ \eta(i) > \eta(j) \quad \text{et} \quad \sigma(\eta(i)) > \sigma(\eta(j))\})$$

On a $I(\sigma\eta) = N_1 + N_4 \quad ; \quad I(\sigma) = N_2 + N_3 \quad \text{et} \quad I(\eta) = N_3 + N_4$, d'où :

$$\epsilon(\sigma)\epsilon(\eta) = (-1)^{N_2+N_3}(-1)^{N3+N_4} = (-1)^{N_2+N_4} = \epsilon(\sigma\eta)$$

Donc, ϵ est un homomorphisme de groupes. Et comme $\epsilon(e_n) = 1$, et $\epsilon(\tau_{i,i+1}) = -1$ où $\tau_{i,i+1}$ est la transposition simple $(i, i+1)$, alors ϵ est surjectif.

Par ailleurs, on a pour tous $1 \leq i < j < n$, $(i,j) = c^{-1}(j-1,j)c$ où $c = (i, i+1, \cdots, j-1)$, autrement écrit, $\tau_{ij} = c\,\tau_{j-1,j}\,c^{-1}$. On a alors

$$\epsilon(\tau_{i,j}) = \epsilon(c)\,\epsilon(\tau_{j-1,j})\,\epsilon(c^{-1}) = \epsilon(c)\,(\epsilon(c))^{-1}\,\epsilon(\tau_{j-1,j}) = \epsilon(\tau_{j-1,j}) = -1$$

On en déduit que si $\sigma \in S_n$, tel que $\sigma = \tau_1\tau_2\cdots\tau_k$ (produit de k transpositions), alors $\epsilon(\sigma) = \epsilon(\tau_1)\epsilon(\tau_2)\cdots\epsilon(\tau_k) = (-1)^k$.

Unicité

Soit ϕ un homomorphisme surjectif de S_n sur $\{-1, 1\}$. Il existe alors une transposition τ tel que $\phi(\tau) = -1$, car si l'image de toute transposition par ϕ est 1, on aura alors $\phi(\sigma) = 1$ pour tout $\sigma \in S_n$ (S_n étant engendré par les transpositions), ceci contredit la surjection de ϕ. Soit alors τ une transposition tel que $\phi(\tau) = -1$. Sachant que toute transposition τ' est une conjuguée de τ alors l'image de τ' par l'homomorphisme ϕ est -1. Et finalement, pour tout $\sigma \in S_n$, il existe k transpositions $\tau_1, \tau_2, \cdots, \tau_k$ tel que $\sigma = \tau_1\tau_2\cdots\tau_k$. D'où :

$$\phi(\sigma) = \prod_{i=1}^{k} \phi(\tau_i) = \prod_{i=1}^{k}(-1) = (-1)^k = \epsilon(\sigma)$$

On conclut que $\phi = \sigma$. □

Corollaire V.1. — *Si σ se décompose d'une part en un produit de m transpositions et d'autre part en un produit de m' transpositions, alors les entiers m et m' sont de même parité.*

— *Si c est un p-cycle alors $\epsilon(c) = (-1)^{p-1}$.*

Preuve. — On suppose que $\sigma = \tau_1\tau_2\cdots\tau_m = \tau'_1\tau'_2\cdots\tau'_m$, alors $(-1)^m = \epsilon(\sigma) = (-1)^{m'}$ d'où m et m' sont de même parité.

— Soit $c = (i_1, i_2)(i_2, i_3)\cdots(i_{p-1}, i_p)$ est produit de $p-1$ transpositions donc $\epsilon(c) = (-1)^{p-1}$.

□

VI Groupe Alterné

Définition VI.0.1. *Pour tout $n \geq 2$, le noyau de ϵ est un sous-groupe de S_n, appelé le $n^{ième}$ groupe alterné et noté A_n. Les éléments de A_n sont les permutations paires.*

Remarque. *A_n est l'ensemble des permutations de S_n qui se décomposent en un nombre pair de transpositions.*

Proposition VI.0.1. *Pour tout $n \geq 2$, A_n est un sous-groupe distingué de S_n, d'indice 2. C'est le seul sous-groupe distingué d'indice 2.*

Preuve. L'homomorphisme $\epsilon : S_n \to \{-1, 1\}$ a pour noyau A_n, donc A_n est un sous-groupe distingué et par la factorisation de ϵ, on a $S_n/A_n \simeq \{-1, 1\}$, donc $[S_n : A_n] = |\frac{S_n}{A_n}| = 2$.
Soit H un sous-groupe distingué de S_n d'indice 2.

H étant distingué donc il existe un homomorphisme $\phi : S_n \to \{-1, 1\}$ tel que $Ker(\phi) = H$ et d'près le premier théorème d'isomorphisme, on a $S_n/H \simeq Im(\phi)$; Comme $[S_n : H] = 2$, ϕ est alors surjectif. Or, ϵ est le seul homomorphisme surjectif de S_n sur $\{-1, 1\}$, d'où $\epsilon = \phi$ et donc $A_n = Ker(\epsilon) = Ker(\phi) = H$. □

Corollaire VI.1. *Pour tout $n \geq 2, |A_n| = \frac{n!}{2}$.*

Exemple. *Pour $n = 2$, $A_2 = \{e_2\}$.*

Pour $n = 3$, $A_3 = \{e_3, c, c^2\} =< c >$ où c est le 3-cycle $(1, 2, 3)$.

Proposition VI.0.2. *Pour $n \geq 3$, le groupe alterné est engendré par les 3-cycles de S_n.*

Preuve. Considérons deux transpositions distinctes τ_1, τ_2.

Si τ_1 et τ_2 sont non disjointes, alors $\exists i, j, k$ distincts deux-à-deux de I_n tel que $\tau_1 = (i, j)$, $\tau_2 = (i, k)$ d'où $\tau_1\tau_2 = (j, i, k) = (i, k, j)$ est un 3-cycle.

Si τ_1 et τ_2 sont disjointes, alors on a $\tau_1 = (i, j)$, $\tau_2 = (k, l)$, avec i, j, k, l distincts deux-à-deux, et par suite $\tau_1\tau_2 = (i, j)(k, l) = (i, l, k)(i, j, k)$ est un produit de deux 3-cycles, et puisque toute permutation de A_n est le produit d'un nombre pair de transpositions, on conclut que les 3-cycles engendrent A_n. □

Lemme 2. *Pour $n \geq 5$, les 3-cycles sont conjugués dans A_n.*

Preuve. Soit $c = (i, j, k)$ un 3-cycle, il existe alors $\sigma \in S_n$ tel que $(1, 2, 3) = \sigma(i, j, k)\sigma^{-1}$ d'après la proposition IV.0.1.

Si $\sigma \notin A_n$, comme $n \geq 5$, on a alors $(4, 5)\sigma \in A_n$ et

$$(4, 5)\sigma c\sigma^{-1}(4, 5) = (4, 5)(1, 2, 3)(4, 5) = (4, 5)^2(1, 2, 3) = (1, 2, 3)$$

donc $(4,5)\sigma c((4,5)\sigma)^{-1} = (1,2,3)$; Ainsi, pour $n \geq 5$, tout 3-cycle est conjugué de $(1,2,3)$ dans A_n. □

Lemme 3. *Pour $n \geq 3$, Si H est un sous-groupe distingué de A_n contenant un 3-cycle alors $H = A_n$.*

Preuve. Soit c un 3-cycle tel que $c \in H$, comme, d'après le lemme 2, tout 3-cycle c' est un conjugué de c dans A_n et puisque $H \trianglelefteq A_n$, alors H contient tous les 3-cycles. Or, A_n est engendré par les 3-cycles, donc $H = A_n$. □

Lemme 4. *Pour $n \geq 5$, si H est un sous-groupe distingué de A_n qui contient le produit de deux transpositions, alors $H = A_n$.*

Preuve. Soit $\sigma = (i,j)(k,l) \in H$ où (i,j) et (k,l) sont deux transpositions disjointes. Puisque $n \geq 5$, il existe $h \in I_n \setminus \{i,j,k,l\}$ et on considère $c = (i,j,h) \in A_n$; On a alors $c^{-1}\sigma c \in H$ (car $H \trianglelefteq A_n$) et $c^{-1}\sigma c = (i,h)(k,l)$ et

$$\begin{aligned} \sigma^{-1}c^{-1}\sigma c &= (i,j)(k,l)(i,h)(k,l) \\ &= (i,j)(k,l)^2(i,h) = (i,h,j) \in H \end{aligned}$$

donc H contient un 3-cycle et d'après le lemme 3, $H = A_n$. □

Théorème VI.1. *Pour $n \geq 5$, le groupe alterné A_n est simple.*

Preuve. Soit H un sous-groupe distingué, différent de $\{e\}$. Soit $\sigma \in H$ avec $\sigma \neq e$. Donc $\sigma = c_1 c_2 \cdots c_k$ est un produit fini des cycles deux-à-deux disjoints et donc permutables, on peut supposer que la longueur de c_i est supérieure à la longueur de c_{i+1}. D'où les cas suivants :

Cas 1- $c_1 = (a_1, a_2, \cdots, a_m)$ est un m-cycle avec $m > 3$.

On considère $c = (a_1, a_2, a_3)$, $c \in A_n$. Puisque $H \trianglelefteq A_n$, on a alors $\sigma^{-1}c^{-1}\sigma c \in H$. On a alors

$$\begin{aligned} c^{-1}\sigma c &= c^{-1}c_1c_2\cdots c_k c = (c^{-1}c_1c)c_2\cdots c_k \\ &= (a_3, a_1, a_2, a_4, a_5, \cdots, a_m)c_2c_3\cdots c_k \end{aligned}$$

et par suite,

$$\begin{aligned} \sigma^{-1}c^{-1}\sigma c &= c_k^{-1}\cdots c_2^{-1}c_1^{-1}(a_3, a_1, a_2, a_4, \cdots, a_m)c_2c_3\cdots c_k, \\ &= c_1^{-1}(a_3, a_1, a_2, a_4, \cdots, a_m) \quad \text{(en commutant)} \\ &= (a_m, a_{m-1}, \cdots, a_3, a_2a_1)(a_3, a_1, a_2, a_4, \cdots, a_m) \\ &= (a_2, a_3, a_m) \quad \text{d'où} \quad (a_2, a_3, a_m) \in H \end{aligned}$$

et d'après le lemme 3, on conclut que $H = A_n$.

Cas 2- $m = 3$ et c_2 est aussi un 3-cycle.

Soit alors $c_1 = (a_1, a_2, a_3)$ et $c_2 = (a_4, a_5, a_6)$, on prend $\eta = c = (a_2, a_3, a_4) \in A_n$, alors

$$\eta^{-1}\sigma\eta = \eta^{-1}\prod_{i=1}^{k} c_i\eta = \prod_{i=1}^{k}\eta^{-1}c_i\eta = \eta^{-1}c_1\eta\eta^{-1}c_2\eta\eta^{-1}c_3\eta\cdots c_k \in H$$

Par suite,

$$\begin{aligned}\sigma^{-1}\eta^{-1}\sigma\eta = & \quad c_1^{-1}c_2^{-1}c_3^{-1}\cdots c_k^{-1}(\eta^{-1}c_1\eta)(\eta^{-1}c_2\eta)c_3c_4\cdots c_k\\ = & \quad c_1^{-1}c_2^{-1}(\eta^{-1}c_1\eta)(\eta^{-1}c_2\eta)\\ = & \quad c_1^{-1}c_2^{-1}(a_1,a_4,a_2)(a_3,a_5,a_6)\\ = & \quad (a_3,a_2,a_1)(a_6,a_5,a_4)(a_1,a_4,a_2)(a_3,a_5,a_6)\\ = & \quad (a_1,a_6,a_2,a_3,a_4)\in H\end{aligned}$$

(a_1,a_6,a_2,a_3,a_4) est un cycle de longueur >3. D'après le premier cas, on conclut que $H=A_n$.

Cas 3- $m=3$ et $\forall\, 2\leq i\leq k$, c_i sont des transpositions.

Soit $c_1=(a_1,a_2,a_3)$. On a alors

$$\begin{aligned}\sigma^2 = & \quad (a_1,a_2,a_3)c_2c_3\cdots c_k(a_1,a_2,a_3)c_2c_3\cdots c_k\\ = & \quad (a_1,a_2,a_3)^2c_2^2c_3^2\cdots c_k^2\\ = & \quad (a_1,a_3,a_2)\in H\end{aligned}$$

et donc $H=A_n$, d'après le lemme 3.

Cas 4- $\forall\, 1\leq i\leq k$, c_i est une transposition, (k est alors un nombre pair).

Si $c_1=(a_1,a_2)$ et $c_2=(a_3,a_4)$, on prend $\eta=(a_2,a_3,a_4)\in A_n$ d'où H contient $\eta^{-1}\sigma\eta$ avec

$$\eta^{-1}\sigma\eta=\prod_{i=1}^{k}\eta^{-1}c_i\eta=\eta^{-1}c_1\eta\eta^{-1}c_2\eta c_3\cdots c_k=(a_2,a_3)(a_4,a_2)c_3\cdots c_k$$

et par suite H contient $\sigma^{-1}\eta^{-1}\sigma\eta=(a_1,a_4)(a_2,a_3)$. On conclut alors, d'après le lemme 4 que $H=A_n$.

□