Remerciements

Tout d'abord, je remercie Dieu qui m'a donné la patience, la foi et la force pour atteindre mon but. Nous exprimons toutes nos gratitudes a Mr Djedidi M.Y, pour l'effort fourni, les conseils prodigués, sa patience et sa persévérance dans le suivi. Cela a été un plaisir et un honneur de travailler avec quelqu'un d'aussi compétente et d'aussi cultivé.

Nous remercions très sincèrement, les membres de jury d'avoir bien voulu accepter de faire partie de la commission d'examinateur.

Nous adressons également nos remerciements, à tous nos enseignants, pour leurs aides inestimables, qui nous ont donné les bases de la science.

Nous tenons à remercier aussi l'ensemble du personnel de l'institut des sciences et technologies et surtout département mathématique.

Enfin, pour finir et pour être sur de n'oublier personne, nous remercions tout le monde.

Table des matières

Introduction générale

En mathématiques, un groupe est un ensemble muni d'une loi de composition interne associative admettant un élément neutre et pour chaque élément de l'ensemble, un élément symétrique, jouent un rôle important dans de nombreuses sciences, et utilisé en physique fondamentale pour comprendre les lois de la relativité restreinte et les phénomènes lies à la symétrie des molécules en chimie.

Le groupe symétrique consiste un ensemble de transformations géométriques (rotation, retrait...).

Dans notre travail nous avons donné une petite idée sur la groupe symétrique, ce mémoire comporte trois chapitre, l'un pour les notients de bases et l'autre pour morphisme et action de groupe et la troisième chapitre pour propriété les groupes symétriques.

Notations

$(G, *)$: un groupe.

$|G|$: l'ordre de groupe.

$H \leq G$ (H est sous-groupe de G).

$H < G$ (H est sous-groupe proppre de G).

$\{H\}_{i \in I}$: une famille de sous-groupe.

$H \oplus K$: la somme directe des sous-groupes .

$f : G \to G'$ (f l'application à G dans G').

$ker\,(f)$: noyau de f.

$Im\,(f)$: Image de f.

$H \lhd G$ (H sous-groupe distingué de G).

$(\leq, <, \subset)$ (relations d'ordre).

R: relation d'équivalance.

S_n : groupe symétrique.

Chapitre 1

Généralités sur les groupes

1.1 Structure de groupe

Définition 1.1.1 *Soit G un ensemble non vide, muni d'un loi de composition interne définie par: $(x, y) \to x * y$*

G est un groupe relativement a cette loi si:

a) la loi est associative.

b) il existe dans $(G, *)$ un élément neutre.

c) tout élément de $(G, *)$ admet un élément symétrique.

Définition 1.1.2 *Un groupe G, est dit commutatif ou abélien, si loi de composition interne de G, est commutative.*

Exemple 1.1.1 • *Les groupes $(\mathbb{Q}, +)$,$(\mathbb{Z}, +)$,$(\mathbb{R}, +)$ sont commutatives dont l'élément neutre est 0.*

- $(\mathbb{R}^*, \cdot)$, $(\mathbb{Q}^*, \cdot)$ *sont des groupes commutatives.*
- $(\mathbb{Z}, \cdot)$ *n'est pas un groupe puisque 0 n'est pas inversible.*

Exemple 1.1.2 *Soit $*$ est un loi de composition interne définie par:*

$\forall a, b \in \mathbb{Z}, a * b = a + b - 4, (\mathbb{Z}, *)$ *est un groupe commutatif*

Solution :

1) *la loi $*$ est commutatif:*

$$a * b = a + b - 4 = b + a - 4 = b * a$$

donc:

$$a * b = b * a$$

2) *la loi $*$ est associative:*

$$(a * b) * c = (a + b - 4) * c = a + b - 4 + c - 4 = a + b + c - 8$$

$$a * (b * c) = a * (b + c - 4) = a + b + c - 4 - 4 = a + b + c - 8$$

donc:

$$(a * b) * c = a * (b * c)$$

3) *on cherche un élément neutre, supposons e un élément neutre dans $\mathbb{Z}$:*

$$\forall a \in \mathbb{Z} : a * e = a \ et \ e * a = a$$

$$a * e = a + e - 4 = a$$

$$\Rightarrow e = 4$$

donc: $e = 4$ un élément neutre.

4) *tout élément de $\mathbb{Z}$ admet un élément symétrique*

supposons x' est symétrique de x:

$$x * x' = e \ et \ x' * x = e$$

$$x * x' = x + x' - 4 = 4$$

donc:

$$x' = 8 - x$$

Alors $(\mathbb{Z}, *)$ est un groupe commutatif

Remarque 1.1.1 *Pour deux élément x et y d'un groupe non commutatif $(G,*)$ on a en générale $x*y \neq y*x$, mais si $y=e$ on a $x*e=e*x$, $\forall x \in G$*

Remarque 1.1.2 *Soit $(G,*)$ un groupe*

1) *G non vide (il contient un élément neutre).*

2) *dans un groupe G tout élément x à une unique symétrique x'.*

3) *l'élément neutre de G est unique il est noté e, l'élement neutre par $(G,+)$ est 0, l'élement neutre par $(G,\times)$ est 1.*

Définition 1.1.3 *Un groupe G est dit fini si le nombre de ses élément est fini, dans ce cas, son cardinal est appelé l'ordre du groupe G, on le note $|G|$, de plus si le groupe n'est pas fini, il est dit infini.*

Exemple 1.1.3 • *$(\mathbb{Z},+)$ est ordre infini puisque $\mathbb{Z}$ est infini.*

• *$(\mathbb{Z}/5\mathbb{Z})$ est fini $|\mathbb{Z}/5\mathbb{Z}|=5$.tel que $\mathbb{Z}/5\mathbb{Z}=\left\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\right\}$*

1.1.1 Règle de calcul dans un groupe

Dans tout ce paragraphe, G désigne un groupe multiplicatif dont l'élément neutre est note e.

1- Puissance n-ième d'un élément *tel que* $n \in \mathbb{N}^*$

Soit $x \in G$, on pose: $xx = x^2$

$(xx)\,x = x\,(xx) = x^3$

pour tout $(n, m) \in \mathbb{Z}^2$, et $x \in G$:

$i)$ $x^n x^m = x^{n+m}$, d'oú $x^n x^m = x^m x^n$

$ii)$ $(x^n)^m = x^{mn} = (x^m)^n$

2- Régle de simplification

Dans un groupe G tout élément a est simplifiable à droit et à gauche c-à-d pour tout x, y dans G

$xa = ya \Rightarrow x = y$ et $ax = ay \Rightarrow x = y$

En effet, si a^{-1} est l'inverse de a

$xa = ya \Rightarrow (xa)\,a^{-1} = (ya)\,a^{-1}$, d'oú $x = y$

Remarque 1.1.3 $(\mathbb{Z}_n, +)$ *est un groupe abélien fini d'ordre* n*, appelé le groupe de classe de congruence de* $\mathbb{Z}$ *modulo* n

$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\right\}$, *tel que* $n \in \mathbb{N}^*$.

1.1.2 Table de cayley d'un groupe fini

Exemple 1.1.4 *Table de cayley de* $\mathbb{Z}_n$

pour $n = 2$ *et* $n = 5$ *les tables de cayley des groupes* $(\mathbb{Z}_2, +)$, $(\mathbb{Z}_5, +)$ *sont respectivement*

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Les deux groupes sont abéliens chacune des tables est symétrique par rapport à la diagonale principale, le table de cayley des groupe $(\mathbb{Z}_5^*, \cdot)$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

1.2 Sous-groupe

Définition 1.2.1 *Soit $(G,*)$ un groupe et H une partie non vide de G, on dit que H est un sous-groupe G si:*

$$\begin{cases} (x,y) \in H \times H \Rightarrow xy \in H & (i) \\ x \in H \Rightarrow x^{-1} \in H & (ii) \end{cases}$$

Remarque 1.2.1 *Les conditions (i) et (ii) impliquent que $e \in H$.*

Théorème 1.2.1 *Soit $(G,*)$ un groupe et H une partie non vide de G, on dit que H un sous-groupe de G, si et seulement si:*

$$\forall\, (x,y) \in H \times H \text{ alors } xy^{-1} \in H \qquad (iii)$$

Preuve. • Supposons que H est un sous-groupe de G, soit $(x,y) \in H \times H$ alors:
$y \in H \Rightarrow y^{-1} \in H$, d'après (ii)
$(x, y^{-1}) \in H \times H \Rightarrow xy^{-1} \in H$, d'après (i)
donc en déduit (iii)
• Supposons(iii) vérifié, soit $(x,y) \in H \times H$
$x \in H \Rightarrow (x,x) \in H \times H$, d'ou $xx^{-1} = e \in H$
$e \in H$ et $x \in H \Rightarrow (e,x) \in H \times H$, d'ou $ex^{-1} = x^{-1} \in H$;
on en déduit que $(iii) \Rightarrow (ii)$.par suite,
$(x,y) \in H \times H \Rightarrow \left(x, y^{-1}\right) \in H \times H$, d'ou $xy \in H$
donc $(iii) \Rightarrow (ii)$. ■

Théorème 1.2.2 *Si e l'élément neutre d'un groupe $(G,*)$ alors il commute avec tous les élément de G. De plus, $\{e\}$ est un sous-groupe de G.*

Définition 1.2.2 *Soit $(G,*)$ un groupe, on dit que H est un sous-groupe propre de G si: $H \neq \{e\}$ et $H \neq G$.*

Notation 1.2.1 • *$H \leq G$: si H est un sous-groupe de G.*

• *$H < G$: si H est un sous-groupe propre de G.*

Proposition 1.2.1 *Soit G un groupe et $\{H_i\}_{i\in I}$ une famille de sous-groupe de G alors*

1- Quel que soit l'ensemble non vide I, $\cap H_i$ est un sous-groupe.

2- Si $\{H_i\}_{i\in I}$ est une famille de sous-groupe totalement ordonnée par l'inclusion alors $\cup H_i$ est un sous-groupe de G.

Preuve. *CF* [3]. ■

Remarque 1.2.2 *En générale $\{\cup H_i\}_{i\in I}$ n'est pas un sous-groupe de G.*

Exemple 1.2.1 *Les groupes $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$, sont des sous-groupes de $(\mathbb{C},+)$, tels que $(\mathbb{Z},+) < (\mathbb{Q},+) < (\mathbb{R},+) < (\mathbb{C},+)$ et les groupes $(\mathbb{Q}^*,\times)$, $(\mathbb{R}^*,\times)$, $(\mathbb{C}^*,\times)$ vérifient: $(\mathbb{Q}^*,\times) < (\mathbb{R}^*,\times) < (\mathbb{C}^*,\times)$.*

Exemple 1.2.2 *Soit G un groupe, nous posons:*

$$Z(G) = \{x \in G : xa = ax, \forall a \in G\}$$

$Z(G)$ est l'ensemble des élément $x \in G$ qui commutent avec tout élément de G, $Z(G)$ est appelé le centre de groupe G et on vérifie, c'est un sous-groupe de G.

Remarque 1.2.3 *$Z(G) < G$ si et seulement si G est non abélien.*

1.2.1 Sous- groupe engendré par une partie non vide d'un groupe

Définition 1.2.3 *Soient G un groupe et S une partie non vide de G, désignons par $\mathcal{H}_S$ l'ensemble des sous-groupe de G contenant S et posons $\langle S\rangle = \underset{H\in\mathcal{H}_S}{\cap} H$*

$\langle S\rangle$ est un sous-groupe de G, appelé sous-groupe de G engendré par S.

Remarque 1.2.4 *Dans l'ensemble des sous-groupes de G ordonné par l'inclusion, $\langle S\rangle$ est le plus petite sous-groupes de G contenant S.*

Définition 1.2.4 *Soit G un groupe et x un élément de G*

a) si le sous-groupe de G engendré par x est de cardinal infini, on dit que x est d'ordre infini dans G.

b) si le sous-groupe de G engendré par x est fini, on dit que x est d'ordre fini dans G et le cardinal du sous-groupe $\langle x\rangle$ s'appelle l'ordre de x dans G, on le note $|X|$.

Remarque 1.2.5 • *Si HK est un sous-groupe de G, alors HK est le sous-groupe de G, engendré par $H\cup K$.*

• *Si G est abélien, quels que soient les sous-groupes H et K de G, HK est un sous-groupe de G.*

Exemple 1.2.3 *puisque tout $n\in\mathbb{Z}$ s'écrit $1+1+\ ...\ +1$ si $n>0$, $(-1)+(-1)+\ ...\ +(-1)$ si $n<0$ et $0=1+(-1)$, $\mathbb{Z}$ est un groupe monogène engendré par 1.*

On remarque que $\mathbb{Z}$ peut aussi être considéré comme engendré par -1.

1.2.2 Somme directe de sous-groupe

Somme directe de deux sous-groupes:

Soit H et K deux sous-groupes d'un groupe abélien $(G,+)$, les sous-groupes de G engendré par $H \cup K$ est $G' = H + K$, qui est appelé somme des sous-groupes H et K.

Définition 1.2.5 *Le sous-groupe $G' = H + K$ est dit somme directe des sous-groupes H et K si: $H \cap K = (0)$, on écrit $G' = H \oplus K$.*

Somme directe d'un famille quelconque de sous-groupes

Définition 1.2.6 *Soit I un ensemble non vide et $\{H_i\}_{i\in I}$ une famille de sous-groupes d'un groupe abélien $(G,+)$, le sous-groupe de $(G,+)$ engendré par $\cup_{i\in I} H_i$ se note $\sum_{i\in I} H_i$ et s'appelle la somme des sous-groupes de H_i, $i \in I$.*

Proposition 1.2.2 *Si I est fini tel que $I = \{1, 2, ..., n\}$, on à:*

$$\sum_{1\leq i\leq n} H_i = \{x_1 + x_2 + ... + x_n, x_i \in H_i, \forall i\,(1 \leq i \leq n)\}$$

Si I est infini, $x \in \sum_{i\in I} H_i$ si et seulement si $x = x_{i1} + x_{i2} + ... + x_{in}$, tel que $n \in \mathbb{N}^*$, $\{i_1, i_2, ..., i_n\} \subseteq I$.

Définition 1.2.7 *$(G,+)$ est un groupe abélien et $\{H_i\}_{i\in I}$ une famille de sous groupe de G, le sous-groupe $\sum_{i\in I} H_i$ est dit somme directe des sous-groupe H_i si:*

$$\forall j \in I, H_j \cap \sum_{\substack{i\in I \\ i\neq j}} H_i = \langle 0\rangle$$

Chapitre 2

Morphisme et action de groupe

2.1 Morphisme de groupe

Définition 2.1.1 *Soient $(G, *)$ et $(G', \circ)$ deux groupe et $f : G \to G'$une application, e et e'éléments neutre de G, G' restpectivement, on dit que f est un morphisme de groupe si:*

$$\forall x, y \in G / f(x * y) = f(x) \circ f(y)$$

Définition 2.1.2 *Soient G, G' deux groupes*

1- Les morphismes d'un groupe G dans G est appelé endomorphisme de G et noté End(G).

2- Un épimorphisme est un morphisme surjectif.

3- Un monomorphisme est un morphisme injectif.

4- Un isomorphisme entre G et G' est un morphisme bijectif entre les deux groupes.

5- Un automorphisme de G est un endomorphisme de G dans lui-même.

6- On note $Hom(G, G')$ l'ensemble de homomorphisme à G dans G'

Définition 2.1.3 *Soit $f \in Hom(G, G')$ on appelle noyau de f :*
l'ensemble noté $\ker(f) = \{x \in G,\ f(x) = e'\}$
et image de f l'ensemble noté $\mathrm{Im}(f) = \{x' \in G', \exists\ x \in G,\ x' = f(x)\}$.

Proposition 2.1.1 *Pour $f \in Hom(G, G')$ on a :*

a) f *surjectif* $\Rightarrow \operatorname{Im} f = G'$

b) f *injectif* $\Rightarrow \ker f = \{e\}$

Preuve. CF[2]. ■

Proposition 2.1.2 *Soient G, G', G'' trois groupes multiplicatives, $f \in Hom(G, G')$ et $g \in Hom(G', G'')$, alors $g \circ f \in Hom(G, G'')$.*

Preuve. Soient x et $y \in G$:

$$\begin{aligned}(g \circ f)(xy) &= g(f(xy)) \\ &= g(f(x)f(y)), \text{ car } f \in Hom(G, G') \\ &= g(f(x))g(f(y)), \text{ car } g \in Hom(G', G'') \\ &= (g \circ f(x))(g \circ f(y)). \blacksquare\end{aligned}$$

Exemple 2.1.1 *1- L'application $f : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ tel que $f : x \to \log x$ est un morphisme de groupe*

car: $\forall x, y \in \mathbb{R}_+^*, f(xy) = log(xy)$

$$\begin{aligned}&= log(x) + log(y) \\ &= f(x) + f(y).\end{aligned}$$

2- L'application $g : (\mathbb{R}, +) \to (\mathbb{R}, \times)$ tel que $g : x \to e^x$ et morphisme de groupe

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

$$\begin{aligned}&= e^x \times e^y \\ &= g(x) \times g(y).\end{aligned}$$

Théorème 2.1.1 (*Décomposition de morphismes*) *Tout morphisme f d'un groupe G dans un groupe G' se factorise pour donner le diagramme commutatif suivant:*

$$\begin{array}{ccc} G & \overset{f}{\underset{\rightarrow}{}} & G' \\ \zeta \downarrow & & \uparrow j \\ G/\ker f & \overset{\rightarrow}{\underset{\bar{f}}{}} & \operatorname{Im} f \end{array}$$

Où $\zeta : G \to G/\ker f$ est la surjection canonique car: $\zeta(x) = \overline{x}$, $\bar{f} : G/\ker f \to \operatorname{Im} f$ est un isomorphisme car: $\bar{f}(\overline{x}) = f(x)$
et l'application $j : \operatorname{Im} f \to G'$ est injection car: $j(x) = x$.

Preuve. *CF* [3]. ■

Proposition 2.1.3 *Soit G un groupe alors $(Aut(G), \circ)$ est un groupe,tel que: $Aut(G)$ l'ensemble des automorphismes de G.*

Preuve. *La composée de deux homomorphismes est un homomorphisme et de deux bijections est une bijection par conséquent $\circ$ est une opération interne dans $Aut(G)$ la loi de composition est associative et admet Id_G pour élément neutre.Si $x \in Aut(G)$ alors x^{-1} appartient également à $Aut(G)$.* ■

2.1.1 Les sous groupes distingués

Définition 2.1.4 *Tout sous-groupe H de G qui est stable par tout automorphisme intérieur de G, est dit sous-groupe distingué, c'est-à-dire: pour tout $a \in G$, on a: $aH = Ha$, ou aHa^{-1}, on noté $H \lhd G$.*

Le centralisateur d'un partie A de G est l'ensemble

$$C(A) = \{x \in G \setminus \forall a \in A; xa = ax\}$$

Le normalisateur d'un sous-groupe de H de G est l'ensemble

$$\mathcal{N}(H) = \left\{g \in G \setminus gHg^{-1} = H\right\}$$

Exemple 2.1.2 • *Les sous-groupes $\{e\}$ et G sont distingués dans G.*

- *Si G est abélien tout sous-groupe H de G est distingué, $H \lhd G$.*
- *Le centre d'un groupe G, $Z(G)$ est un sous-groupe distingué de G.*

Définition 2.1.5 *Un groupe qui n'admet aucun sous-groupe propre distingué est dit simple.*

Théorème 2.1.2 *Siot $f : G \to G'$ un morphisme de groupe, le noyau de f est un sous-groupe distingué de G.*

Preuve. Montrons, $\ker f$ sous-groupe de G, Pour tout a, b$\in \ker f$

on a:

$$f\left(ab^{-1}\right) = f(a)\, f(b)^{-1} = 1_{G'}$$

alors $ab^{-1} \in \ker f$ donc $\ker f$ est un sous-groupe de G

montrons, distingué

soient $a \in \ker f$ et $x \in G$, alors

$f(xax^{-1}) = f(x)f(a)\, f(x)^{-1}$

$= 1_{G'}$, car $f(a) = 1_{G'}$

$\Rightarrow xax^{-1} \in \ker f$

et en remplaçant x par x^{-1} il vient que $\ker f$ est un sous-groupe distingué de G. ■

2.1.2 Groupe quotient

Définition 2.1.6 *Soient $(G, *)$ un groupe, et H un sous-groupe distingué de G, la relation binaire R dèfinie sur G par:*

$$\forall x, y \in G, xRy \Leftrightarrow x * y^{-1} \in H$$

l'ensemble des classes d'éléments de G suivant H est désigné par G/H

Proposition 2.1.4 *R est relation d'équivalence sur G*

Preuve. ***i-*** *R est réflexive, car $\forall x \in G$ alors: $x * x^{-1} = e \in H$, donc $\forall x \in G$, xRx*

ii- *R est symétrique, car $\forall x, y \in G$*

$$\begin{aligned} xRy &\Leftrightarrow x * y^{-1} \in H \\ &\Rightarrow (x * y^{-1})^{-1} \in H \\ &\Rightarrow y * x^{-1} \in H \\ &\Rightarrow yRx \end{aligned}$$

iii- *R est transitive, car $\forall x, y \in G$:*

$(xRy) \wedge (yRz) \Leftrightarrow [(x * y^{-1}) \in H] \wedge [(y * z^{-1}) \in H]$

$\Rightarrow (x * y^{-1}) * (y * z^{-1}) \in H$, *car H est un sous-groupe*

$\Rightarrow (x * (y^{-1} * y) * z^{-1}) \in H$, *car $*$ est associative*

$\Rightarrow (x * z^{-1}) \in H$

$\Rightarrow xRz$

alors R est une relation d'équivalence, on noté G/H l'ensemble quotient G/R ■

Exemple 2.1.3 *Considérons $\mathbb{Z}$ l'ensemble des nombres entiers, $2\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, constitué des entiers pairs alors le*
groupe quotient $\mathbb{Z}/2\mathbb{Z}$ est constitué de deux élément représentant la classe des nombres pairs et impairs.

Définition 2.1.7 *Le nombre $|G : H|$ est appelé indice de H dans G, en effet l'indice représente l'ordre du groupe quotient G/H C'est le nombre de classes de G modulo H.*

Exemple 2.1.4 *L'indice de $n\mathbb{Z}$ dans $\mathbb{Z}$ est $|\mathbb{Z} : n\mathbb{Z}| = n$.*

2.1.3 Thèoreme de cayley

Tout groupe est isomorphe à un sous-groupe du groupe de ses permutations, en particulier tout groupe fini d'ordre n est isomorphe à un sous-groupe du groupe symétrique.

Preuve. CF[2]. ■

2.2 Groupe opérant sur un ensemble(Action de groupe)

Définition 2.2.1 *On dit que le groupe G opère à gauche sur l'ensemble E, si on se donné une loi externe à gauche sur E,notée $(g,x) \to g \cdot x\,(g \in G, x \in E)$ vérifiant les conditions:*

i) pour tous $g_1, g_2 \in G$ et tout $x \in E$, $(g_1 g_2) \cdot x = g_1\,(g_2 \cdot x)$

ii) pour tout $x \in E$, $e \cdot x = x$

On pourrait définir de même un groupe G opérant à droite sur l'ensemble E, par la donnée d'une loi externe à droit $(x,g) \to xg$ telle que: $x\,(g_1 \cdot g_2) = (xg_1) \cdot g_2$ et $x \cdot e = x$ pour $x \in E$, $g_1, g_2 \in G$

2.2.1 Sous-groupe d'isotropie et orbite

Définition 2.2.2 *On définit l'ensemble*

$$G_a = \{g \in G \setminus g \cdot a = a\}$$

Proposition 2.2.1 *Soit $a \in E$, l'ensemble G_a est un sous-groupe de G.*

Preuve. *CF* [4]. ■

Définition 2.2.3 *Le groupe G opère à gauche sur un ensemble E, le sous-groupe G_a des $g \in G$ qui laissent fixe un élément $a \in E$ est appelé le sous-groupe d'isotropie de a*

Proposition 2.2.2 *La relation R définie sur E par:*

$$xRy \Leftrightarrow \exists g \in G \setminus y = gx$$

c èst un relation d'équivalence.

Preuve. • R est réflexive: $\forall x \in E$, xRx puisque $x = e \cdot x$ et $e \in G$

• R est symétrique: soient x, $y \in E$ tel que: xRy, il existe $g \in G$ telque:
$y = gx \Rightarrow x = g^{-1}y$,et comme $g^{-1} \in G$ alors yRx

• R est transitive: soient $x, y, z \in E$ tels que: (xRy et yRz) il existe $g_1, g_2 \in G$ tels que:
$y = g_1 x$ et $z = g_2 y \Rightarrow z = (g_1 g_2)x$

comme $g_1, g_2 \in G$ alors xRz ■

Définition 2.2.4 *Le groupe G opérant à gauche sur l'ensemble E, la relation R est une relation d'équivalence sur E, dont les classes sont appelées les orbites de E suivant G, ou G-orbites de E.*

Définition 2.2.5 *On dit que G opère transitivement sur E si le nombre des orbites suivant G est égal à 1 autrement dit, si pour tout $x \in E$ et tout $y \in E$, il existe $g \in G$ tel que:*

$$y = g \cdot x$$

Dans le cas contraire, on dit que G opère intransitivement sur E. Soit E et G sont finis et G opérant sur E.

2.2.2 Formule des classes

Soit E et G sont finis et G opérant sur E :

$$Card\,(E) = \sum_{a=1}^{n} \frac{card\,(G)}{card\,(G_a)}$$

est une famille de représentation des orbites de E.

2.2.3 Stabilisateurs

Définition 2.2.6 *Soit G un groupe opérant sur un ensemble E le stabilisateur d'un élément x est:*

$$stab\,(x) = \{g \in G \setminus g \cdot x = x\}$$

c'est un sous-groupe de G.

Remarque 2.2.1

$$Stab\,(g \cdot x) = g stab\,(x)\, g^{-1}$$

2.2.4 Groupes opérant fidèlement

Définition 2.2.7 *Soit G un groupe opérant à gauche sur l'ensemble E, on dit que G opère fidèlement sur E, si les relations $g \in G$ et $g \cdot x = x$ pour tout $x \in E$, impliquent $g = e$.*

2.2.5 Opérant par conjugaison

Définition 2.2.8 *Soit G un groupe on appelle opérant par conjugaison l'opérant de G sur lui-même définie par:*

$$g \cdot a = gag^{-1}$$

cette opérant n'est pas fidèle.

Théorème 2.2.1 *Soit G un groupe on appelle opérant par conjugaison sur les sous-groupes l'opérant G sur l'ensemble de ses sous-groupe définie par: $g \cdot H = gHg^{-1}$cette opérant nést pas fidèle.*

Théorème 2.2.2 *Soit Ω une orbite suivant G, le groupe G opèrant à gauche sur l'ensemble E, si $a \in \Omega$ et $b \in \Omega$ les sous-groupes d'isotropie G_a et G_b sont conjugués dans G.*

Preuve. *CF* [4]. ■

Exemple 2.2.1 *Soit H un sous-groupe quelconque de groupe G.Faisons opère H à gauche sur G par traslations à gauche, en définissant sur G la loi externe de domaine H par:*

$$(h, x) \to h \cdot x, (h \in H, x \in G)$$

il est clair que les orbites de G suivant H sont exactement les classes à droite suivant H.

2.2.6 Opérant par translation

Dans ce cas d'étude suivant, on a $G = E$

- G opére sur lui-même par translation à gauche

  $G \times G \to G$

  $(g, x) \to gx$

- G opére sur lui-même par translation à droite

  $G \times G \to G$

  $(g, x) \to xg^{-1}$

Chapitre 3

Les groupes symétriques

3.1 Groupe symétrique

Définition 3.1.1 *Soit E un ensemble non vide, on appelle groupe symétrique de E le groupe des bijections de E.on le note $S\ (E)$, si $E = \{1...n\}$, on le note simplement S_n.*

Les éléments de groupe symétrique S_n sont appelés des permutations et l'ordre de S_n est $n!$.

Proposition 3.1.1 *Le groupe symétrique $(S_n, \circ)$ admet $n!$ éléments.*

Preuve. *L'image du premier élément peut être choisi de n façons celle de second de $(n-1)$ façons..., celle du $K^{ème}$de $(n-k)$ façons ...*

donc le nombre de permutations de S_n est $n!$ ■

Notation 3.1.1 *Toute permutation $\sigma \in S_n$ s'écrit:*

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

Exemple 3.1.1 *1- Dans* S_n, $\sigma_0 = \begin{pmatrix} 1 & 2 & . & . & . & n \\ 1 & 2 & . & . & . & n \end{pmatrix}$ *est une permutation identité.*

2- Le groupe S_3 *à* $3! = 6$ *permutations, à savoir:*

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

soient r *et* $\sigma \in S_n$, *la permutation* $\sigma \circ r$ *appelée permutation produit de* r *et* σ *est définie par:*

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

avec $\sigma \circ r\,(i) = \sigma\,(r\,(i))$

$$\sigma_1 \circ r_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = r_2$$

$$r_3 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = r_1$$

On remarque que: $\sigma_1 \circ r_3 \neq r_3 \circ \sigma_1$, *donc le groupe* S_3 *est non abélien.*

Remarque 3.1.1 *Pour* $n \geq 3$, *le groupe symétrique* S_n *est non abélien*

par exemple: si $n = 2$, S_2 *a* $2! = 2$ *permutations à savoir:*

$$\sigma_0 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \qquad \sigma_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$\sigma_0 \circ \sigma_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$$\sigma_1 \circ \sigma_0 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

3.1.1 Transposition et cycle

Définition 3.1.2 *Une permutation $\gamma \in S_n$ est un cycle de longueur r $(1 \leq r \leq n$ dans $\mathbb{N})$, s'il existe un ensemble ordonné de r entiers distincts dans $N_n : j_1, j_2 ... j_n$, tels que:*

$$\gamma(j_1) = j_2, \quad \gamma(j_2) = j_3, ..., j(r-1) = j_r, \quad \gamma(j_r) = j_1$$

et pour tout $k \in N_n \setminus \{j_1, j_2, ..., j_r\}, \gamma(k) = k$.

Un tel cycle sera noté $\gamma = (j_1, j_2, ...j_r)$.

L'ensemble $\{j_1, j_2, ..., j_r\}$ est le support de γ.

Définition 3.1.3 *Soit $\gamma \in S_n$ une permutation et $i \in \{1...n\}$, on dit que i est un point fixe pour γ si et seulment si $\gamma(i) = i$.*

On note fixe (γ): l'ensemble des pointes fixes de γ dans $\{1...n\}$.

On appelle support de γ on note supp (γ), le complémentaire de l'ensemble des pointes fixes de γ, c-à-d l'ensemble des $i \in \{1...n\}$ tq: $\gamma(i) \neq i$.

Exemple 3.1.2 *Considérons la permutation suivant:*

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

le support de γ est $\{1, 2, 3\}$, on remarque que $\gamma(1) = 2$, $\gamma(2) = 3$, $\gamma(3) = 1$
on dit que, dans le groupe S_4, γ est un cycle de longueur 3 et γ est noté $(1, 2, 3)$.

Définition 3.1.4 *Dans $S_n\,(n \geq 2)$, le cycle de longueur n:*

$$\gamma_1 = (1, 2, ...n) = \begin{pmatrix} 1 & 2 & 3 & . & . & . & n \\ 2 & 3 & 4 & . & . & . & 1 \end{pmatrix}$$

est appelé permutation circulaire des entiers $1, 2, ..., n$

Remarque 3.1.2 • *Dans $(n \geq 3)$ un cycle de longueur n n'est pas nècessairement la permutation circulaire.*

• *Dans S_n, un cycle de longueur $r\,(1 \leq r \leq n)$ sera appelé un r-cycle.*

• *Tout cycle de longueur 1 est l'indentité σ_0: en effet si $\gamma = (j)$, on a $\gamma(j) = j$ et pour tout $k \neq j$ dans N_n, $\gamma(k) = k$ donc $\gamma = \sigma_0$.*

3.1.2 Décomposition d'une permutation

Remarque 3.1.3 *Dans un groupe S_n, on dira que deux cycles sont disjoints, si leurs supports sont disjoints.*

Théorème 3.1.1 *Toute permutation $\sigma \neq \sigma_0$ dans S_n s'écrit sous la forme:*

$$\sigma = \gamma_1 \circ \gamma_2 \circ ... \circ \gamma_s$$

et $s \in \mathbb{N}^*$ tel que: $\gamma_1, \gamma_2, ...\gamma_s$ sont des cycles disjoints, tous différents de σ_0 la décomposition est unique à l'ordre des facteurs près.

Preuve. *CF* [2]. ■

Remarque 3.1.4 *D'après le théorème exprime que tout groupe S_n est engendré par l'ensemble de ses cycles.*

Exemple 3.1.3 *Soit σ la permutation du groupe S_6:*

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

se décompose en cycles $\sigma = \gamma_1 \circ \gamma_2$ oú $\gamma_1 = (1, 5, 3)$ et $\gamma_2 = (4, 6)$.

3.1.3 Signature

Définition 3.1.5 *Pour tout permutation $\sigma \in S_n$, on appelle signature de σ et on note $\zeta(\sigma)$ le nombre:*

$$\zeta(\sigma) = \frac{\prod\limits_{1\leq i<j\leq n}(\sigma(j)-\sigma(i))}{\pi\limits_{1\leq i<j\leq n}(j-i)}$$

Exemple 3.1.4 *Soit* $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *et* $r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3$

alors:

$$\zeta(\sigma_1) = \prod_{1\leq i<j\leq 3}\frac{\sigma(j)-\sigma(i)}{j-i} = \frac{\sigma(2)-\sigma(1)}{2-1}\cdot\frac{\sigma(3)-\sigma(1)}{3-1}\cdot\frac{\sigma(3)-\sigma(2)}{3-2} = \frac{3-2}{2-1}\cdot\frac{1-2}{3-1}\cdot\frac{1-3}{3-2} = 1$$

$$\zeta(\tau_2) = \prod_{1\leq i<j\leq 3}\frac{\sigma(j)-\sigma(i)}{j-i} = \frac{\sigma(2)-\sigma(1)}{2-1}\cdot\frac{\sigma(3)-\sigma(1)}{3-1}\cdot\frac{\sigma(3)-\sigma(2)}{3-2} = \frac{2-3}{2-1}\cdot\frac{1-3}{3-1}\cdot\frac{1-2}{3-2} = -1$$

Théorème 3.1.2 *La signature ζ est un homomorphisme, de groupe S_n dans le groupe multiplicatif $\Gamma = \{-1, 1\}$*

Preuve. CF[4]. ■

3.1.4 Groupe alterné

Définition 3.1.6 *La permutation σ est pair si $\zeta(\sigma) = 1$, sinon elle est dite impaire si $n \geq 2$, la signature ζ est surjective, son noyau est formé par des permutations paires on l'appelle le $n^{ième}$ groupe alterné*

$$A_n = \ker \zeta = \{\sigma \in S_n : \zeta(\sigma) = 1\}$$

Exemple 3.1.5 *Dans σ_3 considérons les permutations:*

$$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

on a :

$$\zeta(\sigma_0) = 1, \zeta(\sigma_1) = \frac{\sigma(2) - \sigma(1)}{2-1} \cdot \frac{\sigma(3) - \sigma(1)}{3-1} \cdot \frac{\sigma(3) - \sigma(2)}{3-2} = 1$$

comme $\sigma_2 = \sigma_1^2$,alors $\zeta(\sigma_2) = 1$

donc $A_3 = \{\sigma_0, \sigma_1, \sigma_2\}$.

Conclusion générale

En mathématiques, un groupe est un ensemble muni d'une loi de composition interne associative admettant un élément neutre et, pour chaque élément de l'ensemble, un élément symétrique, elle est important dans plusieurs domaines comme la chimie et physique...

Dans ce mémoire nous avons étudié, les groupes symétriques, elle est représent par un ensemble de permutations, celui manifestation des l'intérêt les lois expérimentale.

Bibliographie

[1] **Arnailt.Français**, Gilles Bailly -Maitre, Mathématiques L3,Algébre, Pearson Education France 2009

[2] **Calais.Josette**, Eléments de Théorie des groupes, PUF 1984

[3] **Hitta.Amara**, cours d'algébre et exercices corrigés, OPU 1994

[4] **Lelong-Ferrand.Jacqueline,** Jean-Marie Arnaudiés, cours de mathématiques1.Algébre (LELONG-FERRANDARNUDIES), Dunod paris 2003

[5] **Monier.Jean.Marie**, Algébre MPSI, Dunod, paris 2006

[6] **Pécastaings.Français**, Chemins ves L'Algébre T1, VUIBERT 1993