République Algérienne Démocratique Et Populaire
Université 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 : Mathématiques Discrètes

Par

Akrib Meriem Et Bouhali Sarra

Sujet

Présentation d'un groupe par générateurs et relations

Date de soutenance : 04/06/2017

Devant le jury :

Mr. Douadi Mihoubi	Prof. Univ de M'sila	Président
Mr. Nacer Ghadbane	M.C.B. Univ de M'sila	Rapporteur
Mr. Lakhdar Heboub	M.A.A. Univ de M'sila	Examinateur

Promotion : 2016 / 2017

Remerciements

Avant tout je remercie Allah, le tout puissant d'avoir, éclaire notre vie, renforce notre courage et notre volanté pour finir ce travail.

Je tiens à remercier particuliérement mon directeur de mémoire Monsieur Nacer Ghadbane, pour toute l'aide qu'il m'a apporté et son patience, ses conseils et pour avoir guidé ce travail avec beaucoup d'intéret.

Je tiens à remercier aussi Monsieur Douadi Mihoubi, d'avoir accepté de présider ce jury de ce mémoire.

Je tiens à remercier Monsieur Lakhdar Heboub, pour avoir accepté d'examiner mon mémoire.

Mes remerciements s'adressent à tout les enseignants du département de mathématique pour leurs dévouement et leurs générosité.

Je tiens ici à exprimer mes sentiments respectueux à mes chers parents à qui je dédie ce travail pour leur grand soutien.

Un grand merci à ma famille, à mes proches et à mes collégues et pour leurs encouragements et pour leurs amitiés.

Dédicace

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 mes chéres soeurs : salima, fati.

-A mes frères : Mohamed et Sofyane, Seif, Ali , Nasro.

-A mon binome Bouhali Sarra

Je suis fiere d'avoir une amie comme toi , qui m'a soutené et encouragé toute l'année.

-A toute la famille.

-A toute mes amies.

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

Enfin je dédie ce mémoire à mes collègues et tous ceux qui me sont cher.

Notations

$\mathbb{N}$: L'ensemble des entiers naturels.

$\mathbb{Z}$: L'ensemble des entiers relatifs.

$\mathbb{R}$:L'ensemble des entiers réels.

$(G, *)$: groupe muni de la loi $*$.

$M_n(\mathbb{C})$: l'ensemble des matrices (n, n) à coefficients dans $\mathbb{C}$.

$GL_n(\mathbb{R})$: l'ensemble des matrices (n, n) inversibles à coefficients réels.

In : la matrice identité.

$H \prec G$: H est un sous groupe du groupe G.

U : l'ensemble des nombres complexes de module égal à 1.

U_n : l'ensemble des racines n-iémes de l'unité.

$n\mathbb{Z}$: les sous-groupes de $\mathbb{Z}$.

$\langle S \rangle$: l'intersection de tous les sous-groupes de G qui contiennent S.

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

$Im(f)$: l'image de f.

$Ker(f)$: le noyau de f.

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

xRy : x en relation avec y.

xH et Hx : les classes à gauche et à droite de x modulo H.

${}_HR$ et R_H : les relations à gauche et à droite modulo H.

$(G/H)_g$ et $(G/H)_d$: l'ensemble des classes d'équivalence des éléments de G pour la relation à gauche et à droite modulo H.

$[G : H]$: le cardinal de l'ensemble $(G/H)_g$ (ou $(G/H)_d$).

$|G|$: le cardinal de G.

$o(x)$: l'ordre de x.

G/R : l'ensemble quotient de G par la relation R.

G/H : l'ensemble quotient de G par H.

$S(E)$:groupe symétrique de E.

$\mathbb{Z}/n\mathbb{Z}$: l'ensemble des entiers modulo n.

P_n : le sous-ensemble de {1,...,n} des nombres premiers avec n.

$\varphi(n)$: le cardinal de P_n.

D_n : le groupe diédral.

Σ **:** alphabet fini.

Σ^* : l'ensemble des mots sur Σ.

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.

$w(i)$: la i-éme lettre.

$\widetilde{w}$: l'image miroir de w.

$Pref(w)$ (resp $Suff(w)$, $Fac(w)$) : les préfixes (resp suffixes, facteurs) de w.

w^n : la puissance n-iéme de w.

L : langage.

L^n : la puissance n-iéme de langage L.

L^* : l'étoile de Kleene de L.

$\cong$: isomorphe.

$L(X)$: le groupe libre de base X .

$M(X)$: l'ensemble des mots en $X \cup X^{-1}$.

L_X : l'ensemble des mots réduits correspondants à chaque classe de $M(X)/R$.

$\langle X \backslash R \rangle$: la présentation du groupe G par générateurs et relations.

$\langle X \backslash \emptyset \rangle$: la présentation du groupe libre $L(X)$.

$\langle x \backslash x^n \rangle$: la présentation du groupe cyclique d'ordre n.

$\langle x \backslash \emptyset \rangle$: la présentation du groupe monogène d'ordre infini.

$(\{a, b\} \backslash a^n, b^2, abab)$: la présentation du groupe diédral D_n .

Résumé

Dans ce travail, on donne tout d'abord des notions générales sur les groupes, par la suite, on fait une étude sur les groupes monogénes, cycliques et diédraux D_n. D'autre part, nous avons étudié les mots et les langages dans un monoïde libre et quelques propriétés.

Enfin, on s'intéresse au groupe libre, en mettant l'accent sur la propriété universelle qui tout groupe engendré par un ensemble X est isomorphe à un quotient noté $L(X)$ via une congruence.

On donne ensuite quelques présentations des groupes via un quotient d'un groupe libre : groupe monogéne infini, groupe cyclique d'ordre n, groupe diédrale D_n.

Mots clés : Groupe, groupe monogène, groupe cyclique, groupe diédrale, groupe quotient, groupe libre, mot, langage, monoïde libre, homomorphisme de groupes.

Table des matières

Introduction **1**

1 Généralités sur les groupes **2**
1.1 Notions élémentaires sur les groupes 2
1.2 Groupes quotients 10

2 Etude sur les groupes monogènes, cycliques et les groupes diédraux. **18**
2.1 Groupe symétrique 18
2.2 Groupes monogènes 19
2.3 Groupes cycliques 22
2.3.1 Caractérisation des groupes cyclique 22
2.3.2 Sous-groupe d'un groupe cyclique 23
2.3.3 Générateurs d'un groupe cyclique 24
2.4 Groupes Diédraux D_n 25
2.4.1 Isométries du plan 26
2.4.2 Générateurs et ordre de D_n 27
2.4.3 Caractérisation de D_n 29

3 Etude sur les mots et les langages dans un monoïde libre **32**
3.1 Monoïde 32
3.2 Mot et langage 33

4 Présentations de quelques groupes par générateurs et relations **43**
4.1 Groupes libres 43
4.2 Générateurs et relations 50
4.3 Présentation d'un groupe monogène d'ordre infini 52
4.4 Présentation d'un groupe cyclique d'ordre n 53
4.5 Présentation de groupe diédral D_n 54

Conclusion **58**

Bibliographie **58**

Introduction

La notion de groupe a été introduite pour la première fois au début du dix-neuvième 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-neuvième siécle la notion abstraite de groupe et que petit à petit a été construite la théorie de groupes.

Dans ce mémoire nous allons étudier que pour tout ensemble X, il existe un groupe $L(X)$ dans lequel tout élément s'écrit de manière unique en fonction des générateurs $x_i \in X$. C'est le groupe libre de base X. Ce groupe est d'une grande importance, car on verra que tout groupe est isomorphe à un quotient d'un tel groupe. De plus, cela conduit à la notion de groupes présentés par générateurs et relations, qui sont des groupes dans lesquels les écritures des éléments en fonction des générateurs peuvent être simplifiées à l'aide des relations entre ces générateurs. Ces groupes sont particulièrement intéressants pour les possibilités qu'ils offrent, de calculs effectifs sur les éléments et de définitions explicites de morphismes.

Ce travail est composé de quatre chapitres :

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

Dans le deuxième chapitre nous allons étudier les groupes symétriques, monogénes, cycliques et les groupes diédraux.

Dans le troisième chapitre nous intéressons à les notions des mots et les langages dans un monoïde libre et quelques propriétés.

Dans le quatrième chapitre nous avons fait la présentation de quelques groupes par générateurs et relations.

Chapitre 1

Généralités sur les groupes

1.1 Notions élémentaires sur les groupes

Définition 1.1

Soit G un ensemble non vide et $* : \begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & a*b \end{array}$ une application, $(G,*)$ est un groupe si :

a) La loi $*$ est associative ie. $\forall a,b,c \in G,\ a*(b*c) = (a*b)*c$.

b) L'ensemble G posséde un élément neutre e pour $*$ ie : $\exists e \in G, \forall a \in G, a*e = e*a = a$.

c) Tout $a \in G$ admet un symétrique ie : $\forall a \in G,\ \exists b \in G,\ a*b = b*a = e$.

Si, de plus, la loi $*$ est commutative (ie. $\forall a,b \in G,\ a*b = b*a$), alors on dit que G est un groupe commutatif ou abélien.

Exemple 1.1

a) $(M_n(\mathbb{C}),+)$, où $M_n(\mathbb{C})$ désigne l'ensemble des matrices (n,n) à coefficients dans $\mathbb{C}$ est un groupe abélien.

b) Pour tout entier $n \geq 1$, l'ensemble $GL_n(\mathbb{R})$ des matrices carrées d'ordre n inversibles à coefficients réels est un groupe pour la multiplication des matrices. Le neutre en est la matrice identité I_n, car $M \times I_n = I_n \times M = M$ pour toute $M \in GL_n(\mathbb{R})$, le symétrique de M pour la loi $\times$ est la matrice inverse M^{-1},

car $M \times M^{-1} = M^{-1} \times M = I_n$. Dés lors que $n \geq 2$, le groupe $GL_n(\mathbb{R})$ n'est pas abélien.

Table de cayley :

On peut représenter un groupe fini G d'ordre n par un tableau à n lignes et n colonnes portant dans la case d'intersection de la ligne indexé par un élément x de G et de la colonne indexé par un élément y de G la valeur du produit $x.y$. Il est facile de vérifier que tout élément de G apparaît une fois et une seule dans chaque ligne et chaque colonne de la table. Il est clair enfin qu'un groupe fini est abélien si et seulement si sa table est symétrique par rapport à la diagonale principale.

Exemple 1.2

Les tables des groupes $U_2 = \{-1, 1\}, U_3 = \{1, j, j^2\}, U_4 = \{1, i, -1, -i\}$ sont :

	1	-1
1	1	-1
-1	-1	1

	1	j	j^2
1	1	j	j^2
j	j	j^2	1
j^2	j^2	1	j

	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Proprietés d'un groupe :

1. L'élément neutre d'un groupe est unique ($e' = e' * e = e * e' = e$).
2. Le symétrique d'un élément a est unique ($b = (b'a)b = b'(ab) = b'$).
3. $\forall a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.
4. L'équation $ax = b$ a une et une seule solution $x = a^{-1}b$.
5. Le groupe G est régulier à gauche et à droite :

$$\forall a, b, c \in G, c * a = c * b \Longrightarrow a = b \text{ et } a * c = b * c \Longrightarrow a = b.$$

Définition 1.2

Soit G un groupe muni d'une loi de composition interne et soit H un sous ensemble non-vide de G. On dit que H est un sous-groupe de G et on notera $H \prec G$ lorsque les deux conditions suivantes sont vérifiées :

1. H est stable pour la loi. (ce qui signifie $x.y \in H$ pour tous $x, y \in H$).
2. H est stable par passage à l'inverse (ce qui signifie $x^{-1} \in H$ pour tout $x \in H$).

Dans ce cas, la restriction à H de la loi de G définit une loi de composition interne dans H, pour laquelle H est lui-même un groupe.

Remarque 1.1

a) les deux assertions (1) et (2) sont équivalentes à :

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

b) Un groupe G ayant au moins deux éléments admet au moins deux sous groupes : G et le sous-groupe réduit à l'élément neutre.

c) 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.

Exemple 1.3

1. Les ensembles $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ sont des sous-groupes du groupe $\mathbb{C}$ muni de l'addition, mais pas $\mathbb{N}$ (car l'opposé d'un élément de $\mathbb{N}$ n'est pas nécéssairement un élément de $\mathbb{N}$).
2. L'ensemble $\mathbf{U}$ des nombres complexes de module égal à 1 est un sous-groupe de $\mathbb{C}^*$ muni de la multiplication. Pour tout entier $n \geq 1$, l'ensemble $\mathbf{U}_n$ des racines n-ièmes de l'unité est un sous-groupe de $\mathbf{U}$.

Proposition 1.1

Les sous-groupes de $(\mathbb{Z}, +)$ *sont les* $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\}$, *pour* n *parcourant* $\mathbb{N}$.

Preuve.

Il est clair que les $n\mathbb{Z} = \{nx, x \in \mathbb{Z}\}$, pour n parcourant $\mathbb{N}$, sont des sous-groupes de $\mathbb{Z}$.

Réciproquement, soit H un sous-groupe de $\mathbb{Z}$:

Si $H = \{0\}$, alors $H = n\mathbb{Z}$ avec $n = 0$.

Si $H \neq \{0\}$, son intersection avec $\mathbb{N}^*$ est un ensemble non vide d'entiers positifs et possède donc un plus petit élément n. Soit x un élément quelconque de H, la division

euclidienne de x par n donne $x = ny + k$, avec $0 \leq k < n$. Comme $k = x - ny$ appartient à H, k est nul par définition de l'entier n. On en déduit que $H = n\mathbb{Z}$. ■

Définition 1.3

On appelle sous-groupe propre d'un groupe G tout sous groupe distinct de G et de l'élément neutre.

Proposition 1.2

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.

Preuve.

Soit $H = \bigcap_{i \in I} H_i$, $a, b \in H \Rightarrow a, b \in H_i$, $\forall i \Rightarrow ab^{-1} \in H_i$, $\forall i \Rightarrow ab^{-1} \in H$. ■

Remarque 1.2

Une réunion de sous-groupes d'un groupe G n'est en général pas un sous-groupe de G. Par exemple, on vérifiera que $3\mathbb{Z}$ et $5\mathbb{Z}$ sont des sous-groupes de $\mathbb{Z}$, mais que $3 + 5 = 8$ n'appartient pas à $3\mathbb{Z} \cup 5\mathbb{Z}$.

Définition 1.4

Soit G un groupe et $S \subseteq G$.

1. On note $\langle S \rangle$ l'intersection de tous les sous-groupes de G qui contiennent S. C'est un sous-groupe de G appelé sous-groupe engendré par S**.**
2. Si $G = \langle S \rangle$, on dit que G est engendré par S et que S est une partie génératrice de G. Les éléments de S sont appelés générateurs de G**.**

Proposition 1.3

Soient G un groupe et S une partie non vide de G. On a :

$$\langle S \rangle = \{x_1 ... x_n, n \in \mathbb{N}^*, x_i \in S \text{ ou } x_i^{-1} \in S, \forall i, 1 \leq i \leq n\}.$$

Preuve.

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 prouve que H est un sous-groupe de G.

D'où $\langle S\rangle$ est contenu dans H. Il est clair que tout sous-groupe de G contenant S contient H, d'où $\langle S\rangle = H$. ■

Cas partuculier important :

Si $S = \{x\}$ pour $x \in G$, on note alors x le sous-groupe engendré par x et il est clair que $\langle x\rangle = \{x^n, n \in \mathbb{Z}\}$.

Proposition 1.4

Soit G un groupe et $S \subseteq G$ $(S \neq \emptyset)$, $\langle S\rangle = \{x = x_1x_2...x_n, n \in \mathbb{N}^*, x_i \in S \cup S^{-1}, \forall i, 1 \leq i \leq n\}$, $\langle S\rangle$ est le plus petit sous-groupe de G contenant S.

Preuve.

1. On montre que $S \subseteq \langle S\rangle$, on a : $\forall x \in S \Longrightarrow x \in \langle S\rangle$ $(n = 1)$. Donc $S \subseteq \langle S\rangle$.
2. On montre que $\langle S\rangle$ est un sous-groupe de G :
   - $S \neq \emptyset$ et $S \subseteq \langle S\rangle \Longrightarrow \langle S\rangle \neq \emptyset$.
   - Soient $x, y \in \langle S\rangle$, $x \in \langle S\rangle \iff x = x_1x_2...x_n, n \in \mathbb{N}^*, x_i \in S \cup S^{-1}, \forall i, 1 \leq i \leq n.$
     $y \in \langle S\rangle \iff y = y_1y_2...y_r, r \in \mathbb{N}^*, y_i \in S \cup S^{-1}, \forall i, 1 \leq i \leq r.$

     On a : $xy^{-1} = (x_1x_2...x_n)(y_1y_2...y_r)^{-1}.$
     $= (x_1x_2...x_n)(y_r^{-1}y_{r-1}^{-1}...y_1^{-1}).$
     $= z_1z_2...z_nz_{n+1}...z_{n+r}.$

     et $\forall i, 1 \leq i \leq n+r$, $z_i \in S \cup S^{-1} \Longrightarrow xy^{-1} \in \langle S\rangle$.

     Donc $\langle S\rangle$ est un sous-groupe de G.
3. Soit K un sous-groupe de G, on montre que $\langle S\rangle \subseteq K$:

   Soit $x \in \langle S\rangle$, i.e, $x = x_1x_2...x_n, n \in \mathbb{N}^*, x_i \in S \cup S^{-1}, \forall i, 1 \leq i \leq n$, On a :

   $$\begin{cases} S \subseteq K \Longrightarrow S^{-1} \subseteq K \Longrightarrow S \cup S^{-1} \subseteq K. \\ \qquad\qquad et \\ K \text{ un sous-groupe de } G. \end{cases}$$

   $\Longrightarrow \forall i, 1 \leq i \leq n, x_i \in K \Longrightarrow x = x_1x_2...x_n \in K.$

   Donc $\langle S\rangle \subseteq K$.

De 1),2),3) $\langle S\rangle$ est le plus petit sous-groupe de G contenant S. ■

Remarque 1.3

Si la loi de G est notée additivement, on a :

$$S = \{x_1 + \cdots + x_n, n \in \mathbb{N}^*, x_i \in S \text{ et } -x_i \in S, \forall i, 1 \leq i \leq n\}.$$

d'où $\langle x \rangle = \{nx, n \in \mathbb{Z}\}$.

Définition 1.5

Soient $(G, *)$ et $(H, \bullet)$ deux groupes. Une application de G dans H est un morphisme de groupes lorsque :

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

Si $G = H$ et $* = \bullet$, on parle d'endomorphisme**.**

Si f est bijective, on parle d'isomorphisme.

Si f est un endomorphisme bijectif, on parle d'automorphisme.

Exemple 1.4

1. $x \longmapsto \ln x$ réalise un isomorphisme de $(\mathbb{R}_+^*, .)$ sur $(\mathbb{R}, +)$.
2. L'application $\exp : \mathbb{R} \to \mathbb{R}_+^*$ qui à tout nombre réel associe son exponentielle est un morphisme de groupes de $\mathbb{R}$ muni de l'addition dans $\mathbb{R}_+^*$ muni de la multiplication, car : $\exp(x + y) = \exp x \ . \exp y$, pour tous $x, y \in \mathbb{R}$.

Notation 1.1

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

Proposition 1.5

Soient G, G', G'' trois groupes. Alors pour tout f de $Hom(G, G')$ et tout g de $Hom(G', G'')$, $g \circ f$ appartient à $Hom(G, G'')$.

Preuve.

Notons $(G, \cdot)$, $(G', *)$ et $(G'', \triangleright)$. Il est clair que $g \circ f$ est une fonction de G dans G''. Soit $a, b \in G$, montrons que $(g \circ f)(ab) = (g \circ f)(a) \triangleright (g \circ f)(b)$. Puisque f et g

sont des morphismes de groupes on obtient : $(g \circ f)(ab) = g(f(ab)) = g(f(a) * f(b)) = g(f(a)) \triangleright g(f(b)) = (g \circ f)(a) \triangleright (g \circ f)(b)$. ■

Définition 1.6

Soit $f : G \to G'$ un morphisme de groupes.

i) L'ensemble $f(G) = \{x' \in G'; \exists x \in G, f(x) = x'\} = \{f(x);\ x \in G\}$ est appelé l'image de f, et noté $\mathrm{Im}(f)$.

ii) L'ensemble $f^{-1}(\{é\}) = \{x \in G; f(x) = é\}$ est appelé le noyau de f, et noté $\ker(f)$.

Proposition 1.6

Tout élément f de $Hom(G, G')$ vérifie les proprietés 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. $H' < G' \Longrightarrow f^{-1}(H') < G$ avec $f^{-1}(H') = \{x \in G,\ f(x) \in H'\ \}$.

Preuve.

1. Notons 1_G et $1_{G'}$ les éléments neutres respectifs de G et G'. Soit x un élément de G, on a $f(x) = f(x1_G) = f(x)f(1_G)$.Or $f(x) = f(x)1_{G'}$, d'où $f(1_G) = 1_{G'}$.

2. Pour tout x de G on a $1_{G'} = f(1_G) = f(xx^{-1}) = f(x)f(x^{-1})$, d'où $f(x^{-1}) = f(x)^{-1}$.

3. Pour tous y_1 et y_2 dans $f(H)$, il existe x_1 et x_2 dans H tels que $f(x_1) = y_1$ et $f(x_2) = y_2$. D'où $y_1 y_2^{-1} = f(x_1)f(x_2)^{-1} = f(x_1)f(x_2^{-1}) = f(x_1 x_2^{-1})$ qui appartient à $f(H)$.

4. Pour tous x et y dans $f^{-1}(H)$ on a $f(x)$ et $f(y)$ dans H, d'où $f(xy^{-1}) = f(x)f(y)^{-1}$ appartient à H, et xy^{-1} appartient à $f^{-1}(H)$. ■

Théorème 1.2

Soit $f : (G, *, e_G) \longrightarrow (G', \cdot, e_{G'})$ un morphisme de groupes alors :

1. $\ker(f\ )$ est un sous-groupe de G .

2. f est injectif si et seulement si, $\ker(f) = \{e_G\}$.

3. $\mathrm{Im}(f)$ est un sous-groupe de G'.

4. f est surjectif si et seulement si, $\mathrm{Im}(f) = G'$.

Preuve.

1) i) On sait que $e_G \in \ker(f)$ car $f(e_G) = e_{\acute{G}}$, donc $\ker(f)$ est non-vide.

ii) Si $x, y \in \ker(f)$, il suffit de démontrer que $x * y^{-1} \in \ker(f)$ on voi

$f(x * y^{-1}) = f(x) \cdot f(y)^{-1} = e_{G'} \cdot e_{G'}^{-1} = e_{G'}$.

Donc $x * y^{-1} \in \ker(f)$ et $\ker(f)$ est un sous-groupe.

2) i) Si f est injectif on a alors :

$\forall x \in \ker(f), f(x) = e_{G'} = f(e_G) \Rightarrow x = e_G$ et donc $\ker(f) = \{e_G\}$.

ii) Réciproquement si $\ker(f) = \{e_G\}$ pour x, y dans G tels que $f(x) = f(y)$, on a :

$$e_{G'} = f(x)^{-1} \cdot f(x) = f(x)^{-1} \cdot f(y) = f(x^{-1}) \cdot f(y) = f(x * y^{-1}).$$

donc, $x * y^{-1} \in \ker(f)$ et $x * y^{-1} = e_G$, ce qui équivaut à $x = y$.

3) i) On sait que $\mathrm{Im}(f) \neq 0$ car $f(e_G) \in \mathrm{Im}(f)$, donc $\mathrm{Im}(f)$ est non-vide.

ii) Si $x, y \in \mathrm{Im}(f)$, il suffit de démontrer que $x \cdot y^{-1} \in \mathrm{Im}(f)$. Comme $x, y \in \mathrm{Im}(f)$, il existe $a, b \in G$ tels que :

$x = f(a)$ et $y = f(b)$ alors : $x \cdot y^{-1} = f(a) \cdot f(b)^{-1} = f(a * b^{-1}) \in \mathrm{Im}(f)$.

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

Proposition 1.7

Si f est un isomorphisme de groupes de G sur G', alors la bijection réciproque f^{-1} est un isomorphisme de groupes de G' sur G.

Preuve.

Soient x' et y' deux éléments quelconques de G'. Posons $x = f^{-1}(x')$ et $y = f^{-1}(y')$. Parce que f est un morphisme de groupes, on a $f(x.y) = f(x).f(y)$, donc $f(x.y) = x'.y'$, d'où $x.y = f^{-1}(x'.y')$, c'est-à-dire $f^{-1}(x').f^{-1}(y') = f^{-1}(x'.y')$. Ceci prouve que f^{-1}est un morphisme de groupes de G' sur G. ■

1.2 Groupes quotients

Définition 1.7

Soient G un groupe et H un sous-groupe de G. On définie sur G la relation suivante :

$$xRy \Longleftrightarrow x^{-1}y \in H.$$

Proposition 1.8

i) La relation R est une relation d'équivalence.

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

Preuve.

i) 1. La relation R est réflexive car : $\forall x \in G$, comme H est un sous-groupe de G, alors $xx^{-1} = e \in H$, donc $\forall x \in G$, xRx.

2. La relation R est symétrique car : $\forall x, y \in G$:

$$\begin{aligned} xRy &\Longleftrightarrow xy^{-1} \in H. \\ &\Longrightarrow (xy^{-1})^{-1} \in H. \\ &\Longrightarrow yx^{-1} \in H. \\ &\Longrightarrow yRx. \end{aligned}$$

3. La relation R est transitive car : $\forall x, y, z \in G$:

$$\begin{aligned} (xRy) \wedge (yRz) &\Longleftrightarrow [(xy^{-1}) \in H] \wedge [(yz) \in H]. \\ &\Longrightarrow ((xy^{-1})(yz^{-1}) \in H, \text{ car } H \text{ est un sous-groupe.} \\ &\Longrightarrow (x(y^{-1}y)z^{-1}) \in H, \text{ car la loi de } G \text{ est associative.} \\ &\Longrightarrow (xz^{-1}) \in H. \\ &\Longrightarrow xRz. \end{aligned}$$

De $1, 2, 3$ on déduit que R est une relation d'équivalence.

ii) Si xRy il existe $h \in H$ tel que $x^{-1}y = h$, i.e. $y = xh$. ■

Définition 1.8

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

Remarque 1.4

1. On définit une relation d'équivalence à droite modulo H par :

$$(xRy) \Longleftrightarrow (xy^{-1} \in H).$$

et la classe à droite de x modulo H est l'ensemble $Hx = \{hx, h \in H\}$.

Lorsque nous aurons à considérer les relations à gauche et à droite modulo H, nous noterons ces deux relations respectivement ${}_HR$ et R_H.

2. Quel que soit h dans H, on a $Hh = H = hH$ et H est la classe à droite et à gauche de l'élément neutre de G modulo H.
3. Si le groupe G est abélien, en notant sa loi additivement, les relations d'équivalences définies ci-dessus s'écrivent $(xRy) \Leftrightarrow ((x - y) \in H)$, et les relations d'équivalences (resp les classes) à gauche et à droite modulo H coïncident.

Si le groupe G n'est pas abélien, ce n'est plus le cas, en général. On considère dans S_3 le sous-groupe $H = \langle\gamma\rangle$ avec $\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

En remarquant que $S_3 = \{e, \gamma, \sigma, \sigma^2, \gamma \circ \sigma, \sigma \circ \gamma\}$ avec $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, les classes à gauche et à droite modulo H sont respectivement :

$\sigma H = \{\sigma, \sigma \circ \gamma\}$ $\qquad$ $H\sigma = \{\sigma, \gamma \circ \sigma\}$.

$\sigma^2 H = \{\sigma^2, \sigma^2 \circ \gamma = \gamma \circ \sigma\}$ $\qquad$ $H\sigma^2 = \{\sigma^2, \gamma \circ \sigma^2 = \sigma \circ \gamma\}$.

qui sont deux à deux distinctes puisque $\gamma \circ \sigma \neq \sigma \circ \gamma$.

Notation 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) modulo H.

Proposition 1.9

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

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

ii) Les ensembles $(G/H)_g$ et $(G/H)_d$ sont équipotents.

Preuve.

i) Pour tout élément x de G, l'application $\begin{array}{ccc} H & \longrightarrow & xH \\ h & \longmapsto & xh \end{array}$, est évidemment bijective.

ii) soit $\Phi : \begin{array}{ccc} (G/H)_g & \longrightarrow & (G/H)_d \\ xH & \longmapsto & \Phi(xH) = Hx^{-1} \end{array}$,

montrons que Φ est une application. En effet, $xH = yH$ est équivalent à $x^{-1}y \in H$, d'où $x^{-1} \in Hy^{-1}$, et $Hx^{-1} = Hy^{-1}$, c'est-à-dire $\Phi(xH) = \Phi(yH)$.

D'autre part, $Hx^{-1} = Hy^{-1}$ est équivalent à $x^{-1}y \in H$, autrement dit, $xH = yH$. Ceci signifie que $\Phi(xH) = \Phi(yH)$ implique $xH = yH$ et donc que Φ est injective. De plus, pour tout Hx dans $(G/H)_d$, on a $Hx = \Phi(x^{-1}H)$, par conséquent Φ est surjective. Il existe donc une application bijective de $(G/H)_g$ sur $(G/H)_d$, ce qui prouve que ces deux ensembles sont équipotents. ■

Définition 1.9

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.

Définition 1.10

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 1.4 *(de Lagrange).*

Si G est un groupe fini, pour tout sous-groupe H de G on a :

$$|G| = |H|[G : H].$$

Preuve.

Puisque les xH, $x \in G$, sont les classes d'équivalences pour la relation d'équivalence R, elles forment une partition de G,

i.e :

$$G = \bigcup_{x \in \{x_1,\ldots,x_k\}} xH \text{ où } k = |(G/H)_g|$$

$$\begin{aligned} |G| &= |\bigcup_{i=1}^{k} x_i H| \\ &= \sum_{i=1}^{k} |x_i H| \\ &= \sum_{i=1}^{k} |H| \\ &= |H|[G:H] \end{aligned}$$

D'où la formule $|G| = |H|[G:H]$. ■

Remarque 1.5

Ce théorème est souvent énoncé de la façon suivante : dans un groupe fini, l'ordre de tout sous-groupe divise l'ordre du groupe.

Corollaire 1.1

Pour tout groupe fini, l'ordre de tout élément divise l'ordre du groupe.

Preuve.

Pour tout x de G, l'ordre de x est cardinale du sous-groupe $\langle x \rangle$ de G. On applique alors le théorème de Lagrange avec $H = \langle x \rangle$. ■

Définition 1.11

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

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

ii) R est compatible avec la loi si elle est compatible à droite et à gauche.

Proposition 1.10

R est compatible avec la loi de G si et seulement si :

$$\forall x, \acute{x}, y, \acute{y} \in E, [(xR\acute{x}) \text{ et } (yR\acute{y})] \Longrightarrow [xyR\acute{x}\acute{y}].$$

Preuve.

Supposons que R soit compatible avec la loi : alors si xRx' et yRy', on a $xyRx^{'}y$ et $x'yRx'y'$, d'où $xyRx'y'$ par transitivité.

Réciproquement, l'assertion de l'énoncé étant vrai pour tout $x, \acute{x}, y, \acute{y}$, c'est en particulier vrai pour $y = \acute{y}$, d'où si $xR\acute{x}$ alors $xyR\acute{x}y$ et la relation est compatible à droite avec la loi. De même, en considérant $x = \acute{x}$, on montre qu'elle est compatible à gauche. ■

Proposition 1.11

Soient G un ensemble muni d'une loi de composition interne, R une relation d'équivalence définie sur G et G/R l'ensemble quotient de G par la relation d'équivalence R. Alors la loi interne de G induit une loi interne sur G/R, $(\overline{x}, \overline{y}) \rightarrow \overline{xy}$ (où pour $z \in G$, $\overline{z}$ désigne la classe d'équivalence de z) si et seulement si R est compatible avec la loi de G.

Preuve.

La correspondance $(\overline{x}, \overline{y}) \rightarrow \overline{xy}$ définit une loi interne sur G/R si et seulement si elle définit une application $G/R \times G/R \rightarrow G/R$, autrement dit, si et seulement si $(\overline{x} = \overline{x_1}, \overline{y} = \overline{y_1}) \Rightarrow (\overline{xy} = \overline{x_1 y_1})$

d'où le résultat d'aprés la proposition précidante. ■

Remarque 1.6

Si la relation 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 est de même pour la loi induite sur G/R, $\overline{e}$ est l'élément neutre, l'élément symétrique de $\overline{x}$ est $\overline{x^{-1}}$.

Proposition 1.12

Soient G un groupe et R une relation d'équivalence définie sur G, compatible avec la loi de G. Alors l'ensemble quotient G/R, muni de la loi induite par la loi de G (définie par $(\overline{x}, \overline{y}) \rightarrow \overline{xy}$), est un groupe.

Proposition 1.13

Pour tout sous-groupe H d'un groupe G, la relation R_H (resp.${}_H R$) est compatible à droite (resp. à gauche) avec la loi de composition de G .

Réciproquement, si une relation R définie sur un groupe G est compatible à droite (resp. à gauche) avec la loi de composition du groupe G, alors il existe un unique sous-groupe H de G tel que $R = R_H$ (resp. $R =_H R$).

Preuve.

Soient x, y, a des éléments de G tels que $xR_H y$, i.e. $xy^{-1} \in H$. Alors, $(xa)(ya)^{-1} = xaa^{-1}y^{-1}$ appartient à H , i.e. $xaR_H ya$.

Une démonstration analogue donne le résultat pour ${}_H R$.

Soit R une relation d'équivalence définie sur G, compatible à droite avec la loi de G. On note H la classe d'équivalence de l'élément neutre 1_G de G. Montrons que H est un sous-groupe de G. Puisque $1_G \in H$, H est non vide. Pour tous x et y dans H, on a $xR1_G$ et $yR1_G$.

La compatibilité de R avec la loi de G implique que $xy^{-1}Ry^{-1}$; de plus, puisque $yR1_G$, on a $yy^{-1}Ry^{-1}$, d'où $1_G Ry^{-1}$ et $y^{-1}R1_G$.

On en déduit que $xy^{-1}R1_G$, i.e. $xy^{-1} \in H$, ce qui prouve que H est un sous-groupe de G. Vérifions que $R = R_H$. Si xRy alors, d'après la compatibilité, $xy^{-1}R1_G$, d'où $xy^{-1} \in H$ et $xR_H y$. Si $xR_H y$, $xy^{-1} \in H$, donc $xy^{-1}R1_G$ et d'après la compatibilité, xRy. L'unicité de H découle du fait que si $R = R_H$, alors H est la classe d'équivalence de 1_G.

La relation d'équivalence R est donc compatible avec la loi de G si et seulement si il existe un sous-groupe H de G tel que $R =_H R = R_H$. ■

Définition 1.12

Un sous-groupe H d'un groupe G est dit normal (ou distingué) dans G si ${}_H R = R_H$. On note alors $H \lhd G$.

Remarque 1.7

On peut énoncer plusieurs conditions équivalentes pour que H soit un sous-groupe distingué de G :

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. $\forall h \in H$, $\forall x \in G$, $xhx^{-1} \in H$.

Résultats immédiats :

1. Dans un groupe quelconque G, les sous-groupes triviaux $\{e\}$ et G sont distingués.
2. Dans un groupe abélien, tout sous-groupe est distingué.
3. Le noyau d'un homomorphisme de groupes est un sous-groupe distingué : si $f : G \to G'$ est un homomorphisme de groupes, $ker(f) \lhd G$.

Définition 1.13

soient G un groupe et H un sous-groupe normal de G. La relation binaire sur G définie par xRy si et seulement si $xy^{-1} \in H$ est une relation d'équivalence sur G compatible avec la loi du groupe est appelée relation de congruence modulo H.

Théorème 1.5

L'ensemble quotient, noté G/H, muni de la loi $\overline{x}$, $\overline{y} \in G/H$, $\overline{x} \bullet \overline{y} = \overline{xy}$, est un groupe appelé groupe quotient de G par H et la surjection canonique $\pi : G \longrightarrow G/H, x \longmapsto \overline{x}$ est un homomorphisme de groupe (on écrit dans ce cas, $x \equiv y (\text{mod } H)$ pour désigner que xRy).

Preuve.

1. La loi $\bullet$ est bien définie car l'application $\bullet$: $\begin{array}{ccc} (G\backslash H) \times (G\backslash H) & \longrightarrow & (G\backslash H) \\ (\overline{x}, \overline{y}) & \longmapsto & \overline{x} \bullet \overline{y} = \overline{xy} \end{array}$

   Constitue ainsi une loi de composition interne sur $G\backslash H$.

2. La loi $\bullet$ est associative car : $\forall x, y, z \in G : \overline{x} \bullet (\overline{y} \bullet \overline{z}) = \overline{x} \bullet \overline{(yz)} = \overline{x(yz)} = \overline{(xy)z} = \overline{(xy)} \bullet \overline{z} = (\overline{x} \bullet \overline{y}) \bullet \overline{z}$.

3. La loi admet élément neutre $\overline{e} : \forall x \in G : \overline{e} \bullet \overline{x} = \overline{ex} = \overline{xe} = \overline{x} \bullet \overline{e} = \overline{x}$.

4. La loi $\bullet$ admet élément inverse $(\overline{x})^{-1} = \overline{x^{-1}}$:

$$\forall x \in G : \overline{x} \bullet \overline{x^{-1}} = \overline{xx^{-1}} = \overline{e} \text{ et } \overline{x^{-1}} \bullet \overline{x} = \overline{x^{-1}x} = \overline{e}.$$

Enfin, la surjection canonique $\pi : G \longrightarrow G/H, x \longmapsto \overline{x}$ est un morphisme de groupes.

i) $\forall x, y \in G : \pi(x * y) = \overline{xy} = \overline{x} \bullet \overline{y} = \pi(x) \bullet \pi(y)$.

ii) $\pi(e) = \overline{e}$.

■

Exemple 1.5

On considére $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ avec $n \in \mathbb{N}$. Puisque $\mathbb{Z}$ est commutatif, le sous-groupe $n\mathbb{Z}$ est distingué dans $\mathbb{Z}$. Deux entiers x et y sont en relation modulo $n\mathbb{Z}$ si, et seulement si, $x - y \in n\mathbb{Z}$, si, et seulement si, $n/x - y$ (ou $\exists k \in \mathbb{Z} : x - y = nk$) i.e, $x \equiv y (\text{mod } n)$ et ainsi la notation $\mathbb{Z}_n = G/H = \mathbb{Z}/n\mathbb{Z}$ est justifiée.

Chapitre 2

Etude sur les groupes monogènes, cycliques et les groupes diédraux.

2.1 Groupe symétrique

Définition 2.1

Soit E un ensemble non vide, l'ensemble $S(E)$ des bijections de E sur E muni de la loi de composition des applications, est dit groupe symétrique de E.

Si E est fini, de cardinal $n \geq 1$, on note S_n le groupe symétrique de E, les éléments de S_n sont appelés des permutations de E.

Théorème 2.1

Soit E un ensemble fini, de cardinal n, $n \in \mathbb{N}$: $(S_n, \circ)$ est un groupe d'ordre $n!$, pour $n \geq 3$, ce groupe n'est pas commutatif.

Preuve.

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

Soit $n \geq 3$. Pour montrer que S_n est non commutatif, il suffit d'exhiber deux éléments $\sigma, \tau \in S_n$, tels que $\tau \circ \sigma \neq \sigma \circ \tau$. Prenons par exemple :

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

Alors :

$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & ... & n \\ 3 & 2 & 1 & 4 & ... & n \end{pmatrix} \neq \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & ... & n \\ 1 & 3 & 2 & 4 & ... & n \end{pmatrix}$. ■

Théorème 2.2 *(de cayley)*

Tout groupe fini d'ordre n est isomorphe à un sous-groupe de S_n.

Preuve.

Soit G un groupe d'ordre n, noté multiplicativement et d'élément neutre e.

Soit $t_a : \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & ax \end{array}$, t_a est bijective car l'équation d'inconnu x : $ax = b$, admet une seule solution qui est $a^{-1}b$.

L'application $\phi : \begin{array}{ccc} G & \longrightarrow & S(G) \\ a & \longmapsto & t_a \end{array}$

ϕ est un morphisme de groupes de G dans $S(G)$ On a :

$\forall a, b \in G : \phi(ab) = \phi(a) \circ \phi(b)$.

$\phi(a) = id_G \Longleftrightarrow t_a = id_G \Longleftrightarrow a = e$ donc $\ker(\phi) = \{e\}$.

Alors ϕ est un morphisme injectif.

Il existe donc un morphisme injectif de G dans S_n, G est donc isomorphisme à sous-groupe de S_n. ■

2.2 Groupes monogènes

Définition 2.2

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

$$\langle g \rangle = \{g^m : m \in \mathbb{Z}\} = \left\{..., g^{-2}, g^{-1}, e, g, g^2, ..\right\}.$$

où e désigne l'élément neutre de G. Le groupe G est dit monogène s'il existe g

dans G tel que $G = \langle g \rangle$. S'il en est ainsi, g est appelé générateur de G. Nous disons aussi que G est engendré par g. Un groupe monogène est visiblement abélien.

Exemple 2.1

1. $(U_n, *)$ est monogène car $U_n = \langle w \rangle$ avec $w = e^{2i\pi/n}$.
2. $(\mathbb{C}, +)$ et $(\mathbb{C}^*, \times)$ ne sont pas des groupes monogènes.

Proposition 2.1

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

Preuve.

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

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

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

Théorème 2.3

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

Preuve.

La condition proposée pour que G soit monogène est evidemment suffisante. Montrons qu'elle est nécéssaire. Soient G un groupe monogène et g un générateur de G. Nous avons donc :

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

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

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

Il n'est pas ardu de voir que φ est morphisme de groupes surjectif. Le premier théorème d'isomorphismes assure le fait G est isomorphe au groupe quotient $Z/\ker\varphi$,

où *ker* φ désigne le noyau de φ. Or, comme $\ker\varphi$ est un sous-groupe de $\mathbb{Z}$, il existe $n \in \mathbb{N}$ tel que $\ker\varphi = n\mathbb{Z}$. Par conséquent, G est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ et le problème est résolu. ■

Corollaire 2.1

Un groupe est monogène infini si, et seulement si, il est isomorphe à $\mathbb{Z}$.

Preuve.

Soit G un groupe. Il est évident que si G est isomorphe à $\mathbb{Z}$ alors G est monogène infini. Inversement, supposons que G est monongène infini. D'après théorème précidante, il existe $n \in \mathbb{N}$ tel que G soit isomorphe à $\mathbb{Z}/n\mathbb{Z}$. Mais comme G est infini, $\mathbb{Z}/n\mathbb{Z}$ doit être infini, ce qui donne $n = 0$. Finalment, G est isomorphe à $\mathbb{Z}$. ■

Proposition 2.2

Tout sous-groupe d'un groupe monogène infini est un groupe monogène.

Preuve. Soit G un groupe monogène infini. D'aprés théorème précédente, G est isomorphe à $\mathbb{Z}$ par un isomorphisme φ. Soit H un sous-groupe de G.

Comme φ est un homomorphisme, $\varphi(H)$ est un sous-groupe K de $\mathbb{Z}$. Or tout sous-groupe de $\mathbb{Z}$ est monogène donc comme $H = \varphi^{-1}(K)$, H est monogène . ■

Proposition 2.3

Tout groupe monogène infini possède exactement deux générateurs inverse l'un de l'autre.

Preuve.

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

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

Comme g est un générateur de G, $\varphi_h^{-1}(g)$ est obligatoirement un générateur de $\mathbb{Z}$. Mais les seuls générateurs de $\mathbb{Z}$ sont manifestement 1 et -1. Donc, $g = \varphi_h(1) = h$ ou $g = \varphi_h(-1) = h^{-1}$. Ce qu'il fallait démontrer. ■

2.3 Groupes cycliques

2.3.1 Caractérisation des groupes cyclique

Définition 2.3

On appellera groupe cyclique tout groupe monogéne fini, plus précisement, on dit que G est un groupe cyclique d'ordre n si : $G = \langle g \rangle = \{e, g, g^2, g^3, ..., g^{n-1}\}$.

Il est clair un groupe cyclique est toujours abélien.

Exemple 2.2

1. Pour $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\mathbb{Z}, +) = 1$ est cyclique d'ordre n.
2. Notant $U_n = \{z \in \mathbb{C}^*/z^n = 1\}$, on a $(U_n, \times) < (\mathbb{C}^*, \times)$ cyclique d'ordre n.

Corollaire 2.2

Soient G et G' deux groupes isomorphe. Alors, G est cyclique si et seulement si G' est cyclique.

Preuve.

Soit f l'isomorphisme de G vers G'. Comme f est surjective, si G est cyclique alors G' est cyclique.

Comme f^{-1} est surjective, si G' est cyclique alors G est cyclique. D'où G est cyclique si et seulement si G' est cyclique. ■

Corollaire 2.3

Deux groupes cycliques de même ordre sont isomorphes.

Preuve.

Soient G_1 et G_2 deux groupes cycliques d'ordre n de générateurs respectifs g_1 et g_2. Considérons l'application $f : G_1 \longrightarrow G_2$, définie par :

$$\forall k \geq 0 \begin{cases} f(g_1^k) = g_2^k \text{ si } G_1 \text{ et } G_2 \text{ sont deux groupes multiplicatifs}; \\ f(kg_1) = kg_2 \text{ si } G_1 \text{ et } G_2 \text{ sont deux groupes additifs}; \\ f(g_1^k) = kg_2 \text{ si } G_1 \text{ est un groupe additif et } G_2 \text{ un groupe multiplicatif.} \end{cases}$$

L'application f est clairement un isomorphisme entre G_1 et G_2. ■

Corollaire 2.4

Tout groupe cyclique d'ordre $n > 1$ est isomorphe au groupe additif $\mathbb{Z}/n\mathbb{Z}$.

Preuve.

On sait que le groupe $\mathbb{Z}/n\mathbb{Z}$ (additif) est cyclique d'ordre n (engendré par $\bar{1}$). La conclusion est immédiate d'après le corollaire précédent. ■

Théorème 2.4

Tout groupe fini d'ordre premier est cyclique.

Preuve.

Soit G tel que $|G| = p > 0$, p premier. Soit $x \neq 1$ dans G, alors $|\langle x\rangle|$ divise p et comme $|\langle x\rangle| \neq 1$, $|\langle x\rangle| = p = |G|$, d'oú $\langle x\rangle = G$. On a ainsi montré aussi que tout élément de G, différent du neutre, engendre G. ■

2.3.2 Sous-groupe d'un groupe cyclique

Proposition 2.4

Tout sous-groupe, non réduit à l'élément neutre, d'un groupe cyclique est un groupe cyclique.

Preuve.

D'aprés la corollaire 2.4, il suffit de montrer que si $n \in \mathbb{N}^*$ alors tout sous-groupe de $\mathbb{Z}/n\mathbb{Z}$ est cyclique. Soit alors H un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. L'image réciproque $s^{-1}(H)$ par la surjection canonique s de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$. Il existe alors $m \in \mathbb{N}$ tel que $s^{-1}(H) = m\mathbb{Z}$. La restriction de s à $m\mathbb{Z}$ induit manifestement un morphisme de groupes surjectif de $m\mathbb{Z}$ sur H . Le reste se déduit directement de la proposition 2.1. ■

Théorème 2.5

Soit $G = \langle x\rangle$ un groupe cyclique d'ordre n.

Tout sous-groupe H de G est un groupe cyclique engendré par x^d oú d est le plus petit entier > 0 tel que $x^d \in H$. De plus, d/n et $|H| = n/d$.

Preuve.

Soit H un sous-groupe d'un groupe cyclique $\langle a \rangle$, d'élément neutre noté e avec $H \neq \{e\}$. Si $a^n \in H$, alors $a^{-n} \in H$, donc H contient au moins une puissance positive de a. Notons alors d la plus petite puissance telle que $a^d \in H$. Soit $a^s \in H$. La division euclidienne de s par d donne : $s = qd + r$ avec $0 < r < d$ et q, r éléments de $\mathbb{Z}$. Donc, $a^s(a^{-d})^q = a^r \in H$, ce qui contredit la minimalité de d sauf si $r = 0$. Par suite, les exposants de toutes les puissances de a appartenant à H sont divisibles par d, donc $H = \langle a^d \rangle$. ■

Théorème 2.6

Soit $G = \langle x \rangle$ un groupe cyclique d'ordre n, l'ordre de x^k est $\frac{n}{pgcd(n,k)}$.

Preuve.

Posons $d = pgcd(n, k)$. L'ordre de $\langle x^k \rangle$ est par définition le plus petit entier m tel que $x^{km} = e$. Or dire que $x^{km} = e$ est équivalent à dire que n divise km ou encore que n/d divise m. Le plus petit entier naturel m ayant cette propriété est $m = n/d$. ■

2.3.3 Générateurs d'un groupe cyclique

Théorème 2.7

Soit $G = \langle x \rangle$ un groupe cyclique d'ordre $n \geq 2$. Alors les générateurs de G sont les éléments x^k tels que les entiers k et n soient premiers entre eux.

Preuve.

On a $G = \{e, x, x^2, x^3, ..., x^{n-1}\}$. Soit $k \in \mathbb{Z}^*$ et $H = \langle x^k \rangle$. On a $H = G$ si et seulement si $x \in H$ (puisqu'alors H contient toutes les puissances de x et donc tous les éléments de G). Or :

$x \in H \Leftrightarrow$ il existe $u \in \mathbb{Z}$ tel que $x = x^{ku}$;

$x \in H \Leftrightarrow$ il existe $u \in \mathbb{Z}$ tel que $x^{ku-1} = e$;

$x \in H \Leftrightarrow$ il existe $u \in \mathbb{Z}$ tel que $ku - 1$ est multiple de l'ordre n de x;

$x \in H \Leftrightarrow$ il existe $u, v \in Z$ tel que $ku + nv = 1$.

Cette dernière condition équivaut, d'aprés le théorème de Bezout, au fait que k et n sont premiers entre eux, ce qui achève la preuve. ■

Définition 2.4 (Fonction indicatrice d'Euler)

Pour tout $n \in \mathbb{N}^*$, notons P_n le sous-ensemble de $\{1, 2, ...n\}$ des nombres premiers avec n. Le cardinal de P_n est noté $\varphi(n)$. En posant $\varphi(1) = 1$, nous obtenons une application φ définie de $\mathbb{N}^*$ vers $\mathbb{N}^*$ par :

$$\varphi(n) = card(P_n) \text{ pour tout } n \in \mathbb{N}^*$$

L'application φ est appelée fonction indicatrice d'Euler. Il est clair que si $p \in \mathbb{N}$ est un nombre premier alors $\varphi(p) = p - 1$.

Proposition 2.5

Un groupe cyclique d'ordre $n \in \mathbb{N}$ possède $\varphi(n)$ générateurs.

Preuve.

On peut appliquer directement le théoréme 2.7. En particulier, un groupe cyclique d'ordre premier p possède $p - 1$ générateurs.

Pour poursuivre l'étude de la fonction indictrice d'Euler, nous avons besoin de rappeler certains faits concernant le groupe produit de deux groupes. Soient G et H deux groupes dont les lois sont notées multiplicativement. Nous pouvons définir une loi de composition interne sur le produit cartésien $G \times H$ en posant :

$$(g, h)(\acute{g}, \acute{h}) = (g\acute{g}, h\acute{h}) \text{ pour tout } ((g, h), (\acute{g}, \acute{h})) \in (G \times H)^2.$$

Nous obtenons une structure de groupe sur $G \times H$. En particulier, si e_G désigne l'élément neutre de G et e_H désigne celui de H, le couple (e_G, e_H) est l'élément neutre de $G \times H$. ■

2.4 Groupes Diédraux $\mathbf{D}_n$

On considère dans cette partie le plan affine et euclidien P rapporté à un repère orthonormé $(O, \vec{i}, \vec{j})$ et $P(2)$ les groupes des isométries du plan P.

2.4.1 Isométries du plan

Définition 2.5

Une application $f : P \longrightarrow P$ est une isométrie de P si pour tous $A, B \in P$, on a $f(A)f(B) = AB$.

Les isométries du plan sont :

Les translations :

Les points M et $M^{'}$ se correspondent par la translation qui transforme A et B si :

$$ABM^{'}M \text{ est un parallélogramme ou encore } \overrightarrow{AB} = \overrightarrow{MM^{'}}.$$

Les rotations :

Les points M et $M^{'}$ se correspondent par la rotation de centre O et d'angle θ qui transforme A en B si :

$$\widehat{MOM'} = \widehat{AOB} = \theta \text{ et } OM = OM^{'}.$$

Les symétries axiales :

Les points M et $M^{'}$ sont symétriques par rapport à la droite (d) si :

• Les droites $(MM^{'})$ et (d) sont perpendiculaires.

• M et $M^{'}$ sont situés à égale distance de (d).

Ou encore : (d) est la médiatrice de $\left[M\acute{M}\right]$.

Les symétries centrales :

Les point M et $M^{'}$ sont symétrique par rapport au point O si :

O appartient au segment $\left[MM^{'}\right]$ et $OM = OM^{'}$. Ou encore : O est le milieu de $\left[MM^{'}\right]$.

Pour tout entier $n \geq 2$ on considère un polygone régulier P_n à n sommets, centré en O et tel que l'un de ses sommets soit sur l'axe Ox.

On considère alors D_n l'ensemble des isométries du plan P qui conserve le polygone régulier P_n. Autrement dit, qui conservant globalement l'ensemble de ses n sommets.

Définition 2.6

Pour tout $n \geq 2$, le groupe D_n s'appelle le groupe diédral de degré n.

2.4.2 Générateurs et ordre de D_n

Soit s la symétrie orthogonale d'axe OA_0 et r la rotation de centre O et d'angle $2\pi/n$. Donc

$s(O) = O$ 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 $r(A_{n-1}) = A_0$.

Donc s et r préservent P_n.

Théorème 2.8

Soit $n \in \mathbb{N}$, $n \geq 3$, alors $s, r \in D_n$.

De plus, ordre$(s) = 2$, ordre$(r) = n$, et $s\ r\ s = r^{-1}$.

Preuve.

La première partie de théorème est une conséquence de ce qui précède. Pour ce qui est de la deuxième 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 point du plan donc $r^n = Id$ et $r, r^2, ..., r^{n-1} \neq Id$ donc ordre$(r) = n$ (le fait qu'une rotation d'angle $2\pi/n$ est d'ordre n est un résultat bien connu et que l'on vient de redémontrer).

Maintenant : en posant $A_n = A_0$ on a :

$r\ s\ r\ s\ (A_i) = r\ s\ r\ (A_{n-i}) = r\ s\ (A_{n-i+1}) = r\ (A_{i-1}) = A_i$.

Ainsi $r\ s\ r$ fixe plus de trois points du plan, donc $r\ s\ r\ s = Id$.

D'où la relation $s\ r\ s\ r = Id$. ■

Exemple 2.3

1. Pour n=3 on note D_3 le groupe des isométries d'un triangle équilatéral .

Les éléments de D_3 sont

I =identité.

R_1 = la rotation d'angle $2\pi/3$.

R_2 =la rotation d'angle $4\pi/3$.

V =la symétrie par rapport à l'axe de symétrie vertical.

Δ_1 =la symétrie par rapport à la première diagonale.

Δ_2 =la symétrie par rapport à la deuxième diagonale.

Qui se composent suivant la table :

$\circ$	I	R_1	R_2	V	Δ_1	Δ_2
I	I	R_1	R_2	V	Δ_1	Δ_2
R_1	R_1	R_2	I	Δ_2	V	Δ_1
R_2	R_2	I	R_1	Δ_1	Δ_2	V
V	V	Δ_1	Δ_2	I	R_1	R_2
Δ_1	Δ_1	Δ_2	V	R_2	I	R_1
Δ_2	Δ_2	V	Δ_1	R_1	R_2	I

Ce groupe fait partie d'une suite de groupes $D_n, n \geq 3$.

2. Pour $n = 4$ D_4 le groupe des isométries du carré pour la composition des applications.

Les éléments de D_4 sont :

I =identité.

R_1 = la rotation de centre O et d'angle $\pi/2$.

R_2 =la rotation de centre O et d'angle π.

R_3=la rotation de centre O et d'angle $3\pi/2$.

H =la symétrie par rapport à l'axe de symétrie horisontal.

V =la symétrie par rapport à l'axe de symétrie vertical.

Δ_1 =la symétrie par rapport à la première diagonale.

Δ_2 =la symétrie par rapport à la deuxième diagonale.

Qui se composent suivant la table :

$\circ$	I	R_1	R_2	R_3	H	V	Δ_1	Δ_2
I	I	R_1	R_2	R_3	H	V	Δ_1	Δ_2
R_1	R_1	R_2	R_3	I	Δ_1	Δ_2	V	H
R_2	R_2	R_3	I	R_1	V	H	Δ_2	Δ_1
R_3	R_3	I	R_1	R_2	Δ_2	Δ_1	H	V
H	H	Δ_2	V	Δ_1	I	R_2	R_3	R_1
V	V	Δ_1	H	Δ_2	R_2	I	R_1	R_3
Δ_1	Δ_1	H	Δ_2	V	R_1	R_3	I	R_2
Δ_2	Δ_2	V	Δ_1	H	R_3	R_1	R_2	I

Ce groupe fait partie d'une suite de groupes D_n, $n \geq 3$.

Théorème 2.9

$D_n = \langle r, s \rangle = \{r^k, sr^k \ / 0 \leq k \leq n-1\}$.

Preuve.

Les seules isométries qui préservent P_n sont :

i) Les rotations d'angles $2\pi/n$, 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 $s\ r^{n-k}$. D'où le résultat.

■

Proposition 2.6

Pour $n \geq 2$, D_n est un groupe fini d'ordre $2n$.

2.4.3 Caractérisation de D_n

Proposition 2.7

D_n est non abélien pour $n \geq 3$.

Preuve.

Pour $n = 2$, $D_n = \{e, r_1, s, r_1 \circ s\}$ tel que $r_1 \circ s = s \circ r_1$, donc D_2 est abélien.

Pour $n \geq 3$, $s \circ r \circ s \circ r = 1$, on a $s \circ r \circ s \circ r^{-1} = r^{-2}$.

r^{-2} est différent de 1 car r est d'ordre $n > 2$ donc $s \circ r \circ s \circ r^{-1}$est différent de 1. D'où, s étant d'ordre 2, $(s \circ r)(r \circ s)^{-1} = s \circ r \circ s \circ r^{-1}$ est différent de 1 et par conséquent, $s \circ r$ est différent de $r \circ s$

D_n n'est pas abélien. ■

Remarque 2.1

Pour tout k , $0 \leq k \leq n-1$: $(r_1^k \circ s)^2 = e$ implique $s \circ r_1^k = r_1^{-k} \circ s$ ou $s \circ r_1^k = r_1^{n-k} \circ s$.

Proposition 2.8

D_n contient un sous-groupe cyclique d'ordre 2.

Preuve.

On vérifie facilement que la réflexion s d'axe (OI) avec I d'axe 1 appartient à D_n. s est d'ordre 2 donc $\langle s \rangle$ est un sous-groupe cyclique d'ordre 2 de D_n. ■

Proposition 2.9

D_n contient un sous-groupe cyclique d'ordre n.

Preuve.

Les rotations $r(O, \frac{2ik\pi}{n})$ de centre O et de rayon $\frac{2ik\pi}{n}$, $k = 0, ..., n-1$, appartiennent à D_n. Ces rotations auxquelles on ajoute l'identité, forment un sous-groupe cyclique de D_n d'ordre n, engedré par la retation $r(O, \frac{2\pi}{n})$. ■

Proposition 2.10

Pour tout entier k compris entre 1 et $n-1$: $a\ b^k a = b^{-k}$.

Preuve.

Nous allons procèder par récurrence sur k (compris entre 1 et n) :

Cas $k = 1$: $abab = 1$ donc $aba = b^{-1}$.

Supposons que la prpriété est vrai pour jusqu'à l'entier $k-1$. Alors :

$$\begin{aligned} ab^k a &= ab^{k-1}ba \\ &= ab^{k-1}aaba \text{ car } a \text{ est d'ordre } 2 \\ &= b^{1-k}b^{-1} \text{ par hypothèse de récurrence} \\ &= b^{-k}. \end{aligned}$$

■

Théorème 2.10

Si G est un groupe engendré par deux éléments a et b vérifiant $o(a) = n \geq 2, o(b) = 2$ et

$o(ab) = 2$, alors G est isomorphe à D_n.

Preuve.

Comme $o(a) = n$ on voit que G contient un sous-groupe cyclique d'ordre n qui est $\{e, a, ..., a^{n-1}\}$.

Par ailleurs, comme $o(ab) = 2$, on a $a(bab) = e$ et donc $bab = a^{-1}$ et par suite $ba^k b = ba^k b^{-1} = a^{n-k}$ (puisque $b = b^{-1}$).

On en déduit, comme on l'a fait pour D_n, que les éléments $\{e, a, ..., a^{n-1}, b, ab, ..., a^{n-1}b\}$ sont distinct deux à deux. Comme $G = \langle a, b\rangle$, tout élément de G s'écrit comme un produit formel de puissance de a et b, mais comme $ba^k = a^{n-k}b$, on en déduit par récurrence que tout élément de G s'écrit sous la forme $a^i b^j$ avec $i, j \in \mathbb{Z}$, mais comme $o(a) = n$ et $o(b) = 2$, on voit que l'on peut prendre $i = 0, ..., n-1$ et $j = 0, 1$. Ainsi, on a :

$$G = \left\{e, a, ..., a^{n-1}, b, ab, ..., a^{n-1}b\right\}.$$

On voit alors que l'application $\varphi : G \to D_n$ définie par $\varphi(a^i b^j) = r_1^i \circ s^j$.

Est un isomorphisme de groupe. ■

Chapitre 3

Etude sur les mots et les langages dans un monoïde libre

3.1 Monoïde

Définition 3.1

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 :

i) L'opération T est associative : $\forall\ x,\ y,\ z \in M : (xTy)Tz = xT(yTz)$.

ii) Il existe un neutre (unique) $e \in M$ tel que $\forall x \in M : xTe = eTx = x$.

Remarque 3.1

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

Exemple 3.1

Tout groupe est un monoïde, $(\mathbb{N}, +, 0)$est un monoïde qui n'est pas un groupe.

Définition 3.2

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 $\forall\ i \in I$, $(M_i,\ .,\ e)$ est un sous-monoïde de M, alors $(\bigcap_{i \in I} M_i, ., e)$ 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 3.2

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 3.3

Soit M et N deux monoïdes, un morphisme de M dans N est une application, $\mu : M \longrightarrow N$ qui vérifie :

► $\mu(1_M) = \mu(1_N)$.

► $\mu(x.y) = \mu(x).\mu(y)$ pour tous éléments x et y de M.

Exemple 3.3

L'application $n \longmapsto 2^n$ est un homomorphisme de $(\mathbb{N}, +, 0)$ dans $(\mathbb{N}, \times, 1)$.

3.2 Mot et langage

On introduit dans ce paragraphe quelques définitions, propriétés et notations concernant les mots et langages.

Définition 3.4

On appelle vocabulaire (ou alphabet) un ensemble fini quelconque Σ. Exemple $\lambda = \{\heartsuit, \diamondsuit, \clubsuit, \spadesuit\}$, $\Delta = \{1, 0\}, \Phi = \{\rightarrow, \leftarrow, \uparrow, \downarrow\}$ sont des alphabets.

Les éléments d'un vocabulaire sont appelés lettres, caractéres ou symboles.

Exemple 3.4

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

Définition 3.5

Soit Σ un alphabet. Un mot sur Σ 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 des symboles constituant ce mot, on la note $|w|$. Ainsi, $|abcabb| = 6$ et $|aabc| = 4$. 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 Σ est noté Σ^*. Par exemple : $\{0, 1, 2\}^* = \{\varepsilon, 0, 1, 2, 00, 01, 02, 10, 11, 12, 20, 21, 22, 000, 001, ...\}$ (ε est le mot vide).

Définition 3.6

►Si a est une lettre de l'alphabet Σ, pour tout mot $w = a_1a_2...a_k \in \Sigma^*$, on note par :

$$|w|_a = card\{i \in \{1, 2, ..., k\} : a_i = a\}.$$

le nombre d'occurrences de la lettre a dans le mot w et $w(i)$ sa i-ème lettre. Par exemple $|abcabb|_a = 2$ et $|aabc|_c = 1$, $00110(1) = 0$ et $00110(4) = 1$.

►Fonction de parikh : Soit un alphabet Σ de cardinal $n \geq 1$, et ordonné

($\Sigma = \{a_1, a_2, ..., a_n\}$, avec $a_1 \leq a_2 \leq ... \leq a_n$) : On définit alors la fonction de parikh $\Psi : \Sigma^* \longrightarrow \mathbb{N}^n$ par :

$$\Psi(w) = (|w|_{a_1}, ..., |w|_{a_n}).$$

Le n-uple $\Psi(w)$ est appelé vecteur 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 3.7

Soit $w = a_1a_2...a_k$ un mot sur Σ, 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 qualifie de propre s'il différe 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 différe de w et de 1, l'ensemble des préfixes (resp. suffixes, facteurs) de w est noté $Pref(w)$ (resp. $Suff(w)$, $Fac(w)$).

Proposition 3.1

Soit Σ un alphabet :

1. L'ensemble Σ^* est infini.
2. L'ensemble Σ^* est dénombrable.

Preuve.

1. L'ensemble Σ^* est infini, en effet on a $\Sigma^* = \bigcup_{n=0}^{+\infty} \Sigma^n = \Sigma^0 \cup \Sigma^1 \cup ... \cup \Sigma^n \cup ...$

2. Montrons que Σ^* est dénombrable. Comme Σ est fini, on peut donc numéroter ses éléments, par exemple, si $\Sigma = \{\alpha, \beta, \gamma\}$, alors $n(\alpha) = 1, n(\beta) = 2, n(\gamma) = 3$. Ensuit, soit u un mot Σ^*,on considère les longueur $|u|$ premiers nombre premiers, par exemple si $|u| = 5$, on a les 5 premiers nombre premiers sont : $p(1) = 2$, $p(2) = 3$, $p(3) = 5$, $p(4) = 7$, $p(5) = 11$.

On forme le nombre $f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))}$, oú $u(i)$ désigne la i-ème lettre de u par exemple si $u = \alpha\gamma\beta\alpha\alpha$, alors

$f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))} = \prod_{i=1}^{i=5} p(i)^{n(u(i))} = 2^1 \times 3^3 \times 5^2 \times 7^1 \times 11^1$. Donc on peut définir une application $f : \Sigma^* \longrightarrow \mathbb{N}, u \longmapsto f(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))}$ par l'unicité de la

décomposition d'un entier en facteurs premier, l'application f est injective. Enfin, comme f est injective et l'ensemble $\mathbb{N}$ est dénombrable, alors Σ^* est dénombrable. ■

Définition 3.8

Soit Σ un alphabet. On définit l'opération de concaténation sur Σ^* de la façon suivante :

pour tous mots $w = a_1...a_k$ et $w' = b_1...b_l$, où pour $1 \leq i \leq k$, $1 \leq j \leq l$, $a_i, b_j \in \Sigma$, la concaténation de w et w', notée $w.w'$ ou simplement ww' est le mot :

$$C = c_1c_2...c_{k+1} \text{ où } \begin{cases} c_i = a_i, \text{si } 1 \leq i \leq k \\ c_{k+i} = b_i, \text{si } 1 \leq i \leq l. \end{cases}$$

Ainsi, Σ^* muni de l'opération de concaténation est un monoïde de neutre 1. En particulier, on définit la puissance n-ième d'un mot de w comme la concaténation de n copies de w :

$$w^n = \underbrace{w...w}_{n \text{ fois}}.$$

On pose $w^0 = \varepsilon$.

Remarque 3.2

Si le card $(\Sigma) \geq 2$, alors Σ^* est un monoïde non commutatif, i.e., il existe $u, v \in \Sigma^*$ tels que $uv \neq vu$.

Proposition 3.2

Deux mots u et v commutent s'ils sont puissances d'un même troisième, i.e, s'il existe un mot w et des entiers i, j tels que $u = w^i$ et $v = w^j$.

Preuve.

On procède par récurrence sur la longueur de uv. Si $|uv| = 0$, le résultat est immédiat. Supposons à présent le résultat satisfait pour $|uv| = < n$. Soient u, v tels que $|uv| = n$.

On peut même considèrer que $u \neq 1$ et $v \neq 1$ car sinon, le résultat serait trivial. Si $|u| = |v|$, alors il est immédiat que $u = v$. Sinon, on peut supposer que $|u| < |v|$. Donc il existe $\acute{u}$ tel que $v = u\acute{u}$ et $|\acute{u}| < |v|$. Ainsi, $uv = u\acute{u}u = vu = \acute{u}uu$ et donc

on trouve $\acute{u}u = u\acute{u}$. Puisque $|u\acute{u}| < |uv|$, on peut appliquer l'hypothése de récurence. Il existe un mot w et des entiers p, q tels que $u = wp$ et $\acute{u} = wq$. Pour conclure, on remarque que $v = \acute{u}u = w^{p+q}$. ■

Remarque 3.3

Noter que la réciproque du résultat ci-dessus est trivial.

Proposition 3.3 *(de levy)*

Soient x, y, z, t des mots tels que $xy = zt$, alors il existe un mot w tel que :

($xw = z$ avec $y = wt$) ou ($x = zw$ avec $wy = t$). Il en résulte en particulier que si $|x| = |z|$, le mot w est vide et donc $x = z$ et $y = t$.

Preuve.

Posons $x = a_1a_2...a_n$, $y = a_{n+1}...a_m$ avec $a_i \in \Sigma$ et $1 \leq i \leq m$, de même

$z = b_1b_2...b_k$, $t = b_{k+1}...b_q$ avec $b_i \in \Sigma$ et $1 \leq i \leq q$, comme $xy = zt$, nous avons $m = q$ (mais pas nécessairement $n = k$ et $a_i = b_i$ pour $i = 1, 2, ...m$) de sorte que $z = a_1a_2...a_k$ et $t = a_{k+1}...a_m$. Si $|z| = k \leq n = |x|$, posons $w = a_{k+1}...a_n$, alors $x = zw$ avec $wy = t$.

Si $|z| > |x|$ posons $w = a_{n+1}...a_k$ alors $xw = z$ et $y = wt$. ■

Définition 3.9

Soient $(A, \intercal)$ et (B, Δ) deux monoïdes de neutre respectif e_A et e_B. Une application $f : A \longrightarrow B$ est un morphisme (ou encore homomorphisme) de monoïdes si :

► $\forall x, y \in A : f(x \intercal y) = f(x)\Delta f(y)$.

► $f(e_A) = e_B$.

Exemple 3.5

L'application longueur $|.| : \Sigma^* \to \mathbb{N}$ est un morphisme de monoïdes entre $(\Sigma^*, .)$ et $(\mathbb{N}, +)$. En effet :

$$\forall u, v \in \Sigma^* : |uv| = |u| + |v| \text{ et } |\varepsilon| = 0.$$

Exemple 3.6

Soit $\Sigma = \{a_1, a_2, ..., a_n\}$ un alphabet, $n \in \mathbb{N}\backslash\{0,1\}$.

La fonction de parikh $\Psi : \Sigma^* \longrightarrow \mathbb{N}^n$

$$w \longmapsto \Psi(w) = (|w|_{a_1}, ..., |w|_{a_n})$$

est un morphisme de monoïdes entre $(\Sigma^*, .)$ et $(\mathbb{N}^n, +)$.

Exemple 3.7

Soit $\Sigma = \{a_1, a_2, ..., a_n\}$ un alphabet, $n \in \mathbb{N}\backslash\{0,1\}$ et soit $\lambda : \Sigma \longrightarrow \mathbb{N}$

$$a_i \longmapsto \lambda(a_i)$$

une application.

On définit $\tilde{\lambda} : \Sigma^* \longrightarrow \mathbb{N}$ comme suit :

$$\tilde{\lambda}(w) = \sum_{i=1}^{i=n} \lambda(a_i)|w|_{a_i}.$$

$\tilde{\lambda}$ est un homomorphisme de monoïdes .

Si $\forall 1 \leq i \leq n$, $\lambda(a_i) = 1$ alors $\tilde{\lambda} = |.|$.

►La proposition suivante justifie le fait que le monoïde Σ^* soit appelé monoïde libre.

Cette propriété caractérisé le monoïde libre engendré par Σ.

Proposition 3.4

Toute fonction $\mu : \Sigma \longrightarrow M$ de Σ dans un monoïde M se prolonge de façon unique en un morphisme de Σ^* dans M.

Preuve.

Existence : Posons

$$\tilde{\mu}(1) = e_M \text{ et } \tilde{\mu}(a_1a_2...a_n) = \mu(a_1).\mu(a_2)...\mu(a_n), n \in \mathbb{N}, a_i \in \Sigma, 1 \leq i \leq n.$$

Est facile de voir que $\tilde{\mu}$ est bien un homomorphisme.

Unicité : Soient $\tilde{\mu}$ et $\tilde{\lambda}$ deux homomorphismes de Σ^* dans M tels que :

$\forall a \in \Sigma$, $\tilde{\mu}(a) = \tilde{\lambda}(a)$.

Alors $\tilde{\mu}(1) = \tilde{\lambda}(1) = e_M$ et pour tout mot $w = a_1a_2...a_n$:

$$\begin{aligned}\tilde{\mu}(w) &= \tilde{\mu}(a_1a_2...a_n) \\ &= \mu(a_1).\mu(a_2)...\mu(a_n) \\ &= \tilde{\lambda}(a_1).\tilde{\lambda}(a_2)...\tilde{\lambda}(a_n) \\ &= \tilde{\lambda}(a_1a_2...a_n) \\ &= \tilde{\lambda}(w).\end{aligned}$$

■

Proposition 3.5

Les conditions nécessaires et suffisantes pour qu'un monoïde M soit un monoïde libre

1. il existe un homomorphisme λ de M sur N l'ensemble des entiers positifs avec $\lambda^{-1}(0) = 1$ (1 l'élément neutre de M).
2. quelque soit $f_1, f_2, f_3, f_4 \in M$ tels que $f_1f_2 = f_3f_4$ on a l'une des deux situations suivantes :
   - $\exists f_5 \in M : f_1 = f_3f_5$ et $f_5f_2 = f_4$.
   - $\exists f_6 \in M : f_3 = f_1f_6$ et $f_6f_4 = f_2$.

Exemple 3.8

Soit $X \subseteq \Sigma^*$, le monoïde engendé par X est défini par :
$X^* = \{w = x_1x_2...x_n$,où pour $1 \leq i \leq n, x_i \in X, n \in \mathbb{N}\}$.
Montrons que X^* est un monoïde libre.

1. on définit l'homomorphisme λ comme suite :

$$\begin{array}{rccc}\lambda & : & X^* & \longrightarrow & \mathbb{N} \\ & & W & \longmapsto & |w|\end{array}$$

$\lambda^{-1}(0) = \{1\}$.

2. quelque soit $f_1, f_2, f_3, f_4 \in X^*$ tels que $f_1f_2 = f_3f_4$ d'aprés le lemme de levy on a l'une des deux situations suivantes :

- $\exists f_5 \in X^* : f_1 = f_3 f_5$ et $f_5 f_2 = f_4$.
- $\exists f_6 \in X^* : f_3 = f_1 f_6$ et $f_6 f_4 = f_2$.

Définition 3.10

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

Exemple 3.9

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

Définition 3.11

Soient $L, M \subseteq \Sigma^*$, 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-ième 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 $L^0 = \{1\}$.

Proposition 3.6

La concaténation de langages est une opération associative, elle possède $\{1\}$ pour neutre, $\emptyset$ pour absorbant est distributive à droite et à gauche pour l'union, i.e. si L_1, L_2, L_3 sont des langages on a :

$L_1(L_2 L_3) = (L_1 L_2) L_3$.

$L_1\{1\} = \{1\}L_1$.

$L_1\emptyset = \emptyset L_1 = \emptyset$.

$L_1(L_2 \cup L_3) = (L_1 L_2) \cup (L_1 L_3)$.

$(L_1 \cup L_2)L_3 = (L_1 L_3) \cup (L_2 L_3)$.

Définition 3.12

Soit $L \subseteq \Sigma^*$. L'étoile de Kleene de L est donnée par :

$$L^* = \bigcup_{i \geq 0} L^i$$

On rencontre parfois l'opération L^+ définie par :

$$L^+ = \bigcup_{i \geq 0} L^i, \text{i.e } L^+ = L^* \backslash \{1\}.$$

Exemple 3.10

1. Si $L = \{a\}, a \in \Sigma^*$, $L^* = \{1, a, aa, aaa, ...\}$ et $L^+ = \{a, aa, aaa, ...\}$.
2. Soient les deux langages $L = \{u \in \Sigma^* : |u| \text{ pair}\}$ et $L^{'} = \{u \in \Sigma^* : |u| \text{ impair}\}$.

On a alors les égalités suivantes :
$L + L^{'} = L \cup L^{'} = \Sigma^*$.
$LL^{'} = L^{'} = L^{'}L$.
$LL = L$.
$L^{'}L^{'} = L \backslash \{1\}$.

Proposition 3.7

Soit $L \subseteq \Sigma^*$ un langage, le langage L^* est le plus petit langage M tel que :

$$1 \in M, L \subseteq M \text{ et } M^2 \subseteq M.$$

Définition 3.13

Soit f un morphisme de monoïdes entre A^* et B^* : On remarque que f est complétement caractérisé par les images de f sur les symboles de A, si L est un langage sur A, alors l'image de L par le morphisme f est :

$$f(L) = \{f(u) \in B^* : u \in L\}.$$

de la même manière, si M est un langage sur B, alors l'image inverse de M par le morphisme f est :

$$f^{-1}(M) = \{u \in A^* : f(u) \in M\}.$$

Chapitre 4

Présentations de quelques groupes par générateurs et relations

4.1 Groupes libres

Définition 4.1

a) Soient G un groupe et S une partie de G. Le groupe G est dit libre de base S si tout élément x de G s'écrit de manière unique :

$$x = s_{i_1}^{n_1} ... s_{i_k}^{n_k}$$

avec $k, i_1, ..., i_k \in \mathbb{N}$, $n_1, ..., n_k \in \mathbb{Z}$, $s_{i_1}, ..., s_{i_k} \in S$, tels que $s_{i_j} \neq s_{i_{j+1}}$. Si $k = 0$, on pose $x = 1$.

On dit alors que S est une famille génératrice libre de G, ou encore que S est une base de G.

b) Un groupe G est dit libre s'il possède une base.

c) Si le groupe G possède une base finie, il est dit libre de type fini.

Exemple 4.1 Le groupe $(\mathbb{Z}, +)$ est un groupe libre.

Théorème 4.1

Pour tout ensemble X, il existe un groupe libre $L(X)$ de base X.

Posons $X = \{xi\}_{i\in I}$ et considèrons X^{-1} un ensemble équipotent à X, dont on notera les éléments $x_i^{-1}, i \in I$.

Il est important de noter qu'il s'agit là seulement d'une notation, qui sera commode dans la suite. Les éléments x_i^{-1} ne sont pas les inverses des x_i puisque, pour l'instant, X et X^{-1} ne sont que des ensembles sans aucune structure algébrique. On aurait pu noter cet ensemble équipotent à X par Y et ses éléments par y_i, $i \in I$, mais dans la suite, l'écriture des éléments en aurait été compliquée.

Définition 4.2

a) On appelle mot en $X \cup X^{-1}$ toute suite finie d'éléments de $X \cup X^{-1}$:

$$x = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}, \text{où } \epsilon_i = \pm 1.$$

b) Dans l'écriture ci-dessus, l'entier n est la longueur du mot x, qu'on notera $l(x)$.

c) Deux mots $x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$ et $x_{i_1}^{\gamma_1}...x_{i_k}^{\gamma_k}$ sont des mots égaux si $n = k$ et $\forall p$, $1 \leq p \leq n$, $i_p = j_p$ et $\epsilon_p = \gamma_p$.

►Par convention, il n'existe qu'un seul mot de longueur 0, qu'on notera 1. C'est le mot qui correspond à la suite vide de $X \cup X^{-1}$.

On note $M(X)$ l'ensemble des mots en $X \cup X^{-1}$ et on définit sur $M(X)$ un produit (loi de composition interne) par juxtaposition des mots. Plus précisément, si $x = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$ et $y = x_{i_1}^{\gamma_1}...x_{i_k}^{\gamma_k}$ sont deux mots, alors :

$$xy = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}x_{i_1}^{\gamma_1}...x_{i_k}^{\gamma_k}.$$

►Par convention, on pose $1x = x1 = x$. On remarquera que ce produit est associatif, que 1 est élément neutre, mais que $M(X)$ n'est pas un groupe car tout élément autre que 1 ne peut avoir d'inverse. En effet, pour tout x et y dans $M(X)$, on a $l(xy) = l(x) + l(y)$, donc dès que x ou y est différent de 1, $l(xy) > 0$, et $xy \neq 1$. Pour pallier cet inconvénient, on va définir sur $M(X)$ une relation d'équivalence R telle que $M(X)/R$ soit un groupe pour le produit induit par celui de $M(X)$.

Notation 4.2 *Si x et y sont deux mots adjacents, on écrira xAy.*

Définition 4.3

a) Deux mots x et y de $M(X)$ sont adjacents s'il existe $t_1, t_2 \in M(X)$ et $a \in X \cup X^{-1}$ tels que :

$$x = t_1 t_2 \text{ et } y = t_1 a a^{-1} t_2.$$

ou

$$x = t_1 a a^{-1} t_2 \text{ et } y = t_1 t_2.$$

avec la convention $(a^{-1})^{-1} = a$ pour tout $a \in X \cup X^{-1}$.

b) La relation R est définie sur $M(X)$ par :

$$[xRy] \Leftrightarrow [\exists t_1, ..., t_n \in M(X) \text{ tels que } x = t_1, y = t_n \text{ et } t_i A t_{i+1}, i = 1, ..., n-1].$$

Lemme 4.1

La relation R est une relation d'équivalence.

Preuve.

Pour tout x de $M(X)$ on a xRx, en prenant $a = 1$, la relation est donc réflexive. La relation d'adjacence étant symétrique, on en déduit facilement qu'il en est de même pour la relation R. Soient xRy et yRz , on a :

$$(x = t_1)A...A(t_n = y = t_{n+1})A...At_{n+p} = z$$

d'où xRz et la relation R est transitive. ■

Notation 4.3

Pour tout x de $M(X)$, on notera $[x]$ sa classe dans $M(X)/R$.

Lemme 4.2

La relation R est compatible avec la loi interne de $M(X)$.

Preuve.

Soient x, y, z dans $M(X)$, remarquons que $x\ A\ y$ implique que $xz\ A\ yz$. En effet, si $x = t_1 t_2$ et $y = t_1 a a^{-1} t_2$, alors $xz = t_1(t_2 z)$ et $yz = t_1 a a^{-1}(t_2 z)$. Par conséquent, si $(x = t_1)A...At_n$, alors $(xz = t_1 z)A...A(t_n z = yz)$, ce qui prouve que la relation R

est compatible à droite avec la loi de $M(X)$. Un raisonnement analogue montre la compatibilité à gauche. ■

Lemme 4.3

L'ensemble $M(X)/R$ est un groupe pour la loi induite par celle de $M(X)$.

Preuve.

D'après la remarque 1.6, on sait que la loi interne de $M(X)/R$ induite par celle de $M(X)$ est associative et possède un élément neutre. Il suffit donc de montrer que tout élément $[x]$ possède un inverse. Considèrons d'abord le cas où $x \in X \cup X^{-1}$, il est clair que $xx^{-1}R\ 1$, car en prenant $t_1 = t_2 = 1$, on a $xx^{-1} = t_1xx^{-1}t_2$ et $1 = t_1t_2$, d'où $xx^{-1}\ A\ 1$. De la même manière, $x^{-1}xR1$. On en déduit donc que :

$$\forall x \in M(X), [x]^{-1} = [x^{-1}].$$

La projection canonique $\pi : M(X) \to M(X)/R$ vérifie :

$$\pi(xy) = [xy] = [x][y] = \pi(x)\pi(y).$$

Donc, pour tout $x = x_{i_1}^{\epsilon_1}...x_{i_n}^{\epsilon_n}$, $\epsilon_i = \pm 1$, $[x]$ est inversible et a pour inverse :

$$[x]^{-1} = ([x_{i_1}^{\epsilon_1}]...[x_{i_n}^{\epsilon_n}])^{-1} = [x_{i_n}^{\epsilon_n}]^{-1}...[x_{i_1}^{\epsilon_1}]^{-1} = [x_{i_n}^{-\epsilon_n}]...[x_{i_1}^{-\epsilon_1}] = [x_{i_n}^{-\epsilon_n}...x_{i_1}^{-\epsilon_1}].$$

■

Définition 4.4

Un mot x de $M(X)$ est réduit si $x = 1$ ou $x = a_1...a_n$, avec $a_i \in X \cup X^{-1}$ tels que $a_{i+1} \neq a_i^{-1}, i = 1, ..., n-1$.

propriétie 4.1

Chaque classe d'équivalence de $M(X)$ pour la relation R contient un mot réduit et un seul.

Preuve.

L'existence est évidente, car si x est non réduit, il existe un mot u tel que xAu et $l(u) < l(x)$. Comme la fonction l est à valeurs positive ou nulle, en un nombre fini

d'étapes on arrive à un mot réduit.

Pour montrer l'unicité, on introduit la construction suivante : pour tout $x = x_1...x_n$ de $M(X)$ on définit des éléments u_i de la façon suivante :

$u_0 = 1$,

$u_1 = x_1$,

$u_2 = x_1x_2$ si $x_1 \neq x_2^{-1}$ et $u_2 = 1$ sinon.

Et de façon générale, on pose $u_{i+1} = u_ix_{i+1}$ si le dernier terme de u_i est différent de x_{i+1}^{-1}, $u_{i+1} = u_{i-1}$ sinon.

Par définition, chaque mot u_i est réduit et $u_iR(x_1...x_i)$. De plus si x est réduit, alors $x = u_n$.

On appelle u_n la forme réduite de x, qu'on note $r(x)$. ■

Lemme 4.4

Si deux mots sont adjacents leurs formes réduites sont égales.

Preuve.

Soient $x = x_1...x_kx_{k+1}...x_n$ et $y = x_1...x_kaa^{-1}x_{k+1}...x_n$ deux mots adjacents. Alors les suites u_i et v_i respectivement associées sont telles que $u_0 = v_0, ..., u_k = v_k$. Montrons que $u_k = v_{k+2}$.

-Si le dernier terme de u_k est différent de a^{-1} alors :

$$u_k = v_k, v_{k+1} = v_ka, v_{k+2} = v_k = u_k.$$

-Si le dernier terme de u_k est a^{-1}, on a $u_k = ta^{-1}$ et, u_k étant réduit, le dernier terme de t est différent de a, donc :

$$u_k = v_k, v_{k+1} = t, v_{k+2} = ta^{-1} = u_k.$$

On en déduit que pour tout $j \geq 0, u_{k+j} = v_{k+2+j}$ et $u_n = v_{n+2}$, d'où $r(x) = r(y)$. ■

Lemme 4.5

Deux mots équivalents et réduits sont égaux.

Preuve.

Soient x et y deux mots réduits tels que xRy. Il existe $t_1, ..., t_n$ tels que $x = t_1$,

$y = t_n, t_i A t_{i+1}, 1 \leq i \leq n-1$. En considérant la forme réduite de chaque t_i et en appliquant le lemme précédent, on a :

$$x = r(t_1) = ... = r(t_n) = y,$$

d'où le lemme. ■

►En notant L_X l'ensemble des mots réduits correspondants à chaque classe de $M(X)/R$ et en considérant la loi interne définie sur L_X par $(r(x), r(y)) \to r(xy)$, on obtient un groupe dans lequel tout élément x s'écrit de manière unique :

$$x = x_{i_1}^{n_1} ... x_{i_k}^{n_k}$$

avec $i_1, ..., i_k \in \mathbb{N}$, $n_1, ..., n_k \in \mathbb{Z}, x_{i_1}, ..., x_{i_k} \in X$, tels que $x_{i_j} \neq x_{i_{j+1}}$.

D'autre part, l'application qui à un élément de $M(X)/R$ associe l'unique mot réduit qu'il contient, induit un isomorphisme de groupes de $M(X)/R$ sur L_X. Ceci achève la démonstration du théorème 4.1.

Remarque 4.1

a) Si $X = \{x\}$, alors $L(X)$ est un monogène infini engendré par x, donc $L(X)$ est isomorphe à $\mathbb{Z}$.

b) Si $card(X) > 1$, alors $L(X)$ est un groupe non abélien.

En effet, soient x et y dans X tels que $x \neq y$. Alors $xyx^{-1}y^{-1}$ est un mot réduit différent de 1, car de longueur 4. Donc xy est différent de yx dans $L(X)$.

Théorème 4.4 *(propriété universelle du groupe libre).*

Soient G un groupe, S une partie génératrice de G et $i : S \to G$ l'inclusion canonique. Alors le groupe G est libre de base S si et seulement si, pour tout groupe G' et pour toute application $\sigma : S \to G'$, il existe un unique morphisme de groupes $f : G \to G'$ tel que $f \circ i = \sigma$.

Preuve.

Supposons que $G = L(S)$, tout élément x de $L(S)$ s'écrivant de manière unique $x = s_{i_1}^{n_1}...s_{i_k}^{n_k}$, on pose :

$$f(x) = \sigma(s_{i_1})^{n_1}...\sigma(s_{i_k})^{n_k},$$

et $f(1) = 1_G$. Il est clair qu'on définit ainsi un morphisme de groupes $f : L(S) \to G$ vérifiant $f \circ i = \sigma$. De plus, si f' est un autre morphisme de groupes vérifiant $f' \circ i = \sigma$, pour tout x de $L(S)$ on a $f(x) = f'(x)$, d'où l'unicité.

Réciproquement, considérons un couple (G, i) vérifiant l'énoncé ci-dessus. On applique alors cet énoncé avec, pour couple (G', σ), le couple $(L(S), j)$, où $j : S \to L(S)$ est l'inclusion canonique.

Il existe un unique morphisme $g : G \to L(S)$ tel que $g \circ i = j$. D'autre part, on sait qu'il existe un morphisme de groupes $f : L(S) \to G$ prolongeant l'identité de S. En notant $f_{|S}$ et $g_{|S}$ les restrictions de f et g à S, on déduit de ce qui précède que $g \circ f_{|S} = id_S$ et $f \circ g_{|S} = id_S$, d'où $f \circ g = id_G$ et $g \circ f = id_{L(S)}$. Par conséquent les groupes G et $L(S)$ sont isomorphes et, puisque $f(S) = S$, G est libre de base S. ■

Corollaire 4.1

Deux groupes libres de base un même ensemble S sont isomorphes par un unique isomorphisme prolongeant l'identité de S.

Preuve.

Soient G et G' deux groupes libres de bases S. D'aprés le théorème 4.4, il existe un unique morphisme de groupes $f : G \to G'$ tel que $f_{|S} = id_S$ et un unique morphisme de groupes $g : G' \to G$ tel que $g_{|S} = id_S$. On en déduit que $f \circ g = id_G$ et $g \circ f = id_G$.
■

Remarque 4.2

On peut donc parler du groupe libre engendré par S.

Théorème 4.5

Deux ensembles X et Y sont équipotents si et seulement si les groupes libres $L(X)$ et $L(Y)$ sont isomorphes.

Définition 4.5

Si G est un groupe libre, le cardinal d'une partie génératrice libre de G est appelé le rang de G.

Remarque 4.3

Deux groupes libres sont isomorphes si et seulement s'ils ont même rang.

Plus généralement, deux symboles distincts engendrent toujours un groupe libre de rang 2.

Théorème 4.6

Tout groupe est isomorphe à un quotient d'un groupe libre.

Preuve.

Soient G un groupe, S une partie génératrice de G et $i : S \to G$ l'injection canonique. D'après le théorème 4.4, il existe un morphisme de groupes $f : L(S) \to G$ tel que $f_{|S} = id_S$. On a donc $G = S = f(S)$ et f est surjective. On en déduit que G est isomorphe à $L(S)/Ker(f)$. ■

Théorème 4.7

Tout sous-groupe d'un groupe libre est libre.

►Attention. Si G est un groupe libre (même de rang fini) et si H est un sous-groupe de G, il n'existe aucune relation a priori entre le rang de G et celui de H.

4.2 Générateurs et relations

Définition 4.6

Si S est une partie d'un groupe G, le sous-groupe normal de G engendré par S, qu'on notera (S), est l'intersection de tous les sous groupes normaux de G contenant S.Si $S = \emptyset$, on pose $(S) = \{1\}$, où 1est l'élément neutre de G.

►En général, si G est un groupe engendré par une famille $X = \{x_i\}_{i \in I}$, les générateurs x_i sont liés par des relations.

Exemple 4.2

Si $G = x$ est cyclique d'ordre n, le générateur x vérifie la relation $x_n = 1$.

►Une relation liant les générateurs $x_i, i \in I$, peut s'écrire sous la forme $r = 1$, où r est un élément du groupe libre $L(X)$.

Définition 4.7

Soit G un groupe engendré par un ensemble d'éléments $X = \{x_i\}_{i\in I}$, ces éléments vérifiant un ensemble de relations $R = \{r_k = 1_G\}_{k\in K}$.On dit que $\langle X|R\rangle$ est une présentation de G par générateurs et relations si G est isomorphe au groupe $L(X)/(R)$, où (R) est le sous-groupe normal du groupe libre $L(X)$, engendré par les $\{r_k\}_{k\in K}$.

Exemple 4.3

1. Pour tout ensemble X, $\langle X|\emptyset\rangle$ est une présentation du groupe libre $L(X)$.
2. $\langle x|x^n\rangle$ est une présentation du groupe cyclique d'ordre n.

Remarque 4.4

Lorsqu'on donne une présentation d'un groupe G par générateurs et relations, $G = \langle X|R\rangle$, il est utile de supprimer des ensembles X et R les éléments qui sont clairement redondants.

Proposition 4.1

Soient $G = \langle X|R\rangle$ et G' un groupe. Pour définir un morphisme de groupes

$f : G \to G'$, il suffit de définir $f(x)$ pour $x \in X$ et de vérifier que, pour tout r de R, $f(r) = 1_G$.

Preuve.

La donnée des $f(x)$ pour $x \in X$ induit, d'après le théorème 4.4, un morphisme (qu'on notera encore$f$) de $L(X)$ dans G'. Si pour r parcourant R, $f(r) = 1_{G'}$ alors, d'aprés le théorème 1.5, f induit un morphisme de groupes $L(X)/(R) \to G'$. En composant avec l'isomorphisme $G \cong L(X)/(R)$, on obtient un morphisme de groupes $G \to G'$. ■

Remarque 4.5

Soit G un groupe présenté par générateurs et relations, $G = \langle X|R\rangle$, et soit

$f : G \to G'$ un morphisme de groupes. Montrer que le morphisme f est injectif (i.e.$f(x) = 0 \Leftrightarrow x \in (R)$) est équivalent à déterminer toutes les relations existantes

dans G, liant les générateurs. C'est en général trés difficile à faire directement et par fois impossible. Par conséquent, si l'on souhaite montrer que f est un isomorphisme (ce qui est le cas lorsqu'on veut montrer que G est une présentation par générateurs et relations d'un groupe donné G'), il faudra souvent, soit définir un morphisme réciproque, soit montrer, dans le cas où les groupes sont finis, que f est surjectif et que G et G' ont même ordre.

►Attention. On prendra garde au fait qu'un groupe peut admettre plusieurs présentations par générateurs et relations.

4.3 Présentation d'un groupe monogène d'ordre infini

Théorème 4.8

Pour $n \in \mathbb{N}^*$, $\langle x \backslash \emptyset \rangle$ est une présentation du groupe monogène d'ordre infini.

Preuve.

Soit L_X le groupe libre sur $X = \{x\}$ est égale à $\{x^n,\ p \in \mathbb{Z}\}$, isomorphe à $\mathbb{Z}$, et H le sous-groupe normale de L_X engendré par l'ensemble vide, $R = \{\emptyset\}$ c'est-à-dire $H = \{1_{L_X}\}$.

On montrons que le groupe quotient L_X/H est isomorphe au groupe monogène d'ordre infini.

Pour montre que $L_X/H \cong H$ il suffit de vérifier que l'ordre de $\bar{x}$ est infini.

On sait que si $L_X = \langle x \rangle$, alors $L_X/H = \langle \bar{x} \rangle$.

On considère l'application :

$$\begin{array}{rccc} f: & X & \longrightarrow & \mathbb{Z} \\ & x & \longmapsto & 1 \end{array}$$

D'aprés la propriété universelle d'un groupe libre, f se prolonge en $\varphi : L_X \longrightarrow \mathbb{Z}$, φ est un morphisme de groupe, et $\ker \varphi$ sous-groupe normal de L_X.

On suppose que $o(\bar{x}) = n$, $n \in \mathbb{N}^*$:

$$\varphi(x^n) = n(\varphi(x)) = n.1 = 0.$$

Donc :

$$\begin{aligned} \{x^n\} &\subseteq \ker\ \varphi \Longrightarrow H \subseteq \ker\ \varphi. \\ x^n &\in H \Longrightarrow (\bar{x})^n = 1_{L_X/H} \text{ c'est-à-dire } x \in H. \end{aligned}$$

Comme $H \in \ker\ \varphi$, alors $\varphi(x) = 0$, contradiction.

Finalement $o(\bar{x})$ est infini et $L_X/H \cong \mathbb{Z}$. ■

4.4 Présentation d'un groupe cyclique d'ordre n

Théorème 4.9

Pour $n \in \mathbb{N}^*$, $\langle x \backslash x^n \rangle$ est une présentation du groupe cyclique d'ordre n engendré par x.

Preuve.

Soit $L(X)$ le groupe libre sur $X = \{x\}$ est égale à $\{x^p, p \in \mathbb{Z}\}$, isomorphe à $\mathbb{Z}$, et H le sous-groupe normale de $L(X)$ engendré par $R = \{x^n\}$ est $\{x^{np}, p \in \mathbb{Z}\}$.

On montre que le groupe quotient $L(X)/H$ est isomorphe au groupe cyclique $\mathbb{Z}/n\mathbb{Z}$ d'ordre n.

Pour montre que $L(X)/H \cong \mathbb{Z}/n\mathbb{Z}$ il suffit de vérifier que $o(\overline{x}) = n$.

On sait que si $L(X) = \langle x \rangle$, alors $L(X)/H = \langle \overline{x} \rangle$.

On considère l'application :

$$\begin{array}{rccc} f & : & X & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ & & x & \longmapsto & \overline{1} \end{array}$$

D'aprés la propriété universelle d'un groupe libre, f se prolonge en :

$$\varphi : L(X) \longrightarrow \mathbb{Z}/n\mathbb{Z}$$

φ est un morphisme de groupe, et $\ker \varphi$ sous-groupe normale de $L(X)$, et :

$$\varphi(x^n) = n(\varphi(x)) = n.\overline{1} = \overline{0}.$$

Donc :

$$\{x^n\} \subseteq \ker\varphi \Longrightarrow H \subseteq \ker\varphi.$$

$$\text{On a } x^n \in H \Longrightarrow (\overline{x})^n = 1_{L(X)/H}$$

Maintenant on montre que :

$$\forall 1 \leq k < n, (\overline{x})^k \neq 1_{L(X)/H}.$$

$$\text{On a } \varphi(x^k) = k.\varphi(x) = k.\overline{1} \neq \overline{0}.$$

$$x^k \notin \ker\varphi \Longrightarrow x^k \notin H \Longrightarrow (\overline{x})^k \neq 1_{L(X)/H}.$$

Donc $o(\overline{x}) = n$ est $L(X)/H$ est cyclique d'ordre n est $L(X)/H \simeq \mathbb{Z}/n\mathbb{Z}$. ■

4.5 Présentation de groupe diédral D_n

Théorème 4.10

$(\{a,\ b\}\,|a^n, b^2, abab)$, *avec* $a \neq b$ *et* $n \geq 2$ *dans* $\mathbb{N}$ *; est une présentation du groupe diédral* D_n.

Preuve.

Soit $L = L_{\{a,b\}}$ le groupe libre engendré par $\{a, b\}$, et H le sous-groupe normale de L engendré par $R = \{a^n, b^2, abab\}$, c'est-à-dire l'intersection de tous les sous-groupes normaux de L contenant R.

Pour $x \in L$, on note $\bar{x}$ la classe dans le groupe quotient L/H.

L engendré par a et b, L/H engendré par $\bar{a}$ et $\bar{b}$.

Pour montre que $L/H \simeq D_n$, il suffit de vérifier que, dans ce groupe quotient, $\bar{a}$ est d'ordre n, $\bar{b}$ est d'ordre 2, $\overline{ab}$ est d'ordre 2.

Puisque $a^n \in H$, on a évidemment $\bar{a}^n = 1_{L/H}$ et $\bar{b}^n = 1_{L/H}$ et $abab \in H$, on a $\overline{abab} = 1_{L/H}$

1. Montrons que $o(\bar{a}) = n$.

Considérons l'application :

$$f : \{a, b\} \longrightarrow D_n$$

Définie par :

$$f(a) = r(O, \frac{2\pi}{n}) \text{ et } f(b) = s$$

où $r(O, \frac{2\pi}{n})$ est la rotation de centre O et d'angle $\frac{2\pi}{n}$ et s est la symétrie d'axe (OA_0).Grâce à la propriété universelle du groupe libre L, on sait que f peut être prolongée en un unique morphisme

$$\varphi : L_{\{a,b\}} \longrightarrow D_n$$

Son noyau $ker\ \varphi$ est alors un sous-groupe normal de $L_{\{a,b\}}$ et :

$$\varphi(a^n) = r^n = id$$

$$\begin{aligned} \text{donc } \{a^n\} &\subseteq \ker\varphi, \text{ alors } H \subseteq \ker\varphi \\ a^n &\in H \Longrightarrow \bar{a}^n = 1_{L/H}. \end{aligned}$$

De plus, $\forall 1 \leq k \leq n, \varphi\left(a^k\right) = r^k \neq id$ alors $a^k \notin \ker\varphi \Longrightarrow a^k \notin H$ ce qui prouve que $\bar{a}^n \neq 1_{L/H}$. Ainsi, $\bar{a}$ est bien d'ordre n.

2. Montrons que $o(\bar{b}) = 2$.

Considérons l'application :

$$f : \{a, b\} \longrightarrow D_n$$

Définie par :

$$f(a) = r(O, \frac{2\pi}{n}) \text{ et } f(b) = s$$

où $r(O, \frac{2\pi}{n})$ est la rotation de centre O et d'angle $\frac{2\pi}{n}$ et s est la symétrie d'axe (OA_0).

Grâce à la propriété universelle du groupe libre L, on sait que f peut être prolongée en un unique morphisme :

$$\varphi : L_{\{a,b\}} \longrightarrow D_n$$

Son noyau ker φ est alors un sous-groupe normal de $L_{\{a,b\}}$ telle que

$$\varphi(b^2) = s^2 = id$$

$$\begin{aligned} \text{donc } \left\{b^2\right\} &\subseteq \ker\ \varphi, \text{ alors } H \subseteq \ker\ \varphi \\ b^2 &\in H \Longrightarrow \bar{b}^2 = 1_{L/H}. \end{aligned}$$

De plus :

$$\begin{aligned} \text{pour } k &= 1,\ \varphi(b) = s \neq id \\ \text{alors } b &\notin \ker\ \varphi \Longrightarrow b \notin H \end{aligned}$$

ce qui prouve que $\bar{b} \neq 1_{L/H}$.

Ainsi, $\bar{b}$ est bien d'ordre 2.

3. Montrons que $o(\bar{b}) = 2$.

Considérons l'application :

$$f : \{a, b\} \longrightarrow D_n$$

Définie par :

$$f(a) = r(O, \frac{2\pi}{n}) \text{ et } f(b) = s$$

où $r(O, \frac{2\pi}{n})$ est la rotation de centre O et d'angle $\frac{2\pi}{n}$ et s est la symétrie d'axe (OA_0).

Grâce à la propriété universelle du groupe libre L, on sait que f peut être prolongée en un unique morphisme

$$\varphi : L_{\{a,b\}} \longrightarrow D_n$$

Son noyau $\ker\ \varphi$ est alors un sous-groupe normal de $L_{\{a,b\}}$ telle que :

$$\varphi(abab) = id$$

$$\begin{aligned} \text{donc } \{abab\} &\subseteq \ker\ \varphi, \text{ alors } H \subseteq \ker\ \varphi \\ abab &\in H \Longrightarrow \overline{abab} = 1_{L/H}. \end{aligned}$$

De plus :

$$\begin{aligned} \text{pour } k &= 1,\ \varphi(ab) \neq id \\ \text{alors } ab &\notin \ker\ \varphi \Longrightarrow ab \notin H \end{aligned}$$

ce qui prouve que $\overline{ab} \neq 1_{L/H}$.

Ainsi, $\overline{ab}$ est bien d'ordre 2. ■

Conclusion

Dans ce mémoire, on s'intéresse à l'étude de la présentation de quelques groupes via un quotion d'un groupe libre.

Nous avons présenté dans le premier temps les définitions et quelques propriétés sur les notions du groupes.

ensuite nous avons etuder les groupes symétriques, monogénes, cycliques et les groupes diédraux.

Nous avons etuder aussi les mots et les langages dans un monoïde libre.

Finalement nous avons présenté la notion de groupe libre sur un ensemble X, et nous avons donné la présentation par générateurs et relations des groupes suivants :

Présentation d'un groupe monogéne d'ordre infini.

Présentation d'un groupe cyclique d'ordre n.

Présentation de groupe diédral D_n.

Bibliographie

[1] L. Bélair, F. Bergeron et C. Hohlweg. "Introduction à la théorie des groupes-en cours de rédaction", Université du Québec à Montréal, (2016).

[2] L. Bélair et C. Hohlweg. "Algèbre II", (2016).

[3] K. Boulabiar. "Cours d'algèbre M118", Université de Tunis.

[4] J. Calais," Eléments de théorie des groupes", Presses Universitaires de France, 1984.

[5] F. Dumas. "Algèbre : groupes et anneaux 1", Université Blaise Pascal, (2007).

[6] N. Ghadbane. "Etude sur les groupes syntaxiques de petits degrés", Mémoire de magistère Université Mohamed boudiaf-M'sila, (2010).

[7] D.Guin et T. Hausberger. "Algèbre 1, Groupes, Corps et Théorie de Galois", EDP Sciences, (2008).

[8] J-P. Marco et L. Lazzarini. "Mathématiques L1, cours et exercices corrigés", Pearson Education France, (2007).

[9] J-P. Marco, P. Thieullen et J-A. Weil. "Mathématiques L2, cours et exercices corrigés", Pearson Education France, (2007).

[10] K. Moussoud. "Présentation de quelques groupes via un quotient d'un groupe libre", Mémoire de mastre Université Mohamed boudiaf-M'sila, (2014).

[11] M. Rigo. "Théorie des automates et langages formels", Université de Liège, (2009).

[12] D. Schaub. "Eléments de la théorie des groupes", Université d'Angers, (1997).

ملخص:

في هذا العمل نعطي أولا مفاهيم عامة حول الزمر، الزمر الدورية، الزمر الأحادية المنشأ، زمر التقايسات التي تحافظ على مضلع منتظم. بعد ذلك قمنا بدراسة حول الزمر الحرة والان نضع التركيز على الخاصية المميزة والتي تسمح بالبرهان على ان كل زمرة مولدة بمجموعة هي متماثلة مع القسمة عن طريق التطابق. ثم نعطي بعض التمثيلات للزمر عن طريق حاصل قسمة زمرة حرة : زمرة أحادية المنشأ غير منتهية، زمرة دورية ذات الرتبة ن، زمرة التقايسات التي تحافظ على مضلع منتظم.

Résumé :

Dans ce travail, on donne tout d'abord des notions générales sur les groupes, groupes monogènes, groupes cycliques et groupes diédraux D_n par la suite, on fait une étude sur le groupe libre en mettant l'accent sur la propriété universelle qui tout groupe engendré par un ensemble X est isomorphe à un quotient notée $L(X)$ via une congruence. On donne ensuite quelques présentations de groupes via un quotient d'un groupe libre : groupe monogène infini, groupe cyclique d'ordre n, groupe diédral D_n.

Mots clés: groupe, groupe monogène, groupe cyclique, groupe diédral, groupe, groupe libre, mot, homomorphisme, présentations des groupes.

Abstract

In this work, one first of all gives general concepts on the groups, monogenes groups, cyclic groups and diédraux D_n groups. Thereafter, one makes a study on the free group by stressing the universal property which any group generated by a unit X is isomorphic wich a quotient note $L(X)$ by a congruence. One gives then some presentations of groups by a quotient of a free group: infinit monogene group, cyclic group of order n, diédral D_n group.

Key words: group, monogene group, cyclic group, diédral group, quotient group, free group, word, homomorphism, presentations of the groups.