

Table des matières

Introduction	4
1 Structure de Groupe	5
1.1 Notions de groupe:	5
1.2 Sous groupes:	5
1.3 Groupe distingué:	8
1.4 Groupes Quotients:	9
1.5 Homomorphismes de Groupes:	9
1.6 Order de groupe:	13
2 Généralités sur les groupes symétriques	18
2.1 Groupes symétriques :	18
2.1.1 Groupe S_n :	18
2.2 Groupes symétriques d'un ensemble fini:	24
2.3 Signature d'une permutation	28
3 Groupes monogènes:	31
3.1 Classification des groupes monogènes	31
3.2 Générateurs d'un groupe monogène:	34
4 Quelques application aux groupes finis:	38
4.1 Représentations linéaires des groupes :	38
4.1.1 Définitions:	38
4.1.2 Théorie des caractères	41

4.2	Représentations du groupe symétrique:	42
4.2.1	Tableaux de Young:	42
4.2.2	Tableaux standards et base de S^λ :	44
4.2.3	Représentation naturelle de Young	50

Remerciements

La réalisation de ce modeste travail est grâce au bon dieu le tout puissant que nous remercions pour le courage et la patience qu'il nous a attribué pour parvenir à la fin de notre carrière estudiantine.

Al'occasion nous tenons à adresser nos sincères remerciement à l'encadreur:

Monsieur MIHOUBI DOUADI, ET GHADBANE NACER pour sa bienveillance, et pour son aide prècieux qu'il nous a apportée.

Introduction

La notion de groupe a été introduite pour la première fois au début du dix-neuvième siècle. A cette époque elle intervient dans les travaux d'Evariste Galois sur les équations algébriques sous forme de groupes de permutations des racines de ces équations. Presque au même moment les groupes commencent à jouer un rôle en géométrie notamment des groupes symétriques de polygone et de polyèdres réguliers. C'est à partir de cette double origine algébrique et géométrique qu'a été conçue vers la fin du dix-neuvième siècle la notion abstraite de groupe et que Petit à petit a été construite la théorie de groupes.

Dans la théorie de groupe une place importante a été accordée à l'étude de la structure des groupes finis compte tenu des nombreuses interprétations concrètes qui peuvent en être données. C'est précisément dans ce cadre que se place ce mémoire dans lequel ont été traités les groupes monogènes, les groupes Symétriques, et quelques applications aux groupes finis.

Ce travail est composé quatre chapitres :

- Le premier chapitre consiste en un rappel des notions et notations utilisées par la suite: La structure du groupe , sous-groupe , groupes distingués , groupes quotient, homomorphismes des groupes .
- Dans le second chapitre nous avons étudiés les groupes symétriques et quelques propriétés.
- Dans le troisième chapitre nous avons intéressés les groupes monogènes et le groupe cyclique .
- Dans le quatrième chapitre nous avons fait quelques applications des groupes finis : représentations linéaires des groupes et représentations du groupe symétrique.

Chapitre 1

Structure de Groupe

1.1 Notions de groupe:

Définition 1.1.1 : *On appelle groupe tout ensemble non vide G munie d'une loi de composition interne notée \star tel que :*

1. La loi \star est associative .
2. La loi \star possède un élément neutre e .
3. Tout élément de G admet un symétrique unique.

Si de plus la loi est commutative on dit que (G, \star) est un groupe commutatif ou groupe Abélien

Exemple : Un exemple illustratif de groupe abélien est $(\mathbb{Z}, +)$.

1.2 Sous groupes:

Définition 1.2.2 : *Soit (G, \star) un groupe on appelle sous groupe de (G, \star) tout sous ensemble non vide G' de G tel que la restriction de \star à G' en fait un groupe. Comme \star est associative dans G alors sa restriction à G' est aussi associative, par suite $G' \neq \emptyset$ est un sous groupe de (G, \star) s'il est stable par rapport à \star et à l'opération inversion, c'est à dire :*

$$(i) G' \neq \emptyset$$

$$(ii) \forall a, b \in G', a \star b \in G'$$

$$(iii) \forall a \in G', a^{-1} \in G'$$

Il est clair que si (G, \star) est un groupe, alors G' est un sous groupe de G

Proposition 1.2.3 : Soient (G, \star) un groupe et $G' \subset G$, alors

G' est un sous groupe de

$$G \iff \begin{cases} \forall a, b \in G', a \star b^{-1} \in G' \\ G' \neq \emptyset \end{cases}$$

Preuve :

- Soit G' un sous groupe de (G, \star) , alors :

i) \star a un élément neutre dans G' , donc $G' \neq \emptyset$.

ii) Soient $a, b \in G'$ comme G' muni de la restriction de \star est un groupe alors b^{-1} existe dans G' et comme G' est stable par rapport à \star on déduit que $a \star b^{-1} \in G'$.

- Inversement, soit G' un sous ensemble de G tel que:

$$G' \neq \emptyset,$$

$$\forall a, b \in G', a \star b^{-1} \in G'$$

Montrons que G' muni de la restriction de \star est un groupe.

i) Comme $G' \neq \emptyset$ alors il existe $a \in G'$ et d'après la deuxième hypothèse

$$e = a \star a^{-1} \in G'$$

ce qui montre que G' la restriction de \star admet un élément neutre e dans G' .

ii) Soit $x \in G'$, comme $e \in G'$ alors d'après la deuxième hypothèse on aura

$$x^{-1} = e \star x^{-1} \in G'$$

ce qui montre que tout élément x de G' est inversible dans G' par rapport à la restriction de \star à G' .

iii) La restriction de \star à G' est une loi de composition interne car pour tous x et y dans G' d'après ii) on a : $y^{-1} \in G'$ et en utilisant la deuxième hypothèse on déduit que:

$$x \star y = x \star (y^{-1})^{-1} \in G'$$

iv) La restriction de \star à G' est associative car \star est associative dans G .

Remarque : D'après i) de la preuve de la proposition précédente, on voit que : Si e est l'élément neutre d'un groupe (G, \star) alors tout sous groupe de G contient e et on déduit la propriété suivante.

Proposition 1.2.4 : Soient (G, \star) un groupe et e l'élément neutre de \star et G' un sous ensemble de G alors G' est un sous groupe de G si et seulement si :

$$e \in G'$$

$$\forall x, y \in G', x \star y^{-1} \in G'$$

Exemple : Soit (G, \star) un groupe et $G' = \{x \in G : (\forall y \in G, x \star y = y \star x)\}$, alors G' est un sous groupe de G . En effet

i) Si e est l'élément neutre de \star alors $e \in G'$ car :

$$\forall y \in G, e \star y = y \star e = y$$

ii) Soient $x, y \in G'$ alors

$$\begin{aligned} \forall z \in G, (x \star y^{-1}) \star z &= (x \star y^{-1}) \star (z^{-1})^{-1} \\ &= x \star (y^{-1} \star (z^{-1})^{-1}) \text{ car } \star \text{ est associative} \\ &= x \star (z^{-1} \star y)^{-1} \text{ car } y \in G' \\ &= x \star ((z^{-1})^{-1} \star y^{-1}) \\ &= x \star (z \star y^{-1}) \\ &= (x \star z) \star y^{-1} \text{ car } \star \text{ est associative} \end{aligned}$$

$$\begin{aligned} &= (z \star x) \star y^{-1} \text{ car } x \in G' \\ &= z \star (x \star y^{-1}) \text{ car } \star \text{ est associative} \end{aligned}$$

ce qui montre que $x \star y^{-1} \in G'$.

Exemple : Soit $n \in \mathbb{N}$, alors $n\mathbb{Z} = \{n.p, p \in \mathbb{Z}\}$ est un sous groupe de \mathbb{Z} .

En effet :

i) $0 \in n\mathbb{Z}$ car : $\exists p = 0 \in \mathbb{Z} : 0 = n.p$.

ii) Soient $x, y \in n\mathbb{Z}$ alors il existe $p_1, p_2 \in \mathbb{Z}$ tels que:

$$x = n.p_1 \text{ et } y = n.p_2 \text{ donc } x - y = n.p_1 - n.p_2 = n.(p_1 - p_2) = n.p \in n\mathbb{Z}$$

par suite:

$$\forall x, y \in n\mathbb{Z}, x - y \in n\mathbb{Z}$$

De i) et ii) on déduit que $n\mathbb{Z}$ est un sous groupe de \mathbb{Z} .

Pour $n \in \mathbb{N} \setminus \{0, 1\}$, $n\mathbb{Z}$ est un sous groupe propre de \mathbb{Z} .

1.3 Groupe distingué:

Définition 1.3.5 : On dit que H est distingué dans G (ou normal) si pour tout $x \in G$ on a $xH = Hx$. Ceci équivaut à $\forall x \in G : xHx^{-1} = H$, ou encore plus explicite :

$$\forall x \in X : \forall h \in H : xhx^{-1} \in H$$

On note souvent $H \triangleleft G$ pour souligner qu'un sous-groupe $H < G$ est distingué

Exemples:

1. Le centre de tout groupe est distingué.
2. Tout sous-groupe d'un groupe abélien est distingué
3. Les sous-groupes $\{e\}$ et G sont distingués dans G .
4. Si f est un homomorphisme de groupes, alors $\text{Ker } f$ est distingué

1.4 Groupes Quotients:

Définition 1.4.6 : Le groupe G/G' défini s'appelle le groupe quotient de G par G' tel que:

$$G/G' = \{xG' : x \in G\}$$

- Soient (G, \star) un groupe et G' un sous groupe de G . On définit une relation binaire R sur G par :

$$\forall a, b \in G : aRb \iff a \star b^{-1} \in G'$$

Proposition 1.4.7 : R est une relation d'équivalence sur G .

Preuve :

i) R est Reflexive, car : $\forall x \in G$, comme G' est un sous groupe de G , alors $x \star x^{-1} = e \in G'$, donc $\forall x \in G, xRx$

ii) R est Symétrique car $\forall x, y \in G$:

$$\begin{aligned} xRy &\iff x \star y^{-1} \in G' \\ &\implies (x \star y^{-1})^{-1} \in G' \\ &\implies y \star x^{-1} \in G \\ &\implies yRx \end{aligned}$$

iii) R est Transitive car $\forall x, y, z \in G$:

$$\begin{aligned} (xRy) \wedge (yRz) &\iff [(x \star y^{-1}) \in G'] \wedge [(y \star z^{-1}) \in G'] \\ &\implies (x \star y^{-1}) \star (y \star z^{-1}) \in G', \text{ car } G' \text{ est un sous groupe} \\ &\implies (x \star (y^{-1} \star y) \star z^{-1}) \in G, \text{ car } \star \text{ est associative} \\ &\implies (x \star z^{-1}) \in G' \\ &\implies xRz \end{aligned}$$

De i), ii) et iii) on déduit que R est une relation d'équivalence

1.5 Homomorphismes de Groupes:

Dans ce paragraphe, on considère (G, \bullet) et (H, \star) deux groupes, avec e et h leurs éléments neutres respectifs.

Définition 1.5.8 : Une application $f : G \rightarrow H$ est appelée homomorphisme de groupes de G dans H si : $\forall a, b \in G : f(a \bullet b) = f(a) \star f(b)$.

- Si f est bijective on dit que f est un isomorphisme (de groupes) de G sur H . On dit alors que G est isomorphe à H , ou que G et H sont isomorphes.

- Si $G = H$, on dit que f est un endomorphisme de G , et si de plus f est bijective on dit que f est un automorphisme (de groupe) de G .

Exemple : Etant donnés les groupes $(R, +)$ et $(R, *)$, alors les applications:

$$f : (R, +) \rightarrow (R, *) \quad \text{et} \quad g : (R, *) \rightarrow (R, +)$$

$$x \mapsto \exp x \qquad x \mapsto \ln|x|$$

Définition 1.5.9 : Soit $f : G \rightarrow H$ un homomorphisme de groupes. On appelle noyau de f l'ensemble :

$$\begin{aligned} \text{Ker } f &= f^{-1}(\{h\}) \\ &= \{a \in G, f(a) = h\} \end{aligned}$$

et l'image de f l'ensemble:

$$\text{Im } f = f(G) = \{f(a), a \in G\}.$$

Proposition 1.5.10 : Soit $f : G \rightarrow H$ un homomorphisme de groupes , alors:

$$\begin{aligned} 1. & f(e) = h \\ 2. & \forall a \in G, (f(a))^{-1} = f(a^{-1}) \end{aligned}$$

Preuve:

1. h étant l'élément neutre de \star et e celui de \bullet , alors

$$f(e \nabla e) = f(e) = h \star f(e)$$

et comme f est un homomorphisme on déduit que

$$h \star f(e) = f(e) \star f(e)$$

et comme tous les éléments du groupe (H, \star) sont réguliers on déduit que $h = f(e)$.

2. Soit $a \in G$ et montrons que $f(a^{-1})$ est l'inverse de $f(a)$ dans le groupe (H, \star) .
 f étant un homomorphisme de groupe alors:

$$f(a) \star f(a^{-1}) = f(a \bullet a^{-1}) = f(e) \quad \text{et} \quad f(a^{-1}) \star f(a) = f(a^{-1} \bullet a) = f(e)$$

sachant que $f(e) = h$ d'après la première propriété on déduit que:

$$(f(a))^{-1} = f(a^{-1}).$$

Remarque : De la première propriété on déduit que $e \in \ker f$

Proposition 1.5.11 : Soit $f : G \rightarrow H$ un homomorphisme de groupes, alors:

1. L'image d'un sous groupe de G est un sous groupe de H .
2. L'image réciproque d'un sous groupe de H est un sous groupe de G .

Preuve :

1. Soit G' un sous groupe de G et montrons que $f(G')$ vérifie les deux conditions de la caractérisation des sous groupes.

i) Comme G' est un sous groupe de G , alors $e \in G'$ donc $f(e) \in f(G')$ par suite $f(G') \neq \emptyset$.

ii) Soient $a, b \in f(G')$, alors il existe $x, y \in G'$ tels que $a = f(x)$ et $b = f(y)$ donc d'après la deuxième propriété on aura:

$$a \star b^{-1} = f(x) \star (f(y))^{-1} = f(x) \star f(y^{-1}) = f(x \bullet y^{-1})$$

et comme G' est un sous groupe de G alors $(x \bullet y^{-1}) \in G'$ par suite

$$a \star b^{-1} = f(x \bullet y^{-1}) \in f(G')$$

de i) et ii) on déduit que $f(G')$ est un sous groupe de H .

2. Soit H' un sous groupe de H , alors:

i) D'après la première propriété $f(e) = h$ et comme H' est un sous groupe de H alors $h \in H'$ donc $e \in f^{-1}(H')$.

ii) Soient $x, y \in f^{-1}(H')$, alors $f(x), f(y) \in H'$ et comme H' est un sous groupe de G alors $f(x) \star (f(y))^{-1} \in H'$ et de la deuxième propriété on déduit que:

$$f(x \bullet y^{-1}) = f(x) \star f(y^{-1}) = f(x) \star (f(y))^{-1} \in H'$$

ce qui montre que $(x \bullet y^{-1}) \in f^{-1}(H')$.

De i) et ii) on déduit que $f^{-1}(H')$ est un sous groupe de G .

Remarque : Comme cas particuliers des propriétés $\Im m f$ est un sous groupe de (H, \star) et $\ker f$ est un sous groupe de (G, \bullet) .

Proposition 1.5.12 : Soit $f : G \rightarrow H$ un homomorphisme de groupe, alors:

1. f est injective si et seulement si $\text{Ker } f = \{e\}$.

2. f est surjective si et seulement si $\text{Im } f = H$.

3. f est un isomorphisme si et seulement si f^{-1} existe et est un homomorphisme de groupe de H dans G .

Preuve. Soit $f : G \rightarrow H$ un homomorphisme de groupe, alors:

a) Si f est injectif sachant que $e \in \text{Ker } f$ on va montrer que $\text{Ker } f \subset \{e\}$.

Soit $x \in \text{Ker } f$, alors $f(x) = h$ et comme $f(e) = h$ on déduit que $f(x) = f(e)$ et comme f est injectif on déduit que $x = e$, donc $x \in \{e\}$ ce qui montre que $\text{Ker } f = \{e\}$.

b) Inversement supposons que $\text{Ker } f = \{e\}$ et montrons que f est injectif.

Soient $x, y \in G$, alors:

$$\begin{aligned} f(x) = f(y) &\Rightarrow f(x) \star (f(y))^{-1} = h \\ &\Rightarrow f(x) \star f(y^{-1}) = h \\ &\Rightarrow f(x) \star f(y^{-1}) = h \\ &\Rightarrow f(x) \star f(y^{-1}) = h \\ &\Rightarrow f(x \bullet y^{-1}) = h \\ &\Rightarrow (x \bullet y^{-1}) \in \text{Ker } f \\ &\Rightarrow x \bullet y^{-1} = e \text{ car } \text{Ker } f = \{e\} \\ &\Rightarrow x = y \end{aligned}$$

ce qui montre que f est injectif.

2. La preuve de cette propriété est immédiate sachant que $\text{Im } f = f(G)$.

3. On se limitera à démontrer que si f est un isomorphisme, alors

$f^{-1} : H \rightarrow G$ est aussi un homomorphisme. Soient $x, y \in H$, alors il existe $a, b \in G$ tels que:

$$x = f(a) \text{ et } y = f(b)$$

donc

$$a = f^{-1}(x) \text{ et } b = f^{-1}(y)$$

par suite:

$$\begin{aligned} f^{-1}(x \star y) &= f^{-1}(f(a) \star f(b)) \\ &= f^{-1}(f(a \bullet b)) \text{ car } f \text{ homomorphisme} \end{aligned}$$

$$\begin{aligned}
&= a \bullet b \\
&= f^{-1}(x) \bullet f^{-1}(y)
\end{aligned}$$

ce qui montre que f^{-1} est un homomorphisme de groupe de H dans G .

Théorème 1.5.13 : (*Théorème de Cayley*). *Soit G un groupe Il existe un morphisme injectif $c : G \rightarrow S_G$.*

Preuve: On fait agir G sur lui-même par translation à gauche : l'application qui définit cette action est (avec $X = G$)

$$\begin{cases} G \times X \rightarrow X \\ (g, h) \mapsto gh \end{cases}$$

À chaque action de groupes est associé un morphisme de groupes issu du groupe qui agit et à valeurs dans le groupe des permutations de l'ensemble sur lequel G agit (pour de plus amples détails à ce sujet voir la note « action de groupe »). Le morphisme associé à notre action est

$$c : \begin{cases} G \rightarrow S_X = S_G \\ g \mapsto (h \mapsto gh) \end{cases}$$

On dit que c est le morphisme de Cayley de G . Montrons que c est injectif. Pour cela on considère $g \in \text{Kerc}$.

L'application $h \mapsto gh$ est donc l'identité de G . Autrement dit $gh = h$ pour tout $h \in G$. En particulier avec $h = 1_G$, on obtient $g = 1_G$ et c est injective. Ainsi $c(G)$ est un sous-groupe de S_G isomorphe à G .

1.6 Order de groupe:

Définition 1.6.14 : On dit qu'un groupe G est fini si l'ensemble G est fini.

Définition 1.6.15 : On notera $|X|$ le cardinal d'un ensemble fini X . L'ordre d'un groupe fini G , est le nombre $|G|$ d'éléments du groupe. Plus généralement Un élément $g \in G$ est dit d'ordre n ($n \geq 2$) et note par $o(g)$ si:

$$g^n = e \text{ et } g^m \neq e \text{ pour } 1 \leq m \leq n-1.$$

Remarque: $o(g) = 1$ si et seulement si $g = 1$.

Exemple : Une rotation d'angle $\frac{2\pi}{n}$ est un élément d'ordre n du groupe des rotations du plan.

Corollaire 1.6.16 : Soit g appartenant à G . Alors, $\langle g \rangle = \{g^m / m \in \mathbb{Z}\}$.

Démonstration: On rappelle que pour tout entier $m < 0$ on note g^m à la place de $(g^{-1})^n$ où $n = -m$.

les éléments de $\langle g \rangle$ sont de la forme $g_1 \dots g_n$ avec $g_i = g$ ou $g_i^{-1} = g$ pour tout i compris entre 1 et n . Donc en simplifiant tant que c'est possible les g avec les g^{-1} les éléments de $\langle g \rangle$ sont de la forme g^m , m dans \mathbb{Z} .

Proposition 1.6.17 : (Théorème de Lagrange) Soit G un groupe fini et H un sous-groupe de G . Alors $|H|$ divise $|G|$ et

$$|G|/|H| = |H \backslash G| = |G/H|$$

L'entier $|G|/|H|$ s'appelle l'indice de H dans G .

Proposition 1.6.18 : Soit g un élément d'ordre fini du groupe G . Alors l'ordre de g est le plus petit entier strictement positif k tel que $g^k = 1$.

Proposition 1.6.19 : Soit g un élément de G distinct de 1 et d'ordre fini. Alors $\langle g \rangle = \{g^n / 1 \leq n < o(g)\}$.

Démonstration : $\langle g \rangle = \{g^m / m \in \mathbb{Z}\}$. Comme $\langle g \rangle$ est fini il existe un entier strictement positif a tel que $g^a = 1$. On pose k : le plus petit entier strictement positif a tel que $g^a = 1$. Pour tout entier m il existe par division euclidienne un couple (i, n) d'entiers avec $0 \leq n < k$ tel que $m = ik + n$.

D'où

$$\begin{aligned} g^m &= g^{ik+n} \\ &= g^{ik} g^n \\ &= g^{ki} g^n \\ &= (g^k)^i g^n \\ &= 1^i g^n \end{aligned}$$

$$= 1g^n$$

$$= g^n.$$

On en déduit que $\langle g \rangle = \{g^n/1 \leq n < k\}$.

Il reste à montrer que $k = o(g)$. $\langle g \rangle$ est de cardinal $o(g)$ par définition de $o(g)$.

Si $i < j < k$ sont tels que $g^i = g^j$ alors $g^j(g^i)^{-1} = g^{j-i} = 1$. D'où comme $j - i > 0$, on a par hypothèse sur k , $j - i \geq k$. Mais $j < k$ donc $j - i < k$. Contradiction.

D'où si $i < j < k$, $g^i \neq g^j$. On en déduit que $\langle g \rangle = \{g^n/1 \leq n < k\}$ est de cardinal k et donc $k = o(g)$ Dans la démonstration précédente on a prouvé la proposition suivante :

Proposition 1.6.20 : Soient G un groupe g un élément de G d'ordre fini et n un entier strictement positif tel que $g^n = 1$. Alors l'ordre de g divise n .

Démonstration: On pose $x = o(g)$. Par division euclidienne il existe deux entiers a et b tels que $n = ax + b$ avec $0 \leq b < x$. D'où $1 = g^n = g^{ax+b} = g^{ax}g^b = (g^x)^a g^b = g^b$.

Si b n'est pas nul contredit la proposition 1.6.18 D'où $b = 0$ et $o(x)$ divise n .

Groupes à deux éléments:

Soit $G = \{a, b\}$ un ensemble à deux éléments définir toutes les lois de composition internes dans G qui lui confèrent une structure de groupe. Soit \star une loi de composition sur G alors pour que (G, \star) soit un groupe il faut que \star soit interne dans G et admette un élément neutre qui peut être a ou b donc \star doit être définie de la sorte :

1. Si a est l'élément neutre de \star alors

$$a \star a = a$$

$$a \star b = b$$

$$b \star a = b$$

reste à définir $b \star b$ or pour que (G, \star) soit un groupe il faut que tout élément soit inversible en particulier il faut trouver b^{-1} . Si on pose $b \star b = b$ alors on remarque que

$$\forall x \in G$$

$$b \star x \neq a$$

donc b ne sera pas inversible ce qui nous amène à poser

$$b \star b = a$$

Ainsi on a défini une l.c.i. dans G avec un élément neutre a reste à voir si la loi ainsi définie est associative. On a :

$$(a \star a) \star a = a \star a = a \star (a \star a)$$

$$(a \star a) \star b = a \star b = a \star (a \star b)$$

$$(a \star b) \star a = b \star a = a \star b = a \star (b \star a)$$

$$(a \star b) \star b = b \star b = a = a \star a = a \star (b \star b)$$

En remarquant que la loi est commutative on déduit que:

$$(b \star a) \star a = b \star (a \star a)$$

$$(b \star a) \star b = b \star (a \star b)$$

ce qui montre que

$$\forall x, y, z \in G$$

$$x \star (y \star z) = (x \star y) \star z$$

donc \star est associative dans G et par suite (G, \star) est un groupe.

2. Si b est l'élément neutre de \star alors de la même manière on construit la loi \star comme suit :

$$b \star b = b$$

$$b \star a = a$$

$$a \star b = a$$

$$a \star a = b$$

D'après ce qui précède : Il existe deux groupes à deux éléments et formellement on les définit ainsi :

$*$	a	b
a	a	a
b	b	a

et

$*$	a	b
a	b	a
b	a	b

Théorème 1.6.21 : (*Sylow, p -groupes*)

Soit G un groupe fini et p un nombre premier divisant l'ordre de G . On écrit

$$|G| = mp^r$$

avec $p \nmid m$.

On appelle p -Sylow de G tout sous-groupe de G d'ordre p^r et on note $S_p(G)$ l'ensemble des p -Sylow de G .

Chapitre 2

Généralités sur les groupes symétriques

Deux ensembles non vides et équipotents ont à un isomorphisme près le même groupe symétrique

2.1 Groupes symétriques :

2.1.1 Groupe S_n :

Soit n un entier naturel non nul.

Définition 2.1.22 : *On note S_n l'ensemble des permutations de l'ensemble $\{1, \dots, n\}$ c'est à dire l'ensemble des bijections de $\{1, \dots, n\}$ vers $\{1, \dots, n\}$.*

Proposition 2.1.23 : *(S_n, \circ) est un groupe.*

Démonstration: L'identité est une permutation de $\{1, \dots, n\}$ donc S_n n'est pas vide. La composée de deux bijections est une bijection donc on a une loi interne. La composition est clairement associative L'identité est l'élément neutre pour la composition. Enfin tout élément de S_n est inversible d'inverse sa fonction réciproque.

Définition 2.1.24 : *Le groupe S_n est appelé groupe symétrique de degré n .*

Proposition 2.1.25 : *S_n est d'ordre $n!$.*

Démonstration: Soit σ appartenant à S_n .

$\sigma(1)$ peut être n'importe quel des $1 \leq i \leq n$. On a donc n valeurs possibles.

$\sigma(2)$ peut être n'importe quel des $1 \leq i \leq n$ hormis la valeur $\sigma(1)$ puisque σ est injective.

On a donc $n - 1$ valeurs possibles. On arrive ainsi à $n \times (n - 1) \times \dots \times 1 = n!$ bijections possibles.

Proposition 2.1.26 : *Soient X et Y deux ensembles non vides. Si X et Y sont équipotents alors $S(X)$ et $S(Y)$ sont isomorphes.*

Démonstration: Considérons une bijection f de X sur Y . L'application φ_f définie de $S(X)$ vers $S(Y)$ par:

$$\varphi_f(\sigma) = f \circ \sigma \circ f^{-1} \text{ pour tout } \sigma \in S(X)$$

est un isomorphisme de groupes. En effet si $\sigma, \rho \in S(X)$ alors:

$$\begin{aligned} \varphi_f(\sigma \circ \rho) &= f \circ (\sigma \circ \rho) \circ f^{-1} \\ &= (f \circ \sigma \circ f^{-1}) \circ (f \circ \rho \circ f^{-1}) \\ &= \varphi_f(\sigma) \circ \varphi_f(\rho) \end{aligned}$$

Donc φ_f est un morphisme de groupes. De plus si $\sigma \in \ker(\varphi_f)$ alors:

$$\begin{aligned} \sigma &= f^{-1} \circ f \circ \sigma \circ f^{-1} \\ &= f^{-1} \circ \varphi_f(\sigma) \circ f \\ &= f^{-1} \circ id_Y \circ f \\ &= id_X \end{aligned}$$

Ce qui prouve que φ_f est injectif. En outre si $\sigma \in S(Y)$ alors:

$$\begin{aligned} \sigma &= f \circ f^{-1} \circ \sigma \circ f^{-1} \\ &= \varphi_f(f^{-1} \circ \sigma \circ f) \end{aligned}$$

Ainsi φ_f est surjectif. En résumé φ_f est un isomorphisme de groupes de $S(X)$ sur $S(Y)$.

Il est clair que si X est un singleton $\{x\}$ alors $S(X) = \{id_x\}$. Supposons par ailleurs que X contient au moins deux éléments distincts x et y . La permutation de X notée τ_{xy} et définie par:

$$\begin{cases} \tau_{xy}(x) = y \\ \tau_{xy}(y) = x \\ \tau_{xy}(t) = t, \forall t \in X \end{cases}$$

est appelée transposition de $S(X)$. Parfois une transposition τ_{xy} est notée (x, y) .

Observons que $\tau_{xy}^2 = id_X$ soit toute transposition est égale à son propre inverse dans $S(X)$. Nous constatons aisément que si X est réduit à une paire $\{x, y\}$ alors $S(X) = \{id_X, \tau_{xy}\}$.

Par conséquent si X est réduit à un singleton ou à une paire alors le groupe $S(X)$ est abélien. Dans la suite nous comptons prouver la réciproque à savoir le groupe symétrique $S(X)$ n'est abélien que si X contient un ou deux éléments. A cet effet rappelons que le centre d'un groupe G est noté $Z(G)$ et que G est abélien si et seulement si $G = Z(G)$.

Théorème 2.1.27 : *Soit X un ensemble non vide. Le groupe symétrique $S(X)$ est abélien si et seulement si X contient au plus deux éléments. En outre si X admet au moins trois éléments alors $Z(S(X)) = \{id_x\}$.*

Démonstration: Compte tenu de l'analyse faite ci-dessus il reste à envisager le cas où X contient au moins trois éléments. Soient alors $x, y, z \in X$ trois éléments distincts de X .

Nous avons :

$$\begin{aligned} (\tau_{xy} \circ \tau_{xz})(x) &= \tau_{xy}(\tau_{xz}(x)) \\ &= \tau_{xy}(z) \\ &= z \\ y &= \tau_{xy}(y) \\ &= \tau_{xz}(\tau_{xy}(x)) \\ &= (\tau_{xz} \circ \tau_{xy})(x) \end{aligned}$$

donc: $z \neq y$

Ceci nous permet de conclure que $S(X)$ n'est pas abélien. Pour la deuxième partie du théorème considérons $\sigma \in S(X)/\{id_X\}$ et choisissons $x \in X$ tel que $\sigma(x) \neq x$. Posons $y = \sigma(x)$. Comme X contient au moins trois éléments, nous pouvons choisir un élément $z \in X$ autre que x et que y . Observons que

$$\begin{aligned} (\sigma \circ \tau_{xy})(x) &= \sigma(\tau_{xy}(x)) \\ &= \sigma(x) \\ &= y \end{aligned}$$

Or

$$\begin{aligned} (\tau_{yz} \circ \sigma)(x) &= \tau_{yz}(\sigma(x)) \\ &= \tau_{yz}(y) \\ &= z \end{aligned}$$

Il vient que $(\sigma \circ \tau_{xy}) \neq (\tau_{yz} \circ \sigma)$ et par conséquent $\sigma \notin Z(S(X))$. Le résultat annoncé en découle.

Le support de $\sigma \in S(X)$ est l'ensemble noté $supp(\sigma)$ et défini par:

$$supp(\sigma) = \{x \in X : \sigma(x) \neq x\}$$

Il est clair que $\sigma = id_x$ si et seulement si $supp(\sigma) = \emptyset$. En outre si X contient plus de deux éléments alors $\sigma \in S(X)$ est une transposition si et seulement si $supp(\sigma)$ est une paire.

Proposition 2.1.28 : Soit X un ensemble non vide. Si $\sigma \in S(X)/\{id_X\}$ alors:

$$\sigma(x) \in supp(\sigma) \text{ pour tout } x \in supp(\sigma).$$

Démonstration: Soient $x \in supp(\sigma)$ et $y = \sigma(x)$. Supposons que $y \notin supp(\sigma)$.

Donc $\sigma(y) = y$ et par suite $x = y$ car σ est injective. Nous aboutissons à une contradiction. Ceci montre que notre supposition est fautive et par suite $y \in supp(\sigma)$. D'où le résultat. Bien qu'en général $S(X)$ ne soit pas abélien nous pouvons permuter deux permutations à supports disjoints.

Théorème 2.1.29 : Soit X un ensemble contenant au moins deux éléments. Alors deux permutations de $S(X)$ à supports disjoints commutent.

Démonstration: Considérons $\sigma, \rho \in S(X)$ tels que :

$$\text{supp}(\sigma) \cap \text{supp}(\rho) = \emptyset$$

Si l'un des deux supports est vide alors l'une des deux permutations est id_X . La propriété est dans ce cas vérifiée. Supposons donc que les deux supports soient non vides. Soit $x \in \text{supp}(\sigma)$. Alors $x \notin \text{supp}(\rho)$ et d'après 2,1,28 $\sigma(x) \neq \text{supp}(\rho)$. Par conséquent:

$$(\sigma \circ \rho)(x) = \sigma(x) \text{ et } (\rho \circ \sigma)(x) = \rho(x)$$

Le cas où $x \in \text{supp}(\rho)$ se traite par symétrie des rôles de σ et de ρ . Ainsi et coïncident sur $\text{supp}(\sigma) \cup \text{supp}(\rho)$. Il nous reste à envisager le cas échéant où $x \notin \text{supp}(\sigma) \cup \text{supp}(\rho)$. Nous avons dans ce cas

$$(\sigma \circ \rho)(x) = x = (\rho \circ \sigma)(x)$$

En résumé $\sigma \circ \rho = \rho \circ \sigma$, ce qui achève la démonstration. A tout couple $(\sigma, x) \in S(X) \times X$ nous associons une partie de X définie par:

$$\Omega_\sigma(x) = \{\sigma^m(x) : m \in \mathbb{Z}\}$$

et appelée σ -orbite de x .

Exemple : Si l'on reprend la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$ de S_6 .

la décomposition en σ -orbite

$\Omega_\sigma(1) = \{1, 5, 3\}$, $\Omega_\sigma(2) = \{2\}$, $\Omega_\sigma(4) = \{4, 6\}$ de $\{1, 2, 3, 4, 5, 6\}$ implique que $\sigma = (1 \ 5 \ 3)(4 \ 6)$

Théorème 2.1.30 : Soient X un ensemble non vide et $\sigma \in S(X)$. Alors la relation binaire R définie sur X par:

$$xRy \text{ si, et seulement si, } y \in \Omega_\sigma(x)$$

est une relation d'équivalence et $\Omega_x(x)$ est la classe d'équivalence de $x \in X$ modulo R_σ .

Démonstration: Soient $x, y, z \in X$. Comme $x = \sigma^0(x) \in \Omega_\sigma(x)$ la relation R_σ est reflexive. De plus si $xR_\sigma y$ alors il existe $m \in \mathbb{Z}$ tel que $y = \sigma^m(x)$. Il vient que $x = \sigma^{-m}(y) \in \Omega_\sigma(y)$ et donc $yR_\sigma x$. Autrement dit la relation R_σ est symétrique.

Enfin si :

$$xR_\sigma y \text{ et } yR_\sigma z \text{ alors } y \in \Omega_\sigma(x) \text{ et } z \in \Omega_\sigma(y).$$

Nous déduisons qu'il existe $m, n \in \mathbb{Z}$ tels que $y = \sigma^m(x)$ et $z = \sigma^n(y)$. Nous obtenons

$$z = \sigma^n(y) = \sigma^n(\sigma^m(x)) = (\sigma^n \circ \sigma^m)(x) = \sigma^{m+n}(x) \in S(X)$$

Il s'en suit que R est transitive.

En particulier les σ -orbites forment une partition de X . En outre $\Omega_\sigma(x)$ est réduite à un singleton si et seulement si $x \notin \text{supp}(\sigma)$.

D'ailleurs une σ -orbite réduite à un singleton est dite ponctuelle. A ce proposition 2.1.30 entraîne que les σ -orbites non ponctuelles forment une partition de $\text{supp}(\sigma)$.

Proposition 2.1.31 : Soient X un ensemble non vide, $\sigma \in S(X)$ et Ω une σ -orbite fini de cardinal $m \in \mathbb{N}$. Alor $\Omega = \{x, \sigma(x), \dots, \sigma^{m-1}(x)\}$ et $\sigma^m(x) = x$ pour tout $x \in \Omega$

Démonstration: Soit $x \in \Omega$ et $\mathfrak{R} = \{n \in \mathbb{N} : \sigma^n(x) = x\}$. Supposons que $\mathfrak{R} = \emptyset$ et observons que dans ce cas l'application de \mathbb{N} dans Ω qui à tout n fait correspondre $\sigma^n(x)$ est injective. Ceci contredit le fait que Ω soit finie. Donc $\mathfrak{R} \neq \emptyset$. Posons alors $n_0 = \min(\mathfrak{R})$ et remarquons

que $\sigma^{n_0}(x) = x$. Considérons $n \in \mathbb{Z}$ et effectuons la division euclidienne de n par n_0 pour trouver $q, r \in \mathbb{Z}$ tels que :

$$n = qn_0 + r \text{ et } 0 \leq r < n_0 - 1.$$

Donc

$$\sigma^n(x) = \sigma^{qn_0+r}(x) = \sigma^r(\sigma^{qn_0}(x)) = \sigma^r(x)$$

Par suite:

$$\Omega = \{x, \sigma(x), \dots, \sigma^{n_0-1}(x)\}$$

Choisissons p, q dans $\{0, \dots, n_0 - 1\}$ tels que $p < q$. Alors $\sigma^q(x) \neq \sigma^p(x)$ car si non $\sigma^{q-p}(x) = x$ et $q - p < n_0$ et donc $p - q \in \mathfrak{R}$ et $q - p < \min(\mathfrak{R})$, ce qui est une contradiction. Nous en déduisons que $m = n_0$ et donc

$$\Omega = x, \sigma(x), \dots, \sigma^{m-1}(x) \text{ et } \sigma^m(x) = x$$

Ce qu'il fallait démontrer.

2.2 Groupes symétriques d'un ensemble fini:

Supposons que X soit un ensemble fini de cardinal $n \in \mathbb{N}^*$. Nous déduisons de 2.1.26 que l'étude de $S(X)$ revient à l'étude de $S(\{1, 2, \dots, n\})$, le groupe symétrique de l'ensemble $\{1, 2, \dots, n\}$, appelé désormais groupe symétrique de degré n et noté S_n . A cet égard l'élément neutre de S_n est noté ι_n . D'après 2.1.27 $Z(S_n) = \{\iota_n\}$ dès que $n \geq 3$. La composée $\sigma \circ \rho$ de deux permutations $\sigma, \rho \in S_n$ est notée simplement $\sigma\rho$. Une permutation $\sigma \in S_n$ est souvent notée par:

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

Le groupe S_n est fini ce qui ne semble pas très surprenant. Avant de continuer notre étude de S_n remarquons que pour tout $\sigma \in S_n$ les σ -orbites étant des parties de $\{1, 2, \dots, n\}$ sont finies. Une permutation $\sigma \in S_n$ est appelée *cycle* s'il existe une unique σ -orbite non ponctuelle. Dans ce cas le cardinal de cette σ -orbite est appelé longueur du *cycle*. Pour tout $m \in \{1, 2, \dots, n\}$ un *cycle* de longueur m est appelé m -*cycle*. Une transposition $(x, y) \in S_n$ est un 2-*cycle* de support $\{x, y\}$. En vertu de 2.1.31 nous pouvons ajouter que si $m \in \mathbb{N}$, σ est un m -*cycle* de S_n et Ω est l'unique σ -orbite non ponctuelle alors:

$$\sigma = \text{supp}(\sigma) = x, \sigma(x), \dots, \sigma^{m-1}(x) \text{ pour tout } x \in \Omega$$

Un m -*cycle* σ dont l'orbite est $\{x, \sigma(x), \dots, \sigma^{m-1}(x)\}$ est noté $(x, \sigma(x), \dots, \sigma^{m-1}(x))$. Nous avons signalé auparavant qu'une transposition est égale à son propre inverse. Autrement dit une transposition est un élément d'ordre 2 dans S_n . Ce résultat se généralise aux *cycles* de S_n .

Proposition 2.2.32 : *Soit $n \in \mathbb{N}$. Un m – cycle est un élément d'ordre m dans S_n .*

Démonstration: Soient $m \in \mathbb{N}$ et $\sigma = (x, \sigma(x), \dots, \sigma^{m-1}(x))$ un m – cycle dans S_n . D'après 2.1.31 $\Omega = \{x, \sigma(x), \dots, \sigma^{m-1}(x)\}$ est l'unique σ – orbite non ponctuelle et est de cardinal m , $\sigma^{m-1}(x) \neq x$, ce qui prouve que $\sigma^{m-1} \neq \iota_n$. Par ailleurs si $y \in \Omega$ alors $\sigma^m(y) = y$ et ce encore grâce à 2.1.31. En outre pour $y \notin \Omega = \text{supp}(\sigma)$, $\sigma(y) = y$ et donc $\sigma^m(y) = y$. Finalement $\sigma^m = \iota_n$ et σ est d'ordre m .

Le lemme suivant sert à établir le résultat central de ce paragraphe.

Lemme 2.2.33 : *Soient $n \in \mathbb{N}$ et $\sigma_1, \dots, \sigma_m$ des cycles de S_m à supports deux à deux disjoints. Si $\sigma = \sigma_1 \dots \sigma_m$ alors $\text{supp}(\sigma_1), \dots, \text{supp}(\sigma_m)$ forment une partition de $\text{supp}(\sigma)$ et sont les σ – orbites non ponctuelles.*

Démonstration: Par hypothèse $\text{supp}(\sigma_1), \dots, \text{supp}(\sigma_m)$ sont deux à deux disjoints. Soient $x \in \cup_{k=1}^m \text{supp}(\sigma_k)$ et $\ell \in \{1, \dots, m\}$ tel que $x \in \text{supp}(\sigma_\ell)$.

Donc $\sigma_\ell(x) \neq x$. En outre $x \notin \text{supp}(\sigma_k)$ pour tout $k \in \{1, \dots, m\} / \{\ell\}$ et par suite $\sigma_k(x) = x$ pour tout $k \in \{1, \dots, m\} / \{\ell\}$. De plus 2.1.29 entraîne que si $p, q \in \{1, \dots, m\}$ alors $\sigma_p \sigma_q = \sigma_q \sigma_p$. En résumé:

$$\sigma(x) = (\sigma_\ell \sigma_1, \dots, \sigma_{\ell-1} \sigma_{\ell+1}, \dots, \sigma_m)(x) = \sigma_\ell(x) \neq x$$

et donc $x \in \text{supp}(\sigma)$. Inversement si $x \in \text{supp}(\sigma)$ alors $\sigma(x) \neq x$ et par conséquent il existe $\ell \in \{1, \dots, m\}$ tel que $\sigma_\ell(x) \neq x$, soit $x \in \text{supp}(\sigma_\ell)$. Ainsi $x \in \cup_{k=1}^m \text{supp}(\sigma_k)$ et donc:

$$\text{supp}(\sigma) = \cup_{k=1}^m \text{supp}(\sigma_k)$$

Montrons à présent que $\text{supp}(\sigma_1), \dots, \text{supp}(\sigma_m)$ sont les σ – orbites non ponctuelles de σ . Soient $x \in \text{supp}(\sigma)$ et $\ell \in \{1, \dots, m\}$ tel que $x \in \text{supp}(\sigma_\ell)$. Alors tenant compte de 2.1.29 nous pouvons écrire:

$$\begin{aligned} \Omega_\sigma(x) &= \{\sigma^p(x) : p \in \mathbb{Z}\} \\ &= \{(\sigma_1, \dots, \sigma_m)^p(x) : p \in \mathbb{Z}\} \\ &= \{\sigma_\ell^p(x) : p \in \mathbb{Z}\} \\ &= \Omega_{\sigma_\ell} \end{aligned}$$

$$= \text{supp}(\sigma\ell)$$

Ainsi, $\text{supp}(\sigma_1), \dots, \text{supp}(\sigma_m)$ sont des σ – orbites non ponctuelles. Par ailleurs, $\text{supp}(\sigma_1), \dots, \text{supp}(\sigma_m)$ forment une partition des $\text{supp}(\sigma)$ et il en est de même pour les σ – orbites non ponctuelles. Il vient que $\text{supp}(\sigma_1), \dots, \text{supp}(\sigma_m)$ sont précisément les σ – orbites non ponctuelles. Nous sommes à présent en mesure d'établir le résultat principal de cette section à savoir que les cycles engendrent S_n .

Théorème 2.2.34 : *Soit $n \in \mathbb{N}^*$. Toute permutation dans $S_n / \{\ell_n\}$ se décompose de manière unique (à l'ordre des facteurs près) en un produit de cycles à supports deux à deux disjoints.*

Démonstration: Soit $\sigma \in S_n / \{\ell_n\}$. Il existe alors des σ – orbites non ponctuelles . Notons $\Sigma_1, \dots, \Sigma_m$ toutes les σ – orbites non ponctuelles et considérons les permutation $\sigma_1, \dots, \sigma_m \in S_n$ définies par:

$$\sigma_\ell(x) = \sigma(x) \text{ si } x \in \Sigma_\ell \text{ et } \sigma_\ell(x) = x \text{ pour } \ell \in \{1, \dots, m\}$$

sinon.

Il est clair que pour $\ell \in \{1, \dots, m\}$ Σ_ℓ est l'unique σ_ℓ – orbite non ponctuelle. De ce fait $\sigma_1, \dots, \sigma_m$ sont des cycle à supports respectifs $\Sigma_1, \dots, \Sigma_m$ qui sont deux à deux disjoints. De plus si $x \in \text{supp}(\sigma)$ alors il existe $\ell \in \{1, \dots, m\}$ tel que: $x \in \Sigma_\ell$. Donc $\sigma(x) = \sigma_\ell(x)$ et en appliquant 2.1.29 nous obtenons:

$$\begin{aligned} \sigma(x) &= \sigma_\ell(x) \\ &= \sigma_\ell(\sigma_1 \dots \sigma_{\ell-1} \sigma_{\ell+1} \dots \sigma_m)(x) \\ &= (\sigma_1 \dots \sigma_m)(x) \end{aligned}$$

Si par ailleurs $x \notin \text{supp}(\sigma)$ alors $\sigma(x) = x = \sigma_\ell(x)$ pour tout $\ell \in \{1, \dots, m\}$ car

$$\begin{aligned} \text{supp}(\sigma) &= \cup_{k=1}^m \Sigma_k \\ &= \cup_{k=1}^m \text{supp}(\sigma_k) \end{aligned}$$

Finalement

$$\sigma = \sigma_1 \dots \sigma_m$$

D'où l'existence de la décomposition de σ en un produit de cycles à supports deux à deux disjoints. Pour établir l'unicité supposons que $\sigma = \gamma_1 \dots \gamma_\ell$ soit une autre décomposition de σ en produit de cycles à support deux à deux disjoints.

D'après 2.2.33, les σ_ℓ - orbite sont exactement $\text{supp}(\gamma_1), \dots, \text{supp}(\gamma_\ell)$ Ceci prouve que $m = \ell$ et que pour tout $i \in \{1, \dots, m\}$, il existe $j \in \{1, \dots, m\}$ tel que $\text{supp}(\gamma_i) = \text{supp}(\sigma_j)$. Nous en déduisons, via la disjonction des supports que si $x \in \{1, \dots, n\}$ alors:

$$\gamma_i(x) = \sigma_j(x) = x \text{ si } x \in \text{supp}(\gamma_i)$$

et

$$\gamma_i(x) = \sigma_j(x) = \sigma(x)$$

sinon. il vient que $\gamma_i = \sigma_j$. D'où l'unicité.

La décomposition ci-dessus peut-être utilisée pour trouver l'ordre d'une permutation puisque dans un groupe fini G , l'ordre d'un produit de deux éléments d'ordres respectifs ℓ et m qui commutent est égal à $\ell \vee m$. A l'image des cycles les transpositions engendrent le groupe S_n pour $n \geq 2$. Ceci provient de la simple constatation que si $\sigma = (x_1, \dots, x_m)$ est un m - cycle de S_n alors $\sigma = (x_1, x_2) \dots (x_{m-1}, x_m)$ est une décomposition de σ en produits de transpositions. Cependant ce résultat peut-être obtenu directement et avec un peut plus de précisions.

Théorème 2.2.35 : *Soit $n \in \mathbb{N}$ tel que $n \geq 2$. Toute permutation de S_n est produit d'au plus $n - 1$ transpositions.*

Démonstration: Comme $S_2 = \{e, (1, 2)\}$ le résultat est vrai pour $n = 2$. Considérons $n \geq 3$ et supposons que toute permutation de S_{n-1} se décompose en produit d'au plus $n - 2$ transpositions.

Soit $\sigma \in S_n$. Supposons d'abord que $\sigma(n) = n$ et notons $\tilde{\sigma}$ la permutation de S_{n-1} définie par:

$$\tilde{\sigma}(x) = \sigma(x) \text{ pour tout } x \in \{1, \dots, n - 1\}$$

L'hypothèse de récurrence assure l'existence de p ($p \leq n - 2$) transpositions de S_{n-1} notées $\tilde{\tau}_1, \dots, \tilde{\tau}_p$ telles que:

$$\tilde{\sigma} = \tilde{\tau}_1, \dots, \tilde{\tau}_p$$

Pour tout $i \in \{1, \dots, p\}$ nous considérons la transposition τ_i de S_n définie par:

$$\tau_i(n) = n \text{ et } \tau_i(x) = \tilde{\sigma}(x) \text{ pour tout } x \in \{1, \dots, n-1\}$$

Il est simple de constater que:

$$\sigma = \tau_1 \dots \tau_p$$

est produit d'au plus $n-2$ transpositions. Supposons à présent que $\sigma(n) = x < n$. Posons $\gamma = \tau_{xn}\sigma$. Ainsi γ est une permutation de S_n telle que $\gamma(n) = n$. D'après le cas précédent il existe p ($p \leq n-2$) transpositions de S_n telles que :

$$\gamma = \tau_1 \dots \tau_p$$

Par suite:

$$\sigma = \tau_{xn} \tau_1 \dots \tau_p$$

Finalement σ est le produit d'au plus $n-1$ transpositions.

2.3 Signature d'une permutation

Définition 2.3.36 : Soit $\sigma \in S_n$. On appelle nombre d'inversions de σ le nombre de paires $\{i, j\} \in \{1, \dots, n\}$ telles que la restriction de σ à $\{i, j\}$ soit décroissante (i.e. si $i > j$ alors $\sigma(i) < \sigma(j)$ et si $i < j$ alors $\sigma(i) > \sigma(j)$). On note ν_σ cet entier.

Exemple : Dans S_5 on considère $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}$

Les paires $\{i, j\}$ où il y a inversion sont $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}$ et $\{3, 4\}$.

Ainsi on a $\nu_\sigma = 7$.

Lemme 2.3.37 .: Soit $\sigma \in S_n$ et $a, \sigma_1, \dots, \sigma_n$ des nombres réels distincts deux à deux. On pose pour tout $i = 1, \dots, n$, $b_i = a_{\sigma(i)}$. On a:

$$(-1)^{\nu_\sigma} = \prod_{1 \leq i < j \leq n} \frac{b_j - b_i}{a_j - a_i}$$

Preuve : L'ensemble des couples (i, j) tels $1 \leq i < j \leq n$ décrit exactement l'ensemble des paires $\{i, j\}$. Comme σ est une permutation il s'ensuit que

l'ensemble des couples $(\sigma(i), \sigma(j))$ tels que $1 \leq i < j \leq n$ d'écrit lui aussi exactement l'ensemble des paires $\{i, j\}$. Par ailleurs comme

on a:

$$\prod_{1 \leq i < j \leq n} \frac{b_j - b_i}{a_j - a_i} = \frac{\prod_{1 \leq i < j \leq n} b_j - b_i}{\prod_{1 \leq i < j \leq n} a_j - a_i}$$

on voit que ce produit est de module 1. Maintenant si sur le couple $\{i, j\}$ la permutation σ présente une inversion le facteur $b_j - b_i$ au numérateur sera égal à l'opposé d'un facteur $a_{j'} - a_{i'}$ du dénominateur au contraire si ne présente pas d'inversion sur la paire $\{i, j\}$ alors le facteur au dénominateur le facteur $b_j - b_i$ au numérateur sera égal à un facteur $a_{j'} - a_{i'}$ au dénominateur. Le produit considéré est donc égal à $(-1)^m$ où m est le nombre de paires où σ présente une inversion c'est à dire à $(-1)^{\nu_\sigma}$.

Définition 2.3.38 : Soit $\sigma \in S_n$. On appelle signature de σ l'entier (égal à ± 1) $\epsilon_\sigma = (-1)^{\nu_\sigma}$. On dira que est pair (resp. impaire) si $\epsilon_\sigma = 1$ (resp. si $\epsilon_\sigma = -1$).

Corollaire 2.3.39 .: L'application

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

est un morphisme de groupe (l'ensemble $\{1, -1\}$ étant considéré comme sous-groupe multiplicatif de (\mathbb{Q}^*, \cdot)).

Preuve : Soit $\sigma, \sigma' \in S_n$

Prenons des réels a_1, \dots, a_n distincts deux à deux.

Posons pour tout $i = 1, \dots, n$, $b_i = a_{\sigma(i)}$ et $c_i = b_{\sigma'(i)} = a_{\sigma\sigma'(i)}$. Par application de la proposition précédente on a:

$$\begin{aligned} \epsilon_{\sigma\sigma'} &= \frac{\prod_{1 \leq i < j \leq n} c_j - c_i}{\prod_{1 \leq i < j \leq n} a_j - a_i} \\ &= \frac{\prod_{1 \leq i < j \leq n} c_j - c_i}{\prod_{1 \leq i < j \leq n} b_j - b_i} \cdot \frac{\prod_{1 \leq i < j \leq n} b_j - b_i}{\prod_{1 \leq i < j \leq n} a_j - a_i} \end{aligned}$$

$$= \epsilon_{\sigma'} \cdot \epsilon_{\sigma}$$

Proposition 2.3.40 : *Toute transposition est impaire en particulier si $n \geq 2$ alors l'application ϵ est un épimorphisme.*

Preuve : Comme pour tout $l, k \in \{1, \dots, n\}$ distincts on a :

$$(lk) = (1l)(1k)(1l)$$

et que ϵ est un morphisme il suffit de montrer cette proposition dans le cas d'une transposition du type $(1l)$ pour $l \geq 2$. Les inversions de $(1l)$ sont $\{1, 2\}, \{1, 3\}, \dots, \{1, l\}$ et $\{2, l\}, \{3, l\}, \dots, \{l-1, l\}$ (si $l \geq 3$). Il y en a donc $l-1+l-2 = 2l-3$ et donc $\epsilon_{(1l)} = (-1)^{2l-3} = -1$

Corollaire 2.3.41 : *Si $\sigma \in S_n$ est le produit de k transpositions alors $\epsilon_k = (-1)^k$.*

Chapitre 3

Groupes monogènes:

3.1 Classification des groupes monogènes

Le sous-groupe d'un groupe G engendré par un élément g de G est noté $\langle g \rangle$. Il vient rapidement que:

$$\begin{aligned}\langle g \rangle &= \{g^m : m \in \mathbb{Z}\} \\ &= \{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}\end{aligned}$$

où e désigne l'élément neutre de G . Le groupe G est dit monogène s'il existe g dans G tel que $G = \langle g \rangle$. S'il en est ainsi g est appelé générateur de G .

Nous disons aussi que G est engendré par g . Un groupe monogène fini est dit cyclique. Un groupe monogène est visiblement abélien.

Un élément g d'un groupe G est dit de torsion s'il est d'ordre fini. L'ordre d'un élément de torsion g est noté $o(g)$ et l'ordre d'un groupe fini G est noté $o(G)$. Un groupe G est cyclique si et seulement si il existe un élément de torsion g tel que $G = \langle g \rangle$. Dans ce cas nous montrons aisément que :

$$G = \{e, g, g^2, \dots, g^{o(g)-1}, \} \quad \text{et } o(G) = o(g)$$

Notons que nous pouvons remplacer dans les deux égalités ci-dessus g par n'importe quel générateur du groupe cyclique G autre que g .

L'image d'un groupe monogène par un morphisme de groupes est également monogène. Nous pouvons énoncer ce résultat autrement comme suit.

Proposition 3.1.42 : *Soient G un groupe monogène et H un groupe. S'il existe un morphisme de groupes surjectif de G sur H alors H est monogène.*

Démonstration. Soient g un générateur de G et φ un morphisme de groupes surjectif de G sur H . Pour tout $h \in H$, il existe $m \in \mathbb{Z}$ tel que $h = \varphi(g^m)$. Mais comme φ est un morphisme de groupes nous obtenons $h = (\varphi(g))^m$. Il vient que:

$$H = \{(\varphi(g))^m : m \in \mathbb{Z}\}$$

En d'autres termes H est monogène et $\varphi(g)$ en est un générateur.

Rappelons que si $n \in \mathbb{N}^*$ alors l'ensemble $\mathbb{Z}/n\mathbb{Z}$ des classes de congruence modulo n dans \mathbb{Z} est un groupe pour l'addition définie par:

$$\bar{\ell} + \bar{m} = \overline{\ell + m} \text{ pour tout } (\ell, m) \in \mathbb{Z}^2$$

où \bar{m} désigne la classe de congruence de m modulo n . En fait $\mathbb{Z} = n\mathbb{Z}$ est le groupe quotient de \mathbb{Z} par son sous-groupe $n\mathbb{Z} = \{mn : m \in \mathbb{Z}\}$. De plus la surjection canonique s définie de \mathbb{Z} sur $\mathbb{Z} = n\mathbb{Z}$ par $s(m) = m$ pour tout $m \in \mathbb{Z}$ est un morphisme de groupes. Comme \mathbb{Z} est monogène nous pouvons appliquer 3.1.42, ce qui nous permet d'affirmer que $\mathbb{Z}/n\mathbb{Z}$ est monogène. Etant par ailleurs fini, $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Notons au passage que $\bar{1}$ est un générateur du groupe cyclique $\mathbb{Z}/n\mathbb{Z}$. Signalons également que $\mathbb{Z}/0\mathbb{Z}$ est identifié à \mathbb{Z} .

Avant de poursuivre notre étude rappelons que H est un sous-groupe de \mathbb{Z} si et seulement si il existe $n \in \mathbb{N}$ tel que $H/n\mathbb{Z}$. Nous arrivons à présent au résultat central de cette section.

Théorème 3.1.43 : *Un groupe G est monogène si et seulement si il existe $n \in \mathbb{N}$ tel que G soit isomorphe au groupe $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. La condition proposée pour que G soit monogène est évidemment suffisante. Montrons qu'elle est nécessaire. Soient G un groupe monogène et g un générateur de G .

Nous avons donc:

$$G = \{g^m : m \in \mathbb{Z}\}$$

Considérons l'application s définie de \mathbb{Z} dans G par:

$$s(m) = g^m \quad \text{pour tout } m \in \mathbb{Z}$$

Il n'est pas ardu de voir que φ est morphisme de groupes surjectif. Le premier théorème d'isomorphismes assure le fait G est isomorphe au groupe quotient $\mathbb{Z}/\ker\varphi$ où $\ker\varphi$ désigne le noyau de φ . Or comme $\ker\varphi$ est un sous-groupe de \mathbb{Z} il existe $n \in \mathbb{N}$ tel que $\ker\varphi = n\mathbb{Z}$. Par conséquent G est isomorphe à \mathbb{Z}/n et le problème est résolu. Distinguons le cas où le groupe considéré est infini.

Corollaire 3.1.44 : *Un groupe est monogène infini si, et seulement si, il est isomorphe à \mathbb{Z} .*

Démonstration. Soit G un groupe. Il est évident que si G est isomorphe à \mathbb{Z} alors G est monogène infini. Inversement, supposons que G est monogène infini. D'après 3.1.43, il existe $n \in \mathbb{N}$ tel que G soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Mais comme G est infini $\mathbb{Z}/n\mathbb{Z}$ doit être infini ce qui donne $n = 0$. Finalement G est isomorphe à \mathbb{Z} . Traïtons le cas fini.

Corollaire 3.1.45 : *Un groupe G est cyclique si et seulement si il existe $n \in \mathbb{N}^*$ tel que G soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$.*

Démonstration. Soit G un groupe. Il est clair que s'il existe $n \in \mathbb{N}$ tel que G soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$ alors G est cyclique. Réciproquement supposons que G est cyclique. En vertu de 3.1.43, il existe $n \in \mathbb{N}$ tel que G soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$. De plus G est fini et par suite $\mathbb{Z}/n\mathbb{Z}$ est fini. Il vient que $n \neq 0$.

A titre d'exemples pour tout $n \in \mathbb{N}^*$ Dans la suite nous montrons que tout groupe fini d'ordre premier est cyclique.

Proposition 3.1.46 : *Tout groupe fini d'ordre un nombre premier p est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Soit G un groupe tel que $o(G)$ soit un nombre premier. Comme G n'est pas réduit à son élément neutre (rappelons au passage que 1 n'est pas premier), nous pouvons choisir $g \in G$ tel que $g \neq e$. D'après le théorème de Lagrange, $o(g)$ divise $o(G)$. Mais puisque $o(G)$ est premier et $g \neq e$, nous obtenons $o(g) = o(G)$ et par suite $G = \langle g \rangle$. Autrement dit G est cyclique. Nous

pouvons ainsi conclure grâce à 3.1.45. Achéons cette section par un exemple d'un groupe cyclique tiré de la géométrie plane. Supposons que \mathbb{R}^2 soit muni de sa structure canonique de plan affine euclidien et choisissons $n \in \mathbb{N}^*$. Considérons Π_n , un polygone régulier à n cotés. Muni de la composition des applications, l'ensemble $D(\Pi_n)$ des déplacements de \mathbb{R}^2 laissant globalement invariant Π_n est cyclique d'ordre n et la rotation de centre l'isobarycentre de Π_n et d'angle $2\pi/n$ est un générateur de $D(\Pi_n)$. Tenant compte de 3.1.43, nous pouvons représenter un groupe cyclique d'ordre n de différentes manières : La première est algébrique avec μ_n , la deuxième relève de l'arithmétique avec $\mathbb{Z}/n\mathbb{Z}$ et la troisième est de nature géométrique avec $D(\Pi_n)$.

3.2 Générateurs d'un groupe monogène:

Comme les seuls sous-groupes de \mathbb{Z} sont de la forme $n\mathbb{Z}$ avec $n \in \mathbb{N}$, nous pouvons appliquer 3.1.44 pour voir que tout sous groupe non réduit à l'élément neutre d'un groupe monogène infini est isomorphe à $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}^*$.

Proposition 3.2.47 : *Tout sous-groupe non réduit à l'élément neutre d'un groupe monogène infini (respectivement, d'un groupe cyclique) est monogène infini (respectivement, un groupe cyclique).*

Démonstration. Compte tenu de ce qui a été dit juste avant cette proposition, il nous reste à envisager le cas d'un groupe cyclique. D'après 3.1.45, il suffit de montrer que si $n \in \mathbb{N}$ alors tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Soit alors H un sous groupe de $\mathbb{Z}/n\mathbb{Z}$. L'image réciproque $s^{-1}(H)$ par la surjection canonique s de \mathbb{Z} sur $\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de \mathbb{Z} . Il existe alors $m \in \mathbb{N}$ tel que $s^{-1}(H) = m\mathbb{Z}$. La restriction de s à $m\mathbb{Z}$ induit manifestement un morphisme de groupes surjectif de $m\mathbb{Z}$ sur H . Le reste se déduit directement de 3.1.42. Dans la suite, nous caractérisons les diviseurs de l'ordre d'un groupe cyclique en fonctions de ses sous-groupes.

Théorème 3.2.48 : *Soient G un groupe cyclique et d un entier naturel non nul. Alors d divise $o(G)$ si, et seulement si, il existe un unique sous-groupe de G d'ordre d .*

Démonstration. S'il existe un unique sous-groupe de G d'ordre d alors le théorème de Lagrange prouve que d divise $o(G)$. Inversement, supposons que d divise $o(G)$ et posons $q = o(G)/d$.

Considérons un générateur g de G et notons $f = g^q$. Si $f^{d-1} = e$ alors $g^{o(G)-q} = e$, ce qui contredit le fait que g est d'ordre $o(G)$. Donc $f^{d-1} \neq e$. Par ailleurs, $f^d = g^{qd} = g^{o(G)} = e$. Il vient que f est d'ordre d . Le sous-groupe $\langle f \rangle$ de G est d'ordre d . L'existence étant établie, prouvons l'unicité. Soit H un sous-groupe d'ordre d de G . Comme G est cyclique, il en est de même pour H et ce d'après 3.2.47. Soit h un générateur de H . Il existe $r \in \{1, \dots, o(G) - 1\}$ tel que $h = g^r$. Ainsi, $g^{rd} = h^d = e$ car h est d'ordre d . Il vient que $o(G) = qd$ divise rd . Donc q divise r . Posons $\ell = r/q$ et observons que

$$h = g^r = g^{\ell q} = f^\ell \in \langle f \rangle$$

Donc, d'une part $\langle h \rangle$ et $\langle f \rangle$ sont deux groupes cycliques d'ordre d et, d'autre part, $h \in \langle f \rangle$. Il en résulte que $H = \langle h \rangle = \langle f \rangle$ et l'unicité en découle. Les groupes finis d'ordre premiers (qui sont cycliques d'après 3.1.46) peuvent-être caractérisés en fonctions de leurs sous-groupes. Mais rappelons d'abord que les sous-groupes triviaux du groupe G sont $\{e\}$ et G .

Corollaire 3.2.49 : *Soit G un groupe non réduit à son élément neutre. Alors G est fini d'ordre premier si, et seulement, si les seuls sous-groupes de G sont les sous-groupes triviaux.*

Démonstration. Si G est d'ordre premier alors, d'après le théorème de Lagrange, les sous-groupes triviaux de G sont les seuls sous-groupes de G . Inversement, supposons que les sous-groupes triviaux de G sont les seuls sous-groupes de G et choisissons $g \in G$ avec $g \neq e$. Donc le sous-groupe $\langle g \rangle$ de G engendré par g n'est pas réduit à $\{e\}$ et donc, en vertu de la condition imposée à G , $\langle g \rangle = G$.

Il vient que G est monogène. Le reste peut être établi aisément via 3.2.48. La deuxième partie de cette section est consacrée aux générateurs d'un groupe monogène.

Théorème 3.2.50 : *Tout groupe monogène infini possède exactement deux générateurs inverse l'un de l'autre.*

Démonstration. Soient G un groupe monogène infini et g un générateur de G . Soit h un autre générateur de G et φ_h l'isomorphisme de groupes de \mathbb{Z} sur G défini par:

$$\varphi_h(m) = h^m \text{ pour tout } m \in \mathbb{Z}$$

Comme g est un générateur de G , $\varphi_h^{-1}(g)$ est obligatoirement un générateur de \mathbb{Z} .

Mais les seuls générateurs de \mathbb{Z} sont manifestement 1 et -1. Donc,

$$g = \varphi_h(1) = h \text{ ou } g = \varphi_h(-1) = h^{-1}. \text{ Ce qu'il fallait démontrer.}$$

Envisageons le cas fini. Notons $m \wedge n$ (respectivement, $m \vee n$) le plus grand diviseur commun (respectivement, le plus petit multiple commun) de deux entiers naturels non nuls m et n . En particulier, m et n sont premiers entre eux si, et seulement si, $m \wedge n = 1$.

Théorème 3.2.51 : *Soient G un groupe cyclique non réduit à son élément neutre et g un générateur de G . Alors un élément $h \in G$ engendre G si, et seulement si, il existe $m \in \{1, 2, \dots, o(G) - 1\}$ tel que $h = g^m$ et $m \wedge o(G) = 1$.*

Démonstration. Supposons que $h \in G$ soit un générateur de G .

Comme $G \neq \{e\}$ et $h \in G = \{e, g, g^2, \dots, g^{o(G)-1}\}$ il existe $m \in \{1, \dots, o(G) - 1\}$ tel que $h = g^m$. Alors:

$$e = g^{m \vee o(G)} = h^{o(G)/m \wedge o(G)}$$

Or, étant générateur de G , h est d'ordre $o(G)$. D'après le théorème de Lagrange, $o(G)$ divise $o(G) = m \wedge o(G)$. Par suite, $m \wedge o(G) = 1$. Inversement, supposons qu'il existe $m \in \{1, 2, \dots, o(G) - 1\}$ tel que $h = g^m$ et $m \wedge o(G) = 1$.

D'après l'identité de Bezout, il existe $u, v \in \mathbb{Z}$ tels que $um + vo(G) = 1$. Donc:

$$g = g^{um+vo(G)} = h^u$$

Nous déduisons aussitôt que h engendre G . Soient $n \in \mathbb{N}$ et $m \in \{1, 2, \dots, n\}$. D'après 3.2.53, la classe de congruence de m modulo n engendre le groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ si, et seulement si, m est premier avec n .

Chapitre 4

Qualques application aux groupes finis:

4.1 Représentations linéaires des groupes :

4.1.1 Définitions:

Définition 4.1.52 : *On appelle représentation linéaire d'un groupe G la donnée d'un espace vectoriel V et d'un morphisme de groupes :*

$$\rho : G \rightarrow GL(V)$$

L'espace vectoriel V est l'espace de la représentation et la dimension de V son degré. Dans toute la suite, nous n'étudierons que des représentations de groupes finis, à valeurs dans des C -espaces vectoriels de dimension finie.

On peut alors raisonner en termes de matrices puisque l'image de G par ρ est un sous-groupe de $GL(V)$ qui s'identifie par le choix d'une base à $GL_n(C)$ où n est la dimension de V .

Définition 4.1.53 : *On dit que deux représentations linéaires d'un même groupe G , $\rho_i : G \rightarrow GL(V_i), i = 1, 2$, sont équivalentes s'il existe un isomorphisme d'espaces vectoriels, $f : V_1 \rightarrow V_2$, tel que: $\forall g \in G, \rho_2(g) \circ f = f \circ \rho_1(g)$*

En termes de matrices cela signifie que les matrices associées à la première représentation sont semblables à leurs homologues dans la seconde, via la même matrice de passage.

Exemple 4.1.54 :

1. Tous les groupes possèdent la représentation triviale (ou représentation identité) qui envoie tout élément de G sur Id_C . (L'espace de la représentation est C .)

Définition 4.1.55 : Soit V un espace vectoriel et G un groupe. On dit que V est un G -module s'il est muni d'un morphisme de groupes $\rho : G \rightarrow GL(V)$. Cela équivaut à la donnée d'une multiplication externe $G \times V \rightarrow V$ telle que :

1. $gv \in V$
2. $g(cv + dw) = c(gv) + d(gw)$
3. $(gh)v = g(hv)$
4. $1Gv = v$

Pour tous $g, h \in G, v, w \in V, c, d \in C$.

Une représentation de G correspond donc à un G -module.

Définition 4.1.56 : Soit $\rho : G \rightarrow GL(V)$ une représentation linéaire de G , et W un sous-espace vectoriel de V . On dit que W est stable par G si W est stable par tous les $\rho(g)$, $g \in G$. La restriction de ρ à W est alors une représentation de G dans W . Cela correspond à dire que W est un sous- G -module de V .

Théorème 4.1.57 : Soit $\rho : G \rightarrow GL(V)$ une représentation de G , et W un sous-espace stable par G . Alors, il existe un supplémentaire W_0 de W stable par G .

Démonstration: Soit W_1 un supplémentaire quelconque de W dans V , et p le projecteur de V sur W correspondant. Posons :

$$p_0 = \frac{1}{|G|} \sum_{t \in G} \rho(t)p(t)^{-1}, \quad |G| \text{ étant l'ordre de } G$$

Alors, p_0 est un projecteur de V sur W qui commute à tous les éléments de G , donc son noyau, W_0 est stable par G .

Définition 4.1.58 : Une représentation $\rho : G \rightarrow GL(V)$ (resp. un G -module) est dit(e) irréductible (ou simple) si V n'est pas réduit à zéro et si aucun sous-espace vectoriel strict non nul de V n'est stable par G (resp. si V n'admet aucun sous-module autre que lui-même et $\{0\}$).

On vérifie aisément qu'une représentation est irréductible si et seulement si le module associé l'est.

Théorème 4.1.59 : Toute représentation est somme directe de représentations simples.

Démonstration: On raisonne par récurrence sur $\dim(V)$. Si $\dim(V) = 0$ le résultat est clair. Supposons $\dim(V) > 1$. Si V est irréductible il n'y a rien à démontrer. Sinon on peut décomposer V en $V' \oplus V''$ avec V' et V'' de dimensions strictement inférieures à $\dim(V)$ ce qui permet de passer à la récurrence.

Théorème 4.1.60 : Lemme de Schur

Soient V et W deux modules irréductibles de G et $f : V \rightarrow W$ un morphisme de G -modules. Alors $f = 0$ ou f est un isomorphisme de G -modules.

Démonstration: Comme $\ker f$ est un sous-module de V qui est irréductible ce ne peut être que $\{0\}$ ou V . De même grâce à l'irréductibilité de W , $\operatorname{Im} f = \{0\}$ ou $\operatorname{Im} f = W$ ce qui prouve ce qu'on veut.

Corollaire 4.1.61 : Si ρ_1 et ρ_2 sont deux représentations irréductibles non équivalentes, et si $f : V_1 \rightarrow V_2$ est linéaire et vérifie $\forall g \in G, f \cdot \rho_1(g) = \rho_2(g) \cdot f$, alors $f = 0$.

Démonstration: Il suffit de traduire le lemme de Schur en termes de représentations.

Corollaire 4.1.62 : Soit $\rho : G \rightarrow GL(V)$ une représentation irréductible de G (V étant un \mathbb{C} -espace vectoriel de dimension finie). Un endomorphisme f (d'espace vectoriel) de V qui commute à tous les $\rho(g)$, $g \in G$ est une homothétie.

Démonstration.: Comme C est algébriquement clos f admet une valeur propre λ . Mais alors $f - \lambda \text{id}_V$ commute aussi à tous les $\rho(g), g \in G$ donc c'est un morphisme de G -modules. Or $f - \lambda \text{id}_V$ n'est pas injectif d'après le lemme de Schur il est nul : $f = \lambda \text{id}_V$ est une homothétie.

4.1.2 Théorie des caractères

Définition 4.1.63 : Soit $\rho : G \rightarrow GL(V)$ une représentation de G . Pour tout $s \in G$, posons :

$$\chi_\rho(s) = \text{Tr}(\rho(s))$$

On obtient ainsi une fonction χ_ρ sur G à valeurs complexes appelée caractère de la représentation ρ . On démontre alors aisément les propriétés suivantes :

Proposition 4.1.64 : Si χ est le caractère d'une représentation ρ de degré n , on a :

1. $\chi(1) = n$
2. $\chi(s^{-1}) = \chi(s)^*$ (conjugué complexe de $\chi(s)$), pour tout $s \in G$
3. $\chi(tst^{-1}) = \chi(s)$, pour tous $s, t \in G$
4. Si ρ_1 et ρ_2 sont deux représentations irréductibles équivalentes, alors,

$$\chi_{\rho_1} = \chi_{\rho_2}.$$

Définition 4.1.65 : Soient χ et ψ deux fonctions de G dans \mathbb{C} . On définit le produit scalaire de χ et ψ par :

$$\langle \chi, \psi \rangle = \frac{1}{|G|} \sum_{t \in G} \chi(t) \psi(t)^* = \frac{1}{|G|} \sum_{t \in G} \chi(t) \psi(t^{-1})$$

Théorème 4.1.66 : Soient χ et ψ deux caractères irréductibles de G , alors :

$$\langle \chi, \psi \rangle = \delta_{\chi, \psi} \text{ (symbole de Kronecker)}$$

Démonstration: Soient $A = (a_{ij})$ et $B = (b_{ij})$ les matrices des représentations associées à χ et à ψ , de degrés d et f respectivement (les a_{ij} et les b_{ij} sont des fonctions de G dans C). Soit $X = (x_{ij})$ une matrice $d \times f$ quelconque. Posons :

$$Y = \frac{1}{|G|} \sum_{t \in G} A(t)XB(t^{-1})$$

Alors, pour tout $s \in G$,

$$A(s)YB(s^{-1}) = \frac{1}{|G|} \sum_{t \in G} A(st)XB((st)^{-1}) = Y$$

Donc, pour tout $s \in G$, $A(s)Y = YB(s)$.

4.2 Représentations du groupe symétrique:

4.2.1 Tableaux de Young:

Dans cette section il s'agit de construire toutes les représentations irréductibles (à isomorphisme près) du groupe symétrique. Dénérale le nombre de représentations irréductibles d'un certain groupe (à isomorphisme près) est égal au nombre de classes de conjugaison de ce groupe. Dans le cas du groupe symétrique S_n c'est le nombre de partitions de n . On écrit $\lambda \vdash n$ pour la partition $\lambda = (\lambda_1, \dots, \lambda_l)$, $n = |\lambda| = \sum_i \lambda_i$, $\lambda_1 \geq \lambda_2 \geq \dots \geq \lambda_l$. Une méthode pour visualiser une partition est la notion de diagramme de Ferrer.

Définition 4.2.67 : Soit $\lambda = (\lambda_1, \dots, \lambda_l) \vdash n$. Le diagramme de Ferrer t de forme λ est un tableau avec l lignes, tel que la i -ème ligne contienne λ_i cases, $i = 1, \dots, l$.

Définition 4.2.68 : Soit $\lambda \vdash n$. Remplaçons les cases d'un diagramme de Ferrer de forme λ par les nombres $1, 2, \dots, n$ bijectivement. Le tableau ainsi obtenu est un tableau de Young de forme λ . Si $\lambda = (3, 1)$ alors des exemples de tableaux de Young de forme λ sont

$$\begin{array}{ccc} 4 & 1 & 2 \\ 3 & & \end{array} \quad \begin{array}{ccc} 1 & 2 & 3 \\ 4 & & \end{array} \quad \begin{array}{ccc} 3 & 4 & 1 \\ 2 & & \end{array}$$

Définition 4.2.69 . On dit que deux tableaux t_1 et t_2 de même forme λ sont équivalents et on note $t_1 \sim t_2$ si chaque ligne de t_1 contient les mêmes éléments

que la ligne correspondante de t_2 . On appelle *tabloïde* une classe d'équivalence pour cette relation et on note $\{t\}$ le *tabloïde* associé à t .

$$\begin{aligned} \text{si } \lambda = (2, 1), \quad t = \begin{array}{ccc} 1 & 2 & \\ & & 3 \end{array} \\ \text{alors} \\ \{t\} = \left\{ \begin{array}{ccc} 1 & 2 & 3 & 2 \\ & & & 1 \end{array} \right\} = \frac{1}{3} \overline{2} \end{aligned}$$

Si t est un tableau de Young de forme $\lambda = (\lambda_1, \dots, \lambda_l) \vdash n$, alors le nombre de tableaux dans la classe $\{t\}$ est égal à $\lambda_1! \dots \lambda_l! \stackrel{\text{def}}{=} \lambda!$. Ainsi le nombre de λ -tabloïdes est $\frac{n!}{\lambda!}$. Maintenant on peut considérer l'action du groupe symétrique sur l'ensemble de tabloïdes de forme λ en posant $\pi\{t\} = \{\pi t\}$, $\pi \in S_n$.

Cette action est bien définie i.e. ne dépend pas du choix du représentant de $\{t\}$. Il en découle la notion de S_n -module suivant.

Définition 4.2.70 : Soit $\lambda \vdash n$. Soit $\{\{t_1\}, \dots, \{t_k\}\}$ l'ensemble des λ -tabloïdes. Alors $M^\lambda = \mathbb{C}[\{t_1\}, \dots, \{t_k\}]$ est un module de permutation correspondant à λ .

Dans la suite on aura besoin d'encore une définition.

Définition 4.2.71 : Soit M un G -module. Il est dit *cyclique* s'il existe $v \in M$ tel que $Gv = \{gv, g \in G\}$ engendre linéairement M . On dit aussi que le G -module M est engendré par v .

Proposition 4.2.72 :

1. M^λ est cyclique engendré par un λ -tabloïde quelconque. De plus

$$\dim M^\lambda = \frac{n!}{\lambda!}$$

2. V^λ et M^λ sont isomorphes comme S_n -modules.

Démonstration.

1. Il suffit de noter que S_n agit transitivement sur l'ensemble des λ -tabloïdes.

2. Puisque M^λ est cyclique il est engendré comme S_n -module par un tabloïde $\{t\}$ quelconque.

Si π_1, \dots, π_k est une transversale de S_λ alors l'application $\theta : V^\lambda \rightarrow M^\lambda : \pi_i S_\lambda \mapsto \{\pi_i t\}$ est un isomorphisme de S_n -modules.

4.2.2 Tableaux standards et base de S^λ :

En général les polytabloïdes qui engendrent S^λ ne sont pas linéairement indépendants. On cherche donc ici à déterminer une sous-famille de polytabloïdes qui forment une base de S^λ .

Définition 4.2.73 : *Un tableau t est dit standard si ses lignes et ses colonnes sont croissantes. Dans ce cas on dit aussi que les tabloïde et polytabloïde correspondants sont standards.*

$$t = \begin{array}{ccc} 1 & 2 & 3 \\ & 4 & 6 \\ & & 5 \end{array}$$

est standard mais

$$t = \begin{array}{ccc} 1 & 2 & 3 \\ & 5 & 4 \\ & & 6 \end{array}$$

ne l'est pas.

Définition 4.2.74 : *Une composition de n est un l -uplet d'entiers strictement positifs $\lambda = (\lambda_1, \dots, \lambda_l)$ tel que $\sum_i \lambda_i = n$. Les entiers $\lambda_1, \dots, \lambda_l$ sont appelés les parties de la composition. On étend de manière évidente les définitions de diagramme de Ferrer et de tableau pour les compositions. La relation de domination s'étend aussi clairement aux compositions.*

Définition 4.2.75 : *Soit $\{t\}$ un tabloïde de forme λ partition de n . Pour tout i entre 1 et n on définit :*

$$\begin{aligned} \{t^i\} &= \text{le tabloïde formé des éléments de } \{t\} \text{ inférieurs à } i \\ \lambda_i &= \text{la composition qui est la forme de } \{t^i\} \end{aligned}$$

Définition 4.2.76 : *Soit $\{s\}$ et $\{t\}$ deux tabloïdes ayant pour suites de compositions λ^i et μ^i respectivement. On dit que $\{s\}$ domine $\{t\}$ si pour tout i , $\lambda^i \supseteq \mu^i$.*

Lemme 4.2.77 : *Lemme de domination pour les tableaux*

Si $k < l$, et si k apparaît dans une ligne en-dessous de l dans $\{t\}$ alors:

$$\{t\} \triangleleft (k, l)\{t\}$$

Démonstration. Supposons que $\{t\}$ et $(k, l)\{t\}$ ont les suites de compositions λ^i et μ^i . Alors

pour $i < k$ ou $i \geq l$ on a $\lambda^i = \mu^i$.

Etudions maintenant le cas $k \leq i < l$. Si r et q sont les lignes de $\{t\}$ dans lesquelles k et l apparaissent (respectivement), alors : $\lambda^i = \mu^i$ avec la q^e partie diminuée de 1 et la r^e augmentée de 1. Or par hypothèse $q < r$ on trouve donc $\lambda^i \triangleright \mu^i$.

Définition 4.2.78 : Si $v = \sum_i c_i \{t_i\} \in M^\mu$ on dit que $\{t_i\}$ apparaît dans v si $c_i \neq 0$.

Proposition 4.2.79 : Si t est standard et si $\{s\}$ apparaît dans e_t alors $\{t\} \trianglerighteq \{s\}$.

Démonstration : Ecrivons $s = \pi t$ où $\pi \in C_t$ de sorte que $\{t\}$ apparaît dans e_t . On raisonne par récurrence sur le nombre d'inversions de colonne dans s , i.e. le nombre de paires $k < l$ dans la même colonne de s telles que k apparaît plus bas que l . Si s n'a pas d'inversion $s = t$. Ensuite si (k, l) est une inversion

$$\{s\} \triangleright (k, l)s$$

d'après le lemme précédent. Comme $(k, l)\{s\}$ a moins d'inversions que s , $(k, l)\{s\} \trianglelefteq \{t\}$ ce qui achève la récurrence.

Définition 4.2.80 : Soit (A, \geq) un ensemble partiellement ordonné. Un élément $b \in A$ est appelé *maximum* si $\forall c \in A, b \geq c$. Un élément b est dit *maximal* s'il n'existe pas de $c \in A$ vérifiant $c > b$.

Lemme 4.2.81 : Soit v_1, v_2, \dots, v_m des éléments de M^μ . Supposons que pour chaque v_i on puisse choisir un tableau $\{t_i\}$ qui apparaît dans v_i tel que :

1. $\{t_i\}$ est maximum dans v_i
2. les $\{t_i\}$ sont tous distincts.

Alors v_1, \dots, v_m sont linéairement indépendants.

Définition 4.2.82 : Soit $\{s\}$ et $\{t\}$ deux tableaux ayant pour suites de compositions λ^i et μ^i respectivement. On dit que $\{s\}$ domine $\{t\}$ si pour tout i , $\lambda^i \supseteq \mu^i$.

Lemme 4.2.83 : Lemme de domination pour les tableaux

Si $k < l$ et si k apparait dans une ligne en-dessous de l dans $\{t\}$ alors $\{t\} \triangleleft (k, l)\{t\}$.

Démonstration: Supposons que $\{t\}$ et $(k, l)\{t\}$ ont les suites de compositions λ^i et μ^i . Alors

pour $i < k$ ou $i \geq l$ on a $\lambda^i = \mu^i$.

Etudions maintenant le cas $k \leq i < l$. Si r et q sont les lignes de $\{t\}$ dans lesquelles k et l apparaissent (respectivement) alors :

$\lambda^i = \mu^i$ avec la q^e partie diminuée de 1 et la r^e augmentée de 1. Or par hypothèse $q < r$ on trouve donc $\lambda^i \triangleleft \mu^i$.

Définition 4.2.84 : Si $v = \sum_i c_i \{t_i\} \in M^\mu$ on dit que $\{t_i\}$ apparait dans v si $c_i \neq 0$.

Proposition 4.2.85 : Si t est standard, et si $\{s\}$ apparait dans t alors $\{t\} \supseteq \{s\}$.

Démonstration. 'Ecrivons $s = \pi t$ ou $\pi \in C_t$ de sorte que $\{t\}$ apparait dans e_t . On raisonne par récurrence sur le nombre d'inversions de colonne dans s i.e. le nombre de paires $k < l$ dans la même colonne de s telles que k apparait plus bas que l . Si s n'a pas d'inversion $s = t$. Ensuite si (k, l) est une inversion

$$\{s\} \triangleleft (k, l)s$$

d'après le lemme précédent. Comme $(k, l)\{s\}$ a moins d'inversions que s $(k, l)\{s\} \supseteq \{t\}$ ce qui achève la récurrence.

Définition 4.2.86 : Soit (A, \geq) un ensemble partiellement ordonné. Un élément $b \in A$ est appelé maximum si $\forall c \in A, b \geq c$. Un élément b est dit maximal s'il n'existe pas de $c \in A$ vérifiant $c > b$.

Théorème 4.2.87 : *La famille $F = \{e_t : t \text{ est un } \lambda\text{-tableau standard}\}$ est linéairement indépendante.*

Démonstration: $\{t\}$ est maximum dans e_t , e_t par hypothèse, les éléments de F sont distincts donc le lemme précédent s'applique. On veut maintenant montrer que cette famille est une base de S^λ il reste donc à prouver qu'elle engendre S^λ .

Définition 4.2.88 : *Soit A et B deux ensembles disjoints d'entiers positifs. On choisit des permutations π telles que :*

$$S_{A \cup B} = \bigsqcup_{\pi} \pi(S_A \times S_B).$$

L'élément de Garnir correspondant est :

$$g_{A,B} = \sum_{\pi} (\text{sgn } \pi) \pi.$$

Définition 4.2.89 *Soit t un tableau et A et B des parties des colonnes j et $j+1$ respectivement. L'élément de Garnir associé à t (et A, B) est $\Sigma_{\pi} : \pi(\text{sgn } \pi)$ o'ù les π ont été choisis de sorte que les éléments de $A \cup B$ croissent quand on descend les colonnes de t .*

Proposition 4.2.90 : *Soit t , A et B comme dans la définition précédente. Si $|A \cup B|$ est strictement supérieur au nombre d'éléments dans la j^e colonne de t alors $g_{A,B^{e_t}} = 0$.*

Démonstration: Montrons d'abord que $S_{g_{A,B^{e_t}}}^- = 0$

Soit $\sigma \in C_t$ quelconque. D'après les hypothèses il existe $a, b \in A \cup B$ tels que a et b sont dans la même ligne de σt . Mais alors, $(a, b) \in S_{A \cup B}$ donc $S_{A \cup B}^- \{\sigma t\} = 0$ grace au lemme du signe. Comme ceci vaut pour tout σ apparaissant dans k_t on a bien $S_{g_{A,B^{e_t}}}^- = 0$.

Or, $S_{A \cup B} = \bigsqcup_{\pi} \pi(S_A \times S_B)$ donc $S_{A \cup B}^- = g_{A,B}(S_A \times S_B)^-$. En substituant dans l'équation précédente on trouve :

$$g_{A,B}(S_A \times S_B)^- e_t = 0$$

Mais $(S_A \times S_B) \subset C_t$ donc pour $\sigma \in S_A \times S_B$ par le lemme du signe

$$\sigma^- e_t = \sigma^- C_t^- \{t\} = C_t^- \{t\} = e_t$$

Par suite $(S_A \times S_B)^- e_t = |S_A \times S_B| e_t$ et donc $g_{A,B} e_t = 0$.

Définition 4.2.91 : Soit t un tableau, on définit son *tableau de colonne* par :

$$[t] = C_t$$

i.e. l'ensemble des tableaux obtenus en réarrangeant les colonnes de t .

La relation de domination colonne pour les tableaux s'obtient de manière analogue à la relation de domination ligne (i.e. celle définie précédemment).

Définition 4.2.92 : Soit t un tableau, on appelle *descente (de ligne)* de t un couple d'entiers (k, l) , $k < l$ tel que k et l sont adjacents dans une ligne de t , k apparaissant après l .

Théorème 4.2.93 : La famille $F = \{e_t : t \text{ est un } \lambda\text{-tableau standard}\}$ engendre S^λ .

Démonstration: Remarquons tout d'abord que si e_t est engendré par cette famille alors e_s aussi pour tout $s \in [t]$ (en effet on a alors $s = \pi t$ ou $\pi \in C_t$ donc $e_t = (\text{sgn } \pi) e_s$). Ainsi on peut supposer que les colonnes de t sont croissantes. L'ensemble partiellement ordonné des tableaux de colonne admet un élément maximum $[t_0]$ ou t_0 s'obtient en numérotant les cases du tableau de haut en bas, en commençant par la colonne la plus à gauche. Comme t_0 est standard e_{t_0} est engendré par F .

Soit maintenant t un tableau quelconque. Par récurrence on suppose que tout tableau $s \triangleright t$ est engendré par F . Si t est standard il n'y a rien à prouver. Sinon t possède une descente dans une ligne notée i (puisque les colonnes sont

croissantes). Notons aussi j et $j+1$ les numéros des colonnes concernées par cette descente et $a_1 < \dots < a_p$; $b_1 < \dots < b_q$ les entiers qu'elles contiennent respectivement. On a donc :

$$\begin{array}{cc}
 a_1 & b_1 \\
 & \wedge \\
 a_2 & b_2 \\
 \vdots & \wedge \\
 \vdots & \vdots \\
 & \wedge \\
 a_i & b_i \\
 & \wedge \\
 \vdots & \vdots \\
 \wedge & b_q \\
 a_p &
 \end{array}$$

Prenons $A = \{a_i, \dots, a_p\}$ et $B = \{b_1, \dots, b_i\}$. L'élément de Garnir associé $g_{A,B}$ vérifie $g_{A,B}e_t = 0$ donc :

$$e_t = - \sum_{\pi \neq id} (\text{sgn } \pi) e_{\pi t}$$

Enfin, $b_1 < \dots < b_i < a_i < \dots < a_p$ implique que $[\pi t] \triangleright [t]$ pour $\pi \neq id$, grace à l'analogue colonne du lemme de domination pour les tableaux. L'hypothèse de récurrence permet de conclure.

Théorème 4.2.94 : *Résumons les résultats que nous avons obtenus : soit f^λ le nombre de λ -tableaux standards alors:*

1. La famille $F = \{e_t : t \text{ est un } \lambda\text{-tableau standard}\}$ est une base de S^λ .
2. $\dim S^\lambda = f^\lambda$
3. $\sum_{\lambda \vdash n} (f^\lambda)^2 = n!$

4.2.3 Représentation naturelle de Young

Les matrices de la représentation S^λ dans la base standard constituent ce qu'on appelle la représentation naturelle de Young. Dans cette partie, nous allons montrer comment obtenir ces matrices. Comme S_n est engendré par les transpositions de la forme $(k, k+1)$ il suffit de

calculer les matrices correspondant à ces éléments. Pour un tableau t donné il y a trois

possibilités :

1. Si k et $k+1$ sont dans la même colonne alors $(k, k+1) \in C_t$ puis

$$(k, k+1)e_t = -e_t.$$

2. Si k et $k+1$ sont dans la même ligne alors $(k, k+1)t$ a une descente dans cette ligne. On calcule donc $(k, k+1)$ à l'aide des éléments de Garnir : $(k, k+1)e_t = e_t +$ d'autres polytabloïdes $e_{t'}$ avec $[t'] \triangleright [t]$.

3. Si k et $k+1$ ne sont ni dans la même ligne ni dans la même colonne alors $t' = (k, k+1)t$ est standard et $(k, k+1)e_t = e_{t'}$.

Le e_t dans la somme du deuxième cas provient du terme $(k, k+1)$ dans l'élément de Garnir. Bien que nous n'ayons pas d'expression immédiate des autres polytabloïdes comme combinaisons linéaires de polytabloïdes standards une application itérée de ces trois cas permet de les calculer.