REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Boudiaf de M'sila
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques

Mémoire de Master

Domaine : Mathématiques et Informatique
Filière : Mathématiques
Option : Algèbre et Mathématiques Discrètes

Thème

Les monoïdes inverses et leurs représentations matricielles

Présentée par :
ZEGHBA Zeyneb

Soutenu publiquement le : 23/09/2020

Devant le jury composé de :

Mr.MIHOUBI Douadi	Prof. Université de M'sila	**Président**.
Mr.GHADBANE Nacer	MCA. Université de M'sila	**Encadreur.**
Mr.HEBOUB Lakhdar	MAA. Université de M'sila	**Examinateur.**

Année universitaire 2019/2020

Remerciements

Avant tout, je tiens remercier ALLAH qui m'a donné la force de rédiger ce modeste travail.

Je tiens a remercie **Mr. Nacer GHADBANE** *directeur de mon mémoire, pour sa disponibilité et ses conseils judicieux tout au long de ce travail.*

Je tiens à exprimer tout mes respects à mes respects à ma mère, mes fréres et mes soeurs qui m'ont toujours encouragé.

Je remercie tous les professeurs du département de mathématiques sans oublies aussi mes collègues et amies, tous les étudiants et étudiantes de ma promotion, ainsi tous ceux qui participé de loin ou de près à l'elaboration de ce mémoire.

Je remercie toutes les personnes, famille, amis, qui directement ou indirectement ont contribué à la réalisation de ce travail.

Merci

Notation

Σ : alphabet fini.

Σ^* : monoïde libre sur Σ.

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

$|w|_\alpha$: le nombre d'occurence de lettre α dans le mot w.

L : langage sur l'alphabet Σ.

M : monoïde.

S : semi-groupe.

$End(S)$: l'ensemble des endomorphisme de S.

$\mathrm{Reg}(S)$: les éléments réguliers de S.

$\underset{i=k}{\mathcal{R}}$: relation binaire

$\prod_{i=1} E_i$: produit cartésien d'ensembles.

$M_1 \circledast M_2$: produit semi-direct booléen.

Table des matières

Notation

Introduction **1**

1 Notions élémentaires sur les semi-groupes et les monoïdes **2**

1.1 Généralités sur les semi-groupes et les monoïdes 2

1.2 Relations binaires et leurs propriétés 8

2 Etude sur les éléments idempotents d'un monoïde **13**

2.1 Elément idempotent 13

2.2 Propriétés des éléments idempotents 17

3 La représentation matricielle d'un monoïde inverse **21**

3.1 La représntation matricielle 21

3.2 Monoïde inverse 22

Conclusion **29**

Références **31**

Résumé

Ce mémoire s'inscrit dans le cadre de la théorie des monoïdes.

Au premier chapitre, on rappelle des notions élémentaires sur les semi-groupes et les monoïdes.

À la suit, on étude les éléments idempotents d'un monoïde.

En fin, on s'intéresse à la représentation matricielle d'un monoïde inverse.

Mots clés : Magma, semi-groupe, monoïde, monoïde inverse, semi-groupe inverse, élément idempotent.

Abstract

This memory is part of the theory of monoids.

In the first chapter, we recall elementary notions on semi-groups and monoids.

In the following, we study the idempotent elements of a monoid.

Finally, we are interested in the matrix representation of an inverse monoid.

Keywords : Magma, semigroup, monoid, inverse monoid, inverse semigroup, idempotent element.

Introduction

L'algèbre s'appuie sur les structures algébriques, comme la topologie et l'analyse s'appuient sur les structures topologiques, leurs rencontres générant la topologie algébrique, la géométrie algébrique, etc.

Les monoïdes sont des structures algébriques très simples. Ils peuvent être utiles à l'informatique théorique pour formaliser la théorie des langages.

Dans ce mémoire, nous allons étudier les monoïdes inverses et leurs représentations matricielles.

Ce travail et composé de trois chapitres :

Le premier chapitre, consiste à un rappel des notions élémentaires sur les semigroupes et les monoïdes.

Dans le second chapitre, nous allons étudier les éléments idempotents d'un monoïde.

Dans le troisième chapitre, on fait une étude sur la représentation matricielle d'un monoïde inverse.

Chapitre 1

Notions élémentaires sur les semi-groupes et les monoïdes

Ce premier chapitre contient les définitions et les propriétés des outils que nous utiliserons par la suite : magma, semi-groupe, monoïde, monoïde libre, relation d'équivalence et relation d'ordre.

1.1 Généralités sur les semi-groupes et les monoïdes

Definition 1 Soit E un ensemble. On appelle loi de composition interne ou opération binaire sur E toute application de $E \times E$ dans E.

Definition 2 Lorsqu'un ensemble E est muni d'une opération " $*$ ", on dit que le couple $(E, *)$ forme un magma. Dans le cas où E est fini, on peut consigner la loi " $*$ " qui le structure dans un tableau dénommé table de Cayley. Selon le cas, le magma $(E, *)$ est alors qualifié de commutatif ou associatif.

Definition 3 Soit E un ensemble. Une loi $*$ définie sur E est dite :
• Commutative si : $\forall x, y \in E, x * y = y * x$.
• Associative si : $\forall x, y, z \in E : (x * y) * z = x * (y * z)$.

Definition 4 Soient $(E, *)$ et (F, Δ) deux magmas. Un homomorphisme, ou simplement morphisme, est une application $h : E \longrightarrow F$ telle que :

$\forall x, y \in E : h(x * y) = h(x) \Delta h(y)$. En d'autres termes, un morphisme est une application qui préserve la loi. Quand $E = F$ et $* = \Delta$, on dit h est un endomorphisme.

Un isomorphisme est un morphisme bijectif.

Exemple 1.1 La fonction $\log : \mathbb{R}^+ - \{0\} \longrightarrow \mathbb{R}$ représente un morphisme, et même un isomorphisme de $(\mathbb{R}^+ - \{0\}, \div)$ sur $(\mathbb{R}, -)$, puisque, outre le fait qu'elle soit bijective, on a : $\log(a \div b) = \log(a) - \log(b)$.

Definition 5 Soit $(E, *)$ un magma. On dit qu'un élément $e \in E$ est idempotent si $e * e = e$. Le magma est qualifié d'impotent lorsque tous ses éléments le sont. On dit qu'un élément $e \in E$ est absorbant si $\forall x \in E, x * e = e * x = e$. On dit qu'un élément $e \in E$ est neutre si $\forall x \in E, x * e = e * x = x$. Soit $(E, *)$ un magma admettant un élément neutre e, on dit qu'un élément $x \in E$ est symétrisable s'il existe $x' \in E$ vérifiant $x * x' = x' * x = e$.

- $(\mathbb{N} - \{0\}, +)$ est un magma sans idempotents.
- $(\mathbb{N}, +)$ contient exactement un idempotent, l'entier 0.
- $(\mathbb{N}, +)$ contient deux idempotents 0 et 1.
- $(\mathbb{N}, \min)$ est un magma idempotent.

Definition 6 On appelle semi groupe un magma associatif. Un sous semi groupe d'un semi groupe S toute partie H de S qui constitue un semi groupe pour la loi induite par celle de S. En fait, H est un sous semi groupe de S si et seulement si H est stable pour la loi de S : $\forall x, y \in H, xy \in H$.

Exemple 1.2 $(\mathbb{N} - \{0\}, +), (\mathbb{N}, \min)$ sont des semi groupes.

Definition 7 On appelle monoïde tout semi groupe possédant un élément neutre. ce dernier est généralement noté 1. On note M tout monoïde $(M, *, 1)$.

Exemple 1.3 $(\mathbb{N}, +, 0), (\mathbb{N} \cup \{+\infty\}, \min, +\infty)$ sont des monoïdes.

Remarque 1.1 Un Monoïde $(M, \cdot, 1)$ qui est tel que tout élément de M possède un symétrique est un groupe.

Exemple 1.4 Tout groupe est un monoïde, $(\mathbb{N}, +, 0)$ est un monoïde qui n'est pas un groupe.

Definition 8 Soient M un monoïde et $N \subseteq M$. On dit que N est un sous monoïde de M si :

• $1 \in N$, 1 étant l'élément neutre de M,

• $\forall x, y \in N, xy \in N$, N sous semi groupe de M.

Definition 9 Soient $(M, \cdot, 1_M)$ et $(N, *, 1_N)$ deux monoïdes. Un morphisme de monoïdes $h : M \longrightarrow N$ est une application qui vérifie : $\forall x, y \in M, h(x \cdot y) = h(x) * h(y)$ et $h(1_M) = 1_N$.

Exemple 1.5 La fonction exponentielle représente un isomorphisme de $(\mathbb{R}, +)$ dans $(\mathbb{R}_+ - \{0, \times\})$. Elle est bijective et vérifie :
$\exp(x + y) = \exp(x) \times \exp(y)$ et $\exp(0) = 1$.

Definition 10 Soient $(M, \cdot, 1)$ un monoïde et X, Y deux parties de M. On pose $XY = \{xy / x \in X, y \in Y\}$, l'opération sur les parties ainsi définies donne à l'ensemble $\mathcal{P}(M) = 2^M$ une structure de monoïde.
Soit X une partie de M. On définit sa puissance itérée de la manière suivante :

$$\begin{cases} X^0 = \{1\} \\ X^{n+1} = XX^n, n \geq 0 \end{cases}$$

Puis l'on pose $X^* = \bigcup_{n \geq 0} X^n = \{x_1 x_2 ... x_n / n \geq 0, x_i \in X, 1 \leq i \leq n\}$.

Proposition 1.1 *X^* représente le sous monoïde de M engendré par X, pour tout $X \subseteq M$.*

On a $(\mathbb{N}, +) = \{1\}^*$. Et pour tout élément $n \in \mathbb{N}$, dans le monoïde $(\mathbb{N} \cup \{+\infty\}, \min, +\infty)$, on a $\{n\}^* = \{n, +\infty\}$.

Definition 11 Soit $(M, *, 1)$ un monoïde , une congruence sur $(M, *, 1)$ est une relation d'équivalence $\equiv$ stable par multiplication à droite et à gauche, c'est-a-dire :

$$\forall x, y, z \in M : x \equiv y \Rightarrow x \cdot z \equiv y \cdot z \text{ et } z \cdot x \equiv z \cdot y$$

Definition 12 Soit M un monoïde et $\equiv$ une congruence défine sur M. Le quotient $M/\equiv$ est le monoïde des classes de congruence de M pour la relation $\equiv$. La loi de composition de $M/\equiv$ est définie de la manière suivante : $\overline{u} *_{M/\equiv} \overline{v} = \overline{u *_M v}$.
La projection naturelle (la surjection canonique) de M dans $M/\equiv$ est noté P.

Exemple 1.6 Soit le monoïde $(\mathbb{N}, +)$ et soit la relation $\equiv$ définie par $x \equiv y$ si, et seulement si, x et y ont même parité. la relation $\equiv$ est une congruence. Le quotient de $\mathbb{N}$ par cette relation donne un monoïde comprenant deux éléments, notés $\overline{0}$ et $\overline{1}$ correspondant respectivement aux entiers pairs et impairs.

Definition 13 Soit $\equiv$ une congruence sur un monoïde M.
Une partie X de M est dite saturée par $\equiv$ si $\forall x \in X : \overline{x} \subseteq X$.

Definition 14 Soit $(M, \cdot, 1_M)$ un monoïde. Pour tout couple (x, y) d'éléments de M, le quotient à gauche de x par y noté $y^{-1}x$ est l'ensemble $\{z \in M : y \cdot z = x\}$. Le quotient à gauche d'un sous ensemble de M par y est l'union des quotients des éléments du sous ensemble par y, i.e, si $X \subseteq M$, alors $y^{-1}X = \bigcup_{x \in X} y^{-1}x$.

Definition 15 Soit $(M, \cdot, 1_M)$ un monoïde et A un ensemble de générateurs de M. Le graphe de Cayley (gauche) de M par rapport à A est le graphe (M, E), où $E = \{(x, a, y) \in M \times A \times M : y = a \cdot x\}$.

Definition 16 Soit X un ensemble et M un monoïde, une application $\cdot$ de $M \times X$ dans X est une action à gauche de M sur X si :

1. $\forall x \in X, 1_M \cdot x = x$
2. $\forall x \in X, \forall m_1, m_2 \in M : (m_1 m_2) \cdot x = m_1 \cdot (m_2 \cdot x)$.

Definition 17 Soit Σ un ensemble de symboles, appelé alphabet. Les éléments de Σ sont aussi appelés des lettres.

Definition 18 Soit Σ un alphabet, un mot sur Σ est une suite finie de symbole. Par exemple, 00110 et 110 sont deux mots sur l'alphabet $\{0, 1\}$. La longueur d'un mot w est le nombre de symboles constituant ce mot, on le note $|w|$. Ainsi, $|00110| = 5$ et $|110| = 3$. L'unique mot de longueur 0 est le mot correspondant à la suite vide. Ce

mot s'appelle le mot vide et on le note 1, ou bien ϵ. L'ensemble des mots sur Σ est noté Σ^*. Par exemple

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

• Si σ est une lettre de l'alphabet Σ, pour tout mot $w = a_1 a_2 ... a_k$ de Σ^*, on note par : $|w|_\sigma = card\{i \in \{1, 2, ..., k\} : a_i = \sigma\}$.

le nombre d'occurrences de la lettre σ dans le mot w et $w(i)$ sa i-ème lettre.

Par exemple $|00110|_0 = 3$ et $|00110|_1 = 2$, $00110\,(1) = 0$, $00110\,(4) = 1$.

Exemple 1.7 Le biologiste intéressé par l'étude de l'ADN utilisera un alphabet à quatre lettres $\{A, C, G, T\}$ pour les quatre constituants des gènes : Adénine, Cytosine, Guanine et Thymine.

Proposition 1.2 *Soit Σ un alpabet,*

1. *l'ensemble Σ^* est infini.*

2. *l'ensemble Σ^* est dénombrable.*

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

2. On montre que Σ^* est dénombrable. Comme Σ est fini, on peut donc numéroter ses éléments, par exemple, si $\Sigma = \{\alpha, \beta, \gamma\}$, alors $n\,(\alpha) = 1, n\,(\beta) = 2, n\,(\gamma) = 3$. Ensuite, soit u un mot de Σ^*, on considère les longueurs $|u|$ premiers nombres premiers, par exemple si $|u| = 5$, on a les 5 premiers nombres premiers sont $p(1) = 2, p(2) = 3, p(3) = 5, p(4) = 7, p(5) = 11$. On forme le nombre $f\,(u) = \prod_{i=1}^{i=|u|} p(i)^{n(u(i))}$, où $u\,(i)$ désigne la ième 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 premiers, l'application f est injective. Enfin, comme f est injective et l'ensemble $\mathbb{N}$ est dénombrable, alors Σ^* est dénombrable. ■

Definition 19 La concaténation est l'opération qui associe à deux mots u et v le mot noté $u.v$ ou uv défini par : si $u = \alpha_1\alpha_2...\alpha_n$ et $v = \beta_1\beta_2...\beta_p$, alors $uv = \gamma_1\gamma_2...\gamma_{n+p}$ avec $\gamma_i = \alpha_i$ pour $i = 1, ...n$ et $\gamma_{n+i} = \beta_i$ pour $i = 1, ...p$. Par exemple, la concaté-

nation des mots 00011 et 011 donne le mot 00011011. On vérifie facilement que la concaténation est une opération associative admettant le mot vide comme élément neutre :

$$\forall x, y, z \in \Sigma^* : (xy)z = x(yz).$$
$$\forall x \in \Sigma^* : x\epsilon = \epsilon x = x.$$

Proposition 1.3 *Soit Σ un alphabet quelconque le monoïde Σ^* possède les deux propriétés suivantes :*

1. *tout élément de Σ^* est une suite finie d'éléments de Σ.*

2. *deux suites distinctes d'éléments de Σ définissent deus éléments distincts de Σ^*.*

Proposition 1.4 *Soient t, u, v, w quatre mots de monoïde libre Σ^*.*

1. *Si $tu = vw$ et $|t| \leq |v|$ alors il existe un unique mot z de Σ^* tel que $v = tz$ et $u = zw$.*

2. *Si $uv = wt$ et $|u| = |w|$ alors $u = w$ et $v = t$.*

3. *Pour tout $i \in \mathbb{N} - \{0\}$, $(u^i = v^i \Rightarrow u = v)$.*

4. *Le monoïde libre Σ^* est simplifiable, c'est à dire,*

4.1 $uv = uw \Rightarrow v = w$;

4.2 $uv = wv \Rightarrow u = w$;

4.1 $uvw = utw \Rightarrow v = t$.

5. *Les propositions suivantes sont équivalentes :*

5.1 $uv = vu$,

5.2 *Il existe deux entiers n et m non tous deux nuls tels que $u^n = v^m$,*

5.3 *Il existe un mot z et deux entiers p et q tels que $u = z^p$ et $v = z^q$.*

Exemple 1.8 L'application longueur $|.| : \Sigma^* \longrightarrow \mathbb{N}$ est un morphisme de monoïdes entre $(\Sigma^*, .)$ et $(\mathbb{N}, +)$. En effet,
$\forall u, v \in \Sigma^* : |uv| = |u| + |v|$ et $|\epsilon| = 0$.

Exemple 1.9 Soit $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ un alphabet, $n \in \mathbb{N} \setminus \{0, 1\}$.
La fonction de Parikh $\Psi : \Sigma^* \longrightarrow \mathbb{N}^n$, $\Psi(w) = (|w|_{\alpha_1}, ..., |w|_{\alpha_n})$,
est un morphisme de monoïdes entre $(\Sigma^*, .)$ et $(\mathbb{N}^n, +)$.

Exemple 1.10 Soit $\Sigma = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ un alphabet, $n \in \mathbb{N} \setminus \{0, 1\}$.
Et soit $\lambda : \Sigma \longrightarrow \mathbb{N},\ \alpha_i \longmapsto \lambda(\alpha_i)$. On définit $\widetilde{\lambda} : \Sigma^* \longrightarrow \mathbb{N}$ comme suit : $\widetilde{\lambda}(w) = \sum_{i=1}^{i=n} \lambda(\alpha_i) \left|w\right|_{\alpha_i}$
$\widetilde{\lambda}$ est un homomorphisme de monoïdes.
Et si $\forall 1 \leq i \leq n,\ \lambda(\alpha_i) = 1$, alors $\widetilde{\lambda} = |.|$ (le morphisme de longueur).

La proposition suivante justifie le fait que le monoïde Σ^* soit appelé monoïde libre. Cette propriété caractérise le monoide libre engendré par Σ.

Proposition 1.5 *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. L'esistence : Posons
$\widetilde{\mu}(\epsilon) = e_M$ *et* $\widetilde{\mu}(\alpha_1\alpha_2...\alpha_n) = \mu(\alpha_1)\mu(\alpha_2)...\mu(\alpha_n),\ n \in \mathbb{N},\ \alpha_i \in \Sigma,\ 1 \leq i \leq n.$
Et facile de voir que $\widetilde{\mu}$ est bien un homomorphisme.
Unicité : Soient $\widetilde{\mu}$ et $\widetilde{\lambda}$ deux homomorphismes de A^* dans M tels que :
$\forall \alpha \in A, \widetilde{\mu}(\alpha) = \widetilde{\lambda}(\alpha)$
Alors $\widetilde{\mu}(1) = \widetilde{\lambda}(1) = e_M$ et pour tout mot $w = \alpha_1\alpha_2...\alpha_n$
On a $\widetilde{\mu}(w) = \widetilde{\mu}(\alpha_1\alpha_2...\alpha_n) = \mu(\alpha_1)\mu(\alpha_2)...\mu(\alpha_n) = \widetilde{\lambda}(\alpha_1\alpha_2...\alpha_n) = \widetilde{\lambda}(w)$. ■

1.2 Relations binaires et leurs propriétés

Dans ce qui suit, on donne quelques définitions et notations concernant les relations binaires.

Definition 20 Une relation binaire sur un ensemble E est une partie $\mathcal{R}$ de $E \times E$. Si un couple (x, y) est dans $\mathcal{R}$, on note souvent $x\mathcal{R}y$.

Definition 21 Les relations étants des parties de $E \times E$, on définit de manière usuelle le complémentaire $\rceil(\mathcal{R})$, la réunion $\mathcal{R}_1 \cup \mathcal{R}_2$ et l'intersection $\mathcal{R}_1 \cap \mathcal{R}_2$ de relations $\mathcal{R}_1$ et $\mathcal{R}_2$. On a :

- $(x, y) \in \mathcal{R}_1 \cup \mathcal{R}_2$ si, et seulement si $x\mathcal{R}_1y$ ou $x\mathcal{R}_2y$.
- $(x, y) \in \mathcal{R}_1 \cap \mathcal{R}_2$ si, et seulement si $x\mathcal{R}_1y$ et $x\mathcal{R}_2y$.
- $x\rceil(\mathcal{R})y$ si, et seulement si $(x, y) \notin \mathcal{R}$.

• On dit que $\mathcal{R}_1$ implique $\mathcal{R}_2$ (ce qui revient au même de dire que $\mathcal{R}_2$ contient $\mathcal{R}_1$) si, et seulement si $\mathcal{R}_1 \subseteq \mathcal{R}_2$, c'est-à-dire si, et seulement si pour tout x et y de E, $x\mathcal{R}_1 y \Rightarrow x\mathcal{R}_2 y$.

Definition 22 La composition des relations sur E est l'opération sur $\mathcal{P}(E \times E)$ définie par :
$\forall \mathcal{R}_1, \mathcal{R}_2 \in \mathcal{P}(E \times E), \mathcal{R}_1 \circ \mathcal{R}_2 = \{(x,z) \in E \times E : \exists y \in E, (x,y) \in \mathcal{R}_2, (y,z) \in \mathcal{R}_1\}$.
La composition des relations est associative et admet comme élément neutre la relation identité $\mathcal{R}^0 = \{(x,x)\,/x \in E\}$. Autrement dit, $(\mathcal{P}(E \times E), \circ, \mathcal{R}^0)$ est un monoïde.

Exemple 1.11 Soit E l'ensemble des droites d'un plan affine euclidien et $\mathcal{R}_1 = \mathcal{R}_2 = \perp$ où $\perp$ désigne la relation d'ortogonalité. Alors $\mathcal{R}_1 \circ \mathcal{R}_2 = \shortparallel$ avec $\shortparallel$ désigne la relation de parallélisme. En effet, pour toutes droites D et D' du plan E, on a :

$$\left(D \shortparallel D'\right) \Longleftrightarrow \left(\exists D'', D \perp D'' \text{ et } D'' \perp D'\right).$$

On peut donc écrire ici : $\perp \circ \perp = \shortparallel$.

Definition 23 Une relation binaire $\mathcal{R}$ sur E est dite :
• Réflexive si $\mathcal{R}^0 \subseteq \mathcal{R}$, c'est-à-dire $x\mathcal{R}x$ pour tout $x \in E$.
• Antiréflexive si on a $\mathcal{R}^0 \cap \mathcal{R} = \emptyset$, c'est-à-dire il n'existe pas un élément $x \in E$ qui vérifie $x\mathcal{R}x$.
• Symétrique si on a $\mathcal{R}^{-1} \subseteq \mathcal{R}$, c'est-à-dire $y\mathcal{R}x$ dès que $x\mathcal{R}y$.
• Antisymétrique si $\mathcal{R} \cap \mathcal{R}^{-1} = \mathcal{R}^0$, c'est-à-dire si $x\mathcal{R}y$ et $y\mathcal{R}x$, alors $x = y$.
• Transitive si on a $\mathcal{R} \circ \mathcal{R} \subseteq \mathcal{R}$, c'est-à-dire si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x\mathcal{R}z$.
Un ordre sur un ensemble E est une relation binaire réflexive, antisymétrique et transitive. Un ordre strict est une relation binaire antiréflexive et transitive. Un préordre est une relation binaire réflexive et transitive. Une équivalence est une relation binaire sur E qui est réflexive, symétrique et transitive.
Un ordre $\leq$ sur un ensemble E est total si il vérifie la propriété suivante : $\forall x, y \in E$: $x \leq y$ ou $y \leq x$. A une relation d'ordre $\leq$, on associe la relation d'ordre stricte $<$ définie par : $x < y \Longleftrightarrow x \leq y$ et $x \neq y$.

Soit $\mathcal{R}$ une relation binaire définie sur un ensemble E. On dénote par :
• $E \times E$ la relation pleine.
• $\mathcal{R}^0$ l'identité sur E.

- $\mathcal{R}^n$ la n-ième composition de $\mathcal{R}, \mathcal{R}^n = \mathcal{R} \circ \mathcal{R}^{n-1} = \mathcal{R}^{n-1} \circ \mathcal{R}$, pour $n > 0$.
- $\mathcal{R}^r$ la fermeture réflexive de $\mathcal{R}$.
- $\mathcal{R}^{-1}$ l'inverse de $\mathcal{R}$.
- $\mathcal{R}^s$ la fermeture symétrique de $\mathcal{R}$.
- $\mathcal{R}^+$ ou $\mathcal{R}^t$ la fermeture transitive de $\mathcal{R}$.
- $\mathcal{R}^*$ ou $\mathcal{R}^{rt}$ la fermeture réflexive et transitive de $\mathcal{R}$.
- $\mathcal{R}^{rts}$ la fermeture réflexive, transitive et symétrique de $\mathcal{R}$.

Definition 24 Soient $E_1, ..., E_k$ des ensembles partiellement ordonnés par les relations $\leq_i$, $i = 1, ..., k$, respectivement. L'ordre lexicographique $\preceq$ sur $E_1 \times ... \times E_k = \prod_{i=1}^{i=k} E_i$ est défini par :
$(x_1, ..., x_k) \preceq (y_1, ..., y_k)$ si soit $(x_1, ..., x_k) = (y_1, ..., y_k)$, soit il existe un d, $1 \leq d \leq k$ tel que $x_d \leq_d y_d$ avec $x_d \neq y_d$ et pour tout $i = 1, ..., d-1$,on a $x_i = y_i$.

Exemple 1.12 Soit $E_1 = E_2 = \mathbb{N}$ muni de l'ordre usuel. Alors, avec l'ordre lexicographique $\preceq$ sur $\mathbb{N}^2$, on a les couples $(0, i)$ précèdent les couples $(1, i)$, de même $(1, i)$ précèdent $(2, i)$ et ainsi de suite, pour tout $i \in \mathbb{N}$.

Theorem 1 Soit $\mathcal{R}$ une relation binaire définie sur un ensemble E. Il existe une unique relation d'équivalence $\widetilde{\mathcal{R}}$ telle que :
1. $\mathcal{R} \subseteq \widetilde{\mathcal{R}}$.
2. Si $\hat{\mathcal{R}}$ est une relation d'équivalence vérifiant $\mathcal{R} \subseteq \hat{\mathcal{R}} \subseteq \widetilde{\mathcal{R}}$, alors $\hat{\mathcal{R}} = \widetilde{\mathcal{R}}$.
3. La fermeture d'équivalence de $\mathcal{R}$ est définie par :

$$\widetilde{\mathcal{R}} = \bigcap_{\substack{\mathcal{R} \subseteq \hat{\mathcal{R}} \\ \hat{\mathcal{R}} \text{ relation d'équivalence}}} \hat{\mathcal{R}} \qquad \hat{\mathcal{R}} = \mathcal{R}^0 \bigcup (\bigcup_{n=1}^{+\infty} (\mathcal{R} \cup \mathcal{R}^{-1})^n) = \bigcup_{n=1}^{+\infty} (\mathcal{R} \cup \mathcal{R}^{-1} \cup \mathcal{R}^0)^n.$$

Exemple 1.13 Soit $E = \{1, 2, 3, 4\}$ et $\mathcal{R} = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 4)\}$, on a donc

- $\mathcal{R}^s = \mathcal{R} \cup \mathcal{R}^{-1} = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 4), (3, 1), (3, 2), (4, 3)\}$.
- $\mathcal{R}^r = \mathcal{R} \cup \mathcal{R}^0 = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 4), (1, 1), (2, 2), (3, 3), (4, 4)\}$.
- $\mathcal{R}^+ = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 4), (1, 1), (1, 3), (2, 2), (2, 4)\}$.
- $\mathcal{R}^* = \mathcal{R}^+ \cup \mathcal{R}^r = \{(1, 2), (1, 3), (2, 1), (2, 3), (3, 4), (1, 1), (1, 3), (2, 2)(2, 4), (1, 1), (3, 3), (4, 4)\}$.

• $\widetilde{\mathcal{R}} = \mathcal{R}^* \cup \mathcal{R}^s = \left\{ \begin{array}{c} (1,2),(1,3),(2,1),(2,3),(3,4),(1,1),(2,2)(2,4),(3,3), \\ (4,4),(3,1),(3,2),(4,3),(4,2) \end{array} \right\}$.

Proposition 1.6 *Soit $\mathcal{R}$ une relation binaire définie sur un ensemble E. On a*

1. $(\mathcal{R}^r)^s = (\mathcal{R}^s)^r$.
2. $(\mathcal{R}^r)^t = (\mathcal{R}^t)^r$.
3. $(\mathcal{R}^t)^s \subseteq (\mathcal{R}^s)^t$.

Preuve. On fait remarquer que, pour deux relations binaires $\mathcal{R}_1$ et $\mathcal{R}_2$ quelconques sur un même ensemble E, on a :
$(\mathcal{R}_1 \cup \mathcal{R}_2)^{-1} = \mathcal{R}_1^{-1} \cup \mathcal{R}_2^{-1}$.
Ainsi que, pour toute relation binaire $\mathcal{R}$ sur un ensemble E, on a $(\mathcal{R}^0)^{-1} = \mathcal{R}^0$. Par suite, Pour l'identité (1) on a : $(\mathcal{R}^r)^s = (\mathcal{R} \cup \mathcal{R}^0)^s = (\mathcal{R} \cup \mathcal{R}^0) \cup (\mathcal{R} \cup \mathcal{R}^0)^{-1} =$
$\mathcal{R} \cup \mathcal{R}^0 \cup \mathcal{R}^{-1} \cup (\mathcal{R}^0)^{-1} = \mathcal{R} \cup \mathcal{R}^{-1} \cup \mathcal{R}^0 = \mathcal{R}^s \cup \mathcal{R}^0 = (\mathcal{R}^s)^r$.
Notons que pour toute relation binaire $\mathcal{R}$ sur un ensemble E et pour tout entier n, on a $(\mathcal{R} \cup \mathcal{R}^0)^n = \bigcup_{k=0}^{n} \mathcal{R}^k$. Par conséquent, l'identité (2) s'écrit $(\mathcal{R}^r)^t = (\mathcal{R} \cup \mathcal{R}^0)^t =$
$\bigcup_{n=1}^{+\infty} (\mathcal{R} \cup \mathcal{R}^0)^n = \bigcup_{n=1}^{+\infty} \bigcup_{k=0}^{n} \mathcal{R}^k = \bigcup_{n=1}^{+\infty} \mathcal{R}^n = (\bigcup_{n=1}^{+\infty} \mathcal{R}^n) \cup \mathcal{R}^0 = (\mathcal{R}^t)^r$.
Enfin pour (3), on a,
$(\mathcal{R}^t)^s = (\bigcup_{n=1}^{+\infty} \mathcal{R}^n) \cup (\bigcup_{n=1}^{+\infty} \mathcal{R}^n)^{-1} = (\bigcup_{n=1}^{+\infty} \mathcal{R}^n) \cup (\bigcup_{n=1}^{+\infty} \mathcal{R}^{-n})$,du faite que $\mathcal{R}^{-n}$ est la relation $(\mathcal{R}^{-1})^n$. Toujours par définition on a :
$(\mathcal{R}^s)^t = \bigcup_{n=1}^{+\infty} (\mathcal{R} \cup \mathcal{R}^{-1})^n$.
Or, pour tout entier n non nul, $\mathcal{R}^n$ et $\mathcal{R}^{-n}$ sont contenues dans $(\mathcal{R} \cup \mathcal{R}^{-1})^n$, donc dans $(\mathcal{R}^s)^t$. Donc $\mathcal{R}^t$ et $(\mathcal{R}^{-1})^t$ sont aussi contenues dans $(\mathcal{R}^s)^t$. Ce qui donne bien $(\mathcal{R}^t)^s \subseteq (\mathcal{R}^s)^t$. ■

Proposition 1.7 *Une relation d'équivalence $\mathcal{R}$ sur un ensemble E peut être aussi définie des manières suivantes :*

1. *Par la donnée d'un partition $\mathcal{P}$ de E :*

$x\mathcal{R}y \Longleftrightarrow \exists X \in \mathcal{P}$ *tel que :* $x \in X$ *et* $y \in X$.

2. *Par la donnée d'une application f de E dans un ensemble quelconque F :*

$x\mathcal{R}y \Longleftrightarrow f(x) = f(y)$.

3. *Par la donnée d'une application* h *de* $E \times E$ *dans l'ensemble* $U = \{z \in \mathbb{C} : |z| = 1\}$ *vérifiant la condition :*

$\forall (x, y, z) \in E^3, h(x, y)h(y, z) = h(x, z)$.

en posant, $x\mathcal{R}y \Longleftrightarrow h(x, y) = 1$.

Chapitre 2

Etude sur les éléments idempotents d'un monoïde

Ce chapitre contient la définition de semi-groupe inverse, le produit semi-direct de semi-groupes, et les proprietés des éléments idempotents.

2.1 Elément idempotent

Definition 25 Soit $(E, *)$ un magma. On dit que $x \in E$ est idempotent si $x * x = x$. Si tous les éléments de E sont idempotents pour $*$, alors $(E, *)$ est dit idempotent.

- Dans les monoïdes $(\{0,1\}, \vee)$ et $(\{0,1\}, \wedge)$ du domaine booléen muni de la disjonction logique $\vee$ et de la conjonction logique $\wedge$ respectivement, tout élément est idempotent.
- Dans le monoïde $(F^E, \circ)$ des applications d'un ensemble E dans un sous-ensemble F de E muni de la composition de fonctions " $\circ$ ", les éléments idempotents sont les applications $f : E \to F$ telles que pour tout élément x de E, $f(f(x)) = f(x)$ (l'image de tout élément de E est un point fixe de f). Par exemple l'application identité est idempotente.

Exemple 2.1

1. Dans le monoïdes $(\mathbb{N}, \times)$ les éléments idempotents sont 0 et 1.

2. Dans les monoïdes $(P(E), \cup)$ et $(P(E), \cap)$ de l'ensemble des parties d'un ensemble

E muni de l'union ensembliste $\cup$ et de l'intersection ensembliste $\cap$, respectivement, tout élément est idempotent.

Theorem 2 Soit u un élément idempotent d'un monoïde M et soit

$$G_u = \{m \in Mu \cap uM : u \in Mm \cap mM\} \tag{2.1}$$

L'ensemble G_u est un sous groupe de M qui contient tous les sous groupes de M admettant u pour élément neutre.

Preuve. Soit $u = u^2 \in M$. Par définition un élément $m \in M$ appartient à G_u si, et seulement s'il existe $m_1, m_2, m_3, m_4 \in M$ satisfaisant :

$$\begin{aligned} m &= m_1 u = u m_2 \\ u &= m_3 m = m m_4 \end{aligned}$$

Donc en particulier $u \in G_u$ ($m_1 = m_2 = m_3 = m_4 = 1_M$).
Les deux permières relations donnent

$$\begin{aligned} mu &= m_1 \, \mathrm{u}^2 = m_1 u = m \\ um &= \mathrm{u}^2 m_2 = u m_2 = m \end{aligned}$$

Donc u est un élément neutre pour tous les éléments de G_u.
Soit $m' = m'_1 u = u m'_2$ tel que $u = m'_3 m' = m' m'_4$ un autre élément de G_u. On a

$$\begin{aligned} mm' &= mm'u = umm' \\ m'_3 m_3 mm' &= m'_3 um' = m'_3 m' = u \\ mm' m'_4 m_4 &= mum_4 = mm_4 = u \end{aligned}$$

Donc G_u est un sous ensemble stable de M (C'est à dire $G_u G_u \subset G_u$).
Enfin, d'aprés $u^2 = u = m_3 m$ et $m = um$, on voit que $u = um_3 um$ et il n'y a donc pas de perte de généralité à supposer désormais que $um_3 = m_3 u = m_3$.

Considérons le produit mm_3. En utilisant succeivement les hypothèses $m_3 = m_3u, u = mm_4, m_3m = u, mu = m, mm_4 = u$ on obtient :

$$mm_3 = mm_3u = mm_3mm_4 = mum_4 = mm_4 = u$$

Nous avons établi que G_u est un sous ensemble stable admettant un élément neutre u et ayant la propriété qu'à tout $m \in G_u$ corrspond un élément $m_3 = um_3u$ qui satisfait $u = um_3um = mum_3u$.

Ceci montre d'abord que $um_3u \in G_u$ et que l'ensemble G_u muni du produit de M est isomorphe à un groupe puisque chaque élément possède un inverse. Enfin le groupe G_u est maximal car si les éléments m_5 et m_6 de M sont invariant par multiplication par u et satisfont $u = m_5m_6 = m_6m_5$ ils appartiennent à G_u, d'aprés la défintion même de cet ensemble. Ceci terminé la preuve de théorème. ■

Definition 26 Une famille V de monoïdes est une pseudo variété de monoïdes si elle contient tout sous monoïde, tout monoïde quotient, et tout produit direct de deux membres quelconques de ses membres.

Les monoïdes finis forment une variété, de même que les monoïdes commutatifs ; par contre les groupes cycliques ne forment pas une variété puisque le produit direct de deux groupes cycliques n'est plus nécessairement cyclique.

Proposition 2.1 *On définit une opération de composition entre monoïdes. Pour faciliter l'écriture on considère deux monïdes fixes M_1 et M_2 et l'on désigne par R la famille de tous les ensembles de paires d'éléments $(m_1, m_2) \in M_1 \times M_2$.*
Etant donnés des éléments quelconques $r = \{(m_{1,i}, m_{2,i}) : i \in I_r\} \in R; m_1 \in M_1$ et $m_2 \in M_2$ on définit les éléments m_1r et rm_2 de R par les relations

$$\begin{aligned} m_1r &= \{(m_1m_{1,i}, m_{2,i}) : i \in I_r\} \in R \\ rm_2 &= \{(m_{1,i}, m_{2,i}, m_2) : i \in I_r\} \in R. \end{aligned}$$

Definition 27 Soit $(S, \cdot)$ un semigroupe, un élément a de S est regulier, s'il existe un élément x de S tel que $axa = a$. Si chaque élément de S est regulier, alors on dit que $(S, \cdot)$ est regulier.

Proposition 2.2 *Soit V une variété de groupe. Si M_1 et M_2 appartiennent à la pseudo variété de monoïde finis induite par V il en est de même de leur produit semi-direct booléen $M = M_1 \circledast M_2$.*

Preuve. Soit $u = (u_1, r, u_2) \in M$ un idempotent de M et soit G_u le sous groupe maximal de M qui le contient. Il clair que $u_1 = u^2{}_1, u_2 = u^2{}_2$, et que l'application qui envoie tout $g = (r_1, r_g, m_2) \in G_u$ sur la paire $(m_1, m_2) \in M_1 \times M_2$ est un homomorphisme γ de G_u dans le produit direct $G_{u1} \times G_{u2}$ des sous groups $G_{u1} \in M_1$ et $G_{u2} \in M_2$.

Par construction, le noyeau de γ est l'ensemble N des éléments prouver que N se réduit à $\{u\}$ nous aurons établi que γ est un monomorphisme, C'est à dire que G_u est isomorphe à un sous groupe de $G_{u1} \times G_{u2}$.

Soit donc $m = (u_1, s, u_2) \in N$. Puisque $m \in G_u$, m possède un inverse $\overline{m}$ (relativement à u) C'est à dire qu'il existe un élément $\overline{m} = u\overline{m} = \overline{m}u$ tel que $u = m\overline{m} = \overline{m}m$. Il est clair que $\overline{m}$ à la forme $\overline{m} = (u_1, \overline{s}, u_2)$ pour un certain $\overline{s} \in R$. Nous avons les relations suivantes

$$\begin{aligned} r &= u_1 r \cup r u_2 \ \ (\text{d'aprés } u = u^2) \\ r &= u_1 \overline{s} \cup s u_2 \ \ (\text{d'aprés } u = m\overline{m}) \\ s &= u_1 r \cup u_1 s u_2 \cup u_2 \ (\text{d'aprés } m = umu) \end{aligned}$$

La première relation montre que $u_1 r \subset r$; par conséquent $u_1 r = u_1 u_1 \overline{s} \cup u_1 s u_2 \subset r$ d'aprés la seconde relation et, a fortiori $u_1 s u_2 \subset r$. On a la troisième relation s'écrit aussi $s = r \cup u_1 s u_2$ et par conséquent, on établi $s = r$, c'est à dire $m = u$ pour tout $m \in N$. Ceci achève la vérification que tous les sous groupes du produit semi direct M appartiennent à V. ■

Proposition 2.3 *Si F_1 et F_2 sont deux $V'-$langages sur X il en est de même de leur union $F_1 \cup F_2$, du complément relatif $F_1 \diagdown F_2$ et du produit $F_1 F_2$*

$$F_1 F_2 = \{ff' \in X^* : f \in F_1, f' \in F_2\}.$$

Preuve. Soient $\alpha_1 : X^* \to M_1$ et $\alpha_2 : X^* \to M_2$ tels que $M_1, M_2 \in V. \alpha_1^{-1}\alpha_1 F_1 = F_1; \alpha_2^{-1}\alpha_2 F_2 = F_2$.

Nous considérons le produit semi direct $M = M_1 \oplus M_2$ et définissons une application $\alpha : X^* \to M$ en posant $\alpha e = (\alpha_1 e, \{(\alpha_1 e, \alpha_2 e)\}, \alpha_2 e)$ et pour tout $f \in X^*$

$$\alpha f = (\alpha_1 f, \{(\alpha_1 f', \alpha_2 f'') : f', f'' \in X^*; f'f'' = f\}, \alpha_2 f)$$

Il est clair que α est un homomorphisme de X^* sur un certain sous monoïde $\overline{M}$ de M. De plus si $f \in X^*$ on peut savoir en connaissant seulement son image $\alpha f \in \overline{M}$ si $f \in F_1 \cup F_1$ ou $f \in F_1 \setminus F_2$ ou $f \in F_1 F_2$. Donc $\alpha^{-1}\alpha F = F$ pour $F = F \cup F_1, = F_1 \setminus F_2$ ou $= F_1 F_2$. ■

Definition 28 Soit S un semi-groupe, un élément e dans S est appelé un idempotent si $e^2 = ee = e$.
l'ensemble des idempotents de S est noté par $E(S)$, i.e,
$E(S) = \{e \in S : e^2 = e\}$.

Definition 29 Soit S Un semi-groupe, on dit que S est inverse si pour chaque x dans S il existe un élément unique x^* dans S tel que
(i) $xx^*x = x$;
(ii) $x^*xx^* = x^*$.

Proposition 2.4 *Un monoïde fini M admet un unique idempotent si, et seulement si M est un groupe.*

Preuve. En effet, si M n'admet qu'un seul idempotent, alors il s'agit de l'unité 1_M. Toutes les suites des itérés $(m^n)_{n\in\mathbb{N}}$ contiennent alors 1_M et tout élément est inversible. La réciproque est évidente. ■

2.2 Propriétés des éléments idempotents

Definition 30 On dit qu'un semi-groupe S est un semi-groupe inverse si pour chaque élément a dans S, il existe un élément unique a^{-1} dans S tels que $aa^{-1}a = a$ et $a^{-1}aa^{-1} = a^{-1}$. L'élément a^{-1} est généralement appelé un inverse de a dans S. On note aussi qu'à chaque a dans S correspond une paire d'idempotents e et f tels que :

$$aa^{-1} = e, a^{-1}a = f, ea = a, af = a$$

les idempotents e et f sont appelés respectivement les unités gauche et droite de a.

De plus, pour deux éléments quelconques a, b dans S ;

$$(ab)^{-1} = b^{-1}a^{-1}.$$

Definition 31 On dit que deux éléments a et b d'un semi-groupe S sont inverses l'un de l'autre si et seulement si $aba = a$ et $bab = b$.

Definition 32 Soit S un semi-groupe et soit $a \in S$, $L(a)$ désigne le principal idéal à gauche aS ; $R(a)$ désigne le principal idéal à droite Sa. On définit sur S les trois relations :

$aLb \Longleftrightarrow L(a) = L(b)$;

$aRb \Longleftrightarrow R(a) = R(b)$;

$D = L \circ R$.

Theorem 3 Un système $(S, \cdot, -1)$ est un semi-groupe inverse ssi :

1.$(xy)z = x(yz) \forall x, y, z \in S$;

2.$(x^{-1})^{-1} = x$;

3.$(xx^{-1})(yy^{-1}) = (yy^{-1})(xx^{-1})$;

4.$xx^{-1}x = x$.

Exemple 2.2 Soit $S = \{e, a, b\}$. La table de composition sur S est définie comme suit :

$\cdot$	e	a	b
e	e	a	b
a	a	e	a
b	b	a	e

L'nverse est défini comme suit $''-1''$par $a^{-1} = a, b^{-1} = b$ et $e^{-1} = e$.

Alors,$(S, \cdot, -1)$ est un systéme satisfaisant (2), (3), (4) mais pas (1). Ainsi (1) n'est pas une conséquence du reste.

Exemple 2.3 Soit $S = \{e, a, b\}$. La table de composition sur S est définie comme suit :

	e	a	b
e	e	e	e
a	e	a	b
b	e	a	b

L'nverse est défini comme suit $''-1''$par $a^{-1}=b\ \forall x\in S$.

Alors,$(S,\cdot,-1)$ est un systéme satisfaisant (1), (3), (4) mais pas (2). Ainsi (2) n'est pas une conséquence du reste.

Exemple 2.4 Soit X un ensemble avec $|X|\geq 2$. Prend $S=X\times X$ et on considère dans S le produit défini par $(x_1,y_1)(x_2,y_2)=(x_1,y_2)$ et l'inverse par $(x_1,y_1)^{-1}=(y_1,x_1)$.
Alors $(S,\cdot,-1)$ est un systéme satisfaisant (1),(2),(4) mais pas (3).
Soient $x_1,x_2\in X$ avec $x_1\neq x_2$ et soit $y_1,y_2\in X$, alors $(x_1,y_1)(x_1,y_1)^{-1}(x_2,y_2)(x_2,y_2)^{-1}=(x_1,x_2)$ et $(x_2,y_2)(x_2,y_2)^{-1}(x_1,y_1)(x_1,y_1)^{-1}=(x_2,x_1)\neq(x_1,x_2)$.
Ainsi (3) n'est pas une conséquence du reste.

Exemple 2.5 Soit S un semi-groupe d'entiers positifs muni de la multiplication ordinaire. On définit le produit suivant$'$ dans $S\times S$ par $(a,b)^{-1}.(c,d)=(ac,bd)\forall a,b,c,d\in S$. L'iverse dans $S\times S$ comme suit $(a,b)^{-1}=(b,a)$. Alors S satisfait (1),(2) et (3) mais pas (4), comme $(2,1)(2,1)^{-1}(2,1)=(2,1)(1,2)(2,1)=(4,2)\neq(2,1)$.

Theorem 4 Soit S un semi-groupe inverse, soient $a,b\in S$. Si $a\leq b$, alors $ac\leq bc$ pour tout élément c de S.

Preuve. Supposons que $a\leq b$ et soit $c\in S$. Alors on a $a^{-1}\leq b^{-1}$ et par conséquent $c^{-1}a^{-1}\leq c^{-1}b^{-1}$ et pour que $(c^{-1}a^{-1})^{-1}\leq(c^{-1}b^{-1})^{-1}$ et donc $ac\leq bc$. ■

Theorem 5 Soit S est un semi-groupe inverse et soit $x,y\in S$, alors les propositions suivantes sont équivalentes :
a) $x^{-1}y$ est un idempotent de S,
b) $y^{-1}x$ est un idempotent de S,
c) $yy^{-1}x\leq y$ dans l'ordre partiel naturel sur S,
d) $xx^{-1}y\leq x$ dans l'ordre partiel naturel sur S,

e) $x^{-1}yy^{-1} \leq y^{-1}$,
f) $y^{-1}xx^{-1} \leq x^{-1}$.

Theorem 6 Soit S un semi-groupe inverse et soit $a^{-1}b$ un élément idempotent de S, pour $a, b \in S$. Alors pour tout $c \in S, ac \wedge bc$ existe et est égal à $(a \wedge b)c$.

Theorem 7 Soit $a, b \in S$ et soit $a^{-1}b$ un idempotent de S, alors pour tout $c \in S, ca \wedge cb$ existe et est égal à $c(a \wedge b)$.

Theorem 8 Si S un semi-groupe inverse dans lequel a et a^{-1} commutent $\forall a \in S$, alors tout relation de congruence sur $E(S)$ peut être étendue à une congruence sur S.

Theorem 9 Soit Ω un ensemble non vide, on note $I(\Omega) = \{f : X \subseteq \Omega \longrightarrow Y \subseteq \Omega, f \text{ est bijective}\}$. Pour tout semigroupe inverse $(S, \cdot)$, il existe un ensemble non vide Ω tel que $(S, \cdot)$ est isomorphe à $(I(\Omega), \circ)$.

Proposition 2.5 *Étant donnés un semigroupe S et un groupe G. Soit $f : G \to S$ une application satisfaisant les conditions suivantes :*
i) $f(s^{-1})f(s)f(t) = f(s^{-1})f(st)$;
ii) $f(s)f(t)f(t^{-1}) = f(st)f(t^{-1})$;
iii) $f(s)f(e) = f(s)$.

Alors, il existe un homomorphisme unique $f^{\sim} : S(G) \to S$ tel que $f^{\sim}([t]) = f(t)$.

Proposition 2.6 *Pour tout t dans G. Soit $\varepsilon_t = [t][t^{-1}]$. Ensuite, pour chaque t et s dans G.*
i) ε_t est un idempotent auto-adjoint au sens où $\varepsilon_t^* = \varepsilon_t = \varepsilon_t^2$,
ii) $[t]\varepsilon_s = \varepsilon_{t_s}[t]$,
iii) ε_t et ε_s commute.

Preuve. Voir ([14]) ■

Chapitre 3

La représentation matricielle d'un monoïde inverse

3.1 La représntation matricielle

Proposition 3.1 *Soit Q un ensemble non vide. On considère l'ensemble $I(Q)$ défini par*
$I(Q) = \{f : X \subseteq Q \longrightarrow Y \subseteq Q,\ f$ *est injective*$\}$. *Alors,*
$(I(Q), \circ)$ *est semigroupe inverse.*

Proposition 3.2 *Soit S est un semi-groupe inverse pour chaque s dans S, on définit $\tau_s : S \longrightarrow S$ où $\tau_s(x) = sx$. Alors,*
1. $\tau_s \in I(S)$;
2. *l'application $\tau : S \to I(S)$ définie par $\tau(s) = \tau_s$ est un morphisme.*

Proposition 3.3 *Soit S un semigroup, on a,*
$(S, \cdot)$ *est inverse si, et seulement si, s'il existe un ensemble Q tel que S est isomorphe à $(I(Q), \circ)$.*

Definition 33 Soit S un semigroupe et M un monoïde avec 1 son identité. Pour simplifier la notation, nous écrivons S additivement, sans supposer que S est commutatif. Un action à gauche de M sur S est une application de $M \times S$ dans S définie par $(m, s) \mapsto ms$ et satisfait, pour tous s, s_1 et s_2 dans S, m, m_1 et m_2 dans M :
(i) $m(s_1 + s_2) = ms_1 + ms_2$;

(ii) $m_1(m_2 s) = (m_1 m_2)s$;
(iii) $1s = s$.

Corollaire 3.1 *Bien sûr, cela revient simplement à donner un morphisme d'endomorphismes agissant à gauche de S. cette action permet d'un semi-groupe $S\omega M$ sur l'ensemble $S \times M$ avec la multiplication définie par $(s,m)(s',m') = (s + ms', mm')$. Notez que $S\omega M$ s'appelle un produit semi direct de S et M. De plus, si les élément de $S \times M$ sont représentés par des matrices de la forme $\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}$ où $s \in S$ et $m \in M$. Ensuite la formule précésente peut être écrite comme*

$$\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ s + ms' & mm' \end{pmatrix}.$$

Si les éléments de $S \times M$ sont notés par (s,m), alors on peut définir le produit $M\omega S$ par $(m,s)(m',s') = (mm', sm' + s')$.
Si les éléments de $M \times S$ sont représentés par des matrices de la forme $\begin{pmatrix} m & 0 \\ s & 1 \end{pmatrix}$ alors la formule peut être écrite comme

$$\begin{pmatrix} m & 0 \\ s & 1 \end{pmatrix} \begin{pmatrix} m' & 0 \\ s' & 1 \end{pmatrix} = \begin{pmatrix} mm' & 0 \\ sm' + s' & 1 \end{pmatrix}.$$

Definition 34 Proposition 3.4 *Si S est un semi treillies et soit G est un groupe, alors $S\omega G$ est un semigroupe inverse pour tout action gauche de G sur S.*

3.2 Monoïde inverse

Definition 35 Soient S et T deux monoïdes et soit $End(T)$ le monoïde d'endomorphisme de T, et écrivent les endomorphismes comme exposants à droite des arguments. Si $\alpha : S \to End(T)$ est un homomorphisme et si $s \in S$ et $t \in T$, on écrivant t^s pour $t^{\alpha(s)}$, puisque $\alpha(s) \in End(T)$ pour $s \in S$, alors pour $t_1, t_2 \in T, (t_1,t_2)^s = t_1^s t_2^s$. puisque α est un homomorphisme, $(t^{s_1})^{s_2} = t_{s_1 s_2}$ pour tout $t \in T$ et $s_1, s_2 \in S$.

Le produit semi direct $S \times_\alpha T$ est le monoïde avec les éléments $\{(s,t), s \in S, t \in T\}$ et la multiplication $(s_1,t_1)(s_2,t_2) = (s_1 s_2, t_1^{s_2} t_2)$.

Lemme 3.1 *Soit S un monoïde fortement $\pi - inverse$, alors*
(1) *tous S et T sont des monoïdes fortement $\pi - inverse$;*
(2) $u^2 = u$ *pour tout* $u \in E(S)$ *et tout* $u \in E(T)$;
(3) *Si* $t^e t = t$ *pour* $t \in T$ *et* $e \in E(S)$ *alors* $t^e = t$;
(4) $t^e = t$ *pour tout* $t \in RegT$ *et tout* $e \in E(S)$;
(5) *pour chaque* $s \in S$ *et* $t \in T$ *il existe* $m \in \mathbb{N}$ *tel que* $s^m \in RegS$ *et* $t^{s(m)} \in RegT$, *où* $t^{s(m)} = t^{s^{m-1}} t^{s^{m-2}} .....t^s t$.

Theorem 10 Soit S et T deux monoïdes et soit $S \times_\alpha T$ est un monoïde fortement $\pi - inverse$.
(1) $(e,u) \in E(S \times_\alpha T)$ ssi $e \in E(S)$ et $u \in E(T)$;
(2) Pour tout $e \in E(S)$, soit $\alpha^*(e)$ est un restriction de $\alpha(e)$ dans $E(T)$; alors $\alpha^*(e) \in End(E(T))$;
(3) Soit $\alpha^* : E(S) \to End(E(T))$ tel que $e \longmapsto \alpha^*(e)$; alors α^* est un homomorphisme à $E(S)$ de $End(T)$;
(4) $E(S \times_\alpha T) \cong E(S) \times E(T) \cong E(S) \times_{\alpha^*} E(T)$.

Theorem 11 Soit S et T deux monoïdes et soit $S \times_\alpha T$ est un monoïde fortement $\pi - inverse$.
(1) $(s,t) \in \mathrm{Reg}(S \times_\alpha T)$ ssi $s \in \mathrm{Reg}S$ et $t \in \mathrm{Reg}T$.
(2) Pour tout $s \in \mathrm{Reg}S$, soit $\alpha^*(S)$ est un restriction de $\alpha(s)$ dans $\mathrm{Reg}T$; alors $\alpha^*(s) \in End(\mathrm{Reg}T)$.
(3) Definer α^* :$\mathrm{Reg}S \to End(\mathrm{Reg}T)$ par $s \longmapsto \alpha^*(s)$; alors α^*est un homomorphisme à $\mathrm{Reg}S$ de $End(\mathrm{Reg}T)$.
(4) $\mathrm{Reg}(S \times_\alpha T) \cong \mathrm{Reg}(S) \times_{\alpha^*} \mathrm{Reg}(T)$.

Theorem 12 Soit G un groupe et soit l'inclusion $\subseteq$ est une relation totalement ordonnée sur $Sub(G)$. Considére l'ensemble $M(G) = \{Ha : H \leq G, a \in G\}$, on définit l'opération "$*$" sur $M(G)$ par $Ha * Kb = (H \vee aKa^{-1})ab$. On a :
(i) L'ensemble $(H \vee aka^{-1})ab$ est le plus petit élément de $M(G)$ contenant le produit

$HaKb$;
(ii) $(M(G), *)$ est un monoïde inverse;
(iii) $Sub(G)$ est l'ensemble des idempotents.

Preuve. Puisque la relation d'inclusion est totalement ordonnée sur $Sub(G)$. Alors nous avons $(H \vee aKa^{-1}) = H$ ou $(H \vee aKa^{-1}) = aKa^{-1}$. De plus, pour tous $K \in Sub(G)$ et $a \in G$, $aKa^{-1} \in Sub(G)$ parce que l'ensemble $M(G)$ est fermé sous l'opération $*$. Soit $x = hakb \in HaKb$ arbitrairement où h dans H et k dans K. Puisque h est un élément de $H \subseteq H \vee aKa^{-1}$ et $aka^{-1} \in aKa^{-1} \subseteq H \vee aKa^{-1}$, ainsi $x = (haka^{-1})ab$ dans $(H \vee aKa^{-1})ab$ quels rendenents ça $HaKb \subseteq (H \vee aKa^{-1})ab$. Soit $Lc \in M(G)$ contient $HaKb$. Puisque $HaKb \subseteq Lc, 1_G \in H$ et $1_G \in K$ ainsi $1_G a 1_G b = ab \in Lc$. De plus $HaKb \subseteq Lc$ et $1_G \in K$, implique $Hab \subseteq Lc$. D'autre part, $HaKb = (HaKa^{-1})ab \subseteq Lc$ et $1_G \in H$ implique $(aKa^{-1})ab \subseteq Lc$. Donc nous obtenons $(H \vee aKa^{-1})ab \subseteq Lc$ ce qui complète la preuve de (i). En considérant les éléments Ha, Kb et Lc de $M(G)$ nous avons

$$\begin{aligned}(Ha * Kb) * Lc &= ((H \vee aKa^{-1})ab) * Lc, \\ &= ((H \vee aKa^{-1}) \vee (ab)L(ab)^{-1})(ab)c, \\ &= (H \vee aKa^{-1} \vee abLb^{-1}a^{-1})abc.\end{aligned}$$

Aussi, nous obtenons

$$\begin{aligned}Ha * (Kb * Lc) &= Ha * (K \vee bLb^{-1})bc, \\ &= (H \vee a(K \vee bLb^{-1})a^{-1})abc, \\ &= (H \vee aKa^{-1} \vee abLb^{-1}a^{-1})abc.\end{aligned}$$

Cela montre que l'opération est associative et donc $M(G)$ est un semi-groupe. Si $Ha \in M(G)$ alors $Ha * \{1_G\} = \{1_G\} * Ha = Ha$, où $\{1_G\} = \{1_G\}1_G \in Sub(G) \cap M(G)$. Donc, l'élément identité pour $(M(G), *)$ est $\{1_G\}$.Pour les élément Ha et $(a^{-1}Ha)a^{-1}$ de $M(G)$ nous avons

$$\begin{aligned}(Ha * (a^{-1}Ha)a^{-1}) * Ha &= (H \vee a(a^{-1}Ha)a^{-1})aa^{-1} * Ha, \\ &= (H \vee H)1_G * Ha = H * Ha = Ha.\end{aligned}$$

Et

$$(a^{-1}Ha)a^{-1} * Ha * (a^{-1}Ha)a^{-1} = (a^{-1}Ha)a^{-1},$$

Ce qui montre que $(a^{-1}Ha)a^{-1}$ est un inverse de Ha dans monoïde $(M(G), *)$. Donc la preuve de (ii) est complète. Pour (iii) supposons que Ha est idempotent :

$$Ha = Ha * Ha = (H \vee aHa^{-1})a^{2},$$

Puis, en particulier, $a^{2} = 1_G a^{2} \in Ha$, i.e. $a^{2} = ha$ pour même $h \in H$. Par conséquent $a = h \in H$ donc $Ha = H$. Cela signifie que les idempotents de $(M(G), *)$ sont précisément les sous-groupes de G. De puis que pour deux sous-groupes H, K de $G, H * K = K * H = H \vee K$ ce les idempotent commutent et donc $(M(G), *)$ est un monoïde inverse. ■

Proposition 3.5 *Pour chaque $Ha \in M(G)$, l'application $\tau_{Ha} : M(G) \to M(G)$ définie par $\tau_{Ha}(Kb) = (H \vee aKa^{-1})ab$ où $Kb \in M(G) * (a^{-1}Ha)a^{-1}$ est l'élément de $I(M(G))$. De plus, l'application $\tau : M(G) \to I(M(G))$ définie par $\tau(Ha) = \tau_{Ha}$ est une intégration de $M(G)$ dans $I(M(G))$.*

Preuve. $(M(G), *)$ est un monoïde inverse et en utilisant l'inverse de $Ha \in M(G)$, i.e. $(Ha)^{-1} = (a^{-1}Ha)a^{-1}$ la preuve est complète. ■

Proposition 3.6 *(i) Pour tous $H \in Sub(G), H * M(G) * H$ est le sous semi-groupe inverse de $(M(G), *)$.(ii) Pour tous $Ha \in M(G)$,*

$$Ha * (a^{-1}Ha)a^{-1} * M(G) * Ha * (a^{-1}Ha)a^{-1},$$

Et

$$(a^{-1}Ha)a^{-1} * Ha * M(G) * (a^{-1}Ha)a^{-1} * Ha,$$

sont les sous semi-groupes inverse de $(M(G), *)$.

Preuve. Pour (i) nous utilisons le fait que $E_{M(G)} = sub(G)$.

(ii) Depuis pour tous $Ha \in M(G)$, nous avons $(Ha)^{-1} = (a^{-1}Ha)a^{-1}$,

$$Ha * (a^{-1}Ha)a^{-1} * Ha * (a^{-1}Ha)a^{-1} \in E_{M(G)},$$

Et

$$(a^{-1}Ha)a^{-1} * Ha * (a^{-1}Ha)a^{-1} * Ha \in E_{M(G)},$$

donc la preuve est complète. ■

Theorem 13 Soit $(S, +, 0)$ et $(M, \cdot, 1)$ sont deux monoïdes et considérent l'action gauche de M sur S :

$$\begin{aligned} M \times S &\longrightarrow S \\ (m, s) &\longmapsto ms, \end{aligned}$$

tel qu'il satisfait

- $m(s_1 + s_2) = ms_1 + ms_{2,}$
- $m_1(m_2 s) = (m_1 m_2)S,$
- $1s = s,$
- $m0 = 0.$

Pour tous $s, s_1, s_2 \in S$ et $m, m_{1,} m_2 \in M$. Alors on a,

(i) Pour tous $m \in M$; l'application $\theta_m : S \longrightarrow S, s \longmapsto ms$ est un élément de $End(S)$,

(ii) L'application $\theta : (M, \cdot, 1) \longrightarrow End(S, \circ, id_S), m \longmapsto \theta_m$ est un morphisme de monoïdes.

(iii) L'ensemble $S \times M$ avec la multiplication $(s, m)(s', m') = (s + ms', mm')$ est un monoïde.

(iv) Si $K = \left\{ \begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}, s \in S, m \in M \right\}$, alors $(K, \times)$ est un monoïde.

(v) L'application $h : (S \times M, \cdot) \longrightarrow (K, \times), (s, m) \longmapsto \begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}$ est un isomorphisme des monoïdes.

Preuve. Pour tous $s, s' \in S$, $\theta(s+s') = m(s+s') = ms+ms' = \theta(s)+\theta(s')$ et $\theta(0) = m0 = 0$ donc $\theta_m \in End(S)$ et cela a prouvé (i). De puis pour tous $s \in S$, $\theta_{mm'}(s) = (mm')s$ et $(\theta_m \circ \theta_{m'})(s) = \theta_m(m's) = m(m's)$ donc $\theta(mm') = \theta(m) \circ \theta(m')$ où $m, m' \in M$ qui la partie gauche (ii) prouvé. Pour (iii), la propriété de fermeture découle de la définition de la multiplication comme suit. Prendre des éléments $(s, m), (s', m')$ et (s'', m'') de $S \times M$. Alors

$$\begin{aligned} ((s,m)(s',m'))(s'',m'') &= (s+ms', mm')(s'',m''), \\ &= (s+ms'+(mm')s'', (mm')m''). \end{aligned}$$

Aussi, nous avons dans la même manière que,

$$\begin{aligned} (s,m)((s',m')(s'',m'')) &= (s,m)(s'+m's'', m'm'')), \\ &= (s+m(s'+m's''), m(m'm'')), \\ &= (s+ms'+(mm')s'', m(m'm'')). \end{aligned}$$

Donc la multiplication est associative. De plus, pour tous $(s, m) \in S \times M$

$$(s,m)(0,1) = (0,1)(s,m) = (s,m).$$

Cela implique l'élément identité existe donc $S \times M$ est un monoïde. Pour les éléments $\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix}$ et $\begin{pmatrix} 1 & 0 \\ s'' & m'' \end{pmatrix}$ de K nous avons

$$\begin{aligned} \left[\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix}\right] \times \begin{pmatrix} 1 & 0 \\ s'' & m'' \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ s+ms' & mm' \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s'' & m'' \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ s+ms'+mm's'' & (mm')m'' \end{pmatrix}. \end{aligned}$$

Et

$$\begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \times \left[\begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s'' & m'' \end{pmatrix}\right] = \begin{pmatrix} 1 & 0 \\ s+ms'+mm's'' & m(m'm'') \end{pmatrix}.$$

De tout évidence, l'élément d'identité de $(K, \times)$ est $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Donc $(K, \times)$ est un monoïde. Pour (v), il est facile de voir que h est un bijectif. Aussi pour tous $(s, m), (s', m') \in S \times M$:

$$\begin{aligned} h\left[(s,m)(s',m')\right] &= h(s+ms, mm') = \begin{pmatrix} 1 & 0 \\ s+ms' & mm' \end{pmatrix}, \\ &= \begin{pmatrix} 1 & 0 \\ s & m \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ s' & m' \end{pmatrix}, \\ &= h(s,m) \times h(s',m'). \end{aligned}$$

■

Conclusion

Dans ce mémoire, on a fait une étude sur les monoïdes inverses.

Nous avons présenté dans le premier chapitre les définitions et quelques propriétés sur les semi-groupes et les monoïdes.

Ensuite nous avons fait une étude sur les éléments idempotents d'un monoïde.

Finalement nous avons fait une étude sur la représentation matricielle d'un monoïde inverse.

Bibliographie

[1] **A.H.Clifford and G.B.Preston**, "The algebric theory of semigroups", American Mathematical Society, Providence, vol-I, (1964).

[2] **A.H.Clifford and G.B.Preston**, "The algebric theory of semigroups", American Mathematical Society, Providence, vol-II, (1967).

[3] **T. Connor et J. Vercruysse**, "Algèbre I", Cours pour 2ème année de Bachelier en sciences Mathématiques, (2012).

[4] **E.Bédos and M.D.Norling**, "On fell bundles over inverse semigroups and their left regular representations", New York Journal of Mathematics, Vol. 23, pp, 1013-1044, (2017).

[5] **O. GARET**, "Structures Mathématiques", Université D'orliéans, (2005).

[6] **N. Ghadbane**, "Cours Master 1, semi-groupes et automates finis", Université de M'sila (2018).

[7] **N. Ghadbane**, "The inverse monoid associated to a Group and the semi Direct Product of Groups". Journal of Algebra and Related Topics, Vol. 7, pp, 25-34, (2019).

[8] **M.Nivat**, "Variétés et fonctions rationnelles", Université du Québec à Montréal, (1994).

[9] **L. SMOCH**, "Algèbre-semestre 2", Université du Littoral-Côte d'opale, (2009).

[10] **M.P.SCHÜTZE NBERGER**, "Sur Certains variétés et monoïdes finiis", Institut Blaise Pascal Paris, France.

[11] **K.V.R.SRINVAS and R.NANDAKUMAR**, "ALGEBRAIC PROPERTIES AND EXAMPLES OF INVERSE SEMIGROUPS", REGENCY INTITUTE OF TECHNOLOGY, INDIA, (2009).

[12] **A.TROESCH**, "Structure Algébriques", LYCÉE LOUIS-LE-GRAND, Paris (2018).

[13] **Palle E.T-Jorgensen**, "Parial Actions of groups and actions of inverse semigroups", Proceedings of the American Mathematical Society, Vol. 126, pp, 3481-3494, (1998).

[14] **Y. Z.** SHIZHENGLI, and D. WANG, "Semi direct products and wreath products of strongly $\pi-$inverse monoids", Georgian Mathmatical Journal Vol. 3, pp, 293-300, (1996).