UNIVERSITÉ MOHAMED BOUDIAF - M'SILA

MEMOIRE

Présenté à la Faculté des Mathématiques et de l'Informatique

Département de Mathématiques

Pour l'obtention du diplôme de master

Spécialité: Mathématiques

Option: Mathématiques discrètes

Par:

Moussoud Khadidja

Intitulée:

Présentation de quelques groupes Via un quotient d'un groupe libre

Soutenue publiquement le : .../06/2015, devant le jury :

A. AMROUNE	**Prof.**	**Université de M'sila**	**Président**
D. MIHOUBI	**Prof.**	**Université de M'sila**	**Rapporteur**
N. GHADBANE	**M.A.A**	**Université de M'sila**	**Co- Rapporteur**
L. HEBOUB	**M.A.A**	**Université de M'sila**	**Examinateur**

Promotion 2014/2015

Remerciements

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

L'occasion nous tenons à adresser notre sincère remerciement à l'encadreur

Monsieur : MTHOUBI DOUADI, ET GHADBANE NACER pour sa bienveillance, et pour son aide précieux qu'il nous a apportée.

Table des matières

Introduction Générale

La notion de groupe a été introduite pour la première fois au début du dix-neuvième siècle. A cette époque elle intervient dans les travaux d'Evariste Galois sur les équations algébriques sous forme de groupes de 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 siècle la notion abstraite de groupe et que petit à petit a été construite la théorie de groupes.

Dans la théorie de groupe une place importante a été accordée à l'étude de la structure des groupes fini compte tenu des nombreuses interprétations concrètes qui peuvent en être données [4] .

C'est précisément dans ce cadre que se place ce mémoire dans lequel ont été traités les groupes, les groupes cycliques, les groupes monogènes, les groupes Diédraux D_n, les groupes libres, et quelques présentations de groupes.

Ce travail est composé de trois chapitre:

▶ Le premier chapitre consiste en un rappel des notions et notations utilisées par la suite: La structure du groupe, les groupes monogènes, les groupes cycliques, les groupes Diédraux D_n.

▶ Dans le second chapitre nous avons introduit la notion de groupe libre sur un ensemble X et la propriété universelle d'un tel groupe F_X nous a permis de montrer que tout groupe engendré par un ensemble X est isomorphe à un quotient de F_X .

▶ Dans le troisième chapitre nous avons fait quelques présentation de groupes: Présentation d'un groupe monogène d'ordre infini, Présentation d'un groupe cyclique d'ordre n et présentation de groupe diédral D_n.

Chapitre 1

Préliminaires

Ce premier chapitre contient les définitions et les propriétés des objets que nous utiliserons par la suite :

Généralités sur les groupes; les groupes monogènes; les groupes cycliques; les groupes Diédraux D_n.

1.1 Généralités sur les groupes

Définition 1.1.1

Soit M un ensemble et $* : M \times M \to M$ une opération binaire interne et partout définie. L'ensemble M muni de l'opération $*$ possède une structure de monoïde si les propriétés suivantes sont satisfaites

1. *L'opération $*$ est associative* : $\forall x, y, z \in M : (x * y) * z = x * (y * z)$.
2. *Il existe un neutre (unique) $e \in M$ tel que* : $\forall x \in M : x * e = e * x = x$.

Exemple 1.1.1

- *$P(E)$ est un monoïde on pour l'union et l'intersection.*
- *Soit E un ensemble, l'ensemble E^E des application de E vers E, $\left(E^E,\ Id_E,\ \circ\right)$ est un monoïde.*

Définition 1.1.2 *Soient* $(M, *)$ *et* (N, ∇) *deux monoïdes de neutre respectif* e_M *et* e_N. *Une application* $f : M \to N$ *est un morphisme de monoïdes si* :

1. $\forall x, y \in M^2 : f\ (x * y) = f\ (x) \nabla f\ (y)$.
2. $f\ (e_M) = e_N$.

Exemple 1.1.2

- *Pour tout monoïde* $(M,\ *,\ e_M)$ *la fonction identique* : $Id_M : M \to M$ *est morphisme de* $(M,\ *,\ e_M)$ *de lui - même.*
- *On note* $P = \{2^n,\ n \in \mathbb{N}\}$, *l'application* $f : (\mathbb{N},\ +) \to (P,\ \times)$ *définie par* $f\,(n) = 2^n$ *est un morphisme de monoïde.*

Définition 1.1.3

Un groupe est la donnée d'un ensemble non vide G *et d'une loi de composition interne*

$$G \times G \to G$$
$$(x,\ y) \mapsto x * y$$

Vérifiant les propriétés suivantes :

1. *la loi* $*$ *est associative* : $\forall x, y, z \in G, (x * y) * z = x * (y * z)$
2. *il existe un élément neutre* $e \in G$: $\forall x \in G, x * e = e * x = x$
3. *tout élément possède un symétrique* : $\forall x \in G, \exists \bar{x} \in G$ *telque* $x * \bar{x} = \bar{x} * x = e$.

   Si de plus la loi $*$ *est commutative c'est à dire* : $\forall\ x,\ y \in G,\ x * y = y * x$.

   On dit alors que $(G,\ *)$ *est un groupe commutatif ou Abélien.*

Exemple 1.1.3

- *Si* E *est un ensemble non vide, l'ensemble* $P(E)$ *est alors un groupe pour l'opération de différence symétrique*: $(A,\ B) \mapsto A \triangle B = (A \cup B) \backslash (A \cap B)$.
- $M_{n \times n}(\mathbb{R}) = \{$*matrices carrées d'ordre* n *à coèfficients dans* $\mathbb{R}\}$ *muni de l'addition des matrices est un groupe Abélien.*

Proposition 1.1.1 *Soit $(G, *)$ un groupe alors on a les propriétés suivantes* :

1. *Le groupe G non vide.*
2. *L'élément neutre est unique.*
3. *Tout élément possède un unique symétrique.*
4. *Le groupe G est régulier à gauche et à droite* :

$$\forall\ x,\ y,\ z \in G,\ z * x = z * y \Rightarrow x = y \text{ et } x * z = y * z \Rightarrow x = y.$$

Définition 1.1.4 *Soit $(G, *)$ un groupe et soit $H \subset G$ une partie de G. La partie H est un sous-groupe de G si et seulement si les conditions suivantes sont satisfaites* :

1. L'élément neutre e_G appartient à H
2. Pour tout x, y d'éléments de H, $x * y$ appartient à H (H est stable par la loi $*$)
3. Pour tout x appartient à H le symétrique de x par $*$ est dans H.

Notation 1.1.1 *Si H est un sous-groupe de G, on notera $H < G$.*

Proposition 1.1.2 *Soit G un groupe et H un sous-ensemble non-vide. Les assertions suivantes sont équivalentes* :

1. *$H < G$.*
2. *$e_G \in H$, $\forall\ x,\ y \in H$, $x * y^{-1} \in H$.*

Exemple 1.1.4

1. *G et $\{1\}$ sont des sous-groupes de G appelés sous-groupes triviaux de G.*
2. *Pour tout groupe $(G, *)$, on considère $Z(G) = \{x \in G,\ \forall\ y \in G,\ x * y = y * x\}$. C'est un sous-groupe de G, appelé le centre de G. En effet,*

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

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

ii) *Soient* $x,\ y \in Z(G)$

Ona $\forall\ z \in G,\ (x\ *\ y^{-1}) * z = (x\ *\ y^{-1}) * (z^{-1})^{-1}$

$$= x * (y^{-1}\ *\ (z^{-1})^{-1})\ car * est\ associative$$

$$= x * (z^{-1} * y)^{-1}\ car\ y \in Z(G)$$

$$= x * (y * z^{-1})^{-1}\ car\ y \in Z(G)$$

$$= x * (z\ *\ y^{-1})$$

$$= (x * z) * y^{-1} car * est\ associative$$

$$= (z * x) * y^{-1} car\ x \in Z(G)$$

$$= z * (x * y^{-1})\ car * est\ associative$$

Ce qui montre que $x * y^{-1} \in Z(G)$.

Définition 1.1.5 *Soit* H *un sous-groupe de* G. *Si* H *est différent de* G *et* $\{1\}$ *on dit que* H *est un sous-groupe* ***propre*** *de* G.

Proposition 1.1.3 *Soit* G *un groupe les propriétés suivantes sont satisfaites* :

1. *Si* G *est un groupe 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.

2. *Une réunion de sous-groupes d'un groupe* G *n'est en général pas un sous-groupe de* G.

Exemple 1.1.5

On vérifiera que $3\mathbb{Z}$ *et* $5\mathbb{Z}$ *sont des sous-groupes de* $\mathbb{Z}$, *ona* $3 \in 3\mathbb{Z} \cup 5\mathbb{Z}$ *et* $5 \in 3\mathbb{Z} \cup 5\mathbb{Z}$ *mais que* $3 + 5 = 8$ *n'appartiennent pas à* $3\mathbb{Z} \cup 5\mathbb{Z}$, *alors* $3\mathbb{Z} \cup 5\mathbb{Z}$ *n'est pas un sous groupe de* $\mathbb{Z}$.

Définition 1.1.6 *Soient* $(G, \cdot)$ *et* $(G', *)$ *deux groupes.* ***Un morphisme*** *(****ou homomorphisme****)* ***de groupes*** *de* G *dans* G' *est une application* $f : G \to G'$ *vérifiant* :

$$\forall\ (x,\ y) \in G^2,\ f(x \cdot y) = f(x) * f(y).$$

Si f *est de plus bijective, on dit que* f *est un* ***isomorphisme*** *du groupe* G *sur le groupe* G'.

Si $G' = G$, on dit que f est un ***endomorphisme*** *du groupe $(G, *)$ et que c'est un* ***automorphisme*** *du groupe $(G, *)$ si est de plus bijective.*

Exemple 1.1.6

L'application **Det** : $(GL_n(\mathbb{R}), \cdot) \to (\mathbb{R}^*, \times)$ *est un homomorphisme de groupes*

$$\forall\ A,\ B \in GL_n(\mathbb{R}),\ Det(A \cdot B) = Det(A) \times Det(B).$$

Notation 1.1.2 *On note* $\mathbf{Hom(G, G')}$ *l'ensemble des morphismes de groupes de G dans G'.*

Remarque 1.1.1 *Si $(G, *)$ et $(G', \bullet)$ sont deux groupes quelconques, et si f est un isomorphisme de G sur G', alors f^{-1} est un isomorphisme de G' sur G.*

Proposition 1.1.4 *Tout élément f de $Hom(G, G')$ vérifie les propriétés suivantes :*

1. $f\ (e_G) = e_{G'}$
2. $f(x^{-1}) = (f\ (x))^{-1}$ *pour tout élément x de G.*
3. $H < G \Rightarrow f\ (H) < G'$
4. $H' < G' \Rightarrow f^{-1}(H') < G$ *avec* $f^{-1}(H') = \{x \in G,\ f(x) \in H'\}$.

Preuve.

1) On a $f(e_G) = f(e_G * e_G) = f(e_G) \bullet f(e_G)$, en multipliant à droite par $f(e_G)^{-1}$ on obtient

$$\begin{aligned} f(e_G) \bullet f(e_G)^{-1} &= f(e_G) \bullet f(e_G) \bullet f(e_G)^{-1} \\ e_{G'} &= f(e_G). \end{aligned}$$

2) Soit $x \in G$ alors $x * x^{-1} = e_G$ donc $f(x * x^{-1}) = f(e_G)$.

Cela entraîne $f(x) \bullet f(x^{-1}) = e_{G'}$, en multipliant à gauche par $(f\ (x))^{-1}$nous obtenons $f(x^{-1}) = (f\ (x))^{-1}$.

3) i) On a $e_G \in H$, donc $e_{G'} = f(e_G) \in f\ (H)$.

ii) Si $x' = f(x)$, $y' = f(y)$ dans $f\ (H)$ avec x, y dans H alors :

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

4) i) On a $e_{G'} = f(e_G) \in H'$, donc $e_G \in f^{-1}(H')$.

ii) Si x, $y \in f^{-1}(H')$ alors:

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

Donc $x * y^{-1} \in f^{-1}(H')$ [4] et [7] . ■

Proposition 1.1.5 *Soient G, G' et G'' trois groupes et $f : G \to G'$ et $g : G' \to G''$ deux homomorphismes de groupes. Alors la composée $g \circ f : G \to G''$ est un homomorphisme de groupes.*

Définition 1.1.7 *Soit f un morphisme de groupes de G dans G' :*

Le noyau *de f est l'ensemble* :

$$\ker(f) = \{x \in G \setminus f(x) = e_{G'}\}.$$

L'image *de f est l'ensemble* :

$$\mathrm{Im}(f) = \{f(x) \setminus x \in G\}.$$

Théorème 1.1.1 *Soit $f : (G, *, e_G) \to (G', \bullet, e_{G'})$ 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 $f(e_G) = e_{G'}$, 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

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

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

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

donc $x^{-1} * y \in \ker(f)$ et $x^{-1} * y = e_G$, 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 $x \bullet y^{-1} \in \mathrm{Im}(f)$. Comme x, $y \in \mathrm{Im}(f)$, il existe a, $b \in G$ tels que

$$x = f(a) \text{ et } y = f(b). \text{ Alors } x \bullet y^{-1} = f(a) \bullet f(b)^{-1} = f(a * b^{-1}) \in \mathrm{Im}(f).$$

4) La preuve de cette propriété est immédiate sachant que $\mathrm{Im}(f) = f(G)$ [4] et [7]. ■

Définition 1.1.8 *Soient G un groupe et H un sous-groupe de G.*

On appelle relation à droite (resp. à gauche) associée au sous-groupe H la relation sur G définie par:

$$x\ R_d\ y \ \Leftrightarrow\ x\ y^{-1} \in H.$$

$$resp.$$

$$x\ R_g\ y \ \Leftrightarrow\ x^{-1}y \in H.$$

Proposition 1.1.6 *les relations R_d et R_g sont des relations d'équivalence.*

Preuve.

1) La relation R_d **est Réflexive** car: $\forall\ x \in G$, comme H est un sous groupe de G, alors $x\ x^{-1} = e \in H$, donc $\forall\ x \in G$, $x\ R_d\ x$.

2) La relation R_d **est Symétrique** car : $\forall\ x,\ y \in G$:

$$\begin{aligned} x\ R_d\ y\ &\Leftrightarrow x\ y^{-1} \in H \\ &\Rightarrow\ (x\ y^{-1})^{-1}\ \in H \\ &\Rightarrow\ y\ x^{-1} \in H \\ &\Rightarrow\ y\ R_d\ x. \end{aligned}$$

3) La relation R_d **est Transitive** car : $\forall\ x,\ y,\ z \in G$:

$$\begin{aligned} (x\ R_d\ y) \wedge\ (y\ R_d\ z)\ &\Leftrightarrow [(x\ y^{-1}) \in H] \wedge [(y\ z^{-1}) \in H] \\ &\Rightarrow\ ((x\ y^{-1})\ (y\ z^{-1})) \in H,\ \text{car } H \text{ est un sous-groupe} \\ &\Rightarrow\ (x\ (y^{-1}\ y)\ z^{-1}) \in H,\ \text{car la loi de } G \text{ est associative} \\ &\Rightarrow\ (x\ z^{-1})\ \in H \\ &\Rightarrow\ x\ R_d\ z. \end{aligned}$$

De 1), 2),3) on déduit que R_d est une relation d'équivalence (le cas R_g se montrant de manière similaire) [7] . ■

Proposition 1.1.7

1. *La relation R_d est compatible à droite avec la loi de G c'est à dire si x et y sont des éléments de G tels que $x\ R_d\ y$ alors pour tout élément z de G $x\ z\ R_d\ y\ z$.*

2. *La relation R_g est compatible à gauche avec la loi de G c'est à dire si x et y sont des éléments de G tels que $x\ R_g\ y$ alors pour tout élément z de G $z\ x\ R_g\ z\ y$.*

Preuve.

On démontre la proposition pour la relation R_d (le cas R_g se montrant de manière similaire). Soient x et y deux éléments de G tels que $x\ R_d\ y$.

On a alors $x\ y^{-1} \in H$. Mais, pour tout élément z de G,

$$x\ y^{-1}\ =\ x\ z\ z^{-1}\ y^{-1},\ \text{donc}\ x\ z\ z^{-1}\ y^{-1}\ =\ (x\ z)(y\ z)^{-1}\ \in\ H$$

C'est à dire $x\ z\ R_d\ y\ z$ de G. ■

Proposition 1.1.8

La classe d'équivalence d'un élément $x \in G$ pour la relation à droite (resp. à gauche) est l'ensemble

$$\begin{aligned} H\ x &= \{h\ x,\ h\ \in\ H\}. \\ &\quad resp. \\ x\ H &= \{x\ h,\ h\ \in\ H\}. \end{aligned}$$

Preuve.

i) La classe de x pour la relation R_d est l'ensemble

$$\begin{aligned} \{y\ \in\ G\ /\ x\ R_d\ y\} &= \{y\ \in\ G\ /\ x\ y^{-1}\ \in\ H\ \} \\ &= \{y\ \in\ G\ /\ x\ y^{-1} = h,\ h\ \in\ H\} \\ &= \{y\ \in\ G\ /\ y^{-1} = x^{-1}\ h,\ h\ \in\ H\} \\ &= \{y\ \in\ G\ /\ y = h\ x,\ h\ \in\ H\ \} \\ &= \{h\ x,\ h\ \in\ H\} = H\ x. \end{aligned}$$

ii) La classe de x pour la relation R_g est l'ensemble

$$\begin{aligned} \{y\ \in G\ /\ x\ R_g\ y\} &= \{y\ \in\ G\ /\ x^{-1}\ y\ \in\ H\ \} \\ &= \{y\ \in\ G\ /\ x^{-1}\ y = h,\ h\ \in\ H\} \\ &= \{y\ \in\ G\ /\ x\ x^{-1}\ y = x\ h,\ h\ \in\ H\} \\ &= \{y\ \in\ G\ /\ y = x\ h,\ h\ \in\ H\ \} \\ &= \{x\ h,\ h\ \in\ H\} = x\ H. \end{aligned}$$

■

Proposition 1.1.9

L'ensemble des classes d'équivalence des éléments de G pour la relation à droite (resp. à gauche) modulo H est :

$$\begin{aligned} (G/H)_d &= \{H\ x \setminus x\ \in\ G\ \}. \\ (G/H)_g &= \{x\ H \setminus x\ \in\ G\ \}. \end{aligned}$$

Ces ensembles sont aussi appelés ensembles quotients à droite (resp. à gauche) modulo H.

Définition 1.1.9

*On dit qu'un groupe G est **fini** si l'ensemble G est **fini**. Dans ce cas, le cardinal de G est appelé **ordre** de G et noté $|G|$.*

Théorème 1.1.2 (théorème de lagrange)

Soit G un groupe fini et H un sous-groupe de G. Alors $|H|$ divise $|G|$ et

$$|G| / |H| = |H/G| = |G/H|$$

L'entier $|G| / |H|$ s'appelle l'indice de H dans G note $(G : H)$.

Démonstration.

Soit x un élément de G et H un sous-groupe de G. L'application $f : H \to x\ H$ définie par $h \mapsto x\ h$ est bijective et pour tout $x \in G : |x\ H| = |H|$.

Si G est fini on a

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

$$|G| = \left| \bigcup_{i=1}^{k} x_i\ H \right|$$

$$= \sum_{i=1}^{k} |x_i\ H| = \sum_{i=1}^{k} |H| = k \cdot |H|$$

Donc $|G| = k \cdot |H|$, $k = (G : H)$ l'indice de H dans G. ■

Définition 1.1.10

*Un sous-groupe H d'un groupe $(G, *)$ est **distingué** (**ou normal**) si pour tout $x \in G$ on a $x\ H = H\ x$. Ceci équivante à $\forall\ x\ \in\ G : x\ H\ x^{-1} = H$, ou encore plus explicite*

$$\forall\ x\ \in\ G \text{ et } \forall\ h\ \in\ H :\ x * h * x^{-1} \in H.$$

On note alors $H \lhd G$ et on lit H est distingué dans G.

Exemple 1.1.7

1. *$\{e_G\}$ et G sont distingué dans G.*

2. *Soit* $f : (G, *) \to (G', \cdot)$ *un homomorphisme de groupe, Alors* $\ker f$ *est un sous-groupe normal de* G.

   En effet, d'après la définition $\forall\ x \in G, \forall\ h \in \ker f : x\ h\ x^{-1} \in \ker f$. *Ona*

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

   Donc $x\ h\ x^{-1} \in \ker f$ *et* $\ker f$ *sous-groupe normal de* G.

3. *Si* G *est abélien alors tous ses sous-groupes sont distingués.*

Définition 1.1.11

Soient G *un groupe et* H *un sous-groupe distingué de* G. *Alors* $R_g = R_d$, *pour tout* x *élément de* G, $x\ H = H\ x$ *et* $G/H = (G/H)_g = (G/H)_d$.

Soient G *un groupe et* H *un sous-groupe distingué de* G. *La relation binaire sur* G *définie par* $x\ R\ y$ *si, et seulement si,* $x\ y^{-1} \in H$ *est une relation d'équivalence sur* G *compatible avec la loi du groupe et appelée* ***relation de congruence modulo*** H.

Théorème 1.1.3

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

Preuve.

1) La loi $\bullet$ est bien définie **car** l'application

$$\begin{aligned} \bullet \ : \ (G/H) \times (G/H) &\to (G/H) \\ (\bar{x},\ \bar{y}) \ &\mapsto \bar{x} \ \bullet \ \bar{y} = \overline{x\ y} \end{aligned}$$

Constitue ainsi une loi de composition interne sur G/H.

2) La loi $\bullet$ est associative **car** :

$$\forall x,\ y,\ z \ \in \ G \ : \ \bar{x} \bullet (\bar{y} \bullet \bar{z}) = \bar{x} \bullet \overline{(y\ z)} = \overline{x\ (y\ z)} = \overline{(x\ y)\ z} = \overline{(x\ y)} \bullet \bar{z} = (\bar{x} \bullet \bar{y}) \bullet \bar{z}.$$

3) La loi $\bullet$ admet élément neutre $\bar{e}$:

$$\forall\ x \ \in \ G \ : \ \bar{e} \ \bullet \ \bar{x} = \overline{e\ x} = \overline{x\ e} = \bar{x} \ \bullet \ \bar{e} = \bar{x}.$$

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

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

Enfin, la surjection canonique $s : G \to G/H$, $x \mapsto \bar{x}$ est un homomorphisme de groupes

i) $\forall\ x, y \in G^2 : s(x * y) = \overline{x\ y} = \bar{x} \bullet \bar{y} = s(x) \bullet s(y)$

ii) $s(e) = \bar{e}$. ■

Exemple 1.1.8

On considère $G = \mathbb{Z}$ 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 $\exists\ k \in \mathbb{Z} : x - y\ = n\ k$) i.e., $x \equiv y(mod\ n)$ et ainsi la notation $\mathbb{Z}_n = G/H = \mathbb{Z}/n\mathbb{Z}$ est justifiée.

Définition 1.1.12 (groupes symétriques)

Soit n un entier naturel non nul. On note S_n l'ensemble des permutation de l'ensemble $\{1, \ldots, n\}$ c'est à dire l'ensemble des bijections de $\{1, \ldots, n\}$ vers $\{1, \ldots, n\}$. Appelé groupe symétrique de degré n.

Théorème 1.1.4 (Théorème de Cayley)

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

Démonstration.

Soit g un élément de G. L'application $f_g :\ G \to G$ définie par $f_g(x) = g\ x$ est bijective. En effet, injective

$$\begin{aligned} f_g(x_1) = f_g(x_2) &\Rightarrow g\ x_1 = g\ x_2 \\ &\Rightarrow g^{-1}\ g\ x_1 = g^{-1}\ g\ x_2 \\ &\Rightarrow x_1 = x_2. \end{aligned}$$

Et surjective : $\forall\ g \in G$

$$f_g(x) = g\ x = y \Rightarrow x = g^{-1}\ y.$$

c'est donc une permutation de G. L'application

$$F\ :\ G\ \to\ S_G\ ,\ g\ \mapsto\ f_g$$

Est un morphisme de groupes. En effet, $F\ (g\ h)$ est l'application de G dans G qui à x associe $(g\ h)\ x$. Comme $(g\ h)\ x = g\ (h\ x)$, cet élément est aussi l'image de x par l'application $F(g) \circ F(h)$. On en déduit que $F\ (g\ h) = F(g) \circ F(h)$.

De plus, F est injectif. En effet, si $F(g)$ est égal à l'identité, pour tout x de G on a $g\ x = x$, d'où $g = 1_G$, où 1_G est l'élément neutre de G, et $\ker(F) = \{1_G\}$.

Par conséquent, F est un isomorphisme de G sur son image $F(G)$, qui est un sous-groupe de S_G [4]. ■

Exemple 1.1.9

Soit $G = \{1, -1, i, -i\}$ *est un groupe d'ordre* 4, $H = \{f_1, f_{-1}, f_i, f_{-i}\}$ *le sous-groupe de* S_4 *tel que*

$$f_1 : G \to G \qquad f_{-1} : G \to G \qquad f_i : G \to G \qquad f_{-i} : G \to G$$
$$x \longmapsto 1 \cdot x \qquad x \longmapsto -1 \cdot x \qquad x \longmapsto i \cdot x \qquad x \longmapsto -i \cdot x$$

On montre que $G \simeq H$

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$\circ$	f_1	f_{-1}	f_i	f_{-i}
f_1	f_1	f_{-1}	f_i	f_{-i}
f_{-1}	f_{-1}	f_1	f_{-i}	f_i
f_i	f_i	f_{-i}	f_{-1}	f_1
f_{-i}	f_{-i}	f_i	f_1	f_{-1}

On remarquera que sur les tables comme ci-dessus, G *et* H *ont les mêmes propriétés algébriques donc* $G \simeq H$.

1.2 Classification des groupes monogènes

Soit X une partie d'un groupe G. On appelle **sous-groupe engendré** par X et on note $< X >$ l'intersection de tous les sous-groupes de G contenant X.

La partie $< X >$ est le plus petit (au sens de l'inclusion) sous-groupe de G contenant X.

Si H est un sous-groupe de G et si $H =< X >$, on dit que H est engendré par X.

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

$$< g > \ = \ \{ \ g^m \ : \ m \ \in \ \mathbb{Z} \} \ = \ \{ \cdots , \ g^{-2}, \ g^{-1}, \ e, \ g^1, \ g^2, \ \cdots \}$$

Où e désigne l'élément neutre de G.

Définition 1.2.1

Le groupe G est dit **monogène** s'il existe g dans G tel que $G = < g >$

L'élément g est appelé **générateur de** G. Nous dirons aussi que G est **engendré** par g.

Un groupe **monogène** est visiblement abélien.

Exemple 1.2.1 $(\mathbb{Z} \ , +)$ *est monogène engendré par* 1 *ou* -1.

Proposition 1.2.1

Si G est un groupe monogène admettant un élément a pour générateur, si f est un homomorphisme de groupe partant de G, $f(G)$ est un groupe monogène admettant $f(a)$ pour générateur.

Preuve.

Si A est un partie de G, si $< A >$ désigne le sous-groupe de G engendré par A, alors $f \ (< A >)$ est engendré par $f(A)$. En faisant $A = \{a\}$, nous trouvons que, dans nos hypothèse, $f(G)$ est engendré par $f(a)$ [7] . ■

Proposition 1.2.2

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

Preuve.

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

Il vient que

$$G' \ = \ \{(\varphi(g))^m \ : \ m \ \in \ \mathbb{Z}\} .$$

En d'autres termes, G' est monogène et $\varphi(g)$ en est un générateur [5] et [7] . ■

Théorème 1.2.1 *Un groupe G 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 (car $\mathbb{Z} = < 1 >$ est un groupe monogène infini).

Inversement, supposons que G est monongène infini 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 $\mathbb{Z}/\ker\varphi$, où $\ker\varphi$ désigne le noyau de φ. Or, comme $\ker\varphi$ est un sous-groupe de $\mathbb{Z}$, il existe $n \in \mathbb{N}$ tel que

$\ker\varphi = n\ \mathbb{Z}$. Par conséquent G est isomorphe à $\mathbb{Z}\ /n\ \mathbb{Z}$, ce qui donne $n = 0$.

Finalement G est isomorphe à $\mathbb{Z}$ [4] et [5] et [7] . ■

Corollaire 1.2.1 *Deux groupes monogènes infinis sont isomorphes.*

Proposition 1.2.3 *Tout sous-groupe d'un groupe monogène est monogène.*

Preuve.

Soit G un groupe monogène. D'après théorème 1.2.1, 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 [5] . ■

Exemple 1.2.2

Les sous-groupes de $(\mathbb{Z}, +)$ *qui sont de la forme* $n\ \mathbb{Z} = \{n\ .\ p, p \in \mathbb{Z}\}$ *avec* $n \geq 0$ *sont tous monogènes.*

Théorème 1.2.2

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

$$g = \varphi_h(1) = h \text{ ou } g = \varphi_h(-1) = h^{-1}.$$

Ce qu'il fallait démontrer [7]. ■

1.3 Les groupes cycliques

Définition 1.3.1

On dit que G est monogène s'il existe $g \in G$ tel que $G =< g >$. Si de plus, G est fini, on dit alors qu'il est cyclique.

$$\begin{aligned} < g > &= \left\{ \prod_{k=1}^{r} g^{\varepsilon_k} \setminus r \in \mathbb{N}^*, \varepsilon_k = \pm 1 \text{ pour } 1 \leq k \leq r \right\} \\ &= \{g^n \setminus n \in \mathbb{Z}\} \end{aligned}$$

Pour un groupe additif, on a

$$< g > = \{n\ g \mid n \in \mathbb{Z}\}$$

On rappelle qu'un élément $g \in G$ est dit d'ordre fini si le groupe $< g >$ est fini et l'ordre de g est alors le cardinal de $< g >$. On note $o(g)$ cet ordre et on a

$$(o(g) = n \in \mathbb{N}^*) \Leftrightarrow (< g > = \{g^r | 0 \leq r \leq n-1\})$$

$n = o(g)$ est le plus petit entier naturel non nul tel que $g^n = 1$ (ou $n\ g = 0$ pour un groupe additif).

Le théorème de Lagrange nous dit que si G est fini, alors l'ordre de $g \in G$ divise l'ordre de G.

Exemple 1.3.1

- *Pour* $n \in \mathbb{N}^*$, $(\mathbb{Z}/n\ \mathbb{Z}\ , +) =< \bar{1} >$ *est cyclique d'ordre* n.
- *Le groupe multiplicatif* Γ_n *des racines* $n-$*émies de l'unité, qui est cyclique d'ordre* n, *est isomorphe à* $\mathbb{Z}/n\ \mathbb{Z}$ *par l'application* $\bar{k} \to e^{\frac{2ik\pi}{n}}$.

Remarque 1.3.1

1. *Un groupe cyclique est nécessairement commutatif.*
2. *Deux groupes cycliques sont isomorphes si et seulement s'ils ont le même ordre.*
3. *Dire que* G *est cyclique d'ordre* n *signifie que* G *est de cardinal égal à* n *et qu'il existe dans* G *au moins un élément* g *d'ordre* n. *Dans ce cas, on a*

$$G \ = \ < g > \ = \ \left\{1,\ g,\ \ldots,\ g^{n-1}\right\}.$$

Proposition 1.3.1

Soit $G =< g >$ *un groupe cyclique d'ordre* n. *Les générateurs de* G *sont les* g^k *où* k *est un entier compris entre* 1 *et* $n-1$ *premier avec* n.

Corollaire 1.3.1 *Soit* $G =< g >$ *un groupe cyclique d'ordre* n. *L'ordre de* g^k *est* $\frac{n}{PGCD\ (k,\ n)}$.

Définition 1.3.2

La fonction indicatrice d'Euler est la fonction qui associe à tout entier naturel, non nul n, *noté* $\varphi(n)$, *le nombre d'entiers compris entre* 1 *et* n *qui sont premiers avec* n.

Le nombre de générateurs *d'un groupe cyclique* G *d'ordre* n *est donc égal à* $\varphi(n)$.

Proposition 1.3.2

Soient G *et* G' *deux groupes et* $f : G \to G'$*un homomorphisme de groupes surjectif. Si* G *est cyclique engendré par* g *alors* G' *est cyclique engendré par* $f(g)$.

Preuve.

Comme G est fini, G' est fini car f est surjective ($Card\, G' < Card\, G$). Soit g le générateur de G. Comme f est surjective, tout élément de G' s'écrit sous la forme $f\ (g^n)$ où n est un entier compris entre 1 et $|G| - 1$. D'où, f étant un homomorphisme, $f\ (g^n) = f\ (g)^n$.

G' est donc un groupe cyclique engendré par $f\ (g)$ [5] et [7]. ■

Corollaire 1.3.2 *Soient G et G' deux groupes isomorphes. Alors, G est cyclique si et seulement si G' est cyclique.*

Preuve.

Soit f l'isomorphisme de G vers G'. D'après la Proposition précédente, 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. ■

Théorème 1.3.1 *Un groupe G est cyclique si et seulement si il existe $n \in \mathbb{N}^*$ tel que G soit isomorphe à $\mathbb{Z}/n\ \mathbb{Z}$.*

Démonstration.

Soit G un groupe. Il est clair que s'il existe $n \in \mathbb{N}^*$ tel que G soit isomorphe à $\mathbb{Z}/n\ \mathbb{Z}$ alors G est cyclique.

Réciproquement, supposons que G est cyclique et g un générateur de G et soit

$$\begin{aligned} \psi\ :\ \mathbb{Z}/n\ \mathbb{Z} &\to\ G \\ \bar{x}\ &\mapsto\ g^x \end{aligned}$$

Si $\bar{x} = \bar{y}$ alors $\exists\ k \in \mathbb{Z}$ tel que $x = y + k\ n$ donc

$$g^x = g^{y\ +\ k\ n} = g^y (g^n)^k = g^y\ 1^k = g^y$$

Donc ψ l'application est bien définie.

$\psi(\bar{x} + \bar{y}) = g^{x\ +\ y} = g^x g^y = \psi(\bar{x})\ \psi(\bar{y})$ donc est un morphisme de groupe.

ψ est évidemment surjective et comme $Card(G) = n = Card(\mathbb{Z}/n\ \mathbb{Z})$, est bijective donc c'est un isomorphisme [4] et [5] . ■

1.3.1 Sous-groupes d'un groupe cyclique

Proposition 1.3.3 *Tout sous-groupe d'un groupe cyclique est cyclique.*

Preuve.

Soit G un groupe cyclique d'ordre n. D'après le théorème 1.3.1, G est isomorphe à

$\mathbb{Z}/n\,\mathbb{Z}$ par un isomorphisme ψ. Soit H un sous-groupe de G. Comme ψ est un homomorphisme $\psi(H)$ est un sous-groupe K de $\mathbb{Z}/n\,\mathbb{Z}$. Or tout sous-groupe de $\mathbb{Z}/n\,\mathbb{Z}$ est cyclique donc, comme $H = \psi^{-1}(K)$, H est cyclique d'après le théorème 1.3.1 . ■

Exemple 1.3.2 $\mathbb{Z}/6\mathbb{Z}$ *a* 4 *sous-groupe distincts*:

1. *d'ordre* $6 \to \mathbb{Z}/6\mathbb{Z}$
2. *d'ordre* $1 \to <\bar{0}>$
3. *d'ordre* 2 *engendré par* $\bar{3} \to <\bar{3}> = \{\bar{0}, \bar{3}\}$
4. *d'ordre* 3 *engendré par* $\bar{2} \to <\bar{2}> = \{\bar{0}, \bar{2}, \bar{4}\}$

Donc le 4 *sous-groupe sont des groupes cycliques.*

Théorème 1.3.2 *Soit* $G =< g >$ *un groupe cyclique d'ordre* $n \geq 2$. *Pour tout diviseur* d *de* n, *il existe un unique sous-groupe d'ordre* d *de* G, *c'est le groupe cyclique* $H = < g^{\frac{n}{d}} >$.

1.4 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.

1.4.1 Isométries du plan

Définition 1.4.1

Une application $f : P \to P$ *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 en B si

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

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 symétrie axiale :

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 $[MM']$.

Les symétrie centrale :

Les points M et M' sont **symétriques par rapport au point** O si :

O appartient au segment $[MM']$ et $OM = OM'$. **Ou encore** : O est le milieu de $[MM']$.

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

1.4.2 Générateurs et ordre de $\mathbf{D}_n$

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

$$\begin{aligned} s\ (O) &= O \text{ et } s(A_i) = A_{n-i}, \text{ pour tout } 1 \leq i \leq n-1 \\ r\ (A_i) &= A_{i+1}, \text{ pour tout } 1 \leq i \leq n-1, \text{ et } r(A_{n-1}) = A_0 \end{aligned}$$

Donc s et r préservent P_n.

Théorème 1.4.1 *Soit $n \in \mathbb{N}$, $n \geq 3$, alors s, $r \in D_n$.*

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

Démonstration.

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 points du plan donc $r^n = Id$ et $r, r^2, \ldots, r^{n-1} \neq Id$ 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 $r\ s\ r\ s$ fixe plus de trois points du plan, donc $r\ s\ r\ s = Id$.

D'où la relation $s\ r\ s\ r = Id$ [5] . ■

Exemple 1.4.1

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 =*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 horizontal*

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

$\Delta_1 =$ *la symétrie par rapport à la première diagonale*

$\Delta_2 =$ *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 1.4.2 $D_n = < r, s > = \{r^k, sr^k \ / 0 \leq k \leq n-1\}$.

Démonstration.

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

1.4.3 Caractérisation de $\mathbf{D}_n$

Proposition 1.4.2 *D_n est non abélien pour $n \geq 3$.*

Preuve.

Pour $n = 2$, $D_2 = \{e,\ r_1,\ s,\ r_1 \circ s\}$ 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 [5] . ■

Remarque 1.4.1 *Pour tout k et $0 \leq k \leq n-1$ $(r_1^k \circ s)^2 = e$ implique $s \circ r_1^k = r_1^{-k} \circ s$ d'ou $s \circ r_1^k = r_1^{n-k} \circ s$.*

Proposition 1.4.3 *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 $< s >$ est un sous-groupe cyclique d'ordre 2 de D_n. ■

Proposition 1.4.4 *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 $\frac{2k\pi}{n}$, $k = 0, ..., n-1$, appartiennent à D_n . Ces rotations auxquelles on ajoute l'identité, forment un sous-groupe cyclique de D_n d'ordre n, engendré par la rotation $r\ (O, \frac{2\pi}{n})$. ■

Proposition 1.4.5 *Pour tout entier k compris entre 1 et $n-1$ $a\ b^k\ a = b^{-k}$.*

Démonstration.

Nous allons procéder par récurrence sur k (compris entre 1 et n) : Cas $k = 1$: $a\ b\ a\ b = 1$ donc $a\ b\ a = b^{-1}$. Supposons que la propriété est vraie pour jusqu'à l'entier $k-1$. Alors,

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

Théorème 1.4.3

Si G est un groupe engendré par deux éléments a et b vérifiant $o(a) = n \geq 2$, $o(b) = 2$ et $o(a\ b) = 2$, 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 $\{e, a, \ldots, a^{n-1}\}$.

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

On en déduit, comme on l'a fait pour D_n, que les éléments $\{e, a, \ldots, a^{n-1}, b, a\ b, \ldots, a^{n-1}\ b\}$ sont distinct deux à deux. Comme $G = < a, b >$, tout élément de G s'écrit comme un produit formel de puissance de a et de b, mais comme $b\ a^k = a^{n-k}\ b$, 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 $i = 0, \ldots, n-1$ et $j = 0, 1$. Ainsi, on a

$$G = \{e,\ a, \ldots,\ a^{n-1},\ b,\ ab, \ldots,\ a^{n-1}\ b\}$$

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 [5] . $\blacksquare$

Chapitre 2

Groupes libres

Dans le chapitre, nous avons défini la notion de groupe libre sur un ensemble X et la propriété universelle d'un tel groupe F_X nous a permis de montre que tout groupe engendré par un ensemble X est isomorphe à un quotient de F_X.

2.1 Généralités sur les mots, monoïde libre

Un alphabet est un ensemble dont les éléments sont **des lettres**. Les alphabets sont toujours supposés finis. **Un mot** est une suite finie de lettres que l'on note par simple juxtaposition :

$$u = a_1\ a_2\ \ldots a_n\ ,\ a_i\ \in\ A$$

Le mot vide est le seul mot composé d'aucune lettre. Il est not ε ou 1. **La longueur** d'un mot u est le nombre de lettres qui le composent, et est notée $|u|$. Le mot vide est le seul mot de longueur 0.

On noté A^* **l'ensemble des mots** sur A .

Soient A un alphabet, $a \in A$ et $u \in A^*$. On note $|u|_a$ **le nombre d'occurrences** *de la lettre a dans le mot u. Si l'on note $u = u_1\ u_2\ ...u_n$:*

$$|u|_a = card\{i\ \in\ [1,\ n],\ u_i\ =\ a\}.$$

Le produit de concaténation de deux mots $u = a_1\ a_2\ \cdots\ a_n$ et $v = b_1\ b_2\ \cdots\ b_m$ est le mot $u\ v$ obtenu par juxtaposition :

$$u\ v\ =\ a_1\ a_2\ \cdots\ a_n\ b_1\ b_2\ \cdots\ b_m.$$

Exemple 2.1.1

$243+(5*(1+6))$ *est un mot sur l'alphabet* $A = \{0,\ 1,\ 2,\ \cdots\ 9,\ +,\ -,\ *,\ /,\ (,),$ *où*$+,\ -,\ *,\ /,\ (,)\}$ *de longueur* 13.

Définition 2.1.1 *L'ensemble* A^* *muni de la concaténation dit le* ***monoïde libre engendré par*** A.

Théorème 2.1.1

Soit A *un alphabet. Soit* $(M, *, e)$ *un monoïde et soit* f *une application de* A *dans* M. *Il existe un et un seul homomorphisme* $f^* : A^* \to M$ *tel que* $\forall\ a \in A,\ f^*(a) = f(a)$.

Preuve.

Existence : Posons $f^*(1) = e_M$ et $f^*(a_1 \cdots\ a_n) = f(a_1) * \ldots * f(a_n)$. Il est facile de voir que f^* est bien un homomorphisme.

Unicité : Soient g et g' deux homomorphismes de A^*dans M tels que $\forall\ a \in A$, $g(a) = g'(a)$. Alors $g(1) = g'(1) = e_M$ et pour tout mot $u = a_1 \cdots\ a_n$,

$$g(u) = g(a_1)\ \ldots\ g(a_n) = g'(a_1)\ \ldots\ g'(a_n) = g'(u).$$

Donc il existe un et un seul homomorphisme f^*. ■

2.2 Groupe libre

2.2.1 Partie libre d'un groupe

Soit G un groupe, et X une partie de G. Si on trouve $x_{i_1}, \ldots, x_{i_n}$ dans X, et $\varepsilon_1, \ldots, \varepsilon_n$ dans $\{-1, 1\}$ tels que le produite $x_{i_1}^{\varepsilon_1} \ldots x_{i_n}^{\varepsilon_n}$ Soit l'élément neutre de G, on dit que l'expression

$$x_{i_1}^{\varepsilon_1} \ldots x_{i_n}^{\varepsilon_n} = 1 \qquad (1)$$

Est une **relation** entre les éléments de X. Si dans cette relation il existe un i tel que $x_i = x_{i+1}$, et $\varepsilon_i = -\varepsilon_{i+1}$, l'associativité de la loi de composition permet d'obtenir une relation réduite équivalente en supprimant $x_i^{\varepsilon_i} x_{i+1}^{\varepsilon_{i+1}}$. En continuant ainsi tant qu'une telle simplification est possible, on obtient à la fin une relation irréductible, toujours équivalente

à (1). Il est possible que cette expression finale soit simplement "1 = 1", auquel cas la relation de départ (1) est dite **triviale**. Par exemple

$$a^{-1}\ b\ a\ a^{-1}\ b^{-1}\ a = 1\ ;\ x\ z^{-1}\ y^2\ t\ t^{-1}\ y^{-2}\ z\ x^{-1} = 1.$$

Si l'expression (1) est **non triviale**, on dira que les éléments de X sont **liés** par cette relation.

Remarquons alors que pour tout morphisme φ de G dans un groupe quelconque G', les images des éléments de X sont eux aussi liés par une relation **non triviale**, celle obtenue formellement à partir de (1) en remplaçant x_i par $\varphi(x_i)$.

S'il n'existe aucune relation non triviale liant les éléments de X, on dit que X est une partie **libre** du groupe G.

Un groupe G est dit libre sur X si X est une partie à la fois libre et génératrice de G.

Définition 2.2.1 [4, *p.* 65]

*Soient G un groupe et X une partie de G. **Le groupe** G est dit **libre** de **base** X si tout élément g de G s'écrit de manière unique*

$$g = x_{i_1}^{n_1} \dots x_{i_k}^{n_k}$$

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

Si $k = 0$, on pose $x = 1$.

*On dit alors que X est une **famille génératrice libre de** G, ou encore que X soit une **base** de G. Un groupe G est dit **libre** s'il possède une base.*

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

Exemple 2.2.1 *Le groupe $(\mathbb{Z}, +)$ est un groupe libre de base $\{1\}$.*

Proposition 2.2.1 *Pour tout ensemble X il existe un groupe libre $G(X)$ de base X.*

2.2.2 Construction d'un groupe libre

Soit $X = \{x_i\}_{i \in I}$ un ensemble. Soit X^{-1} un ensemble disjoint de X et qui en bijection avec X, dont on notera les éléments x_i^{-1}, $i \in I$. 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.

L'ensemble $X \cup X^{-1}$ s'appelle un **l'alphabet** du groupe libre.

Définition 2.2.2 [4, *p.* 66] *et* [5, *p.* 330]

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

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

Dans l'écriture ci-dessus, l'entier n *est la* ***longueur*** *du mot* u*, qu'on notera* $|u|$ *.*

Deux mots $x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ *et* $x_{j_1}^{\gamma_1} ... x_{j_k}^{\gamma_k}$ *sont* ***des mots égaux*** *si*

$$n = k \text{ et } \forall p \ , 1 \ \leq \ p \leq \ n \ , \ i_p = j_p \text{ et } \epsilon_p = \gamma_p.$$

Exemple 2.2.2 *Si* $X = \{x, y, z\}$, $x\ y\ z$, $x\ y\ y\ z\ z^{-1}\ x\ x^{-1}\ x$ *sont des mots en* $X \cup X^{-1}$.

Remarque 2.2.1 *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

- Quelque soit $u \in M(X)$, on pose $1u = u1 = u$
- Plus précisément, si $u = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n}$ et $v = x_{j_1}^{\gamma_1} ... x_{j_k}^{\gamma_k}$ sont deux mots, alors

$$u\ v = x_{i_1}^{\epsilon_1} \dots x_{i_n}^{\epsilon_n} x_{j_1}^{\gamma_1} ... x_{j_k}^{\gamma_k}.$$

  donc $|u\ v| = |u| + |v|$.

Remarque 2.2.2

1. *Un mot de longueur* 1 *est un élément de* $X \cup X^{-1}$ *tout mot de longueur* $n > 0$ *est donc produit de* n *mot de longueur* 1.
2. *Le produit de mot défini dans* $M(X)$ *est associatif et* 1 *est élément unité.*

3. $M(X)$ n'est pas un groupe car tout élément autre que 1 ne peut avoir d'inverse.

On va définir sur $M(X)$ une relation d'équivalence R.

Définition 2.2.3 [4, *p.* 67] *et* [5, *p.* 331]

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

$$u = t_1\ t_2 \text{ et } v = t_1 a a^{-1} t_2$$

$$Ou$$

$$u = t_1 a a^{-1} t_2 \text{ et } v = t_1\ t_2$$

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

Si u et v sont deux mots adjacents, on écrira $u\,\mathrm{A}v$.

Exemple 2.2.3 *Soit $X = \{x,\ y\}$, alors :*

1. $x^{-1}xyy^{-1}A\ yy^{-1}$ on prend $t_1 = 1$ et $t_2 = yy^{-1}$ et $a = x^{-1}$

2. $x^{-1}xyy^{-1}\ A\ x^{-1}x$ on prend $t_1 = x^{-1}x$ et $t_2 = 1$ et $a = y$.

Remarque 2.2.3 *quelque soient u et v dans $M(X)$, $u\,\mathrm{A}v \Rightarrow v\,\mathrm{A}u$.*

Définition 2.2.4 *La relation R est définie sur $M(X)$ par*

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

Proposition 2.2.2 [4, *p.* 67] *et* [5, *p.* 332]

La relation binaire R définie ci-dessus est une relation d'équivalence dans $M(X)$ compatible avec le produit des mots.

Démonstration.

i) Pour tout u de $M(X)$ on a $u\ R\ u$, 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 $u\ R\ v$ et $v\ R\ w$, on a $(u = t_1)\ A...A\ (t_n = v = t_{n+1})\ A...A\ t_{n+p} = w$, d'où $u\ R\ w$ et la relation R est transitive.

ii) Soient u, v, w dans $M(X)$, remarquons que u A v implique que $u\ w\ A\ v\ w$. En effet, si $u = t_1\ t_2$ et $v = t_1 a a^{-1} t_2$,

alors $u\ w = t_1\ (t_2\ w)$ et $v\ w = t_1 a a^{-1}\ (t_2\ w)$.

Par conséquent, si $(u = t_1)\ A...A\ (t_n = v)$, alors $(u\ w = t_1\ w)\ A...A\ (t_n\ w = v\ w)$, 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. [4] ■

Notation 2.2.1 *Pour tout u de $M(X)$ on notera $[u]$ sa classe dans $M(X)/R$.*

Proposition 2.2.3 [4, *p.* 68] *et* [5, *p.* 332]

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

Démonstration.

On a 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 $[u]$ possède un inverse. Considérons d'abord le cas où $u \in X \cup X^{-1}$, il est clair que $uu^{-1} R 1$, car en prenant $t_1 = t_2 = 1$, on a $uu^{-1} = t_1 u u^{-1} t_2$ et $1 = t_1\ t_2$, d'où $uu^{-1} R 1$. De la même manière, $u^{-1} u R 1$. On en déduit donc que

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

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

$$\pi(u\ v) = [u\ v] = [u][v] = \pi(u)\pi(v).$$

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

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

Définition 2.2.5

On dira qu'un groupe est libre sur un ensemble X, s'il est engendré par X et isomorphe au groupe $M(X)/R$ défini ci-dessus.

Définition 2.2.6 *Un mot u de $M(X)$ est* ***réduit*** *si $u = 1$ ou $u = a_1 ... a_n$, avec $a_i \in X \cup X^{-1}$ tels que $a_{i+1} \neq a_i^{-1}$, $i = 1, ..., n-1$.*

Exemple 2.2.4

1. *tout mot de longueur* 1 *est réduit.*

2. *Si* $X = \{x, y\}$, $xxyx^{-1}$, $x^{-1}yxyy$ *sont des mots réduits.*

Proposition 2.2.4 [4, *p.* 68] *et* [5, *p.* 334]

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

Démonstration.

On remarque d'abord que chaque classe contient un mot réduit : il suffit en effet de choisir un mot de longueur minimale parmi ceux de la classe. Soit maintenant $u = a_1 \dots a_n \in M(X)$.

On construit par récurrence une suite de mots réduit (u_i) en posant $u_0 = 1$, $u_1 = a_1$, $u_2 = a_1\, a_2$ si $a_1 \neq a_2^{-1}$ et 1 sinon , puis si u_i est un mot réduit équivalent a $a_1 \dots a_i$ on construit u_{i+1} de la maniéré suivante : si $u_i = 1$, $u_{i+1} = a_{i+1}$, sinon u_i est de la forme $t_1 \dots t_k$ et on pose $u_{i+1} = u_i\, a_{k+1}$ si $a_{k+1} \neq t_k^{-1}$, $t_1 \dots t_{k-1}$ sinon.

Alors u_n est un mot réduit équivalent a u, que nous noterons $r(u)$. En n, par construction, si u et v sont équivalents alors $r(u) = r(v)$, et si u est réduit alors $r(u) = u$.

Donc si u et v sont équivalents et réduit, alors $u = r(u) = r(v) = v$, d'où l'unicité. ■

Remarque 2.2.4

1. *Deux mots équivalents et réduits sont égaux.*

2. *Si* $X = \{x\}$ *alors* $M(X)/R$ *est un monogène infini engendré par* x, *donc* $M(X)/R$ *est isomorphe à* $\mathbb{Z}$.

3. *Si* $card(X) > 1$ *alors* $M(X)/R$ *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.

On suppose que

$$\begin{aligned} si\ [xy] = [yx] &\Rightarrow [xy]\,[xy]^{-1} = [1] \\ &\Rightarrow [xy]\,[yx]^{-1} = [1] \\ &\Rightarrow [xyx^{-1}y^{-1}] = [1]\,. \end{aligned}$$

Contradiction. *Donc* $[xy]$ *est différent de* $[yx]$ *dans* $M(X)/R$.

4. *tout groupe isomorphe à un groupe libre est libre.*

   En effet, si θ *un isomorphisme du groupe libre* $M(X)/R$ *sur un groupe* G, *alors* G *est librement engendre par* $\theta(X)$.

   En particulier, le groupe $M(X)/R$ *est librement engendré par* $\{[x_i];\ x_i \in X\}$.

Remarque 2.2.5

Désigne par L_X ***l'ensemble des mots réduits*** *de* $M(X)$, L_X *est un ensemble de représentation des classes d'équivalences distinctes* $[u] \in M(X)/R$.

La bijection qui à chaque classe $[u]$ *associe l'unique mot réduit qu'elle contient,* $r(a)$, *permet de défini dans* L_X *une loi*

$$\begin{aligned} L_X \times L_X &\ \rightarrow\ L_X \\ (u,\ v) &\ \longmapsto\ r(u\ v) \end{aligned}$$

Telle que L_X *est un groupe engendré par* X *et isomorphe au groupe* $M(X)/R$.

Donc L_X est groupe libre engendre par X.

2.2.3 Rang d'un groupe libre

Définition 2.2.7 *Si* G *est un groupe libre, le cardinal d'une partie génératrice libre de* G *est appelé le* ***rang*** *de* G.

En particulier, un groupe libre est de ***rang fini*** n, *s'il possède une partie génératrice libre* ***finie*** *de cardinale* n.

Corollaire 2.2.1 *Si* F *est un groupe libre et si* X *et* Y *sont deux parties génératrice de* F, *alors* $card(X) = card(Y)$

Théorème 2.2.1 (Propriéte universelle du groupe libre) [5, *p.* 338]

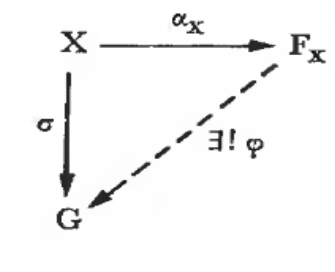
Soient F un groupe, X une partie génératrice de F et $\alpha : X \to F$ l'injection canonique. Alors le groupe F est libre de base X si et seulement si, pour tout groupe G et pour toute application $\sigma : X \to G$, il existe un unique morphisme de groupes $\varphi : F \to G$ tel que

$\varphi \circ \alpha = \sigma$.

Preuve.

Supposons que $F = F_X$, α_X désignant L'injection canonique de X dans F_X, démontrons que le couple (F_X, α_X) vérifie la propriété énoncée.

Dans le diagramme :



Où G et σ sont donnés, définissons $\varphi : F_X \to G$ en posant, pour tout $u \in F_X$, écrit sons la forme $u = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}$ tel que $n \in \mathbb{N}$, $x_{i_j} \neq x_{i_{j+1}}$:

$$\varphi(u) = (\sigma(x_{i_1}))^{\varepsilon_1}(\sigma(x_{i_2}))^{\varepsilon_2} \dots (\sigma(x_{i_n}))^{\varepsilon_n} \text{ et } \varphi(1) = e$$

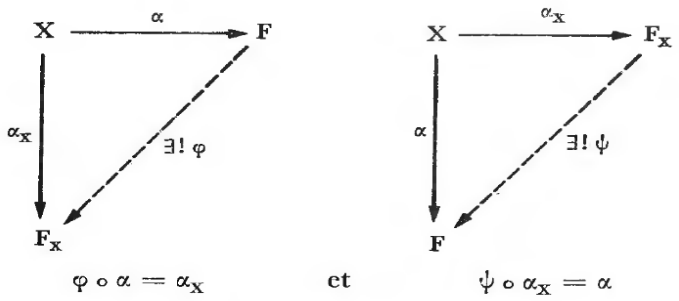
Où e est l'élément neutre de G.

On définit ainsi un morphisme $\varphi \in Hom(F_X, G)$ tel que $\varphi(x) = \sigma(x)$ quel que soit $x \in X$, donc $\varphi \circ \alpha_X = \sigma$.

De plus, si $\varphi' \in Hom(F_X, G)$ et $\varphi' \circ \alpha_X = \sigma$, alors pour tout $u \in F_X$, on a $\varphi'(u) = \varphi(u)$, d'où l'unicité de φ. **Réciproquement**, considérons un groupe F engendré par une partie non vide X, telle que, Si α est l'injection canonique de X dans F, le couple (F, α) vérifiant les conditions énoncées dans le théorème .

Compte tenu de l'hypothèse et du résultat précédent, il existe $\varphi \in Hom(F, F_X)$ et $\psi \in Hom(F_X, F)$

Tel que les diagrammes suivants commutent :



On en déduit que $\psi \circ \varphi \circ \alpha = \alpha$ et $\varphi \circ \psi \circ \alpha_X = \alpha_X$, d'où $\psi \circ \varphi_{/X} = id_X$ et $\varphi \circ \psi_{/X} = id_X$
φ et ψ sont des morphismes de groupes, F et F_X sont engendrés par X, par suit
$\psi \circ \varphi = id_F$ et $\varphi \circ \psi = id_{F_X}$, d'où $F \simeq F_X$ et $\psi(X) = X$ implique F libre sur X [5] . ■

Théorème 2.2.2 *Tout groupe est isomorphe à un quotient d'un groupe libre.*

Preuve.

Soient G un groupe, X une partie génératrice de G et $\sigma : X \to G$ l'injection canonique. D'après le théorème de propriété universelle, il existe un morphisme de groupes $\varphi : F_X \to G$ tel que $\varphi|_X = id_X$. On a donc $G = < X > = < \varphi(X) >$ et φ est surjective. On en déduit que G est isomorphe à $F_X/Ker(\varphi)$ [5] . ■

2.3 Sous-groupes des groupes libres

Théorème 2.3.1

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

Définition 2.3.1 (Rang d'un sous-groupe d'un groupe libre)

*Si F est un groupe libre de **rang fini** et si H est un sous-groupe de F, d'indice fini, alors H est un groupe libre de **rang fini***

Un groupe libre de rang fini peut contenir un sous-groupe de rang infini

Plus généralement, si F est un groupe libre et si $H \neq (1)$ est d'indice infini dans F, alors H est de rang infini.

Chapitre 3

Présentation de quelques groupes

Dans ce chapitre, nous avons défini la notion de présentation d'un 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. Par exemple on étude : Présentation d'un groupe monogéne d'ordre infini, Présentation d'un groupe cyclique d'ordre n, Présentation de groupe diédral D_n.

3.1 Généralités sur les présentations de groupe

Soit G un groupe, et X une partie génératrice de G. D'après le théorème de propriété universelle d'un groupe libre sur X, l'injection naturelle de X dans G se prolonge en un unique morphisme de groupe φ de F_X vers G, et comme $G = < X >$, φ est surjectif. Le premier théorème d'isomorphisme permet alors d'affirmer que $G = \operatorname{Im}\varphi$ est isomorphe à $F_X/\ker\varphi$, d'ou le théorème : tout groupe est isomorphe à un groupe quotient d'un groupe libre.

Notons de plus que chaque élément r de $\ker\varphi$ fournit une relation non triviale "$r = 1$" entre les éléments de X dans G.

Inversement, toute relation non triviale dans G liant les éléments de X s'écrit sous la forme "$r = 1$" avec $r \in \ker\varphi$.

Ce qui précède montre que le groupe G est entièrement déterminé (à isomorphisme prés) une fois que l'on connait une partie génératrice X et l'ensemble $\ker\varphi$ des relation non triviales liant les éléments de X.

Il est généralement impossible d'énumérer de manière exhaustive tous les éléments de $\ker\varphi$; mais la donnée d'une partie R de F_X

D'autre part, si R est une partie d'un groupe F_X, le sous-groupe normal de F_X engendré par R, qu'on notera (R), est l'intersection de tous les sous-groupe normaux de F_X contenant R. Si $R = \phi$, on pose $(R) = \{1\}$, où 1 est élément neutre de F_X.

Définition 3.1.1 [4, *p.* 72]

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

Une présentation de groupe $< X/R >$ est ***finement engendrée*** *si X est fini,* ***finement relatée*** *si R est fini, et* ***finement présentée*** *si X et R sont finis.*

Exemple 3.1.1

1. *Pour $n \in \mathbb{N}^*$, $< x|\ x^n >$ est une présentation du groupe cyclique d'ordre n engendré par x.*

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

3. *quel que soit l'ensemble X, $F_X = \frac{F_X}{(1)}$, donc $< X|\ \phi >$ est une présentation du groupe libre F_X, c'est -à-dire que F_X est un groupe engendré par $X = \{x_i\}_{i\,\in\,I}$,tel que les x_i ne vérifient aucune relation .*

4. *$(x/\ x^6)$ est une présentation de $\mathbb{Z}_6$.*

Remarque 3.1.1

Tout groupe possède au moins une présentation. L'identité $G \to G$ (vue comme application ensembliste) s'étend de manière unique en un homomorphisme $f : F(G) \to G$.

Alors, $G \simeq F(G)/\ \ker f$, i.e., $(G : \ker f)$ est une présentation de G.

3.2 Présentation d'un groupe monogène d'ordre infini

Théorème 3.2.1 [4]

Pour $n \in \mathbb{N}^*$, $< x|\ \phi >$ est une présentation du groupe monogène d'ordre infini.

Preuve.

Soit F_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 F_X engendré par l'ensemble vide, $R = \{\phi\}$ c'est-à-dire $H = \{1_{F_X}\}$.

On montrons que le groupe quotient F_X/H est isomorphe au groupe monogène $\mathbb{Z}$ d'ordre infini.

Pour montre que $F_X/H \simeq \mathbb{Z}$ il suffit de vérifier que l'ordre de $\bar{x}$ est infini.

On sait que si $F_X = < x >$, alors $F_X/H = < \bar{x} >$.

On considère l'application

$$\begin{aligned} f\ :\ X\ &\rightarrow\ \mathbb{Z} \\ x\ &\mapsto\ 1 \end{aligned}$$

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

$$\varphi\ :\ F_X\ \rightarrow\ \mathbb{Z}$$

φ est un morphisme de groupe, et $\ker\varphi$ sous-groupe normal de F_X.

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

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

Donc

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

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

Finalement $o(\bar{x})$ est infini et

$$F_X/H\ \simeq\ \mathbb{Z}.$$

■

3.3 Présentation d'un groupe cyclique d'ordre n

Théorème 3.3.1 [4]

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

Preuve.

Soit F_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 F_X engendré par $R = \{x^n\}$ est $\{x^{np},\ p \in \mathbb{Z}\}$.

On montre que le groupe quotient F_X/H est isomorphe au groupe cyclique $\mathbb{Z}/n\,\mathbb{Z}$ d'ordre n.

Pour montre que $F_X/H \simeq \mathbb{Z}/n\,\mathbb{Z}$ il suffit de vérifier que $o(\bar{x}) = n$.

On sait que si $F_X = < x >$, alors $F_X/H = < \bar{x} >$.

On considère l'application

$$\begin{aligned} f\ :\ X\ &\to\ \mathbb{Z}/n\,\mathbb{Z} \\ x\ &\mapsto\ \bar{1} \end{aligned}$$

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

$$\varphi\ :\ F_X\ \to\ \mathbb{Z}/n\,\mathbb{Z}$$

φ est un morphisme de groupe, et $\ker\varphi$ sous-groupe normal de F_X, et

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

Donc

$$\begin{aligned} \{x^n\}\ \subseteq\ \ker\varphi\ &\Rightarrow\ H\ \subseteq\ \ker\varphi \\ \text{On a } x^n\ \in\ H\ &\Rightarrow\ (\bar{x})^n\ =\ 1_{F_X/H}. \end{aligned}$$

Maintenant on montre que

$$\begin{aligned} \forall\ 1\ \leq\ k\ <\ n,\ (\bar{x})^k\ &\neq\ 1_{F_X/H} \\ \text{On a } \varphi(x^k)\ &=\ k\ \varphi(x) = k \cdot \bar{1} \neq \bar{0} \\ x^k\ \notin\ \ker\varphi\ &\Rightarrow\ x^k\ \notin\ H\ \Rightarrow\ (\bar{x})^k\ \neq\ 1_{F_X/H} \end{aligned}$$

Donc $o(\bar{x}) = n$ est F_X/H est cyclique d'ordre n est $F_X/H \simeq \mathbb{Z}/n\,\mathbb{Z}$. ■

3.4 Présentation de groupe diédral D_n

Théorème 3.4.1 [4]

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

Preuve.

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

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

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

Pour montrer que F/H est isomorphe au groupe diédral D_n, il suffit de vérifier que, dans ce groupe quotient, $\bar{a}$ est d'ordre n, $\bar{b}$ est d'ordre 2, $\overline{a\ b}$ est d'ordre 2.

Puisque $a^n \in H$, on a évidemment $\bar{a}^n = 1_{F/H}$ et $b^2 \in H$, $\overline{b^2} = 1_{F/H}$ et $a\ b\ a\ b \in H$, on a $\overline{a\ b\ a\ b} = 1_{F/H}$.

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

Considérons l'application

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

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 F, on sait que f peut être prolongée en un unique morphisme

$$\varphi\ :\ F_{\{a,\ b\}}\ \rightarrow\ D_n.$$

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

$$\varphi(a^n) = r^n = id$$
$$\text{donc } \{a^n\}\ \subseteq\ \ker\varphi,\ \text{alors } H\ \subseteq\ \ker\varphi$$
$$a^n\ \in\ H\ \Rightarrow\ \bar{a}^n = 1_{F/H}.$$

De plus

$$\forall\ 1 \leq k < n\ ,\ \varphi(a^k) = r^k \neq id$$
$$\text{alors } a^k \notin \ker\varphi \Rightarrow a^k \notin H$$

Ce qui prouve que $\bar{a}^k \neq 1_{F/H}$.

Ainsi, $\bar{a}$ est bien d'ordre n.

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

Considérons l'application

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

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 F, on sait que f peut être prolongée en un unique morphisme

$$\varphi\ :\ F_{\{a,\ b\}}\ \rightarrow\ D_n.$$

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

$$\varphi(b^2) = s^2 = id$$
$$\text{donc } \{b^2\} \subseteq \ker\varphi,\ \text{alors } H \subseteq \ker\varphi$$
$$b^2 \in H \Rightarrow \overline{b^2} = 1_{F/H}.$$

De plus

$$\text{pour } k = 1\ ,\ \varphi(b) = s \neq id$$
$$\text{Alors } b \notin \ker\varphi \Rightarrow b \notin H$$

Ce qui prouve que $\bar{b} \neq 1_{F/H}$.

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

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

Considérons l'application

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

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 F, on sait que f peut être prolongée en un unique morphisme

$$\varphi \ : \ F_{\{a,\, b\}} \ \rightarrow \ D_n.$$

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

$$\varphi(a\ b\ a\ b) = id$$
$$\text{donc } \{a\ b\ a\ b\} \ \subseteq \ \ker \varphi, \text{ alors } H \ \subseteq \ \ker \varphi$$
$$a\ b\ a\ b \ \in \ H \ \Rightarrow \ \overline{a\ b\ a\ b} = 1_{F/H}.$$

De plus

$$\text{pour } k \ = \ 1 \ , \ \varphi(a\ b) \ \neq \ id$$
$$\text{Alors } a\ b \ \notin \ \ker \varphi \ \Rightarrow \ a\ b \ \notin \ H$$

Ce qui prouve que $\overline{a\ b} \neq 1_{F/H}$.

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

Conclusion générale

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

Nous avons présenté dans un premier temps les définition et quelques propriétés sur les notions suivantes : Généralités sur les groupes, les groupes cycliques, les groupes monogènes et les groupes Diédraux D_n.

Ensuite nous avons présenté la notion de groupe libre sur un ensemble X et la propriété universelle d'un tel groupe F_X qui nous a permis de montrer que tout groupe engendré par un ensemble X est isomorphe à un quotient de F_X.

Finallement nous avons présent :

- ▶ Présentation d'un groupe monogéne d'ordre infini
- ▶ Présentation d'un groupe cyclique d'ordre n
- ▶ Présentation de groupe diédral D_n.

Bibliographie

[1] ABDEREZAK. OULD HOUCINE, Introduction à la Théorie Élémontaire des Groupes Libres, Université Lyon, Année 2009 − 2010.

[2] A. Ben Kilani & S, Msallem Ghorbel, Groupes, Anneaux, Corps, Exemples et Applications, Centre de Publication Universitaire, Tunis, 2006.

[3] A. Kostrikin, Introduction à L'algèbre, Edition MIR, 1986.

[4] D. Guin & T. Hansberger, Algèbre Tome 1 Groupes, Corps et Théorie de Galois, Belin, 1997.

[5] J. Calais, Éléments de Théorie des Groupes, Presses Universitaires de France, Paris, 1998.

[6] J. Marco & Z. Mohamed, Mathématiques L2 Cours Complet avec 700 Tests et Exercices Corrigés, Pearson Education France, Paris, 2007.

[7] N. Bakkai, Groupes Finis et Symetries, Mémoire, Master, Université de M'sila, 2013.

[8] P. S. Alexandroff & Gloden, Introduction à La Théorie des Groupes, Dunod, Paris, 1968.

[9] S. Lang, Structures Algèbriques, Inter Editions, 1976.

[10] WILLIAM J. GILBERT et W. KEITH NICHOLSON, Modern Algebra With Application, John Wiley & Sons ,Inc, Allrights reserved, Année 2004 − 2005.

ملخص

في هذه العمل نعطي اولا مفاهيم عامة حول الزمر، الزمر الدورية، الزمر احادية المنشأ، زمرة 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 n، 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 méttant l'accent sur la propriété universelle qui tout groupe engendré par un ensemble X est isomorphe à un quotient noteé F_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 diédrale, groupe quotient, 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 with a quotient note F_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, diédrale group, quotient group, free group, word, homomorphism, presentations of the groups.