UNIVERSITE MOHAMED BOUDIAF DE M'SILA

Faculté des Mathématiques et de l'Informatique

Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Algèbre et Mathématique Discrètes

Par

Nabiha Ben madani

Sujet

Sur le produit en couronne de groupes

Devant le jury :

Mr. Nourdine Midoune	MCA. Univ de M'sila	Président
Mr. Nacer Ghadbane	MCB. Univ de M'sila	Encadreur
Mr. Lakhdar Heboub	MAA. Univ de M'sila	Examinateur

Promotion : 2017 / 2018

Remerciements

Je remercie tout d'abord mon Dieu qui m'a donné la force pour terminer ce modeste travail.

Je tiens à remercier mon promoteur: le professeur ***N.Ghadbane*** *pour la confiance qu'il m'a témoignée en me proposant ce sujet, ses encouragements et sa patience.*

Les discussions scientifiques qu'il a su générer, ses remarques et ses suggestions qui m'ont permis de finaliser ce modeste travail. Je souhaite lui transmettre ma reconnaissance et ma plus profonde gratitude.

Je remercie aussi tous les membres du Jury pour l'honneur qu'ils m'ont fait, en acceptant de juger ce travail.

Je ne peux pas clôturer mes remerciements sans se retourner vers les êtres qui me sont les plus chers; ma famille qui ont eu un rôle essentiel et continu dans ma réussite.

Merci

Dédicace

Je dédie ce modeste travail :

-À mes parents ma mère et mon père.

-À mes frères RACHID, KHALIL, ABDELGHANI

-À mes soeurs AHLEM, HABIBA, RAHMA, NESRIN

-À la femme de mon frère HANAN.

-À toute la famille.

-À tous mes amies.

-Je tiens à remercier l'ensemble de tous les étudiants et toutes les étudiantes de ma promotion,

En fin je dédie ce mémoire à mes collègues et tous ceux qui me sont chers.

Table des matières

Notations

$\emptyset$: l'ensemble vide

GL_n : groupe linéaire des matrices

$\langle B \rangle$: sous-groupe engendré par la partier B

$|G|$: l'ordre de G

$O(x)$: l'ordre de x

Aut : automorphisme

$\simeq$: isomorphe

$\ker f$: noyau de f

$\mathrm{Im}\, f$: image de f

R_g: relation d'équivalence à gauche

R_d: relation d'équivalence à droite

(G/H) : ensemble des classes

$H \lhd G$: H est sous-groupe normale de G

$[G : H]$: indice de H dans G

$Orb(x)$: orbite de x

S_n : groupe symétrique

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

$Supp$: support

A_n : groupe alterné

$G_1 \times G_2$: produit direct de G_1 et G_2

$H \rtimes_\theta G$: produit semi-direct de H par G relativement à θ

GW_rH : produit en couronne de G et H.

Introduction générale

La notion de groupe a été introduite explicitement en mathématique, au début du dix-neuvième siècle. Elle intervient en effet à cette époque, pour la première fois, dans les travaux relatifs aux équations algébriques dans les travaux d'Evariste Galois (1811-1832) . A peu près au même moment, les groupes commencent à jouer un rôle en géométrie, notamment, des groupes de symétries de polygones ou polyèdres réguliers. Ainsi, 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, progressivement, a été construite la théorie des groupes.

Les groupes sont à la base d'autres notions mathématiques comme les anneaux, les corps, les espaces vectoriels. Mais vous les retrouvez aussi en arithmétique, en cryptographie.

Le produit en couronne dans la théorie de groupe est un produit spécialisé de deux groupes. Le produit en couronne est un outil important dans la classification des groupes de permutation.

Ce mémoire se compose de trois chapitre :

Dans le premier chapitre on donne un rappel des notions et notations utilisées par la suite : lois de compositions internes, notion de groupe, sous-groupe, homomorphisme de groupe, relation déquivalence modulo un sous-groupe, théorème de Lagrange, groupe quotient, groupe cyclique, groupe opérant sur un ensemble.

Dans le deuxième chapitre nous avous étudier les groupes symètriques et quelques propriétés.

Dans le troisième chapitre on étudie le produit direct, produit semi direct, et produit en couronne de groupes, et dans la fin de ce chapitre, en applicant le produit en couronne sur le groupe de permutation.

Chapitre 1

Notions élémentaires sur les groupes

Introduction

Ce premier chapitre contient les définitions et les propriétés des outils que nous utiliserons par la suite : lois de compositions internes, notion de groupe, sous-groupe, homomorphisme de groupe, relation d'équivalence modulo un sous-groupes, théorème de Lagrange, groupe quotient, groupe cyclique, groupe opérant sur un ensemble.

Contenu

1.7. Groupe quotient.

1.8. Groupe cyclique.

1.9. Groupe opérant sur un ensemble.

1.1 Lois de compositions internes

Définition 1.1.1

Une loi de composition interne sur un ensemble E est une application de $E \times E$ dans E. À un couple (x, y), on associe, donc un élément noté $x * y$, $x + y$, ou $xy, ...$, appelé composé de x et de y . Une loi de composition interne sur E est :

1- Associative si : $\forall x, y, z \in E, (x * y) * z = x * (y * z)$;

2- commutative si : $\forall x, y \in E, x * y = y * x$;

3- elle admet un élément neutre e si $\forall x \in E : x * e = e * x = x$, si l'élément neutre existe, il est unique ;

4- un élément x est inversible (ou symétrisable) dans $(E, *)$ s'il existe $x^{'} \in E$, (dit inverse ou symétrique de x) tel que : $x * x^{'} = x^{'} * x = e$.

Exemples 1.1.2

1- $E = \mathbb{N}$ et $* = +$

$$+ : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$$

$$(n, m) \longmapsto n + m$$

2- $E = \mathbb{R}$ et $* = \times$

$$\times : \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

$$(x, y) \longmapsto x \cdot y$$

1.2 Notions de groupes

Définition 1.2.1

Soit G un ensemble non vide muni d'une loi de composition interne noté " $*$ ". G est un groupe pour la loi " $*$ " si :

1- La loi " $*$ "est associative : $\forall x, y, z \in G : x * (y * z) = (x * y) * z$;

2- la loi " $*$ "possède un élément neutre : $\exists e \in G, \forall x \in G, x * e = e * x = x$;

3- tout élément $x \in G$ possède un symétrique unique $x^{'} \in G$ tel que : $x * x^{'} = x^{'} * x = e$.

Exemples 1.2.2

1- $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sont des groupes abéliens.

2- $(\mathbb{Q}^*, \times), (\mathbb{R}^*, \times), (\mathbb{C}^*, \times)$ sont des groupes abéliens.

3- L'ensemble $GL_n(\mathbb{R})$ des matrices carrées $n \times n$ inversible à coefficients dans $\mathbb{R}$ muni de la multiplication des matrices est un groupe non commutatif. L'élément neutre est la matrice identité.

1.3 Sous-groupe

Définition 1.3.1

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

$$\begin{aligned} (i) H &\neq \emptyset; \\ (ii) \forall a, b &\in H, a * b \in H; \\ (iii) \forall a &\in G^{'}, a^{-1} \in H. \end{aligned}$$

Proposition 1.3.2

Soient $(G,*)$ un groupe et $H \subseteq G$, alors :

$$H \text{ est un sous-groupe de } G \Leftrightarrow \begin{cases} (i) H \neq \emptyset; \\ (ii) \forall a, b \in H, a * b^{-1} \in H. \end{cases}$$

Définition 1.3.3

Soit $(G,\cdot)$ un groupe et H un sous-groupe de G, on dit que H est un sous-groupe distingué ou normale ($H \lhd G$) de G s'il vérifie l'une des propriétés suivantes :

1- $\forall g \in G : gH = Hg$;

2- $\forall g \in G, \forall h \in H : ghg^{-1} \in H$.

Exemples 1.3.4

1- $Z(G) = \{x \in G, xa = ax, \forall a \in G\}$ est appelé le centre du groupe G c'est un sous-groupe de G.

2- $G_n = \left\{z \in \mathbb{C}, \exists k \in \mathbb{N}, (z^n)^k = 1\right\}$ est un sous-groupe de $(\mathbb{C}^*,\cdot)$:

i) $G_n \neq \emptyset; \forall k \in \mathbb{N}, (1^n)^k = 1 \Longrightarrow 1 \in G_n$;

ii) soient $z_{1,}z_2 \in G_n$, on montre que $z_1 \cdot z_2 \in G_n$

on a : $\begin{cases} z_1 \in G_n \Longleftrightarrow \exists k \in \mathbb{N}, (z_1^n)^{k_1} = 1 \\ z_2 \in G_n \Longleftrightarrow \exists k \in \mathbb{N}, (z_2^n)^{k_2} = 1 \end{cases}$

$$\begin{aligned} \text{alors } (z_1 \times z_2)^{n^{h_1+k_2}} &= (z_1^{n^{h_1+k_2}}) \cdot (z_2^{n^{h_1+k_2}}) \\ &= (z_1^{nk_1})^{nk_2} \cdot (z_2^{nk_2})^{nk_1} \\ &= 1^{nk_1} \cdot 1^{nk_2} \end{aligned}$$

donc $z_1 \cdot z_2 \in G_n$.

iii) soit $z \in G_n$, on montre que $z^{-1} = \frac{1}{z} \in G_n$

$$\text{on a } z \in G_n \Longleftrightarrow \exists k \in \mathbb{N}, (z^n)^k = 1$$

$$\Longrightarrow \exists k \in \mathbb{N}, ((\tfrac{1}{z})^n)^k = \tfrac{((1)^n)^k}{((z)^n)^k} = \tfrac{1}{((z)^n)^k} = 1$$

donc $z^{-1} = \frac{1}{z} \in G_n$.

Alors G_n est un sous-groupe de $(\mathbb{C}^*,\cdot)$.

Lemme 1.3.5

Les sous-groupes additifs de $\mathbb{Z}$ *sont de la forme* $n\mathbb{Z}, n \in \mathbb{N}$.

Preuve

$n\mathbb{Z}$ est clairement un sous-groupe de $\mathbb{Z}$. Inversement, soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$, sinon soit $n > 0$, le plus petit tel que $n \in H$ et soit $h \in H$. Alors par division euclidienne, on peut écrire $h = nq + r$, avec $0 \leq r < n$. Mais $r = h - nq \in H$, donc si $r \neq 0$, il y a contradiction avec la minimalité de n, d'où $r = 0$ et $h = nq$ c'est-à-dire $H \subset n\mathbb{Z}$. L'inclusion inverse étant immédiate, $H = n\mathbb{Z}$.

Proposition 1.3.6

L'intersection d'une famille de sous-groupe $H_i, i \in I$ *d'un groupe* G *est un sous-groupe de* G.

Preuve

Soit $H = \cap_{i \in I} H_i \neq \emptyset$;

i) $\forall i \in I, 1_G \in H_i \Longrightarrow 1_G \in \cap_{i \in I} H_i$

$\Longrightarrow H \neq \emptyset$;

ii) $a, b \in H \Longrightarrow \forall i, a, b \in H_i$

$\Longrightarrow \forall i, ab^{-1} \in H_i$

$\Longrightarrow ab^{-1} \in H$.

Proposition 1.3.7

Soit G *un groupe,* $B \subseteq G, \mathcal{F} = \{H/H$ *sous-groupe de* G *qui contient* $B\}$, *alors :*

$\bigcap_{H \in, \mathcal{F}} H$ *est un sous-groupe de* G *appelle sous-groupe engendré par la partie* B, *est noté par* $\langle B \rangle$, *c'est à dire* $\langle B \rangle = \bigcap_{H \in, \mathcal{F}} H$.

Exemple 1.3.8

$\langle \{2\} \rangle = 2\mathbb{Z}$, est un sous-groupe de $(\mathbb{Z}, +)$.

Définition 1.3.9 (Ordre d'un groupe, ordre d'un élément)

Un groupe G est dit fini s'il n'a qu'un nombre fini d'élément. Dans ce cas, le cardinal de G s'appelle l'ordre du groupe G et est noté $|G|$. Soient G un groupe et x un élément de

G. On appelle ordre de x, qu'on note $Ord(x)$, le cardinal de $\langle x \rangle$. Si ce cardinal est infini, on dit que x est d'ordre infini.

Exemples 1.3.10

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

2- $Ord(\mathbb{R}) = \infty$(infinie).

1.4 Homomorphisme de groupes

Dans ce partie, on considère $(G, \cdot)$ et $(H, *)$ deux groupes, avec 1_G et 1_H leurs éléments neutres respectifs.

Définition 1.4.1

Une application $f : G \longrightarrow H$ est appelée homomorphisme de groupes de G dans H si :$\forall a, b \in G : f(a \cdot b) = f(a) * f(b)$. Si f est bijective on dit que f est isomorphisme de groupes de G sur H. On dit alors que G est isomorphe à H qu'on note $G \simeq H$, 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.

Notations 1.4.2

1- L'ensemble des morphismes de groupes de G dans H est noté $Hom(G, H)$.

2- L'ensemble des endomorphismes d'un groupe G est noté $End(G)$.

3- L'ensemble des automorphismes d'un groupe G est noté $Aut(G)$.

Exemples 1.4.3

1- Soient G un groupe et H un sous-groupe de G;

l'injection canonique $i : H \longrightarrow G$

$$x \longmapsto x$$

est un morphisme de groupes.

2- Soient $(\mathbb{R}, +)$ et $(\mathbb{R}, \times)$, des groupes, alors les applications :

$$f : (R, +) \longrightarrow (R, *) \qquad \text{et} \qquad g : (R, *) \longrightarrow (R, +)$$
$$x \longrightarrow \exp(x) \qquad\qquad x \longrightarrow \ln|x|$$

sont des homomorphismes de groupes.

Proposition 1.4.4

Soit $f : G \longrightarrow H$ un homomorphisme de groupes, alors :

1- $f(1_G) = 1_H$;

2- $\forall a \in G : (f(a))^{-1} = f(a^{-1})$;

3- $\forall a \in G, \forall n \in \mathbb{Z} : f(a^n) = (f(a))^n$.

Preuve

1- 1_H étant l'élément neutre de " $*$ " et 1_G celui de " $\cdot$ ", alors

$$f(1_G \cdot 1_G) = f(1_G) = 1_H * f(1_G)$$

et comme f est homomorphisme on déduit que

$$1_H * f(1_G) = f(1_G) * f(1_G)$$

et comme tous les éléments du groupe $(H, *)$ sont réguliers on déduit que $1_H = f(1_G)$.

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

f étant un homomorphisme de groupe alors :

$$f(a) * f(a^{-1}) = f(a \cdot a^{-1}) = f(1_G) \qquad \text{et} \qquad f(a^{-1}) * f(a) = f(a^{-1} \cdot a) = f(1_G)$$

sachant que $f(1_G) = 1_H$ d'après la première propriété on déduit que :

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

3- pour $n = 0, x^0 = 1_G$ et $(f(x))^0 = 1_H$; on est ramené au (i).

Pour $n > 0, x^n = xx...x$ (n fois), d'où

$$f(x^n) = f(x)f(x)...f(x) \text{ } (n \text{ fois})$$

donc $\qquad f(x^n) = (f(x))^n.$

Pour $n < 0$, on pose $n = -n', n' > 0$;

$$x^n = (x^{-1})^{n'} \Longrightarrow f(x^n) = (f(x^{-1}))^{n'} = (f(x))^{-n'}$$

d'où $\qquad f(x^n) = (f(x))^n.$

Définition 1.4.5

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

$$\begin{aligned} \ker f &= f^{-1}(\{1_H\}) \\ &= \{a \in G, f'(a) = 1_H\} \end{aligned}$$

et l'image de f l'ensemble :

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

Proposition 1.4.6

Soit $f : G \longrightarrow H$ un homomorphisme de groupes, alors :

1- *f est injective si, et seulement si* $\ker f = \{1_G\}$*;*

2- *f est surjective si, et seulement si* $\operatorname{Im} f = H$*.*

Théorème 1.4.7 (premier théorème d'isomorphisme)

Considérons deux groupes $(G, *, 1_G)$ et $(H, \cdot, 1_H)$. Soit $f : G \to H$ un morphisme de groupes. Alors, il existe un isomorphisme naturel de groupes

$$G/\ker f \simeq \operatorname{Im} f.$$

1.5 Relation d'équivalence modulo un sous-groupe

Définition 1.5.1

Soit H un sous-groupe d'un groupe G. On définit sur G une relation d'équivalence, appelée relation d'équivalence à gauche (résp, à droite) associée à H, par :
$a\Re_g b \Longleftrightarrow a^{-1}b \in H$ (résp, $a\Re_d b \Longleftrightarrow ab^{-1} \in H$).

La classe à gauche de a pour cette relation est l'ensemble des $b \in G$ qui sont liés à a par $\Re_g$, c'est à dire, l'ensemble $\{b \in G/b\Re_g a\} = \{b \in G/b^{-1}a \in H\} = Ha$ (de même, la classe à droite de a est aH).

Définition 1.5.2

L'ensemble des classes à gauche $(G/H)_g$ est le quotient de G par cette relation d'équivalence (et de même pour $(G/H)_d$).

Lemme 1.5.3

Soit $H < G$ un sous-groupe de G. Il existe une bijection de l'ensemble des classes à droite sur l'ensemble des classes à gauche. D'où $|(G/H)_d| = |(G/H)_g|$.

Preuve

Il faut d'abord définir une application de $(G/H)_d$ dans $(G/H)_g$. Soit donc xH une classe à droite, associons-lui la classe à gauche Hx^{-1}. Cette correspondre est une application. En effet, si on prend deux représentations de la classe xH (c'est à dire deux éléments de xH), x et $x^{'}$, alors $xH = x^{'}H$. La correspondance définie ci-dessus fait correspondre à xH aussi bien Hx^{-1} que $Hx^{'-1}$. Pour qu'elle soit une application, il faut que ces deux classes à gauche coïncident, autrement dit que $x\Re_g x^{'}$. Or $x\Re_d x^{'}$, d'où $x^{-1}x^{'} \in H$ ou encore $x^{-1}x^{'} \in H \Longrightarrow x^{'-1} \in Hx^{-1}$, donc $Hx^{-1} = Hx^{'-1}$ cette application est clairement est bijective, d'où le résultat.

Définition 1.5.4

Le cardinal de l'ensemble des classes à gauche (= le cardinal de l'ensemble des classes à droite) est appelé indice de H dans G et noté $[G : H]$, on a donc $[G : H] = |(G/H)_g| = |(G : H)_d|$.

1.6 Théorème de Lagrange

Théorème 1.6.1 (Lagrange)

L'ordre d'un sous-groupe H d'un groupe fini G divise L'ordre de G. L'indice $[G:H]$ divise aussi $|G|$ et $[G:H] = |G|/|H|$.

Preuve

G est clairement la réunion disjointes des Hx (en effet : tout élément x de G appartient au moins à Hx et $Hx \cap Hy = \emptyset$ ou $Hx = Hy$). D'où $|G| = \sum |Hx|$. De plus, $|Hx| = |H|$, pour tout x, car l'application $H \longrightarrow Hx, h \longrightarrow hx$, est bijective, d'où $|Hx| = |Hy|$, pour tous $x, y \in G$, et la somme ci-dessus est égale au nombre de classes fois $|H|$, ce qui est précisément la formule cherchée. Conséquence : si n ne divise pas $|G|$, alors il n'existe pas de sous-groupe de G d'ordre n, si n divise $|G|$, il n'existe pas nécessairement de sous-groupe d'ordre n.

Corollaire 1.6.2

Soient H, H' deux sous-groupes d'un groupe fini $G, H \subset H'$, alors $[G:H] = \left[G:H'\right]\left[H':H\right]$.

La preuve est immédiate :

$[G:H] = |G|/|H| = \dfrac{[G:H]\,|H'|}{|H|} = \left[G:H'\right]\dfrac{|H'|}{|H|} = \left[G:H'\right]\left[H':H\right]$.

1.7 Groupe quotient

Définition 1.7.1

Soit G un groupe et H un sous-groupe normale de G, on écrit alors $H \lhd G$, notons dans ce cas que l'ensemble quotient gauche $(G/H)_g$ coïncide avec l'ensemble quotient à droite $(G/H)_d$.

$$(G/H)_g = \{gH / g \in G\}$$

$$(G/H)_d = \{Hg / g \in G\}$$

Si $H \lhd G$ alors l'ensemble quotient $(G/H, \cdot)$ a une structure de groupe dit groupe quotient :

1- L'opération sur les classes est définie par : pour $g_1H, g_2H \in (G/H), \exists g_3 \in G$:

$g_1H \cdot g_2H = g_1g_2H = g_3H \in (G/H)$;

2- la loi " $\cdot$ " est associative : $g_1H \cdot (g_2H \cdot g_1H) = (g_1H \cdot g_2H) \cdot g_1H$;

3- la classe H désigne l'élément neutre $\forall gH \in (G/H) : gH \cdot H = H \cdot gH = gH$;

4- on a $gH \cdot g^{-1}H = g \cdot g^{-1}H = eH = H$, ce qui montre $g^{-1}H$ est symétrique de gH.

1.8 Groupe cyclique

Définition 1.8.1

Soit $(G, \cdot)$ un groupe s'il existe $g \in G$ tel que $G = \langle g \rangle$ dans ce cas, on dit que le groupe G est monogène .

Définition 1.8.2

Soit $(G, \cdot)$ un groupe s'il existe $g \in G$ tel que $G = \langle g \rangle$, $|G| = n$ et $G = \{g, g^2, g^3, ...g^n = 1_G\}$, avec $\forall i, j \in \overline{1, n}, i \neq j, g^i \neq g^j$, dans ce cas G est dit groupe cyclique.

Exemple 1.8.3

$(\mathbb{Z}/3\mathbb{Z}, \overline{+})$ est un groupe cyclique où $\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$;

la table de Cayley de $(\mathbb{Z}/3\mathbb{Z}, \overline{+})$ est :

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

1.9 Groupe opérant sur un ensemble

Définition 1.9.1

On dit qu'un groupe G opère (à gauche) sur un ensemble E, si on a une application

$$f : G \times E \longrightarrow E,$$

on écrit habituellement $g \cdot x$ pour $f(g, x)$, telle que pour tout $x \in E$, et tout $g_1, g_2 \in G$ on ait

1- $1_G \cdot x = x$, où 1_G désigne le neutre de G;

2- $(g_1g_2) \cdot x = g_1 \cdot (g_2 \cdot x)$.

On dit aussi que f est une action de G sur E, ou encore que G agit sur E par f. Bien étendu, il peut avoir plusieurs actions différents d'un groupe sur le même ensemble.

Exemples 1.9.2

1- Le groupe linéaire $Gl_n(\mathbb{R})$ opère sur $\mathbb{R}^n$ de la manière suivante : pour $A \in Gl_n(\mathbb{R}), v \in \mathbb{R}^n, (A; v) \longmapsto Av \in \mathbb{R}^n$. On vérifie immédiatement que cela définit bien une opération sur $\mathbb{R}^n$.

2- On peut aussi faire opérer les matrices inversibles $Gl_n(\mathbb{C})$ sur l'ensemble $M_n(\mathbb{C})$ des matrices $n \times n$ de la manière suivante : $(A; M) \longmapsto AMA^{-1}$. Dans ce cas, rappelons que deux matrices M, M' sont semblables si, et seulement si elles appartiennent a la même orbite sous l'action de $Gl_n(\mathbb{C})$. Chaque orbite possède alors un représentant "canonique" : sa forme de Jordan. Il y a donc un nombre fini d'orbites.

Notation 1.9.3

Si G un groupe qui opère sur l'ensemble E on dit que E est un G-ensemble.

Définition 1.9.4

Pour G agissant sur E, et x dans E, l'orbite de x, noté $Orb(x)$, est l'ensemble de tous les points de E de la forme $g \cdot x$, pour g parcourant G. En formule,

$$Orb(x) = \{y \in E : \text{ il existe } g \in G \text{ tel que } y = g \cdot x\}.$$

Exemple 1.9.10

Soit G le groupe de toutes les rotations du plan de centre P, et E est le cercle de centre P, $Orb(M) =$ le cercle de centre P et de rayon PM.

Définition 1.9.11

E étant un G-ensemble, le sous-groupe G_x de G, associé à tout $x \in E$ et défini par : $Stab\,(x)_G = \{g \in G; g \cdot x = x\}$ est appelé stabilisateur de x.

Lemme 1.9.12

Si un groupe fini G opère sur l'ensemble fini S, et $s \in S$, alors :

$$|Orb(s)| = \frac{|G|}{|stab(s)|}.$$

Chapitre 2

Etudes sur les groupes symétriques

Introduction

Dans ce chapitre on donne les définitions et les propriétés des outils que nous utiliserons par la suite :
groupe de permutation, composition de permutations, notion de σ-orbite (ou orbite suivant σ), cycle dans S_n. Transposition, décomposition d'une permutation en un produit de cycles ou en un produit de transpositions, inversion d'une permutation. Calcule de la signature, groupe alterné.

Contenu

2.6. Inversion d'une permutation. Calcule de la signature.

2.7. Groupe alterné.

2.1 Groupe de permutation

Soit n un entier naturel non nul.

Définition 2.1.1

On note S_n l'ensemble des permutations de l'ensemble $\{1, 2, ..., n\}$ c'est-à-dire l'ensemble des bijections de $\{1, 2, ..., n\}$ vers $\{1, 2, ..., n\}$.

Proposition 2.1.2

Le couple $(S_n, \circ)$ *est un groupe .*

Preuve

L'identité est une permutation de $\{1, 2, ..., n\}$ 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 2.1.3

Le groupe S_n est appelé groupe symétrique de degré n.

Notations 2.1.4

1- Si $\sigma : \{1, 2, ..., n\} \longrightarrow \{1, 2, ..., n\}$ est un permutation, on dénote par :

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

2- L'élément neutre Id_X est représenté par :

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

2- L'élément inverse σ^{-1} de σ par :

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

Bien qu'il s'agit de la composition, on parle souvent du $\ll$ produit de σ par τ $\gg$, et l'on écrit aussi $\sigma\tau$ au lieu de $\sigma \circ \tau$, qui signifier $\ll$ effectuer d'abord la permutation τ, puis la permutation σ $\gg$.

Exemple 2.1.5

Soit la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 7 & 6 & 3 & 4 \end{pmatrix}$, l'inverse de σ est :

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

Proposition 2.1.6

Le cardinal de S_n est $n!$.

Preuve

Une permutation de S_n est entièrement déterminée par les images de $\{1, 2, ..., n\}$, qui sont des éléments distincts de $\{1, 2, ..., n\}$. Pour compter le nombre d'éléments σ de S_n, observons que pour l'image de 1, il ya n choix, pour l'image de 2 il ya $n-1$ choix (car $\sigma(2) \notin \{\sigma(1)\}$), pour l'image de 3, il ya $n-2$ choix (car $\sigma(3) \notin \{\sigma(1), \sigma(2)\}$), et ainsi de suite, enfin pour l'image de n, il ya 1 choix (car $\sigma(n) \notin \{\sigma(1), ..., \sigma(n-1)\}$). Donc au total, il ya $n! = n.(n-1)...2.1$ permutation de $\{1, ..., n, \}$ c'est l'ordre du groupe S_n.

Exemples 2.1.7

1- Pour $n = 2, |S_2| = 2! = 2$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}.$$

2- Pour $n = 3, |S_3| = 3! = 6$

$$S_3 = \left\{ \begin{array}{l} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \\ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \end{array} \right\}.$$

2.2 Composition de permutations

La composition $\tau\sigma$, de deux permutations σ et τ de S_n, correspondonds à superposer deux tels diagrammes de flèches, plaçant celui de σ au-dessus de celui de τ. Ainsi, le composé de $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$
s'obtient en $\ll$ suivant $\gg$ les flèches dans la figure obtenue par cette superposition

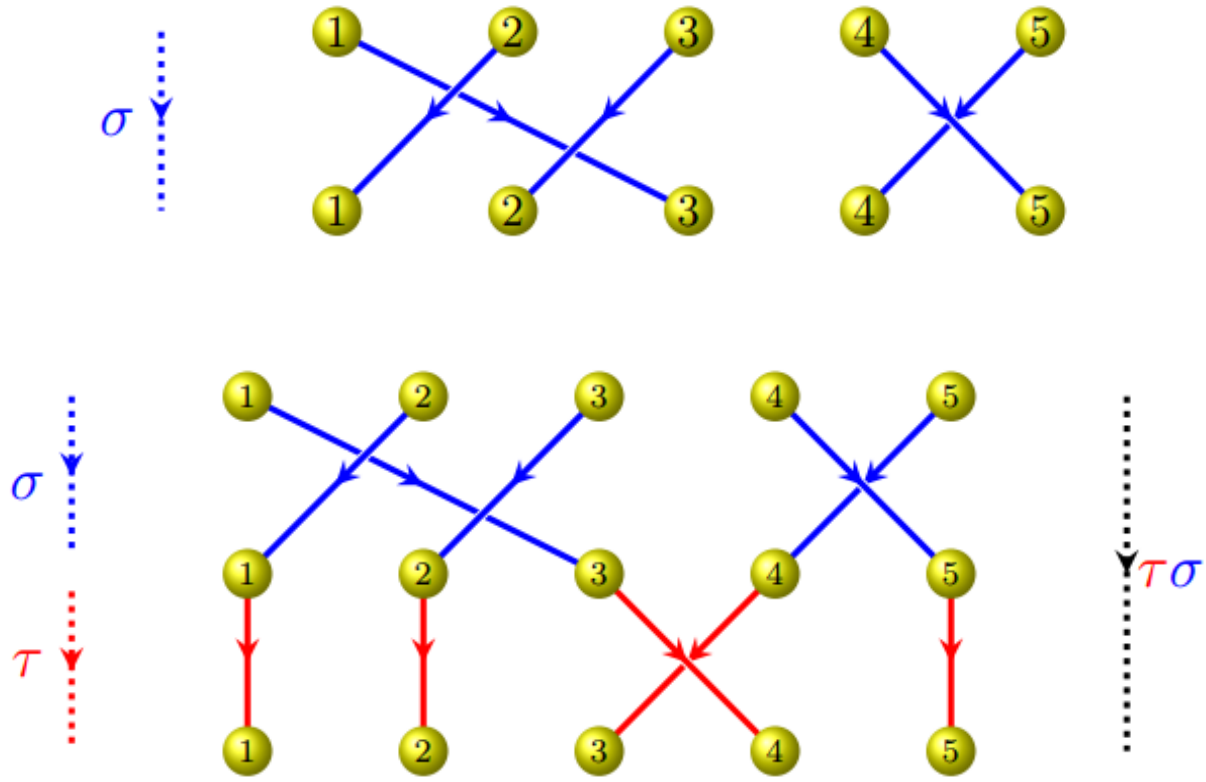

Figure 1.1 *Composition de permutation.*

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

Proposition 2.2.1

Si $n \geq 3, S_n$ est un groupe non commutatif.

Preuve

Soit $n \geq 3$. Pour montrer que S_n est non commutatif, soient $\sigma, \pi \in S_n$, pour $\sigma = \begin{pmatrix} a & b & c & x & ... & y \\ b & c & a & x & ... & y \end{pmatrix}$ et $\pi = \begin{pmatrix} a & b & c & x & ... & y \\ b & a & c & x & ... & y \end{pmatrix}$, on calcul $\pi \circ \sigma$ et $\sigma \circ \pi$.

$\pi \circ \sigma = \begin{pmatrix} a & b & c & x & ... & y \\ a & c & b & x & ... & y \end{pmatrix}$, et $\sigma \circ \pi = \begin{pmatrix} a & b & c & x & ... & y \\ c & b & a & x & ... & y \end{pmatrix}$,

donc $\pi \circ \sigma \neq \sigma \circ \pi$.

Alors, si $n \geq 3$ le groupe S_n est non commutatif.

Par exemple $n = 3 : \pi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ et $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

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

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

donc $\pi \circ \sigma \neq \sigma \circ \pi$.

2.3 Notion de σ-orbite (ou orbite suivant σ)

Définition 2.3.1 (Ordre d'une permutation)

On appelle ordre d'une permutation $\sigma \in S_n$ le plus petit entier $p \in \mathbb{N}^*$ tel que $\sigma^p = Id$. On rappelle la convention d'écriture $\sigma^p = \underbrace{\sigma \circ ... \circ \sigma}_{p \text{ foi}}$.

Exemple 2.3.2

$$\text{Soit } S_3 = \left\{ \pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \right.$$
$$\left. \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

$Ord(\pi_1) = 1, Ord(\pi_4) = Ord(\pi_5) = Ord(\pi_6) = 2, Ord(\pi_2) = Ord(\pi_3) = 3.$

Définition 2.3.3

Soit $\sigma \in S_n$, le support de σ est l'ensemble :

$$Supp(\sigma) = \{i \in N_n; \sigma(i) \neq i\} \text{ où } N_n = \{1, 2, ..., n\}.$$

Remarque 2.3.4

Dans $S_n, \sigma = e$ si, et seulement si $Supp(\sigma) = \emptyset$.

Proposition 2.3.5

Dans tout groupe S_n, deux permutations dont les supports sont disjoints commutent.

Preuve

La propriété étant immédiate pour $n = 1$, supposons $n > 1$ et considérons $\sigma_1 \neq \sigma_2$ dans S_n tels que $Supp(\sigma_1) \cap Supp(\sigma_2) = \emptyset$. Si l'une des deux permutations est l'identité,

la propriété est vérifiée. Supposons les deux supports non vides, soit $i \in Supp(\sigma_1)$, alors $i \notin Supp(\sigma_2)$ et $\sigma_1(i) \notin Supp(\sigma_2)$, par suit :

$$\sigma_1 \circ \sigma_2(i) = \sigma_1(i) \text{ et } \sigma_2 \circ \sigma_1(i) = \sigma_1(i),$$

de même pour $i \in Supp(\sigma_2)$, on a :

$$\sigma_1 \circ \sigma_2(i) = \sigma_2(i) \text{ et } \sigma_2 \circ \sigma_1(i) = \sigma_2(i).$$

D'autre part, s'il existe $i \in N_n$ tel que $i \notin Supp(\sigma_1) \cup Supp(\sigma_2)$, alors $\sigma_1 \circ \sigma_2(i) = i$ et $\sigma_2 \circ \sigma_1(i) = i$. On en conclut que $\sigma_1 \circ \sigma_2 = \sigma_2 \circ \sigma_1$.

Définition 2.3.6

A toute permutation $\sigma \in S_n$, on associe la relation binaire R_σ définie dans N_n par :

$$iR_\sigma k \Longleftrightarrow \exists r \in \mathbb{Z}, \sigma^r(i) = k.$$

Il est facile de vérifier que R_σ est une relation d'équivalence dans N_n et que la classe d'équivalence modulo R_σ d'un élément $i \in N_n$ est :

$$\Omega_\sigma(i) = \{\sigma^r(i); r \in \mathbb{Z}\}.$$

Définition 2.3.7

Pour tout $\sigma \in S_n$ et tout $i \in N_n$, $\Omega_\sigma(i)$ s'appelle la σ-orbite de i (ou l'orbite de i suivant σ).

Remarques 2.3.8

1- Supposons $n > 1$ et $\sigma \neq e$ dans S_n tel que $Ord(\sigma) = p$, on a alors : $\langle\sigma\rangle = \{\sigma^r; r \in \mathbb{Z}\} = \{e, \sigma, ..., \sigma^{p-1}\}$; par suit, en notant $|\Omega_\sigma(i)|$ le cardinal de la σ-orbite de i, on a pour tout $i \in N_n$: $1 \leq |\Omega_\sigma(i)| \leq p$. Si $i \notin Supp(\sigma_1)$, alors $\Omega_\sigma(i) = \{i\}$, donc $|\Omega_\sigma(i)| = 1$. Une σ-orbite de cardinal 1 sera dite ponctuelle, si $i \in Supp(\sigma_1)$, on a nécessairement $2 \leq |\Omega_\sigma(i)| \leq p$.

2- Si $\{i_1, i_2, ..., i_t\}$ est une famille de représentations des σ-orbite distinctes de N_n, les $\{\Omega_\sigma(i_q)\}_{1 \leq q \leq t}$ forment une partition de N_n, d'où $n = \sum_{1 \leq q \leq t} |\Omega_\sigma(i_q)|$.

Exemple 2.3.9

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

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

2.4 Cycle dans S_n. Transposition

Définition 2.4.1 (cycle)

Une permutation $\sigma \in S_n$ est un cycle de longueur r $(1 \leq r \leq n)$ dans un ensemble ordonné de r entiers distincts de $N_n, \{i_1, i_2, ..., i_r, \}$ tel que : $\sigma(i_1) = i_2, \sigma(i_2) = i_3, ..., \sigma(i_{r-1}) = i_r, \sigma(i_r) = i_1$, et pour tout $k \in N_n \backslash \{i_1, i_2, ..., i_r\}, \sigma(k) = k$. Un tel cycle sera noté $\sigma = (i_1 i_2 ... i_r)$.

Remarques 2.4.2

1- Un cycle $(i_1 i_2 ... i_r)$ peut aussi noté $(i_k i_{k+1} ... i_r i_1 i_2 ... i_{k-1})$ quel que soit k $(1 \leq k \leq r)$.

2- Tout cycle de longueur 1 est l'identité e : en effet, si $\sigma = (i)$, on a $\sigma(i) = i$ et pour tout $k \neq i$, donc $\sigma = e$.

Exemples 2.4.3

1- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 3 & 5 & 1 & 4 & 2 & 7 \end{pmatrix} = (162354)$ est un cycle de longueur 6.

2- $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 4 & 1 & 3 & 6 & 5 \end{pmatrix} = (1243)(56)$ cette permutation contenant un cycle de longueur 2 et un cycle de longueur 4.

Définition 2.4.4

On dira que les cycles $\sigma = (i_1 i_2 ... i_p)$ et $\tau = (j_1 j_2 ... j_q)$ sont disjoints, si les ensembles $\{i_1, i_2, ..., i_p\}$ et $\{j_1, j_2, ..., j_q\}$ sont disjoints.

Définition 2.4.5 (Transposition)

Un cycle de longueure 2 dans S_n $(n \geq 2)$ est appelé transposition. Si $\sigma = (i_1 i_2)$, on a $\sigma(i_1) = i_2, \sigma(i_2) = i_1$, et $\sigma(k) = k$, pour tout $k \in N_n \backslash \{i_1, i_2\}$, qui notée par $\tau_{i_1 i_2}$. Une

transposition dans S_n est donc une permutation qui, dans N_n, échange deux éléments et laisse invariants tous les autres (lorsque $n \geq 3$).

Exemples 2.4.6

1- $S_2 = \{e, \tau\}$ où τ est la transposition qui échange 1 et 2.

2- $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (34)$ est une transposition τ_{34}.

Remarque 2.4.7

Pour $n \geq 2$ dans N_n, le nombre des transpositions dans S_n est égale au nombre de couples $(i, j) \in N_n \times N_n$ tel que $i \neq j$; ce nombre est donc $C_n^2 = \frac{n(n-1)}{2}$.

Définition 2.4.8 (permutation circulaire)

Dans S_n $(n \geq 2)$, le cycle de longueur n : $\tau = (1, 2, ..., n) = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ 2 & 3 & 4 & ... & 1 \end{pmatrix}$, est appelé permutation circulaire des entiers 1, 2, ..., n.

Remarques 2.4.9

1- Dans S_n $(n \geq 3)$ un cycle de longueur n n'est pas nécessairement la permutation circulaires.

Par exemple, dans S_4 : $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ est le cycle $(1, 3, 4, 2)$ différent de $(1, 2, 3, 4)$.

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

Proposition 2.4.10

Dans tout groupe S_n, un r-cycle est un élément d'ordre r.

Preuve

Soit $\gamma = (j_1, j_2, ..., j_r)$ un r-cycle dans S_n.

- Si $r = 1$, alors $\gamma = e$, donc $O(\gamma) = 1$.

- Supposons $1 < r \leq n$ pour tout k $(1 \leq k \leq r)$, on a : $\gamma(j_k) = j_{k+1}$, $\gamma^2(j_k) = j_{k+2}, ..., \gamma^{r-k}(j_k) = j_r, ..., \gamma^r(j_k) = j_k$. D'autre part, si $r < n$ et $i \notin supp(\gamma)$, alors

$\gamma(i) = i$. Les r élément $j_1, j_2, ..., j_r$ étant distincts, r est le plus petit entier positif tel que $\gamma^r = e$, d'où $Ord(\gamma) = r$.

Corollaire 2.4.11

Si τ est une transposition dans S_n, alors $\tau^2 = e$ donc $\tau^{-1} = \tau$.

2.5 Décomposition d'une permutation en un produit de cycles ou en un produit de transpositions

Théorème 2.5.1

Toute permutation $\sigma \neq e$ dans S_n s'écrit sous la forme :

$$\sigma = \gamma_1 \circ \gamma_2 \circ ... \circ \gamma_s .....(*),$$

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

Preuve

Soit $\sigma \neq e$ dans S_n; le support de σ étant non vide, il existe au moins une σ-orbite non ponctuelle $\Omega_\sigma(i)$. Si $\Omega_\sigma(i) = \{i, \sigma(i), ..., \sigma^{p-1}(i)\}$ avec $2 \leq p \leq n$; posons $i = j_1, \sigma(i) = j_2, ..., \sigma^{p-1}(i) = j_p$ et notons γ le cycle $(j_1 j_2 ... j_p)$. La restriction de σ à $\{j_1, j_2, ..., j_p\}$ est égal à restriction de γ à son support. Ainsi, à toute σ-orbite non ponctuelle Ω, on peut associer un cycle γ dont le support est Ω. Soit $\{\Omega_q\}_{1 \leq q \leq s}$ la famille des σ-orbites non ponctuelle distinctes dans N_n. A toute σ-orbite Ω_q associons, comme plus haut, le cycle γ_q, dont le support est Ω_q. Les σ-orbites Ω_q $(1 \leq q \leq s)$ sont deux à deux disjoints, donc ils commutent entre eux. Posons $\sigma' = \gamma_1 \circ \gamma_2 \circ ... \circ \gamma_s$ et comparons σ' et σ. Soit $j = \bigcup_{1 \leq q \leq s} \Omega_q$; il existe $1, (1 \leq l \leq s)$ tel que $j \in \Omega_l$. Puisque $\sigma_{|\Omega} = \gamma_{l\,|\Omega}$, on a $\sigma(j) = \gamma_l(j)$. D'autre part, on peut écrire $\sigma' = \gamma_l \circ \prod_{\substack{1 \leq q \leq s \\ q \neq l}} \gamma_q$; pour $q \neq l, \gamma_q(j) = j$, d'où $\sigma'(j) = \gamma_l(j)$. De plus, s'il existe $k \in N_n \setminus \bigcup_{1 \leq q \leq s} \Omega_q$, on a $\sigma(k) = k$ et aussi $\sigma'(k) = k$. On en conclut que $\sigma = \sigma'$.

Supposons que $\sigma = \gamma_1' \circ \gamma_2' \circ ... \circ \gamma_r'$ soit une autre décomposition de σ en un produit de cycles disjoints, tous différents de e. Pour tout p $(1 \leq p \leq r)$, notons Ω_p' la γ_p'-orbite non

ponctuelle; les cycles $\gamma_p^{'}$ étant disjoints, les σ-orbites non ponctuelles sont alors les $\Omega_p^{'}$, pour $1 \leq p \leq r$. La décomposition de N_n en σ-orbites étant unique, on en déduit que $r = s$ et qu'il existe une permutation π dans le groupe symétrique S_s telle que $\Omega_p^{'} = \Omega_{\pi(p)}$ et par suit $\gamma_p^{'} = \gamma_{\pi(p)}$; d'où l'unicité de la décompositon $(*)$ à l'ordre des facteurs près.

Exemple 2.5.2

Soit la permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix} \in S_6$. La décomposition de N_6 en σ-orbites implique $\sigma = \gamma_1 \circ \gamma_2$ où $\gamma_1 = (153)$ et $\gamma_2 = (46)$.

Théorème 2.5.3

Pour tout $n \geq 2$ dans N_n, toute permutation $\sigma \in S_n$ se décompose, de manière non unique, en un produit de transposition.

Preuve

Si $n \geq 2$ implique qu'il existe au moins une transposition τ dans S_n. $e = \tau^2$, donc e est produit de transpositions. Sachant que toute permutation $\sigma \neq e$ dans S_n est un produit de cycles, il suffit de prouver que tout cycle est un produit de transposition, soit $\gamma = (j_1 j_2 ... j_r)$ dans S_n, tel que $1 < r \leq n$. Notons $(j_p j_q)$ la transposition qui échange j_p et j_q tels que $1 \leq p < q \leq n$; en écrivant $(j_p j_q)$ $(j_l j_m)$ à la place de $(j_p j_q) \circ$ $(j_l j_m)$, posons : $\gamma^{'} = (j_1 j_2)(j_2 j_3)...(j_{r-1} j_r)$. Pour tout k $(1 \leq k \leq r-1)$, on a $\gamma^{'}(j_k) = j_{k+1} = \gamma(j_k)$; de plus $\gamma^{'}(j_r) = j_1 = \gamma(j_r)$. S'il existe $k \in N_n \backslash supp(\gamma)$, alors $\gamma^{'}(k) = k = \gamma(k)$. On en déduit que $\gamma^{'} = \gamma$, d'où $(j_1 j_2 ... j_r) = (j_1 j_2)(j_2 j_3)...(j_{r-1} j_r)$.....” $*^{'}$ ”

De la décomposition canonique d'une permutation σ en un produit de cycles, on peut donc déduire une permutation σ en un produit de transposition, mais cette dernière n'est pas unique si $n \geq 3$, car, étant donné une transposition quelconque (jk) dans S_n, on vérifie facilement que $(jk) = (1j)(1k)(1j)$.....” $*^{''}$ ”

D'autre part, si j, k, l sont trois entiers distincts dans N_n, on a : $(j,k)(k,l) \neq (k,l)(j,k)$, on en déduit que dans une décomposition d'une permutation $\sigma \in S_n$ $(n \geq 3)$ en un produit de transposition, deux transpositions distincts non disjointes ne sont pas permutables.

Exemples 2.5.4

1- Soit $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 2 & 5 \end{pmatrix}$; γ est le cycle (2465) dans S_6;

en appliquant la formule " $*'$ ", on obtient : $\gamma = (24)(46)(65)$.

2- Soit $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 6 & 3 & 4 \end{pmatrix}$; σ est le cycle $(153)(46)$ dans S_6;

en appliquant la formule " $*'$ ", on obtient : $\sigma = (15)(53)(46)$. D'après la relation " $*$" ", on peut écrire, $(53) = (15)(13)(15)$, on en déduit que $\sigma = (13)(15)(46)$.

2.6 Inversion d'une permutation. Calcule de la signature

Définition 2.6.1 (Inversion d'une permutation)

Soit $\sigma \in S_n$. On appelle nombre d'inversion de σ le nombre de pair $\{i, j\} \in \{1, ..., n\}$ telle que la restrictions de σ à $\{i, j\}$ soit décroissante (*i.e.* si $i > j$ alors $\sigma(i) < \sigma(j)$). On note $I(\sigma)$ cet entier.

Exemple 2.6.2

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 ya a inversion sont $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{1, 5\}, \{2, 3\}, \{2, 4\}$ et $\{3, 4\}$. Ainsi on a $I(\sigma) = 7$.

Définition 2.6.3 (Signature d'une permutation)

On appelle signature de σ l'entier valant $+1$ ou -1 défini par :

$$\epsilon(\sigma) = (-1)^{I(\sigma)} = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

Corollaires 2.6.4

- *Si $\sigma = e$, alors $\epsilon(e) = 1$.*

- *Si τ est une transposition dans S_n, alors $\epsilon(\tau) = -1$.*

- *Si γ est une r-cycle dans S_n, alors $\epsilon(\gamma) = (-1)^{r-1}$.*

Définition 2.6.5

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

Proposition 2.6.6

Quelle que soient deux permutations $\sigma, \gamma \in S_n$, on a $\epsilon(\sigma\gamma) = \epsilon(\sigma)\epsilon(\gamma)$. En d'autres termes, l'application

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

ϵ est un morphisme de groupes.

Preuve

- $\forall \sigma \in S_n$, $\epsilon(\sigma) = \{+1, -1\}$;
- Soient σ et γ deux éléments de S_n,

σ se décompose en produit de transposition $\sigma = \prod_{k=1}^{p} \tau_k, \epsilon(\sigma) = (-1)^p$.

γ se décompose en produit de transposition $\gamma = \prod_{k=1}^{q} \tau_k^{'}, \epsilon(\gamma) = (-1)^q$.

Alors : $\sigma\gamma = \left(\prod_{k=1}^{p} \tau_k\right)\left(\prod_{k=1}^{q} \tau_k^{'}\right)$.

Donc $\epsilon(\sigma\gamma) = (-1)^{p+q} = (-1)^p(-1)^q = \epsilon(\sigma)\epsilon(\gamma)$.

2.7 Groupe alterné

Définition 2.7.1

Pour tout entier $n \geq 2$, le noyau de ϵ est appelé n-ième groupe alterné. On le note A_n. Le sous-groupe A_n de S_n est donc l'ensemble des permutations de S_n qui sont de signature 1 (c'est-à-dire qui se décomposent en un nombre paire de transposition).

Proposition 2.7.2

Pour tout entier $n \geq 2$, le groupe A_n est fini d'ordre $\frac{n!}{2}$.

Preuve

Soient $X = \{\tau \in S_n, \epsilon(\tau) = -1\}$, et $A_n = \{\sigma \in S_n, \epsilon(\sigma) = 1\}$. Le sous-ensemble X est non vide. Si l'on fixe $\tau \in X$. On défini l'application :

$$\begin{aligned} \varphi : A_n &\longrightarrow X \\ \sigma &\longmapsto \tau\sigma. \end{aligned}$$

L'application φ est bien défini car :

$\forall \sigma_1, \sigma_2 \in S_n : \sigma_1 = \sigma_2 \Longrightarrow \tau\sigma_1 = \tau\sigma_2$

$\Longrightarrow \varphi(\sigma_1) = \varphi(\sigma_2).$

Et on a $\varphi(\tau\sigma) = \varphi(\tau) \cdot \varphi(\sigma)$

$= -1 \times 1 = -1.$

On montre que l'application φ est bijective

1- L'injectivité : $\epsilon(\sigma_1) = \epsilon(\sigma_2) \Longrightarrow \tau\sigma_1 = \tau\sigma_2$

$\Longrightarrow \tau^{-1}\tau\sigma_1 = \tau^{-1}\tau\sigma_2$

$\Longrightarrow \sigma_1 = \sigma_2.$

2- La surjectivité : $\forall \gamma \in X, \exists \sigma \in A_n : \gamma = \varphi(\sigma)$

$\gamma = \varphi(\sigma) \Longleftrightarrow \gamma = \tau\sigma$

$\Longrightarrow \sigma = \tau^{-1}\gamma$

alors $\epsilon(\tau^{-1}\gamma) = 1$. Donc φ est bijective.

On a $S_n = X \cup A_n$ et $X \cap A_n = \emptyset \Longrightarrow |S_n| = |X| + |A_n|$,

et comme $|X| = |A_n| \Longrightarrow |S_n| = 2|A_n|$

$\Longrightarrow |A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$.

Exemples 2.7.3

1- Pour $n = 2$, on a $A_2 = \{e\}$.

2- Pour $n = 3$, on a $A_3 = \{e, \sigma, \sigma^2\}$ avec $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Chapitre 3

Produit en couronne de groupes

Introduction

Dans ce chapitre, on présente des notions sur le produit direct, produit semi direct et produit en couronne, et dans la fin de ce chapitre, en applicant le produit en couronne sur le groupe de permutation.

Contenu

3.1. Produit direct de groupes;

3.2. Produit semi-direct de groupes;

3.3. Produit en couronne de groupes;

3.4. Produit en couronne de groupes de permutation.

3.1 Produit direct des groupes

Soient $(G_1, .)$ et $(G_2, *)$ deux groupes.

Proposition 3.1.1

L'ensemble $G_1 \times G_2$ muni de la loi interne $(g_1, g_2)(g_1^{'}, g_2^{'}) = (g_1.g_1^{'}, g_2 * g_2^{'})$ est un groupe.

Preuve

Soient $g_1, g_1^{'}, g_1^{''}$ appartenant à G_1 et $g_2, g_2^{'}, g_2^{''}$ appartenant à G_2. Comme G_1 et G_2 sont des groupes, on a :

$$\begin{aligned}((g_1, g_2)(g_1^{'}, g_2^{'}))(g_1^{''}, g_2^{''}) &= (g_1 g_1^{'}, g_2 g_2^{'})(g_1^{''}, g_2^{''}) \\ &= ((g_1 g_1^{'}) g_1^{''}, (g_2 g_2^{'}) g_2^{''}) \\ &= (g_1 (g_1^{'} g_1^{''}), g_2 (g_2^{'} g_2^{''})) \\ &= (g_1, g_2)(g_1^{'} g_1^{''}, g_2^{'} g_2^{''}) \\ &= (g_1, g_2)((g_1^{'}, g_2^{'})(g_1^{''}, g_2^{''})).\end{aligned}$$

D'où la loi sur $G_1 \times G_2$ est associative.

Cette loi admet l'élément $(1_{G_1}, 1_{G_2})$ comme élément neutre et tout élément (g_1, g_2) de $G_1 \times G_2$ est inversible d'inverse (g_1^{-1}, g_2^{-1}). Donc $G_1 \times G_2$ est un groupe.

Exemples 3.1.2

1- Soient $(\mathbb{Z}, +)$ et $(\mathbb{Q}^*, \times)$ deux groupes.

L'ensemble $\mathbb{Z} \times \mathbb{Q}^*$muni de la loi interne $(x, y)(x^{'}, y^{'}) = (x + x^{'}, y \times y^{'})$ a un structure de groupe.

i) Cette loi admet l'élément $(0, 1)$ comme élément neutre :

$$\begin{aligned}\forall (x, y) \in \mathbb{Z} \times \mathbb{Q}^* (x, y)(0, 1) &= (x + 0, y \times 1) \\ &= (x, y);\end{aligned}$$

ii) tout élément (x, y) de $\mathbb{Z} \times \mathbb{Q}^*$ admet un symétrique $(-x, y^{-1})$:

$$(x, y)(-x, y^{-1}) = (0, 1).$$

2- Soient $S_3 = \{e, \tau_1, \tau_2, \tau_3, \sigma_1, \sigma_2\}$ et $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ deux groupes.

L'ensemble $S_3 \times \mathbb{Z}_2$ muni de la loi interne $(\tau, \overline{x}) \cdot (\sigma, \overline{y}) = (\tau \circ \sigma, \overline{x} + \overline{y})$ a un structure de groupe.

Définition 3.1.3

Le groupe $G_1 \times G_2$ est appelé produit direct de groupes G_1 et G_2.

Propriété 3.1.4

Le groupe $G_1 \times G_2$ est abélien si, et seulement si G_1 et G_2 sont abéliens.

Preuve

Le groupe $G_1 \times G_2$ est abélien si, et seulement si pour tous les g_1 et $g_1^{'}$ appartenant à G_1 et g_2 et $g_2^{'}$ appartenant à G_2 $(g_1, g_2)(g_1^{'}, g_2^{'}) = (g_1^{'}, g_2^{'})(g_1, g_2)$ c'est-à-dire :
$(g_1 g_1^{'}, g_2 g_2^{'}) = (g_1^{'} g_1, g_2^{'} g_2)$.
D'où $G_1 \times G_2$ est abélien si, et seulement si $g_1 g_1^{'} = g_1^{'} g_1$ pour tous les g_1 et $g_1^{'}$ appartenant à G_1 et $g_2 g_2^{'} = g_2^{'} g_2$ pour tous les g_2 et $g_2^{'}$ appartenant à G_2, c'est-à-dire si, et seulement si G_1 et G_2 sont abéliens.

3.2 Produit semi-direct de groupes

Soient G et H deux groupes.
Soit θ un homomorphisme de G dans $Aut(H)$. Pour tout g appartenant à G, on note θ_g à la place $\theta(g)$. Puisque $\theta_g(h^{'})$ appartenant à H pour tout élément $h^{'}$ de H, on peut définir une loi interne sur $G \times H$ en posant : $(g, h)(g^{'}, h^{'}) = (gg^{'}, h\theta_g(h^{'}))$.

Proposition 3.2.1

L'ensemble $G \times H$ muni de la loi interne $(g, h) \cdot (g^{'}, h^{'}) = (gg^{'}, h\theta_g(h^{'}))$ est un groupe.

Preuve

i) Montrons que la loi " $\cdot$ " est associative : soient $h, h^{'}$ et $h^{''}$appartenant à H et $g, g^{'}$ et $g^{''}$ appartenant à G.

$$\begin{aligned}((g, h) \cdot (g^{'}, h^{'})) \cdot (g^{''}, h^{''}) &= ((gg^{'}, h\theta_g(h^{'}))(g^{''}, h^{''}) \\ &= (gg^{'}g^{''}, h\theta_g(h^{'})\theta_{gg^{'}}(h^{''})) \\ &= (gg^{'}g^{''}, h\theta_g(h^{'})\theta_g(\theta_{g^{'}}(h^{''})) \text{ car } \theta \text{ est un homomorphisme.}\end{aligned}$$

D'autre part

$$(g,h)\cdot((g^{'},h^{'})\cdot(g^{''},h^{''})) = (g,h)\cdot(g^{'}g^{''},h^{'}\theta_{g^{'}}(h^{''}))$$
$$= (gg^{'}g^{''},h\theta_{g}(h^{'}\theta_{g^{'}}(h^{''}))$$
$$= (gg^{'}g^{''},h\theta_{g}(h^{'})\theta_{g}(\theta_{g^{'}}(h^{''})) \text{ car } \theta \text{ est un homomorphisme.}$$

D'où $((g,h)\cdot(g^{'},h^{'}))\cdot(g^{''},h^{''}) = (g,h)\cdot((g^{'},h^{'})\cdot(g^{''},h^{''}))$ et la loi est associative.

ii) Pour tout élément h de H et pour tout élément g de G on a :

$(g,h)\cdot(1,1) = (g1,h\theta_{g}(1)) = (g,h)$ et $(1,1)\cdot(g,h) = (1g,\theta_{1}(h)) = (g,Id(h)) = (g,h)$ car θ est un homomorphisme donc la loi " $\cdot$ " admet l'élément $(1,1)$ comme élément neutre.

iii) Soient h appartenant à H et g appartenant à G montrons que (g,h) admet un inverse.

Comme θ_{g} est bijective, il existe un élément $h^{'}$ de H tel que $\theta_{g}(h^{'}) = h^{-1}$.

D'où $(g,h)\cdot(g^{-1},h^{'}) = (gg^{-1},h\theta_{g}(h^{'})) = (gg^{-1},h^{'}h^{-1}) = (1,1)$.

Comme θ est un homomorphisme de G dans $Aut(H)$ on a :

$$\theta_{g^{-1}} = (\theta_{g})^{-1}. \text{ D'où } \theta_{g^{-1}}(h^{-1}) = h^{'}.$$

$\theta_{g^{-1}}$ est un homomorphisme donc $\theta_{g^{-1}}(h) = \theta_{g^{-1}}((h^{-1}))^{-1} = (\theta_{g^{-1}}(h^{-1}))^{-1} = h^{'^{-1}}$ on en déduit que

$(g^{-1},h^{'})\cdot(g,h) = (g^{-1}g,h^{'}\theta_{g^{-1}}(h)) = (g^{-1}g,h^{'}\theta_{g^{-1}}(h)) = (g^{-1}g,h^{'}h^{'^{-1}}) = (1,1)$. D'où (g,h) admet $(g^{-1},\theta_{g^{-1}}(h^{-1}))$ comme inverse.

On en déduit que $G\times H$ est un groupe pour la loi $(g,h)\cdot(g^{'},h^{'}) = (gg^{'},h\theta_{g}(h^{'}))$.

Définition 3.2.2

Le groupe $G\times H$ muni de la loi $(g,h)\cdot(g^{'},h^{'}) = (gg^{'},h\theta_{g}(h^{'}))$ est appelé produit semi-direct de G par H relativement à θ et noté par $G\rtimes_{\theta} H$.

3.3 Produit en couronne de groupes

Définition 3.3.1

Soient H et K deux groupes. On dit que H agit sur K comme un groupe si chaque k de K à correspond un unique élément k^h de K tel que pour h_1, h_2, h de H et k_1, k_2, k de K

$$(k^{h_1})^{h_2} = k^{h_1 h_2}, k^{1_H} = k \text{ et } (k_1 k_2)^h = k_1^h k_2^h$$

Théorème 3.3.2

Soient H et G deux groupes. Soit $H^G = \{f : G \longrightarrow H\}$ l'ensemble de tous les fonctions définies sur G avec des valeurs dans H.

1- *$(H^G, \cdot)$ est un groupe où la loi " $\cdot$ "est définie par : $\forall \varphi, \psi \in H^G, \forall x \in G : (\varphi \cdot \psi)(x) = \varphi(x) \cdot_H \psi(x)$.*

2- *Le groupe G agit sur H^G tel que :*

$$G \times H^G \longrightarrow H^G$$

$$(a, \varphi) \longmapsto a \cdot \varphi$$

$a \cdot \varphi$ noté φ^a où $\varphi^a(x) = \varphi(xa^{-1})$.

3- *L'ensemble de tous les paires (a, φ), avec la multiplication donnée par $(a, \varphi)(b, \psi) = (ab, \varphi^b \psi)$, où $a, b \in G$, et $(\varphi, \psi) \in H^G$ est un groupe noté par $GW_r H^G$, s'appelle le produit en couronne de G et H.*

Preuve

1- $(H^G, \cdot)$ est un groupe où la loi " $\cdot$ "est définie par $\forall \varphi, \psi \in H^G, \forall x \in G : (\varphi \cdot \psi)(x) = \varphi(x) \cdot \psi(x)$:

i) H^G est non vide, il est contient par exemple l'élément défini par : pour tout x dans $G, x \longmapsto 1_H$, la loi " $\cdot$ " est interne puisque si $\varphi, \psi \in H^G$, alors $\varphi(x), \psi(x) \in H$, par conséquent $\varphi(x) \cdot \psi(x) \in H$, donc $(\varphi \cdot \psi)(x) \in H$, finalement $\varphi \cdot \psi \in H^G$.

ii) La loi est associative sur H, alors elle est aussi associative dans H^G.

iii) L'élément e de $G \longrightarrow H$ donné par $e(x) = 1_H$, pour tout $x \in G$, où 1_H est l'élément neutre de H, est l'élément neutre de $(H^G, \cdot)$. En effet :

$\forall \varphi \in H^G : \varphi \cdot e = e \cdot \varphi = \varphi, (\varphi \cdot e)(x) = \varphi(x) \cdot e(x) = \varphi(x) \cdot 1_H = \varphi(x)$.

iv) Chaque élément $\varphi \in H^G$ admet un élément symétrique noté φ^{-1}est défini par : $\forall x \in G, \varphi^{-1}(x) = (\varphi(x))^{-1}$. On a : $\varphi \cdot \varphi^{-1} = e$, de même $\varphi^{-1} \cdot \varphi = e$.

Et $(\varphi \cdot \varphi^{-1})(x) = \varphi(x) \cdot \varphi^{-1}(x) = \varphi(x) \cdot (\varphi(x))^{-1} = 1_H$.

Alors $(H^G, \cdot)$ est un groupe.

2- Le groupe G agit sur H^G tel que $(a, \varphi)(x) = \varphi^a(x) = \varphi(xa^{-1})$, avec $a, x \in G, \varphi \in H^G$:

i) $(\varphi^a)^b(x) = \varphi^a(xb^{-1})$
$= \varphi((xb^{-1})a^{-1})$
$= \varphi(x(ab)^{-1})$
$= \varphi^{ab}(x)$.

ii) $\varphi^{1_G}(x) = \varphi(x1_G^{-1}) = \varphi(x)$.

iii) $(\varphi\psi)^a(x) = \varphi\psi(xa^{-1})$
$= \varphi(xa^{-1})\psi(xa^{-1})$
$= \varphi^a(x)\psi^a(x)$.

3- Maintenant nous montrons que $G \times H^G$ est un groupe avec la multiplication.

i) La loi est interne sur $G \times H^G$ par définition.

ii) L'associativité : soient $\varphi, \psi, \eta \in H^G$ et $a, b, c \in G$:

$$((a, \varphi)(b, \psi))(c, \eta) = (ab, \varphi^b\psi)(c, \eta)$$
$$= ((ab)c, (\varphi^b\psi)^c\eta).$$

D'autre part

$$(a, \varphi)((b, \psi)(c, \eta)) = (a, \varphi)(bc, \psi^c\eta)$$
$$= (a(bc), \varphi^{bc}\psi^c\eta)$$
$$= ((ab)d, \varphi^{bc}\psi^c\eta).$$

iii) Soit $\varphi \in H^G, \varphi^{1_G} = \varphi, g \in G$, l'application $\varphi \longrightarrow \varphi^g$ est un automorphisme de H^G. Alors si e l'élément neutre de $H^G, e^g = e$. On a :

$$\begin{aligned}(a,\varphi)(1_G,e) &= (a1_G, \varphi^{1_G}e)\\ &= (a,\varphi e)\\ &= (a,\varphi).\end{aligned}$$

Aussi

$$\begin{aligned}(1_G,e)(a,\varphi) &= (1_G a, e^a\varphi)\\ &= (a,e\varphi)\\ &= (a,e).\end{aligned}$$

Alors l'élément neutre est existé.

iv) On a $(a,\varphi)(a^{-1},(\varphi^{-1})^{(a)^{-1}}) = (a^{-1},(\varphi^{-1})^{(a)^{-1}})(a,\varphi) = (1_G,e)$. Alors l'inverse de (a,φ) est $(a^{-1},(\varphi^{-1})^{(a)^{-1}})$.

Proposition 3.3.3

1- *Si G et H^G sont des groupes fini, alors le produit W en couronne est un groupe fini d'ordre $|W| = |G| \cdot |H|^{|G|}$.*

2- *Les groupes H^G et G sont des sous-groupes de W.*

3- *$GW_rH^G = G \times H^G$.*

Preuve

1- Il est claire.

2- On a l'applications $\Phi : H^G \longrightarrow G \times H^G$ donnée par $f \longmapsto (1_G, f)$, et $\Psi : G \longrightarrow G \times H^G$ donnée par $a \longmapsto (a,e)$. Φ et Ψ sont des homomorphismes car :

$$\begin{aligned}\Phi(f_1f_2) = (1_G, f_1f_2) &= (1_G1_G, f_1^{(1_G)}f_2)\\ &= (1_G,f_1)W_r(1_G,f_2)\\ &= \Phi(f_1)W_r\Phi(f_2).\end{aligned}$$

Et

$$\Psi(ab) = (ab, e) = (ab, e^b e)$$
$$= (a, e)W_r(b, e)$$
$$= \Psi(a)W_r\Psi(b).$$

- L'injectivité de $\Phi : H^G \longrightarrow G \times H^G$

$$f \longmapsto (1_G, f)$$

$\ker \Phi = \{f \in H^G : \Phi(f) = (1_G, e)\}$, où $e : G \longrightarrow H, x \longmapsto e(x) = 1_H$

$= \{f \in H^G : \Phi(f) = (1_G, f) = (1_G, e)\}$, donc $f = e$,

$\ker \Phi = \{e\}$. Alors Φ est injective.

D'après le premier théorème d'isomorphisme on a : $H^G/\ker \Phi \simeq \operatorname{Im} \Phi \leq G \times H^G$, et comme $\ker \Phi = \{e\}$, alors $H^G/\{e\} \simeq \operatorname{Im} \Phi \leq G \times H^G$, alors $H^G \simeq \operatorname{Im} \Phi \leq G \times H^G$. Donc H^G est un sous-groupe de $G \times H^G$.

- L'injectivité de $\Psi : G \longrightarrow G \times H^G$

$$a \longmapsto (a, e)$$

$\ker \Psi = \{a \in G : \Psi(a) = (1_G, e)\}$, où 1_G est l'élément neutre de G.

$= \{a \in G : \Psi(a) = (a, e) = (1_G, e)\}$, donc $a = 1_G$,

$\ker \Psi = \{1_G\}$. Alors Ψ est injective.

D'après le premier théorème d'isomorphisme on a : $G/\ker \Psi \simeq \operatorname{Im} \Psi \leq G \times H^G$, et comme $\ker \Psi = \{1_G\}$, alors $G/\{1_G\} \simeq \operatorname{Im} \Psi \leq G \times H^G$, alors $G \simeq \operatorname{Im} \Psi \leq G \times H^G$. Donc G est un sous-groupe de $G \times H^G$.

3- On a $GW_rH^G = G \times H^G$, car $(a, e)W_r(1_G, f) = (a1_G, e^{1_G} f) = (a, f)$, pour tous $(a, f) \in G \times H^G$.

3.4 Produit en couronne des groupes de permutation

Théorème 3.4.1

Soit $S(T)$ et $S(\Delta)$ sont des groupes de permutation sur T et Δ respectivement. Soit $S(T)^{\Delta}$ l'ensemble de tous les applications de Δ vers le groupe de permutation $S(T)$, i.e. $S(T)^{\Delta} = \{f : \Delta \longrightarrow S(T)\}$. Pour tout $f_1, f_2 \in S(T)^{\Delta}, (S(T)^{\Delta}, \cdot)$ est un groupe où $f_1 \cdot f_2$ est définie par : pour tout δ dans Δ, $(f_1 \cdot f_2)(\delta) = f_1(\delta) \cdot f_2(\delta)$.

Preuve

i) $S(T)^{\Delta}$ est non vide, il est contient par exemple l'élément défini par : pour tout δ dans $\Delta, \delta \longmapsto id_T$. La loi " $\cdot$ " est interne puisque, si $f_1, f_2 \in S(T)^{\Delta}$, alors $f_1(\delta), f_2(\delta) \in S(T)$. Par conséquent $f_1(\delta) \cdot f_2(\delta) \in S(T)$ donc $(f_1 \cdot f_2)(\delta) \in S(T)$, finalement $f_1 \cdot f_2 \in S(T)^{\Delta}$.

ii) La loi est associative sur $S(T)$, alors elle est aussi associative dans $S(T)^{\Delta}$.

iii) L'élément e de $\Delta \longrightarrow S(T)$ donné par $e(\delta) = id_T$, pour tout $\delta \in \Delta$, où id_T est l'élément neutre de $S(T)$, est l'élément neutre de $(S(T)^{\Delta}, \cdot)$. En effet $\forall f \in S(T)^{\Delta} : f \cdot e = e \cdot f = f$, et $(f \cdot e)(\delta) = f(\delta) \cdot e(\delta) = f(\delta) \cdot id_T = f(\delta)$.

iv) Chaque élément $f \in S(T)^{\Delta}$ admet un élément symétrique noté f^{-1}est défini par : $\forall \delta \in \Delta, f^{-1}(\delta) = (f(\delta))^{-1}$. On a : $f \cdot f^{-1} = e$, de même $f^{-1} \cdot f = e$.

Et $(f \cdot f^{-1})(\delta) = f(\delta) \cdot f^{-1}(\delta) = f(\delta) \cdot (f(\delta))^{-1} = id_T$.

Alors $(S(T)^{\Delta}, \cdot)$ est un groupe.

Proposition 3.4.2

Le groupe $S(\Delta)$ agit sur $S(T)^{\Delta}$ comme suit : $S(\Delta) \times S(T)^{\Delta} \longrightarrow S(T)^{\Delta}, (s, f) \longmapsto s \cdot f = f^s$, où $f^s(\delta) = (f \circ s^{-1})(\delta) = (fs^{-1})(\delta)$, pour tout $\delta \in \Delta$.

Preuve

Soit $f, f_1, f_2 \in S(T)^{\Delta}$ et $s, s_1, s_2 \in S(\Delta)$.

i) $((s_1 s_2) \cdot f)(\delta) = f^{(s_1 s_2)}(\delta)$

$= (f(s_1 s_2)^{-1})(\delta)$

$= (f(s_2^{-1} s_1^{-1}))(\delta)$

$= (f s_2^{-1})(s_1^{-1}(\delta))$

$= (s_2 \cdot f)(s_1^{-1}(\delta))$

$= (s_1 \cdot (s_2 \cdot f))(\delta).$

ii) $f^{id_{\Delta}}(\delta) = (f id_{\Delta}^{-1})(\delta)$

$= (f id_{\Delta})(\delta)$

$= (f)(\delta).$

iii) $(f_1 f_2)^s(\delta) = (f_1 f_2 \circ s^{-1})(\delta)$

$= f_1 f_2(s^{-1}(\delta))$

$= f_1(s^{-1}(\delta)) f_2(s^{-1}(\delta))$

$= f_1^s(\delta) f_2^s(\delta).$

Proposition 3.4.3

L'ensemble de tous les paires (f, s) avec la multiplication donnée par $(f_1, s_1)(f_2, s_2) = \left(f_1 f_2^{s_1^{-1}}, s_1 s_2\right)$, où $s_1, s_2 \in S(\Delta), f_1, f_2 \in S(T)^{\Delta}$, est un groupe noté par $S(T)^{\Delta} W_r S(\Delta)$, s'appelle le produit en couronne de $S(T)^{\Delta}$ par $S(\Delta)$.

Preuve

i) La loi est interne sur $S(T)^{\Delta} \times S(\Delta)$ par définition.

ii) L'associativité : soient $f_1, f_2, f_3 \in S(T)^{\Delta}$ et $s_1, s_2, s_3 \in S(\Delta)$.

$((f_1, s_1)(f_2, s_2))(f_3, s_3) = \left(f_1 f_2^{s_1^{-1}}, s_1 s_2\right)(f_3, s_3)$

$= \left(f_1 f_2^{s_1^{-1}} f_3^{(s_1 s_2)^{-1}}, s_1 s_2 s_3\right)$

$$= \left(f_1 f_2^{s_1^{-1}} f_3^{s_2^{-1} s_1^{-1}}, s_1 s_2 s_3\right).$$

D'autre part :

$$\begin{aligned}(f_1, s_1)((f_2, s_2)(f_3, s_3)) &= (f_1, s_1)\left(f_2 f_3^{s_2^{-1}}, s_2 s_3\right) \\ &= \left(f_1 (f_2 f_3^{s_2^{-1}})^{s_1^{-1}}, s_1 s_2 s_3\right) \\ &= \left(f_1 f_2^{s_1^{-1}} f_3^{s_2^{-1} s_1^{-1}}, s_1 s_2 s_3\right).\end{aligned}$$

iii) Pour tout $f \in S(T)^{\Delta}$, on a $f^{id_\Delta} = f$. Soit $s \in S(\Delta)$, l'application $f \mapsto f^s$ est automorphisme de $S(T)^{\Delta}$. Si e est l'élément neutre de $S(T)^{\Delta}$, tel que $e^s = e$.

Alors : $(f^{-1})^s = (f^s)^{-1}, (f, s)(e, id_\Delta) = \left(f e^{s^{-1}}, s \circ id_\Delta\right) = (f, s)$.

D'autre part : $(e, id_\Delta)(f, s) = \left(e f^{(id_\Delta)^{-1}}, id_\Delta \circ s\right) = (f, s)$.

Alors (e, id_Δ) est l'élément neutre de $S(T)^{\Delta} \times S(\Delta)$.

iv) On a $(f, s)\left((f^{-1})^s, s^{-1}\right) = \left((f^{-1})^s, s^{-1}\right)(f, s) = (e, id_\Delta)$. Alors l'inverse de (f, s) est $((f^{-1})^s, s^{-1})$.

Proposition 3.4.4

1- *Si $S(\Delta)$ et $S(T)^{\Delta}$ sont des groupes fini, alors le produit W en couronne est un groupe d'ordre $|W| = |S(T)|^{|\Delta|} \cdot |S(\Delta)|$.*

2- *Les groupes $S(T)^{\Delta}$ et $S(\Delta)$ sont des sous-groupes de W.*

3- $S(T)^{\Delta} W_r S(\Delta) = S(T)^{\Delta} \times S(\Delta)$.

4- *L'action de W sur $T \times \Delta$ est donné par $(f, s)(\gamma, \delta) = (f(\delta)(\gamma), s(\delta))$, pour tous $(f, s) \in S(T)^{\Delta} \times S(\Delta)$ et $(\gamma, \delta) \in T \times \Delta$.*

Preuve

1- Il est claire;

2- On a l'applications $\Phi : S(T)^{\Delta} \longrightarrow S(T)^{\Delta} \times S(\Delta)$, $f \mapsto (f, id_\Delta)$, et $\Psi : S(\Delta) \longrightarrow S(T)^{\Delta} \times S(\Delta), s \mapsto (e, s)$. sont des homomorphismes car :

$$\begin{aligned}\Phi(f_1f_2) = (f_1f_2, id_\Delta) &= \left(f_1 f_2^{(id_\Delta)^{-1}}, id_\Delta \circ id_\Delta\right)\\ &= (f_1, id_\Delta)W_r(f_2, id_\Delta)\\ &= \Phi(f_1)W_r\Phi(f_2).\end{aligned}$$

Et

$$\begin{aligned}\Psi(s_1 \circ s_2) = (e, s_1 \circ s_2) &= \left(ee^{(s_1)^{-1}}, s_1 \circ s_2\right)\\ &= (e, s_1)W_r(e, s_2)\\ &= \Psi(s_1)W_r\Psi(s_2).\end{aligned}$$

- L'injectivité de $\Phi : S(T)^\Delta \longrightarrow S(T)^\Delta \times S(\Delta)$

  $$f \longmapsto (f, id_\Delta)$$

  $\ker\Phi = \{f \in S(T)^\Delta : \Phi(f) = (e, id_\Delta)\}$, où $e : \Delta \longrightarrow S(T), \delta \longmapsto e(\delta) = id_T$

  $= \{f \in S(T)^\Delta : \Phi(f) = (f, id_\Delta) = (e, id_\Delta)\}$, donc $f = e$,

  $\ker\Phi = \{e\}$. Alors Φ est injective.

  D'après le premier théorème d'isomorphisme on a : $S(T)^\Delta/\ker\Phi \simeq \operatorname{Im}\Phi \leq S(T)^\Delta \times S(\Delta)$, et comme $\ker\Phi = \{e\}$, alors $S(T)^\Delta/\{e\} \simeq \operatorname{Im}\Phi \leq S(T)^\Delta \times S(\Delta)$, alors $S(T)^\Delta \simeq \operatorname{Im}\Phi \leq S(T)^\Delta \times S(\Delta)$. Donc $S(T)^\Delta$ est un sous-groupe de $S(T)^\Delta \times S(\Delta)$.

- L'injectivité de $\Psi : S(\Delta) \longrightarrow S(T)^\Delta \times S(\Delta)$

  $$s \longmapsto (e, s)$$

  $\ker\Psi = \{s \in S(\Delta) : \Psi(s) = (e, id_\Delta)\}$, où id_Δ est l'élément neutre de $S(\Delta)$

  $= \{s \in S(\Delta) : \Psi(s) = (e, s) = (e, id_\Delta)\}$, donc $s = id_\Delta$,

  $\ker\Psi = \{id_\Delta\}$. Alors Ψ est injective.

  D'après le premier théorème d'isomorphisme on a : $S(\Delta)/\ker\Psi \simeq \operatorname{Im}\Psi \leq S(T)^\Delta \times S(\Delta)$, et comme $\ker\Psi = \{id_\Delta\}$, alors $S(\Delta)/\{id_\Delta\} \simeq \operatorname{Im}\Psi \leq S(T)^\Delta \times S(\Delta)$, alors $S(\Delta) \simeq \operatorname{Im}\Psi \leq S(T)^\Delta \times S(\Delta)$. Donc $S(\Delta)$ est un sous-groupe de $S(T)^\Delta \times S(\Delta)$.

3- On a $S(T)^\Delta W_r S(\Delta) = S(T)^\Delta \times S(\Delta)$, car : $(f, id_\Delta)W_r(e, s) = \left(fe^{(id_\Delta)^{-1}}, id_\Delta \circ s\right) = (f, s)$, pour tous $(f, s) \in S(T)^\Delta \times S(\Delta)$.

4- Soient $(f_1, s_1)(f_2, s_2) \in S(T)^{\Delta} \times S(\Delta)$ et $(\gamma, \delta) \in T \times \Delta$.

i) $(e, id_{\Delta})(\gamma, \delta) = (e(\delta)(\gamma), id_{\Delta}(\delta)) = (id_T(\gamma), \delta) = (\gamma, \delta)$

ii) $((f_1, s_1)(f_2, s_2))(\gamma, \delta) = \left(f_1 f_2^{s_1^{-1}}, s_1 s_2\right)(\gamma, \delta)$

$$= \left(f_1 f_2^{s_1^{-1}}(\delta)(\gamma), s_1 s_2(\delta)\right)$$
$$= \left(\left(f_1(\delta) f_2^{s_1^{-1}}(\delta)\right)(\gamma), s_1 s_2(\delta)\right)$$
$$= (f_1(\delta)(f_2 \circ s_1)(\delta))(\gamma), s_1 s_2(\delta)).$$

D'autre part

$$(f_1, s_1)((f_2, s_2)(\gamma, \delta)) = (f_1, s_1)(f_2(\delta)(\gamma), s_2(\delta))$$
$$= (f_1(s_2(\delta))(f_2(\delta)(\gamma)), s_1 s_2(\delta)).$$

Proposition 3.4.5

Sous l'action de W sur $T \times \Delta$, le stabilisateur de tout point (γ, δ) dans $T \times \Delta$ dénoté par $W_{(\gamma,\delta)}$ est donné par : $W_{(\gamma,\delta)} = S(T)^{\Delta}(\delta)_{\gamma} \times S(\Delta)_{\delta}$. Où $S(T)^{\Delta}(\delta)_{\gamma}$ est l'ensemble de tout le $f(\delta)$ qui stabilisent γ, et $S(\Delta)_{\delta}$ est le stabilisateur de δ sous l'action de $S(\Delta)$ sur Δ.

Preuve

On a :

$$W_{(\gamma,\delta)} = \{(f, s) \in S(T)^{\Delta} \times S(\Delta)/(f, s)(\gamma, \delta) = (\gamma, \delta)\}$$
$$= \{(f, s) \in S(T)^{\Delta} \times S(\Delta)/(f(\delta)\gamma, s(\delta)\gamma) = (\gamma, \delta)\}$$
$$= \{(f, s) \in S(T)^{\Delta} \times S(\Delta)/f(\delta)\gamma = \gamma, s(\delta)\gamma = \delta\}$$
$$= S(T)^{\Delta}(\delta)_{\gamma} \times S(\Delta)_{\delta}.$$

Exemple 3.4.6

On considère les groupes de permutation $S(T) = \{(1), (12)\}$ et $S(\Delta) = \{(1), (12), (13), (23), (123), (132)\}$ sur les ensembles $T = \{1, 2\}$ et $\Delta = \{1, 2, 3\}$ respectivement. Soit $S(T)^{\Delta} = \{f : \Delta \longrightarrow S(T)\}$, tel que $|S(T)|^{|\Delta|} = 2^3 = 8$. Les applications sont :

$f_1 : 1 \longmapsto (1), 2 \longmapsto (1), 3 \longmapsto (1)$

$f_2 : 1 \longmapsto (1), 2 \longmapsto (1), 3 \longmapsto (12)$

$f_3 : 1 \longmapsto (1), 2 \longmapsto (12), 3 \longmapsto (1)$

$f_4 : 1 \longmapsto (1), 2 \longmapsto (12), 3 \longmapsto (12)$

$f_5 : 1 \longmapsto (12), 2 \longmapsto (1), 3 \longmapsto (1)$

$f_6 : 1 \longmapsto (12), 2 \longmapsto (1), 3 \longmapsto (12)$

$f_7 : 1 \longmapsto (12), 2 \longmapsto (12), 3 \longmapsto (1)$

$f_8 : 1 \longmapsto (12), 2 \longmapsto (12), 3 \longmapsto (12)$

On a :

$$S(T)^{\Delta} \times S(\Delta) = \big\{(f, s)/f \in S(T)^{\Delta}, s \in S(\Delta)\big\}$$
$$= \{(f_i, (1)), (f_i, (12)), (f_i, (13)), (f_i, (23)), (f_i, (123)), (f_i, (132))\}, \text{ tel que}$$

$: 1 \leq i \leq 8$

Et

$$\big|S(T)^{\Delta} \times S(\Delta)\big| = \big|S(T)^{\Delta}\big| \cdot |S(\Delta)| = 8 \cdot 6 = 48.$$

Alors $(S(T)^{\Delta} \times S(\Delta), \cdot)$ est un groupe avec la loi défini par $(\varphi, s_1)(\psi, s_2) = \Big(\varphi\psi^{(s_1)^{-1}}, s_1 s_2\Big)$.

On a :

$$T \times \Delta = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3)\}.$$

Le stabilisateur de $(1,1)$ dénoté par :

$$W_{(1,1)} = S(T)^{\Delta}(1)_1 \times S(\Delta)_1$$
$$= \{f_1, f_2, f_3, f_4\} \times \{(1), (23)\}$$
$$= \{(f_1, (1)), (f_2, (1)), (f_3, (1)), (f_4, (1)), (f_1, (23)), (f_2, (23)), (f_3, (23)), (f_4, (23))\}.$$

Alors $W_{(1,1)}$ est un sous-groupe de $S(T)^{\Delta} \times S(\Delta)$ d'ordre 8.

De la même façon on a :

$$W_{(1,2)} = S(T)^{\Delta}(2)_1 \times S(\Delta)_2$$
$$= \{f_1, f_2, f_5, f_6\} \times \{(1), (13)\}$$
$$= \{(f_1, (1)), (f_2, (1)), (f_5, (1)), (f_6, (1)), (f_1, (13)), (f_2, (13)), (f_5, (23)), (f_6, (23))\}.$$

Alors $W_{(1,2)}$ est un sous-groupe de $S(T)^{\Delta} \times S(\Delta)$ d'ordre 8.

$$W_{(1,3)} = S(T)^{\Delta}(3)_1 \times S(\Delta)_3$$
$$= \{f_1, f_3, f_5, f_7\} \times \{(1), (12)\}$$
$$= \{(f_1, (1)), (f_3, (1)), (f_5, (1)), (f_7, (1)), (f_1, (12)), (f_3, (12)), (f_5, (12)), (f_7, (12))\}.$$

Alors $W_{(1,3)}$ est un sous-groupe de $S(T)^{\Delta} \times S(\Delta)$ d'ordre 8.

$$W_{(2,1)} = S(T)^{\Delta}(1)_2 \times S(\Delta)_1$$
$$= \{f_1, f_2, f_3, f_4\} \times \{(1), (23)\}$$

$= \{(f_1,(1)),(f_2,(1)),(f_3,(1)),(f_4,(1)),(f_1,(23)),(f_2,(23)),(f_3,(23)),(f_4,(23))\}.$

Alors $W_{(2,1)}$ est un sous-groupe de $S(T)^{\Delta} \times S(\Delta)$ d'ordre 8.

$W_{(2,2)} = S(T)^{\Delta}(2)_2 \times S(\Delta)_2$

$= \{f_1, f_2, f_5, f_6\} \times \{(1),(13)\}$

$= \{(f_1,(1)),(f_2,(1)),(f_5,(1)),(f_6,(1)),(f_1,(13)),(f_2,(13)),(f_5,(13)),(f_6,(13))\}.$

Alors $W_{(2,2)}$ est un sous-groupe de $S(T)^{\Delta} \times S(\Delta)$ d'ordre 8.

$W_{(2,3)} = S(T)^{\Delta}(3)_2 \times S(\Delta)_3$

$= \{f_1, f_3, f_5, f_7\} \times \{(1),(12)\}$

$= \{(f_1,(1)),(f_3,(1)),(f_5,(1)),(f_7,(1)),(f_1,(12)),(f_3,(12)),(f_5,(12)),(f_7,(12))\}.$

Alors $W_{(2,3)}$ est un sous-groupe de $S(T)^{\Delta} \times S(\Delta)$ d'ordre 8.

En conclusion, nous avons :

$|W_{(1,1)}| = |W_{(2,1)}| = |W_{(1,2)}| = |W_{(2,2)}| = |W_{(1,3)}| = W_{(2,3)}$.

Pour $(\gamma,\delta) \in T \times \Delta$, on a $\left|W_{(\gamma,\delta)}\right| \cdot |W(\gamma,\delta)| = |W|$, alors $|W(\gamma,\delta)| = \dfrac{|W|}{\left|W_{(\gamma,\delta)}\right|} = \dfrac{48}{8} = 6.$

Dans cet exemple, on a :

$(f_1,(1))(1,1) = (f_2,(1))(1,1) = (f_3,(1))(1,1) = (f_4,(1))(1,1) = (1,1)$

$(f_1,(12))(1,1) = (f_2,(12))(1,1) = (f_3,(12))(1,1) = (f_4,(12))(1,1) = (1,2)$

$(f_1,(13))(1,1) = (f_2,(13))(1,1) = (f_3,(13))(1,1) = (f_4,(13))(1,1) = (1,1)$

$(f_1,(23))(1,1) = (f_2,(23))(1,1) = (f_3,(23))(1,1) = (f_4,(23))(1,1) = (1,1)$

$(f_1,(123))(1,1) = (f_2,(123))(1,1) = (f_3,(123))(1,1) = (f_4,(123))(1,1) = (1,2)$

$(f_1,(132))(1,1) = (f_2,(132))(1,1) = (f_3,(132))(1,1) = (f_4,(132))(1,1) = (1,3)$

$(f_5,(1))(1,1) = (f_6,(1))(1,1) = (f_7,(1))(1,1) = (f_8,(1))(1,1) = (2,1)$

$(f_5,(12))(1,1) = (f_6,(12))(1,1) = (f_7,(12))(1,1) = (f_8,(12))(1,1) = (2,2)$

$(f_5,(13))(1,1) = (f_6,(13))(1,1) = (f_7,(13))(1,1) = (f_8,(13))(1,1) = (2,3)$

$(f_5,(23))(1,1) = (f_6,(23))(1,1) = (f_7,(23))(1,1) = (f_8,(23))(1,1) = (2,1)$

$(f_5,(123))(1,1) = (f_6,(123))(1,1) = (f_7,(123))(1,1) = (f_8,(123))(1,1) = (2,2)$

$(f_5,(132))(1,1) = (f_6,(132))(1,1) = (f_7,(132))(1,1) = (f_8,(132))(1,1) = (2,3)$

Alors l'orbite de $(1,1)$ est $\{(1,1),(1,2),(1,3),(2,1),(2,2),(2,3)\} = T \times \Delta$.

Conclusion

Nous avons présenté dans ce travail le produit en couronne de groupes, plus précissement le produit en couronne des groupes de symétries, d'autre part on fait une étude sur l'action de groupe précédent sur le produit cartésien de deux ensembles.

Bibliographie

[1] Ibrahim A. A. et Audu M. S. On wreath product of permutation groups, Proyecciones Vol. 26, N°1, pp. 73-90, (May 2007).

[2] F. Bergeron. MAT 2250 Introduction à la théorie des groupes (à partir de notes de Luc Bélair et Christophe Hohlweg), Université du Québec à Montréal, (13 décembre 2015).

[3] J. Calais. Eléments de Théorie des groupes, Presses Universitaires de France, (1984).

[4] T. Connor et J. Vercruysse. Algébre I, Cours pour $2^{\text{ième}}$ année de Bachelier en sciences mathématiques, Université Libre de Bruxelles, (12 septembre 2012).

[5] J.R. Durbin. Modern Algebra An Introduction, The University of Texas at Austin, (2003).

[6] D. Frodone, M. Maumy-Bertrand et F. Bertrand. Mathématiques Algèbre et géométrie en 30 fiches, Dunod, Paris, (2009).

[7] N. Ghadbane. Cours Master 1, Semi-groupe de transformation et décomposition d'automate fini, Université de M. Boudiaf M'silla, (2017-2018).

[8] J.D.P. Meldrum Wreath products of groups and semi-groups, University of Edinburgh, (1995).

[9] D. Mihoubi. Cours $3^{\text{ième}}$ anneé licence, Introduction à la Théorie des groupes, Université de M.Boudiaf M'sila, (2015-2016).

[10] A. E. Nagy and C. L. Nehaniv. Cascade Product of Permutation Groups, Centre for computer science and informatics, U. K and Centre for research in mathematics, Australia, (2013).

[11] J.J. Rotman. An Introduction to the Théory of Groups, Department of Mathematics, Univercity of Illinois, (1994).

[12] J.L. Rouget. le groupe symétrique, cours internet http ://www.maths-france.fr, (2016).

[13] Audu M. S. Wreath Product of Permutation Group, A Research Oriented Course In Arithmetics of Elliptic Curves, Groups and Loops, Lecture Notes Series, National Mathematical Centre, Abuja, (2001).

[14] D. Schaub.Eléments de la Théorie des groupes, Licence de Mathématiques, Université d'Angers, (1997/98).

ملخص

هذه مذكرة ماستر رياضيات متقطعة، هي جزء من نظرية الزمر. في هذا العمل نتبع الخطوات الآتية:

- معلومات عامة عن الزمر.

- دراسة حول الزمر المتجانسة.

- الجداء الحلقي للزمر المتجانسة.

الكلمات المفتاحية: زمرة - تشاكل الزمر- تأثيرات الزمر- الجداء المباشر- جداء الشبه مباشر- الجداء الحلقي.

Résumé:

Ce mémoire de master mathématiques discrètes s'inscrit dans le cadre de la théorie des groupes. Dans ce travail, nous avons suivrons les étapes suivantes :

• Notions élémentaires sur les groupes.

• Etudes sur les groupes symétriques.

• Le produit en couronne de groupes symétriques.

Mots clés:

Groupe, morphisme de groupes, actions de groupe, produit direct, produit semi direct et produit en couronne.

Abstract:

This memory of master degree mathematics discrete lies within the scope of the theory of the groups. In this work, we have will follow the following stages :

• General information on the groups.

• Study on the groups symmetrical.

• The wreath product on the group of permutation.

Key words:

Group, morphisms of groups, acts of groups, direct product, semi direct product, wreath product.