2012-01-01

Inverse Semigroups and Inverse Categories

Alexandra Macedo
University of Texas at El Paso, abogdan@miners.utep.edu

INVERSE SEMIGROUPS AND INVERSE CATEGORIES

ALEXANDRA MACEDO

Department of Mathematical Sciences

APPROVED:

Emil Daniel Schwab, Ph.D., Chair

Helmut Knaust, Ph.D.

Cristian Botez, PhD.

Benjamin C. Flores, Ph.D.
Interim Dean of the Graduate School

Dedicated
to my parents Alexandru and Marta Bogdan,
to my husband Oscar,
and to my daughter Alexa.

INVERSE SEMIGROUPS AND INVERSE CATEGORIES

by

ALEXANDRA MACEDO, M.S.

THESIS

Presented to the Faculty of the Graduate School of

The University of Texas at El Paso

in Partial Fulfillment

of the Requirements

for the Degree of

MASTER OF SCIENCE

Department of Mathematical Sciences

THE UNIVERSITY OF TEXAS AT EL PASO

August 2012

Acknowledgements

I hereby would like to express my deepest gratitude to the honorable members of my thesis committee for their guidance and suggestions. I am most grateful to my advisor and committee chair Dr. Emil Schwab for all his patience, motivation, help, time, and dedication. Without his vast knowledge, superb work ethic, and guidance this Thesis Dissertation would have not been possible. I could not have asked for a better advisor and mentor.

I would like to give special thank to Dr. Helmut Knaust. With his advice, assistance, and support I was able to get through rough academic and administrative challenges. My acknowledgement also goes to Dr. Cristian Botez for accepting to be part of my thesis committee.

Last but not the least, I would like to thank my family for their unconditional love and support.

All in all, this Thesis Dissertation is not only a product of my hard work, but it is also an achievement of those around me.

Abstract

The theory of inverse semigroups forms a major part of semigroup theory. This theory has deep connections with important mathematical disciplines, not only classical ones such as geometry, functional analysis, number theory, but also with more recent theories: the theory of algorithms, graph theory, the mathematical theory of automata, etc. The importance of inverse semigroups, first and foremost, is that they form an abstract class of algebraic structures which are isomorphic to semigroups of partial bijections.

This thesis is organized in two parts, inverse semigroups in Part 1, and inverse categories (that arises if we apply a basic property of inverse semigroups to morphisms of a category) in Part 2.

In the first chapter of my thesis, I set out the basic properties of semigroups and inverse semigroups: this includes the isomorphism theorem for semigroups, the algebraic properties of inverse semigroups connected with inverses, idempotent elements, Green's relations, etc. The examples presented at the end of the first chapter include the inverse semigroups of partial bijections, the free monogenic inverse semigroup and an inverse semigroup-like set which is an analogue of group-like sets. The last example was used in our paper [9], and was one of the examples suggested the need for an inverse semigroup-like set theory.

The theory of inverse categories, a natural generalization of the theory of inverse monoids, may be regarded as the theory of partial isomorphisms. In chapter two of this thesis, I present the basic properties of inverse categories which are analogous to the properties of inverse semigroups. Four examples of inverse categories are discussed (given) at the end of my thesis: the inverse category of partial bijections, the inverse category of invertible matrices, the inverse

category that represent an equivalence relation, and an inverse category as a subcategory of the category of based sets and based functions.

Table of Contents

Chapter 1

Semigroups

The foundations of semigroup theory were set by the Russian mathematician A.K. Suschkewitsch in 1928. At the beginning the theory of semigroups was related and compared with the theory of groups and rings. The study of the semigroups requires also the study of congruences. The first mathematician that introduced the inverse semigroups was V.V. Wagner, in 1952. However, he referred them as *generalized groups.* In 1954 G.B. Preston reintroduced the same theory, but he called them *inverse semigroups*.

1.1 Basic Concepts of Semigroups

A ***semigroup*** is considered to be an algebraic structure $(\mathcal{S}, \mathcal{w}_2)$, where $\mathcal{S}$ is a nonempty set and $\mathcal{w}_2$ is an associative binary operation on $\mathcal{S}$. The binary operation is defined as a function $\mathcal{w}_2 : \mathcal{S} \times \mathcal{S} \to \mathcal{S}$. For simplicity we will denote the binary operation $\mathcal{w}_2(x, y)$ with the multiplication symbol xy, for all $x, y \in \mathcal{S}$. The associative property is $x(yz) = (xy)z$, for any elements $x, y, z \in \mathcal{S}$.

Definition 1.1. *If there exists an element e of a semigroup $\mathcal{S}$ with the property that for all $x \in \mathcal{S}$, we have $ex = xe = x$, then e is called the* ***identity element*** *of $\mathcal{S}$. A semigroup with an identity element is called a* ***monoid****.*

Observation 1.2. From now on, we will denote the identity element by 1. Therefore, the relation above can be written as follows $1x = x1 = x$.

Proposition 1.3. *A monoid cannot have more than one identity element.*

Proof. Let $1 \in \mathcal{S}$ be the identity element such that for any $x \in \mathcal{S}$ we have $1x = x1 = x$. Suppose there is another element $1^{'} \in \mathcal{S}$ with the same property that for any $x \in \mathcal{S}$ we have $1^{'}x = x1^{'} = x$. Using the identity element we can write $1^{'} = 1^{'}1$. We know that $1^{'}x = x$, for any $x \in \mathcal{S}$. This implies that $1^{'} = 1^{'}1 = 1$. Therefore, the identity element is unique. □

Now, we can define the set of all units. The set of all units of $\mathcal{S}$, denoted by $U(\mathcal{S})$, can be described as follows $U(\mathcal{S}) = \{x \in \mathcal{S} \mid \text{there is } a\ x^{'} \in \mathcal{S} \text{ such that } xx^{'} = x^{'}x = 1\} \subseteq \mathcal{S}$.

Definition 1.4. *A* ***zero element*** *of a semigroup $\mathcal{S}$ is an element $\sigma \in \mathcal{S}$ with the property that for all $x \in \mathcal{S}$, we have $\mathcal{S} \neq \{\sigma\}$ and $\sigma x = x\sigma = \sigma$.*

Observation 1.5. From now on, for simplicity, we will denote the zero element by 0. Therefore, the relation above can be written as follows $0x = x0 = 0$.

Proposition 1.6. *A semigroup cannot have more than one zero element*.

Proof. Let $0 \in \mathcal{S}$ be the zero element such that for any $x \in \mathcal{S}$ we have $0x = x0 = 0$. Suppose there is another element $0^{'} \in \mathcal{S}$ with the property that for any $x \in \mathcal{S}$ we have $0^{'}x = x0^{'} = 0^{'}$. Using the fact that $0^{'}x = x0^{'} = 0^{'}$ we can write $0^{'} = 0^{'}0$. For any $x \in \mathcal{S}$ we know that $x0 = 0$, thus, we obtain $0^{'} = 0^{'}0 = 0$. This implies that $0^{'} = 0$. Therefore, the zero element is unique. □

A semigroup is called **commutative** if for any elements x, y from $\mathcal{S}$ we have $xy = yx$. Let $\mathcal{S}$ be a semigroup with $x \in \mathcal{S}$ and consider k a positive integer. We can denote the **power** of an element by the following relations: $x^1 = x$ and $x^{k+1} = x^k x$.

Observation 1.7. Let $\mathcal{S}$ be a monoid and $x \in \mathcal{S}$, then by notation $x^0 = 1$.

Proposition 1.8. *In a semigroup $\mathcal{S}$, for any element $x \in \mathcal{S}$ and n, m any positive integers, the following property holds:* $x^n x^m = x^{n+m}$.

Proof. We will use the induction after n. For $n = 1$ we have $x^m \cdot x^1 = x^{m+1}$ is true. Assume the relation true for $n = k$. Thus, $x^m \cdot x^k = x^{m+k}$. Let $n = k + 1$. We have to prove that $x^m \cdot x^{k+1} = x^{m+k+1}$. So, $x^m \cdot x^{k+1} = x^m \cdot (x^k \cdot x) = (x^m \cdot x^k) \cdot x = x^{m+k} \cdot x = x^{m+k+1}$. □

Definition 1.9. *Let $\mathcal{S}$ be a semigroup and consider an element e from $\mathcal{S}$. The element e is called* ***idempotent,*** *if* $e^2 = e \cdot e = e$.

Observation 1.10. In any semigroup $\mathcal{S}$, if the identity element or the zero element exist, they are idempotents. Also, if e is idempotent, then $e^n = e$, for any n positive integer.

Examples of semigroups:

- Any group is a semigroup.
- Any ring under multiplication is a semigroup.
- $(\mathbb{Z}_+, +)$, $(\mathbb{Z}_+, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}_n, \cdot)$ are semigroups; where $\mathbb{Z}$ is the set of integers,

$\mathbb{Z}_+$ is the set of non-negative integers, $\mathbb{Z}_n$ the complete set of residues modulo *n*, and $+$ and $\cdot$ are the normal operations of addition and multiplication.

- Given $\mathcal{C}$ a category, and *A* is an object of $\mathcal{C}$, then the morphisms in $\mathcal{C}$ from *A* to *A*, $\mathcal{Hom}_{\mathcal{C}}(A, A)$, is a semigroup.
- Let $\mathcal{S}(A) = \{f \mid f: A \to A\}$, where f are functions from A to A, and $\mathcal{S}(A)$ is closed under the usually function composition $\circ$. Then, $(\mathcal{S}(A), \circ)$ is a semigroup and it is called the **symmetric semigroup** on *A*.

Definition 1.11. *Take $\mathcal{S}$ and $\mathcal{S}'$ to be two semigroups such that $\mathcal{S}'$ is the subset of $\mathcal{S}$, $\mathcal{S}' \subseteq \mathcal{S}$. We call $\mathcal{S}'$ a* ***subsemigroup*** *if $\mathcal{S}'$ is closed under multiplication (i.e. for any $x, y \in \mathcal{S}'$, $xy \in \mathcal{S}'$).*

Definition 1.12. *Let $\mathcal{S}$ and $\mathcal{T}$ be two semigroups and consider the mapping $f: \mathcal{S} \to \mathcal{T}$ from $\mathcal{S}$ into $\mathcal{T}$. We say that f is a semigroup* ***homomorphism,*** *if for any , $y \in \mathcal{S}$, $f(xy) = f(x)f(y)$. A bijective semigroup homomorphism is called a semigroup* ***isomorphism***.

Observation 1.13. The composition of two semigroup homomorphisms is a homomorphism. For instance, if $f: \mathcal{S} \to \mathcal{T}$ and $h : \mathcal{T} \to \mathcal{V}$ are homomorphisms, it implies that $(f \circ h) : \mathcal{S} \to \mathcal{V}$ is also a homomorphism.

For $\mathcal{S}$ and $\mathcal{T}$ two monoids and for the mapping $f: \mathcal{S} \to \mathcal{T}$ we can say that f is a **monoid homomorphism** from $\mathcal{S}$ to $\mathcal{T}$**,** if f is a homomorphism that preserves identity elements $f(1) = 1$

Definition 1.14. *Let $\mathcal{S}$ be a semigroup and consider ψ an equivalent relation on $\mathcal{S}$. We say that ψ is a* ***congruence*** *on $\mathcal{S}$, if for any elements x, x', y, y' from $\mathcal{S}$, with the properties $x\,\psi\,y$ and $x'\psi\,y'$, we have $xx'\psi\,yy'$.*

Before we continue with the next properties, we need to introduce more terminology and notations. Given the mapping $f: \mathcal{S} \to \mathcal{T}$ a semigroup homomorphism, we will define an equivalence relation on $\mathcal{S}$, denoted $kerf$, where $kerf \subseteq \mathcal{S}^2$ as it follows: for any $x, \mathrm{y} \in \mathcal{S}$, $x\, kerf\, \mathrm{y}$, if and only if, $f(x) = f(y)$.

Furthermore, we will call the set $\mathcal{S}/kerf$ the quotient of $\mathcal{S}$ by $kerf$ and for any $\hat{x}, \hat{y} \in \mathcal{S}/\ker f$ we will consider the well defined operation $\hat{x}\hat{y} = \widehat{xy}$. It is easy to verify that $(\mathcal{S}/kerf, \cdot)$ is a semigroup called the **quotient semigroup.** We define the projection $p: \mathcal{S} \to \mathcal{S}/ker\, f$ such that $p(x) = \hat{x}$.

Let $\mathcal{S}$ be a semigroup and $\mathcal{S}'$ its subsemigroup. The inclusion mapping $i : \mathcal{S}' \hookrightarrow \mathcal{S}$ is defined by $i(x) = x$.

Proposition 1.15. *Given $f: \mathcal{S} \to \mathcal{T}$ a surjective semigroup homomorphism, let ψ be a congruence on $\mathcal{T}$. Let's define $f^{-1}(\psi)$ by $xf^{-1}(\psi)y$ if and only if, $fx\,\psi\,fy$. Consequently, $f^{-1}(\psi)$ is a congruence on $\mathcal{S}$ that includes* $\ker f$.

Theorem 1.16. *(The Isomorphism Theorem). Given $f: \mathcal{S} \to \mathcal{T}$ a semigroup homomorphism, we have the following statements:*

(i) The image of f, im f is a subsemigroup of $\mathcal{T}$. ($f(\mathcal{S}) = im\, f$).

(ii) $kerf$ is a congruence on $\mathcal{S}$.

(iii) *There exists an unique isomorphism $\theta: \mathcal{S}/ker\, f \to im\, f$ such that the diagram is commutative (i.e. $f = i \circ \theta \circ p$).*

$$\begin{array}{ccc} \mathcal{S} & \xrightarrow{f} & \mathcal{T} \\ p \downarrow & & \uparrow i \\ \mathcal{S}/\,ker f & \xrightarrow[\theta]{} & im\, f \end{array}$$

Figure 1.1 Commutative Diagram for the Isomomorphism Theorem

Proof. *(i)* We have to show that if $y_1,\, y_2 \in im\, f$ then $y_1 y_2 \in im\, f$.

Given $y_1,\, y_2 \in f(\mathcal{S}) = im\, f$, there exist $x_1,\, x_2 \in \mathcal{S}$ such that $f(x_1) = y_1$, $f(x_2) = y_2$ and $x_1 x_2 \in \mathcal{S}$. First we take the product of $y_1 y_2$, and then we substitute $y_1,\, y_2$ with $f(x_1)$ and $f(x_2)$, respectively. The next step is to use the fact that f is a homomorphism. Hence, we obtain $y_1 y_2 = f(x_1) f(x_2) = f(x_1 x_2)$. Since we know that $x_1 x_2 \in \mathcal{S}$, it implies that $f(x_1 x_2) \in f(\mathcal{S})$. So, the product $y_1 y_2 \in f(\mathcal{S}) = im\, f$. Therefore, $im\, f$ is a subsemigroup of $\mathcal{T}$.

(ii) We have to show that $x_1 x_2 \ker f\, y_1 y_2$.

Let $x_1,\, x_2,\, y_1,\, y_2 \in \mathcal{S}$, such that $x_1 \ker f\, y_1$ and $x_2 \ker f\, y_2$. By the definition of the $\ker f$ we have, $x_1 \ker f\, y_1$, it implies that $f(x_1) = f(y_1)$ and $x_2 \ker f\, y_2$ it implies that $f(x_2) = f(y_2)$. In what follows, we will use these equalities as well as the properties of the homomorphism.

$$f(x_1 x_2) = f(x_1) f(x_2) = f(y_1) f(y_2) = f(y_1 y_2) \Longrightarrow x_1 x_2 = y_1 y_2 \Longrightarrow x_1 x_2 \ker f\, y_1 y_2 \,.$$

(iii) We have to show that there exist a isomorphism $\theta: \mathcal{S}/ker\, f \to im\, f$. We take $\theta(\widehat{x}) = f(x)$, where θ is well defined: for any x' from $\widehat{x}$ we have $x' \ker f\, x$ that implies $f(x') = f(x)$.

We will verify that θ is bijective. Let $\widehat{x_1}$, $\widehat{x_2} \in \mathcal{S}/\ker f$ such that $\theta(\widehat{x_1}) = \theta(\widehat{x_2})$. Based on the definition of θ, we know that $\theta(\widehat{x_1}) = f(x_1)$ and $\theta(\widehat{x_2}) = f(x_2)$. Consequently, from $f(x_1) = f(x_2)$ it implies that $x_1 \ker f\, x_2$, thus $\widehat{x_1} = \widehat{x_2}$, hence, θ is injective. Given $y \in im\, f$, there exists $x \in \mathcal{S}$ such that $f(x) = y$. Furthermore, there exists $\hat{x} \in \mathcal{S}/\ker f$ with $\theta(\widehat{x}) = f(x) = y$. So, θ is surjective. Since θ is injective and surjective, it implies θ is bijective.

Now, we will verify that θ is a homomorphism. Let's take $\widehat{x}$, $\widehat{y} \in \mathcal{S}/\ker f$. Then, we have $\theta(\widehat{x}\,\widehat{y}) = \theta(\widehat{xy}) = f(xy) = f(x)f(y) = \theta(\widehat{x})\theta(\hat{y})$, this implies that θ is a homomorphism. Therefore, θ is a isomorphism.

We have to show that $f = i \circ \theta \circ p$ as well as the uniqueness of θ. Given any $x \in \mathcal{S}$, we have:

$$(i \circ \theta \circ p)(x) = (i \circ \theta)\big(p(x)\big) = (i \circ \theta)(\widehat{x}) = i\big(\theta(\widehat{x})\big) = i\big(f(x)\big) = f(x) \Longrightarrow i \circ \theta \circ p = f.$$

Suppose there is another $\theta^{'}: \mathcal{S}/ker\ f \rightarrow im\ f$ with the property that $i \circ \theta' \circ p = f$. Since $i \circ \theta \circ p = f$ and also $i \circ \theta' \circ p = f$, it means that $i \circ \theta \circ p = i \circ \theta' \circ p$. Based on the fact that i is injective, we can imply that $\theta \circ p = \theta^{'} \circ p \Longrightarrow \theta = \theta'$. □

Theorem 1.17. *([7] p.12) If $f: \mathcal{S} \rightarrow \mathcal{T}$ is an injective homomorphism, the homomorphism $h : \mathcal{U} \rightarrow \mathcal{T}$ factors through f ($h = f \circ k$, for some $k: \mathcal{U} \longrightarrow \mathcal{S}$) if and only if, $im\, h \subseteq \mathrm{im}\, f$; then h factors uniquely through f (h is unique).*

Theorem 1.18. *([7] p.12) If $f: \mathcal{S} \rightarrow \mathcal{T}$ is a surjective homomorphism, the homomorphism $h : \mathcal{S} \rightarrow \mathcal{U}$ factors through f ($h = k \circ f$, for some $k: \mathcal{T} \longrightarrow \mathcal{U}$) if and only if, $ker\ f \subseteq \ker h$; then h factors uniquely through f (k is unique).*

Proof. *([7])* If $h : \mathcal{S} \rightarrow \mathcal{U}$ factors through f $(h = k \circ f,\ for\ some\ k)$, then $x \ker f y$ implies $f(x) = f(y)$, $h(x) = k\big(f(x)\big) = k\big(f(y)\big) = h(y)$, and $x \ker h y$. So, $ker\ f \subseteq \ker h$.

Conversely, we will assume that $ker\ f \subseteq \ker h$. We are looking for a homomorphism k that satisfies $k\big(f(z)\big) = h(z)$, for any $z \in \mathcal{S}$. We shall prove that there exists a well defined mapping $k: \mathcal{T} \longrightarrow \mathcal{U}$ which assigns $h(z)$ to $f(z)$, for any $z \in \mathcal{S}$. For each $t \in \mathcal{T}$, there is at least one $h(z)$ to assign to t , since f is surjective. If $h(z')$ and $h(z'')$ are assigned to t, then $t = f(z') = f(z'')$, $z' \ker f\ z''$, $z' \ker h\ z''$, since $ker\ f \subseteq \ker h$ and $h(z') = h(z'')$. Thus at most one element is assigned to t. Hence, a mapping $k: \mathcal{T} \longrightarrow \mathcal{U}$ is well-defined by $k\big(f(z)\big) = h(z)$ for any $z \in \mathcal{S}$.

Since f and h are homomorphisms, $k\big(f(x)f(y)\big) = k\big(f(xy)\big) = h(xy) = h(x)h(y) = k\big(f(x)\big)k\big(f(y)\big)$ for any $f(x), f(y) \in \mathcal{T}$, and k is a homomorphism. Also, by definition we have $h = k \circ f$. If $k': \mathcal{T} \longrightarrow \mathcal{U}$ is another homomorphism such that $h = k' \circ f$, then k and k' agree on $im\ f = \mathcal{T}$, and $k = k'$. □

1.2. Inverse Semigroups

We will begin this section by giving the description of some terms and notations. Let $\mathcal{S}$ be a semigroup and $a \in \mathcal{S}$. We say that a is **regular** if based on the definition there exist $x \in \mathcal{S}$ such that we have $a = axa$. A semigroup $\mathcal{S}$ is called a **regular semigroup** if each element of $\mathcal{S}$ is regular.

Given $\mathcal{S}$ a semigroup and $a, b \in \mathcal{S}$, we say that b is an **inverse** of a if $a = aba$ and $b = bab$ and we say that a and b are mutually inverse. In general, the inverse of an element is not unique in a semigroup.

Definition 1.19. *We call $\mathcal{S}$ an* ***inverse semigroup*** *if each element of $\mathcal{S}$ has an unique inverse.*

We will use for the set of all idempotents of the semigroup $\mathcal{S}$, the following notation: $E(\mathcal{S}) = \{ e \in \mathcal{S} : e^2 = e \}$

Proposition 1.20. *Consider $\mathcal{S}$ a semigroup and $a, b \in \mathcal{S}$,then,*

(i) If a is regular, then a has an inverse.

(ii) If a, b are mutually inverse, then $ab, ba \in E(\mathcal{S})$.

Proof. (i) We have to show that there exist an $b \in \mathcal{S}$ such that $a = aba$ and $b = bab$.

If a is regular it implies that there exists an element $x \in \mathcal{S}$ such that $a = axa$. Let's take the element $b \in \mathcal{S}$ that satisfies the relation $b = xax$. Next, we will substitute $b = xax$ in $a = aba$ and $b = bab$. So, we obtain $aba = a(xax)a = axaxa = (axa)xa = axa = a$ and $bab = (xax)a(xax) = xaxaxax = x(axa)xax = xaxax = x(axa)x = xax = b$. Given the fact that $aba = a$ and $bab = b$, it implies that b is an inverse of a.

(ii) We have to show that $(ab)^2 = ab$ and $(ba)^2 = ba$.

Since a, b are mutually inverse, we have that $a = aba$ and $b = bab$. Thus, using these equalities we get the following $(ab)^2 = abab = (aba)b = ab \implies ab \in E(\mathcal{S})$ and $(ba)^2 = baba = (bab)a = ba \implies ba \in E(\mathcal{S})$. □

If $\mathcal{S}$ is an inverse semigroup, with $a, b \in \mathcal{S}$ and b is the unique inverse of a, then we can denote b by a^{-1} (the inverse of a). As a result, we can write the following observation.

Observation 1.21. *Given $\mathcal{S}$ an inverse semigroup, then,*

(i) $a = aa^{-1}a$ *and* $a^{-1} = a^{-1}aa^{-1}$ *, for any* $a \in \mathcal{S}$.

(ii) $(a^{-1})^{-1} = a$ *, for any* $a \in \mathcal{S}$.

(iii) $e^{-1} = e$ *, for any* $e \in E(\mathcal{S})$.

(iv) $aa^{-1}, a^{-1}a \in E(\mathcal{S})$ *, for any* $a \in \mathcal{S}$.

(v) $\mathcal{S}$ *is a regular semigroup.*

In the following part of the section, we will talk about the Green's relations.

Consider $\mathcal{S}$ a semigroup, and a nonempty subset $\mathcal{A} \subseteq \mathcal{S}$, then $\mathcal{A}$ is a **left ideal** of $\mathcal{S}$, if $\mathcal{S}\mathcal{A} \subseteq \mathcal{A}$ (i.e. for any $x \in \mathcal{S}$ and $a \in \mathcal{A}$ we have $xa \in \mathcal{A}$). We say that $\mathcal{A}$ is a **right ideal** of $\mathcal{S}$, if $\mathcal{A}\mathcal{S} \subseteq \mathcal{A}$ (i.e. for any $x \in \mathcal{S}$ and $a \in \mathcal{A}$ we have $ax \in \mathcal{A}$).

Definition 1.22. *Let $\mathcal{S}$ be a semigroup and $a \in \mathcal{S}$. The smallest left ideal containing a, denoted by $\mathcal{S}^1 a = \mathcal{S}a \cup \{a\}$, is called* ***the left principal ideal*** *generated by a. Analogous, we can define*

the right principal ideal *generated by* a *, denoted by* $a\mathcal{S}^1 = a\mathcal{S} \cup \{a\}$ *as the smallest right ideal containing* a *.*

Definiton 1.23. *Given* $\mathcal{S}$ *a semigroup with* $a, b \in \mathcal{S}$, *Green's Relations* $\mathcal{L}$ and $\mathcal{R}$ *are defined as follow:*

(i) $a\,\mathcal{L}\,b$ *if* $\mathcal{S}^1 a = \mathcal{S}^1 b$, *(i.e. there exist* $x, y \in \mathcal{S}^1$ *such that* $xa = b$ *and* $yb = a$ *).*

(ii) $a\,\mathcal{R}\,b$ *if* $a\mathcal{S}^1 = b\mathcal{S}^1$, *(i.e. there exist* $z, t \in \mathcal{S}^1$ *such that* $az = b$ *and* $bt = a$ *).*

Proposition 1.24. *The Green's Relations* $\mathcal{L}$ *and* $\mathcal{R}$ *commute, if for any* $a, b \in \mathcal{S}$, *there exist* $x, y \in \mathcal{S}$ *such that* $a\,\mathcal{L}\,x\,\mathcal{R}\,b$ *if and only if* $a\mathcal{R}\,y\,\mathcal{L}\,b$ *.*

Proof. Assume that $a\,\mathcal{L}\,x\,\mathcal{R}\,b$, for some $x \in \mathcal{S}$, then there exist $u, v, p, r \in \mathcal{S}^1$, such that $ua = x, vx = a$ and $xp = b,\ br = x$. Since $vx = a$, then $vxr = ar$. Next we will use the fact that $vx = a,\ \ br = x$ and $xp = b$, therefore we have $a = vx = vbr = vxpr$, this implies that $a\,\mathcal{R}\,vxp$. Since $xp = b$, we can notice that $vxp = vb$. Given that $ua = x$, then $b = xp = uap$, since $vx = a$, then $b = xp = uap = uvxp$. This implies that $vxp\,\mathcal{L}\,b$. Since $a\,\mathcal{R}\,vxp$ and $vxp\,\mathcal{L}\,b$ we can conclude that $a\,\mathcal{R}\,vxp\,\mathcal{L}\,b$, therefore, if we denote $vxp = y \in \mathcal{S}$, we have $a\,\mathcal{R}\,y\,\mathcal{L}\,b$. Similarly we can show that if $b\,\mathcal{L}\,y\,\mathcal{R}\,a$, for some $y \in \mathcal{S}$, implies that $b\,\mathcal{R}\,x\,\mathcal{L}\,a$, where $x \in \mathcal{S}$. Therefore, $\mathcal{L}$ and $\mathcal{R}$ commute. □

Both relations, $\mathcal{L}$ and $\mathcal{R}$ are equivalent relations on $\mathcal{S}$ and they commute, as shown in Proposition 1.24. Hence, we can denote the equality $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L} = \mathcal{D}$, where $\mathcal{D}$ is also an equivalent relation.

Next, we will describe some of the notations we will refer later.

$\mathcal{L}_a$ is the $\mathcal{L}$ equivalence class containing a, $\mathcal{R}_a$ is the $\mathcal{R}$ equivalence class containing a , and $\mathcal{D}_a$ is the $\mathcal{D}$ equivalence class containing a .

Given $\mathcal{S}$ a regular semigroup, for any $a \in \mathcal{S}$, then $\mathcal{L}_a$ ($\mathcal{R}_a$) contains at least one idempotent.

Theorem 1.25. *([5] p.130) If $\mathcal{S}$ semigroup, the following statements are equivalent:*

(i) $\mathcal{S}$ is an inverse semigroup.

(ii) $\mathcal{S}$ is regular and the idempotent elements commute.

(iii) For any $a \in \mathcal{S}$, each $\mathcal{L}$– class and each $\mathcal{R}$– class of $\mathcal{S}$, contains an unique idempotent.

Proof. $(i \Longrightarrow ii)$ Given $e, f \in E(\mathcal{S})$. If $x = (ef)^{-1} \Longrightarrow (ef)x(ef) = ef$ and $x(ef)x = x$. Let $y = fxe$, then $y^2 = fxefxe = f(xefx)e = fxe = y \Longrightarrow y^2 = y \in E(\mathcal{S}) \Longrightarrow y^{-1} = y \in E(\mathcal{S})$. Next, we will show that $y^{-1} = ef$ by using the inverse property.

$$(ef)y(ef) = effxeef = efxef = ef$$

$$y(ef)y = (fxe)ef(fxe) = fxeeffxe = fxefxe = yy = y$$

From the above equalities it implies that $y^{-1} = ef \in E(\mathcal{S})$.

The proof for $fe \in E(\mathcal{S})$ is similar. It follows,

$$f(fe)ef = effeef = efef = (ef)^2 = ef.$$

$$fe(ef)fe = feeffe = fefe = (fe)^2 = fe.$$

Thus, $(ef)^{-1} = fe$. Since ef and fe are idempotents, it implies $ef = fe$.

$(ii \Longrightarrow iii)$ If $\mathcal{S}$ is regular it means that each $\mathcal{L}$– class and each $\mathcal{R}$– class of $\mathcal{S}$ contains at least one idempotent. Let $e, f \in E(\mathcal{S})$ such that $e, f \in \mathcal{L}_a \Longrightarrow e \, \mathcal{L} \, f \Longrightarrow$ there exist $x, y \in \mathcal{S}$

such that $xe = f,\ yf = e$. Using these equalities we get:

$$fe = (xe)e = xe^2 = xe = f$$

$$ef = (yf)f = yf^2 = yf = e$$

Given that the idempotents comute, we have $= ef \implies e = f$.

$(iii \implies i)$ We know that each $\mathcal{D}$– class contains an idempotent, then for any $a \in \mathcal{S}$, there is an element $e \in E(\mathcal{S})$ such that $e \in \mathcal{D}_a \implies e\,\mathcal{D}\,a$. So, since $e \in E(\mathcal{S}) \implies e$ is regular and we know that $e\,\mathcal{D}\,a$, thus, for any $a \in \mathcal{S}$, a is regular $\implies \mathcal{S}$ is regular semigroup.

$\mathcal{S}$ regular semigroup with $a \in \mathcal{S}$ it implies that there exists $a' \in \mathcal{S}$ such that $aa'a = a$ and $a'aa' = a'$. Let a', a'' be inverses of $a \implies \left.\begin{matrix} aa'a = a \ \ and \ \ a'aa' = a \\ aa''a = a \ \ and \ \ a''aa'' = a'' \end{matrix}\right| \implies a' = a'(aa')$.

Given $aa'\mathcal{R}a$ and $aa''\mathcal{R}a$ it means that $aa'\ \mathcal{R}\ aa'' \implies aa', aa'' \in \mathcal{R}_a$. Using the fact that $\mathcal{R}$ contains an unique idempotent we have $aa' = aa''$. Similarly we prove $a'a = a''a$.

Hence, $a' = a'(aa') = (a'a)a'' = a''aa'' = a''$. □

Proposition 1.26. *([5] p.131) Let $\mathcal{S}$ be an inverse semigroup, then,*

(i) $(ab)^{-1} = b^{-1}a^{-1}$, *for any $a, b \in \mathcal{S}$.*

(ii) $a^{-1}ea \in E(\mathcal{S})$, $aea^{-1} \in E(\mathcal{S})$, *for any $a \in \mathcal{S}$ and any $e \in E(\mathcal{S})$.*

(iii) $a\,\mathcal{R}\,b$ if and only if $aa^1 = bb^{-1}$, and $a\mathcal{L}b$ if and only if $a^{-1}a = b^{-1}b$, for any $a, b \in \mathcal{S}$.

(iv) If $e, f \in E(\mathcal{S})$, then $e\,\mathcal{D}\,f$ in $\mathcal{S}$ if and only if there exists $a \in \mathcal{S}$ such that $aa^{-1} = e$ and $a^{-1}a = f$.

Proof. *(i)* We have to show that for any $a, b \in \mathcal{S}$ the two equalities below occur $(ab)(b^{-1}a^{-1})(ab) = ab$ and $(b^{-1}a^{-1})(ab)(b^{-1}a^{-1}) = b^{-1}a^{-1}$.

We will use the fact that bb^{-1} and $a^{-1}a$ are idempotents.

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

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

Therefore, $(ab)^{-1} = b^{-1}a^{-1}$, for any $a, b \in \mathcal{S}$.

(ii) We need to show that $(a^{-1}ea)^2 = a^{-1}ea$ and $(aea^{-1})^2 = aea^{-1}$.

$(a^{-1}ea)^2 = a^{-1}ea\, a^{-1}ea = a^{-1}e(a\, a^{-1})ea = a^{-1}(a\, a^{-1})eea = (a^{-1}a\, a^{-1})e^2a = a^{-1}ea$

$(aea^{-1})^2 = aea^{-1}aea^{-1} = ae(a^{-1}a)ea^{-1} = a(a^{-1}a)eea^{-1} = (aa^{-1}a)e^2a^{-1} = aea^{-1}$.

So, $a^{-1}ea \in E(\mathcal{S})$, $aea^{-1} \in E(\mathcal{S})$, for any $a \in \mathcal{S}$ and any $e \in E(\mathcal{S})$.

(iii) ($\Longrightarrow$) Since $a\,\mathcal{R}\,b$, $a\,\mathcal{R}\,aa^{-1}$ and $b\,\mathcal{R}\,bb^{-1}$ it implies $aa^{-1}, bb^{-1} \in \mathcal{R}_a = \mathcal{R}_b$.

We know that $a^{-1}a$ and bb^{-1} are idempotents and that the class of a, $\mathcal{R}_a$ contains a unique idempotent. Therefore, $a^{-1} = bb^{-1}$.

($\Longleftarrow$) Given that $aa^{-1} = bb^{-1}$, $a\,\mathcal{R}\,aa^{-1}$ and $b\,\mathcal{R}\,bb^{-1}$ it implies that $a\,\mathcal{R}\,b$.

The proof for $a\,\mathcal{L}\,b$ is similar.

(iv) From $e\,\mathcal{D}\,f \Longrightarrow e(\mathcal{R} \circ \mathcal{L})f \Longrightarrow$ there exists $a \in \mathcal{S}$ such that $e\,\mathcal{R}\,a$ and $e\,\mathcal{L}\,f$.

Using the statement *(ii)* of the theorem it implies that $ee^{-1} = aa^{-1}$ and $a^{-1}a = f^{-1}f$. Since $e, f \in E(\mathcal{S}) \Longrightarrow aa^{-1} = ee^{-1} = e^2 = e$ and $a^{-1}a = f^{-1}f = f^2 = f$. □

Example 1.27. *The Symmetric Inverse Semigroup on X*

Given any two sets X and Y , we define a **partial function** from X to Y as a function f from a subset of X, called the *domain* of f, $dom(f)$, to a subset of Y, called the *image* of $f, im\, f$

Let A be a subset of X, then the identity function 1_A on A is a partial function from X to X, called *partial identity*. We will denote by $0_{X,Y}$ the empty partial function from X to Y. Next, we will define the composition of two partial functions $f: X \longrightarrow Y$ and $g: Y \longrightarrow Z$, as follows: $(g \circ f)(x) = g\big(f(x)\big)$, where $dom(g \circ f) = \{x \in X \mid f(x) \in dom(g)\}$. Furthermore, we can notice that if $im\, f$ and $dom(g)$ are disjoint, then the composition of f and g is equal to the empty partial function, i.e. $g \circ f = 0_{X,Y}$.

If a partial function $f\colon dom(f) \longrightarrow im\, f$ is bijective, then f is called a **partial bijection**. One of the properties of partial bijections is that the composition of partial bijections is also a partial bijection.

Consider the set $\mathcal{J}(X)$ of all partial bijections from a set X to X. $\mathcal{J}(X)$ is closed under the composition (i.e. if $f, g \in \mathcal{J}(X)$ then $g \circ f \in \mathcal{J}(X)$). Remark that the empty partial function, $0_{X,Y}$ is included in $\mathcal{J}(X)$. If $f\colon X \longrightarrow Y$ is a partial bijection, then f has an inverse, denoted by $f^{-1}\colon Y \longrightarrow X$, such that f^{-1} is also a partial bijection and it follows that $dom(f^{-1}) = im\, f$, $im\, f^{-1} = dom(f)$ and $f^{-1}(y) = x$ if and only if $f(x) = y$. Based on these equalities we can conclude that $f^{-1} \circ f = 1_{dom\,(f)}$, $f \circ f^{-1} = 1_{im\, f}$, $(f^{-1})^{-1} = f$, and $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Thus, $f \circ (f^{-1} \circ f) = f \circ 1_{dom\,(f)} = f$ and $f^{-1} \circ f \circ f^{-1} = f^{-1} \circ 1_{im\, f} = f^{-1}$, hence, $\mathcal{J}(X)$ is a regular semigroup. As a result, we can verify that $\mathcal{J}(X)$ is an inverse semigroup called the **symmetric inverse semigroup** on *X*.

In order to prove that $\mathcal{J}(X)$ is an inverse semigroup, we must show that its itempotents commute. First, we need to be able to recognize the idempotents. The idempotents of $\mathcal{J}(X)$ are the partial identities on X. Let $E(\mathcal{J}(X))$ be the set of all itempotents of $\mathcal{J}(X)$. If $1_A, 1_B \in E(\mathcal{J}(X))$, then we have that $1_A \circ 1_B = 1_{A\cap B}$ and $1_B \circ 1_A = 1_{A\cap B}$, so, $1_A \circ 1_B = 1_B \circ 1_A = 1_{A\cap B}$, it implies that the idempotents commute.

Since we showed that $\mathcal{J}(X)$ is a regular semigroup and that the idempotents commute, we can conclude that $\mathcal{J}(X)$ is an inverse semigroup.

One of the earliest result proved in the inverse semigroup theory is the Wagner-Preston Theorem: "*Any inverse semigroup can be embedded in a symmetric inverse semigroup*". The

Wagner-Preston theorem is an analogue of Cayley's Theorem for groups.

Example 1.28. *The free monogenic inverse semigroup*

The free inverse semigroups are one of the most important and interesting classes of inverse semigroups. In [11] there are presented five isomorphic copies of the free monogenic inverse semigroup. The first isomorphic copy is developed in what follows and is partially related to results from [11]. We give the details of our calculations.

Let $\mathbb{Z}_-$ be the set of non-positive integers, $\mathbb{Z}_+$ the set of non-negative integers, and $\mathbb{Z}$ the set of all integers. Consider the set

$$S = \{(i,u,a) \in \mathbb{Z}_- \times \mathbb{Z} \times \mathbb{Z}_+ |\ i \le u \le a\}$$

equipped with a multiplication defined by

$$(i,u,a) \cdot (j,v,b) = \big(\min(i, j+u), u+v, \max(a, b+u)\big)$$

1) The multiplication is associative:

We have:

$[(i,u,a) \cdot (j,v,b)] \cdot (k,w,c) =$

$$= (\min[\min(i, j+u), k+u+v], u+v+w, \max[\max(a, b+u), c+u+v])$$

and

$(i,u,a) \cdot [(j,v,b) \cdot (k,w,c)] =$

$$= (\min[i, u+\min(j, k+v)], u+v+w, \max[a, u+\max(b, c+v)])$$

In order to show that the multiplication is associative we need to prove that

$$[(i,u,a) \cdot (j,v,b)] \cdot (k,w,c) = (i,u,a) \cdot [(j,v,b) \cdot (k,w,c)]\ .$$

This equality is true only if:

- $\min[\min(i, j+u), k+u+v] = \min[i, u+\min(j, k+v)]$

and

- $\max[\max(a, b+u), c+u+v] = \max[a, u+\max(b, c+v)]$.

We have to consider the following four cases.

a) If $i \le j+u$ and $i \le k+u+v$, then

$$\min[\min(i, j+u), k+u+v] = i$$

and

$$\min[i, u+\min(j, k+v)] = \begin{cases} i, & if\ j \le k+v \\ i, & if\ j \ge k+v \end{cases} .$$

b) If $i \le j+u$ and $i \ge k+u+v$ (that is $j \ge i-u \ge k+v$), then

$$\min[\min(i, j+u), k+u+v] = k+u+v$$

and

$$\min[i, u+\min(j, k+v)] = k+u+v.$$

c) If $i \ge j+u$ and $j+u \le k+u+v$ (therefore $j \le k+v$), then

$$\min[\min(i, j+u), k+u+v] = j+u$$

and

$$\min[i, u+\min(j, k+v)] = j+u.$$

d) If $i \ge j+u$ and $j+u \ge k+u+v$ (consequently $j \ge k+v$), then

$$\min[\min(i, j+u), k+u+v] = k+u+v$$

and

$$\min[i, u+\min(j, k+v)] = k+u+v.$$

We need to check the second equality for the following four cases.

a) If $a \ge b+u$ and $a \ge c+u+v$, then

$$\max[\max(a, b+u), c+u+v] = a$$

and

$$\max[a, u + \max(b, c + v)] = a \text{ in both cases } b \geq c + v \text{ and } b \leq c + v.$$

b) If $a \geq b + u$ and $a \leq c + u + v$ (that is $b \leq a - u \leq c + v$), then

$$\max[\max(a, b + u), c + u + v] = c + u + v$$

and

$$\max[a, u + \max(b, c + v)] = c + u + v \text{ .}$$

c) If $a \leq b + u$ and $b + u \geq c + u + v$ (therefore $b \geq c + v$), then

$$\max[\max(a, b + u), c + u + v] = b + u$$

and

$$\max[a, u + \max(b, c + v)] = b + u \text{ .}$$

d) If $a \leq b + u$ and $b + u \leq c + u + v$ (consequently $b \leq c + v$), then

$$\max[\max(a, b + u), c + u + v] = c + u + v$$

and

$$\max[a, u + \max(b, c + v)] = c + u + v \text{ .}$$

2) The set of the idempotents of $\mathcal{S}$ is

$$E(\mathcal{S}) = \{(i, 0, a) \mid i \in \mathbb{Z}_-;\ a \in \mathbb{Z}_+\} \text{ .}$$

Let's take an element $(i, 0, a)$ from $E(\mathcal{S})$. We can apply the multiplication as follows:

$$(i, 0, a)^2 = (i, 0, a) \cdot (i, 0, a) = (\min(i, i), 0, \max(a, a)) = (i, 0, a).$$

Hence $(i, 0, a)$ is an idempotent. Now, let (i, u, a) be an element of $\mathcal{S}$ such that $(i, u, a)^2 = (i, u, a)$. Then $u + u = u$, and therefore $u = 0$. It follows that $\{(i, 0, a) \mid i \in \mathbb{Z}_-;\ a \in \mathbb{Z}_+\}$ is the set of all idempotents of $\mathcal{S}$.

$2'$) The identity element is $1 = (0,0,0)$.

Let's consider $x = (i, u, a)$ to be an elements of $\mathcal{S}$. The element 1 is an identity element, if $1 \cdot x = x \cdot 1 = x$.

$1 \cdot x = (0,0,0) \cdot (i, u, a) = (\min(0, i + 0), 0 + u, \max(0, a + 0)) = (\min(0, i), u, \max(0, a)) =$

$= (i, u, a)$.

$x \cdot 1 = (i, u, a) \cdot (0,0,0) = (\min(i, 0 + u), u + 0, \max(a, 0 + u)) = (\min(i, u), u, \max(a, u)) =$

$= (i, u, a)$.

Hence, the element $1 = (0,0,0)$ is the identity element of $\mathcal{S}$.

3) The idempotents commute.

Let's take two elements, $(i, 0, a)$ and $(j, 0, b)$ from $E(\mathcal{S})$. In order to prove that the idempotents commute, we need to show that $(i, 0, a) \cdot (j, 0, b) = (j, 0, b) \cdot (i, 0, a)$.

We have:

$(i, 0, a) \cdot (j, 0, b) = (\min(i, j), 0, \max(a, b)) = (\min(j, i), 0, \max(b, a)) = (j, 0, b) \cdot (i, 0, a)$

It follows that the idempotents commute.

4) The inverse of an element.

Let $x = (i, u, a)$ and $x^{-1} = (i - u, -u, a - u)$. Then,

$xx^{-1}x = (i, 0, a)(i, u, a) = (i, u, a) = x$;

$x^{-1}xx^{-1} = (i - u, -u, a - u)(i, 0, a) = (i - u, -u, a - u) = x^{-1}$.

It follows that $x = (i, u, a)$ *and* $x^{-1} = (i - u, -u, a - u)$ are mutually inverse.

The conclusion is that $\mathcal{S}$ is an inverse semigroup. This semigroup is the free inverse semigroup generated by a singleton.

Remark. Since $x^{-1}x = (i-u, 0, a-u)$ *and* $xx^{-1} = (i, 0, a)$, it follows:

$(i,u,a)\mathcal{L}(j,v,b) \Leftrightarrow i-u = j-v$ *and* $a-u = b-v$;

$(i,u,a)\mathcal{R}(j,v,b) \Leftrightarrow i = j$ *and* $a = b$,

where $\mathcal{L}$ and $\mathcal{R}$ are the Green's relations.

The following example is special in the sense that it is not a semigroup. The operation is defined partially with "inverse semigroup properties".

Example 1.29. *An inverse semigroup - like set*

If $\omega: X \times X \to X$ is a partial function (i.e. a function $\omega: D \to X$ where D is a subset of $X \times X$) then it is called a partial binary operation on X. In the following we will refer to an example of partial binary operation with "inverse semigroup" properties.

If $\mathcal{S}$ is a semigroup with zero, then $\mathcal{S}^* = \mathcal{S} - \{0\}$ has a partial binary operation induced by the semigroup product. The set $\mathcal{S}^*$ equipped with this partial binary operation is called a presemigroup. If for any non-zero elements $x, y \in \mathcal{S}$ we have $xy \neq 0$ then the presemigroup $\mathcal{S}^*$ is just a semigroup. Now let P be a set equipped with a partial product. When a 0 is adjoined and all undefined product are defined to be zero then the set $P^0 = P \cup \{0\}$ become a set equipped with a binary operation. This binary operation can be associative or not. In the first case P is a presemigroup, and the semigroup P^0 can be, in particular, an inverse semigroup (with zero).

In this section we will consider a set Q equipped with a partial binary product. Although this is not a presemigroup, we will inspect the "inverse semigroup" properties of this algebraic structures. Recall that if *x* and *y* are elements of Q and the product *xy* is defined, we write $\exists xy$.

Let

$$Q = \left\{(a,b,m) \in {\mathbb{Z}_+}^3 \mid a, b \leq m\right\}$$

equipped with a partial product defined by:

$$(a,b,m)\cdot(a',b',m') = \begin{cases} (a+a'-b,\ b',\ m') & if \quad m \le m',\ \ b \le a' \ and \ \ a'-b \le m'-m \\ (a, b+b'-a', m) & if \quad m \ge m',\ \ b \ge a' \ and \ \ b-a' \le m-m' \end{cases}$$

This partial product is not associative.

For example, if $x=(2,4,4), y=(3,2,6), z=(7,8,20)$ then $x\cdot(y\cdot z)=(6,8,20)$ but $(x\cdot y)\cdot z$ is undefined since $x\cdot y$ is undefined. For this reason, Q is not converted into a semigroup (with zero) by adjoining a zero such that $x\cdot y=0$ if $x\cdot y$ is undefined and $0\cdot x = x\cdot 0 = 0\cdot 0 = 0$.

Now, we will study the inverse semigroup properties of $(Q,\ \cdot)$.

1) Partial associativity:

Let $x=(a,b,m),\ y=(a',b',m'),\ z=(a'',b'',m'')$ *three elements in* Q. *If* $\exists xy,\ \exists yz$ *then* $\exists (xy)z,\ \exists x(yz)$ *and* $(xy)z = x(yz)$.

We consider the following cases:

Case 1: $m \le m', b \le a', a'-b \le m'-m \ and \ m' \le m'', b' \le a'', a''-b' \le m''-m'$.

$$(x\cdot y)\cdot z = [(a,b,m)\cdot(a',b'm')]\cdot(a'',b'',m'') = (a+a'-b,b',m')\cdot(a'',b'',m'')$$

$$= (a+a'-b+a''-b',\ b'',m'') = (a+a'+a''-b'-b,\ b'',m'')$$

$$= (a,b,m)\cdot(a'+a''-b',b'',m'') = (a,b,m)\cdot[(a',b',m')\cdot(a'',b'',m'')]$$

$$= x\cdot(y\cdot z)$$

Case 2: $m \le m', b \le a', a'-b \le m'-m \ and \ m' \ge m'', b' \ge a'', b'-a'' \le m'-m''$.

$$(x\cdot y)\cdot z = [(a,b,m)\cdot(a',b'm')]\cdot(a'',b'',m'') = (a+a'-b,b',m')\cdot(a'',b'',m'')$$

$$= (a+a'-b, b'+b''-a'',m') = (a,b,m)\cdot(a',b'+b''-a'',m')$$

$$= (a,b,m)\cdot[(a',b',m')\cdot(a'',b'',m'')] = x\cdot(y\cdot z) = x\cdot(y\cdot z)$$

Case 3: $m \geq m^{'}, b \geq a^{'}, b - a^{'} \leq m - m' \; and \; m^{'} \geq m^{''}, b^{'} \geq a^{''}, b' - a^{''} \leq m^{'} - m''.$

$$(x \cdot y) \cdot z = [(a, b, m) \cdot (a^{'}, b^{'} m^{'})] \cdot (a^{''}, b^{''}, m^{''}) = (a, b + b^{'} - a', m) \cdot (a^{''}, b^{''}, m^{''})$$

$$= (a, b + b^{'} - a^{'} + b^{''} - a^{''}, m) = (a, b + b^{'} + b^{''} - a^{''} - a', m)$$

$$= (a, b, m) \cdot (a^{'}, b' + b^{''} - a'', m^{'}) = (a, b, m) \cdot [(a^{'}, b^{'}, m^{'}) \cdot (a^{''}, b^{''}, m^{''})]$$

$$= x \cdot (y \cdot z)$$

Case 4: $m \geq m^{'}, b \geq a^{'}, b - a^{'} \leq m - m' \; and \; m^{'} \leq m^{''}, b^{'} \leq a^{''}, a'' - b^{'} \leq m^{''} - m'$.

This particular case can be divided in additional two cases:

- If $m \leq m^{''}, b + b^{'} - a^{'} \leq a^{''} \; and \; a^{''} - b - b^{'} + a^{'} \leq m^{''} - m$, then

$$(x \cdot y) \cdot z = [(a, b, m) \cdot (a^{'}, b^{'} m^{'})] \cdot (a^{''}, b^{''}, m^{''}) = (a, b + b^{'} - a^{'}, m) \cdot (a^{''}, b^{''}, m^{''})$$

$$= (a + a^{''} - b - b^{'} + a^{'}, b^{''}, m'') = (a, b, m) \cdot (a^{''} - b^{'} + a^{'}, b^{''}, m^{''})$$

$$= (a, b, m) \cdot [(a^{'}, b^{'}, m') \cdot (a^{''}, b^{''}, m'')] = x \cdot (y \cdot z)$$

- If $m \geq m^{''}, b + b^{'} - a^{'} \geq a^{''} \; and \; b + b^{'} - a^{'} - a^{''} \leq m - m''$, then

$$(x \cdot y) \cdot z = [(a, b, m) \cdot (a^{'}, b^{'} m^{'})] \cdot (a^{''}, b^{''}, m^{''}) = (a, b + b^{'} - a^{'}, m) \cdot (a^{''}, b^{''}, m^{''})$$

$$= (a, b + b^{'} - a^{'} + b^{''} - a^{''}, m) = (a, b, m) \cdot (a^{'} + a^{''} - b^{'}, b^{''}, m^{''})$$

$$= (a, b, m) \cdot [(a^{'}, b^{'}, m') \cdot (a^{''}, b^{''}, m'')] = x \cdot (y \cdot z).$$

2) The set of the idempotents of Q is

$$E(Q) = \{(a, a, m) \in Q\}.$$

3) The idempotents commute:

$If \;\; e, f \; \in E(Q) \; such \; that \;\; \exists \; e \cdot f \;\; then \;\; \exists \; f \cdot e \;\; and \;\; e \cdot f = f \cdot e \in E(Q).$

4) The inverse:

Let $x = (a, b, m)$ and $x^{-1} = (b, a, m)$. Then,

(a) $(x^{-1})^{-1} = x$; if $\exists\, x \cdot y$ $then$ $\exists\, y^{-1} \cdot x^{-1}$ and $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$;

(b) $\exists\, x^{-1} \cdot x$, $\exists\, x \cdot x^{-1}$ and $x^{-1} \cdot x = (b, b, m)$, $x \cdot x^{-1} = (a, a, m)$.

Moreover:

(c) $\exists\, x \cdot (x^{-1} \cdot x)$, $\exists\, (x \cdot x^{-1}) \cdot x$ and $x \cdot (x^{-1} \cdot x) = (x \cdot x^{-1}) \cdot x = x$.

Remarks.

1. Consulting the properties 1) - 4) of 1.28 and 1.29, we find a correlation between these properties. Therefore we used the name “inverse semigroup – like set” in the title of Example 1.29.

2. Following Jekel [4] and Lawson [7], a group-like set P is a set equipped with a partial binary operation $\circ$, with a distinguished element 1, and an involution $x \longmapsto x^{-1}$ $((x^{-1})^{-1} = x)$, satisfying the following axioms:

(P_1) $\exists\, (x, 1)$, $\exists\, (1, x)$ and $1 \circ x = x \circ 1 = x$ for all $x \in P$;

(P_2) $\exists\, (x, x^{-1})$, $\exists\, (x^{-1}, x)$ and $x \circ x^{-1} = x^{-1} \circ x = 1$ for all $x \in P$;

(P_3) if $\exists\, (x, x^{-1})$, $\exists\, (x^{-1}, x)$ and $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

An example of a group-like set is the set of integers $\mathbb{Z}$ with the usual addition on the set $D = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid xy \leq 0\}$ as the partial binary operation, 0 is the distinguished element, and $x \longmapsto -x$ is the involution.

We can see that $\big(3 + (-5)\big) + 7 = 5$ but $3 + (-5 + 7)$ is not defined and therefore, $\big(3 + (-5)\big) + 7 \neq 3 + (-5 + 7)$. Thus in the group-like set of integers the usual addition is not associative and the group-like set of integers cannot be converted into a semigroup (with zero) by adjoining a zero such that $x \circ y = 0$ if $x \circ y$ is undefined.

Chapter 2

Categories

The foundations of the theory of categories were set in 1945 when the article “General Theory of Natural Equivalences” of S. Eilemberg and S. MacLane was published. The theory of categories is a branch of mathematics that studies the properties of particular mathematical concepts in an abstract approach. Various fields of mathematics can be characterized as categories. By using the theory of categories several mathematical results were stated and proved, much easier than with any other method.

2.1. Basic Concepts of Categories

Definition 2.1. *A **category** $\mathcal{C}$ is a mathematical concept given by:*

(i) A class of objects of $\mathcal{C}$, denoted $Ob\ \mathcal{C}$, whose elements are called objects of $\mathcal{C}$.

(ii) For each pair of objects (A,B) from $Ob\ \mathcal{C}$, a set denoted $\mathcal{H}om_{\mathcal{C}}(A,B)$ and called the set of morphisms from A to B.

(iii) For each three objects A, B, C from $Ob\ \mathcal{C}$, a mapping

$$\mu_{ABC}\colon \mathcal{H}om_{\mathcal{C}}(A,B)\times\mathcal{H}om_{\mathcal{C}}(B,C)\longrightarrow\mathcal{H}om_{\mathcal{C}}(A,C)$$

*is called the **composition of morphisms**.*

The concept of category complies with the following axioms:

Ax1. *If (A,B) and (C,D) are two distinct pairs of objects from $\mathcal{C}$, then $\mathcal{H}om_{\mathcal{C}}(A,B)$* and $\mathcal{H}om_{\mathcal{C}}(C,D)$ are disjoint.

Ax2. *If $f\in\mathcal{H}om_{\mathcal{C}}(A,B)$, $g\in\mathcal{H}om_{\mathcal{C}}(B,C)$, $h\in\mathcal{H}om_{\mathcal{C}}(C,D)$ are arbitrary, then the composition of morphisms is associative: $\mu_{ACD}(\mu_{ABC}(f,g),h)=\mu_{ABD}\big(f,\mu_{BCD}(g,h)\big)$.*

Ax3. *For each object* $A \in Ob\,\mathcal{C}$*, there exists an element* $1_A \in \mathcal{H}om_{\mathcal{C}}(A,A)$*, such that, for each* $X \in Ob\,\mathcal{C}$*:* $f \in \mathcal{H}om_{\mathcal{C}}(A,X)$ then $\mu_{AAX}(1_A, f) = f$ *and*

$g \in \mathcal{H}om_{\mathcal{C}}(X,A)$ then $\mu_{XAA}(g, 1_A) = g$.

Definition 2.2. *For any* $A \in Ob\,\mathcal{C}$*, the morphism* 1_A *, is called the* ***identity morphism****.*

The identity morphism is unique.

Definition 2.3. *We call* $\mathcal{C}$ *a* ***small category*** *if* $Ob\,\mathcal{C}$ *is a set.*

Definition 2.4. *A category* $\mathcal{C}$ *is called* ***subcategory*** *of the category* $\mathcal{D}$*, denoted by* $\mathcal{C} \subseteq \mathcal{D}$*, if:*

(i) $Ob\,\mathcal{C} \subseteq Ob\,\mathcal{D}$

(ii) *For each A, B from* $Ob\,\mathcal{C}$*,* $\mathcal{H}om_{\mathcal{C}}(A,B) \subseteq \mathcal{H}om_{\mathcal{D}}(A,B)$

(iii) *The composition of morphisms from* $\mathcal{C}$ *is induced by the composition of morphisms from* $\mathcal{D}$*.*

(iv) *For each* $A \in Ob\,\mathcal{C}$ *the morphism* $1_A \in \mathcal{H}om_{\mathcal{D}}(A,A)$ *belongs to* $\mathcal{H}om_{\mathcal{C}}(A,A)$*.*

There are many examples of categories. Next, we will describe a few of them.

- *Rel (the category of binary relations)* – The objects are sets, the morphisms, $\mathcal{H}om_{Rel}(A,B) = \{\, (A,B,R) \mid R \subseteq A \times B \,\}$ are binary relations from A to B and μ is the usual composition of binary relations.
- *Ens (the category of sets)* – The objects of Ens are sets, the morphisms from A to B are functions from A to B and the product of morphisms is the usual composition of functions.
- *Grp (the category of groups)* – The objects are groups, the morphisms are group

homomorphisms and the product of morphisms is the usual composition.

- *Ord (the category of the ordered sets)* – The objects are the ordered sets (posets), the morphisms are the isotone functions and the product of morphisms is the usual composition of functions.

- *Rng (the category of rings)* − The objects are rings, the morphisms are ring homomorphisms and the product of morphisms is the usual composition. *Rngu* is the category of rings with unity.

- R^{Mod} *(the category of R−modules)* − The objects are R-modules, the morphisms are *R*−modules homomorphisms and the product of morphisms is the usual composition of functions.

- $\mathcal{m}_{\mathbb{R}}$ *(the category of matrices with real elements)* − The objects are the positive integers $Ob\,\mathcal{m}_{\mathbb{R}} = \mathbb{Z}_{+} = \{1, 2, 3, ...\}$, the morphisms are the sets of matrices $\mathcal{Hom}(n, m) = \left\{ \left(a_{ij}\right)_{n\times m} \mid a_{ij} \in \mathbb{R} \right\}$ and the product of morphisms is the usual product of matrices.

- $\mathcal{C}_p$ *(the ordered category of a poset* $(\mathcal{P}, \leq)$) – The objects are the elements of a poset, $\mathcal{P},\ Ob\,\mathcal{C}_p = \mathcal{P}$, the morphisms are $\mathcal{Hom}_{\mathcal{C}}(x, y) = \begin{cases} \{(x, y)\}, & if\ x \leq y \\ \emptyset, & if\ x \nleq y \end{cases}$, and the composition is $x \leq y,\ y \leq z \Longrightarrow x \leq z.$ For the case of the composition of morphisms we use the notation $(x, y)(y, z) = (x, z)$.

- *Latt* – The objects are lattices, the morphisms are homomorphisms of lattices and the product μ is the usual composition of functions.

Before we continue with the next theorems, for simplicity, we will use the notation :

$f: A \longrightarrow B$ or $A \xrightarrow{f} B$, as a replacement for $f \in \mathcal{Hom}_{\mathcal{C}}(A, B)$. In this case A is called the *domain* and B is called the *codomain*. If $f: A \longrightarrow B$ and $: B \longrightarrow C$, then we will denote $\mu_{ABC}(f, g) = gf$.

Definition 2.5. *Let $\mathcal{C}$ be a category, $f \in \mathcal{H}om_{\mathcal{C}}(A, B)$, then:*

*(i) f is a **monomorphism**, if for any $u, v \in \mathcal{H}om_{\mathcal{C}}(X, A)$, $fu = fv \Longrightarrow u = v$.*

*(ii) f is an **epimorphism**, if for any $u, v \in \mathcal{H}om_{\mathcal{C}}(B, Y)$, $uf = vf \Longrightarrow u = v$.*

*(iii) f is a **bimorphism**, if f is a monomorphism and f is an epimorphism.*

In the following, we will give a few examples of monomorphisms, epimorphisms and bimorphisms.

Proposition 2.6. *Let $f: A \longrightarrow B$ be a morphism in Ens, then:*

(i) f is monomorphism if and only if f is an injective function. Also, this statement is true in the case of the categories Grp, Rngu, R^{Mod}.

(ii) f is epimorphism if and only if f is a surjective function. Also, this statement is true in the case of the categories Grp and R^{Mod}.

Proof. *(i)*$(\Longrightarrow)$ Given that f is a monomorphism, suppose $x_1, x_2 \in A$ such that $x_1 \neq x_2$ $f(x_1) = f(x_2)$. Let $X = \{x_1, x_2\}$, $u: X \longrightarrow A$ and $v: X \longrightarrow A$ such that $u(x) = x_1$ and $v(x) = x_2$ for any $x \in X$.

$(fu)(x) = f\big(u(x)\big) = f(x_1) = f(x_2) = f\big(v(x)\big) = (fv)(x) \Longrightarrow fu = fv$, but $u \neq v$.

Contradiction with f monomorphism.

($\Longleftarrow$) Let f be an injective function and consider $u: X \longrightarrow A$ and $v: X \longrightarrow A$ such that $fu = fv \Longrightarrow (fu)(x) = (fv)(x) \Longrightarrow f\big(u(x)\big) = f\big(v(x)\big)$, for any $x \in X$.

Since f is an injective function, it implies that $(x) = v(x) \Longrightarrow u = v$, for any $x \in X$.

(ii)($\Longrightarrow$) Given that $f: A \longrightarrow B$ is an epimorphism, suppose that f is not surjective. Let's take an element $b_0 \in B$ such that $b_0 \notin Imf$. Consider $Y = \{*,\ b_0\}$, where $* =$ is not an element of *B*. Let $u: B \longrightarrow Y$ and $v: B \longrightarrow Y$ such that $u(y) = *$ and $v(y) = \begin{cases} *, & if\ y \neq b_0 \\ b_0, & if\ y = b_0 \end{cases}$,

for any $y \in B$.

$(uf)(x) = u\big(f(x)\big) = * = v\big(f(x)\big) = (vf)(x) \Longrightarrow uf = vf$, but $u \neq v$, for any $x \in A$.

Contradiction with f epimorphism.

($\Longleftarrow$) Assume f is a surjective function, it implies that for any $y \in B$, there exists $x \in A$ such that $f(x) = y$. Let $u: B \longrightarrow Y$ and $v: B \longrightarrow Y$ such that $uf = vf$.

$u(y) = u\big(f(x)\big) = (uf)(x) = (vf)(x) = v\big(f(x)\big) = v(y)$, for any $y \in B$. Therefore, $u = v$.

□

Theorem 2.7. *Let* $\mathcal{M}_{\mathbb{R}}$ *be a category of matrices. Consider* $A: n \longrightarrow m$ *a morphism in* $\mathcal{M}_{\mathbb{R}}$ *and* $A = \left(a_{ij}\right)_{m\times n}$. *Then*

(i) A is a monomorphism if and only if $rank\ A = n$.

(ii) A is an epimorphism if and only if $rank\ A = m$.

Proof. *(i)* We have $A: n \longrightarrow m$ in $\mathcal{M}_{\mathbb{R}}$, $A = \left(a_{ij}\right)_{m\times n}$ .We will consider the system below.

$$S = \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0 \end{cases}.$$

The system S has one solution if $rank\ A = n$, where n is the number of columns. If $A > n$, then we have more than one solution.

($\Longrightarrow$) A is monomorphism if and only if, for any $U: p \longrightarrow n$ and $V: p \longrightarrow n$ such that $AU = AV \Longrightarrow U = V$. Suppose $rank\ A \neq n$, then there exists $(x_1^0, x_2^0, \dots, x_n^0)$ a nontrivial solution for the system S. We can represent U, V as follows:

$$U = \begin{pmatrix} x_1^0 & 0 & \dots & 0 \\ x_2^0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ x_n^0 & 0 & \dots & 0 \end{pmatrix}_{n\times p}, \quad V = \begin{pmatrix} 0 & \cdots & 0 \\ 0 & & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{pmatrix}_{n\times p}.$$

So, $A_{m\times n} \cdot U_{n\times p} = 0_{m\times p} = A_{m\times n} \cdot V_{n\times p} = 0_{m\times p}$. But we have $U \neq V$. This is a contradiction with the fact that A is a monomorphism, thus, $rank\ A = n$.

($\Longleftarrow$) We know that $rank\ A = n$. Let $U: p \longrightarrow n$ and $V: p \longrightarrow n$ such that $AU = AV \Longrightarrow AU - AV = 0 \Longrightarrow A(U - V) = 0$. Let's denote $U - V = Z$. Therefore, $A \cdot Z = 0$. This implies that the p columns of Z are the solutions for the system S. But, since $rank\ A = n$, it means that the system has only the trivial solution. Furthermore, it implies that $Z = 0 \Longrightarrow U - V = 0 \Longrightarrow U = V \Longrightarrow A$ is a monomorphism.

The proof for part *(ii)* is similar. □

Theorem 2.8. *Let $\mathcal{C}$ be a category and $f \in \mathcal{H}om_{\mathcal{C}}(A, B)$, $g \in \mathcal{H}om_{\mathcal{C}}(B, C)$. Then:*

(i) *If f and g are monomorphisms then gf is a monomorphism.*

(ii) *If f and g are epimorphisms then gf is an epimorphism.*

(iii) *If gf is a monomorphism then f is a monomorphism.*

(iv) *If gf is an epimorphisms then g is an epimorphism.*

Proof. Let $h, k \in \mathcal{Hom}_{\mathcal{C}}(A, \cdot)$.

(i) $(gf)h = (gf)k \Longrightarrow g(fh) = g(fk) \xrightarrow{g\ monomorp\ hism} fh = fk \xrightarrow{f\ monomorp\ hism} h = k.$

(ii) $h(gf) = k(gf) \Longrightarrow (hg)f = (kg)f \xrightarrow{f\ epimorp\ hism} hg = kg \xrightarrow{g\ epimorp\ hism} h = k.$

(iii) $fh = fk \Longrightarrow g(fh) = g(fk) \Longrightarrow (gf)h = (gf)k \xrightarrow{gf\ monomorp\ hism} h = k.$

(iv) $hg = kg \Longrightarrow (hg)(f) = (kg)(f) \Longrightarrow h(gf) = k(gf) \xrightarrow{gf\ epimorp\ hism} h = k.$ □

Definition 2.9. *Consider $\mathcal{C}$ a category and $f: A \longrightarrow B$ a morphism in $\mathcal{C}$.*

(i) f is called ***coretraction*** *if there exists a morphism $g: B \longrightarrow A$ such that $g \circ f = 1_A$ (has left inverse).*

(ii) f is called ***retraction*** *if there exists a morphism $g: B \longrightarrow A$ such that $f \circ g = 1_B$ (has right inverse).*

(iii) f is called ***isomorphism*** *if f is both coretraction and retraction, it means there exists a morphism $g: B \longrightarrow A$ such that $g \circ f = 1_A$ and $f \circ g = 1_B$. We will say that A and B are isomorphisms and we denote it by $A \simeq B$.*

Proposition 2.10. *Let $\mathcal{C}$ be a category and $f: A \longrightarrow B$ a morphism in $\mathcal{C}$.*

(i) if f is a coretraction, then f is a monomorphism.

(ii) if f is a retraction, then f is an epimorphism.

(iii) if f is an isomorphism, then f is a bimorphism.

Proof. *(i)* If f is a coretraction, then there exists $g: B \longrightarrow A$, such that $gf = 1$.

Let's consider $u: B \longrightarrow Y$ and $v: B \longrightarrow Y$ such that $fu = fv \Longrightarrow g(fu) = g(fv) \Longrightarrow (gf)u =$

$(gf)v \Longrightarrow u = v$, hence, f is a monomorphism.

(ii) If f is a retraction, then there exists $g: B \longrightarrow A$, such that $fg = 1$. Let's consider $u: B \longrightarrow Y$ and $v: B \longrightarrow Y$ such that $uf = vf \Longrightarrow (uf)g = (vf)g \Longrightarrow u(fg) = v(fg) \Longrightarrow u = v$, thus, f is an epimorphism.

The proof of part *(iii)* is similar. □

Proposition 2.11. *Consider the category Ens and $f: A \longrightarrow B$ a morphism from Ens.*

(i) f is a coretraction, if and only if, f is a monomorphism.

(ii) f is a retraction, if and only if, f is an epimorphism.

(iii) f is an isomorphism, if and only if, f is a bimorphism.

Proof. *(i)* ($\Longrightarrow$) See Proposition 2.11.

($\Longleftarrow$) f is a monomorphism $\overset{\text{Ens}}{\Longrightarrow} f$ is injective $\Longrightarrow$ there exists $g: B \longrightarrow A$ such that

$g(y) = \begin{cases} f^{-1}(y), & if\ y \in f(A) \\ a, & if\ y \notin f(A) \end{cases}$, where $a \in A$.

Thus, $gf = 1_A \Longrightarrow f$ coretraction.

(ii) ($\Longrightarrow$) See Proposition 2.11.

($\Longleftarrow$) f is an epimorphism $\overset{\text{Ens}}{\Longrightarrow} f$ is surjective $\Longrightarrow$ for any $y \in B,\ f^{-1}(y) \neq \emptyset$.

Consider $g: B \longrightarrow A$ such that $B \ni y \longmapsto$ select only one $x \in f^{-1}(y) \subseteq A$.

Therefore, $fg = 1_B \Longrightarrow f$ retraction.

(iii) The proof is derived from parts *(i) and (ii).* □

Definition 2.12. *A category $\mathcal{C}$ is called **balanced** if any bimorphism is an isomorphism.*

Definition 2.13. *Let $\mathcal{C}$ a category and $A \in Ob\ \mathcal{C}$.*

A is called ***initial object*** *if for any* $\in Ob\ \mathcal{C}$, $|\mathcal{H}om_{\mathcal{C}}(A, X)| = 1$.

A is called ***terminal object*** *if for any* $\in Ob\ \mathcal{C}$, $|\mathcal{H}om_{\mathcal{C}}(X, A)| = 1$.

Here are some examples of initial and terminal objects in some categories.

- In Ens, we have the empty set, $\emptyset$, as the initial object and the singleton (set with one element) as the terminal object.
- In Grp, the initial and the terminal object are the same: the singleton group $\{e\}$.
- In Rngu, the initial object is $(\mathbb{Z}, +, \cdot)$, where $\mathbb{Z}$ is the set of integers and $+, \cdot$ are the usual operations of addition and multiplication.

2.2. Inverse Categories

Definition 2.14. *Given a category $\mathcal{C}$, we say that $\mathcal{C}$ is a* ***regular category****,if for any $f \in \mathcal{H}om_{\mathcal{C}}(A,B)$, there exists $g \in \mathcal{H}om_{\mathcal{C}}(B,A)$ such that $fgf = f$.*

Definition 2.15. *Given a category $\mathcal{C}$, we say that $\mathcal{C}$ is an* ***inverse category****,if for any $f \in \mathcal{H}om_{\mathcal{C}}(A,B)$, there exists an unique $g \in \mathcal{H}om_{\mathcal{C}}(B,A)$ such that $fgf = f$ and $gfg = g$.*

If we denote $g = f^{-1}$ then we have $ff^{-1}f = f$ and $f^{-1}ff^{-1} = f^{-1}$, where $f: A \longrightarrow B$ and $f^{-1}: B \longrightarrow A$.

Definition 2.16. *If $\mathcal{C}$ is a category, then $f \in \mathcal{H}om_{\mathcal{C}}(A,A)$is called* ***idempotent*** *if $ff = f$.*

Observation 2.17. *If $\mathcal{C}$ is an inverse category, then $(\mathcal{H}om_{\mathcal{C}}(A,A), \ \cdot)$ is an inverse semigroup.*

Observation 2.18. *If $\mathcal{C}$ is an inverse category and $f \in \mathcal{H}om_{\mathcal{C}}(A,B)$ then ff^{-1} and $f^{-1}f$ are idempotents.*

Proof: $(ff^{-1})(ff^{-1}) = ff^{-1}ff^{-1} = (ff^{-1}f)f^{-1} = ff^{-1}$.

Proposition 2.19. *Let $f: A \longrightarrow B$, and $g: B \longrightarrow C$. Given $\mathcal{C}$ an inverse category, then:*

(i) $(gf)^{-1} = f^{-1}g^{-1}$.

(ii) $1_A^{-1} = 1_A$, *for any $A \in Ob\ \mathcal{C}$.*

Proof. *(i)* We have $A \xrightarrow{f} B \xrightarrow{g^{-1}g} B \xrightarrow{ff^{-1}} B \xrightarrow{g} C$. We know that $g^{-1}g, ff^{-1} \in \mathcal{H}om_{\mathcal{C}}(B,B)$ are idempotents. Using Observation 2.23, it implies that $g^{-1}g$ and ff^{-1} commute. Furthermore,

$$(gf)(f^{-1}g^{-1})(gf) = g(ff^{-1})(g^{-1}g)f \xRightarrow{g^{-1}g\ ,\ ff^{-1} commute} (gg^{-1}g)(ff^{-1}f) = gf$$

Similarly, $(f^{-1}g^{-1})(gf)(f^{-1}g^{-1}) = f^{-1}g^{-1}$.

(ii) $1_A \cdot 1_A \cdot 1_A = 1_A$, because 1_A is unique.

Theorem 2.20. *Given $\mathcal{C}$ a category, $\mathcal{C}$ is an inverse category, if and only if, $\mathcal{C}$ is a regular category and its idempotents commute.*

Proof. ($\Longrightarrow$) We have $\mathcal{C}$ an inverse category and let $i \in \mathcal{H}om_{\mathcal{C}}(A,A)$ be an idempotent morphism. Then, the unique solution of the system $\begin{cases} ixi = i \\ xix = x \end{cases}$ is $x = i$. Consequently, we can denote $i^{-1} = i$. If we consider $i_1,\ i_2 \in \mathcal{H}om_{\mathcal{C}}(A,A)$ to be idempotent morphisms from the inverse category $\mathcal{C}$ and $(i_1 i_2)^{-1}$ is the solution of the system

$$S_1 = \begin{cases} i_1 i_2 x i_1 i_2 = i_1 i_2 \\ x\, i_1 i_2\, x = x \end{cases}$$

Hence, $(i_1 i_2)^{-1}\, i_1$ and $i_2 (i_1\, i_2)^{-1}$ also satisfy the system S_1 .

Therefore, $(i_1 i_2)^{-1} = (i_1 i_2)^{-1} i_1 = i_2 (i_1 i_2)^{-1}$.

Since $(i_1 i_2)^{-1}(i_1\, i_2)^{-1} = (i_1\, i_2)^{-1} i_1 i_2 (i_1\, i_2)^{-1} = (i_1\, i_2)^{-1}$ it implies that the morphism $(i_1\, i_2)^{-1}$ is idempotent. In conclusion, $(i_1\, i_2)^{-1} = i_1\, i_2$.

Using the same method we show that the morphism $i_2 i_1$ is also idempotent.

Given that $(i_1\, i_2)(i_2\, i_1)(i_1\, i_2) = i_1\, i_2 i_1\, i_2 = i_1\, i_2$ and $(i_2\, i_1)(i_1\, i_2)(i_2\, i_1) = i_2\, i_1 i_2\, i_1 = i_2\, i_1$, it implies that $i_2\, i_1$ is a solution of the system S_1 . Therefore, $(i_1\, i_2)^{-1} = i_2\, i_1$.

($\Longleftarrow$) Given $\mathcal{C}$ regular it implies that for any $f \in \mathcal{Hom}_{\mathcal{C}}(A,B)$, there exists $g \in \mathcal{Hom}_{\mathcal{C}}(B,C)$ such that $fgf = f$. Moreover, there exists a morphism $h \in \mathcal{Hom}_{\mathcal{C}}(B,C)$ such that $h = gfg$. Therefore, we have the results:

- $fhf = f(gfg)f = (fgf)gf = fgf = f$.
- $hfh = (gfg)f(gfg) = g(fgf)gfg = gfgfg = g(fgf)g = gfg = h$.

Next, suppose there exists another morphism $k \in \mathcal{Hom}_{\mathcal{C}}(B,C)$ such that $fkf = f$ and $kfk = k$. We showed earlier that $fhf = f$ and $hfh = h$. Thus, we have

$$\left.\begin{array}{l} k = kfk = k(fhf)k = kfhfk = k(fh)(fk) \xRightarrow{idempotents \quad commute} k(fk)(fh) = kfh \\ h = hfh = h(fkf)h = hfkfh = (hf)(kf)h \xRightarrow{idempotents \quad comm\,ute} (kf)(hf)h = kfh \end{array}\right| \Rightarrow h = k$$

□

We now give some examples of inverse categories:

Example 2.21. *The inverse category of partial bijections Bij.*

Recall that partial functions and partial bijections were defined in 1.27. It is straightforward to see that the category of partial bijections *Bij* defined by: the objects are sets and the morphisms are partial bijections, is a subcategory of *Rel*. The category *Rel* is not an inverse category, but the category *Bij* is an inverse category. As well as inverse semigroups, the inverse categories are fully described by categories of partial bijections. Any inverse category is isomorphic with a subcategory of the category *Bij*. Thus it is obtained a generalization of the Wagner-Preston Theorem relating to inverse semigroups. In fact we can see that some concepts of inverse semigroups can be introduced in inverse categories, and the properties of inverse categories are analogues to the properties of inverse monoids.

Let $f\colon X \longrightarrow Y$ be a partial bijection and $g : imf \longrightarrow domf$ defined by:

$$g(y) = x, \quad \text{where} \quad x \in \, domf \quad \text{such that} \quad f(x) = y.$$

Then g is a partial bijection from *Y* to *X* and

$$f \circ g \circ f = f \quad ; \quad g \circ f \circ g = g \; .$$

It follows that *Bij* is a regular category.

Note that,

$$domg = imf \qquad img = domf.$$

Now, for any subset *A* of *X* the identity function 1_A on *A* is a partial function from *X* to itself. It is straightforward to check that in *Bij* the idempotents are the partial identities. Since,

$$1_A \circ 1_B = 1_{A\cap B} = 1_{B\cap A} = 1_B \circ 1_A$$

it follows that the idempotents commute. By Theorem 2.20, the category *Bij* is an inverse category.

Example 2.22. *The inverse category of invertible matrices*

An *n by n* matrix *A* is called **invertible** (nonsingular or nondegenerate) if there exists an *n by n* matrix *B* such that $AB = BA = I_n$, where I_n denotes the *n by n* identity matrix. Note that non-square matrices do not have an inverse.

The category of matrices $\mathcal{M}_{\mathbb{R}}$ is a regular category but it is not an inverse category. The subcategory of $\mathcal{M}_{\mathbb{R}}$ with the positive integers as objects and with invertible matrices as morphisms is an inverse category. The composition of morphisms is the multiplication of matrices. The set of morphisms *Hom*(*m*,*n*) is empty unless *m* = *n*, in which case it is the set of all *n by n* invertible matrices.

Example 2.23. *The inverse category that represents an equivalence relation*

A partition of a set X is a set of nonempty subsets of X such that every element x in X is in exactly one of these subsets. The nonempty subsets of a partition are called **cells** (or block or part) of the partition. An equivalence relation on X is a relation that partitions the set X so that two elements of the set are considered equivalent if and only if they are element of the same cell.

If X is a set with an equivalence relation denoted by $\sim$ then an inverse category representing this equivalence relation can be formed as follows:

- The objects are the elements of X;
- For any two elements x and y in X, there is a single morphism from x to y if and only if $x \sim y$.

Example 2.24. *An inverse category as a subcategory of the category of based sets and based functions*

The category of sets with base point and functions preserving base points is defined as follows. Its objects are pairs (X, x), where X is a nonempty set and x is an element of X. The morphisms are functions of X into Y carrying the base point of X into the base point of Y for each pair of sets X, Y. The composition of morphisms is the usual composition of functions.

Let $\mathcal{C}$ be the subcategory of the category of based sets and based functions defined by:

- The objects are the sets with base point;
- A morphism from (X, x) to (Y, y) is a set function f from X to Y so that $f(x) = y$, and the set $\{u \in X | f(u) = v\}$ contains at most one element for each $v \in Y - \{y\}$. Then f^{-1} defined by:

$$f^{-1}(v) = \begin{cases} u & if \ f(u) = v \neq y \\ x & otherwise \end{cases}$$

is the unique morphism from (Y, y) to (X, x) such that:

$$f \circ f^{-1} \circ f = f \quad ; \quad f^{-1} \circ f \circ f^{-1} = f^{-1}.$$

It follows that this subcategory of the category of based sets and based functions is an inverse category.

References

[1] O. Ciucurel, E. Schwab, *Introduction to the Theory of Categories*, Mirton, Timisoara, 1999.

[2] P. A. Grillet, *Semigroups: An Introduction to the Structure Theory.* Marcel Dekker Inc., 1995.

[3] C. D. Hollings, *Some First Tantalizing Steps into Semigroup Theory*, Mathematics Magazine, Vol. 80, No 5 (2007), 331-344.

[4] S. M. Jekel, *Simplicial* K(G,1)'s, Manuscripta Math. 21 (1977), 189-203.

[5] J. M. Howie, *An Introduction to Semigroup Theory.* Academic Press, 1976.

[6] M. V. Lawson, *Inverse Semigroups. The Theory of Partial Symmetries.* World Scientific, Singapore, 1998.

[7] M. V. Lawson, *E*-unitary Inverse Semigroups,* in Semigroups, Algorithms, Auromata and Languages, World Scientific Publishing (2002), 195-214.

[8] S. Lipscomb, *Symmetric Inverse Semigroups.* American Mathematical Society, 1996.

[9] A. Macedo, E. D. Schwab, *Maximal Elements and their Group-like Set,* Annals Tibiscus, Computer Science Series, Vol.9, No.1 (2011), 107-114.

[10] B. Mitchell, *Theory of Categories.* Academic Press, 1965.

[11] M. Petrich, *Inverse Semigroups,* John Wiley & Sons, Inc., 1984.

Index

Curriculum Vita

Alexandra Macedo was born in May 25, 1984 in Oradea, Romania. Proud daughter of Marta and Alexandru Bogdan, Alexandra graduated with a Bachelor's Degree in Mathematics and Informatics, in July 2007. The following year, in 2008 she decides to leave her home town to come to the United States to pursue a graduate degree.

As a graduate student of the University of Texas at El Paso, Alexandra participated in grant funded programs and attended various conferences. Her dedication, work ethic, and drive gave her the tools to complete a Master's degree in Statistics in 2009.

To further her education, she decided to enroll once again as a graduate student to pursue a Master's degree in Mathematics. Currently, she is about to complete this degree.

Alexandra is also working towards becoming an educator for a College or University. As a means to meet this goal, Alexandra has strengthened her pedagogical ideas through research, training and practice.

In addition, throughout this journey, Alexandra met her husband, Oscar Macedo. Together, they have started a wonderful family and are proud parents of their beautiful daughter Alexa Macedo.

Permanent address: 14236 Honey Point Dr
El Paso, Texas, USA, 79938

This thesis was typed by the author.