2013-01-01

Generalizations of Dirichlet Convolution

Juan Carlos Villarreal
University of Texas at El Paso, jcvillarreal2@miners.utep.edu

GENERALIZATIONS OF DIRICHLET CONVOLUTION

JUAN CARLOS VILLARREAL

Department of Mathematical Sciences

APPROVED:

Emil D. Schwab, Chair, Ph.D.

Helmut Knaust, Ph.D.

Marian M. Manciu, Ph.D.

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

to my

WIFE

and to my

MOTHER and FATHER

with love

GENERALIZATIONS OF DIRICHLET CONVOLUTION

by

JUAN CARLOS VILLARREAL

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

May 2013

Acknowledgements

I would like to express my gratitude to my advisor Dr. Emil Schwab from the Mathematical Science Department of The University of Texas at El Paso for all his help, support, and advice in completing this thesis, and more important this masters program. Without his knowledge, his input, and his time, I would have not been able to accomplish all that I have done. I would like to thank him for all the time he dedicated to me as a teacher while I was attending his courses, and for all the knowlegde I learned in these ones. I appreciate the opportunity he gave me to do research during one semester and have the oportunity to present the results at New Mexico State University. Finally more than anything I would like to thank him for being a great mentor and helping me to write my thesis.

Moreover I would like to thank the members of my committee Dr. Helmut Knaust from the Mathematical Science Department and Dr. Marian Manciu from the Physical Science Department for accepting helping me with my thesis and for devoting some of their valuable time to accomplish this. I really appreciate your comments and your input in this work.

I would also like to thank my parents for support me all the time and helping me accomplish all my goals. I am who I am beacuase of them. I appreciate all their advice and comments and for always pushing me to my full potential and showing me that I can always accomplish great things. Thank you for always having time for me.

Finally, I would like to thank my wife Laura for all her love and patience. For all her support, advice and for putting up with me without complaining. I am so grateful to have the honor to be married to someone like you. Thank you for always being there for me. Thank you for being the love of my life.

Introduction

In the field of number theory, arithmetic functions have played a very important role. The arithmetic functions are functions whose domain is the positive integers and the range the complex numbers. The study of this functions as well as two special classes of arithmetic functions called multiplicative and completely multiplicative is the main content of chapter 1. In this chapter we explore the properties that arise from the Dirichlet convolution applied to arithmetic functions. We also explore the characteristics of multiplicative and completely multiplicative arithmetic functions showing some characterizations as well as some of the most important examples. One of the main components of this chapter is the Möbius function as well as the Möbius inversion formula. Moreover in chapter 1 we present a theorem from E. D. Schwab that uses arithmetic functions to characterize prime numbers as well as my own characterization that involves the Möbius function.

In chapter 2 we present a generalization for the Dirichlet convolution for arithmetic functions. We start by presenting K-convolutions and the necessary conditions for this operation such that together with the classical addition, the set of arithmetic functions forms a commutative ring with unity. Furthermore, we also show another type of convolution called regular convolution that involves another type of Möbius function and the Möbius inversion formula. We show that the Dirichlet convolution as well as the unitary convolution are cases of regular convolutions and that in some sense these two define the boundaries for all regular convolutions.

Finally, in chapter 3 we show a generalization of the Dirichlet convolution in the theory of categories. First we start by introducing the basic definitions of this theory and some of the main properties as well as the most common examples. Moreover we present a special type of categories called Möbius categories as well as the concept of the incidences algebra

that allows us to generalize the concepts of arithmetic functions algebra with Dirichlet convolution. We also define a Mӧbius incidence function and a Mӧbius inversion formula for the incidence algebra. We finish this chapter with our example of a computation of the Mӧbius function in a Mӧbius category.

Table of Contents

Chapter 1

Dirichlet Convolution

The theory of arithmetic functions is a wide subject within the field of number theory. We can say that this subject starts in the correspondence between the mathematicians Leonard Euler and Daniel Bernoulli in the year 1741. The Dirichlet convolution has played a big role in the development of this theory. The set of arithmetic functions together with addition and Drichlet convolution form a commutative ring with unity. One of the main arithmetic functions, the Möbius function, was first introduced by August Möbius in 1832 in his work on the inversion of series of functions.

1.1 Arithmetic Functions

Definition 1.1 *Let $\mathcal{A}$ represent the set of* ***arithmetic functions****, which consists of all complex valued functions defined on the set of positive integers* $\mathbb{N}$

$$\mathcal{A} = \{f | f : \mathbb{N} \to \mathbb{C}\}.$$

We define some binary operations inside the set of arithmetic functions.

For every arithmetic functions f, g addition is defined in the classical way

$$(f + g)(n) = f(n) + g(n).$$

Moreover we include another binary operation called Dirichlet convolution defined as

follows

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d}).$$

We begin with showing that the set of arithmetic functions together with addition and Dirichlet convolution forms not only a ring, but an integral domain.

Theorem 1.2 *The set of arithmetic functions together with addition and Dirichlet convolution* $(\mathcal{A}, +, *)$ *is an integral domain.*

Proof.

First let us show that $\mathcal{A}$ together with addition forms an abelian group

- Commutativity: let $f, g \in \mathcal{A}$ and $n \in \mathbb{N}$

$$(f + g)(n) = f(n) + g(n) = g(n) + f(n) = (g + f)(n)$$

- Associativity: let $f, g, h \in \mathcal{A}$ and $n \in \mathbb{N}$

$$(f+(g+h))(n) = f(n)+(g+h)(n) = f(n)+g(n)+h(n) = (f+g)(n)+h(n) = ((f+g)+h)(n)$$

- Identity: $0(n) = 0$ for every $n \in \mathbb{N}$, if $f \in \mathcal{A}$ and $n \in \mathbb{N}$ then:

$$(f + 0)(n) = f(n) + 0(n) = f(n) + 0 = f(n)$$

- Inverse: $(-f)(n) = -f(n)$ for any $n \in \mathbb{N}$ we have:

$$(f + (-f))(n) = f(n) + (-f)(n) = f(n) + (-f(n)) = 0 = 0(n)$$

Now let us show that $\mathcal{A}$ together with Dirichlet convolution forms an abelian monoid

- Commutativity: let $f, g \in \mathcal{A}$ and $n \in \mathbb{N}$

$$(f * g)(n) = \sum_{d_1 d_2 = n} f(d_1)g(d_2) = \sum_{d_1 d_2 = n} g(d_2)f(d_1) = (g * f)(n)$$

- Associativity: let $f, g, h \in \mathcal{A}$ and $n \in \mathbb{N}$

$$((f * g) * h)(n) = \sum_{dd_3 = n} (f * g)(d)h(d_3)$$

$$= \sum_{dd_3 = n} \left(\sum_{d_1 d_2 = d} f(d_1)g(d_2) \right) h(d_3)$$

$$= \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3)$$

$$= \sum_{d_1 d = n} f(d_1) \left(\sum_{d_2 d_3 = d} g(d_2)h(d_3) \right)$$

$$= \sum_{d_1 d = n} f(d_1)(g * h)(d) = (f * (g * h))(n)$$

- Identity: let $n \in \mathbb{N}$ and

$$\delta(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

$$(\delta * f)(n) = \sum_{d|n} \delta(d) f(\frac{n}{d})$$

$$= \delta(1)f(n) + \sum_{d|n, d>1} \delta(d) f(\frac{n}{d})$$

$$= 1 \cdot f(n) + 0 = f(n)$$

Now let us show that Dirichlet convolution distributes over addition in $\mathcal{A}$. Let f, g, h be arithmetic functions and $n \in \mathbb{N}$

$$(f*(g+h))(n) = \sum_{d|n} f(d)(g+h)(\frac{n}{d}) = \sum_{d|n} f(d)\left(g(\frac{n}{d}) + h(\frac{n}{d})\right)$$

$$= \sum_{d|n}\left(f(d)g(\frac{n}{d}) + f(d)h(\frac{n}{d})\right) = \sum_{d|n} f(d)g(\frac{n}{d}) + \sum_{d|n} f(d)h(\frac{n}{d})$$

$$= (f*g)(n) + (f*h)(n).$$

So far we have shown that $(\mathcal{A}, +, *)$ is a ring. We will now proceed to show that it is an integral domain. For this we need to show that $(\mathcal{A}, +, *)$ has no zero divisors.

Let $f, g \in \mathcal{A}$ such that $f \neq 0$ and $g \neq 0$. Then there exists $n, m \in \mathbb{N}$ such that $f(n) \neq 0$ and $g(m) \neq 0$. Without loss of generality let n, m be the smallest positive integers such that $f(n) \neq 0$ and $g(m) \neq 0$.

$$(f*g)(nm) = \sum_{d|nm} f(d)g\left(\frac{nm}{d}\right)$$

$$= \sum_{d|nm, d<n} f(d)g\left(\frac{nm}{d}\right) + f(n)g(m) + \sum_{d|nm, d>n} f(d)g\left(\frac{nm}{d}\right) = f(n)g(m) \neq 0,$$

since $d < n$ implies that $f(d) = 0$ and $d > n$ implies that $\frac{nm}{d} < m$ which implies that $g\left(\frac{nm}{d}\right) = 0$.

Therefore, it follows that $f * g \neq 0$ and $(\mathcal{A}, +, *)$ has no zero divisors.

Thus we have shown that $(\mathcal{A}, +, *)$ is an integral domain.//

The ring of arithmetic functions $\mathcal{A}$ has many properties, we will discuss some of them.

Definition 1.3 *Given a ring R, let $U(R)$ represent the set of units of R*

$$U(R) = \left\{x \in R \,|\, \exists x^{-1} \text{ such that } xx^{-1} = x^{-1}x = 1\right\},$$

that is the set of all the invertible elements of R, where 1 represents the unity element.

In the next theorem we will prove that the invertible elements of $\mathcal{A}$ are those who satisfy a simple property.

Theorem 1.4 *An arithmetic function f has a Dirichlet convolution inverse in $\mathcal{A}$ (i.e. $f \in U(\mathcal{A})$) if and only if $f(1) \neq 0$.*

Proof.

Assume $f \in U(\mathcal{A})$, then there exists $f^{-1} \in \mathcal{A}$ such that $f * f^{-1} = f^{-1} * f = \delta$. Then

$$(f * f^{-1})(1) = \delta(1) \Rightarrow f(1)f^{-1}(1) = 1 \Rightarrow f(1) \neq 0.$$

Converseley, assume that $f \in \mathcal{A}$ such that $f(1) \neq 0$. Define a function

$$\tilde{f}(n) = \begin{cases} \frac{1}{f(1)} & \text{if } n = 1 \\ -\frac{1}{f(1)} \sum_{d|n} f(d)\tilde{f}\left(\frac{n}{d}\right) & \text{if } n \geq 2 \end{cases}$$

We will show that in fact $\tilde{f} = f^{-1}$.

If $n = 1$, then

$$(f * \tilde{f})(1) = f(1)\tilde{f}(1) = f(1) \cdot \frac{1}{f(1)} = 1.$$

Now let $n > 1$, then

$$(f * \tilde{f})(n) = \sum_{d|n} f(n)\tilde{f}\left(\frac{n}{d}\right)$$

$$= f(1)\tilde{f}(n) + \sum_{d|n, d>1} f(d)\tilde{f}\left(\frac{n}{d}\right)$$

$$= f(1)\left(-\frac{1}{f(1)}\sum_{d|n} f(d)\tilde{f}\left(\frac{n}{d}\right)\right) + \sum_{d|n, d>1} f(d)\tilde{f}\left(\frac{n}{d}\right) = 0.$$

Therefore, $f * \tilde{f} = \delta$ which implies that $\tilde{f} = f^{-1}$.//

As a consequence from the definition of the inverse of an arithmetic function f, in particular, given a prime p,

$$f^{-1}(p) = -\frac{1}{f(1)}\sum_{d|p, d>1} f(d)f^{-1}\left(\frac{p}{d}\right) = -\frac{f(p)f^{-1}(1)}{f(1)}$$

Let us observe that the set of invertible elements together with Dirichlet convolution, $(U(\mathcal{A}), *)$, is an abelian group.

1.2 Multiplicative Arithmetic Functions

Now, inside the set of arithmetic functions we will consider a special type of functions that are of special interest.

Definition 1.5 *A non-zero arithmentic function f is called **multiplicative** if and only if*

$$f(mn) = f(m)f(n)$$

whenever m and n are relatively prime.

Proposition 1.6 *If f is multiplicative, then $f(1) = 1$.*

Proof.

If f is multiplicative, then $f \neq 0$. Therefore, there exists $k \in \mathbb{N}$ such that $f(k) \neq 0$ and $f(k) = f(1 \cdot k) = f(1)f(k)$ which implies that $f(1) = 1//$

Moreover, it follows that all the multiplicative functions are invertible and we have:

Proposition 1.7 *The set of multiplicative functions is a subset of the set of invertible elements of $\mathcal{A}$*

Let us observe also that the unity δ is also multiplicative. Furthermore, given two multiplicative functions f, g, we have $f = g$ if and only if $f(p^\alpha) = g(p^\alpha)$ for every p prime.

Now, if we take the set of multiplicative functions together with Dirichlet convolution, it can be shown that it is a subgroup of the group of units of $\mathcal{A}$ together with Dirichlet convolution.

Theorem 1.8 *Let $\mathcal{M}$ be the set of multiplicative arithmetic functions, then $(\mathcal{M}, *)$ is a subgroup of $(U(\mathcal{A}), *)$.*

Proof.

First let us show that $\mathcal{M}$ is closed under Dirichlet convolution.

Let m and n be relatively prime, then

$$(f*g)(nm) = \sum_{d|nm} f(d)g\left(\frac{nm}{d}\right) = \sum_{d=d_1d_2, d_1|n, d_2|n} f(d_1d_2)g\left(\frac{nm}{d_1d_2}\right)$$

$$= \sum_{d_1|n, d_2|n} f(d_1)f(d_2)g\left(\frac{n}{d_1}\right)g\left(\frac{m}{d_2}\right) = \sum_{d_1|n} f(d_1)g\left(\frac{n}{d_1}\right)\sum_{d_2|n} f(d_2)g\left(\frac{m}{d_2}\right)$$

$$= (f*g)(n)\cdot(f*g)(m),$$

since $d = d_1d_2$ such that $(d_1, d_2) = 1$ implies that $\left(\frac{n}{d_1}, \frac{m}{d_2}\right) = 1$. Therefore $\mathcal{M}$ is closed under Dirichlet convolution.

Now let us show that $U(\mathcal{M}) = \mathcal{M}$.

Let $f \in \mathcal{M}$ and define

$$g(n) = \begin{cases} 1 & \text{if } n = 1 \\ f^{-1}(p_1^{\alpha_1})f^{-1}(p_2^{\alpha_2})\dots f^{-1}(p_k^{\alpha_k}) & \text{if } n > 2 \text{ and } n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k} \end{cases}$$

First will show that $g \in \mathcal{M}$

Let $n, m > 1$ such that $(n, m) = 1$ and $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}, m = p_{k+1}^{\alpha_{k+1}}p_{k+2}^{\alpha_{k+2}}\dots p_s^{\alpha_s}$, where p_i are distinct primes for every $1 \le i \le s$. Now

$$g(nm) = g\left(\prod_{i=1}^{s} p_i^{\alpha_i}\right) = \prod_{i=1}^{s} f^{-1}(p_i^{\alpha_i})$$

$$= \prod_{i=1}^{k} f^{-1}(p_i^{\alpha_i}) \prod_{i=k+1}^{s} f^{-1}(p_i^{\alpha_i}) = g(n)g(m)$$

Then we will show that in fact $g = f^{-1}$. Let p be a prime, then

$$(f * g)(p^\alpha) = \sum_{d|p^\alpha} f(d) g\left(\frac{p^\alpha}{d}\right) = \sum_{i=0}^{\alpha} f(p^i) g(p^{\alpha-i})$$

$$= \sum_{i=0}^{\alpha} f(p^i) f^{-1}(p^{\alpha-i}) = (f * f^{-1})(p^\alpha) = e(p^\alpha)$$

which implies that $g = f^{-1}$. Therefore we can conlude that $(\mathcal{M}, *)$ is a subgroup of $(U(\mathcal{A}), *)$//

Examples. Next we will present some of the most important examples of multiplicative functions

- i, where $i(n) = n$ for every $n \in \mathbb{N}$.
- ζ, where $\zeta(n) = 1$ for every $n \in \mathbb{N}$.
- τ, where $\tau(n) = \sum_{d|n} 1$, the number of divisors of n, for every $n \in \mathbb{N}$. τ is multiplicative:

  $$\tau(n) = \sum_{d|n} 1 = \sum_{d|n} \zeta(d)\zeta\left(\frac{n}{d}\right) = (\zeta * \zeta)(n) \Rightarrow \tau = \zeta * \zeta \in \mathcal{M}$$

  since $\mathcal{M}$ is closed under Dirichlet convolution.
- σ, where $\sigma(n) = \sum_{d|n} d$, the sum of the divisors of n, for every $n \in \mathbb{N}$. σ is multiplicative:

  $$\sigma(n) = \sum_{d|n} d = \sum_{d|n} i(d)\zeta\left(\frac{n}{d}\right) = (i * \zeta)(n) \Rightarrow \sigma = i * \zeta \in \mathcal{M}$$

  since $\mathcal{M}$ is closed under Dirichlet convolution.

Since $\zeta(1) \neq 0$, it is invertible. We denote ζ^{-1} by μ and we call it the ***Möbius*** function.

Moreover, since ζ is multiplicative, its Dirichlet convolution inverse μ is also multiplicative. Now, $\mu * \zeta = \delta$ implies that

$$\sum_{d|n} \mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

Proposition 1.9 *The Möbius function μ is*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2|n, \text{ where } p \text{ is a prime} \\ (-1)^k & \text{if } n = p_1 p_2 \dots p_k, \text{ where } p_i \text{ are distinct primes } \forall 1 \leq i \leq k \end{cases}$$

Proof.

First let $n = 1$, then

$$\sum_{d|1} \mu(1) = 1 \Rightarrow \mu(1) = 1$$

.

Now let $n = p$, where p is a prime, then

$$\sum_{d|p} \mu(p) = 0 \Rightarrow \mu(1) + \mu(p) = 0 \Rightarrow 1 + \mu(p) \Rightarrow \mu(p) = -1$$

Hence it follows that if $n = p_1 \dots p_k$ where p_i are distinct primes for every $1 \leq i \leq k$,

$$\mu(n) = \mu(p_1) \dots \mu(p_k) = (-1)^k$$

since μ is a multiplcative function.

Now let $n = p^\alpha$ for some p prime and $\alpha \geq 2$ a positive integer, we proceed by induction.

If $\alpha = 2$,

$$\sum_{d|p^2} \mu(p^2) = 0 \Rightarrow \mu(1) + \mu(p) + \mu(p^2) = 0 \Rightarrow 1 + (-1) + \mu(p^2) = 0 \Rightarrow \mu(p^2) = 0.$$

Thus assume it is true for $2 \leq \alpha \leq k-1$, then

$$\sum_{d|p^k} \mu(p^k) = \sum_{i=0}^{k} \mu(p^i) = 0 \Rightarrow \mu(1) + \mu(p) + \sum_{i=2}^{k-1} \mu(p^i) + \mu(p^k) = 0 \Rightarrow \mu(p^k) = 0$$

by our induction hypothesis. Therefore $\mu(p^\alpha) = 0$ for every $\alpha \geq 2$ a positive integer.

Now let n be any positive integer such that $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ is its prime factorization and for at leats one $1 \leq i \leq k$, $\alpha_i \geq 2$. Without loss of generality let $\alpha_1 \geq 2$, then

$$\mu(n) = \mu(p_1^{\alpha_1})\mu\left(\frac{n}{p_1^{\alpha_1}}\right) = 0$$

since μ is multiplicative.//

Observation 1.10 *Also using the properties of ζ we can show that if f is multiplicative and $F(n) = \sum_{d|n} f(n)$, then F is multiplicative:*

$$F(n) = \sum_{d|n} f(n) \Rightarrow F(n) = \sum_{d|n} f(n)\zeta\left(\frac{n}{d}\right) \Rightarrow F = f * \zeta \in \mathcal{M}$$

since $\mathcal{M}$ is closed under Dirichlet convolution.

One of the most important consequences of the Möbius function is the Möbius inversion formula.

Corollary 1.11 *Given two arithmetic functions f and g, $f(n) = \sum_{d|n} g(d)$ if and only if $g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right)$, since*

$$f = g * \zeta \Leftrightarrow g = f * \mu$$

$$\text{and } \zeta^{-1} = \mu.$$

We will now present another very important arithmetic function in the study of number theory.

Definition 1.12 *The* ***Euler indicator*** *denoted by ϕ is defined as the number of positive integers that are less than or equal to n and that are relatively prime to n.*

Before trying to derive a formula for ϕ we will prove the following theorem.

Theorem 1.13

$$\sum_{d|n} \phi(d) = n$$

for every positive integer n.

Proof.

Let n be a positive integer, then define subsets of the set $\{1, 2, \ldots, n\}$ in the following way:

$$A_d = \{x \mid 1 \leq x \leq n \text{ and } (x, n) = d\}$$

where d represents the divisors of n. Now, from the construction of A_d, if $x \in A_d$ then

$x = dx'$ for some divisor x' of x. Observe that $(x, n) = d$ if and only if $\left(x', \frac{n}{d}\right) = 1$ and $1 \leq x \leq n$ if and only if $1 \leq x' \leq \frac{n}{d}$. Thus we can define a new subset of $\{1, 2, \ldots, n\}$ in the following way:

$$A'_d = \left\{x' \mid 1 \leq x' \leq \frac{n}{d} \text{ and } \left(x', \frac{n}{d}\right) = 1\right\}$$

.

Note that from the above observations A_d and A'_d have the same number of elements for every divisor d of n and that this number is $\phi\left(\frac{n}{d}\right)$. Since every element of the set $\{1, 2, \ldots, n\}$ is exactly in one of the sets A_d, this forms a partition of $\{1, 2, \ldots, n\}$ each with cardinality of $\phi\left(\frac{n}{d}\right)$. Therefore

$$\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d) = n.//$$

We can derive many identities using the euler indicator, one of them is the following

Corollary 1.14 We have

$$i = \phi * \zeta$$

Proof.

$$i(n) = n = \sum_{d|n} \phi(d) = \sum_{d|n} \phi(d)\zeta\left(\frac{n}{d}\right) = (\phi * \zeta)(n).//$$

We also have

$$i = \phi * \zeta \Rightarrow \phi = i * \mu.$$

Therefore ϕ is also multiplicative since it is the Dirichlet convolution of two multiplica-

tive arithmetic functions, thus we can derive a formula for ϕ if we find the value of $\phi(p^\alpha)$ for some prime p and $\alpha \geq 1$.

Theorem 1.15 *Given a positive integer $n > 1$ such that $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$, then*

$$\phi(n) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right).$$

Proof. Let $\alpha \geq 1$, then

$$\phi(p^\alpha) = (\mu * i)(p^\alpha) = \sum_{d|p^\alpha} \mu(d) i\left(\frac{p^\alpha}{d}\right)$$

$$= \mu(1)i(p^\alpha) + \mu(p)i(p^{\alpha-1}) + \ldots + \mu(p^\alpha)i(1) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$$

since $\mu(p^\alpha) = 0$ for every $\alpha \geq 2$.

Hence,

$$\phi(n) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}) = \prod_{i=1}^{t} \phi(p_i^{\alpha_i}) = \prod_{i=1}^{t} p_i^\alpha \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) .//$$

Now that we have a formula for ϕ we can also derive a formula for its Dirichlet convolution inverse ϕ^{-1}. Since ϕ is multiplicative so is ϕ^{-1}, thus it also suffices to kwow the value of $\phi^{-1}(p^\alpha)$.

Theorem 1.16 *Given a positive integer $n > 1$ such that $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_t^{\alpha_t}$, then*

$$\phi^{-1}(n) = \prod_{i=1}^{t} (1 - p_i).$$

Proof. We will prove by induction that for a prime p and a positive integer α, $\phi^{-1}(p^\alpha) = 1 - p$.

If $\alpha = 1$, then

$$0 = (\phi * \phi^{-1})(p) = \phi(1)\phi^{-1}(p) + \phi(p)\phi^{-1}(1) = \phi^{-1}(p) + p - 1$$

$$\Rightarrow \phi^{-1}(p) = 1 - p.$$

Thus, assume the result holds for $= 1, 2, \ldots, \alpha - 1$, then

$$0 = (\phi * \phi^{-1})(p^\alpha) = \phi(1)\phi^{-1}(p^\alpha) + \phi(p)\phi^{-1}(p^{\alpha-1}) + \ldots + \phi(p^{\alpha-1})\phi^{-1}(p) + \phi(p^\alpha)\phi^{-1}(1)$$

$$= \phi^{-1}(p^\alpha) + (p-1)(1-p) + \ldots + p^{\alpha-2}(p-1)(1-p) + p^{\alpha-1}(p-1)$$

$$= \phi^{-1}(p^\alpha) + (p-1)(1-p)(1 + p + \ldots + p^{\alpha-2}) + p^{\alpha-1}(p-1)$$

$$= \phi^{-1}(p^\alpha) + (p-1)(1-p)\left(\frac{p^{\alpha-1}-1}{p-1}\right) + p^{\alpha-1}(p-1)$$

$$= \phi^{-1}(p^\alpha) + (1-p)(p^{\alpha-1} - 1 - p^{\alpha-1})$$

$$\Rightarrow \phi^{-1}(p^\alpha) = 1 - p.$$

Thus, by induction $\phi^{-1}(p^\alpha) = 1 - p$ for every $\alpha \geq 1$. Therefore given a positive integer n such that $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$

$$\phi^{-1}(n) = \prod_{1=1}^{t} \phi^{-1}(p_i^{\alpha_i}) = \prod_{i=1}^{t} (1 - p_i).//$$

We will also show another characterization of ϕ^{-1}.

Theorem 1.17

$$\phi^{-1} = \mu i * \zeta$$

Proof. First let us note that $\mu i * \zeta$ is multiplicative, then

$$(\mu i * \zeta)(p^\alpha) = \mu(1)i(1)\zeta(p^\alpha) + \mu(p)i(p)\zeta(p^{\alpha-1}) + \ldots + \mu(p^\alpha)i(p^\alpha)\zeta(1) = 1 - p$$

since $\mu(p^\alpha) = 0$ for $\alpha \geq 2$.

Therefore, since ϕ^{-1} and $\mu i * \zeta$ obtain the same values at the prime powers, $\phi^{-1} = \mu i * \zeta.//$

Corollary 1.18

$$\mu * \phi^{-1} = \mu i.//$$

We will now show more identities using arithmetic functions.

$$(i * i)(n) = \sum_{d|n} i(d) i\left(\frac{n}{d}\right) = n \sum_{d|n} 1 = n\tau(n) \Rightarrow i * i = i\tau$$

using the previous identity and also some shown before, we can derive two more

$$i * i = i\tau \Rightarrow \phi * \zeta * i = i\tau \Rightarrow \phi * \sigma = i\tau,$$

and

$$\tau * \phi = \tau * \mu * i \Rightarrow \tau * \phi = \zeta * i \Rightarrow \sigma = \phi * \tau.$$

1.3 Characterizations of Prime Numbers via Arithmetic Functions

Now we present a theorem that gives a characterization of prime numbers through arithmetic functions.

Theorem 1.19 [5] *Given two positive arithmetic functions f and g such that $f(1) = g(1) = 1$,*

$$n \text{ is prime } \Leftrightarrow (f+g)(n) = (f*g)(n).$$

Proof.

Let f and g be two positive arithmetic functions such that $f(1) = g(1) = 1$.

$$(f*g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = f(1)g(n) + \sum_{d|n, d\neq 1,n} f(d)g\left(\frac{n}{d}\right) + f(n)g(1)$$

$$= f(n) + g(n) + \sum_{d|n, d\neq 1,n} f(d)g\left(\frac{n}{d}\right)$$

Now, since $\sum_{d|n,d\neq 1,n} f(d)g\left(\frac{n}{d}\right) = 0$ if and only if n is prime, the result follows.//

We show examples of the applications of this theorem with some arithmetic functions that we have mentioned before.

- Since $\sigma * \phi = i\tau$,

$$n \text{ is prime } \Leftrightarrow (\sigma + \phi)(n) = n\tau(n).$$

- Since $\sigma = \phi * \tau$,

$$n \text{ is prime } \Leftrightarrow (\phi + \tau)(n) = \sigma(n).$$

In the Theorem 1.19, the arithmetic functions are positive valued functions. Now we present one more characterization without using the positive condition.

Theorem 1.20 *(Villarreal)*

$$n \text{ is prime } \Leftrightarrow (\mu + \phi^{-1})(n) = (\mu * \phi^{-1})(n).$$

Proof.

Using the fact that $\mu * \phi^{-1} = \mu i$ one can also express the theorem in the following way

$$n \text{ is prime } \Leftrightarrow (\mu + \phi^{-1})(n) = (\mu i)(n).$$

If $n = 1$ or $p^2 | n$ for some prime p, then $(\mu + \phi^{-1})(n) \neq \mu(n)i(n)$.
Assume that $n = p_1 p_2 \dots p_t$ is a product of t distinct primes. Then

$$(\mu + \phi^{-1})(n) = \mu(n)i(n) \Leftrightarrow (-1)^t + \prod_{i=1}^{t}(1 - p_i) = (-1)^t n \Leftrightarrow$$

$$\Leftrightarrow 1 + (-1)^t \prod_{i=1}^{t}(1 - p_i) = n \Leftrightarrow 1 + \phi(n) = n \Leftrightarrow n \text{ is prime.//}$$

1.4 Completely Multiplicative Arithmetic Functions

Now, if in the definition of multiplicative functions we do not restrict m and n to be relatively prime we define another type of arithmetic function.

Definition 1.21 *A non-zero arithmetic function f is called* ***completely multiplicative*** *if and only if*

$$f(mn) = f(m)f(n)$$

for every m, n positive integers.

If f is completely multiplicative, obviously it is multiplicative. Moreover given a prime p and α a positive integer, $f(p^\alpha) = (f(p))^\alpha$, which implies that f is defined by the value it takes at the prime numbers.

Examples. Some examples of completely multiplicative arithmetic functions

- δ, ζ, and i are trivial examples.
- i_k, the power function, where $i_k(n) = n^k$, where $k \in \mathbb{C}$, for every $n \in \mathbb{N}$.
- λ, the Liouville function, where $\lambda(n) = (-1)^{\Omega(n)}$, where $\Omega(n)$ is the number of prime factors of n counting multiplicity, for every $n \in \mathbb{N}$.

We have many characterizations of completely multiplicative functions, we will show some of the most classical.

Proposition 1.22 [3] *A multiplicative function f is completely multiplicative if and only if $f^{-1} = \mu f$.*

Proof.

Assume f is completely multiplicative and let n be a positive integer then

$$(\mu f * f)(n) = \sum_{d|n} (\mu f)(d) f\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) f(d) f\left(\frac{n}{d}\right)$$

$$f(n) \sum_{d|n} \mu(d) = f(n)\delta(n) = \begin{cases} f(1) = 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$$

therefore $\mu f * f = \delta$ which implies that $f^{-1} = \mu f$.

Conversely, assume that $f^{-1} = \mu f$. We need to show that $f(p^\alpha) = (f(p))^\alpha$ for p prime and α a positive integer. We proceed by induction.

For $\alpha = 1$ is obvious.

So assume it is true for every $1 \leq \alpha \leq k - 1$. Let us observe that by our hypothesis, if $l \geq 2$, then

$$f^{-1}(p^l) = (\mu f)(p^l) = \mu(p^l) f(p^l) = 0.$$

Therefore it follows that

$$0 = \delta(p^k) = (f^{-1} * f)(p^k) = \sum_{d|p^k} f^{-1}(d) f\left(\frac{p^k}{d}\right)$$

$$= \sum_{i=0}^{k} f^{-1}(p^i) f(p^{k-i}) = f^{-1}(1) f(p^k) + f^{-1}(p) f(p^{k-1})$$

$$= f(p^k) - f(p)(f(p))^{k-1} = f(p^k) - (f(p))^k$$

by our hypothesis and since $f^{-1}(p) = -f(p)$. Therefore it follows that

$$f(p^{\alpha}) = f(p)^{\alpha}.$$

Therefore the asummption is true for every $\alpha \geq 1$ positive integer. Thus, f is completely multiplicative.//

As a consequence we obtain another characterization.

Corollary 1.23 [3] *A multiplicative function f is completely multiplicative if and only if $f^{-1}(p^{\alpha}) = 0$ for every prime p and for every $\alpha \geq 2$ a positive integer.*

We now present one of the most useful caractherizations for completely multiplicative arithmetic functions.

Theorem 1.24 [3] *Let f be an arithmetic function with $f(1) \neq 0$, then the following are equivalent:*

(1) *f is completely multiplicative;*

(2) *(Lambek) $f(g * h) = fg * fh$,*
for all arithmetic functions g and h;

(3) *$f(g * g) = fg * fg$,*
for any arithmetic function g;

(4) *(Carlitz) $\tau f = f * f$,*
where $\tau(n)$ is the number of positive divisors of n.

Proof.

(1)⇒(2)

Assume f is completely multiplicative, we will show that f distributes multiplication over dirichlet convolution. Let n be a positive integer, then

$$f(g * h)(n) = f(n) \sum_{d|n} g(d) h\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} f(d) g(d) f\left(\frac{n}{d}\right) h\left(\frac{n}{d}\right) = (fg * fh)(n)$$

since f is completely multiplicative.

(2)⇒(3)

Assume that $f(g * h) = fg * fh$ for all arithmetic functions g and h. Let $g = h$ and the result is inmediate.

(3)⇒(4)

Assume that $f(g * g) = fg * fg$ for any arithmetic function g. Let $g = \zeta$. Using the fact that $\tau = \zeta * \zeta$, and that $(f\zeta)(n) = f(n)\zeta(n) = f(n)$ (that is $f\zeta = f$) we obtain,

$$f\tau = f(\zeta * \zeta) = f\zeta * f\zeta = f * f.$$

(4)⇒(1)

Assume that $\tau f = f * f$. Then, if $n = 1$

$$f(1) = f(1)\tau(1) = (f * f)(1) = \sum_{d|1} f(d) f\left(\frac{1}{d}\right) = f(1)f(1)$$

which implies that $f(1) = 1$ since $f(1) \neq 0$.

Now, let $n \geq 2$ be a positive integer such that $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ is its prime factorization. We will prove by induction on $\alpha = \alpha_1 + \alpha_2 + \ldots + \alpha_k$ that $f(n) = (f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2} \ldots (f(p_k))^{\alpha_k}$, which would implie that f is completely multiplicative.

If $\alpha = 1$ then n is a prime number and the result is obvious.

Now we assume that the result hold for all $1 \leq \gamma < \alpha_1 + \alpha_2 + \ldots + \alpha_k$. So let $\alpha \geq 2$, thus $\tau(n) > 2$. Now let d be a divisor of n such that $d \neq 1$ and $d \neq n$ with $d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$ its prime factorization, where $0 \leq \beta_i \leq \alpha_i$ for every $1 \leq i \leq k$. By our induction hypothesis it follows that

$$f(d) f\left(\frac{n}{d}\right)$$

$$= (f(p_1))^{\beta_1}(f(p_2))^{\beta_2} \ldots (f(p_k))^{\beta_k}(f(p_1))^{\alpha_1-\beta_1}(f(p_2))^{\alpha_2-\beta_2} \ldots (f(p_k))^{\alpha_k-\beta_k}$$

$$= (f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2} \ldots (f(p_k))^{\alpha_k}.$$

Therefore, we have

$$(f\tau)(n) = f(n)\tau(n) = (f * f)(n) = \sum_{d|n} f(d)\left(\frac{n}{d}\right)$$

$$f(1)f(n) + \sum_{d|n,\, d\neq 1,\, d\neq n} f(d)\left(\frac{n}{d}\right) + f(n)f(1)$$

$$= 2f(n) + (\tau(n) - 2)(f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2} \ldots (f(p_k))^{\alpha_k}$$

which implies that

$$f(n)\tau(n) = 2f(n) + (\tau(n) - 2)(f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2} \ldots (f(p_k))^{\alpha_k}$$

$\Rightarrow$

$$f(n)(\tau(n)-2)=(\tau(n)-2)(f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}$$

thus

$$f(n)=(f(p_1))^{\alpha_1}(f(p_2))^{\alpha_2}\ldots(f(p_k))^{\alpha_k}$$

since $\tau(n)>2$. Therefore f is completely multiplicative.//

Chapter 2

Generalizations of Dirichlet Convolution for Arithmetic Functions

In this section we discuss a generalization to the notion of convolution, showing that the set of arithmetic functions together with addition and a "special" convolution that we will introduce also forms a commutative ring with unity. This type of convolutions which are called K-convolutions were introduced in 1966 in the work by T. M. K. Davidson. Moreover we will also discuss about a more general form of convolution which is called regular arithmetic convolution, which was introduced in 1963 by W. Narkiewicz.

2.1 K-convolutions

Definition 2.1 *Let K be a complex-valued function on the set of all ordered pairs (n, d) where n is a positive integer and d is a divisor of n. We define the binary operation K-**convolution** of two arithmetic functions as follows*

$$(f *_K g)(n) = \sum_{d|n} K(n, d) f(d) g\left(\frac{n}{d}\right)$$

for every n positive integer.

As an observation if $K(n, d) = 1$ for every ordered pair (n, d), then the K-convolution of two arithmetic functions is just the Dirichlet convolution.

Theorem 2.2 [3] *Let $*_K$ to be a K-convolution on the set of arithmetic functions. Then:*

(1) *δ is the unity element if and only if $K(n,n) = K(n,1) = 1$ for every n positive integer.*

(2) *The K-convolution of multiplicative functions is multiplicative if and only if $K(mn, de) = K(m,d)K(n,e)$ for all $m, n, d,$ and e such that $d|m$ and $e|n$ and $(m,n) = 1$.*

(3) *K-convolution is associative if and only if $K(n,d)K(d,e) = K(n,e)K\left(\frac{n}{e}, \frac{d}{e}\right)$ for all n, d and e such that $d|n$ and $e|d$.*

(4) *K-convolution is commutative if and only if $K(n,d) = K\left(n, \frac{n}{d}\right)$ for all n and d such that $d|n$.*

Proof.

(1)

Assume δ is the unity element then for every arithmetic function f we have

$$f *_K \delta = \delta *_K f = f.$$

Also let us note that

$$(f *_K \delta)(n) = \sum_{d|n} K(n,d) f(d) \delta\left(\frac{n}{d}\right) = K(n,n) f(n)$$

and

$$(\delta *_K f)(n) \sum_{d|n} K(n,d) \delta(d) f\left(\frac{n}{d}\right) = K(n,1) f(n)$$

for every positive integer n.

By our assumption δ is the unity for all arithmetic functions, therefore let $f = \zeta$, which implies that $K(n,n) = K(n,1) = 1$ for every positive integer n.

Conversely, assume that $K(n,n) = K(n,1) = 1$ for every n positive integer, thus

$$(f *_K \delta)(n) = K(n,n)f(n) = f(n) = K(n,1)f(n) = (\delta *_K f)(n),$$

which implies that δ is the unity element.

(2)

Assume that the K-convolution of multiplicative functions is multiplicative, also let m, n, d, and e be such that $d|m$ and $e|n$ and $(m,n) = 1$. Define arithmetic functions f and g in the following way

$$f(k) = \begin{cases} 1 & \text{if } k|de \\ 0 & \text{otherwise} \end{cases}$$

and

$$g(k) = \begin{cases} 1 & \text{if } k|\frac{mn}{de} \\ 0 & \text{otherwise} \end{cases}$$

The functions f and g are multiplicative. Let us observe that

$$(f *_K g)(m)(f *_K g)(n) = \sum_{t|m} K(m,t)f(t)g\left(\frac{m}{t}\right) \sum_{s|n} K(n,s)f(s)g\left(\frac{n}{s}\right)$$

$$= K(m,d)f(d)g\left(\frac{m}{d}\right) \cdot K(n,e)f(e)g\left(\frac{n}{e}\right) = K(m,d)K(n,e)$$

and

$$(f *_K g)(mn) = \sum_{t|mn} K(mn,t)f(t)g\left(\frac{mn}{t}\right)$$

$$= K(mn,de)f(de)g\left(\frac{mn}{de}\right) = K(mn,de).$$

Since $f *_K g$ is multiplicative by our assumption we have

$$(f *_K g)(m)(f *_K g)(n) = (f *_K g)(mn)$$

which implies that

$$K(m,d)K(n,e) = K(mn,de).$$

Conversely, assume that $K(mn,de) = K(m,d)K(n,e)$ for all m,n,d, and e such that $d|m$ and $e|n$ and $(m,n)=1$ and let f and g be multiplicative, then

$$(f *_K g)(mn) = \sum_{d|mn} K(mn,d)f(d)g\left(\frac{mn}{d}\right)$$

$$\sum_{d_1|m,\, d_2|n} K(mn,d_1d_2)f(d_1)f(d_2)g\left(\frac{m}{d_1}\right)g\left(\frac{n}{d_2}\right)$$

$$\left(\sum_{d_1|m} K(m,d_1)f(d_1)g\left(\frac{m}{d_1}\right)\right)\left(\sum_{d_2|n} K(n,d_2)f(d_2)g\left(\frac{n}{d_2}\right)\right)$$

$$= (f *_K g)(m)(f *_K g)(n).$$

Therefore $f *_K g$ is multiplicative.

(3)

Assume that K-convolution is associative and let n be a positive integer and suppose that $d|n$ and $e|d$. Define arithmetic functions f, g and h in the following way

$$f(k) = \begin{cases} 1 & \text{if } k = e \\ 0 & \text{otherwise} \end{cases}$$

$$g(k) = \begin{cases} 1 & \text{if } k = \frac{d}{e} \\ 0 & \text{otherwise} \end{cases}$$

and

$$h(k) = \begin{cases} 1 & \text{if } k = \frac{n}{d} \\ 0 & \text{otherwise} \end{cases}$$

Let us observe that

$$((f *_K g) *_K h)(n) = \sum_{d|n} K(n,d)(f *_K g)(d)h\left(\frac{n}{d}\right)$$

$$= K(n,d)(f *_K g)(d) = K(n,d) \sum_{e|d} K(d,e)f(e)g\left(\frac{d}{e}\right)$$

$$= K(n,d)K(d,e)f(e)g\left(\frac{d}{e}\right) = K(n,d)K(d,e)$$

and

$$(f *_K (g *_K h))(n) = \sum_{d|n} K(n,d)f(d)(g *_K h)\left(\frac{n}{d}\right)$$

$$= K(n,e)f(e)(g *_K h)\left(\frac{n}{d}\right) = K(n,e)\sum_{t|\frac{n}{e}} K\left(\frac{n}{e},t\right) g(t)h\left(\frac{n}{et}\right)$$

$$= K(n,e)K\left(\frac{n}{e},\frac{d}{e}\right) g\left(\frac{d}{e}\right) h\left(\frac{n}{d}\right) = K(n,e)K\left(\frac{n}{e},\frac{d}{e}\right).$$

Since K-convolution is associative we have

$$K(n,d)K(d,e) = K(n,e)K\left(\frac{n}{e},\frac{d}{e}\right).$$

Coversely, assume that $K(n,d)K(d,e) = K(n,e)K\left(\frac{n}{e},\frac{d}{e}\right)$ for all n, d and e such that $d|n$ and $e|d$, then for every arithmetic functions f, g and h we have

$$((f *_K g) *_K h)(n) = \sum_{d|n} K(n,d)(f *_K g)(d)h\left(\frac{n}{d}\right)$$

$$\sum_{d|n}\sum_{e|d} K(n,d)K(d,e)f(e)g\left(\frac{d}{e}\right) h\left(\frac{n}{d}\right)$$

$$= \sum_{e|n}\sum_{\frac{d}{e},\frac{n}{e}} K(n,e)K\left(\frac{n}{e},\frac{d}{e}\right) f(e)g\left(\frac{d}{e}\right) h\left(\frac{\frac{n}{e}}{\frac{d}{e}}\right)$$

$$\sum_{e|n} f(e)(g *_K h)\left(\frac{n}{e}\right) = (f *_K (g *_K h))(n)$$

thus K-convolution is associative.

(4)

Assume K-convolution is commutative and let n be a positive integer with $d|n$. Define arithmetic functions f and g in the following way

$$f(k) = \begin{cases} 1 & \text{if } k = d \\ 0 & \text{otherwise} \end{cases}$$

and

$$g(k) = \begin{cases} 1 & \text{if } k = \frac{n}{d} \\ 0 & \text{otherwise} \end{cases}$$

Let us observe that

$$(f *_K g)(n) = \sum_{d|n} K(n,d) f(d) g\left(\frac{n}{d}\right) = K(n,d) f(d) g\left(\frac{n}{d}\right) = K(n,d)$$

and

$$(g *_K f)(n) = \sum_{d|n} K(n,d) g(d) f\left(\frac{n}{d}\right) = K\left(n, \frac{n}{d}\right) g\left(\frac{n}{d}\right) f(d) = K\left(n, \frac{n}{d}\right).$$

Since K-convolution is commutative it follows that

$$K(n,d) = K\left(n, \frac{n}{d}\right).$$

Conversely, assume that $K(n,d) = K\left(n, \frac{n}{d}\right)$ for all n and d such that $d|n$ and let f and g be two arithmetic functions, then

$$(f *_K g)(n) = \sum_{d|n} K(n,d) f(d) g\left(\frac{n}{d}\right)$$

$$= \sum_{\frac{n}{d}|n} K\left(n, \frac{n}{d}\right) g\left(\frac{n}{d}\right) f(d) = (g *_K f)(n)$$

Therefore K-convolution is commutative.//

It is simple to show that K-convolution distributes over addition. Let f, g and h be arithmetic functions, then

$$(f *_K (g+h))(n) = \sum_{d|n} K(n,d) f(d)(g+h)\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} K(n,d) f(d) g\left(\frac{n}{d}\right) + \sum_{d|n} K(n,d) f(d) h\left(\frac{n}{d}\right)$$

$$= (f *_K g)(n) + (f *_K h)(n).$$

Thus, K-convolution distributes over addition.

Therefore (1), (3), (4) from theorem 2.2 are the necessary conditions for $(\mathcal{A}, +, *_K)$ to be a commutative ring with unity.

From this point on we will refer to this ring as the K-ring of arithmetic functions. Now we will show the necessary condition for an element of this ring to have a K-convolution inverse, which is similar to the condition shown for the Dirichlet convolution.

Theorem 2.3 [3] *In the K-ring of arithmetic functions* $(\mathcal{A}, +, *_K)$ *an arithmetic function* f *has a* K*-convolution inverse if and only if* $f(1) \neq 0$.

Proof.

Assume f has an inverse f^{-1}, then

$$1 = \delta(1) = (f *_K f^{-1})(1) = K(1,1) f(1) f^{-1}(1)$$

which implies that $f(1) \neq 0$.

Conversely, assume that $f(1) \neq 0$ and define f^{-1} in the following way

$$f^{-1}(1) = \frac{1}{f(1)}$$

and

$$f^{-1}(n) = -\frac{1}{f(1)} \sum_{d|n,\, d>1} K(n,d) f(d) f^{-1}\left(\frac{n}{d}\right)$$

for every $n \geq 2$.

If $n = 1$ we have

$$(f *_K f^{-1})(1) = \sum_{d|1} K(1,d) f(d) f^{-1}(1) = f(1)\frac{1}{f(1)} = 1 = \delta(1)$$

If $n \geq 2$ we have

$$(f *_K f^{-1})(1) = \sum_{d|n} K(n,d) f(d) f^{-1}\left(\frac{n}{d}\right)$$

$$= K(n,1) f(1) f^{-1}(n) + \sum_{d|n,\, d>1} K(n,d) f(d) f^{-1}\left(\frac{n}{d}\right)$$

$$= f(1)\left(-\frac{1}{f(1)} \sum_{d|n,\, d>1} K(n,d) f(d) f^{-1}\left(\frac{n}{d}\right)\right) + \sum_{d|n,\, d>1} K(n,d) f(d) f^{-1}\left(\frac{n}{d}\right)$$

$$= 0 = \delta(n)$$

(note that $K(n,1) = 1$ from Theorem 2.2(1))

Therefore $f *_K f^{-1} = \delta$ and since in this case K-convolution is commutative $f^{-1} *_K f = \delta$, therefore f has an inverse.//

2.2 Regular Arithmetic Convolutions

We will now introduce a special case which is of high interest of K-convolutions.

Definition 2.4 *A K-convolution is called **regular arithmetic convolution** if the following conditions are satisfied:*

(I) ***(1)-(4)*** *of Theorem 2.2 hold for K.*

(II) *$K(n,d) = 0$ or 1 for all n and d such that $d|n$.*

(III) *If $\zeta^{-1} = \mu_K$ then $\mu_K(p^\alpha) = 0$ or -1 for all primes p and all integers $\alpha \geq 1$.*

We will now show two examples of regular arithmetic convolutions.

Examples:

- **Dirichlet convolution.** It has been mentioned before that if we define $K(n,d) = 1$ for all ordered pairs (n,d) such that $d|n$, then the K convolution is just the Dirichlet convolution which of course satisfies **(I)** and $\mu_K = \mu$ the classical Möbius function.

- **Unitary convolution.** Define the function K in the following way

$$K(n,d) = \begin{cases} 1 & \text{if } \left(d, \frac{n}{d}\right) = 1 \\ 0 & \text{otherwise} \end{cases}$$

for all n and d such that $d|n$.

We will refer to a divisor d of n such that $\left(d, \frac{n}{d}\right) = 1$ as a ***unitary divisor*** of n and we will use the following notation, $d||n$. Thus let f and g be arithmetic functions, then for all n

$$(f *_K g)(n) = \sum_{d|n} K(n,d) f(d) g\left(\frac{n}{d}\right) = \sum_{d||n} f(d) g\left(\frac{n}{d}\right).$$

First we need to verify that **(1)**-**(4)** hold for K

(1)

$(n,1) = 1$ and $(1,n) = 1$, therefore $K(n,n) = K(n,1) = 1$.

(2)

Let m, n, d and e such that $d|m$, $e|n$ and $(m,n) = 1$. Certainly if $\left(d, \frac{m}{d}\right) > 1$ or $\left(e, \frac{n}{e}\right) > 1$ then $\left(de, \frac{mn}{de}\right) > 1$. Now if $\left(d, \frac{m}{d}\right) = 1$ and $\left(e, \frac{n}{e}\right) = 1$ then $\left(de, \frac{mn}{de}\right) = 1$.

(3)

Let n, d, and e such that $d|n$ and $e|d$. Showing that $K(n,d)K(d,e) = K(n,e)K\left(\frac{n}{e}, \frac{d}{e}\right)$ is equivalent to showing that

(a) $\left(d, \frac{n}{d}\right) = 1$ and $\left(e, \frac{d}{e}\right) = 1$

(b) $\left(e, \frac{n}{e}\right) = 1$ and $\left(\frac{d}{e}, \frac{\frac{n}{e}}{\frac{d}{e}}\right) = 1$

are equivalent. Since **(2)** holds due to the properties of multiplicative functions when only need to how this for $n = p^\alpha$, $d = p^\beta$ and $e = p^\gamma$, where p is a prime and $0 \le \gamma \le \beta \le \alpha$. Then it suffices to show the equivalence between

(a*) $(\beta = \alpha$ or $\beta = 0)$ and $(\gamma = \beta$ or $\gamma = 0)$

(b*) $(\gamma = \alpha$ or $\gamma = 0)$ and $(\beta = \alpha$ or $\beta = \gamma)$

Ussing the fact that $0 \leq \gamma \leq \beta \leq \alpha$, it follows that these two statements are equivalent.

(4)

Since $\left(n, \frac{n}{d}\right) = \left(\frac{n}{d}, d\right)$, it follows that $K(n,d) = K\left(n, \frac{n}{d}\right)$.

Now, certainly $K(n,d) = 0$ or 1 for all n and d such that $d|n$.

Finally, let us denote $\zeta^{-1} = \mu_U$ for this particular $K-convolution$, then

$$\sum_{d||n} \mu_U(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

If $n = 1$ then we have

$$1 = \sum_{d||1} \mu_U(d) = \mu_U(1)$$

which implies that $\mu_U(1) = 1$.

Now let $n = p$ be prime and $\alpha \geq 1$, then

$$0 = \sum_{d||p^\alpha} \mu_U(d) = \mu_U(1) + \mu_U(p^\alpha) = 1 + \mu_U(p^\alpha)$$

which implies that $\mu_U(p^\alpha) = -1$ for every p prime and every $\alpha \geq 1$. Therefore the third condition is satisfied and this proves that the unitary convolution is regular.

Using the definition of regular arithmetic convolution we introduce another definition.

Definition 2.5 *Suppose that K-convolution is a regular arithmetic convolution. Then for each n define the set:*

$$\Lambda(n) = \{d : \; d|n \text{ and } K(n,d) = 1\}.$$

Then we shall refer to the regular arithmetic convolution Λ, and we write $*_\Lambda$ and μ_Λ in place of $*_K$ and μ_K.

Now let f and g be two arithmetic functions, then

$$(f *_\Lambda g)(n) = \sum_{d \in \Lambda(n)} f(d) g\left(\frac{n}{d}\right)$$

for every n positive integer.

Now, let n be a positive integer and let $\Lambda(n)$ be a nonempty set of divisors of n. Then for all n and d such that $d|n$ define

$$K(n,d) = \begin{cases} 1 & \text{if } d \in \Lambda(n) \\ 0 & \text{if } d \notin \Lambda(n) \end{cases}$$

The resulting K-convolution may or may not be a regular arithmetic convolution.

For regular arithmetic convolutions, the conditions **(1)-(4)** from Theorem 2.2 will be:

(1*) $1, n \in \Lambda(n)$ for every n positive integer.

(2*) If $(m, n) = 1$ then

$$\Lambda(mn) = \{de \,:\, d \in \Lambda(m) \text{ and } e \in \Lambda(n)\}$$

(3*) $d \in \Lambda(n)$ and $e \in \Lambda(d)$ if and only if $e \in \Lambda(n)$ and $\frac{d}{e} \in \Lambda\left(\frac{n}{e}\right)$.

(4*) If $d \in \Lambda(n)$ then $\frac{n}{d} \in \Lambda(n)$.

Next, we present a problem that shows a necessary condition for $\zeta^{-1} = \mu_\Lambda$ to have $\mu_\Lambda(p^\alpha) = 0$ or -1 for all primes p and all integers $\alpha \geq 1$.

Theorem 2.6 [3] *If a K-convolution satisfies **(I)** and **(II)** then it satisfies **(III)** if and only if for each prime p and each $\alpha \geq 1$ there is a divisor t of α such that*

$$\Lambda(p^\alpha) = \left\{1, p^t, p^{2t}, \ldots, p^\alpha\right\}$$

and

$$\Lambda(p^{st}) = \left\{1, p^t, p^{2t}, \ldots, p^{st}\right\}$$

for $1 \leq s \leq \frac{\alpha}{t}$.

Proof.

Assume that the K-convolution satisfies **(I)**, **(II)** and **(III)**. Let

$$\Lambda(p^\alpha) = \{1, p^{\alpha_1}, p^{\alpha_2}, \ldots, p^{\alpha_k}\}$$

where $0 < \alpha_1 < \alpha_2 < \ldots < \alpha_k = \alpha$.

Now suppose there exists j with $0 < j < \alpha_1$ such that $p^j \in \Lambda(p^{\alpha_1})$. Since $p^{\alpha_1} \in \Lambda(p^\alpha)$ and $p^j \in \Lambda(p^{\alpha_1})$, by **(3*)** it follows that $p^j \in \Lambda(p^\alpha)$ which contradicts our assumption, therefore $\Lambda(p^{\alpha_1}) = \{1, p^{\alpha_1}\}$.

Since $\zeta^{-1} = \mu_\Lambda$, we have $\mu_\Lambda(1) = 1$ and

$$0 = \mu_\Lambda(1) + \mu_\Lambda(p^{\alpha_1}) = 1 + \mu_\Lambda(p^{\alpha_1})$$

which implies that $\mu_\Lambda(p^{\alpha_1}) = -1$. Then

$$0 = \mu_\Lambda(1) + \mu_\Lambda(p^{\alpha_1}) + \mu_\Lambda(p^{\alpha_2}) + \ldots + \mu_\Lambda(p^{\alpha_k})$$

$$= 1 + (-1) + \mu_\Lambda(p^{\alpha_2}) + \ldots + \mu_\Lambda(p^{\alpha_k}) = \mu_\Lambda(p^{\alpha_2}) + \ldots + \mu_\Lambda(p^{\alpha_k})$$

by **(III)** $\mu_\Lambda(p^{\alpha_i}) = 0$ for $2 \le i \le k$.

Let $t = \alpha_1$. We will prove the result by induction on $1 \le s \le k$, that $\alpha_s = st$ and $\Lambda(p^{st}) = \{1, p^t, p^{2t}, \ldots, p^{st}\}$.

If $s = 1$, then $\alpha_1 = t$ and $\Lambda(p^t) = \{1, p^t\} = \Lambda(p^{\alpha_1}) = \{1, p^{\alpha_1}\}$ which is true. Therefore assume that $s \ge 2$ and that the result holds for $s = 1, 2, \ldots, k-1$.

By (3*), $\Lambda(p^{\alpha_k})$ is a subset of $\left\{1, p^t, \ldots, p^{(k-1)t}, p^{\alpha_k}\right\}$. It has been shown that $\mu_\Lambda(p^{\alpha_i}) = 0$ for $2 \le i \le k$, thus p^t is an element of $\Lambda(p^{\alpha_k})$. By **(4*)**, since $p^t \in \Lambda(p^{\alpha_k})$, then $p^{\alpha_k - t} \in \Lambda(p^{\alpha_k})$, and since $(k-2)t < \alpha_k - t < \alpha_k$ it imples that $\alpha_k - t = (k-1)t$, which means that $\alpha_k = kt$ and $p^{(k-1)t} \in \Lambda(p^{\alpha_k})$.

Now let $2 \le i \le k-2$, and $n = p^{kt}$, $d = p^{it}$ and $e = p^t$, then

$$\frac{d}{e} = p^{(i-1)t} \in \Lambda(p^{(k-1)t}) = \Lambda\left(\frac{n}{e}\right)$$

and

$$e = p^t \in \Lambda(p^{kt}) = \Lambda(n)$$

thus by **(3*)** it implies that

$$p^{it} = d \in \Lambda(n) = \Lambda(p^{kt}).$$

Therefore,

$$\Lambda(p^{\alpha_k}) = \Lambda(p^{kt}) = \left\{1, p^t, p^{2t}, \ldots, p^{kt}\right\}$$

thus the result holds for all $1 \leq s \leq k$. Therefore

$$\Lambda(p^{st}) = \left\{1, p^t, p^{2t}, \ldots, p^{st}\right\}$$

for $1 \leq s \leq \frac{\alpha}{t}$.

Conversely, assume that **(I)** and **(II)** hold. Let p be prime and let $\alpha \geq 1$ and assume that

$$\Lambda(p^{\alpha}) = \left\{1, p^t, p^{2t}, \ldots, p^{\alpha}\right\}$$

where t is a divisor of α and

$$\Lambda(p^{st}) = \left\{1, p^t, p^{2t}, \ldots, p^{st}\right\}$$

for $1 \leq s \leq \frac{\alpha}{t}$.

Since $\Lambda(p^t) = \{1, p^t\}$ we have

$$0 = \mu_\Lambda(1) + \mu_\Lambda(p^{\alpha_1}) = 1 + \mu_\Lambda(p^{\alpha_1})$$

which implies that $\mu_\Lambda(p^{\alpha_1}) = -1$.

Now assume that $\alpha > t$. Since $\Lambda(p^{2t}) = \{1, p^t, p^{2t}\}$ we have

$$0 = \mu_\Lambda(1) + \mu_\Lambda(p^t) + \mu_\Lambda(p^{2t}) = 1 + (-1) + \mu_\Lambda(p^{2t}) = \mu_\Lambda(p^{2t})$$

By induction on the same manner it follows that $\mu_\Lambda(p^i) = 0$ for $2t \leq i \leq \alpha$. Therefore it follows that $\mu_K(p^\alpha) = 0$ or -1 for all primes p and all integers $\alpha \geq 0$.//

Using these results we now introduce the following definition.

Consider a regular arithmetic convolution Λ. If p is a prime and $\alpha \geq 1$. Then

$$\Lambda(p^\alpha) = \left\{1, p^t, p^{2t}, \ldots, p^{kt}\right\},\ \alpha = kt.$$

Definition 2.7 *The divisor t of α is called **type of** p^α **with respect to** Λ, and we will use the notation $t_\Lambda(p^\alpha)$.*

The following consequence follows from the previous theorem.

Corollary 2.8 [3] *Let p be a prime and $\alpha, \beta \geq 1$. If $\Lambda(p^\alpha) \cap \Lambda(p^\beta) \neq \{1\}$ then $t_\Lambda(p^\alpha) = t_\Lambda(p^\beta) = t$ and (assuming $\alpha \leq \beta$) $\Lambda(p^\alpha)$ consists of the $\left(\frac{\alpha}{t} + 1\right)$ smallest integers in $\Lambda(p^\beta)$.*

Proof.

If $p^\gamma \in \Lambda(p^\alpha) \cap \Lambda(p^\beta)$ and $p^\gamma > 1$ then $t_\Lambda(p^\alpha) = t_\Lambda(p^\gamma) = t_\Lambda(p^\beta)$. Therefore there exists h and k such that $\alpha = ht$ and $\beta = kt$, and by our assumption that $\alpha \leq \beta$, we have

$$\Lambda(p^\alpha) = \left\{1, p^t, p^{2t}, \ldots, p^{ht}\right\}$$

and

$$\Lambda(p^\beta) = \left\{1, p^t, p^{2t}, \ldots, p^{ht}, p^{(h+1)t}, \ldots, p^{kt}\right\} = \Lambda(p^\alpha) \cap \left\{p^{(h+1)t}, \ldots, p^{kt}\right\}$$

which implies that $\Lambda(p^\alpha)$ consists of the $(ht+1) = \left(\frac{\alpha}{t} + 1\right)$ smallest integers in $\Lambda(p^\beta)$.//

A regular arithmetic convolution Λ is determined by the sets $\Lambda(p^\alpha)$ for every prime p and every positive integer α.

We will denote the Dirichlet convolution by D. Then for every p^α, we have

$$D(p^\alpha) = \left\{1, p, p^2, \ldots, p^\alpha\right\}$$

which implies that $t_D(p^\alpha) = 1$.

We will denote the unitary convolution by U. Then for every p^α, we have

$$U(p^\alpha) = \{1, p^\alpha\}$$

which implies that $t_U(p^\alpha) = \alpha$.

Therefore using this results and the results of the previous theorems, it follows that if Λ is an arbitrary arithmetic convolution, then for every p^α, we have

$$U(p^\alpha) \subseteq \Lambda(p^\alpha) \subseteq D(p^\alpha).$$

Thus, every arithmetic convolution is "in between" the unitary convolution and the Dirichlet convolution.

Definition 2.9 *Let Λ be a regular arithmetic convolution. A positive integer n such that $\Lambda(n) = \{1, n\}$ is called **primitive** (with respect to Λ).*

These primitives have some properties. By **(2*)** if n is primitive then $n = p^\alpha$ where p is prime and α is a positive integer. Moreover, we can say that p^α is primitive if and only if $t_\Lambda(p^\alpha) = \alpha$. Also, as shown in the previous theorem, if p is prime and α a positive integer, then

$$\mu_\Lambda(p^\alpha) = \begin{cases} -1 & \text{if } p^\alpha \text{ is primitive} \\ 0 & \text{otherwise} \end{cases}$$

Now we will present an analogue of a very important application of the Möbius function. Using the fact that $\zeta^{-1} = \mu_\Lambda$ we have an analogue of the Möbius inversion formula:

Let f and g be arithmetic functions then

$$f(n) = \sum_{d \in \Lambda(n)} g(d)$$

if and only if

$$g(n) = \sum_{d \in \Lambda(n)} f(d) \mu_{\Lambda} \left(\frac{n}{d} \right)$$

for every positive integer n.

Chapter 3

Generalizations of Dirichlet Convolutions in Categories

3.1 Basic Concepts in Categories

Category theory is a branch of mathematics that tries to generalize the structures and the properties of mathematical concepts in an abstract way. It provides a general conceptual framework with many results in diverse areas of mathematics such as geometry, topology, theoretical computer science, and foundational mathematics. In the years of 1942 to 1945 Samuel Elienberg and Saunders Mac Lane introduced the concepts of categories, functors and natural transformations as part of their work in algebraic topology. Category theory has contributed to many areas of mathematics, leading to many results that have been stated and proved, in a much simpler way than without the use of categories.

Let us begin by defining the basic concepts of categories.

Definition 3.1 *A category $\mathcal{C}$ is a mathematical structure consisting of the following entities:*

1. *A class of objects denoted $Ob\mathcal{C}$.*
2. *For every two objects A and B of $Ob\mathcal{C}$, a set $Hom_{\mathcal{C}}[A, B]$ of morphims from A to B. If $\alpha \in Hom_{\mathcal{C}}[A, B]$, we shall call A the domain of α and B the codomain.*

3. *For every* $A, B, C \in Ob\mathcal{C}$ *a function from* $Hom_{\mathcal{C}}[A, B] \times Hom_{\mathcal{C}}[B, C]$ *to* $Hom_{\mathcal{C}}[A, C]$ *such that* $(\alpha, \beta) \longmapsto \beta\alpha$. *This function is called composition.*

The composition functions are subject to two axioms:

Axiom a *Associativity: For every morphims* α, β, γ *we have* $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ *whenever the compositions make sense.*

Axiom b *Existence of identities: For every* $A \in Ob\mathcal{C}$ *there exists an element* $1_A \in Hom_{\mathcal{C}}[A, A]$ *such that* $1_B\alpha = \alpha = \alpha 1_A$ *for every* $\alpha \in Hom_{\mathcal{C}}[A, B]$ *. The identity morphism is unique.*

Moreover, we also have special cases of categories.

Definition 3.2 *If* $Ob\mathcal{C}$ *is a set then we called the category a* ***small category****.*

Definition 3.3 *We shall call the category* $\mathcal{C}'$ *a* ***subcategory*** *of* $\mathcal{C}$ *if the following conditions are satisfied:*

1. $Ob\mathcal{C}' \subseteq Ob\mathcal{C}$.
2. $Hom_{\mathcal{C}'}[A, B] \subseteq Hom_{\mathcal{C}}[A, B]$ *for every* $A, B \in Ob\mathcal{C}'$.
3. *For any two morphism, the composition in* $\mathcal{C}'$ *is the same as in* $\mathcal{C}$.
4. 1_A *is the same in* $\mathcal{C}'$ *as in* $\mathcal{C}$ *for every* $A \in Ob\mathcal{C}$.

Moreover, if $Hom_{\mathcal{C}'}[A, B] = Hom_{\mathcal{C}}[A, B]$ for every $A, B \in Ob\mathcal{C}'$, we call $\mathcal{C}'$ a **full subcategory** of $\mathcal{C}$.

Definition 3.4 *A category* $\mathcal{C}^*$ *is called the* ***dual category*** *of a category* $\mathcal{C}$ *if the following are satisfied:*

1. $Ob\mathcal{C} = Ob\mathcal{C}^*$.

2. $Hom_{\mathcal{C}}[A, B] = Hom_{\mathcal{C}^*}[B, A]$.

3. *The composition* $\beta\alpha$ *in* $\mathcal{C}^*$ *is defined as the composition* $\alpha\beta$ *in* $\mathcal{C}$.

A very important concept in category theory is the concept of diagram commutativity.

Definition 3.5 *Given three morphisms* f, g, h*, we say that the following diagram* ***commutes*** *if and only if* $h = gf$.

$$\begin{tikzcd} \bullet \arrow[rr, "h"] \arrow[dr, "f"'] & & \bullet \\ & \bullet \arrow[ur, "g"'] & \end{tikzcd}$$

There exists many examples of categories, we will just mention some of the most common.

1. **Set** - The category of sets. The objects are sets, the morphisms $Hom_{Set}[A, B]$ are all the functions from A to B, and the composition function is the usual composition of functions.

2. **Pfn** - The category of sets and partial functions. The objects are sets as in **Set**

3. **Set**$_0$ - The category of sets with base point. The objects are ordered pairs (A, a) where A is a set and $a \in A$, the morphisms $Hom_{Set_0}[A, B] = \{f | f : A \to B \; and \; f(a) = b\}$, and the composition is the usual composition of functions.

4. **Top** - The category of topological spaces. The objects are topological spaces, the morphims are continuous mappings, and the composition is defined since the composition of two continuous mappings is also continuous.

5. **Mon, Sgp, Grp, Rng** - The Categories of Monoids, Semigroups, Groups, and Rings respectively. The objects are monoids, semigroups, groups, and rings respectively, the morphims are the usual morphisms, and the composition is the usual composition.

6. **A monoid (M,*)** - A monoid $(M, *)$ seen as a category. A monoid itself can be considered a category with one object denoted by $\bullet$, the morphism are the elements of M, and the composition is the operation $*$.

7. **Vect**$_K$ - The Category of Vector Spaces over a field K. The objects are all the vector spaces over a field K, the morphisms are the K-Linear transformations, and the composition is the usual composition of linear transformations.

8. **Pos** - The Category of Posets. The objects are posets, the morphisms are monotone functions, and the composition is the usual composition of functions.

9. **A poset (P,$\leq$)** -A Poset $(P, \leq)$ seen as a category. The objects are the elements of P, for any two objects $a, b \in P$ there exists a morphism between them if and only if $a \leq b$, and there is at most one such morphism, and the composition defined by $(c, b)(b, a) = (c, a)$ is well defined since $a \leq b \leq c \Rightarrow a \leq c$.

In category theory the notions of injectivity and surjectivity are generalized in the following way:

Definition 3.6 *A morphism $\alpha \in Hom_{\mathcal{C}}[A, B]$ is called a **corretraction** if there exists a morphism $\beta \in Hom_{\mathcal{C}}[B, A]$ such that $\beta\alpha = 1_A$.*

Definition 3.7 *A morphism $\alpha \in Hom_{\mathcal{C}}[A, B]$ is called a **retraction** if there exists a morphism $\beta \in Hom_{\mathcal{C}}[B, A]$ such that $\alpha\beta = 1_B$.*

Definition 3.8 *A morphism α that is both a retraction and a corretraction is called an **isomorphism**.*

Definition 3.9 *A morphism whose domain is the same as the codomain is called an **endomorphism**.*

Definition 3.10 *An endomorphism that is also an isomorphism is called an* ***automorphism****.*

Definition 3.11 *A morphism* $\alpha \in Hom_{\mathcal{C}}[A, B]$ *is called a* ***monomorphism*** *if* $\alpha\beta = \alpha\gamma$ *implies* $\beta = \gamma$ *for every* β, γ *with codomain A.*

Definition 3.12 *A morphism* $\alpha \in Hom_{\mathcal{C}}[A, B]$ *is called an* ***epimorphism*** *if* $\beta\alpha = \gamma\alpha$ *implies* $\beta = \gamma$ *for every* β, γ *with domain A.*

Definition 3.13 *A morphims which is both a monomorphism and an epimorphism is called a* ***bimorphism****.*

Now let us prove some properties that we obtain from these types of morphism in category theory.

Proposition 3.14 [2] *If* $\alpha \in Hom_{\mathcal{C}}[A, B]$ *is both a corretraction and an epimorphism, then it is an isomorphism.*

Proof.

Let $\beta\alpha = 1_A$, then

$$(\alpha\beta)\alpha = \alpha(\beta\alpha) = \alpha 1_A = \alpha = 1_B\alpha,$$

since α is an epimorphism it follows that $\alpha\beta = 1_B$. Therefore α is a retraction which means that it is also an isomorphim.//

Proposition 3.15 [2] *If* $\alpha \in Hom_{\mathcal{C}}[A, B]$ *is both a retraction and an monomorphism,*

then it is an isomorphism.

Proof.

Let $\alpha\beta = 1_A$, then

$$\alpha(\beta\alpha) = (\alpha\beta)\alpha = 1_A\alpha = \alpha = \alpha 1_B,$$

since α is an monomorphism it follows that $\beta\alpha = 1_B$. Therefore α is a coretraction which means that it is also an isomorphim.//

Proposition 3.16 [2] *Let $\mathcal{C}$ be a category and $\alpha \in Hom_{\mathcal{C}}[A, B]$. Then following statements are true:*

- *If α is a coretraction, then it is a monomorphism.*

Proof.

Since α is a coretraction, there exists $\beta \in Hom_{\mathcal{C}}[B, A]$ such that $\beta\alpha = 1_A$. Now assume $\alpha\gamma = \alpha\delta$ for some $\gamma, \delta \in Hom_{\mathcal{C}}[C, A]$. We have

$$\gamma = 1_A\gamma = (\beta\alpha)\gamma = \beta(\alpha\gamma) = \beta(\alpha\delta) = (\beta\alpha)\delta = 1_A\delta = \delta,$$

therefore α is a monomorphism.//

- *If α is a retraction, then it is an epimorphism.*

Proof.

Since α is a coretraction, there exists $\beta \in Hom_{\mathcal{C}}[B, A]$ such that $\alpha\beta = 1_B$. Now assume $\gamma\alpha = \delta\alpha$ for some $\gamma, \delta \in Hom_{\mathcal{C}}[B, C]$. We have

$$\gamma = \gamma 1_B = \gamma(\alpha\beta) = (\gamma\alpha)\beta = (\delta\alpha)\beta = \delta(\alpha\beta) = \delta 1_B = \delta,$$

therefore α is an epimorphism.//

Now let us consider this type of morphism in an example, in this case the commonly known category **Set**.

Proposition 3.17 [7] *Consider the category **Set**, then the following statements are true:*

- *If $f \in Hom_{Set}[B, A]$ is injective as a function, then it is monomorphism.*

Proof.

Assume that $f \circ g = f \circ h$ for some $g, h \in Hom_{Set}[C, B]$. We have

$$f(g(x)) = (f \circ g)(x) = (f \circ h)(x) = f(h(x))$$

for every $x \in C$. Since f is injective, that implies that $g(x) = h(x)$ for every $x \in C$, which implies that$f$ is a monomorphism.//

- *If $f \in Hom_{Set}[A, B]$ is surjective as a function, then it is an epimorphism.*

Proof.

Assume that $g \circ f = h \circ f$ for some $g, h \in Hom_{Set}[B, C]$. Now, consider any $y \in B$. Since f is surjective we have $f(x) = y$ for some $x \in A$. Then

$$g(y) = g(f(x)) = (g \circ f)(x) = (h \circ f)(x) = h(f(x)) = h(y)$$

for every $y \in B$, which implies that f is an epimorphism.//

We must also mention certain types of objects that are of special interest in the study of categories.

Definition 3.18 *An object I of a cateory $\mathcal{C}$ is called **initial** if for every object A there is a unique morphism α such that $\alpha : I \to A$.*

Definition 3.19 *An object F of a cateory $\mathcal{C}$ is called **final** if for every object B there is a unique morphism β such that $\beta : B \to F$.*

Definition 3.20 *An object 0 that is both initial and final is called a **zero object**.*

Examples

- Consider the category **Set**. The initial object is $\emptyset$ because for every $A \in Ob\mathbf{Set}$ there exists a unique function $f : \emptyset \to A$, since the function does not have any requirements that it must satisfy. The final object is any singleton set $\{a\}$, since for every $A \in Ob\mathbf{Set}$ there exists a unique function $f : A \to \{a\}$ that maps every element of A into a.

- Consider the category **Grp**. The initial object is the trivial group $\{e\}$, where e is an identity element, since for every $G \in Ob\mathbf{Grp}$ there is a unique homomorphism $\varphi : e \to G$ that maps e into the identity of G. The final object is again $\{e\}$, since $G \in Ob\mathbf{Grp}$ there is a unique homomorphism $\varphi : G \to \{e\}$ that maps every element of G into e. Therefore $\{e\}$ is a zero object.

We can also define mappings between two categories which arise the concept of Functors, which we will define in the following.

Definition 3.21 *Given two categories $\mathcal{C}$ and $\mathcal{D}$,a* ***(covariant) functor*** $T : \mathcal{C} \to \mathcal{D}$ *is an assigment that maps every object $A \in Ob\mathcal{C}$ to an object $T(A) \in Ob\mathcal{D}$, and every morphims $\alpha \in Hom_{\mathcal{C}}[A, B]$ to a morphism $T(\alpha) \in Hom_{\mathcal{D}}[T(A), T(B)]$.*

A (covariant) functor needs to satisfy these two conditions:

1. *If $\alpha\beta$ makes sense in $\mathcal{C}$, then $T(\alpha\beta) = T(\alpha)T(\beta)$.*

2. *For every $A \in Ob\mathcal{C}$ we have $T(1_A) = 1_{T(A)}$*

For ***contravariant functor*** *the first condition is different*

1. *If $\alpha\beta$ makes sense in $\mathcal{C}$, then $T(\alpha\beta) = T(\beta)T(\alpha)$*

Examples

- The Power Set functor $\mathcal{P} : \mathbf{Set} \to \mathbf{Set}$ that maps every set to its power set and every function $f : A \to B$ to the function that maps $C \subseteq A$ into its image $f(C) \subseteq B$.

- The forgetful functor $F : \mathbf{Grp} \to \mathbf{Set}$ that maps every group to its underlying set and every homomorphism to its underlying set function.

- Given two monoids M and N viewed as categories, a functor is a monoid morphism from M to N.

- Given two posets P and R viewed as categories, a functor is a monotone map.

3.2 Mӧbius Categories

Mӧbius categories play an important role as a generalization of the concept of Mӧbius inversion and Dirichlet Convolution. We will denote the set of morphism of a category $\mathcal{C}$ by $Mor\mathcal{C}$.

Definition 3.22 *A **decomposition-finite** category is a small category $\mathcal{C}$ such that for each morphism α, the set*

$$< \alpha >= \{(\beta, \gamma) \in Mor\mathcal{C} \times Mor\mathcal{C} \ : \ \beta\gamma = \alpha\}$$

is finite.

Definition 3.23 *If $\alpha = \alpha_1\alpha_2 \ldots \alpha_n$, then we say that n is the degree of the decomposition $\alpha = \alpha_1\alpha_2 \ldots \alpha_n$. The supremum of the degrees of decompositions without identities of a morphism α is called the **length** of α and it is denoted by $l(\alpha)$.*

Definition 3.24 *A morphism is called **idecomposable** if it has no decompositions without identities of a degree$\geq$2.*

Proposition 3.25 [4] *Let $\mathcal{C}$ be a decomposition-finite category. Then the following statements are equivalent:*

(1) *$\mathcal{C}$ is a category with finite length (i.e. $l(\alpha)$ is finite for any $\alpha \in Mor\mathcal{C}$);*

(2) *(a) $\mathcal{C}$ has no non-identity retractions and coretractions,*
(b) if $\alpha\beta = \alpha$ then β is an identity;

(3) *(a) $\mathcal{C}$ has no non-identity retractions and coretractions,*
(b) if $\beta\alpha = \alpha$ then β is an identity.

Proof.

(1)$\Rightarrow$(2),(3)

Assume that $\mathcal{C}$ is a category with finite length and let β, γ be two morphims of $\mathcal{C}$. If $\beta\gamma$ is an identity, then β is an identity if and only if γ is an identity. If $\beta\gamma$ is an identity and β, γ are not identities then

$$1_{Dom\gamma} = 1_{Dom\gamma}^n = (\beta\gamma)(\beta\gamma)\dots(\beta\gamma) = \beta\gamma\beta\gamma\dots\beta\gamma$$

is a decomposition of $1_{Dom\gamma}$ without identities. Thus $l(1_{Dom\gamma}) \geq 2n$ for any positive integer n, which contradicts our assumption that $\mathcal{C}$ has finite length. Therefore it must be the case that if $\beta\gamma$ is an identity, then β and γ are identities. Therefore $\mathcal{C}$ has no non-identity retractions and coretractions.

Now, if $\alpha\beta = \alpha$ then $\alpha\beta^n = \alpha$ for any positive integer n. By our assumption that $\mathcal{C}$ has finite length it must be the case that β is an identity. Similarly if $\beta\alpha = \alpha$ then β is an identity.

(2)⇒(1)

Assume that $\mathcal{C}$ has no non-identity retractions and coretractions and if $\alpha\beta = \alpha$ then β is an identity. Suppose now that there exists a morphism α of $\mathcal{C}$ such that α has no finite length. Now $(\alpha, 1_{Dom\alpha}), (1_{Codom\alpha}, \alpha) \in < \alpha >$,, thus if $| < \alpha > | = m$ it must be the case that $m \geq 2$, then there exists $n > m$ and $\alpha_1, \alpha_2, \dots, \alpha_n$ not identities such that $\alpha = \alpha_1\alpha_2\dots\alpha_n$. By our assumption for any positive integers s and t such that $1 \leq s < t \leq n$, the morphism $\alpha_s\dots\alpha_t$ is not an identity. Since $n > m$, there exists positive integers p and q such that $1 \leq p < q \leq m$ and

$$(\alpha_1\dots\alpha_p, \alpha_{p+1}\dots\alpha_n) = (\alpha_1\dots\alpha_q, \alpha_{q+1}\dots\alpha_n),$$

where

$$(\alpha_1 \dots \alpha_p, \alpha_{p+1} \dots \alpha_n), (\alpha_1 \dots \alpha_q, \alpha_{q+1} \dots \alpha_n) \in <\alpha> \setminus \{(\alpha, 1_{Dom\alpha}), (1_{Codom\alpha}, \alpha)\}.$$

Thus

$$\alpha_1 \dots \alpha_p = \alpha_1 \dots \alpha_p \alpha_{p+1} \dots \alpha_q.$$

By our assumption it must be the case that $\alpha_{p+1} \dots \alpha_q$ is an identity, which contradicts our assumption that $\mathcal{C}$ has no non-identity retractions and coretractions. Therefore $\mathcal{C}$ is a category with finite length.

Definition 3.26 *A **Möbius category** is a decomposition-finite category with finite length.*

By our previuos proposition it follows that in a Möbius category the identity morphisms are idecomposable and they have length 0. The non-identity idecomposable morphisms have length 1.

Definition 3.27 *Let α be a morphism of a Möbius category, then the decomposition $\alpha = \alpha_1 \alpha_2 \dots \alpha_n$ is called **elementary** if and only if $\alpha_1, \alpha_2, \dots, \alpha_n$ are all non-identity idecomposable morphisms.*

Definition 3.28 *The **incidence algebra** $A(\mathcal{C})$ of a decomposition-finite category $\mathcal{C}$ is the $\mathbb{C}$-algebra of all complex valued functions (called incidence functions) $\xi : Mor\mathcal{C} \to \mathbb{C}$ with the usual vector space structure and multiplication given by convolution:*

$$(\xi * \psi)(\alpha) = \sum_{(\beta,\gamma) \in <\alpha>} \xi(\beta)\psi(\gamma)$$

Where the identity element of $A(\mathcal{C})$, η is defined by

$$\eta(\alpha) = \begin{cases} 1 & \text{if } \alpha \text{ is an identity morphism} \\ 0 & \text{otherwise} \end{cases}$$

Since given an incidence function $\xi \in A(\mathcal{C})$ we have

$$(\xi * \eta)(\alpha) = \sum_{(\beta,\gamma)\in<\alpha>} \xi(\beta)\eta(\gamma) = \xi(\alpha)\eta(1_{Dom\alpha}) = \xi(\alpha)$$

and

$$(\eta * \xi)(\alpha) = \sum_{(\beta,\gamma)\in<\alpha>} \eta(\beta)\xi(\gamma) = \eta(1_{Codom\alpha})\xi(\alpha) = \xi(\alpha),$$

thus η is the identity element.

Now, let α be a morphism of $\mathcal{C}$ and define the incidence function ξ_α in the following way:

$$\xi_\alpha(\gamma) = \begin{cases} 1 & \text{if } \gamma = \alpha \\ 0 & \text{if } \gamma \neq \alpha \end{cases}$$

Moreover, $\xi_\alpha * \xi_\beta = \xi_{\alpha\beta}$ if the composition $\alpha\beta$ makes sense, since for an incidence function γ

$$(\xi_\alpha * \xi_\beta)(\gamma) = \sum_{\eta\lambda\in<\gamma>} \xi_\alpha(\eta)\xi_\beta(\lambda)$$

will only be equal to 1 if $\alpha\beta = \gamma$, and 0 otherwise, which is the definition of $\xi_{\alpha\beta}$.

Theorem 3.29 [4] *Let $\mathcal{C}$ be a decomposition-finite category. The following statements*

are equivalent:

(1) *$\mathcal{C}$ is a Möbius category;*

(2) *An incidence function $\xi \in A(\mathcal{C})$ has a convolution inverse if and only if $\xi(1_A) \neq 0$ for all $A \in Ob\mathcal{C}$, where 1_A denotes the identity morphism from A to A.*

Proof.

(1)⇒(2)

Assume $\mathcal{C}$ is a Möbius category and that $\xi \in A(\mathcal{C})$ has a convolution inverse call it ψ. Then $\xi * \psi = \psi * \xi = \eta$ which implies that

$$1 = \eta(1_A) = (\xi * \psi)(1_A) = \xi(1_A)\psi(1_A)$$

for every $A \in Ob\mathcal{C}$. Therefore $\xi(1_A) \neq 0$ for every $A \in Ob\mathcal{C}$.

Conversely, assume that $\xi(1_A) \neq 0$ for all $A \in Ob\mathcal{C}$. Define an incidence function $\psi \in A(\mathcal{C})$ in the following way:

$$\psi(\alpha) = \begin{cases} \frac{1}{\xi(\alpha)} & \text{if } \alpha \text{ is and identity} \\ -\frac{1}{\xi(1_{Codom\alpha})} \sum_{(\beta,\gamma)\in<\alpha>,\, \gamma\neq\alpha} \xi(\beta)\psi(\gamma) & \text{if } l(\alpha) \geq 1 \end{cases}$$

in which the second equation is well defined since suppose that $\psi(\delta)$ has been defined for all $\delta \in Mor\mathcal{C}$ such that $l(\delta) \leq l(\alpha)$. Now, if $(\beta,\gamma) \in< \alpha >$ and $\gamma \neq \alpha$ then $l(\gamma) < l(\alpha)$; thus $\psi(\gamma)$ has been defined.

Now if $\alpha = 1_A$ is an identity then,

$$(\xi * \psi)(1_A) = \xi(1_A)\psi(1_A) = \xi(1_A)\frac{1}{\xi(1_A)} = 1 = \eta(1_A)$$

and if $l(\alpha) \geq 1$ then,

$$(\xi * \psi)(\alpha) = \sum_{(\beta,\gamma)\in<\alpha>} \xi(\beta)\psi(\gamma)$$

$$= \xi(1_{Codom\alpha})\psi(\alpha) + \sum_{(\beta,\gamma)\in<\alpha>,\, \gamma\neq\alpha} \xi(\beta)\psi(\gamma)$$

$$= \xi(1_{Codom\alpha}) \left(-\frac{1}{\xi(1_{Codom\alpha})} \sum_{(\beta,\gamma)\in<\alpha>,\, \gamma\neq\alpha} \xi(\beta)\psi(\gamma) \right) + \sum_{(\beta,\gamma)\in<\alpha>,\, \gamma\neq\alpha} \xi(\beta)\psi(\gamma)$$

$$= 0 = \eta(\alpha).$$

Thus, $\xi * \psi = \eta$.

Now, since $\psi(\alpha) \neq 0$ for any identities α, there exists an incidence function $\psi' \in A(\mathcal{C})$ such that $\psi * \psi' = \eta$. Then

$$\psi * \xi = \psi * \xi * \eta = \psi * \xi * \psi * \psi' = \psi * \eta * \psi' = \psi * \psi' = \eta$$

Therefore, $\xi^{-1} = \psi$.

(2)⇒(1)

Assume that an incidence function $\xi \in A(\mathcal{C})$ has a convolution inverse if and only if $\xi(1_A) \neq 0$ for all $A \in Ob\mathcal{C}$. To show that $\mathcal{C}$ is a Möbius Category we need to show that:

(a) $\mathcal{C}$ has no non-identity retractions and coretractions,

(b) if $\alpha\beta = \alpha$ then β is an identity.

Let us prove **(a)** first. Suppose that $\alpha\beta = 1_{Dom\beta}$ with α non-identity, then β is also a non-identity morphism of $\mathcal{C}$. Thus, for any identity morphisn γ, we have

$$(\eta + \xi_\alpha)(\gamma) = \eta(\gamma) + \xi_\alpha(\gamma) = 1 + 0 = 1$$

and

$$(\eta - \xi_\beta)(\gamma) = \eta(\gamma) - \xi_\beta(\gamma) = 1 - 0 = 1.$$

Therefore by our assumption $\eta + \xi_\alpha$ and $\eta - \xi_\beta$ have a convolution inverse. This implies that $(\eta + \xi_\alpha) * (\eta - \xi_\beta)$ has a convolution inverse in the incidence algebra $A(\mathcal{C})$. But

$$[(\eta + \xi_\alpha) * (\eta - \xi_\beta)]\,(1_{Dom\beta}) = \sum_{(\delta,\lambda)\in<1_{Dom\beta}>} (\eta + \xi_\alpha)(\delta)(\eta - \xi_\beta)(\lambda)$$

$$= (\eta + \xi_\alpha)(1_{Dom\beta})(\eta - \xi_\beta)(1_{Dom\beta}) = (\eta + \xi_\alpha - \xi_\beta - \xi_{\alpha\beta})(1_{Dom\beta}) = 1 + 0 - 0 - 1 = 0,$$

which is a contradiction to our assumption. Therefore $\mathcal{C}$ has no non-identity retractions and coretractions.

Now let us prove **(b)**. Suppose that $\alpha\beta = \alpha$ where β is a non-identity morphism. Then we obtain

$$(\eta - \xi_\alpha) * (\eta - \xi_\beta) = \eta - \xi_\alpha - \xi_\beta + \xi_{\alpha\beta} = \eta - \xi_\alpha - \xi_\beta + \xi_\alpha = \eta - \xi_\beta$$

and

$$(\eta + \xi_\alpha) * (\eta - \xi_\beta) = \eta + \xi_\alpha - \xi_\beta - \xi_{\alpha\beta} = \eta + \xi_\alpha - \xi_\beta - \xi_\alpha = \eta - \xi_\beta.$$

Setting this two together we obtain that

$$(\eta - \xi_\alpha) * (\eta - \xi_\beta) = (\eta + \xi_\alpha) * (\eta - \xi_\beta).$$

Now since β is a non-identity morphism we have

$$(\eta - \xi_\beta)(1_A) = \eta(1_A) - \xi_\beta(1_A) = 1 - 0 = 1$$

for every $A \in Ob\mathcal{C}$. Hence $\eta - \xi_\beta$ has a convolution inverse and we obtain

$$(\eta-\xi_\alpha)*(\eta-\xi_\beta) = (\eta+\xi_\alpha)*(\eta-\xi_\beta) \Rightarrow (\eta-\xi_\alpha)*(\eta-\xi_\beta)*(\eta-\xi_\beta)^{-1} = (\eta+\xi_\alpha)*(\eta-\xi_\beta)*(\eta-\xi_\beta)^{-1}$$

$$\Rightarrow \eta - \xi_\alpha = \eta + \xi_\alpha$$

but

$$-1 = (\eta - \xi_\alpha)(\alpha) = (\eta + \xi_\alpha) = 1$$

which is a contradiction. Therefore β is an identity morphism of $\mathcal{C}$.

Therefore $\mathcal{C}$ is a Möbius Category.//

Like we have define a Möbius function before, we can define the Möbius function μ of a Möbius category $\mathcal{C}$ as the convolution inverse of the zeta function ζ of the incidence algebra $A(\mathcal{C})$ define as $\zeta(\alpha) = 1$ for every $\alpha \in Mor\mathcal{C}$. Then the Möbius inversion formula for the Möbius category $\mathcal{C}$ is the following: if ξ is an incidence function then

$$\nu = \xi * \zeta \quad \Leftrightarrow \quad \xi = \nu * \mu \quad \text{and} \quad \psi = \zeta * \xi \quad \Leftrightarrow \quad \xi = \mu * \psi.$$

Definition 3.30 *Let α be a morphism of a category $\mathcal{C}$. The **interval** $I\alpha$ is the category constructed as follows:*

- $ObI\alpha = \{(\alpha_0, \alpha_1) \ : \ \alpha_0, \alpha_1 \in Mor\mathcal{C} \text{ and } \alpha = \alpha_1\alpha_0\}$
- $Hom((\alpha_0, \alpha_1), (\beta_0, \beta_1)) = \{\lambda \in Mor\mathcal{C} \ : \ \beta_0 = \lambda\alpha_0 \text{ and } \beta_1\lambda = \alpha_1\}$

- *If* $\delta : (\beta_0, \beta_1) \to (\gamma_0, \gamma_1)$ *is another morphism of* $I\alpha$*, the composition* $\delta\lambda$ *is the morphism* $(\alpha_0, \alpha_1) \to (\gamma_0, \gamma_1)$ *in* $I\alpha$*.*

Definition 3.31 *A small category* $\mathcal{C}$ *is called one-way if*

1. The set $Hom_{\mathcal{C}}(X, X)$ is a singleton for any object X of $\mathcal{C}$;
2. If $Hom_{\mathcal{C}}(X, Y) \neq \emptyset$ and $Hom_{\mathcal{C}}(Y, X) \neq \emptyset$, then $X = Y$.

Theorem 3.32([1],[6])

(a) *A small category is a Möbius category if and only if all intervals of* $\mathcal{C}$ *are finite and one-way.*

(b) *If* $\mathcal{C}$ *is a Möbius category then any interval* $I\alpha$ *for* $\alpha \in Mor\mathcal{C}$ *is also a Möbius category such that*

$$\mu(\alpha) = \mu_{I\alpha}(\alpha),$$

where μ *is the Möbius function of* $\mathcal{C}$ *and* $\mu_{I\alpha}$ *is the Möbius function of* $I\alpha$*.*

Remarks

(1) The morphism α of $\mathcal{C}$ is also a morphism of $I\alpha$ from $\alpha 1_A$ to $1_B\alpha$ if $\alpha \in Hom_{\mathcal{C}}(A, B)$.

(2) If $I\alpha$ is a bounded poset (as a category) then $\mu(\alpha) = \mu_{I\alpha}(0, 1)$.

3.2.1 An Example

Let m be a positive integer, $\mathbb{Z}_m$ the cyclic group of addition modulo m, $\mathbb{Z}_-$ the set of non-positive integers, and $\mathbb{Z}_+$ the set of non-negative integers. Now, let C_m be the category defined by:

- $ObC_m = \mathbb{Z}_m \times \mathbb{Z}_-$

- $Hom_{C_m}((\bar{x}, i), (\bar{y}, j)) = \{(a, \bar{x}, i, j) \;:\; a \in \mathbb{Z}_+,\; a \le i - j,\; \bar{a} + \bar{x} = \bar{y}\}$
- $(b, \bar{y}, j, k) \circ (a, \bar{x}, i, j) = (a + b, \bar{x}, i, k)$ is the composition of two morphisms $(a, \bar{x}, i, j) : (\bar{x}, i) \to (\bar{y}, j)$ and $(b, \bar{y}, j, k) : (\bar{y}, j) \to (\bar{z}, k)$.

First we will show that this category is in fact a M$\ddot{o}$bius category. Let $(a, \bar{x}, i, j) : (\bar{x}, i) \to (\bar{y}, j)$ be a morphism in C_m. First, we examine the factorizations in C_m of this morphism, that is the objects of the category $I(a, \bar{x}, i, j)$. Let

$$(a, \bar{x}, i, j) = (a - b, \bar{z}, k, j) \circ (b, \bar{x}, i, k)$$

be a factorization of $(a, \bar{x}, i, j)$, i.e. diagram 1 is commutative.

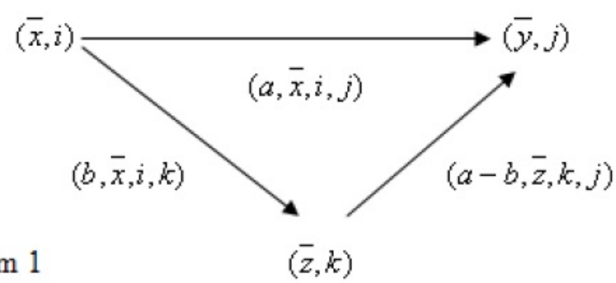

Diagram 1

We have:

$$a > 0,\; i, j \le 0,\; a \le i - j \text{ and } \bar{a} + \bar{x} = \bar{y} \; (\text{since } (a, \bar{x}, i, j) \in Hom_{C_m}((\bar{x}, i), (\bar{y}, j)))$$

and

$$0 \le b \le a,\; k \le 0,\; b \le i - k,\; a - b \le k - j,\; \bar{b} + \bar{x} = \bar{z} \; (\overline{a - b} + \bar{z} = \bar{y} \text{ is a consequence}).$$

Now, for a fixed integer b, $0 \le b \le a$,

- $\bar{z}$ is uniquely determined by: $\bar{z} = \bar{b} + \bar{x}$. We denote by $\overline{z_b}$ the residue class.

- The values of k are determined by the condition: $a - b + j \leq k \leq i - b$. Since,

$$i - b - (a - b + j) = i - j - a \geq 0,$$

it follows that the values of k are the following:

$$k_0 = a - b + j,\ k_1 = a - b + j + 1, \ldots, k_t = a - b + j + t, \ldots, k_{i-j-a} = i - b.$$

Thus

Proposition 3.33 [6] *The set of objects of $I(a, \bar{x}, i, j)$ is finite for any morphism $(a, \bar{x}, i, j)$ of C_m.*

With the above notations there exists a morphims of C_m from $(\overline{z_b}, k_t)$ to $(\overline{z_b}, k_p)$ such that the diagram 2 is commutative if and only if $k_p \leq k_t$ (that is, if and only if $p \leq t$), where $0 \leq p,\ t \leq i - j - a$. It is clear that this morphism $(0, \overline{z_b}, k_t, k_p)$ of C_m is uniquely determined by the commutative diagram 2.

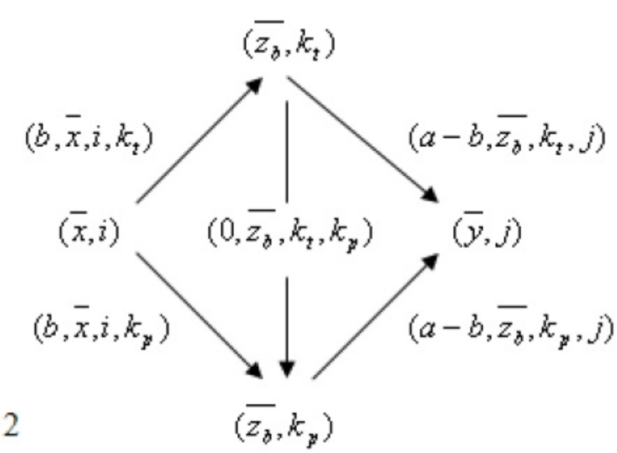

Diagram 2

Thus

Proposition 3.34 [6] *The set of morphisms* $Hom_{I(a,\bar{x},i,j)}(X_{b,t}, X_{b,p})$, *where*

$$X_{b,t} = (\bar{x}, i) \overset{(b,\bar{x},i,k_t)}{\rightarrow} (\overline{z_b}, k_t) \overset{(a-b,\overline{z_b},k_t,j)}{\rightarrow} (\bar{y}, j)$$

and

$$X_{b,p} = (\bar{x}, i) \overset{(b,\bar{x},i,k_p)}{\rightarrow} (\overline{z_b}, k_p) \overset{(a-b,\overline{z_b},k_p,j)}{\rightarrow} (\bar{y}, j)$$

is non-empty and it is a singleton if and only if $p \leq t$.

A similar examination of the commutativity in C_m of the diagram 3 leads us to conclude that (the notations are the same as in Proposition 3.34):

Proposition 3.35 [6] *The set of morphims* $Hom_{I(a,\bar{x},i,j)}(X_{b,t}, X_{b',p})$ *is non-empty and it is a singleton if and only if* $b \leq b'$ *and* $p \leq t$.

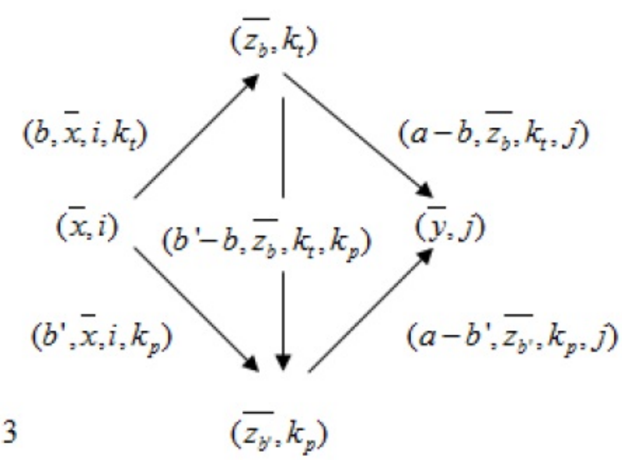

Diagram 3

By theorem 3.32 and the previous results, we obtain the following proposition.

Proposition 3.36 [6] *The category C_m is a Möbius category, and every interval of C_m is a finite lattice.*

The diagram 4 is the Hasse diagram of the finite lattice $I(a, \bar{x}, i, j)$. Now, a well known result of the theory of Möbius functions of posets,

$$\mu_P(0, 1) = c_0 - c_1 + c_2 - c_3 + \dots$$

where c_i is the number of chains $0 = x_0 < x_1 < x_2 < \dots < x_i = 1$ of length i between 0 and 1 ($c_0 = 0, c_1 = 1$), and the equalities $\mu(a, \bar{x}, i, j) = \mu_{I(a,\bar{x},i,j)}(a, \bar{x}, i, j) = \mu_{I(a,\bar{x},i,j)}(0, 1)$ implies:

Proposition 3.37 [6] *The Möbius function μ of the Möbius category C_m is given by:*

$$\mu(a, \bar{x}, i, j) = \begin{cases} 1 & \text{if } a = 0 \text{ and } j = i \quad \text{or} \quad a = 1 \text{ and } j = i - 2 \\ -1 & \text{if } a = 0 \text{ and } j = i - 1 \quad \text{or} \quad a = 1 \text{ and } j = i - 1 \\ 0 & \text{otherwise} \end{cases}$$

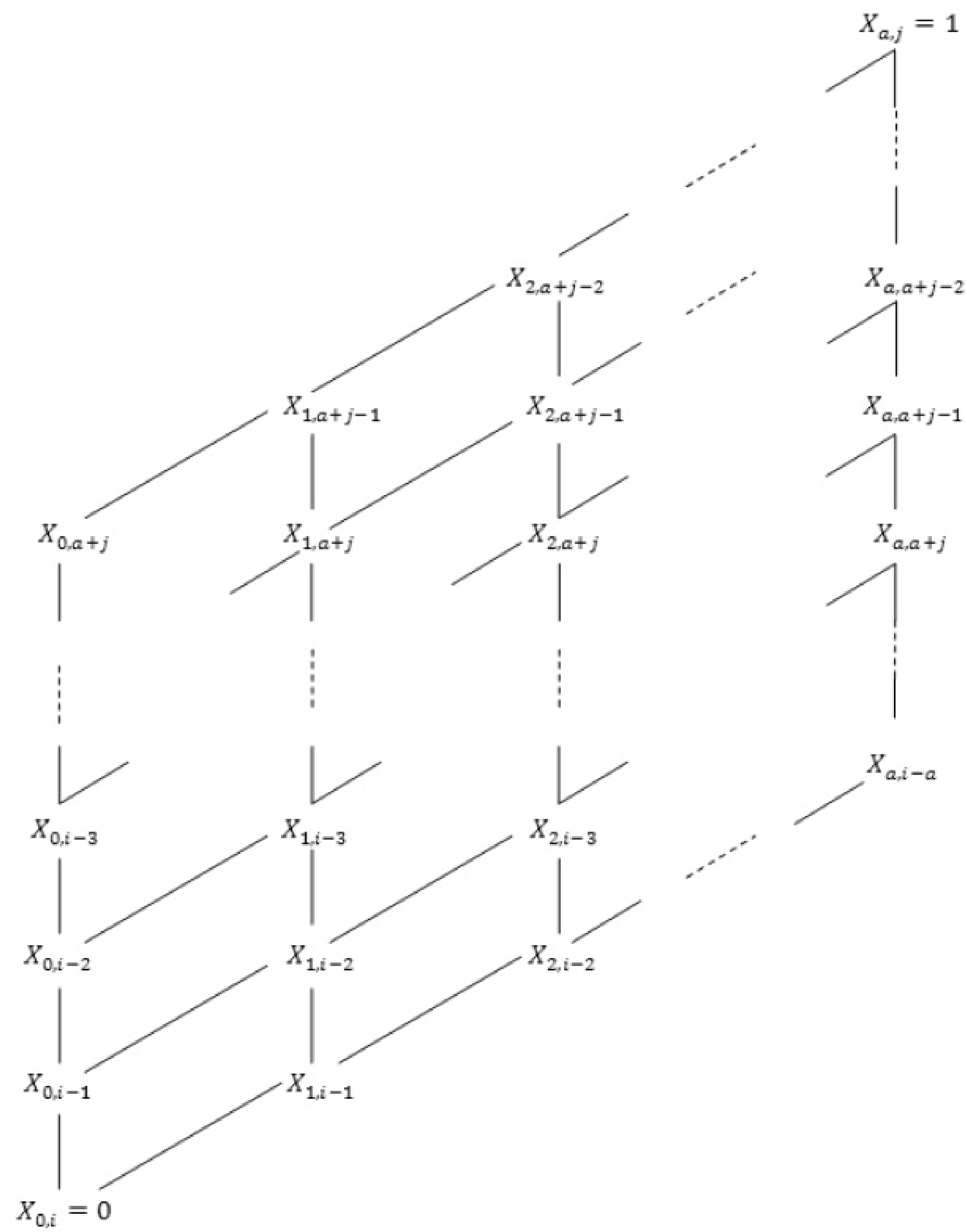

Diagram 4

(b=0) (b=1) (b=2) ----- (b=a)

References

[1] F.W.Lawvere, M.Menni, *The Hopf algebra of Mobius intervals*, Theory and Applications of Categories,Vol.24 No.10, 2010.

[2] B. Mitchell, *Theory of Categories*, New York, Academic Press, 1965.

[3] P. J. McCarthy, *Introduction to arithmetical functions*, Springer Verlag, 1986.

[4] E. D. Schwab, *Mobius Categories and Combinatorial Inverse Monoids*, Lecture Notes, UTEP, 2006.

[5] E. D. Schwab, L. Toth, *On some elementary number theoretic inequalities involving the Dirichlet convolution*' Sem. Arghiriade Nr. 24, Yniversity of Timisoara, 1990.

[6] E. D. Schwab, J. Villarreal, *The computation of the Mobius function of a Mobius category*, 2012-Hawaii University International Conference on Mathematics and Engineering Technology, Honolulu, [arXiv:1210.7697 - 29 Oct. 2012]

[7] H. Simmons, *An introduction to category theory*, Cambridge; New York, 2011.

Curriculum Vitae

Juan Carlos Villarreal was born on November 4, 1988 in El Paso, TX. The second child of Raul Villarreal and Patricia Manriquez. Grew up in Ciudad Juarez, Chihuahua, Mexico, completing his elementary and secondary education in this city. He graduated number three from his high school class from Preparatoria El Chamizal. He entered The University of Texas at El Paso in the fall of 2007.

In the fall of 2010 he earned his bachelor of science degree in mathematics with a minor in secondary education; he graduated with the highest honors. He entered in the Master of Science in Mathematics program from The University of Texas at El Paso in the spring of 2011. During his studies, he worked with the Mathematical Science Department as a Teaching Assistant while he was also working with the El Paso Independent School District as a mathematics tutor. He worked as a mathematics teacher at Andress High School in the fall of 2012, and he is he has been teaching matemathics at Transmountain Early College High School since the spring of 2013.

Permanent address: 11296 Duster Dr.
El Paso, Texas 79934
USA