Université mohamed boudiaf-M'sila
Faculté des Mathématiques et de l'Informatique
Departement de Mathématiques

MEMOIRE de fin d'étude

Présenté pour l'obtention du diplôme de MASTER

Domaine : Mathématiques et Informatiques

Filière : Mathématiques

Option : Mathématiques Appliquées et discrètes

Par

-Messeguem Leyla -Bettache Amina

THÈME

Etude sur les automorphismes de groupe : Applications sur les codes

Soutenu publiquement le : 04/06/ 2017

Devant le jury composé de :

1)Mr. Douadi Mihoubi Prof. Univ de M'sila Président
2)Mr. Nacer Ghadbane Prof. Univ de M'sila Encadreur
3)Mr. Lakhdar Heboub MA/A. Univ de M'sila Examinateur

Dirigé par :

Mr. Nacer Ghadbane

Année: **2016/2017**

Remerciements

Avant tout nous remercions **Allah**, le tout puissant d'avoir, éclairé notre vie, renforcé notre courage et notre volanté pour finir ce travail.

nous tenons à remercier particuliérement notre encadreur Dr. **Nacer Ghadbane**, pour toute l'aide qu'il nous a apporté et sa patience ses conseils et pour avoir guidé ce travail avec beaucoup d'intéret.

nous tenons à remercier aussi Pr. **Douadi Mihoubi,** d'avoir accepté de présider le jury de ce mémoire.

nous tenons à remercier Dr **Lakhdar Heboub,** pour avoir accepté d'examiner notre mémoire.

nos remerciements s'adressent également à tout les enseignants du département de mathématiques pour leurs dévouement et leurs générosité.

nous tenons ici à exprimer nos sentiments respectueux à nos chers parents à qui nous dédions ce travail pour leur grand soutien.

Un grand merci à nos familles, à nos proches et à nos collégues pour leurs encouragements et pour leurs amitiés.

Dédicace

Messeguem Leyla

Au nom de Allah chément et le miséricordieux.

-Je dédie ce modeste travail.

- A Mon pére

Tes sacrifices et tes Priéres m'ont permis de vivre ce jour. Rien ne saurait exprimer la fierté, la reconnaissance et l'amour que

je te porte. que Dieu le tout puissant te procure, santé et

longue vie.

A Ma Mére

Avec tout mon amour pour ton soutien et tes encouragements. j'espére rester à la hauteur de tes espoirs que Dieu te protége et t'accorde santé et longue vie

-A la famille Messegueme.

-A toute nos amies.

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

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

Dédicace

Bettache Amina

Au nom de Allah chément et le miséricordieux.

-Je dédie ce modeste travail.

- A Mon pére

Tes sacrifices et tes Priéres m'ont permis de vivre ce jour. Rien ne saurait exprimer la fierté, la reconnaissance et l'amour que

je te porte. que Dieu le tout puissant te procure, santé et

longue vie.

A Ma Mére

Avec tout mon amour pour ton soutien et tes encouragements. j'espére rester à la hauteur de tes espoirs que Dieu te protége et t'accorde santé et longue vie

-A la famille Bettache.

-A toute nos amies.

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

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

Résumé:

Ce mémoire de master mathématiques appliquées et discrètes s'inscrit dans le cadre de la théorie des groupes et leurs applications sur les codes.

Dans ce travail, nous suivrons les étapes suivantes :

- Généralités sur les groupes.
- Etude sur les automorphismes de groupes.
- Quelques applications sur les codes.

Mots clés :

Groupe , sous-groupe , groupe quotient, ,groupe symétrique , groupe monogèn ,groupe cyclique, groupe diédrale, Morphisme de

Summary:

This memory of master degree mathematics applied and discrete lies within the scope of the theory of the groups and their applications on the codes.

In this work, we will follow the following stages:

- General information on the groups.
- Study on the automorphisms of groups.
- Some applications on the codes.

Keywords:

Group, sub-group, quotient group, group symmetrical, monogèn group, cyclic group, group diadrèle Homomorphism of group, the Core and the Image of a homomorphism of group, automorphism of group, monoid, Code.

[redacted] :

[redacted].

[redacted] :

[redacted].

[redacted].

[redacted].

Notations

A **:** Alphabet fini.

A^*: L'ensemble des mots sur A.

A^+ : $A^* - \{\varepsilon\}$

I : L'ensemble d'indice.

$|w|$: la longeur du mot w.

$|w|_\sigma$: le nombre d'occurence de la lettre σ dans le mot w.

$\cong$: isomorphe.

$H \lhd G$: H est un sous groupe normal du groupe$G$.

$Z(G)$: le centre de groupe G.

$Aut(G)$: le groupe des automorphismes de groupe G.

$Int(G)$: le groupe des automorphismes intérieurs de groupe G.

$Hom(G, G')$: l'ensemble des morphismes de groupes de G dans G'.

$End(G)$: l'ensemble des morphismes de groupes de G dans lui-même.

P_n : polygone régulier de n sommets.

D_n : groupe diédral.

S_n : groupe symétrique.

GL_n : groupe général linéaire de degré n.

$X\,(G, H)_\Phi$: code à groupe.

Table des matières

Introduction

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

Dans ce mémoire, on s'intéresse à l'étude des automorphismes d'un groupe. Deux groupes G et G' sont dits isomorphes et on note cette relation par $G \simeq G'$, s'il existe un isomorphisme de groupes de G dans G'. Dans ce cas G et G' sont dans la même classe de la relation $\simeq$ définie sur l'ensemble des groupes. Cette notion est d'une extrême importance pour la classification des groupes. Si deux groupes G et G' sont isomorphes alors ils ont la même structure algébrique ou bien les mêmes propriétés algébriques, en d'autres mots G' représente G.

Ce travail est composé de trois chapitres :

Le premier chapitre consiste à un rappel des notions élémentaires sur les groupes.

Dans le deuxième chapitre, on s'intéresse aux trois théorèmes d'isomorphismes, les automorphismes d'un groupe cyclique.

Enfin, on donne dans le troisième chapitre la construction de certains codes à groupes

Chapitre 1

Généralité sur les groupes

1.1 Notion de groupe

Définition 1.1.1

Un groupe $(G\ ;*)$ est un ensemble G muni d'une loi interne (ou loi de composition interne), c'est -à-dire une application

$$G \times G \to G$$

$$(x; y) \to x * y$$

Possédant les propriétés suivantes :

(i) *La loi est associative :* $\forall x, y, z \in G \quad (x * y) * z = x * (y * z)$

(ii) *Il existe un élément* $e \in G$*, appelé élément neutre de G, tel que :*

$$\forall g \in G, g * e = e * g = g.$$

(iii) *pour tout élément* $g \in G$*, il existe g' ∈ G, appelé symétrique de g, tel que :* $g * g\prime = g\prime * g = e$.

Exemples 1.1.1

1. $(\mathbb{Z}, +)$ *est un groupe.*

2. $(\mathbb{Q}^*, \times)$ *est un groupe.*

3. $(\mathbb{R}, +)$ *est un groupe.*

4. $(\mathbb{N}, +)$ *n'est pas groupe car par exemple l'élément 1 n'admet pas un symétrique dans* $(\mathbb{N}, +)$.

5. *Soit* E *un ensemble. On note* S_E *le groupe des applications bijectives de* E *dans* E *(ou permutations de* E*) pour la loi de composition interne définie par la composition des applications.*

   Si $E = \{1, 2, 3\}$ *les éléments de* S_E *sont*

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

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

   On notera ce groupe S_3*, et de façon générale on notera* S_n *le groupe* S_E *pour* $E = \{1, ..., n\}$*. Le groupe* S_E *est appelé groupe des permutations de l'ensemble E, ou groupe symétrique.*

Remarque 1.1.1

Si $(E, *)$*possède un élément neutre* e*, alors*

1. l'élément neutre e est unique : en effet, soit e' un élément neutre alors

$$e = e * e' = e' * e = e'.$$

2. Si $A \subseteq E$ est stable pour $*$, $(A, *)$ posséde un élément neutre si et seulement si $e \in A$. De plus, dans ce cas, e est l'élément neutre de $(A, *)$.

Remarque 1.1.2

Si $(G, *)$ *est un groupe tel que la loi* $*$ *vérifier à la propriété :* $\forall x, y \in G$, $x * y = y * x$*, le groupe* $(G, *)$ *est dit commutatif ou encore abélien.*

Exemples 1.1.2

1. *Les groupes* $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \times)$, $(M_n(\mathbb{C}), +)$ *sont abéliens.*

2. *Le groupe* $(GL_n(\mathbb{C}), \times)$ *n'est pas abélien.*

3. *Si card* $E \geq 3$ *, le groupe* S_E *n'est pas abélien.*

Remarque 1.1.3

En général, dans un goupe non abélien, $(xy)^n \neq x^n y^n$, $n \in \mathbb{N}$. *Mais si* $xy = yx$*, alors* $(xy)^n = x^n y^n$, $n \in N$.

Ordre d'un groupe

Définition 1.1.2

Un groupe G *est dit fini s'il n'a qu'un nombre fini d'éléments. 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 $o(x)$, le cardinal de $\langle x \rangle$. Si ce cardinal est infini, on dit que x est d'ordre infini.

Remarque 1.1.4

1. *Soient G un groupe fini et x un élément de G, alors $o\langle x \rangle \leq |G|$.*
2. *Dans tout groupe G, l'élément neutre est le seul élément d'ordre* 1.
3. *Dans $(\mathbb{Z}, +)$, tous les éléments non nuls sont d'ordre infini.*

Proposition 1.1.1

Soient G un groupe et x un élément d'ordre fini de G. Alors $o(x)$ est le plus petit entier positif s tel que $x^s = 1_G$.

Démonstration.

Si pour tout i et j dans $\mathbb{Z}$, $i \neq j$ on a $x^i \neq x^j$, alors l'ordre de x est infini, ce qui est contraire à l'hypothèse. Donc il existe $p > q$ tel que $x^p = x^q$ i.e. $x^{p-q} = 1_G$, avec $p - q > 0$.

L'ensemble $\{s \in \mathbb{N}^*, x^s = 1_G\}$ est un ensemble non vide d'entiers positif s, il admet donc un plus petit élément n. Alors x = $\{1_G, ..., x^{n-1}\}$, et $o(x) = n$. ■

Exemples 1.1.3

1. *Une rotation d'angle $\frac{2\pi}{n}$ est un élément d'order n du groupe des rotation du plan.*
2. *Dans le groupe S_3, les éléments τ_1, τ_2, τ_3 sont d'ordre* 2, *les éléments σ_1 et σ_2 d'ordre* 3. *Le groupe S_3 est d'ordre 6 plus généralement , pour tout $n \geq 2$, le groupe S_n est d'ordre $n!$.*
3. *Dans $(\mathbb{Z}, +)$ tous les éléments non nuls sont d'ordre infini et $ord(0) = 1$! En effet si $n \neq 0$, alors $n\mathbb{Z} = \langle n \rangle$ est en bijection avec $\mathbb{Z}$ et est donc, de ce fait, infini.*

Les sous groupes

Définition 1.1.3

Un ensemble $H \subseteq G$ est un sous-groupe de G si il vérifie les conditions suivantes :

1. *H est non vide.*
2. *H est un sous-ensemble stable de $(G, *)$.*
3. *$x^{-1} \in H$ pour tout $x \in H$.*

Notation 1.1.1 *Si H est un sous-groupe de G, on écrit $H \leq G$. Un sous-groupe différent de G et de $\{e\}$ est dit sous-groupe propre.*

Proposition 1.1.2

Un sous-ensemble non vide H d'un groupe G est un sous-groupe de G si et seulement si

1. *$\forall (x, y) \in H \times H,\ xy \in H$.*
2. *$\forall x \in H,\ x^{-1} \in H$.*

Remarque 1.1.5

1. *Les deux assertions 1 et 2 de la proposition sont équivalentes à*

$$\forall (x, y) \in H \times H, xy^{-1} \in H \text{ et } e_G \in H.$$

2. *Un groupe G ayant au moins deux éléments admet au moins deux sous-groupes : G et le sous-groupe réduit à l'élément neutre.*
3. *Il est clair que si H est un sous-groupe d'un groupe G et si K est un sous-groupe de H, alors K est un sous-groupe de G.*

Exemples 1.1.4

1. $(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$.
2. $(\mathbb{Q}^*,\times) \leq (\mathbb{R}^*,\times) \leq (\mathbb{C}^*,\times)$.
3. *Les sous-groupes de* $(\mathbb{Z},+)$ *sont les* $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\}$, *pour* n *parcourant* N.
4. $\{e\}$ *et* G *sont les sous-groupes triviaux du groupe* G.

Proposition 1.1.3

Soient G *un groupe,* I *un ensemble non vide et* $\{H_i\}_{i\in I}$ *une famille de sous-groupes de* G. *Alors* $\bigcap_{i\in I} H_i$ *est un sous-groupe de* G.

Remarque 1.1.6

Une réunion de sous-groupes d'un groupe G *n'est pas en général un sous-groupe de* G. *Par exemple, on sait que* $3\mathbb{Z}$ *et* $5\mathbb{Z}$ *sont des sous-groupes de* $(\mathbb{Z},+)$. *Montrons que* $3\mathbb{Z}\cup 5\mathbb{Z}$ *n'est pas un sous groupe de* $(\mathbb{Z},+)$. *On a* $3 \in 3\mathbb{Z}\cup 5\mathbb{Z}$ *et* $5 \in 3\mathbb{Z}\cup 5\mathbb{Z}$, *mais* $3+5=8 \notin 3\mathbb{Z}\cup 5\mathbb{Z}$. *Donc* " $+$ " *n'est pas interne sur* $3\mathbb{Z}\cup 5\mathbb{Z}$.

Sous-groupes engendrés

Définition 1.1.4

soit G *un groupe et* S *une partie de* G , *on appelle Sous-groupe engendré par* S, *et On note* $< S >$ *le plus petit (pour la relation d'inclusion) Sous-groupe de* G *contenant* S.

Proposition 1.1.4

C'est l'intersection de tous les sous-groupes de G *qui contiennent* S.

Proposition 1.1.5

Soient G *un groupe et* S *une partie non vide de* G *on a*

$$< S >= \{x_1....x_n, n \in \mathbb{N}^*, x_i \in S \text{ où } x_i^{-1} \in S, \forall i\ 1 \leq i \leq n\}.$$

Démonstration.

Notons

$$H = \{\prod_{i=1}^{n} x_i, n \in \mathbb{N}^*, x_i \in S \text{ où } x_i^{-1} \in S, \forall i, 1 \leq i \leq n\}$$

On remarque que S est contenu dans H. Soient $x = x_1....x_n$ et $y = y_1....y_p$ des éléments de H, alors $xy^{-1} = x_1....x_n y_p^{-1}....y_1^{-1}$ appartient à H, ce qui preve que H est un sous-groupe de G, D'où $< S >$ est contenu dans H, Il est claire que tout sous-groupe de G contenant S contient H, D'où $< S >$. ■

Remarque 1.1.7

Si la loi de G est notée additivement, on a

$< S > = \{x_1 + ... + x_n, n \in \mathbb{N}^*, \pm x_i \in S, \forall i 1 \leq i \leq n\}$ *D'où* $< x > = \{nx, n \in \mathbb{Z}\}$.

Exemples 1.1.5

Soit le groupe $(\mathbb{Z}, +)$

1. *Le sous-groupe engendré par* $E_1 = \{2\}$ *est* $H_1 = 2\mathbb{Z}$.
2. *Le sous-groupe engendré par* $E_2 = \{8, 12\}$ *est* $H_2 = 4\mathbb{Z}$.
3. *Le sous-groupe engendré par* $E = \{a, b\}$ *est* $H = n\mathbb{Z}$ *où* $n = pgcd(a, b)$.

Sous-groupes normaux

Définition 1.1.5

On dit qu'un sous-groupe H d'un groupe G est normal (ou distingué) dans G s'il est stable par conjugaison, c'est-à-dire si : $\forall h \in H, \forall x \in G, xhx^{-1} \in H$.

Notation 1.1.2

Si H est un sous-groupe normal de G, on note $H \lhd G$.

Proposition 1.1.6

Un sous-groupe H d'un groupe G est normal dans G si et seulement s'il vérifie les conditions équivalentes :

1. $\forall x \in G,\ xH \subset Hx$
2. $\forall x \in G,\ xH = Hx$
3. $\forall x \in G,\ xHx^{-1} \subset H$
4. $\forall x \in G,\ xHx^{-1} = H$
5. $\forall h \in H, \forall x \in G\ xhx^{-1} \in H$
6. *Il existe un groupe G' et un morphisme de groupes $f : G \to G'$ tel que*

$$H = Ker(f).$$

Exemples 1.1.6

1. *Le centre du groupe $Z(G)$ est normal dans G. En effet, si $x \in G$, alors $xg = gx$ pour tout $g \in Z(G)$. Donc $xZ(G) = Z(G)x$.*
2. *$Int(G) \lhd Aut(G)$.*
3. *Si G est un groupe abélien, tout sous-groupe est normal dans G.*
4. *L'intersection de sous-groupes normaux dans G est un sous-groupe normal dans G.*

Remarque 1.1.8

Soient G un groupe, H et K deux sous-groupes de G. Si H est normal dans G, alors HK est un sous-groupe de G et H est un sous-groupe normal de HK.

Groupe quotients

On considère un groupe G, H un sous-groupe de G, et on définit sur G la relation :

$$(xRy) \iff (x^{-1}y \in H).$$

Proposition 1.1.7

1. *La relation R est une relation d'équivalence.*

2. *Soit x un élément de G, sa classe d'équivalence pour la relation R est l'ensemble $xH = \{xh,\ h \in H\}$.*

Définition 1.1.6

La relation R est appelée relation d'équivalence à gauche modulo H et xH la classe à gauche de x modulo H.

Notation 1.1.3

On note $(G/H)g$ $(resp.(G/H)d)$ l'ensemble des classes d'équivalence des éléments de G pour la relation à gauche$(resp.$à droite$)$ modulo H. Ces ensembles sont aussi appelés ensembles quotients à gauche$(resp.$à droite $)$ moduloH.

Proposition 1.1.8

Soient G un groupe et H un sous-groupe de G.

1. *Toute classe à gauche xH (resp.à droite Hx) est équipotente à H.*

2. *Les ensembles $(G/H)g$ et $(G/H)d$ sont équipotents.*

Définition 1.1.7

Soit E un ensemble muni d'une loi de composition interne (notée multiplicativement) sur lequel est définie une relation d'équivalence R.

Notation 1.1.4

1. *R est compatible à droite ($resp.$ à gauche) avec la loi si, quels que soient x, y a dans E, on a $(xRy) \Longrightarrow (xaRya)(resp.\ (xRy) \Longrightarrow (axRay))$.*

2. *R est compatible avec la loi si elle est compatible à droite et à gauche.*

Définition 1.1.8

Soient G un groupe et H un sous-groupe de G. On appelle indice de H dans G, qu'on note $[G : H]$, le cardinal de l'ensemble $(G/H)g$ $(ou\ (G/H)d)$.

Théorème 1.1.1 $(de\ Lagrange)$

Si G est un groupe fini, pour tout sous-groupe H de G on a $|G| = |H|[G : H]$. En particulier, $|\ H\ |$ divise $|\ G\ |$.

Théorème 1.1.2 $(formule\ de\ l\ 'indice\ )$

Si H est un sous-groupe d'indice fini d'un groupe G et si K est un sous-groupe de G contenant H $(H \subseteq K \subseteq G)$, alors K est d'indice fini dans G et $[G : H] = [G : K][K : H]$.

Remarque 1.1.9

Si la relationn R est compatible avec la loi de G, la loi induite sur G/R par celle de G est définie par $\overline{xy} = \overline{xy}$.

Il est clair que si la loi de G est associative (resp.commutative , resp admet un élément neutre e , resp.tout élément x admet un élément symétrique x^{-1}), il en est de même pour la loi induite sur G/R, e est l'élément neutre, l'élément symétrique de x est x^{-1}.

Théorème 1.1.3

Soit G un groupe et H un sous-groupe normal de G, alors la fonction

$$\begin{aligned} G/H \times G/H &\longrightarrow G/H \\ (xH\ ,\ yH) &\longrightarrow xHyH = xyH \end{aligned}$$

munit G/H d'une structure de groupe. On l'appelle le groupe quotient de G par H. De plus

1. *$e_{G/H} = H$ et $(xH)^{-1} = x^{-1}H$.*
2. *la fonction $\pi : G \longrightarrow G/H$ définie par $\pi(x) = xH$ est un morphisme de groupe surjectif appelé épimorphisme canonique.*
3. *$ker(\pi) = H$.*

Notation 1.1.5

En notation additive, on obtient commme loi de composition interne :

$$(x + H) + (y + H) = (x + y) + H$$

Groupe Symétrique

Considerons plus en detail le groupe symetrique S_E des permutation d'un ensemble E de cardinal n commençons par calculer son ordre.

Proposition 1.1.9

Soit $n \in \mathbb{N}^*$, alors $|S_n| = n!$ plus generalement si E et F deux ensemble de cardinal n alors l'ensemble $B(E, F)$ des bijection de E dans F est de cardinal $n!$

Remarque 1.1.10

Si $E = \{1, ..., n\}$ *on note traditionnellement* S_E *par* S_n *ses élément sont réprésentés par des matrice* $2 \times n$

Si $\sigma \in S_n$ *on note* $\sigma = \begin{pmatrix} 1 & 2 & ..... & n \\ \sigma(1) & \sigma(2) & ..... & \sigma(n) \end{pmatrix}$ *ou plus simplement* $\sigma(1)\ \sigma(2).....\sigma(n)$.

1.2 Morphismes de groupes

Définition 1.2.1

Soient $(G, *)$ *et* $(G', *')$ *deux groupes. Un morphisme (ou homomorphisme) de groupes de* G *dans* G' *est une application* $f : G \to G'$ *vérifiant :*

$$\forall (x, y) \in G \times G,\ f(x * y) = f(x) *' f(y).$$

Remarque 1.2.1

1. *Un morphisme de groupes bijectif est dit isomorphisme(de groupes) .Deux groupes sont dits isomorphes s'il existe un isomorphisme de G sur G' .*
2. *Si* f *est un isomorphisme, l'application réciproque* f^{-1} *est un isomorphisme.*
3. *Un morphisme d'un groupe* G *dans lui-même est appelé* endomorphisme .
4. *Un isomorphisme d'un groupe* G *dans lui-même est appelé* automorphisme *de* G.

Notation 1.2.1

On note $Hom(G, G')$ *l'ensemble des morphismes de groupes de* G *dans* G'. *On note* $End(G)$ *l'ensemble des morphismes de groupes de* G *dans lui-même, qu'on appelle endomorphismes de* G.

Proposition 1.2.1

Tout élément f *de* $Hom(G, G')$ *vérifie les propriétés suivantes :*

1. $f(1_G) = 1_{G'}$.

2. $f(x^{-1}) = f(x)^{-1}$ *pour tout élément* x *de* G.

3. $H < G \Rightarrow f(H) < G'$.

4. $H' < G' \Rightarrow f^{-1}(H') < G$ *avec* $f^{-1}(H') = \{x \in G \ , \ f(x) \in H'\}$.

Notation 1.2.2

Si deux groupes G *et* G' *sont isomorphes, on note* $G \simeq G'$. *Les éléments de* $End(G)$ *qui sont des isomorphismes sont appelés automorphismes de* G. *Ils forment un groupe pour la composition des applications, noté* $Aut(G)$.

Théorème 1.2.1 ***(de Cayley)***

Tout groupe G *est isomorphe à un sous-groupe du groupe* S_G *de ses permutations.*

Définition 1.2.2

Soit G *un groupe opérant sur un ensemble* E.

1. *Pour tout* g *dans* G, *l'application*

$$\begin{aligned} \gamma_g : E &\longrightarrow E \\ x &\longrightarrow g.x \end{aligned}$$

est une permutation de E.

2. *Soit* S_E *le groupe des permutations de* E, *l'application*

$$\begin{aligned} \gamma \ : G &\longrightarrow S_E \\ g &\longrightarrow \ \gamma_g \end{aligned}$$

est un morphisme de groupes.

Exemples 1.2.1

1. *Soient G, G' deux groupes et e' l'élément neutre de G'. L'application*

$$f : G \longrightarrow G'$$
$$x \longrightarrow e'$$

est un homomorphisme de groupes.

2. *Soit G un groupe noté multiplicativement et $a \in G$. L'application*

$$\Phi : Z \longrightarrow G$$
$$n \longrightarrow a^n$$

est un homomorphisme de groupes.

1.2.1 Le noyau et l'image d'un morphisme de groupe

Définition 1.2.3

Le noyeau d'un morphisme $\theta : G \rightarrow G'$ noté $Ker(\theta)$, est le sous-groupe de G formé de l'image inverse de e' par θ c-à-d :

$$Ker(\theta) = \theta^{-1}(e') = \{g \in G : \theta(g) = e'\}$$

D'autre part On considère aussi l'image d'un morphisme θ

$$\mathrm{Im}(\theta) = \theta(G) = \{\theta(x) : x \in G\}$$

$Im(\theta)$ est aussi un sous-groupe de G'.

Proposition 1.2.2

Si $\theta : G \to G'$ est un morphisme de groupe, alors

1. *Le noyau $Ker(\theta)$ est un sous-groupe de G.*

2. *θ est injective ssi $Ker(\theta) = \{e\}$.*

3. *θ est surjective ssi $Im(\theta) = G'$.*

Proposition 1.2.3

Soit $f : (G, *, e_G) \longrightarrow (H, \cdot\ , e_H)$ un morphisme de groupes

1. $Kerf$ est un sous-groupe normal de G.

2. Imf est un sous-groupe de H.

3. f est un monomorphisme si et seulement si $Kerf = \{e_G\}$.

4. f est un epimorphisme si et seulement si $Imf = H$.

Exemple 1.2.2

Soit $n \in \mathbb{N}^*$. On considérons l'application $f : \mathbb{Z} \longrightarrow \mathbb{C}^*$ définie par $f(K) = e^{2\pi ik/n}$ .C'est un morphisme du groupe $(\mathbb{Z}, +)$ dans le groupe $(\mathbb{C}^*, .)$ car pour tous $k, l \in \mathbb{Z}$,

$$f(k+l) = e^{2\pi i(k+l)/n} = e^{2\pi ik/n} e^{2\pi il/n} = f(k)f(l).$$

- *L'image de f est $Im(f) = \{e^{2\pi ik/n} \mid k \in \mathbb{Z}\} = \{e^{2\pi ik/n} \mid k = 0, 1, ..., n-1\} = U_n$.*
- *Le noyau de f est $Ker(f) = \{k \in \mathbb{Z} \mid f(k) = 1\} = \{k \in \mathbb{Z} \mid e^{2\pi ik/n} = 1\} = n\mathbb{Z}$.*

1.2.2 Automorphismes intérieurs

Soit G un groupe et $g \in G$. La fonction

$$\begin{aligned} \varphi_g : G &\to G \\ x &\longmapsto gxg^{-1} \end{aligned}$$

est un automorphisme de groupe appelé automorphisme intérieur de G. En effet,

1. φ_g est un endomorphisme : soit $x, y \in G$ alors

$$\varphi(xy) = gxyg^{-1} = gxeyg^{-1} = gx\left(g^{-1}g\right)yg^{-1} = \left(gxg^{-1}\right)\left(gyg^{-1}\right).$$

2. φ_g est inversible d'inverse $\left(\varphi_g\right)^{-1} = \varphi_{g^{-1}}$ pour $x \in G$ on a

$\varphi_{g^{-1}} \circ \varphi_g(x) = \varphi_{g^{-1}}(gxg^{-1}) = g^{-1}(gxg^{-1})(g^{-1})^{-1} = g^{-1}(gxg^{-1})g = x = g(g^{-1}xg)g^{-1} = \varphi_g \circ \varphi_{g^{-1}}(x)$

donc

$$\varphi_{g^{-1}} \circ \varphi_g = \varphi_g \circ \varphi_{g^{-1}} = Id_G$$

On note $Int(G)$ le groupe des automorphismes intérieurs de G.

Proposition 1.2.4

Soit G un groupe. Alors $Int(G) \leq Aut(G)$.

Proposition 1.2.5

Soit G et G' deux groupes.

1. *Si $\theta : G \longrightarrow G'$ est un morphisme de groupes bijectif, alors $\theta^{-1} : G' \longrightarrow G$ est aussi un morphisme de groupes bijectif.*

2. *$Aut(G)$ est l'ensemble des endomorphismes de G bijectifs.*

3. $Aut\,(G)$ est un sous-groupe de S_G.

Exemple 1.2.3

Soit G un groupe, $a \in G$. Alors l'application

$$\begin{aligned} \tau_a : G &\longrightarrow G \\ x &\longrightarrow axa^{-1} \end{aligned}$$

est un automorphisme de G appelé automorphisme intérieur. On a $\tau_e = Id_G$ et si G est commutatif, $\tau_a = Id_G$ $\forall a \in G$.

Centre d'un groupe

Définition 1.2.4

Si G un groupe, On appelle Centre du groupe l'ensemble des éléments qui commutent avec tous les autre : $Z(G) = \{\mathbf{x} \in G \ ; \ pour\ tout\ g\ de\ G,\ \mathbf{x}g = g\mathbf{x}\}$.

1.2.3 Groupe Diédrale $\mathbf{D}_n$

Définition 1.2.5

Le groupe diédral D_n est le groupe des isométries d'un plan qui preserve P_n .

Exemple 1.2.4

D_3 est le groupe des isométries du Triangle.

D_4 est le groupe des isométries du Carré.

D_5 est le groupe des isométries du pentagone.

D_6 est le groupe des isométries du l'hexagone.

• *Si $f \in D_4$ alors f doit être une permutation des sommets $A_0 = A_4, A_1, A_2, A_3$ Donc les seuls éléments de D_4 sont :Id ,la rotation r de centre O qui envoie A_0 sur A_1, la rotation*

r^2 de centre O qui envoie A_0 sur A_2, la rotation r^3 de centre O qui envoie A_0 sur A_3 On remarque que $r^4(A_0) = A_4 = A_0$ Donc $r^4 = Id$ mais aussi

S la symétré orthogonale d'axe OA_0.

t la symétré orthogonale d'axe la médiatrice à $[A_0, A_1]$.

S' la symétré orthogonale d'axe OA_0.

t' la symétré orthogonale d'axe la médiatrice à $[A_1, A_2]$.

On observe que $t = rs$, $s\prime = r^2 s$, $t\prime = r^3 s$ Donc $D_4 = \{Id$, $r, r^2, r^3, s, rs, r^2 s, r^3 s\}$ est d'ordre $2.4 = 8$.

Générateurs et Ordre de $\mathbf{D}_n$

Soit S la Symétrique orthogonal d'axe OA_0 et r la rotation de centre O et d'ongle $2\pi/n$ Donc $S(0) = 0$ et $S(A_i) = A_{n-i}$, pour tout $1 \leq i \leq n-1$ $r(A_i) = A_{i+1}$, pour tout $1 \leq i \leq n-1$, et $r(A_{n-i}) = A_0$. Donc s et r préservent P_n, d'où on a le.

Théorème 1.2.2

Soit $n \in \mathbb{N}$, $n \geq 3$, alors

1. *$s, r \in D_n$ de plus $ordre(s) = 2$, $ordre(r) = n$, et $srs = r^{-1}$*
2. *$D_4 = \langle r, s\rangle = \left\{r^k \text{ , } sr^k / 0 \leq k \leq n-1\right\}$ est un groupe d'ordre $2n$*

Démonstration.

1. La premier partie de la proposition est une conséquence de ce qui précède. Pour ce qui est de la deuxiéme partie : par définition, une symétrie vérifie $s^2 = Id$ et $s \neq Id$ Donc $ordre(s) = 2$ de plus puisque $r^n(A_i) = A_i r^n$ $(n \geq 3)$ fixe au moins trois points du plan, donc $r^n = Id$ et $r, r^2, r^3, ..., r^{n-1} \neq Id$. Donc $ordre(r) = n$ (le fait qu'unne rotation d'angle $2\pi/n$ est d'ordre m est un resultat bien connu et

que l'onvient de rédémontrer). Maintenant : en posant $A_n = A_0$ on a $rsrs(A_i) = rsr(A_i) = rs(A_{n-i+1}) = r(A_{i-1}) = A_i$ Ainsi $rsrs$ fixe plus de trois points du plan, Donc $rsrs = Id$. D'où la relation $srsr = Id$.

2. Les seules isométries qui préservent p_n sont :

   (i) Les rotation d'angle $2\pi/n$, c'est -à-dire, les $r^k(Id = r^0)$

   (ii) Les symétries d'axe OA_k et celles passant par les médiatrices des segments $[A_i, A_{i+1}]$ (qui peuvent être les mêmes, selon que si n est pair ou impair) : c'est à dire les sr^{n-k} D'où le resultat.

■

1.2.4 Groupes monogènes et cycliques

Définition 1.2.6

Un groupe G est dit monogène s'il est engendré par l'un de ses éléments Autrement dit , $\exists a \in G$ tel que : $G = \langle a \rangle$.

Définition 1.2.7

Un groupe G est dit cyclique s'il est monogène et fini .

Proposition 1.2.6

- *Tout groupe monogène est abélien .*
- *Tout sous groupe d'un groupe cyclique est cyclique .*

Exemples 1.2.5

1. *Soient $n \in \mathbb{Z}$ et $S = \{n\}$ un singleton de $\mathbb{Z}$. Alors $\langle n \rangle = n\mathbb{Z}$, donc n engendre $n\mathbb{Z}$, et $n\mathbb{Z}$ est un groupe monogène engendre par n. En particulier, $\mathbb{Z} = \langle 1 \rangle$.*

2. *Soit* $n \in \mathbb{N}^*$, *Alors* $U_n = \{e^{2\pi ik/n} \ / k = 0, ..., n-1\}$ *est un groupe cyclique (car* $e^{2\pi ik/n} = (e^{2\pi i/n})^k$ *) engendre par* $e^{2\pi ik/n}$.

3. *Soit* $n \in \mathbb{N}^*$, $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ *est un groupe cyclique d'ordre* n *engendré par* $\overline{1} : \overline{0} = 0.\overline{1}$, $\overline{1} = 1.\overline{1}$, $\overline{2} = \overline{1} + \overline{1} = 2.\overline{1}$, ... , $\overline{n-1} = (n-1).\overline{1}$.

Théorème 1.2.3

Soit $G = \langle x \rangle$ *un groupe monogène, alors*

1. *Si* G *est infini alors* $G \simeq (\mathbb{Z}, +)$.

2. *Si* G *est d'ordre fini, alors* $G \simeq (\mathbb{Z}/n\mathbb{Z}, +)$.

Chapitre 2

Etude sur les automorphismes de groupe

2.1 Les trois théorèmes d'isomorphismes

Les ≪ *théorèmes d'isomorphisme* ≫ ont pour but de décrire la structure et les propriétés générales des morphismes de groupes. Ils en donnent des décompositions canoniques.
Dans une terminologie moderne, on dit de l'énoncé suivant qui est la propriété universelle du quotient de groupes.

Théorème 2.1.1 ***(Premier théorème d'isomorphisme)***
Soit G un groupe, $N \lhd G$ et $\pi : G \longrightarrow G/N$ la surjection canonique. Si $\theta : G \longrightarrow G'$ est un morphisme de groupes tel que $N \subseteq \ker(\theta)$, alors il existe un unique morphisme

$$\varphi : G/N \longrightarrow G'$$

tel que $\theta = \varphi \circ \pi$. De plus

1. *si $N = \ker(\theta)$ alors φ est un monomorphisme.*

2. si θ est un épimorphisme, alors φ l'est aussi.

Plus spécifiquement, si θ est un épimorphisme, et $N = ker(\theta)$, alors φ est un isomorphisme.

On peut formuler ce résultat en terme du diagramme commutatif suivant :

$$\begin{array}{ccc} & \theta & \\ G & \longrightarrow & G' \\ \pi \downarrow & \nearrow \exists!\varphi & \\ G/N & & \end{array}$$

On déduit immédiatement le résultat suivant.

Corollaire 2.1.1

Si $\theta : G \longrightarrow G'$ est un morphisme de groupes, alors

$$G/ker(\ \theta) \simeq Im(\ \theta)$$

En particulier, si G est fini on a : $|G| = |ker(\ \theta)| \cdot |Im(\ \theta)|$.

Démonstration. (*demonstration de Premier théorème d'isomorphisme*)

• Pour l'existence, on débute en montrant que la fonction $\varphi : G/N \longrightarrow G'$, définie par $\varphi(xN) = \theta(x)$, est bien définie. Autrement dit, si $xN = yN$ alors on veut vérifier que $\theta(x) = \theta(y)$ Or, l'hypothèse implique que $x^{-1}yN = N$ et donc $x^{-1}y \in N \subseteq ker(\theta)$.

Il s'ensuit que $\theta(x^{-1}y) = e$.

Puisque θ est un morphisme, il en découle que $\theta^{-1}(x)\,\theta(y) = e$, et donc que $\theta(x) = \theta(y)$.

La fonction φ est donc bien définie.

Pour le reste de l'énoncé du théorème, on montre d'abord que φ est un morphisme de groupes.

En effet, pourxN , $x'N \in G/N$ on constate que

$\varphi(xN.x'N) = \varphi(xx'N) = \varphi \circ \pi(xx') = \theta(xx') = \theta(x)\,\theta(x') = \varphi \circ \pi(x)\,\varphi \circ \pi(x') = \varphi(xN)\,\varphi(x'N)$.

Maintenant, si pour tout $y \in G'$ on a $x \in G$ tel que $\theta(x) = y$ (est un épimorphisme), alors $\varphi(xN) = \varphi \circ \pi(x) = \theta(x)$ et donc φ est un épimorphisme.

D'autre part, lorsque $N = ker(\theta)$, on a $ker(\varphi) = N$.

En effet, si $\varphi(xN) = e$ alors $\theta(x) = e$ et donc $x \in N$, mais alors $x \in N$ et $xN = N$.

On en conclut que φ est bien un monomorphisme.

• L'unicité de φ se vérifie comme suit. Soit φ et φ', tels que : $\theta = \varphi \circ \pi = \varphi' \circ \pi$. Pour $x \in G$ on a : $\theta(x) = \varphi \circ \pi(x) = \varphi' \circ \pi(x)$ donc $\varphi(\pi(x)) = \varphi'(\pi(x))$.

Donc pour $xN \in G/N$ on a $\varphi(xN) = \varphi'(xN)$ et donc $\varphi = \varphi'$ ■

Exemples 2.1.1

1. *On a* $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$ *En effet, on observe d'abord que* $\mathbb{R} \lhd \mathbb{C}$*, car* $(\mathbb{R}, +)$ *est abélien.*

   De plus, on a un épimorphisme de groupes

   $$\theta : \mathbb{C} \longrightarrow \mathbb{R}$$

   défini par $\theta(a + ib) = b$*. Son noyau est* $ker(\theta) = \mathbb{R}$

   En vertu du théorème d'isomorphisme, il existe donc un unique isomorphisme

   $$\varphi : \mathbb{C}\ /\mathbb{R} \longrightarrow \mathbb{R}$$

   tel que $\theta = \varphi \circ \pi$*, comme annoncé.*

2. *L'application*

   $$f : (R^*, \times) \longrightarrow (R^*, +)$$
   $$x \longrightarrow |x|$$

est un homomorphisme des groupes. Alors, puisque $ker f = \{-1, 1\}$ *et* $Im f = R_+^*$, $R^*/\{-1, 1\} \simeq R_+^*$.

3. *On pose* $G = (\mathbb{Z}\ ,\ +)$ *et* $G' = \langle i \rangle = (\{1\ ,\ -1\ ,\ i\ \ ,-i\}\ ,\ \times) \leq (\mathbb{C}^*\ ,\ \times)$ *alors*

$$\theta : (\mathbb{Z}\ ,+) \longrightarrow (\{1\ ,-1\ ,\ i\ \ ,-i\}\ ,\times)$$

défini par :

$$\theta\,(n) = i^n$$

θ *est surjectif et* $ker\,(\theta) = 4\mathbb{Z}$

alors en applice le premier théoréme d'isomorphisme

$$G/ker\,(\ \ \theta) \simeq Im\,(\ \ \theta) \iff \mathbb{Z}/4\mathbb{Z} \approxeq \{1\ ,-1\ ,\ i\ \ ,-i\}$$

Lemme 2.1.1

Soit H *un sous-groupe de* G *et* N *un sous-groupe normal d'un groupe* G *.Alors ,*

$$\langle H \cup N \rangle = HN = NH.$$

Théorème 2.1.2 ***(Deuxieme théoréme d'isomorphisme).***

Soient H *un sous-groupe et* N *un sous-groupe normal d'un groupe* G*. Alors ,*

1. N *est un sous-groupe normal de* HN.
2. $H \cap N$ *est un sous-groupe normal de* H.
3. $H/(N \cap H) \cong HN/N$.
4. *si* G *est en outre fini, alors* $|HN| = \frac{|H||N|}{|H \cap N|}$.

Démonstration.

(1.) Grâce au Lemme précédent on sait que $HN = \langle H \cup N \rangle$ est un sous-groupe de G qui contient N.Comme N est un sous-groupe normal de G, N est clairement un sous-groupe normal de HN.

(2.) On considère l'application

$$f : H \longrightarrow HN/N,\ f(h) = hN \tag{2.1.1}$$

Vérifions que f est un homomorphisme de groupes .Pour

$$h_1, h_2 \in H, f(h_1)f(h_2) = (h_1N)(h_2N) = (h_1h_2)N = f(h_1h_2)$$

En outre ,$h \in Kerf$ ssi $hN = N$, c'est-à-dire $h \in N$.

Donc $Kerf = N \cap H$ et en particulier, $N \cap H$ est sous-groupe normale de H.

(3.) Considérons de nouveau le morphisme (2.1.1) Comme pour tous $h \in H$ et $n \in N$,

$$hnN = hN$$

il suit que f est surjective.

Le premier théorème d'isomorphisme nous dit alors que $H/(N \cap H) \cong HN/N$.

(4.) Du point (3.) on déduit que

$$[H : (H \cap N)] = [HN : N]$$

Alors

$$\frac{\mid H \mid}{\mid H \cap N \mid} = \frac{\mid HN \mid}{\mid N \mid}$$

et dés lors

$$\mid HN \mid = \frac{\mid H \mid\mid N \mid}{\mid H \cap N \mid}.$$

■

Exemple 2.1.2

Considérons le groupe additif $G = Z$, $H = 9Z$ *et* $K = 12Z$. *Alors,* $H + K = 3Z$, $H \cap K = 36Z$ *et ainsi* $(9Z)/(36Z) \simeq (3Z)/(12Z)$.

Théorème 2.1.3 ***(Troisieme théoréme d'isomorphisme).***

Soient H *et* N *des sous groupes normaux d'un groupe* G *avec* $N \leq H$, *alors*

1. H/N est un sous-groupe normal de G/N
2. $(G/N)/(H/N) \cong G/H$

Démonstration.

(a) Définissons une application

$$\psi : G/N \longrightarrow G/H \quad \psi(gN) = gH$$

On peut facilement vérifier que est bien défini et est un épimorphisme de groupes.

En outre, $gN \in Ker\psi$ ssi $\psi(gN) = gH = H$ c'est- a-dire $g \in H$. Donc $Ker\psi = \{gN \ / \ g \in H\} = H/N$ et en particulier H/N est un sous-groupe normal de G/N.

(b) Si on applique le premier théoréme d'isomorphisme au morphisme on obtient immédiament $(G/N)/(H/N) \cong G/H$.

■

Exemple 2.1.3

$$\textit{Soient } H = 2\mathbb{Z},\ N = 4\mathbb{Z}\ ,\ \textit{on a} \begin{cases} 2\mathbb{Z} \lhd \mathbb{Z} \\ 4\mathbb{Z} \lhd \mathbb{Z} \\ 4\mathbb{Z} \leq 2\mathbb{Z} \end{cases}$$

$$\begin{cases} 2\mathbb{Z}/4\mathbb{Z} \lhd \mathbb{Z}/4\mathbb{Z} \\ (\mathbb{Z}/4\mathbb{Z})/(2\mathbb{Z}/4\mathbb{Z}) \ \simeq\ \mathbb{Z}/2\mathbb{Z} \end{cases}$$

2.2 les automorphismes d'un groupe cyclique

Cette section sera consacrée à du résultat suivant :

Etant donné un groupe cyclique G, le groupe des automorphismes de G est isomorphe au groupe $G^{\times}$ des éléments générateurs de G où $G^{\times} = \left\{g^k : p\gcd(k,n) = 1\right\}$. En d'autres mots $Aut(G) \ \simeq\ G^{\times}$

Un automorphisme d'une groupe G est un morphisme bijectif de G vers G. L'ensemble des automorphismes d'un groupe G, note $Aut(G)$, muni de la composition des applications, i.e $(Aut(G), \circ)$ est un groupe.

La proposition suivante montre que les automorphismes de $\mathbb{Z}/n\mathbb{Z}$ sont de la forme

$$f_{\overline{m}}(\overline{x}) = \overline{mx}$$

avec $\overline{m} \in (\mathbb{Z}/n\mathbb{Z}\ )^{\times}$ et $\overline{x} \in \mathbb{Z}/n\mathbb{Z}$.

Proposition 2.2.1

Soit $n \in \mathbb{N}^*$,

1. *Pour tout* $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, *l'application* $f_{\overline{m}} : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ *definie par :* $\overline{x} \longmapsto \overline{mx}$ *est un automorphisme de* $\mathbb{Z}/n\mathbb{Z}$.

2. *L'application* $\Psi : Aut(\mathbb{Z}/n\mathbb{Z}) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^{\times}$ *definie par :* $f \longmapsto \Psi(f) = f\left(\overline{1}\right)$ *est un isomorphisme de groupes.*

Démonstration.

1. L'application $f_{\overline{m}}$ est un homomorphise. En effet, pour $\overline{x}, \overline{y} \in \mathbb{Z}/n\mathbb{Z}$ on a :

$$f_{\overline{m}}(\overline{x}+\overline{y}) = \overline{m}\ (\overline{x}+\overline{y}) = \overline{mx}+\overline{my} = f_{\overline{m}}(\overline{x}) + f_{\overline{m}}(\overline{y})$$

   Montrons que $f_{\overline{m}}$ est sujectif, soit $\overline{y} \in \mathbb{Z}/n\mathbb{Z}$, l'equation $\overline{y} = f_{\overline{m}}(\overline{x})$ est équivalente à $\overline{y} = \overline{mx}$, comme $\overline{m} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, il existe donc $(\overline{m})^{-1} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, dit l'inverse de $\overline{m}$, et on a $(\overline{m})^{-1}\overline{y} = (\overline{m})^{-1}\overline{mx}$ et par suite $\overline{x} = (\overline{m})^{-1}\overline{y}$, ce qui montre que $f_{\overline{m}}$ est bien surjective. Comme $f_{\overline{m}} : \mathbb{Z}/n\mathbb{Z} \longmapsto \mathbb{Z}/n\mathbb{Z}$ est surjectif et $\mathbb{Z}/n\mathbb{Z}$ et de cardinal fini, alors $f_{\overline{m}}$ est bien injectif, et par conséquent $f_{\overline{m}}$ est un élément du groupe $(Aut(\mathbb{Z}/n\mathbb{Z}), \circ)$.

2. Il est clair que si $f \in Aut(\mathbb{Z}/n\mathbb{Z}.)$, alors $f\left(\overline{1}\right)$ est un élément générateur de $\mathbb{Z}/n\mathbb{Z}$. En effet, comme f est surjectif et $\mathbb{Z}/n\mathbb{Z} = \langle\overline{1}\rangle$ alors $f\left(\overline{1}\right) \in (\mathbb{Z}/n\mathbb{Z})^{\times}$.Vérifions tout d'abord que Ψ est un morphisme de groupe. Soit $f, g \in Aut(\mathbb{Z}/n\mathbb{Z})$, on montre qu'on a $\Psi(f \circ g) = \Psi(f) \cdot \Psi(g)$ ce qui équivalent à dire $(f \circ g)\left(\overline{1}\right) = f\left(\overline{1}\right) \cdot g\left(\overline{1}\right)$.

   On a $(f \circ g)\left(\overline{1}\right) = f\left(g\left(\overline{1}\right)\right)$, avec $g\left(\overline{1}\right) \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, alors $\exists 1 \leq k \leq n-1$ tel que:

$pgcd\,(k,n)=1$ et $g\left(\overline{1}\right)=\overline{k}$. Donc

$$f\ \left(g\left(\overline{1}\right)\right)=f\left(\overline{k}\right)=f\ \left(\overline{1}+\overline{1}+...+\overline{1}\right)=k\ f\ \left(\overline{1}\right)=f\ \left(\overline{1}\right)\cdot g\left(\overline{1}\right)$$

Par conséquent, l'application Ψ est un morphisme de groupe.

Montrons que $ker\Psi=\left\{id_{\mathbb{Z}/n\mathbb{Z}}\right\}$ ce qui permet d'assurer que Ψ est injectif.

On a : $ker\Psi=\left\{f\in Aut\,(\mathbb{Z}/n\mathbb{Z}):\Psi\,(f)=\overline{1}\right\}=\left\{f\in Aut\,(\mathbb{Z}/n\mathbb{Z}.):f\ \left(\overline{1}\right)=\overline{1}\right\}$,

comme $f\in Aut\,(\mathbb{Z}/n\mathbb{Z})$ et $f\ \left(\overline{1}\right)=\overline{1}$, alors pour tout $\overline{t}\in\mathbb{Z}/n\mathbb{Z}$, on a :

$$f\ \left(\overline{t}\right)=f\ \left(\underbrace{\overline{1}+\overline{1}+...+\overline{1}}_{t\ fois}\right)=tf\ \left(\overline{1}\right)=t\cdot\overline{1}=\overline{t}.$$

Donc $f\ \left(\overline{1}\right)=\overline{1}\Longleftrightarrow f=id_{\mathbb{Z}/n\mathbb{Z}}$. Et par suite, $ker\ \Psi=\left\{id_{\mathbb{Z}/n\mathbb{Z}}\right\}$.

Enfin, l'application Ψ est surjectif car pour tout $\overline{m}\in(\mathbb{Z}/n\mathbb{Z}\ )^{\times}$, $\exists f_{\ \overline{m}}\in Aut\,(\mathbb{Z}/n\mathbb{Z})$, avec $\Psi\,(f_{\overline{m}})=f_{\ \overline{m}}\left(\overline{1}\right)=\overline{m}\ \cdot\overline{1}=\overline{m}$.

Finalement , on a bien $(\mathbb{Z}/n\mathbb{Z}\ )^{\times}\simeq Aut\,(\mathbb{Z}/n\mathbb{Z}.)$.

■

Exemple 2.2.1

Pour $n=6$, on a $(\mathbb{Z}/n\mathbb{Z}\ )^{\times}=\left\{\overline{1},\overline{5}\right\}$, dont la table de Cayley du groupe est décrite ci-contre:

.	$\overline{1}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{1}$

On a dans ce cas $Aut\,(\mathbb{Z}/6\mathbb{Z})=\{f_{\overline{1}}\ ,\ f_{\overline{5}}\}$, avec $f_{\overline{1}}=\left(\begin{smallmatrix}\overline{0}&\overline{1}&\overline{2}&\overline{3}&\overline{4}&\overline{5}\\ \overline{0}&\overline{1}&\overline{2}&\overline{3}&\overline{4}&\overline{5}\end{smallmatrix}\right)$

et $f_{\overline{5}} = \begin{pmatrix} \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\ \overline{0} & \overline{5} & \overline{4} & \overline{3} & \overline{2} & \overline{1} \end{pmatrix}$

Le groupe $Aut\,(\mathbb{Z}/6\mathbb{Z}\ , \circ)$ dont la table est

$\circ$	$f_{\overline{1}}$	$f_{\overline{5}}$
$f_{\overline{1}}$	$f_{\overline{1}}$	$f_{\overline{5}}$
$f_{\overline{5}}$	$f_{\overline{5}}$	$f_{\overline{1}}$

est idetique à celle à du groupe $\left((\mathbb{Z}/n\mathbb{Z}\ )^{\times}\ , \cdot\right)$ ce qui montre que ces deux groupes sont bien isomorphes.

A présent, on montre que si $G = \langle g \rangle$ est un groupe cyclique d'ordre n, alors l'ensemble $G^{\times}$ des éléments générateurs de G muni de l'opération $*$ définie ci-dessous dans la proposition suivant a une structure de groupe commutatif d'élément neutre le générateur g.

Proposition 2.2.2

Soient G un groupe cyclique d'ordre n, d'élément neutre noté 1_G, et g un générateur de G, l'ensemble $G^{\times}$ des éléments générateurs de G muni de l'opération $*$ définie par :

$$\forall g^k, g^{k'} \in G^{\times} : g^k * g^{k'} = g^{kk'}$$

avec $k, k' \in \{1, ..., n-1\}$, $pgcd(k, n) = 1$, $pgcd(k', n) = 1$, est un groupe commutatif.

Exemple 2.2.2

Soit G un groupe cyclique d'ordre 6, donc $G = \{1_G, g, g^2, g^3, g^4, g^5\}$ et $G^{\times} = \{g, g^5\}$, dont la table de cayley du groupe $(G^{\times}, *)$ est décrite ci-contre :

$*$	g	g^5
g	g	g^5
g^5	g^5	g

On a par exemple $g^5 * g^5 = g^{25} = g^{4\times 6+1} = (g^6)^4.g^1 = 1_G.g^1 = g$.

Proposition 2.2.3

Soit G un groupe cyclique d'ordre $n \in \mathbb{N}^*$ de générateur g.

1. *Pour tout $g^K \in G^\times$, l'application $f_{g^k} : G \longrightarrow G$, définie par : $g^t \longmapsto g^{kt}$, avec $0 \leq t \leq n-1$ est un automorphisme de G.*

2. *L'application $\Psi : Aut(G) \longrightarrow (G)^\times$, définie par $f \longmapsto \Psi(f) = f(g)$, est un isomorphisme de groupes.*

Démonstration.

1. L'application f_{g^k} est un homomorphisme. En effet, pour $g^t, g^{t'} \in G$,on a :

$$f_{g^k}(g^t g^{t'}) = f_{g^k}(g^{t+t'}) = g^{k(t+t')} = g^{kt+kt'} = g^{kt}.g^{kt'} = f_{g^k}(g^t).f_{g^k}(g^{t'}).$$

   Montrons que f_{g^k} est injectif : soit $(g^t, g^{t'}) \in G^2$, alors

   $f_{g^k}(g^t) = f_{g^k}(g^{t'}) \iff g^{kt} = g^{kt'} \iff g^{k(t-t')} = 1_G \iff n$ divise $k(t-t')$,

   Ona $\begin{cases} n \text{ divise } K(t-t') \\ pgcd(k,n) = 1 \end{cases}$ d'aprés le lemme de Gausse, alors n divise $t-t'$, donc $\exists q \in \mathbb{Z} : t - t' = qn$.

   Et comme $1 \leq t \leq n-1$ et $1 \leq t' \leq n-1$, alors $t - t' = 0$, *donc* $t = t'$.Comme $f_{g^k} : G \longrightarrow G$ est injectif et G est de cardinal fini, alors f_{g^k} est surjectif, et par conséquent f_{g^k} est un élément du groupe $(Aut(G), \circ)$.

2. L'application Ψ est bien définie car si $f \in Aut(G)$, alors $f(g)$ est un élément de $G^\times$ de sorte que $f(g)$ est un générateur de $(G, .)$.

   De plus si $f, h \in Aut(G)$ avec $f = g$, on a donc $f(g^t) = h(g^t)$ pour tout $t \in \{0, 1, ..., n-1\}$ en particulier $f(g) = h(g)$ ce qui montre qu'on bien $\Psi(f) = \Psi(h)$.

L'application Ψ est un morphisme, en effet, soit $f, h \in Aut(G)$, avec $f(g) = g^{k'}$, $h(g) = g^k$ et $g^{k'}$, g^k appartient à $G^\times$.

On a $(f \circ h)(g) = f(h(g)) = f(g^k) = (f(g))^k = (g^{k'})^k = g^{kk'} = g^{k'} * g^k = f(g) * h(g)$ ce qui montre $\Psi(f \circ h) = \Psi(f) * \Psi(h)$.

Montrons que $Ker\Psi = \{id_G\}$ ce qui permet d'assurer que Ψ est injectif.

On a $Ker\Psi = \{f \in Aut(G) : \Psi(f) = g\} = \{f \in Aut(G) : f(g) = g\}$, comme $f \in Aut(G)$ et $f(g) = g$, alors pour tout $1 \leq t \leq n-1$, $f(g^t) = f(g.g.....g) = (f(g))^t = g^t$.

Donc $f(g) = g \iff f = id_G$. Et $Ker\Psi = \{id_G\}$, par conséquent Ψ est injectif.

L'application Ψ est surjectif, car pour tout $g^k \in (G)^\times, \exists f_{g^k} \in Aut(G)$

Avec $\Psi(f_{g^k}) = f_{g^k}(g) = g^k$.

Finalement $(G)^\times \simeq Aut(G)$.

■

Exemple 2.2.3

Soit G un groupe cyclique d'ordre 5, donc $G = \{1_G, g, g^2, g^3, g^4\}$ et $G^\times = \{g, g^2, g^3, g^4\}$. Le groupe $(G^\times, *)$ dont la table est

$*$	g	g^2	g^3	g^4
g	g	g^2	g^3	g^4
g^2	g^2	g^4	g	g^3
g^3	g^3	g	g^4	g^2
g^4	g^4	g^3	g^2	g

Dans ce cas $Aut(G) = \{f_g, f_{g^2}, f_{g^3}, f_{g^4}\}$, avec

$$f_g = \begin{pmatrix} 1_G & g & g^2 & g^3 & g^4 \\ 1_G & g & g^2 & g^3 & g^4 \end{pmatrix}, \; f_{g^2} = \begin{pmatrix} 1_G & g & g^2 & g^3 & g^4 \\ 1_G & g^2 & g^4 & g & g^3 \end{pmatrix},$$

$$f_{g^3} = \begin{pmatrix} 1_G & g & g^2 & g^3 & g^4 \\ 1_G & g^3 & g & g^4 & g^2 \end{pmatrix} \text{ et } f_{g^4} = \begin{pmatrix} 1_G & g & g^2 & g^3 & g^4 \\ 1_G & g^4 & g^3 & g^2 & g \end{pmatrix}.$$

Le groupe $(Aut(G), \circ)$ *dont la table est*

$*$	f_g	f_{g^2}	f_{g^3}	f_{g^4}
f_g	f_g	f_{g^2}	f_{g^3}	f_{g^4}
f_{g^2}	f_{g^2}	f_{g^4}	f_g	f_{g^3}
f_{g^3}	f_{g^3}	f_g	f_{g^4}	f_{g^2}
f_{g^4}	f_{g^4}	f_{g^3}	f_{g^2}	f_g

Chapitre 3

codes à groupe

Monoide

Définition 3.0.1

Un monoïde est un ensemble M muni d'une loi interne, i.e. d'une application

$$T : M \times M \longrightarrow M$$

qui satisfait aux conditions suivantes :

- *L'opération T est associative : $\forall x, y, z \in M$: $(xTy)Tz = xT(yTz)$.*
- *Il existe un neutre (unique) $e \in M$ tel que $\forall x \in M : xTe = eTx = x$.*

Remarque 3.0.1

Un monoïde (M, T, e) qui est tel que tout élément de M possède un inverse est un groupe.

Exemple 3.0.4

Tout groupe est un monoïde ; $(N, +, 0)$ est un monoïde qui n'est pas un groupe.

Définition 3.0.2

Soit un monoïde $M = (M\ ,.,\ e\ )$. Un sous-monoïde de M est un triplet $M' = (\ M',\ .,\ e')$ tel que :

1. $M' \subseteq M$.

2. $e = e'$.

3. $\forall\ m, m' \in M' : m\ .m' \in M'$.

▶ *Soit* I *est ensemble d'indices et si* $\forall\ i \in I$, $M_i = (M_i, ., e)$ *est un sous-monoïde de* M , *alors* $(\cap_{i\in I}\ M_i, ., e)$ *est un sous-monoïde de M.*

▶ *Soit* Y *une partie d'un monoïde* M . *On appelle sous-monoïde engendré par* Y , *le plus petit sous-monoïde de* M *contenant* Y , *on le note* Y^* *D'après ce qui précède* , Y^* *est l'intersection de tous les sous-monoïdes de* M *qui contiennent* Y .

Exemple 3.0.5

Soit $N = (\mathbb{N}, +, 0)$ *Soit A l'ensemble des nombres pairs et B l'ensemble des nombres impairs.* $(A, +, 0)$ *est le sous-monoïde de* N *engendré par* $\{2\}$ *tandis que* $(B, +, 0)$ *n'est pas un sous-monoïde de* N .

Définition 3.0.3

Soit M *et* N *deux monoïdes, un morphisme de* M *dans* N *est une application*

$$\mu : M \longrightarrow N$$

qui vérifie :

▶ $\mu\ (1_M) = 1_N$.

▶ $\mu\ (xy) = \mu\ (x)\mu(y)$, *pour tous éléments* x *et* y *de* M.

Exemple 3.0.6

L'application

$$n \longmapsto 2^n$$

est un homomorphisme de $(\mathbb{N}\ , +, 0)$ *dans* $(\mathbb{N}\ , \times, 1)$.

Définition 3.0.4

1. *Soit* M *un sous monoïde de* A^*

▶ M *est libérable ssi*

$$(\forall\ m_1 \in M\ ,\ \forall\ m_2 \in M,\ \forall\ w \in A^* : (m_1 w \in M \ \text{ et } \ w m_2 \in M \implies w \in M))$$

▶ M *est unitaire à droite ssi*

$$(\forall\ m \in M\ ,\ \forall\ w \in A^* : mw \in M \implies w \in M)$$

▶ M *est unitaire à gauche ssi*

$$(\forall\ m \in M\ ,\ \forall\ w \in A^* : wm \in M \implies w \in M)$$

▶ *M est biunitaire si il est unitaire à droite et à gauche.*

2. *Soit M une partie de* A^*

▶ *Un mot* $w \in A^*$ *est complétable dans* M *s'il existe* $u, v \in A^*$ *tel que* $uwv \in M$.

▶ *On dit que* w *est incomplétable dans* M *s'il n'est pas complétable.*

▶ *On dit que* M *est complet si tout mot de* A^* *est complétable dans* M *; sinon on dit que* M *est coupant.*

▶ *Les notions de copmlétude à droite ou à gauche sont évidents.*

Mots et Langages

Définition 3.0.5

Un alphabet est un ensemble fini. Un alphabet sera en général désigné par une lettre grecque majuscule.

Ainsi $A = \{a, b, c, d\}, \triangle = \{\bigstar, \emptyset, \heartsuit, \measuredangle\}, \Omega = \{0, 1\}$ *sont des alpha-bets.*

Les éléments d'un alphabet sont appelés lettres ou symboles.

Exemple 3.0.7

Le biologiste intéressé par l'étude de l'ADN utilisera un alphabet à quatre lettres $\{A, C, G, T\}$ *pour les quatre constituants des gènes : Adénine, Cytosine, Guanine et Thy-mine.*

Définition 3.0.6

Soit A un alphabet. Un mot sur A est une suite finie de symbole. Par exemple, abcabb et aabc sont deux mots sur l'alphabet $\{a, b, c\}$*. La longueur d'un mot w est le nombre de symboles constituant ce mot, on la not* $\mid w \mid$*.*

Ainsi, $\mid abcabb \mid = 6$ *et* $\mid aabc \mid = 4$ *. L'unique mot de longueur* 0 *est le mot correspondant à la suite vide. Ce mot s'appelle le mot vide et on la note* 1*, ou bien* ϵ*.*

L'ensemble des mots sur A est noté A^**. par exemple,*

$\{0, 1, 2\}^* = \{\epsilon, 0, 1, 2, 00, 01, 02, 10, 11, 12, 20, 21, 22, 000, 001, ...\}$*(* ϵ *est le mot vide).*

Définition 3.0.7

Si a est une lettre de l'alphabet A, pour tout mot $w = a_1 a_2 ... a_K \in A^*$*; on note par :* $\mid w \mid_a = card\{i \in \{1, 2, ..., k\} : a_i = a\}$*. Par exemple* $\mid abcabb \mid_a = 2$ *et* $\mid aabc \mid_c = 1$*.*

- *Fonction de parikh : Soit un alphabet A de cardinal* $n \geq 1$*, et ordonné* ($A = \{a_1, a_2, ..., a_n\}$*, avec* $a_1 \leq a_2 \leq ... \leq a_n$*).*

  On définit alors la fonction de parikh $\Psi : A^* \longrightarrow \mathbb{N}^n$ *par*

$$\Psi(w) = (\mid w \mid_{a_1}, ..., \mid w \mid_{a_n}).$$

Le n-uple $\Psi(w)$ est appelé vécteur de parikh de w, il est claire que si $n \geq 2$, alors Ψ n'est pas injectif.

On appelle image miroir d'un mot $w = a_1a_2...a_k$ le mot $\widetilde{w} = a_k...a_1$.

Définition 3.0.8

Soit $w = a_1a_2...a_k$ un mot sur A, les mots :

$$1, a_1, a_1a_2, ..., a_1a_2...a_{k-1}, a_1a_2...a_k = w$$

sont les préfixes de w. Un préfixe de w différent de 1 et w est dit propre.
De façon semblable

$$1, a_k, a_{k-1}a_k, ..., a_2...a_k, a_1a_2...a_k = w,$$

sont les suffixes de w. Un suffixe de w qualifié de propre s'il diffère de 1 et de w. Soient $1 \leq i \leq j \leq k$, le mot $a_i...a_j$ est un facteur du mot w, on parle de facteur propre lorsque ce dernier diffère de w et de 1, l'ensemble des préfixes (resp. suffixes, facteurs) de w est noté Pref(w)(resp. Suff(w), Fac(w)).

Définition 3.0.9

Un langage sur A est simplement un ensemble (fini ou infini) de mots sur A. En d'autres termes, un langage est une partie deA^*. On distingue en particulier le langage vide $\emptyset$; qui ne contient aucun mot.

Exemple 3.0.8

Considérons l'alphabet $A = \{a, b, c\}$ l'ensemble $\{b; ab; aa; babba\}$ est un langage fini.
L'ensemble L_{2a} des mots sur A comprenant un nombre paire de a est aussi un langage ($infini$), $L_{2a} = \{ 1, b, c, aa, bb, bc, cb, cc, aab, aac, aba, aca, ..., abaacaaa, ...\}$.

Définition 3.0.10

Soient $L, M \subseteq A^*$, deux langages. La concaténation des langages L et M est le langage,

$$LM = \{uv : u \in L, v \in M\}$$

En particulier, on peut définir la puissance n-iéme d'un langage L, $n > 0$, par :

$$L^n = \{w_1...w_n : \forall i \in \{1, ..., n\}, w_i \in L\}$$

Et on pose $L^0 = \{1\}$.

3.1 Code à longueurs variables

Les codes sont les bases des sous-monoïdes libres, ce sont les ensembles de mots qui conduisent à un décodage unique.

Définition 3.1.1

On dit qu'un mot $u \in A^*$ est facteur de $w \in A^*$ s'il existe deux mots $f, g \in A^*$ tel que $w = fug$. Si $f = 1$($resp$.$g = 1$) on dit que u est facteur gauche ($préfixe$) ($resp$.$droite$ ($suffixe$)) de w.

• *Le mot u est un facteur ($resp$. $facteur\ gauche$, $facteur\ droite$) propre si $u \neq w$.*

Exemple 3.1.1

Soit l'alphbet $A = \{a, b, c\}$ et le mot $w = aabc$, alors ab est un facteur de w , mais ac ne l'est pas ; le mot aa est un préfixe de w et abc est un suffixe de w.

Définition 3.1.2

Une partie X de A^* est préfixe ($resp$. $suffixe$) si aucun facteur gauche ($resp$.$droite$) propre d'un mot de X n'est dans X , en symboles :

$XA^+ \cap X = \emptyset$ *ou* $X^{-1}X = \{1\}$ $resp(A^+X \cap X = \emptyset$ *ou* $XX^{-1} = \{1\})$:

- *X est bipréfixe s'il est à la fois préfixe et suffixe.*

Définition 3.1.3

Une partie X *de* A^* *est un code ssi tout mot de* X^+ *admet une unique factorisation en mots de* X*. Autrement dit, toute relation :*

$$x_1x_2x_3...x_n = x\prime_1x'_2x'_3...x'_m \left(x_i \ , \ x'_j \in X\right)$$

entraine $n = m$ *et* $x_i = x'_i$ *pour tout* $i = 1; 2, ..., n$

On dit qu'un code X *sur* A *est maximal dans* A^* (*au sens de l'inclusion*) *si pour tout code* $X' \subseteq A^*$,

$$X \subseteq X' \Longrightarrow X = X'$$

Exemple 3.1.2

Soit l'alphbet $A = \{a, b\}$*; l'ensemble* $X = \{a, ab, ba\}$ *n'est pas un code puisque :*

$aba \in X^+$ *et* $aba = a(ba) = (ab)a$ (*le mot aba admet donc deux factorisations différentes en mots de* X).

Proposition 3.1.1

Toute partie préfixe ($resp$. $suffixe$, $bipréfixe$) $X \neq \{1\}$ *est un code, on appelle code préfixe* (*resp code* $suffixe$, *code* $bipréfixe$).

Exemple 3.1.3

Soient l'alphbet $A = \{a, b\}$ *et l'ensemble* $X = \{a^nb^n : n \geq 1\}$

Montrons que X *est préfixe, i.e* $X^{-1}X = \{1\}$

$u \in X^{-1}X \iff \exists\ x_0, x_1 \in X\ , u \in A^*\ : x_0 = x_1u$

Donc $\exists\ (m; r) \in (\mathbb{N}^*)^2 : a^mb^m = a^rb^ru$

$$\Longrightarrow m = r \text{ et } u = 1$$

Donc $X^{-1}X = \{1\}$

Alors X est un code préfixe.

Proposition 3.1.2

Soit X une partie de A^*

X est un code $\iff$ $(\forall w \in A^* : (X^*w \cap X^* = \emptyset)$ et $(wX^* \cap X^* = \emptyset)) \Longrightarrow w \in X$.

Proposition 3.1.3

Un sous monoïde M de A^* est unitaire à droite (resp. à gauche, biunitaire) ssi son ensemble de générateur minimal est un code préfixe (resp. suffixe, bipréfixe).

3.2 Codes à groupe

Proposition 3.2.1

Soient G un groupe, H un sous-groupe de G, $\Phi : A^* \longrightarrow G$ un morphisme.

Posons $X^* = \Phi^{-1}(H)$ avec X l'ensemble minimal générateur de X^*. Alors :

1. *X est un code bipréfixe.*

2. *Si Φ est surjectif, X est un code maximal bipréfixe.*

Démonstration.

1. Nous allons démontrer que X^* est sous-monoïde biunitaire de A^*, en effet, soit $p, pq \in X$ *alors $\Phi(p)$ et $\Phi(pq)$ sont dans H d'ou $\Phi(q) = (\Phi(p))^{-1}\Phi(pq)$, est dans H et donc $q \in X^*$, ainsi X^* est unitaire à droite.

   De la même façon, on démontre que X^* est unitaire à gauche.

   Donc X est un code bipréfixe.

2. Supposons maintenant que Φ est surjectif. Si $X^* = A^*$, alors $X = A$; et par suite (2) est prouvé. Sinon soit w un mot quelconque de A^*, $w \notin X^*$. Comme Φ est

surjectif ($\Phi(A^*) = G$), $\Phi(w) \in G$; et G est un groupe donc il existe $v \in A^*$ tel que $\Phi(v) = [\Phi(w)]^{-1}$. Les mots vw et wv sont dans X^* puisque $\Phi(vw) = \Phi(wv) = 1 \in H$ et naturallement $wvw \in (X \cup \{w\})^*$, mais wvw admet deux factorisations distinctes en mots de $X \cup \{w\}$:

$wvw = w(vw) = (wv)w$ et donc $X \cup \{w\}$ ne peut pas être un code, pour tout $w \in X$.
Donc X est un code maximal. ■

Remarque 3.2.1

- *Dans le cas où le morphisme Φ est surjectif, la base X de X^* (qui est donc toujours un code bi-préfixe maximal) est nommée code à groupe. Nous dirons que c'est le code à groupe défini à partir de G, H et Φ , nous le noterons*

$$X(G, H)_\Phi \text{ ou } X(G, H)$$

ou tout simplement X selons le contexte.

- *Soit $X = X(G, H)_\Phi$ un code à groupe. Nous dirons que X est de degré d si $[G : H] = d$. Nous dirons que X est régulier si $H = \{1\}$. Les codes à groupes réguliers sont donc les bases des noyaux de morphismes surjectifs de A^* sur un groupe quelconque .*

Proposition 3.2.2

Soient G un groupe, H un sous-groupe de G:

$$\Phi : A^* \longrightarrow G$$

un morphisme surjectif, et $L = \Phi^{-1}(H)$.

L est un monoïde complet.

Démonstration.

$$L \text{ est complet} \iff \forall w \in A^*, \exists u, v \in A^* : uwv \in L$$

$$\iff \forall w \in A^*, \exists u, v \in A^* : \Phi(uwv) \in H$$

$$\text{donc} \quad \forall w \in A^*, \exists u, v \in A^* : \Phi(u)\Phi(w)\Phi(v) \in H$$

Soit $w \in A^*, [\Phi(w)]^{-1}[\Phi(w)][\Phi(1)] = 1 \in H$

On pose : $\Phi(u) = [\Phi(w)]^{-1}, \Phi(v) = \Phi(1)$

donc L est complet. ■

Théorème 3.2.1

Soit $X \subseteq A^*$: Alors X est un code à groupe si et seulement si $M(X^*)$ est un groupe.

3.2.1 Codes à groupe avec G =($\mathbb{Z}$; +)

Proposition 3.2.3

Soit

$$\Phi : A^* \longrightarrow \mathbb{Z}$$

un morphisme, H un sous-groupe de $\mathbb{Z}$.

Posons

$$X^* = \Phi^{-1}(H)$$

avec X l'ensemble minimal générateur de X^*. Alors :

1. *X est un code bipréfixe .*
2. *Si Φ est surjectif, X est un code maximal bipréfixe.*

Exemples 3.2.1

1. *Soit* $\Psi : \{a,b\}^* \longrightarrow \mathbb{Z}$ *définit par :*

$$\Psi(a) = 1, \Psi(b) = -1 \text{ et } \Psi(1) = 0$$

Ψ *est un morphisme surjectif puisque :*

$\forall z \in \mathbb{Z}$, $\exists w \in \{a,b\}^* : \Psi(w) = z$

On a, si $z = 0, w = 1$, *si* $z > 0, w = a^z$, *si* $z < 0, w = b^{-z}$.

$\Psi^{-1}(\{0\}) = \{w \in \{a,b\}^* : |w|_b = |w|_a\}$ *et* $[\mathbb{Z} : \{0\}]$ *est infinie.*

2. *Soit* $\Psi : \{a\}^* \longrightarrow \mathbb{Z}$ *définit par :*

$$\Psi(a) = k,\ k \in \mathbb{Z}\ , \Psi(1) = 0$$

Montrons que Ψ *est un homomorphisme de monoïdes.*

i- $\Psi(1) = 0$ *par défnition.*

ii- *Soit* $w\ , w' \in \{a\}^* :\ \Psi\left(w\ w'\right) = k\left|w\ w'\right| = k\left(|w| + \left|w'\right|\right) = k\,|w| + k\left|w'\right| = \Psi(w) + \Psi\left(w'\right)$

donc Ψ *est un homomorphisme*

Soit $H = n\mathbb{Z}$, $n \in \mathbb{N}$, *un sous-groupe de* $\mathbb{Z}$

$$\begin{aligned}
\Psi^{-1}(n\mathbb{Z}) &= \{w \in \{a\}^* : \Psi(w) \in n\mathbb{Z}\} \\
&= \{w \in \{a\}^* :\ k\ |w| \in n\mathbb{Z}\} \\
&= \{w \in \{a\}^* :\ k\ |w| \equiv 0 \,(\mathrm{mod}\, n)\}
\end{aligned}$$

$$\begin{aligned} w \in \Psi^{-1}(n\mathbb{Z}) &\iff k\,|w| \equiv 0 \,(\mathrm{mod}\, n) \\ &\iff \overline{k\,|w|} = \overline{0} \\ &\iff \overline{k} \cdot \overline{|w|} = \overline{0} \end{aligned}$$

par exemple : si $n = 5$ *et* $k = 2$

$\overline{\lvert w\rvert}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2} \cdot \overline{\lvert w\rvert}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$

$$\begin{aligned} w \in \Psi^{-1}(5\mathbb{Z}) &\iff 2\,|w| \equiv 0 \,(\mathrm{mod}\, 5) \\ &\iff \overline{|w|} = 5 \cdot \gamma \ , \ \gamma \in \mathbb{N} \end{aligned}$$

Donc $X^* = \left\{w = (a^{5\gamma}) = (a^5)^{\gamma}, \gamma \in \mathbb{N}\right\}$ *et* $X = \{a^5\}$

▶ *si* $n = 6$ *et* $k = 4$

$\overline{\lvert w\rvert}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{4} \cdot \overline{\lvert w\rvert}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$

$$\begin{aligned} w \in X^* &\iff w \in \Psi^{-1}(6\mathbb{Z}) \\ &\iff \overline{4}\,|w| \equiv 0 \,(\mathrm{mod}\, 6) \\ &\iff |w| \equiv 0 \,(\mathrm{mod}\, 6) \quad ou \quad |w| \equiv 3 \,(\mathrm{mod}\, 6) \end{aligned}$$

Donc :

$$X^* = \left\{w = \left(a^{6\gamma}\right) = \left(a^6\right)^{\gamma}, \gamma \in \mathbb{N}\right\} \cup \left\{w = a^{6\alpha+3} = a^3\left(a^6\right)^{\alpha}, \ \alpha \in \mathbb{N}\right\}$$

Alors :

$$X = \left\{a^3\right\}$$

Proposition 3.2.4

soit X un code à groupe. Alors X est fini si et seulement si $X = A^n$.

3.2.2 Codes à groupe avec G =($\mathbb{Z}/n\mathbb{Z}$; +)

Proposition 3.2.5

Soit

$$\Phi : A^* \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

un morphisme, H un sous-groupe de $\mathbb{Z}$ /$n\mathbb{Z}$,

definit par $\Phi(a) = \overline{1}$ pour tout $a \in A$ et $\Phi(1) = 0$

Posons

$$X^* = \Phi^{-1}(H)$$

avec X l'ensemble minimal générateur de X^*. Alors :

1. *X est un code bipréfixe.*
2. *Si Φ est surjectif, X est un code maximal bipréfixe.*

Exemples 3.2.2

1. *Soit $\mathbb{Z}/n\mathbb{Z}$ le groupe cyclique d'ordre n et $\Phi : A^* \longrightarrow \mathbb{Z}/n\mathbb{Z}$ le morphisme défini par : $\Phi(a) = \overline{1}$, $\forall a \in A$, $\Phi(\varepsilon) = \overline{0}$*

$$X^* = \Phi^{-1}\left(\left\{\overline{0}\right\}\right) = \{w \in A^* : |w| \equiv 0 \,(\mathrm{mod}\, n)\}$$

et $X\left(\mathbb{Z}/n\mathbb{Z}, \left\{\overline{0}\right\}\right)_\Phi$ est le code uniforme de longueur n donc $X = A^n$.

2. *Soit*

$$\Phi : \{a, b\}^* \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

défini par :

$$\Phi(a) = \overline{0}\ et\ \Phi(b) = \overline{1}\ et\ \Phi(1) = \overline{0}$$

$\Phi^{-1}\left(\left\{\overline{0}\right\}\right) = \{w\ \in \{a,b\}^* : |w|_b \equiv 0 \pmod 2\}$.

Sa base $X = ba^*b \cup \{a\}$ *est donc un code à groupe régulier de degré* 2.

Théorème 3.2.2

Soit $X \subseteq A^*$ *un code à groupe. Alors* X *est rationnel si et seulement si il est de degré fini*

Exemple 3.2.3

Soit

$$\Phi : \{a,b\}^* \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

défini par :

$\Phi(a) = \overline{0}$ *et* $\Phi(b) = \overline{1}$ *et* $\Phi(1) = \overline{0}$

$\Phi^{-1}\left(\left\{\overline{0}\right\}\right) = \{w\ \in \{a,b\}^* : |w|_b \equiv 0 \pmod 2\}$.

Sa base $X = ba^*b \cup \{a\}$ *est donc un code à groupe régulier de degré 2, donc* X *est rationnel.*

Théorème 3.2.3

Soit $X \subseteq A^*$ *un code fini.* $M(X^*)$ *est un groupe si et seulement si* $X = A^n$. *Et dans ce cas* $M(X^*)$ *est cyclique d'ordre* n.

3.2.3 Codes à groupe avec G =($\mathbf{S}_n$, $\circ$)

Proposition 3.2.6

Soit

$$\Phi \ : A^* \longrightarrow S_n$$

un morphisme, H un sous-groupe de S_n .

Posons

$$X^* = \ \Phi^{-1}(H)$$

avec X l'ensemble minimal générateur de X^*. Alors :

1. *X est un code bipréfixe.*
2. *Si Φ est surjectif, X est un code maximal bipréfixe.*

Exemples 3.2.4

► *Soit $A = \{a_1, a_2, ...a_{n-1}\}$*

et

$$\Psi : A^* \longrightarrow (S_n, \circ)$$

définie par :

$\Psi(a_i) = \Gamma_{i\ ,\ i+1}$, $1 \leq i \leq n\ -1$ *et* $\Psi(1) = id_{\ E}$, $E = \mathbb{N}_n = \{1, 2, ..., n\}$ *où*

$\Gamma_{i\ ,\ i+1}$ *est la permutation qui échange i et $i+1$. Ψ est un homomorphisme de monoïdes.*

► *Soit H un sous-groupe de S_n, H le groupe Alterné c'est-à-dire $H = \{\sigma \in S_n : \varepsilon(\sigma) = 1\}$, $\varepsilon(\sigma)$ est la signature de σ, définie par $\varepsilon(\sigma) = (-1)^{\Gamma}$ tel que Γ est le nombre de transpositions qui composent σ.*

On a :
$$\begin{aligned} X^* &= \Psi^{-1}(H) = \{w \in A^* : \Psi(w) \in H\} \\ &= \{w \in A^* : |w| \quad paire\} \end{aligned}$$

• *si* $A = \{a_1\}$, *on a donc* $\Psi : A^* \longrightarrow (S_2, \circ)$ *définie par :*

$$\Psi(a_1) = \Gamma_{1,2} = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

et

$$\Psi(1) = id_E = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$$

$$E = \mathbb{N}_2 = \{1, 2\}$$

$$\begin{aligned} X^* = \Psi^{-1}(H) &= \{w \in A^* : \Psi(w) \in H\} \\ &= \{w \in A^* : |w| \quad paire\} \\ &= \{1, a_1a_1, a_1a_1a_1a_1, a_1a_1a_1a_1a_1a_1, ..\} \end{aligned}$$

Et donc $X = \{a_1a_1\} = A^2$.

• *Si* $A = \{a_1, a_2\}$, $\Psi : A^* \longrightarrow (S_3, \circ)$ *définie par :*

$$\Psi(a_1) = \Gamma_{1,2} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\Psi(a_2) = \Gamma_{2,3} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\Psi(1) = id_E = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$E \ = \mathbb{N}_3 = \{1, 2, 3\}$$

Et par conséquent

$$\begin{aligned} X^* \ = \ \Psi^{-1}(H) \ &= \ \{w \in A^* : \Psi(w) \in H\} \\ &= \ \{w \in A^* : |w| \quad paire\} \end{aligned}$$

Et $X = \{a_1a_1, a_1a_2a_2a_1, a_2a_2\} = A^2$

• *Si* $A = \{a_1, a_2, a_3\}, \Psi : A^* \longrightarrow (S_4, \circ)$ *est donc définie par :*

$$\Psi(a_1) = \Gamma_{1,2} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

$$\Psi(a_2) = \Gamma_{2,3} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

$$\Psi(a_3) = \Gamma_{3,4} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

$$\Psi(1) = id_E = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

$$E \ = \mathbb{N}_4 = \{1, 2, 3, 4\}$$

$$\begin{aligned} X^* \ = \ \Psi^{-1}(H) \ &= \ \{w \in A^* : \Psi(w) \in H\} \\ &= \ \{w \in A^* : |w| \quad paire\} \end{aligned}$$

$X = \{a_1a_1, a_1a_2, a_1a_3, a_2a_1, a_2a_2, a_2a_3, a_3a_1, a_3a_2, a_3a_3\} = A^2$

- *Si* $A = \{a_1, a_2, ..., a_{n-1}\}$

$$\begin{aligned} X^* &= \Psi^{-1}(H) &&= \{w \in A^* : \Psi(w) \in H\} \\ &&&= \{w \in A^* : |w| \quad paire\} \end{aligned}$$

Et $X = \{a_1a_1, a_1a_2, ..., a_1a_{n-1}, a_2a_1, a_2a_2, ..., a_2a_{n-1}, ..., a_{n-1}a_1, a_{n-1}a_2, ..., a_{n-1}a_{n-1}\} = A^2$

Conclusion générale

Nous avons présenté dans ce travail la notion de groupe et les applications sur les codes et on a construit des codes à groupes dans les cas particuliers suivants :

- codes à groupes dans le cas où $G = (\mathbb{Z}, +)$ et $H = n\mathbb{Z}$, $n \in \mathbb{N}$.
- codes à groupes dans le cas où $G = (\mathbb{Z}/n\mathbb{Z}, +)$.
- codes à groupes dans le cas où $G = (S_n, \circ)$ et $H = A_n$.

Bibliographie

[1] D. Guin, T. Hausberger. *Groupes, Corps et théorie de Galois,* EDP sciences, Année 2008.

[2] F. Dumas, *Algèbre : Groupes et Anneaux 1,* Universit e Blaise Pascal, Année 2007 – 2008.

[3] F. Pécastaings. *Chemins vers l'algèbre tome 1*, Vuibert, Année 1993.

[4] L. Bélair et C. Hohlweg, *MAT2000 – Algèbre II,* 8 septembre 2016

[5] L.Bélair et F.Bergeron et C. Hohlweg, *Introduction à la théorie des groupes - encours de rédaction,* Université du Québec à Montréal, 2 décembre 2016.

[6] L. Schwartz, *Algèbre $3^{ième}$ Année*. Dunod, Année 2003.

[7] M. Demazure. *Cours d'algèbre*, Paris, Cassini, Année 1997.

[8] N.Ghadbane, *Etude sur les groupes syntaxiques de petits degrés,* Mémoire de magister, Universite de M'sila, Année 2010.

[9] T.Connor et J.Vercruysse, *Algèbre I Cours pour $2^{ème}$ année de Bachelier en sciences mathématiques,* Université Libre de Bruxelles, 12 septembre 2012.