الجمهوريـــة الجزائـــريـــة الديمقراطيـــة الشعبيـــة
République Algérienne Démocratique et Populaire
وزارة التعليـــــم العالـــي والبحـــث العلمـــي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Ref :……

Centre Universitaire de Mila

Institut des sciences et de la technologie **Département de Mathématiques et Informatique**

Groupe symétrique

Mémoire préparé En vue de l'obtention du diplôme de licence en Mathématiques

Préparé par :
Loucif Fatima
Begbagui Farida
Merouane Samia

Encadré par :
Kecies Mohamed

Filière : **mathématiques**

Année universitaire : 2012/2013

*** Remerciements ***

Nous tenons à remercier en premier et avant tout, notre créateur <<ALLAH>>, qui nous aide à réaliser ce travail.

Nos sincères gratitudes et remerciements à notre encadreur Mohamed Kecies pour le grand soutient moral et leur aides précieuses qui nous apportez durant tout ce travail.

Nous adressons, également, mes remerciements chaleureux aux membres de l'institut des sciences et de la technologie et à tous ceux qui ont pris part de près ou de loin, à la réalisation de ce travail.

Fatima, Farida et Samia

Table des matières

Introduction Générale

La notion de groupe est une abstraction des opérations naturelles, telles que l'addition, la multiplication ou la composition, lorsqu'elles sont inversibles. Cette notion permet de modéliser des situations qui se retrouvent dans beaucoup de disciplines, non seulement en mathématiques, mais aussi en chimie et en physique. La notion de permutation exprime l'idée de réarrangement d'objets discernables. Une permutation de n objets distincts rangés dans un certain ordre, correspond à un changement de l'ordre de succession de ces n objets. La permutation est une des notions fondamentales en combinatoire, c'est-à-dire pour des problèmes de dénombrement et de probabilités discrètes. Les permutations servent également à fonder la théorie des groupes, celle des déterminants, à définir la notion générale de symétrie, etc.

Ce mémoire est réparti sur l'introduction générale, et trois chapitres. Le premier chapitre est composé de deux parties. Dans la première, on a commencé par une brève introduction aux fonctions, et dans la deuxième partie on a étudié les applications et leurs propriétés, en particulier celles concernant l'injectivité, la surjectivité et la bijectivité. Dans le deuxième chapitre nous avons donné les différents concepts des groupes et morphismes de groupes. Enfin, dans le dernier chapitre, on a présenté une étude générale de groupe symétrique, dont la composition des permutations, la décomposition en produit des cycles et transpostions.

Chapitre 1

Fonctions et applications

Dans ce chapitre nous rappelons quelques généralités sur les fonctions et applications, qui on aura besoin par la suite.

1.1 Fonctions et applications

1.1.1 Fonctions

Définition 1.1.1 *Soient E, F deus ensembles.*
1) On appelle fonction d'un ensemble E vers un ensemble E, toute correspondance (ou relation) f, qui, à chaque élément x de E, fait correspondre au plus un élément y de E.
2) On dit que E est l'ensemble de départ ou la source et que E est l'ensemble d'arrivée ou le but.
3) On appelle graphe de f noté G_f ou Γ_f l'ensemble

$$\Gamma_f = \{(x, f(x)), x \in E\}$$

4) L'élément y associé à x par f s'appelle l'image de x et se note souvent $f(x)$. (C.à.d : $y = f(x)$)
5) La partie de E formée des éléments auxquels est associé un élément de E s'appelle le domaine de définition de f et se note souvent $Dom(f)$ ou $D(f)$: C.à.d

$$D(f) = \{x \in E, \exists y \in F : f(x) = y\}$$

6) L'ensemble $f(E)$ est appelé image de f et est noté $Im(f)$ formé de toutes les images des éléments de E. C.à.d

$$\mathrm{Im}(f) = f(E) = \{y \in F, \exists x \in E : f(x) = y\} = \{f(x) \in F, x \in E\}$$

Remarque 1.1.2
1) Une fonction f est souvent notée de la manière suivante

$$E \xrightarrow{f} F \quad ou \quad \begin{array}{rccc} f: & E & \longrightarrow & F \\ & x & \longmapsto & f(x) = y \end{array}$$

2) Si $y = f(x)$, alors x s'appelle antécédent de y.
3) Si $f : E \longrightarrow F$ est une fonction, alors

$$(x, y) \in \Gamma_f \Longleftrightarrow x \in D(f) \text{ et } y = f(x)$$

4) $f : E \longrightarrow F$ est une fonction si et si $\forall x \in E, \forall y_1, y_2 \in F : (x, y_1)$ et $(x, y_2) \in \Gamma_f \Longrightarrow y_1 = y_2$

Exemple 1.1.3
1) La correspondance f qui associe à chaque entier naturel le mois correspondant est une fonction de $E = \mathbb{N}$ dans l'ensemble

$F = \{janvier, fevrier, mars, avril, mai, juin, juillet; août; septembre, octobre, novembre, decembre\}$

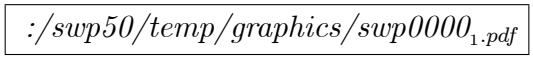
On a dans ce cas $f(2) = fevrier$ et $f(17)$ n'existe pas. $D(f) = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

2) La correspondance qui associe à chaque mois le nombre possible de jours du mois n'est une fonction de l'ensemble $\mathbb{N}$ de l'exemple précédent dans F, car elle fait associer à février, les deux éléments 28 et 29.

Remarque 1.1.4 *La représentations d'une fonction $f : E \longrightarrow F$ dépend de la nature des ensembles E et F. Les représentations les plus utilisées sont les suivantes :*
1) Représentation au moyen d'une formule. Soit la fonction $f : \mathbb{Z} \longrightarrow \mathbb{N}$ telle que $f(x) = x^2$
2) Représentation au moyen d'une table de valeurs (utile dans le cas où E est fini). Soit la fonction $f : \{-2, -1, 0, 1, 2, 3\} \longrightarrow \mathbb{N}$ telle que

n	-2	-1	0	1	2	3
$f(n)$	4	1	0	1	4	9

3) Représentation au moyen d'un graphe. Soit la fonction $f : \mathbb{R} \longrightarrow \mathbb{R}$ *telle que* $f(x) = \frac{1}{x}$



1.1.2 Applications

Définition 1.1.5 *On appelle application d'un ensemble* E *dans un ensemble* F *toute fonction* f *de* E *vers* F *telle que tout élément de* E *a une image unique dans* F*. C.à.d*

$$\forall x \in E, \exists! y \in F : f(x) = y$$

Autrement dit $D(f) = E$*.*

Notation 1.1.6
1) On note $\mathcal{F}(E, F)$ *ou* F^E *l'ensemble de toutes les applications de* E *vers* F*.*
2) Si les deux ensembles E *et* F *sont égaux, on note plus simplement* $\mathcal{F}(E)$*.*

Définition 1.1.7 *Soient* f, g *deux applications. On dit que* f *et* g *sont égales si et seulement si elles ont le même ensemble de départ* E*, même ensemble d'arrivé* F *et le même graphe, c'est à dire* $\forall x \in E : f(x) = g(x)$*. On écrit dans ce cas* $f = g$*.*

Exemple 1.1.8 *Les applications* f *et* g *définies de* $\mathbb{N}$ *dans* $\mathbb{Z}$ *par* $f(x) = \cos \pi x$ *et* $g(x) = (-1)^n$ *sont égales. C.à.d* $f = g$*.*

Définition 1.1.9
1) On définit l'application identité de E *dans* E*, notée* Id_E *par* $\forall x \in E : f(x) = x$
2) Si A *est une partie de* E*, l'application* i *de* A *dans* E *définie par* $\forall x \in A : f(x) = x$ *est appelée l'injection canonique de* A *dans* E*.*
3) Une application $f : E \longrightarrow F$ *est dite constante s'il existe un élément* c *de* F*, tel que* $\forall x \in E : f(x) = c$*. En particulier si* $c = 0$*, alors* f *est appelée l'application nulle.*
4) Si A *est une partie de* E*, alors on appelle application caractéristique ou indicatrice de* A*, et on note* χ_A *l'application de* E *vers* $\{0, 1\}$*, définie par*

$$\chi_A(x) = \begin{cases} 1, & si\ x \in A \\ 0, & si\ x \notin A \end{cases}$$

Définition 1.1.10 *Soient* E, F, G *trois ensembles,* f *dans* $\mathcal{F}(E, F)$ *et* g *dans* $\mathcal{F}(F, G)$*. La composée de* f *par* g*, notée* $g \circ f$*, est l'application de* E *vers* G*, définie par* $\forall x \in E$:

$(g \circ f)(x) = g(f(x))$. *On écrit*

$$\begin{array}{rccc} g \circ f : & E & \longrightarrow & G \\ & x & \longmapsto & g(f(x)) = y \end{array}$$

Définition 1.1.11 *On appelle (une) involution (où application involutive) de E toute application $f : E \longrightarrow E$ telle que $f \circ f = Id_E$.*

Exemple 1.1.12
1) L'application Id_E est involutive.
2) L'application (complémentaire) $A \longmapsto \overline{A}$ est une involution de $\mathcal{P}(E)$.
3) L'application (conjugué) $z \longmapsto \overline{z}$ est une involution de $\mathbb{C}$.

Remarque 1.1.13
1) Si $f, g \in \mathcal{F}(E)$, alors on dit que f et g commutent si $g \circ f = f \circ g$.
2) On note que Id_E commute avec toute application $f \in \mathcal{F}(E)$.
3 La composition des applications en général n'est pas commutative, c'est à dire qu'il ne se peut que $g \circ f \neq f \circ g$.
4) Si $f \in \mathcal{F}(E, F)$, alors $Id_F \circ f = f$ et $f \circ Id_E = f$.
5) Si $f \in \mathcal{F}(E)$, alors on pose par convention $f^0 = Id_E$. On définit alors les puissances f^n par

$$\forall n \in \mathbb{N}^* : f^n = f^{n-1} \circ f = f \circ f \circ ... \circ f \text{ (n fois)}$$

Proposition 1.1.14 *Soient $f \in \mathcal{F}(E, F), g \in \mathcal{F}(F, G), h \in \mathcal{F}(G, H)$, alors $(h \circ g) \circ f = h \circ (g \circ f)$.*

Preuve. Les applications $(h \circ g) \circ f$ et $h \circ (g \circ f)$ ont le même ensemble de départ E et le même ensemble d'arrivée H.
Soit $x \in E$, alors $((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$. Alors $(h \circ g) \circ f = h \circ (g \circ f)$. ■

Définition 1.1.15 *Soit f une application de E dans F.*
1) On dit que f est une application injective (ou une injection) si tout élément y de F possède au plus un antécédent par f.
Une définition équivalente est

$$\forall x, x' \in E : x \neq x' \Longrightarrow f(x) \neq f(x')$$

c'est à dire f conserve les différences.
Une autre définition équivalente (souvent la plus utile) est

$$\forall x, x' \in E : f(x) = f(x') \Longrightarrow x = x'$$

2) On dit que f est une application surjective (ou une surjection) si tout élément y de F possède au moins un antécédent par f.
Autrement dit

$$\forall y \in f, \exists x \in E : f(x) = y$$

Une autre définition équivalente est $f(E) = \mathrm{Im}(f) = F$.
3) On dit que f est une application bijective (ou une bijection) si f est à la fois injective et surjective. C'est-à-dire si tout élément $y \in F$ possède un antécédent x et un seul dans E.

$$\forall y \in f, \exists! x \in E : f(x) = y$$

Proposition 1.1.16 *Soient les applications $f : E \longrightarrow F$ et $g : F \longrightarrow G$. Alors*
1) Si f et g sont injectives, alors $g \circ f$ est injective.
2) Si f et g sont surjectives, alors $g \circ f$ est surjective.
3) Si f et g sont bijectives, alors $g \circ f$ est bijective.
4) Si $g \circ f$ est injective, alors f est injective.
5) Si $g \circ f$ est surjective, alors g est surjective.

Preuve.
1) Supposons f et g injectives. Soient x et x' dans E tels que $(f \circ g)(x) = (f \circ g)(x')$. Alors $f(g(x)) = f(g(x\prime))$ donc, par injectivité de f, on a $g(x) = g(x')$. L'injectivité de g donne alors $x = x'$.
2) Supposons f et g surjectives. Soient z dans G. Comme g est surjective, il existe $y \in F$ tel que $z = g(y)$, de même par sujectivité de f, l'élément y de F a un antécédent $x \in E$ qui vérifie $y = f(x)$. Donc $z = g(f(x)) = (gf)(x)$ ce qui prouve le résultat.
3) Conséquence des deux points précédents.
4) Supposons $g \circ f$ injective. Soient x et x' dans E tels que $f(x) = f(x')$, alors $(g \circ f)(x) = (g \circ f)(x')$. Alors , par injectivité de $g \circ f$, on a $x = x'$.
5) Supposons $g \circ f$ surjective. Alors

$$\begin{aligned} \forall z \quad \in \quad & G, \exists x \in E : z = (g \circ f)(x) = g(f(x)) \\ \Longrightarrow \quad & \forall z \in G, \exists f(x) \in F : z = g(f(x)) \\ \Longrightarrow \quad & \forall z \in G, \exists y = f(x) \in F : z = g(y) \\ \Longrightarrow \quad & g \text{ est surjective} \end{aligned}$$

■

Définition 1.1.17 *Si f est une application bijective de E dans F, alors tout élément $y \in F$ admet un antécédent unique, que l'on note $x = f^{-1}(y)$. On définit ainsi une*

application de F dans E : $y \in F \longmapsto f^{-1}(y)$ qui associe à tout élément y de F son unique antécédent $x \in E$. Cette application s'appelle l'application réciproque de f et se note f^{-1}. On a donc

$$\forall (x,y) \in E \times F : y = f(x) \Longleftrightarrow x = f^{-1}(y)$$

De plus f^{-1} vérifie $f^{-1} \circ f = Id_E$ et $f \circ gf^{-1} = Id_F$.

Proposition 1.1.18 *Soit $f : E \longrightarrow F$ une application. Pour que f soit bijective il faut et il suffit qu'il existe une application $g : F \longrightarrow E$ telle que :*

$$\begin{cases} g \circ f = Id_E \\ f \circ g = Id_F \end{cases}$$

De plus, sous ces hypothèses, on a $g = f^{-1}$.

Preuve.
1) Si f est bijective, alors f^{-1} existe en tant qu'application et il est clair que

$$\begin{cases} f^{-1} \circ f = Id_E \\ f \circ f^{-1} = Id_F \end{cases}$$

2) Réciproquement, s'il existe $g : F \longrightarrow E$ telle que

$$\begin{cases} g \circ f = Id_E \\ f \circ g = Id_F \end{cases}$$

Alors d'après la proposition (1.1.16) et comme Id_E est injective et surjective, on déduit que f est injective et surjective, donc bijective. De même pour g. Enfin

$$g = g \circ \left(f \circ f^{-1}\right) = (g \circ f) \circ f^{-1} = Id_E \circ f^{-1} = f^{-1}$$

■

Proposition 1.1.19
1) Si une application admet une application réciproque, celle-ci est unique.
2) Soient f une bijection de E vers F et g une bijection de F vers G. Alors

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}$$

3) Si $f : E \longrightarrow F$ est une bijection, alors $f^{-1} : F \longrightarrow E$ est une bijection et $\left(f^{-1}\right)^{-1} = f$.

Preuve.
1) On suppose qu'il existe deux applications réciproques f_1 et f_2 à une application f de E vers F. On considère $f_1 \circ f \circ f_2$. On obtient

$$\begin{cases} f_1 \circ f \circ f_2 = (f_1 \circ f) \circ f_2 = Id_E \circ f_2 = f_2 \\ f_1 \circ f \circ f_2 = f_1 \circ (f \circ f_2) = f_1 \circ Id_F = f_2 \end{cases} \Longrightarrow f_1 = f_2$$

2) On a $g \circ f$ est une bijection comme le montre une proposition (1.1.16) précédente. Soit $z \in G$ quelconque, soit $y \in F$ son unique antécédent par g, et soit $x \in E$ l'unique antécédent de y par f. On a donc $x = f^{-1}(y)$ et $y = g^{-1}(z)$ donc

$$x = f^{-1}\left(g^{-1}(z)\right) = \left(f^{-1} \circ g^{-1}\right)(z)$$

Ce qui montre également que $(g \circ f)(x) = z$, c'est à dire $x = (g \circ f)(z)^{-1}$, d'où l'égalité annoncée.
3) On a $f \circ f^{-1} = Id_F$, donc $f \circ f^{-1} \circ (f^{-1})^{-1} = Id_F \circ (f^{-1})^{-1}$, c'est-à-dire $f \circ Id_E = Id_F \circ (f^{-1})^{-1}$. Donc $f = (f^{-1})^{-1}$. ■

Définition 1.1.20 *Soit $f : E \longrightarrow F$ où E et F sont deux ensembles. Soient $A \in \mathcal{P}(E), B \in \mathcal{P}(F)$.*
1) On appelle image directe de A par f et on note $f(A)$ l'ensemble

$$f(A) = \{y \in F, \exists x \in A : f(x) = y\} = \{f(x) \in F, x \in A\} \subset F$$

2) On appelle image réciproque de B par f et on note $f^{-1}(B)$ l'ensemble

$$f^{-1}(B) = \{x \in E, \exists y \in B : f(x) = y\} = \{x \in E, f(x) \in B\} \subset E$$

Soit f une application d'un ensemble E vers un ensemble F. Il y a plusieurs moyens de créer de nouvelles applications en ne modifiant que l'ensemble de départ ou l'ensemble d'arrivée.

Définition 1.1.21 *Soit f une application de E vers F et soit A une partie de E, E' un ensemble tel que $E \subset E'$.*
1) On appelle restriction de f à A et on note $f_{|A}$ l'application définie par

$$\begin{array}{rccc} f_{|A} : & A & \longrightarrow & F \\ & x & \longmapsto & f_{|A}(x) = f(x) \end{array}$$

De plus $f_{|A} = f \circ i$ ou $i : A \longrightarrow E$ est l'injection canonique.

2) On appelle prolongement de f à E', toute application g de E' vers F telle que

$$\forall x \in E : g(x) = f(x)$$

Autrement dit, $g_{|E} = f$.
De plus si $i : E \longrightarrow E'$ est l'injection canonique, alors g est un prolongement de f à E' si et seulement si $g \circ f = i$.

Exemple 1.1.22 *On peut prendre*

$$g : \begin{array}{ccc} \mathbb{R}^* & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \frac{\sin x}{x} \end{array} \quad et \quad f : \begin{array}{ccc} \mathbb{R} & \longrightarrow & \mathbb{R} \\ x & \longmapsto & \begin{cases} \frac{\sin x}{x}, \ si \ x \neq 0 \\ 0, \ \ si \ x = 0 \end{cases} \end{array}$$

Alors g est la restriction de f à $\mathbb{R}^*$ et f est le prolongement de g à $\mathbb{R}$.

Définition 1.1.23 *Soient E, F deux ensembles, $f : E \longrightarrow F$ une application, $A \in \mathcal{P}(E), B \in \mathcal{P}(F)$ telles que*

$$\forall a \in A : f(a) \in B$$

On appelle application induite par f sur A et B l'application $\begin{array}{ccc} A & \longrightarrow & B \\ x & \longmapsto & f(x) \end{array}$.
En particulier, Soient $f : E \longrightarrow F$ une application et A une partie de E stable par f (C-à-d : $f(A) \subset A$) , alors l'application induite par f sur A au départ et A à l'arrivée est appelée application induite par f sur A et notée souvent f_A. On a donc

$$f_A \begin{array}{ccc} A & \longrightarrow & A \\ x & \longmapsto & f(x) \end{array}$$

Proposition 1.1.24 *Si E est un ensemble fini et $f : E \longrightarrow F$ une application, alors*

$$\begin{array}{rcl} f \ est \ injective & \Longleftrightarrow & Card(f(E)) = Card(E) \\ f \ est \ surjevtive & \Longleftrightarrow & Card(f(E)) = Card(F) \\ f \ est \ bijective & \Longleftrightarrow & Card(f(E)) = Card(E) = Card(F) \end{array}$$

On en déduit que si E et F sont finis de même taille, alors

$$f \ est \ injective \Longleftrightarrow f \ est \ surjevtive \Longleftrightarrow f \ est \ bijective$$

Preuve. On a E et F sont finis de même taille, alors

$$\begin{aligned} f \text{ est injective} &\iff Card(E) = Card(f(E)) \iff \\ Card(f(E)) &= Card(F) \iff f(E) = F \iff f \text{ est surjective} \end{aligned}$$

■

Chapitre 2

Structures algébriques

Les objectifs de ce chapitre sont :

Rappeler la structure de groupe, les règles de calculs. Définir les notions de morphisme, de noyau, de sous groupe. Définir les notions de sous groupes engendrés par une partie.

2.1 Loi de composition interne

Définition 2.1.1
1) On appelle loi de composition interne (ou opération interne) (en abrégé : LCI) sur un ensemble non vide E, toute application $*$ de $E \times E$ dans E.
2) L'image $*(x, y)$ est souvent notée $x * y$.

Exemple 2.1.2
1) Les opérations usuelles $+, .$ sont des lois de composition internes sur $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
2) La composition $\circ$ est une loi de composition interne sur l'ensemble $\mathcal{F}(E, E)$ des applications de E dans E.
3) $\cap, \cup, \triangle$ (intersection, union, différence symétrique) sont des lois de composition internes sur $\mathcal{P}(E)$

Définition 2.1.3
1) Un ensemble E muni d'une ou plusieurs loi de composition internes est appelé structure algébrique.
2) Le couple $(E, *)$ est appelé un magma.

Remarque 2.1.4 *Si les lois sont notées $*_1, *_2, ..., *_n$, alors la structure algébrique est notée $(E, *_1, *_2, ..., *_n)$.*

Exemple 2.1.5 $(\mathbb{N}, +), (\mathbb{Z}, +, -), (\mathbb{R}, +, .), (\mathcal{F}(E, E), \circ)$ *et* $(\mathcal{P}(E), \cap)$ *sont des structures algébriques.*

Définition 2.1.6 *Soit $*$ une loi de composition interne sur E.*
1) Une partie A de E est dite stable pour $*$ si et seulement si

$$\forall x, y \in A : x * y \in A$$

2) Si A une partie stable de E pour $*$, alors la lci dans A définie par $\begin{array}{ccc} A \times A & \longrightarrow & A \\ (x, y) & \longmapsto & x * y \end{array}$ *est appelée lci induite sur A par $*$ de E. Autrement dit la restriction de la loi $*$ à $A \times A$ définit une loi de composition interne sur A.*

Exemple 2.1.7
1) $\mathbb{R}^+$ une partie de $\mathbb{R}$ est stable pour la multiplication.
2) $\mathbb{R}^-$ une partie de $\mathbb{R}$ n'est pas stable pour la multiplication.

Définition 2.1.8 *Soit $*$ une LCI sur un ensemble non vide E. Alors, On dit que*
1) La loi $*$ est commutative, si et si $\forall x, y \in E : x * y = y * x$.
2) La loi $*$ est associative, si et si $\forall x, y, z \in E : (x * y) * z = x * (y * z)$.
3) e de E est neutre à droite (resp : à gauche) pour $*$ si et si $\forall x \in E : x * e = x$. (resp : $\forall x \in E : e * x = x$)
4) e de E est dit élément neutre (ou élément unité) pour $*$ si et si e est neutre à droite et à gauche. C'est-à-dire

$$\forall x \in E : x * e = e * x = x$$

5) x de E possède :
i) Un symétrique à gauche noté x'_g si et si $x' * x = e$. On dit alors que x est symétrisable à gauche.
ii) Un symétrique à droite noté x'_d si et si $x * x' = e$. On dit alors que x est symétrisable à droite.
iii) Un symétrique x' si et si $x * x' = x' * x = e$. On dit alors que x est symétrisable.

Notation 2.1.9
1) Lorsque la loi est notée additivement $+$, l'élément neutre est noté 0_E et le symétrique de x est noté $-x$ (appelé opposé de x)
2) Si la loi notée multiplicativement ., alors l'élément neutre est noté 1_E et le symétrique de x est noté x^{-1} ou $\frac{1}{x}$ (appelé inverse de x).

Exemple 2.1.10
1) La somme $+$ et le produit .sur $\mathbb{C}$ (donc sur ses sous-ensembles) est associative et commutative, et admettent pour neutres respectifs 0 et 1.
2) La composition $\circ$ sur $\mathcal{F}(E)$ est une loi associative, admettant Id_E comme élément

neutre, et les seuls éléments inversibles sont les applications bijectives.
3) Les lois $\cup, \cap, \triangle$ *sur* $\mathcal{P}(E)$ *sont associatives et commutatives. Elles admettent pour neutres respectifs* ϕ, E, ϕ.
4) Seul ϕ *(resp : E) est inversible dans* $(\mathcal{P}(E), \cup)$ *(resp :* $(\mathcal{P}(E), \cap)$*).*

Définition 2.1.11
1) On appelle demi groupe tout ensemble non vide E muni d'une loi de composition interne $*$ *associative.*
2) On appelle monoïde (ou demi groupe unitaire) tout demi groupe $(E, *)$ *ayant un élément neutre* e.
Si en plus $*$ *est commutative, le monoïde est dit commutatif.*

Exemple 2.1.12
1) $(\mathbb{N}, +)\,(\mathbb{N}, .)$ *sont des monoïdes commutatifs.*
2) Pour tout ensemble E, on a $(\mathcal{P}(E), \cap), (\mathcal{P}(E), \cup)$ *sont des monoïdes commutatifs.*

Proposition 2.1.13 *Soit E un ensemble muni d'une loi de composition interne* $*$*, alors*
1) L'élément neutre e, s'il existe, il est unique.
2) Si $*$ *est associative et admet un élément neutre e, alors l'élément inverse* x^{-1} *de x, s'il existe il est unique, de plus si* $x, y \in E$ *sont inversibles alors* $x * y$ *est inversible et*

$$\begin{cases} (x*y)^{-1} = y^{-1} * x^{-1} \\ (x^{-1})^{-1} = x \end{cases}$$

Preuve.
1) Supposons e' un autre élément neutre de $*$, alors $e * e' = e$ et comme e est aussi un élément neutre alors $e * e\prime = e\prime$, d'où l'égalité $e' = e$.
2) Supposons x' un autre inverse de x, alors $x' * x = e$, ainsi

$$x^{-1} = (x' * x) * x^{-1} = x' * (x * x^{-1}) = x'$$

donc l'inverse est unique.
On a $x * x^{-1} = e = x^{-1} * x$, et puisque l'inverse est unique, alors x est l'inverse de x^{-1}, c.à.d $(x^{-1})^{-1} = x$.
Supposons que $x, y \in E$ sont inversibles. Alors

$$\begin{cases} (y^{-1} * x^{-1}) * (x * y) = y^{-1} * x^{-1} * x * y = e \\ (x * y) * (y^{-1} * x^{-1}) = x * y * y^{-1} * x^{-1} = e \end{cases}$$

et puisque l'inverse est unique, alors $(y^{-1} * x^{-1})$ est l'inverse de $x * y$, c.à.d $(x * y)^{-1} = y^{-1} * x^{-1}$. ■

2.2 Groupes et morphismes de groupes

2.2.1 Groupes

Définition 2.2.1 *On appelle groupe tout monoïde $(G,*)$ dont tous les éléments sont inversibles. Autrement dit $(G,*)$ est un groupe si la loi $*$ est associative, et admet un élément neutre e et tout élément de G est inversible (symétrisable).*
Si en plus $*$ est commutative, alors le groupe G est dit commutatif ou abélien.

Exemple 2.2.2
1) Les structures $(\mathbb{Q}^*,.),(\mathbb{R}^*,)(\mathbb{C},^*,.)$ sont des groupes commutatifs.
2) $(P(E),\cap)$ n'est pas un groupe, puisque l'inverse de ϕ n'existe pas.
3) Si E un ensemble. On note $\sigma(E)$ l'ensemble des bijections de E dans E. Alors $(\sigma(E),\circ)$ est un groupe (en général non abélien).
4) $(\mathbb{Z}/n\mathbb{Z},+)$ où $n\in\mathbb{N}^*$ est un groupe abélien.

Définition 2.2.3 *On dit qu'un groupe $(G,*)$ est fini si l'ensemble G est fini. Dans ce cas, le cardinal de G est appelé ordre de G et noté $ord(G)$ ou $|G|$.*

Exemple 2.2.4 *$G=(\mathbb{Z}/n\mathbb{Z},+)$ où $n\in\mathbb{N}^*$ est un groupe fini d'ordre n.*

Définition 2.2.5 ***Puissances entières dans un groupe :***
Soit $(G,*)$ un groupe, $n\in\mathbb{Z}$ et $a\in G$. On définit les puissance entières ($n^{ème}$) de a de la façon suivante

$$\begin{cases} a^0=e \\ a^n=a*a^{n-1}, n>0 \\ a^n=(a^{-n})^{-1}, n<0 \end{cases}$$

Pour n strictement positif, on a donc $a^n=\underbrace{a*a*...*a}_{n\ fois}$ et pour n strictement négatif, $a^n=\underbrace{a^{-1}*a^{-1}*...*a^{-1}}_{n\ fois}$.
Si la loi est notée additivement, alors on note na au lieu de a^n. On a alors

$$\begin{cases} 0a=e \\ na=a+(n-1)a, n>0 \\ na=-(-na), n<0 \end{cases}$$

On obtient ainsi les "règles de calcul" suivantes :

$$\forall x,y \in (G,.), \forall m,n \in \mathbb{Z} : \begin{cases} x^n x^m = x^{n+m} = x^{m+n} = x^m x^n \\ (x^n)^m = x^{nm} = x^{mn} = (x^m)^n \end{cases}$$

$$\forall x,y \in (G,+), \forall m,n \in \mathbb{Z} : \begin{cases} (n+m)\,x = nx + mx \\ (nm)\,x = n\,(mx) \end{cases}$$

Définition 2.2.6 *On appelle sous groupe d'un groupe $(G,*)$ toute partie non vide H de G qui est elle même un groupe pour la loi restreinte à H. Autrement dit H est sous groupe de $(G,*)$ si et si*

$$\begin{cases} i) e \in H \\ ii) \forall x \in H : x^{-1} \in H \\ iii) \forall x,y \in H : x * y \in H \end{cases}$$

Exemple 2.2.7

1) *Si $(G,*)$ est un goupe, alors $\{e\}$ et G sont des sous groupes de G appelés sous groupes trivaux.*

2) *$(\{-1,1\},\cdot)$ est un sous groupe de groupe $(\mathbb{R}^*,\cdot)$.*

3) *Les sous groupes de $(\mathbb{Z},+)$ sont $n\mathbb{Z} = \{na, a \in \mathbb{Z}\}$ où $n \in \mathbb{N}^*$.*

Proposition 2.2.8 ***Caractérisation des sous groupes :***
Soient $(G,*)$ un groupe et H une partie non vide de G. Alors H est un sous groupe de G si et seulement si

$$\begin{cases} i) e \in H \\ ii) \forall x,y \in H : x * y^{-1} \in H \end{cases}$$

Preuve.

Soit H un sous groupe non vide de G et soit $(x,y)^2$. Alors y^{-1} est un élément de H et il en est de même du produit $x * y^{-1}$.

Soit H une partie non vide de G vérifiant $\forall x,y \in H : x * y^{-1} \in H$. Soit $x \in H$. On a : $e = x * x^{-1} \in H$ donc l'élément neutre de G est élément de H. Pour tout $(e,x) \in H^2, e * x^{-1} \in H$ donc $x^{-1} \in H$. Enfin, pour tout $(x,y) \in H^2$, on a $(x,y^{-1}) \in H$ et donc $x * (y^{-1})^{-1} = x * y \in H$. ■

Proposition 2.2.9 *Soient $(G,*)$ un groupe, $(H_i)_{i\in I}$ une famille de sous groupes de G. Alors $\bigcap_{i\in I} H_i$ est un sous groupe de G.*

Preuve. Notons $H = \bigcap_{i\in I} H_i$ et montrons que Hest un sous groupe de G. Utilisons la caractérisation précédente.

i) On a $\forall i \in I : e \in H_i$, donc $e \in H$.
ii)Soit $(x, y) \in H^2$. On a alors $(x, y) \in H_i^2, \forall i \in I$. Ce qui amène que $\forall i \in I : x * y^{-1} \in H_i$ car H_i est un sous-groupe de G. Ce qui amène aussi que $x * y^{-1} \in H$. Alors H est bien un sous-groupe de G. ■

Remarque 2.2.10 *En général, l'union quelconque de sous groupes d'un groupe $(G, *)$, n'est pas nécessairement un sous groupe de $(G, *)$. Par exemple*

$$G = (\mathbb{Z}, +), H_1 = 2\mathbb{Z}, H_2 = 3\mathbb{Z}$$

La proposition précédente permet la définition suivante :

Définition 2.2.11 ***Sous groupes engendrés***
Soit A une partie d'un groupe $(G, *)$. L'intersection de tous les sous groupes de G contenant A est un sous groupe de G, appelé sous groupe engendré par A et est noté $\langle A \rangle$. La partie A est appelée partie génératrice de $\langle A \rangle$. On a ainsi

$$\langle A \rangle = \bigcap_{\substack{H \ sg \ de \ G \\ H \subset G}} H$$

Théorème 2.2.12 *Soit A une partie d'un groupe $(G, *)$: Alors :*
1) $\langle A \rangle$ est le plus petit (Au sens de l'inclusion) sous groupe de $(G, *)$, contenant A.
2) Si $A = \phi$, alors $\langle A \rangle = \{e\}$.

Preuve.
1) On sait que $\langle A \rangle$ est l'intersection de tous les sous groupes contenant A, alors il contient A et $\langle A \rangle$ est un sous groupe de G. D'autre part, si un sous groupe H contient A, on a $H \cap \langle A \rangle = \langle A \rangle$, alors H contient $\langle A \rangle$, et $\langle A \rangle$ est le plus petit des sous groupes contenant A.
2) Si $A = \phi$, il est clair que $\{e\}$ contient A et c'est le plus petit sous groupe de G, donc $\langle A \rangle = \{e\}$. ■

Théorème 2.2.13 *Soit A une partie non vide d'un groupe $(G, *)$: Alors :*
$\langle A \rangle = \left\{a_1 * a_2 * ... * a_p : p \in \mathbb{N}^* \text{ et } a_i \in A \text{ ou } a_i^{-1} \in A, i \in \{1, 2, ..., p\}\right\}$ *c'est-à-dire l'ensemble des composés multiples des éléments de A et de symétriques d'éléments de A.*

Preuve. Soit

$$H = \left\{a_1 * a_2 * ... * a_p : p \in \mathbb{N}^* \text{ et } a_i \in A \text{ ou } a_i^{-1} \in A, i \in \{1, 2, ..., p\}\right\}$$

Nous allons montrer que H est un sous groupe de G et H est le plus petit sous groupe de G.
Puisque $A \neq \phi$, il existe $a_1 \in A$, et donc $e = a_1 * a_1^{-1}$, alors l'élément neutre $e \in H$.
Soient

$$\begin{aligned} x &= a_1 * a_2 * ... * a_p \in H, p \in \mathbb{N}^* \\ y &= b_1 * b_2 * ... * b_{p'} \in H, p' \in \mathbb{N}^* \end{aligned}$$

On pose

$$d_k = \begin{cases} a_k, & \text{si } 1 \leq k \leq p \\ b_{k-p}, & \text{si } p+1 \leq k \leq p+p' \end{cases}$$

Alors

$$x * y = (a_1 * a_2 * ... * a_p) * (b_1 * b_2 * ... * b_{p'}) = d_1 * d_2 * ... * d_{p+p'} \in H$$

Soit $x = a_1 * a_2 * ... * a_p \in H, p \in \mathbb{N}^*$, alors

$$\begin{cases} a_1^{-1}, a_2^{-1}, ..., a_p^{-1} \in A \\ x^{-1} = (a_1 * a_2 * ... * a_p)^{-1} = a_p^{-1} * a_{p-1}^{-1} * ... * a_1^{-1} \in H \end{cases}$$

Donc H est un sous groupe de G.
D'autre part, on a $A \subset H$. Par conséquent $\langle A \rangle \subset H$.
Inversement,tous les éléments de la forme $a_1 * a_2 * ... * a_p$ appartiennent à tout sous groupe contenant A, alors ils appartiennent à $\langle A \rangle$, d'où l'inclusion $H \subset \langle A \rangle$ et par suite l'égalité $H = \langle A \rangle$. ■

Définition 2.2.14
1) Un groupe engendré par une partie A finie est appelé groupe de type fini.
2) Un groupe engendré par un seul élément a (C.à.d $A = \{a\}$) est appelé groupe monogène noté $\langle a \rangle$ et a un générateur de $\langle a \rangle$. Dans ce cas, on a

$$\begin{cases} \langle a \rangle = \{..., a^{-2}, a^{-1}, a^0 = e, a, a^2, ...\} = \{a^m, m \in \mathbb{Z}\} \\ ou \\ \langle a \rangle = \{..., -2a, -a, 0a = e, a, 2a, ...\} = \{ma, m \in \mathbb{Z}\}, \text{ si la loi } * \text{ est additive.} \end{cases}$$

3) Un groupe monogène fini, est appelé groupe cyclique.

Exemple 2.2.15
1) Le groupe $(\mathbb{Z}, +)$ est un groupe monogène, car $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. En effet, pour tout

$n \in \mathbb{Z}$, on a

$$n = \begin{cases} \underbrace{1+1+...+1}_{n\ fois}, n > 0 \\ 0 = 1 + (-1) \\ \underbrace{(-1)+(-1)+...+(-1)}_{-n\ fois}, n < 0 \end{cases}$$

2) Pour tout $n \in \mathbb{N}^*, (\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique.$\mathbb{Z}/n\mathbb{Z} = \langle \dot{1} \rangle$.

Définition 2.2.16 ***Ordre d'un élément*** *:*
Soit $(G, *)$ un groupe d'élément neutre e. On appelle ordre d'un élément a de G, et on note $ord(a)$, l'ordre de $\langle a \rangle$.

$$ord\,(a) = Card\,(\langle a \rangle)$$

On a deux cas possibles.
1^{er} cas : il existe $k \in \mathbb{N}^*, a^k = e$, alors $ord(a)$ est fini et c'est le plus petit $k \in \mathbb{N}^*$ vérifiant $a^k = e$ ou 0_G dans le cas additif.

$$ord\,(a) = \min\left\{k \in \mathbb{N}^* : a^k = e\right\}$$

$2^{ème}$ cas : pour tout $k \in \mathbb{N}^*$, $a^k \neq e$, alors $ord(a)$ est infini.

Remarque 2.2.17 *Si $(G, *)$ est un groupe d'élément neutre e et $a \in G$. Alors*

$$ord\,(a) = k \Longleftrightarrow \begin{cases} a^k = e \\ \forall i \in \mathbb{N} : a^i = e \Longrightarrow k \mid i \end{cases}$$

Exemple 2.2.18
1) $ord\,(e_G) = 1$.
2) Si $G = \{-1, 1\}$ muni de la multiplication, alors $ord\,(-1) = 2$.
3) Dans le groupe $(\mathbb{Z}, +)$, on a $ord\,(1) = \infty = ord\,(-1)$ et $ord\,(0) = 1$.

2.2.2 Morphismes de Groupes

Définition 2.2.19 *Soient $(G_1, *), (G_2, \top)$ deux groupes et $f : (G_1, *) \longrightarrow (G_2, \top)$ une application,on dit que f est un morphisme de groupe G_1 dans G_2 si et seulement si*

$$\forall x, y \in G_1 : f\,(x * y) = f\,(x) \top f\,(y)$$

On dit de plus que f est un :
Endomorphisme lorsque $G_1 = G_2$ et $* = \top$.

Isomorphisme lorsque f est bijective. On dit que G_1 et G_2 sont isomorphe, $G_1 \approx G_2$.
Automorphisme lorsque f est un endomorphisme bijective.

Exemple 2.2.20
1) L'application $f : (\mathbb{C}^*, .) \longrightarrow (\mathbb{R}^*, .)$ telle que $f(z) = |z|$ est un morphisme de groupes. Car

$$\forall z, z' \in \mathbb{C}^* : f(z.z') = |z.z'| = |z|.|z'| = f(z).f(z')$$

2) L'application $f : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^*, .)$ telle que $f(x) = e^x$ est un isomorphisme de groupes. Car

$$\forall x, y \in \mathbb{R} : f(x+y) = e^{x+y} = e^x.e^y = f(x).f(y)$$

3) Pour tout élément a d'un groupe $(G, *)$, l'application $f_a : (G, *) \longrightarrow (G, *)$ telle que $f_a(x) = a * x * a^{-1}$ est un automorphisme du groupe $(G, *)$.

Proposition 2.2.21 *Soit $f : (G, *) \longrightarrow (G', T)$ un morphisme du groupes, alors*
1) $f(e) = e'$ (e et e' sont respectivement les éléments neutres de G et G').
2) Pour tout $x \in G : f(x^{-1}) = (f(x))^{-1}$.

Preuve.
1) On a $f(e) T f(e) = f(e * e) = f(e) = f(e) T e' = e' T f(e)$, alors $f(e) = e'$.
2) Soit $x \in G$, alors

$$\begin{cases} f(x) T f(x^{-1}) = f(x * x^{-1}) = f(e) = e' \\ f(x^{-1}) T f(e) = f(x^{-1} * x) = f(e) = e' \end{cases} \Longrightarrow f\left(x^{-1}\right) = (f(x))^{-1}$$

■

Proposition 2.2.22 *Si $f : (G_1, *) \longrightarrow (G_2, \mathsf{T})$ et $g : (G_2, \mathsf{T}) \to (G_3, \triangle)$ deux morphismes de groupes ,alors $g \circ f : (G_1, *) \to (G_3, \triangle)$ est un morphisme de groupes.*

Preuve. Soit $x, y \in G_1$, alors

$$\begin{aligned} (g \circ f)(x * y) &= g(f(x * y)) \\ &= g(f(x) \mathsf{T} f(y)) \\ &= g(f(x)) \triangle g(f(y)) \\ &= (g\circ) f(x) \triangle (g \circ f)(y) \end{aligned}$$

Donc $g \circ f$ est un morphisme de groupes. ■

Proposition 2.2.23 *Si $f : (G_1,) \longrightarrow (G_2, \mathsf{T})$ est un isomorphisme de groupes, alors $f^{-1} : (G_2, \mathsf{T}) \longrightarrow (G_{1,*})$ est un isomorphisme de groupe.*

Preuve. Supposons que f est un isomorphisme de groupes, alors f est bijective. Par conséquent f^{-1} existe est bijective. Montrons que f^{-1}est un morphisme de groupes. Soient $y, y' \in G_2$, alors

$$y, y' \in G_2 \Longrightarrow \begin{cases} y = f(x), x \in G_1 \\ y' = f(x'), x' \in G_1 \end{cases}$$

On obtient

$$f\left(f^{-1}(y) * f^{-1}(y')\right) = f\left(f^{-1}(y)\right) \intercal f\left(f^{-1}(y')\right)$$

$$\begin{aligned} &\Longrightarrow \quad f\left(f^{-1}(y) * f^{-1}(y')\right) = y \intercal y' \\ &\Longrightarrow \quad f\left(f^{-1}(y) * f^{-1}(y')\right) = f\left(f^{-1}(y \intercal y')\right) \end{aligned}$$

Or f est injective, alors

$$f^{-1}(y \intercal y') = f^{-1}(y) * f^{-1}(y')$$

■

Définition 2.2.24 *Soit $f : G_1 \longrightarrow G_2$ un morphisme de groupes. On note e_1 l'élément neutre de groupe G_1 et e_2 l'élément neutre de groupe G_2. Alors*
1) On appelle noyau de f, et on note $\ker(f)$ *l'ensemble*

$$\ker(f) = \{x \in G_1 : f(x) = e_2\} = f^{-1}\{e_2\}$$

2) On appelle image de f, et on note $\mathrm{Im}(f)$ *l'ensemble*

$$\mathrm{Im}(f) = \{y \in G_2 : \exists x \in G_1, f(x) = y\} = f(G_1)$$

Proposition 2.2.25 *Soit $f : (G_1, *) \longrightarrow (G_2, \intercal)$ un morphisme de groupe. Alors*
1) L'image directe d'un sous-groupe de G_1 par f est un sous-groupe de G_2. En particulier $\mathrm{Im}(f)$ *est un sous groupe de G_2.*
2) L'image réciproque d'un sous-groupe de G_2 par f est un sous-groupe de G_1. En particulier $\ker(f)$ *est un sous groupe de G_1.*

Preuve. Soient H_1 un sous groupe de G_1, H_2 un sous groupe de G_2. Alors
1) Soit H_1 est un sous groupe de G_1, alors $e_1 \in H_1$ donc $e_2 = f(e_1) \in f(H_1)$.
Soient y et y' dans $f(H_1)$, alors il existe x et x' dans H_1 tels que $f(x) = y$ et $f(x') = y'$.
Or f est un morphisme, on a

$$y \intercal y'^{-1} = f(x) \intercal (f(x'))^{-1} = f(x) \intercal f\left(x'^{-1}\right) = f\left(x * x'^{-1}\right) \in f(H_1)$$

car $x * x'^{-1} \in H_1$.
Or G_1 est un sous groupe de G_1, alors $\mathrm{Im}(f) = f(G_1)$ est un sous groupe de G_2.
2) Soit H_2 est un sous groupe de G_2, alors $e_2 = f(e_1)$ et $e_2 \in H_2$ donc $e_1 \in f^{-1}(H_2)$.
Soient x et x' dans $f^{-1}(H_2)$. On a

$$f\left(x * x'^{-1}\right) = f(x) \top f\left(x'^{-1}\right) = f(x) \top (f(x'))^{-1} \in H_2$$

Donc car $x * x'^{-1} \in H_2$.
Or $\{e_2\}$ est un sous groupe de G_2, alors $f^{-1}(\{e_2\}) = \ker(f)$ est un sous groupe de G_1.
■

Théorème 2.2.26 *Soit $f : (G_1, *) \longrightarrow (G_2, \top)$ un morphisme de groupes. Alors*
1) f est injective si et seulement si $\ker(f) = \{e_1\}$.
2) f est surjective si et seulement si $\mathrm{Im}(f) = G_2$.

Preuve.
1) Supposons que f est injectif. Comme f est un morphisme, on a $e_1 \in \ker(f)$. Comme f est injectif, alors e_1 est le seul élément de e_2 dans G_1, ce qui prouve que $\ker f = \{e_1\}$.
Réciproquement, supposons que $\ker f = \{e_1\}$. Soient $x, y \in G_1$ tel que $f(x) = f(y)$. Montrons que $x = y$. On multiplie à droite l'égalité $f(x) = f(y)$ par $(f(y))^{-1}$. On obtient

$$f(x) \top (f(y))^{-1} = f(y) \top (f(y))^{-1} = e_2$$

D'après les propriétés des morphismes de groupes, on a $f(x * y^{-1}) = e_2$. Donc $x * y^{-1} \in \ker(f)$ et forcément $x * y^{-1} = e_1$. On multiplie à droite par y les deux membres de cette égalité et on obtient $x = y$, ce qui prouve que f est injectif.
2) La preuve de cette propriété est immédiate, sachant que $\mathrm{Im}(f) = f(G_1)$. ■

Chapitre 3

Groupe symétrique

Le but de ce chapitre est de donner une étude générale de groupe de permutations

3.1 Premières notions

Définition 3.1.1 *Soit E un ensemble quelconque fini de cardinal $n \in \mathbb{N}^*$. Une permutation ou une substitution de E est une bijection de E vers lui même. L'ensemble des permutations de E est noté $S(E)$. En particulier, si $E = \{1, 2, ..., n\}$ tel que $n \in \mathbb{N}^*$, alors on note S_n l'ensemble des permutations sur $\{1, .., n\}$.*

Définition 3.1.2 *Soit E un ensemble. On appelle groupe symétrique de E l'ensemble des applications bijectives de E sur E muni de la composition d'applications $\circ$. On le note $S(E)$. Un cas particulier courant est le cas où E est l'ensemble fini $E = \{1, 2, ..., n\}$, $n \in \mathbb{N}^*$, on note alors S_n le groupe symétrique de cet ensemble. Les éléments de S_n sont appelés permutations et S_n est appelé groupe des permutations d'ordre n ou groupe symétrique d'indice n.*
On note les éléments de S_n par σ.

Notation 3.1.3 *Lorsque E est fini, une permutation α de E peut être représentée par un tableau parenthésé à deux lignes, la première énumérant les éléments de E et la seconde les images par σ des éléments de la première ligne (dans le même ordre). Alors pour toute permutation $\sigma \in S_n$, on note*

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

pour signifier que σ est la bijection $\sigma : k \in E \longmapsto \sigma(k)$.

Exemple 3.1.4 *Soit $\sigma \in S_6$ définie par $\sigma(1) = 2, \sigma(2) = 4, \sigma(3) = 5, \sigma(4) = 6, \sigma(5) = 3, \sigma(6) = 1$, alors σ se note*

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

Définition 3.1.5 ***Permutation identité***
Si une permutation laisse le premier élément à la première place, le deuxième élément à la deuxième place, et ainsi de suite, alors elle ne change pas du tout la position des éléments. Cette permutation est l'application identique, et elle est appelée permutation identique. Elle est le plus souvent notée $e = Id$ où

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

Définition 3.1.6 ***Produit ou Composition de permutations***
Les permutations de E sont définies comme des applications de E dans E, il est donc possible de définir leur produit de composition, qui se note $\circ$. Donc la composition (ou produit) de deux permutations σ_1 et σ_2 de S_n est la permutation $\sigma = \sigma_1 \circ \sigma_2$ obtenue en appliquant σ_2 puis σ_1 au résultat :

$$\forall i \in \{1, 2, ..., n\} : (\sigma_1 \circ \sigma_2)(i) = \sigma_1(\sigma_2(i))$$

C'est à dire

$$\begin{cases} \sigma_1 = \begin{pmatrix} 1 & 2 & ... & k & ... & n \\ \sigma_1(1) & \sigma_1(2) & ... & \sigma_1(k) & ... & \sigma_1(n) \end{pmatrix} \\ \sigma_2 = \begin{pmatrix} 1 & 2 & ... & k & ... & n \\ \sigma_2(1) & \sigma_2(2) & ... & \sigma_2(k) & ... & \sigma_2(n) \end{pmatrix} \end{cases}$$
$$\Longrightarrow \quad \sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & ... & k & ... & n \\ \sigma_1(\sigma_2(1)) & \sigma_1(\sigma_2(2)) & ... & \sigma_1(\sigma_2(k)) & ... & \sigma_1(\sigma_2(n)) \end{pmatrix}$$

Exemple 3.1.7 *Soient $\sigma_1, \sigma_2 \in S_5$ telles que*

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix}$$

alors

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$$

Remarque 3.1.8 *En général, le produit de deux permutations n'est pas commutatif, par exemple*

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \in S_5$$

alors

$$\begin{aligned} \sigma_1 \circ \sigma_2 &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix} \\ &\neq \sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix} \end{aligned}$$

Définition 3.1.9 *Pour toute permutation $\sigma \in S_n$ et tout entier relatif r, la permutation σ^r de E est définie par*

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

Définition 3.1.10 ***Permutation inverse***
La permutation inverse (ou réciproque) de la permutation σ de S_n est la permutation σ^{-1} telle que $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = Id$. Elle s'obtient en échangeant positions et éléments dans σ

$$\forall i \in \{1, 2, ..., n\} : \sigma^{-1}(\sigma(i)) = i$$

Remarque 3.1.11 *Toutes les permutations sont inversibles.*

Exemple 3.1.12 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \in S_5$, *alors* $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}$, *car*

$$\begin{cases} (\sigma \circ \sigma^{-1})(1) = 1 \\ (\sigma \circ \sigma^{-1})(2) = 2 \\ (\sigma \circ \sigma^{-1})(3) = 3 \\ (\sigma \circ \sigma^{-1})(4) = 4 \\ (\sigma \circ \sigma^{-1})(5) = 5 \end{cases} \Longrightarrow \begin{cases} \sigma(\sigma^{-1}(1)) = 1 \\ \sigma(\sigma^{-1}(2)) = 2 \\ \sigma(\sigma^{-1}(3)) = 3 \\ \sigma(\sigma^{-1}(4)) = 4 \\ \sigma(\sigma^{-1}(5)) = 5 \end{cases} \Longrightarrow \begin{cases} \sigma^{-1}(1) = 4 \\ \sigma^{-1}(2) = 2 \\ \sigma^{-1}(3) = 1 \\ \sigma^{-1}(4) = 5 \\ \sigma^{-1}(5) = 3 \end{cases}$$

Définition 3.1.13 *Soit $\sigma \in S_n$. On appelle point fixe de σ, tout élément $k \in \{1, 2, ..., n\}$ tel que $\sigma(k) = k$.*

Proposition 3.1.14 *Soit $n \in \mathbb{N}^*$, alors S_n muni de la composition des applications $\circ$, forme un groupe, appelé le groupe symétrique de $E = \{1, ..., n\}$. Qu'on note (S_n, o).*

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

$$\begin{array}{rccc} \circ : & S_n \times S_n & \longrightarrow & S_n \\ & (f, g) & \longmapsto & f \circ g \end{array}$$

est une loi de composition interne dans S_n.
L'élément neutre de S_n est l'application identité Id. En effet, pour tout $f \in S_n$ et pour tout $x \in E$, on a

$$(f \circ Id_E)(x) = f(x) = (Id_E \circ f)(x)$$

d'où $f \circ Id_E = Id_E \circ f$.
Comme $f \in S_n$ est bijective, alors son application inverse f^{-1} existe, c'est aussi une permutation de E.
On sait que la composition des applications est une loi associative. Donc (S_n, o) est un groupe. ■

Proposition 3.1.15 *Soit $n \in \mathbb{N}^*$, alors S_n est un groupe fini d'ordre $n!$. Si $n \geq 3$, S_n est un groupe non commutatif.*

Preuve. Une permutation de S_n est entièrement déterminée par les images de $1, ..., n$, qui sont des éléments distincts de $1, ..., n$. Pour compter le nombre d'éléments σ de S_n, observons que pour l'image de 1, il y a n choix, pour l'image de 2, il y a $n-1$ choix (car $\sigma(2) \notin \{\sigma(1)\}$), pour l'image de 3, il y a $n-2$ choix (car $\sigma(3) \notin \{\sigma(1), \sigma(2)\}$), et ainsi de suite, enfin pour l'image de n, il y a 1 choix (car $\sigma(n) \notin \{\sigma(1), \sigma(2), ..., \sigma(n-1)\}$). Donc au total, il y a $n(n-1)...2.1 = n!$ permutations de $\{1, ..., n\}$, c'est l'ordre du groupe S_n.
Soient $n \geq 3$, i, j et k trois éléments distincts de $\{1, ..., n\}$. Soit σ_1 une application bijective qui à i associe j, à j associe i et qui fixe k. Soit σ_2 une application bijective qui à i associe k, à k associe i et qui fixe j. C-à-dire

$$\begin{cases} \sigma_1(i) = j, \sigma_1(j) = i, \sigma_1(k) = k \\ \sigma_2(i) = k, \sigma_2(k) = i, \sigma_2(j) = j \end{cases}$$

Alors

$$\begin{cases} (\sigma_1 \circ \sigma_2)(i) = k \\ (\sigma_2 \circ \sigma_1)(i) = j \end{cases} \Longrightarrow \sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$$

et par conséquent S_n n'est pas abélien. ■

Exemple 3.1.16 *Prenons par exemple dans S_4 :*

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

On a

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \neq \sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Proposition 3.1.17 *(S_1, o) et (S_2, o) sont abéliens.*

Preuve. On a $S_1 = \{Id\}$ donc S_1 est abélien. S_2 est composé de l'identité Id et de la permutation échangeant 1 et 2, donc S_2 est abélien. ■

Proposition 3.1.18 *Le groupe symétrique $S(E)$ d'un ensemble quelconque de cardinal n est isomorphe à S_n .*

Preuve. On a E est un ensemble fini de cardinal n, alors (d'après les ensembles de cardinal fini) il existe une bijection f de E sur $E_n = \{1, 2, ..., n\}$. On considère l'application g définie par

$$\begin{array}{rccl} g: & S(E) & \longrightarrow & S_n \\ & \sigma & \longmapsto & g(\sigma) = f^{-1} \circ \sigma \circ f \end{array}$$

L'application g est un isomorphisme de groupes. En effet :
Il est clair que $S(E)$ et S_n sont deux groupes.
Or f^{-1}, σ, f sont des applications bijectives, alors g est bijective.
Soient $\sigma_1, \sigma_2 \in S(E)$. Alors

$$\begin{array}{rcl} g(\sigma_1 \circ \sigma_2) & = & f^{-1} \circ (\sigma_1 \circ \sigma_2) \circ f = f^{-1} \circ \left(\sigma_1 \circ \left(f \circ f^{-1}\right) \circ \sigma_2\right) \circ f \\ & = & \left(f^{-1} \circ \sigma_1 \circ f\right) \circ \left(f^{-1} \circ \sigma_2 \circ f\right) = g(\sigma_1) \circ g(\sigma_2) \end{array}$$

Alors g est un morphisme de groupes. Par conséquent $S(E)$ et S_n sont isomorphes. ■

En conséquence, il suffit de connaître les propriétés du groupe S_n pour en déduire celles du groupe $S(E)$. C'est pourquoi la suite de ce travail ne portera que sur S_n.

Définition 3.1.19 *Soit σ un élément de S_n. On appelle support de σ et on note $supp(\sigma)$, l'ensemble des éléments i de $E = \{1, 2, ..., n\}$ tels que $\sigma(i) \neq i$.*

$$supp(\sigma) = \{i \in \{1, 2, ..., n\} : \sigma(i) \neq i\} \subset E$$

Si $i \notin supp(\sigma)$, alors i est un point fixe de σ.

Exemple 3.1.20
1) Le support de l'identité est l'ensemble vide.
2) Le support $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 6 & 4 & 2 & 5 \end{pmatrix} \in S_6$ *est* $supp(\sigma) = \{2, 3, 5, 6\}$.

Proposition 3.1.21 *Soient* $\sigma \in S_n$, $A = supp(\sigma)$. *Alors* A *est stable par* σ *et on peut identifier* σ *à une permutation sur* A *ou n'importe quelle partie* B *telle que* $A \subset B \subset E = \{1, 2, .., n\}$.

Preuve. Soit $i \in A$, alors $\sigma(i) \neq i$. Or σ est injective, alors

$$\sigma(\sigma(x)) \neq \sigma(x) \Longrightarrow \sigma(i) \in supp(\sigma) = A$$

Alors A est stable par σ. Ainsi $\sigma_{/A}$ définit une bijection de A dans A (loi induite). On peut donc considérer que $\sigma_{/A} \in S(A)$. ■

Exemple 3.1.22 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 3 & 1 & 5 & 6 & 7 \end{pmatrix} \in S_7$. *Alors on peut considérer que* $\sigma \in S_4$ *ou même* $S(A = \{1, 4\})$.

Proposition 3.1.23 *Si deux éléments de* S_n *ont leurs supports disjoints alors ils commutent.*

Preuve. Notons S_1 le support de σ_1 et S_2 le support de σ_2. Alors $S_1 \cap S_2 = \phi$. Nous voulons montrer que

$$\forall i \in E = \{1, 2, ..., n\} : (\sigma_1 \circ \sigma_2)(i) = (\sigma_2 \circ \sigma_1)(i)$$

Distinguons les cas suivant :
Si $i \in E - S_1 \cup S_2$, alors

$$\begin{cases} (\sigma_1 \circ \sigma_2)(i) = \sigma_1(\sigma_2(i)) = \sigma_1(i) = i \\ (\sigma_2 \circ \sigma_1)(i) = \sigma_2(\sigma_1(i)) = \sigma_2(i) = i \end{cases} \Longrightarrow \sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$$

Si $i \in S_1 \cup S_2$: alors
Si $i \in S_1$, alors d'après la proposition (3.1.21), on a $\sigma_1(i) \in S_1$ et comme S_1 et S_2 sont disjoints, alors $i, \sigma_1(i) \notin S_2$. D'où $\sigma_1(\sigma_2(i)) = \sigma_1(i)$ et $\sigma_2(\sigma_1(i)) = \sigma_1(i)$. On obtient $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.
Le cas où $i \in S_2$ est analogue. Dans tous les cas σ_1 et σ_2 commutent. ■

Remarque 3.1.24 *La réciproque est fausse. Par exemple les permutations* $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *et* $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ *commutent et elles ont le même support* $\{1,2,3\}$.

Corollaire 3.1.25 *Si* $\sigma \in S_n$, *alors* $supp(\sigma) = supp(\sigma^{-1})$.

Preuve. Soit $i \in E$, tel que $i \in supp(\sigma)$, alors

$$\begin{aligned} \sigma(i) \neq i &\Longrightarrow \sigma^{-1}(\sigma(i)) \neq \sigma^{-1}(i) \\ &\Longrightarrow i \neq \sigma^{-1}(i) \\ &\Longrightarrow i \in supp\left(\sigma^{-1}\right) \end{aligned}$$

Puisque σ^{-1} est injective. D'autre part, on a

$$\begin{aligned} i \in supp\left(\sigma^{-1}\right) &\Longrightarrow i \neq \sigma^{-1}(i) \\ &\Longrightarrow \sigma(i) \neq \sigma\left(\sigma^{-1}(i)\right) \\ &\Longrightarrow \sigma(i) \neq i \\ &\Longrightarrow i \in supp(\sigma) \end{aligned}$$

■

Définition 3.1.26 *Soient* $n \geq 2$, $i, j \in E = \{1, 2, ..., n\}$ *tel que* $i < j$. *On appelle transposition de* i *et* j *et on note* $\tau_{i,j}$ *ou* (ij) *une permutation de* S_n *définie par*

$$\begin{cases} \tau_{i,j}(i) = j \\ \tau_{i,j}(j) = i \\ \tau_{i,j}(k) = k, \forall k \in E - \{i, j\} \end{cases}$$

C'est-à-dire une transposition est une permutation qui échange deux éléments et laisse les autres inchangés.

Exemple 3.1.27 *Pour* $n = 5$, $\tau_{2,4} = (2,4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix}$.

Remarque 3.1.28

1) On pose par convention $\tau_{i,i} = Id$.

2) Une transposition vérifie $\tau_{i,j} \circ \tau_{i,j} = Id$ *et* $\tau_{i,j}^{-1} = \tau_{i,j}$ *. En effet :*

Montrons que $\forall k \in E : (\tau_{i,j} \circ \tau_{i,j})(k) = Id(k) = k$. *On distingue les cas suivants :*
Si $k \in E - \{i, j\}$, *alors*

$$\tau_{i,j}(k) = k \Longrightarrow (\tau_{i,j} \circ \tau_{i,j})(k) = k = Id(k)$$

Si $k = i$, *alors*

$$\tau_{i,j}(i) = j \Longrightarrow \tau_{i,j}(\tau_{i,j}(i)) = \tau_{i,j}(j) = i = Id(i)$$

Si $k = j$, *alors*

$$\tau_{i,j}(j) = i \Longrightarrow \tau_{i,j}(\tau_{i,j}(j)) = \tau_{i,j}(i) = j = Id(j)$$

De même pour $\tau_{i,j}^{-1}$.

3.2 Décomposition en produit de transpositions

Théorème 3.2.1 *Les transpositions engendrent le groupe symétrique* S_n.

Cela signifie que toute permutation appartenant à S_n est la composée d'un nombre fini de transpositions appartenant à S_n. Autrement dit toute permutation peut s'exprimer comme le produit de transpositions (ou d'inverse de transpositions, mais on remarque que les transpositions sont involutives).

Preuve. Faisons la preuve par récurrence sur n :
1) Pour $n = 2$. On a deux permutations. C'est-à-dire $S_2 = \{\sigma_1 = Id, \sigma_2 = \tau_{1,2}\}$. Alors

$$\begin{aligned} \sigma_1 &= Id = \tau_{1,2} \circ \tau_{1,2} = \tau_{1,2}^2 \\ \sigma_2 &= \tau_{1,2} \end{aligned}$$

Donc $\tau_{1,2}$ engendre S_2.
Supposons le théorème vrai à l'ordre n. Autrement dit les transpositions de $E = \{1, 2, ..., n\}$ engendrent S_n et soit $\sigma \in S_{n+1}$, alors on a deux cas possibles :

1^{er}cas : $\sigma(n+1) = n+1$:
Comme σ est bijective, alors (proposition 3.1.21) on définit (une restriction de σ sur $E = \{1, 2, ..., n\}$)

$$\begin{array}{rccc} \sigma' : & \{1, 2, ..., n\} & \longrightarrow & \{1, 2, ..., n\} \\ & k & \longmapsto & \sigma'(k) = \sigma(k) \end{array}$$

σ' est une permutation appartenant à S_n et par hypothèse de récurrence elle s'écrit comme composée de transpositions appartenant à S_n. C'est-à-dire il existe $N \in \mathbb{N}^*$ et des trans-

positions $T'_1, T'_2, ..., T'_N$ telles que

$$\sigma' = T'_1 \circ T'_2 \circ ... \circ T'_N$$

En notant pour chaque $r \in \{1, 2, ..., n+1\}$, on définit l'application (un prolongement)

$$\begin{array}{rccl} T_r : & \{1,2,...,n+1\} & \longrightarrow & \{1,2,...,n+1\} \\ & k & \longmapsto & T_r(k) = \begin{cases} T'_r(k), \text{ si } 1 \leq k \leq n \\ n+1, \text{ si } k = n+1 \end{cases} \end{array}$$

Il est clair que $T_1, T_2, ..., T_N$ sont des transpositions de $\{1, 2, ..., n+1\}$ et que $\sigma = T_1 \circ T_2 \circ ... \circ T_N$.

$2^{ème}$ cas : $\sigma(n+1) \neq n+1$ (ie : $\sigma(n+1) = m$) :
On considère une permutation $p = \tau_{n+1,\sigma(n+1)} \circ \sigma$. On a $p \in S_{n+1}$ et

$$p(n+1) = \left(\tau_{n+1,\sigma(n+1)} \circ \sigma\right)(n+1) = \tau_{n+1,\sigma(n+1)}(\sigma(n+1)) = n+1$$

D'après l'étude de premier cas, il existe $N \in \mathbb{N}^*$ et des transposition $T_1, T_2, ..., T_N$ de $\{1, 2, ..., n+1\}$ telles que

$$p = T_1 \circ T_2 \circ ... \circ T_N$$

$$\begin{array}{ll} \Longrightarrow & \tau_{n+1,\sigma(n+1)} \circ \sigma = T_1 \circ T_2 \circ ... \circ T_N \\ \Longrightarrow & \sigma = \tau^{-1}_{n+1,\sigma(n+1)} \circ T_1 \circ T_2 \circ ... \circ T_N = \tau_{n+1,\sigma(n+1)} \circ T_1 \circ T_2 \circ ... \circ T_N \end{array}$$

puisque $\tau^{-1}_{n+1,\sigma(n+1)} = \tau_{n+1,\sigma(n+1)}$. Donc σ est un produit de transpositions de $\{1, 2, ..., n+1\}$.
■

Remarque 3.2.2 *La décomposition d'une permutation en composée de transpositions n'est pas unique.*

Exemple 3.2.3 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix} \in S_6$ *, alors on peut écrire* $\sigma = (12)(26)(45)$.
En effet

$$\begin{array}{rcl} (12)(26)(45) & = & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 4 & 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 4 & 5 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 5 & 4 & 6 \end{pmatrix} = \\ & = & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 3 & 5 & 4 & 1 \end{pmatrix} \end{array}$$

Définition 3.2.4 *Soient $\sigma \in S_n$ et $i \in E = \{1, 2, ..., n\}$. On appelle une orbite de i selon σ (ou σ-orbite de i) et on note $Orb_\sigma(i)$, $Orb(i)$ ou simplement $O_\sigma(i)$ l'ensemble des images de i par les itérés de σ c'est-à-dire*

$$O_\sigma(i) = \left\{\sigma^k(i) \in \{1, 2, ..., n\}, k \in \mathbb{N}\right\}$$

Exemple 3.2.5 *Soit* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix} \in S_6$ *, alors on a*

$$Orb(1) = \{1, 3, 5\} = Orb(3) = Orb(5), Orb(2) = \{2\}, Orb(4) = Orb(6) = \{4, 6\}$$

En effet :

$$\sigma^0(1) = 1, \sigma(1) = 5, \sigma^2(1) = \sigma(5) = 3, \sigma^3(1) = \sigma(3) = 1$$

Remarque 3.2.6
1) Si $\sigma \in S_n$ et $i \in E = \{1, 2, ..., n\}$, alors $Orb_\sigma(i) = \left\{\sigma^k(i) : k \in \{0, 1, ..., n-1\}\right\}$. Cela signifie qu'il suffit de calculer un nombre fini de $\sigma^k(i)$ pour avoir $Orb_\sigma(i)$. Ce nombre est au maximum n (de 0 à $n-1$), mais ce n'est pas forcément n. (Généralement k est l'ordre de σ).
2) Une orbite réduite à un élément (i.e. cardinal de $O_\sigma > 1$) est dite "triviale". Il y a autant d'orbites triviales que de points fixes par σ. En effet, si x est fixe par σ, alors $O_\sigma(x) = \left\{\sigma^k(x), k \in \mathbb{N}\right\} = \{x\}$.

Proposition 3.2.7 *Soient $\sigma \in S_n$ et $E = \{1, 2, ..., n\}$, alors la relation $\Re$ définie sur E par*

$$\forall x, y \in E : x \Re y \Longleftrightarrow y \in Orb_\sigma(x)$$

est une relation d'équivalence.

C'est-à-dire les σ-orbites sont des classes d'équivalences, elles forment donc une partition de E.

Preuve.
1) La réflexivité : On a $\forall x \in E : x = \sigma^0(x)$ donc $x \Re x$.
2) La symétrie : Soient $x, y \in E$ et soit m le plus petit entier non nul tel que $x = \sigma^m(x)$.

Alors

$$\begin{aligned} x\Re y &\Longrightarrow y \in Orb_{\sigma}(x) \\ &\Longrightarrow \text{il existe un entier } r \leq m \text{ tel que } y = \sigma^{r}(x) \\ &\Longrightarrow \text{il existe un entier } r \leq m \text{ tel que } \sigma^{m-r}(y) = \sigma^{m-r}(\sigma^{r}(x)) \\ &\Longrightarrow \text{il existe un entier } r \leq m \text{ tel que } \sigma^{m-r}(y) = \sigma^{m}(x) = x \\ &\Longrightarrow x \in Orb_{\sigma}(y) \\ &\Longrightarrow y\Re x \end{aligned}$$

3) La transitivité : Soient $x, y, z \in E$, alors

$$\begin{aligned} \left\{ \begin{array}{l} x\Re y \\ y\Re z \end{array} \right. &\Longrightarrow \left\{ \begin{array}{l} \text{il existe un entier } r \leq m \text{ tel que } y = \sigma^{r}(x) \\ \text{il existe un entier } s \leq m \text{ tel que } z = \sigma^{s}(y) \end{array} \right. \\ &\Longrightarrow z = \sigma^{s}(y) = \sigma^{s}(\sigma^{r}(x)) = \sigma^{s+r}(x) \\ &\Longrightarrow x \in Orb_{\sigma}(z) \\ &\Longrightarrow x\Re z \end{aligned}$$

■

Définition 3.2.8 *Soit $p \in \{2, 3, ..., n\}$. Une permutation de S_n est appelée un cycle si et seulement si elle ne possède qu'une seule orbite non réduite à un élément. C'est-à-dire un $p-$cycle dans S_n est une permutation $\sigma \in S_n$ telle que toute les orbites sont réduites un à singleton sauf une qui est de cardinal p. L'entier p est alors appelé la longueur du cycle.*

Exemple 3.2.9

1) Dans S_5, considérons $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 4 & 1 \end{pmatrix}$, on a $Orb_{\sigma_1}(1) = \{1, 2, 5\}, Orb_{\sigma_1}(3) = \{3\}, Orb_{\sigma_1}(4) = \{4\}$. Donc σ_1 est un cycle. Comme $Card(Orb_{\sigma_1}(1)) = 3$, alors on dit que σ_1 est un $3-$cycle et on le note $\sigma_1 = \begin{pmatrix} 1 & 2 & 5 \end{pmatrix}$.

2) Dans S_5, considérons $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$, on a $Orb_{\sigma_2}(1) = \{1, 2\}, Orb_{\sigma_2}(3) = \{3, 4, 5\}$. Donc σ_2 n' est pas un cycle.

Définition 3.2.10 *Soient $\sigma \in S_n$, avec $n \geq 2$. Soit $p \in \{2, 3, ..., n\}$.*
1) On dit que σ est un cycle de longueur p s'il existe p éléments $a_1, a_2, ..., a_p \in E =$

$\{1, 2, ..., n\}$ *distincts deux à deux tels que*

$$\begin{cases} \sigma(a_1) = a_2, \sigma(a_2) = a_3, ..., \sigma(a_{p-1}) = a_p, \sigma(a_p) = \sigma(a_1) \\ \sigma(b) = b, \forall b \in E - \{a_1, a_2, ..., a_p\} \end{cases}$$

$$\iff \begin{cases} \sigma(a_i) = a_{i+1}, \ si\ 1 \leq i \leq p-1 \\ \sigma(a_p) = a_1, \\ \sigma(b) = b, \ pour\ les\ autres\ valeurs\ de\ p \end{cases}$$

L'ensemble $\{a_1, a_2, ..., a_p\}$ *est appelé le support de* σ. *On écrit*

$$\sigma = \begin{pmatrix} a_1 & a_2 & ... & a_{p-1} & a_p & a_{p+1} & ... & a_n \\ a_2 & a_3 & ... & a_p & a_1 & a_{p+1} & ... & a_n \end{pmatrix}$$

2) Une telle permutation est aussi appelée $p-$*cycle ou cycle d'ordre* p. *En général, on représente un tel cycle en écrivant* $\sigma = \begin{pmatrix} a_1 & a_2 & ... & a_p \end{pmatrix}$.
3) Dans S_n, *un cycle de longueur* n *est appelé une permutation circulaire.*

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

4) Un $2-$*cycle est appelé une transposition.*

Remarque 3.2.11 *1)* $e = Id$ *n'est pas un cycle.*
2) Si $\sigma = \begin{pmatrix} a_1 & a_2 & ... & a_p \end{pmatrix}$, *alors* $\sigma^{-1} = \sigma = \begin{pmatrix} a_p & a_{p-1} & ... & a_1 \end{pmatrix}$.
3) Soit σ *un cycle de longueur* $p \geq 2$. *Alors* $\sigma^p = Id$ *et* $\forall k \in \{1, 2, ..., p-1\} : \sigma^k \neq Id$. *Pour cela il suffit de prendre* $m = qp + r$.
4) Si $\sigma = \begin{pmatrix} a_1 & a_2 & ... & a_p \end{pmatrix}$ *est un* p*-cycle alors il se décompose en produit de transpositions comme suit*

$$\sigma = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ ... \circ \begin{pmatrix} a_{p-1} & a_p \end{pmatrix}$$

Définition 3.2.12 *On dit que deux cycles* σ *et* σ' *dans* S_n *sont disjoints si leurs supports sont disjoints dans* E.

Proposition 3.2.13 *Deux cycles* σ_1 *et* σ_2 *de* S_n *à supports disjoints commutent.*

Preuve. Notons S_1 le support de σ_1 et S_2 le support de σ_2. Montrons que $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$. Soit $x \in E$, alors on distingue les cas suivants :
Si $x \in S_1$, alors il n'est pas dans le support de σ_2, donc $\sigma_2(x) = x$. Par conséquent,

$(\sigma_1 \circ \sigma_2)(x) = \sigma_1(x)$ et puisque $\sigma_1(x)$ est dans le support de σ_1, il n'est pas dans le support de σ_2 et donc $\sigma_2(\sigma_1(x)) = \sigma_1(x)$. De même, si x est dans le support de σ_2, on trouve $(\sigma_1 \circ \sigma_2)(x) = (\sigma_2 \circ \sigma_1)(x) = \sigma_2(x)$.
Si enfin x n'est ni dans le support de σ_1, ni dans le support de σ_2, il est invariant à la fois par σ_1 et σ_2 d'où $(\sigma_1 \circ \sigma_2)(x) = (\sigma_2 \circ \sigma_1)(x) = x$. ■

3.3 Décomposition en produits de cycles disjoints

Théorème 3.3.1 *Toute permutation de $E = \{1, 2, ..., n\}$ se décompose de manière unique (à l'ordre des facteurs près) en un produit de cycles à supports deux à deux disjoints de longueur supérieure ou égale à 2. C'est-à-dire, si $\sigma \in S_n$ tel que $\sigma \neq Id$. Alors il existe $k \geq 1$ et $c_1, c_2, ..., c_k$ des cycles de longueurs $l_i \geq 2$, à support deux à deux disjoints, tels que $\sigma = c_1 \circ c_2 \circ ... \circ c_k$.*

L'ordre des facteurs n'est pas important dans le produit, car les permutations à support disjoint commutent.

Preuve.

1) **Existence :** Faisons la preuve par récurrence sur n :
Pour $n = 2$. On a deux permutations. C'est-à-dire $S_2 = \{\sigma_1, \sigma_2\}$. Où $\sigma_1 = Id$ et σ_2 est le cycle $c = \begin{pmatrix} 1 & 2 \end{pmatrix}$. Alors

$$\begin{aligned} \sigma_1 &= Id = c \circ c = c^2 \\ \sigma_2 &= c \end{aligned}$$

Donc σ_2 engendre S_2.
Soient $n \geq 2$ et $\sigma \in S_{n+1}$, alors on a deux cas possibles :

1^{er}cas : $\sigma(n+1) = n+1$:
On raisonne comme la preuve de théorème (3.2.1). Comme σ est bijective, alors l'application induite

$$\begin{array}{rccc} \sigma' : & \{1, 2, ..., n\} & \longrightarrow & \{1, 2, ..., n\} \\ & k & \longmapsto & \sigma'(k) = \sigma(k) \end{array}$$

σ' est une permutation de $\{1, 2, ..., n\}$ et par hypothèse de récurrence elle s'écrit comme composée de cycles de $\{1, 2, ..., n\}$ deux à deux disjoints. C'est-à-dire il existe $v \in \mathbb{N}^*$ et des cycles $c'_1, c'_2, ..., c'_v$ tels que

$$\sigma' = c'_1 \circ c'_2 \circ ... \circ c'_v$$

En notant pour chaque $r \in \{1,2,...,v\}$, on définit l'application

$$\begin{array}{rccl} c_r: & \{1,2,...,n+1\} & \longrightarrow & \{1,2,...,n+1\} \\ & k & \longmapsto & c_r(k) = \begin{cases} c'_r(k), \text{ si } 1 \leq k \leq n \\ n+1, \text{ si } k = n+1 \end{cases} \end{array}$$

Il est clair que $c_1, c_2, ..., c_v$ sont des cycles deux à deux disjoints de $\{1,2,...,n+1\}$ et que $\sigma = c_1 \circ c_2 \circ ... \circ c_v$.

$2^{ème}$ cas : $\sigma(n+1) \neq n+1$:

Comme les $n+2$ entiers $n+1, \sigma(n+1), \sigma^2(n+1), ..., \sigma^{n+1}(n+1)$ sont dans $\{1,2,...,n+1\}$, il existe $(k,l) \in \{0,1,...,n+1\}^2$ tel que : $k < l$ et $\sigma^k(n+1) = \sigma^l(n+1)$. En notant $m = l-k$, on a $m \in \{1,2,...,n+1\}$ et $\sigma^m(n+1) = n+1$.

Ainsi l'ensemble $\{q \in \{1,2,...,n+1\} : \sigma^q(n+1) = n+1\}$ est une partie non vide de $\mathbb{N}^*$, donc admet un plus petit élément, noté p.

On a alors $\sigma^p(n+1) = n+1$.

D'autre part, les p entiers $n+1, \sigma(n+1), \sigma^2(n+1), ..., \sigma^{p-1}(n+1)$ sont deux à deux distincts car, s'il existait $(k,l) \in \{0,1,...,p-1\}^2$ tel que $k < l$ et $\sigma^k(n+1) = \sigma^l(n+1)$, alors on aurait, en notant $q = l-k$: $q \in \{1,2,...,n+1\}$, $\sigma^q(n+1) = n+1, q \leq p-1$, ce qui contredirait la définition de p.

Notons c le $p-$cycle $c = \begin{pmatrix} n+1 & \sigma(n+1) & ... & \sigma^{p-1}(n+1) \end{pmatrix}$ et $\rho = c^{-1} \circ \sigma$ de sorte que

$$\rho(n+1) = c^{-1}(\sigma(n+1)) = n+1$$

D'après l'étude du premier cas, il existe $v \in \mathbb{N}$ et des cycles $c_1, c_2, ..., c_v$ de $\{1,2,...,n+1\}$ à supports deux à deux disjoints, tels que $\rho = c_1 \circ c_2 \circ ... \circ c_v$.

Comme

$$\rho(n+1) = n+1, \rho(\sigma(n+1)) = \sigma(n+1), ..., \rho\left(\sigma^{p-1}(n+1)\right) = \sigma^{p-1}(n+1)$$

les supports des cycles $c_1, c_2, ..., c_v$ ne contiennent aucun des éléments $n+1, \sigma(n+1), ..., \sigma^{p-1}(n+1)$.

Finalement,

$$\sigma = c \circ c_1 \circ c_2 \circ ... \circ c_v$$

où $c, c_1, c_2, ..., c_v$ sont des cycles de $\{1,2,...,n+1\}$ à supports deux à deux disjoints.

2) **Unicité :** Soient

$$\sigma = c_1 \circ c_2 \circ ... \circ c_v = d_1 \circ d_2 \circ ... \circ d_{v'}$$

deux décomposition de σ en cycles à supports deux à deux disjoints. Remarquons d'abord que $c_1, c_2, ..., c_v$ commutent entre eux deux à deux et que $d_1, d_2, ..., d_{v'}$ commutent entre eux deux à deux.

Le cas où $\sigma = Id$ est immédiat.
Supposons que $\sigma \neq Id$. Alors il existe $i \in \{1, 2, ..., n\}$ tel que $\sigma(i) \neq i$, puis $r \in \{1, 2, ..., v\}$ et $r' \in \{1, 2, ..., v'\}$ tels que i soit dans le support de c_r et dans le support de $d_{r'}$. Comme dans le cas d'existence, alors il existe $p \in \mathbb{N}^*$ tel que

$$\begin{cases} i, \sigma(i), ..., \sigma^{p-1}(i) \text{ sont deux à deux distincts} \\ \sigma^p(i) = i \end{cases}$$

On a alors

$$c_r = d_r = \left(i, \sigma(i), ..., \sigma^{p-1}(i)\right)$$

En réitérant, on en déduit $v' = v$ et $\{c_1, c_2, ..., c_v\} = \{d_1, d_2, ..., d_{v'}\}$. ■

Exemple 3.3.2 *On a*

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

Remarque 3.3.3 ***Méthode :*** *Comment trouver la décomposition d'une permutation en cycles à supports disjoints ?*
Soit σ une permutation donnée dans S_n. Pour trouver sa décomposition :
1) Prendre un entier k entre 1 et n
2) Calculer $\sigma(k), \sigma^2(k)$, etc. jusqu' à $\sigma^r(k) = k$.
3) Ecrire le cycle correspondant : $c_1 = (k; \sigma(k), ..., \sigma^{r-1}(k))$.
4) Recommencer avec un autre entier k non déjà rencontré : on obtient des cycles $c_1, c_2, ..., c_s$.
5) Ecrire finalement $\sigma = c_1 \circ c_2 \circ ... \circ c_s$.

3.4 Groupe alterné

Définition 3.4.1 *Soit $\sigma \in S_n$. Alors*
1) On dit qu'un couple $(i, j) \in \{1, 2, ..., n\}^2$ est une inversion de σ si et seulement si $i < j$ et $\sigma(i) > \sigma(j)$.
On note $I(\sigma)$ le nombre d'inversions de σ.
2) On appelle signature de σ le nombre noté $\varepsilon(\sigma)$ ou $sgn(\sigma)$, défini par $\varepsilon(\sigma) = (-1)^{I(\sigma)}$.
3) On dit qu'une permutation est paire si le nombre $I(\sigma)$ des inversions est pair, c'est-à-dire $\varepsilon(\sigma) = 1$.
4) Si le nombre $I(\sigma)$ des inversions est impair, c'est-à-dire $\varepsilon(\sigma) = -1$, alors on dit que σ est impaire.

Exemple 3.4.2 *Pour* $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 5 & 3 \end{pmatrix}$, *on a les inversions sont présentées par les couples* $(1,2)$, $(1,3)$, $(1,5)$, $(4,5)$, *alors* $I(\sigma) = 4$ *et* $\varepsilon(\sigma) = 1$ *et* σ *est paire.*

Exemple 3.4.3 *La permutation identique* $Id = e$ *n'a aucune inversion, alors* $I(e) = 0$ *et* $\varepsilon(e) = 1$. *Par conséquent* e *est paire.*

Proposition 3.4.4 *Toute transposition est impaire.*

Preuve. Soient $i < j$ deux éléments distincts de $\{1, 2, ..., n\}$ et $\tau_{i,j}$ la transposition qui échange i et j. Alors

$$\sigma = \begin{pmatrix} 1 & ... & i-1 & i & i+1 & ... & j-1 & j & j+1 & ... & n \\ 1 & ... & i-1 & j & i+1 & ... & j-1 & i & j+1 & ... & n \end{pmatrix}$$

a) Les couples (p, q) tels que $1 \leq p \leq i-1$ ne présentent aucune inversion.
b) Les couples (p, q) tels que $p = i$ et $i+1 \leq q \leq j$ présentent tous des inversions, qui sont au nombre de $j - i$.
c) Les couples (p, q) tels que $p = i$ et $j+1 \leq q \leq n$ ne présentent aucune inversion.
d) Les couples (p, q) tels que $i+1 \leq p \leq j-1$ et $q = j$ présentent tous des inversions, qui sont au nombre de $j - i - 1$.
e) Les couples (p, q) tels que $j \leq p \leq n$ ne présentent aucune inversion.
Par conséquent le nombre des inversions de $\tau_{i,j}$ est $2(i-j)-1$, alors elle est impaire. ■

Proposition 3.4.5 *Expression algébrique de la signature :*
Soit $E = \{1, 2, ..., n\}$ *et* $\sigma \in S_n$ *une permutation . On a les expressions suivantes pour sa signature :*

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{\substack{\{i,j\} \subset E \\ i \neq j}} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Preuve. Considérons une paire $\{i, j\} \subset E$ avec $i \neq j$. Puisque $\frac{\sigma(i)-\sigma(j)}{i-j} = \frac{\sigma(j)-\sigma(i)}{j-i}$ on peut supposer que $i < j$.
On pose

$$P = \prod_{i<j} \frac{\sigma(j) - \sigma(i)}{j - i} = \prod_{\{i,j\}} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Montrons que $P = \varepsilon(\sigma)$.
On remarque que le produit $p = \prod_{i<j} (j - i)$ est un entier positif. Si on pose $p' = \prod_{i<j} (\sigma(j) - \sigma(i))$,

alors on conclut que p et p' ne peuvent différer que par le signe. Donc s'intéresse à p'. Si (i,j) est une inversion de σ, $i<j$ et $\sigma(i)>\sigma(j)$ donc

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

Si (i,j) n'est pas une inversion de σ, alors

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

On peut donc écrire

$$P=(-1)^{I(\sigma)}\frac{\prod\limits_{\{i,j\}}|\sigma(j)-\sigma(i)|}{\prod\limits_{\{i,j\}}|j-i|}$$

On remarque également que

$$\prod_{\{i,j\}}|\sigma(j)-\sigma(i)|=\prod_{\{k,l\}}|k-l|$$

En effet, puisque σ est bijective, pour toute paire $\{k,l\}$ de E il existe une unique paire $\{i,j\}$ telle que $\{k,l\}=\{\sigma(i),\sigma(j)\}$. Finalement,

$$P=(-1)^{I(\sigma)}\frac{\prod\limits_{\{i,j\}}|\sigma(j)-\sigma(i)|}{\prod\limits_{\{i,j\}}|j-i|}=(-1)^{I(\sigma)}$$

■

Exemple 3.4.6 *Pour* $\sigma=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\in S_4$, *les couples* $(1,3),(1,4),(2,3),(2,4)$ *et* $(3,4)$ *présentent une inversion. On a*

$$\varepsilon(\sigma)=\frac{(4-3)(2-3)(1-3)(2-4)(1-4)(1-2)}{(2-1)(3-1)(4-1)(3-2)(4-2)(4-3)}=-1$$

Proposition 3.4.7 *L'application signature*

$$\begin{array}{rccc}\varepsilon: & (S_n,\circ) & \longrightarrow & (\{-1,1\},\times)\\ & \sigma & \longmapsto & \varepsilon(\sigma)\end{array}$$

est un morphisme du groupes.

Preuve. Il est clair que $(S_n, \circ)$ et $(\{-1,1\}, \times)$ sont deux groupes. Soient $\sigma_1, \sigma_2 \in S_n$, alors

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

Mais comme toute paire $\{k,l\}$ s'écrit de façon unique $\{\sigma_2(j), \sigma_2(i)\}$ où $\{i,j\}$ est une paire, alors

$$\varepsilon(\sigma_1\circ\sigma_2) = \prod_{\{k,l\}} \frac{\sigma_1(k)-\sigma_1(l)}{k-l}.\prod_{\{i,j\}} \frac{\sigma_2(j)-\sigma_2(i)}{j-i} = \varepsilon(\sigma_1)\times\varepsilon(\sigma_2)$$

■

Proposition 3.4.8 ***(Définition)***
La signature ε étant un morphisme de groupes, son noyau est un sous-groupe du groupe symétrique, appelé groupe alterné. On le note A_n. Ainsi

$$A_n = \ker(\varepsilon) = \varepsilon^{-1}(\{1\}) = \{\sigma \in S_n : \varepsilon(\sigma) = 1\}$$

C'est-à-dire A_n est l'ensemble des permutations paires de $E = \{1,2,...,n\}$ et $card(A_n) = \frac{n!}{2}$.

Preuve. On sait que le noyau d'un morphisme de groupes est un sous groupe. Ainsi $A_n = \ker(\varepsilon) = \varepsilon^{-1}(\{1\})$ est un sous groupe de S_n.
D'autre part, on a

$$S_n = A_n \cup (S_n - A_n) = A_n \cup^c A_n$$

Donc

$$card(S_n) = card(A_n) + card(S_n - A_n) = n!$$

De plus pour toute transposition fixée τ l'application

$$\begin{array}{rccc} \varphi: & A_n & \longrightarrow & S_n - A_n \\ & \sigma & \longmapsto & \tau\circ\sigma \end{array}$$

est bijective. On obtient

$$\varphi(A_n) = S_n - A_n$$

Donc

$$card(A_n) = card(S_n - A_n) \Longrightarrow card(A_n) = \frac{n!}{2}$$

■

Exemple 3.4.9 *Pour* $n = 3$, *alors* $S_3 = \left\{e, \tau_{1,2}, \tau_{1,3}, \tau_{2,3}, c_1 = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}, c_2 = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}\right\}$. *On trouve*

$$A_n = \{e, c_1, c_2\}$$

Bibliographie

[1] Daniel Guin, Thomas Hausberger, *Algèbre 1, groupes, corps et théorie de Galois*. EDP sciences

[2] Jean- Marie Monier. *Algèbre 1, cours et 600 exercices corrigés*. 1^{ere} année MPSI,PCSI, PTSI $2^{ème}$ édition. DUNOD, Paris 2000.

[3] Jean-Pierre Escofier, T*oute d'algèbre de la licence, Cours et exercices corrigés,* 2ème édition, Dunod, Paris, 2002, 2006.

[4] Jean-Pierre Ramis, André Warusfel ,Xavier Buff , Josselin Garnier , Emmanuel Halberstadt ,Thomas Lachand-Robert , François Moulin , Jacques Sauloy, *Mathématiques, tout-en-un pour la licence, Niveau L1. Cours complet et 270 exercices corrigés*. Dunod, Paris, 2006.

[5] Rémy Goblot, Guy Auliac, Jean Delcourt, *Mathématiques, algèbre et géométrie*. Dunod, Paris, 2005.