

SELECTED ALGEBRAIC STRUCTURES OF  
NUMBER-THEORETIC FUNCTIONS

By

THOMAS RAY HAMEL

Bachelor of Science  
Fort Hays Kansas State College  
Hays, Kansas  
1961


Master of Arts  
Kansas State Teachers College  
Emporia, Kansas  
1967

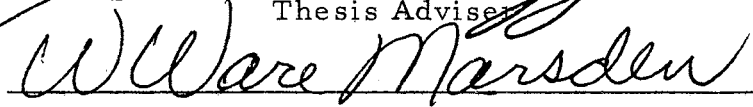
Submitted to the Faculty of the Graduate College  
of the Oklahoma State University  
in partial fulfillment of the requirements  
for the Degree of  
DOCTOR OF EDUCATION  
July, 1971

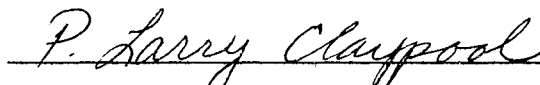
OKLAHOMA  
STATE UNIVERSITY  
LIBRARY  
DEC 31 1971


SELECTED ALGEBRAIC STRUCTURES OF  
NUMBER-THEORETIC FUNCTIONS

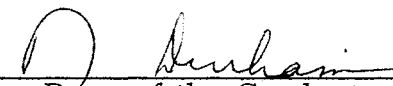
Thesis Approved:

  
\_\_\_\_\_  
Thesis Adviser

  
\_\_\_\_\_

  
\_\_\_\_\_

  
\_\_\_\_\_

  
\_\_\_\_\_  
Dean of the Graduate College

## ACKNOWLEDGEMENTS

I wish to express my appreciation to all those who assisted me in the preparation of this dissertation. Particularly, I would like to thank Dr. Gerald K. Goff for serving as my thesis advisor and for his continued interest in me and my work for the past two years. My thanks go to Dr. Jeanne L. Agnew for her guidance, encouragement, and suggestions which led to the selection of this thesis topic.

I also wish to thank Dr. Ware Marsden for serving as my committee chairman. For their suggestions and cooperation, my thanks go to Dr. P. Larry Claypool and Dr. Robert T. Alciatore.

My special thanks go to my wife, Nancy, and to our children, Daniel and Paul, who have had to sacrifice immensely through the years of study.

## TABLE OF CONTENTS

| Chapter  | Page |
|--|------|
| I. HISTORICAL SETTING AND PURPOSE . . . . .  | 1    |
| Algebraic Structure . . . . .  | 2    |
| Number-Theoretic Functions . . . . .   | 3    |
| Purpose . . . . .  | 8    |
| II. PRELIMINARY CONCEPTS . . . . .   | 9    |
| Abstract Algebra . . . . .   | 9    |
| Convolution Product of Arithmetic<br>Functions . . . . .   | 11   |
| The Möbius Inversion Function . . . . .  | 20   |
| Unitary Product of Arithmetic Functions . . . . .  | 25   |
| III. RINGS OF ARITHMETIC FUNCTIONS . . . . .   | 27   |
| Sum of Arithmetic Functions . . . . .  | 27   |
| Ordinary Product of Arithmetic Functions . . . . .   | 28   |
| Cauchy Product of Arithmetic Functions . . . . .   | 31   |
| Convolution Product of Arithmetic<br>Functions . . . . .   | 35   |
| Unitary Product of Arithmetic Functions . . . . .  | 37   |
| Pi Product of Arithmetic Functions . . . . .   | 38   |
| Delta Product of Arithmetic Functions . . . . .  | 40   |
| IV. OPERATORS ON ALGEBRAS OF ARITHMETIC<br>FUNCTIONS . . . . .   | 44   |
| The Logarithm Operator L . . . . .   | 47   |
| The Logarithm Operator L <sup>J</sup> . . . . .  | 60   |
| The Exponential Operator E . . . . .   | 64   |
| General Powers of Arithmetic Functions . . . . .   | 65   |
| Trigonometric Operators . . . . .  | 69   |
| Extension to Complex Algebras . . . . .  | 83   |
| V. CONVOLUTIONS WITH THE MÖBIUS FUNCTION . . . . .   | 90   |
| Formulas for $\mu_{\sigma}^k \varphi$ , $\mu_{\sigma}^k \sigma$ , and $\mu_{\sigma}^k \iota$ . . . . .           | 90   |
| Formulas for $\mu_{\sigma}^k \tau$ , $\mu_{\sigma}^k \varepsilon$ , $\mu_{\sigma}^k \nu$ , and $\mu^k$ . . . . . | 97   |

| Chapter                               | Page |
|---------------------------------------|------|
| VI. SUMMARY AND CONCLUSIONS . . . . . | 106  |
| Other Results . . . . .               | 108  |
| Ideas for Continued Study . . . . .   | 111  |
| BIBLIOGRAPHY . . . . .                | 113  |

LIST OF TABLES

| Table  | Page |
|--|------|
| I. A Portion of the Negative Pascal Triangle . . . . . | 103  |

## CHAPTER I

### HISTORICAL SETTING AND PURPOSE

The student of mathematics must continually attempt to find and identify patterns in the mathematics he encounters. Only through this assimilation process can he hope to gain a true understanding and full appreciation. Courant [5] describes mathematics as an expression of the human mind which reflects the active will, the contemplative reason, and the desire for aesthetic perfection. Courant also asserts that, without doubt, all mathematical development has its psychological roots in more or less practical requirements, but that once the pressure of practical applications has exerted itself mathematics outgrows its immediate needs. This trend from the applied to the theoretical has appeared ever since ancient history.

Eves [9] credits man's rapid progress in recent decades in the control and understanding of his environment to the mathematical developments of the last few centuries. In particular, the ability through mathematics to study, in a generalized form, order abstracted from the particular objects and phenomena which exhibit it. The modern postulational method in mathematics with the increasing trend to more generalization and abstraction can be traced directly to two sources of approximately simultaneous origin--the creation of non-Euclidean geometry by Lobachevsky and Bolyai and the discovery of abstract algebraic structure by British mathematicians [9]. This

statement justifies, in part at least, an investigation of the algebraic structure of any mathematical system under consideration. In this dissertation the algebraic structure of the number-theoretic functions will be considered. Chapter Five of Eves [9] gives an interesting historical development of the emergence of algebraic structure in modern mathematics. The following brief account borrows freely from that development.

### Algebraic Structure

The first of the British mathematicians to study seriously the fundamental principles of algebraic structure was George Peacock who in about 1830 made a distinction between what he called "arithmetical algebra" and "symbolical algebra." The former was taken to be the study which results from the use of symbols to denote ordinary positive decimal numbers along with the signs for the operations, like addition and subtraction, to which these numbers are subjected. In "arithmetical algebra" there can be restrictions on the operations. For example,  $a - b$  is possible only if  $a$  is greater than  $b$ . Peacock's "symbolized algebra" adopted the operations of "arithmetical algebra" but ignored the restrictions. Peacock's justification of this extension was called the principle of the permanence of equivalent forms. An example of Peacock's use of the principle of the permanence of equivalent forms was his assertion that the formula  $a^m a^n = a^{m+n}$ , which follows directly from the definition of  $a^m$  and  $a^n$  for positive integral values of  $m$  and  $n$ , will hold without any restrictions on the base  $a$  or on the exponents  $m$  and  $n$ . As a mathematical concept the principle of the permanence of equivalent forms is not used today although at one time



it was regarded as a powerful concept. It still serves as a guide to mathematicians in the formulation of new more general definitions in such a way that certain properties of the old definitions are preserved.

A British contemporary of Peacock, Duncan Farquharson Gregory, published a paper in 1840 which clearly brought out the commutative and distributive laws of algebra. Augustus DeMorgan published several articles in the 1840's that added to the work of the British algebraists. Soon the work of the British algebraists was taken up elsewhere. The Irish mathematician William Rowan Hamilton and the German mathematician Hermann Gunther Grassmann published results in 1853 and 1844, respectively, that are given as much credit for the liberation of algebra from traditional holds as the discovery of non-Euclidean geometry by Lobachevsky and Bolyai is credited for the liberation of geometry. Hamilton had his result as early as 1843 but did not publish it until ten years later. Hamilton and Grassmann independently invented algebraic systems in which the commutative law of multiplication did not hold. This was considered a very radical and unnatural undertaking. The English mathematician Arthur Cayley in 1857 discovered a noncommutative algebra different from those of Hamilton and Grassmann. Eves credits the German historian of mathematics, Hermann Hankel, with a very thorough development of the early algebraic concepts in an article published in 1867.

#### Number-Theoretic Functions

LeVegue [13] defines a number-theoretic function (arithmetic function) as any function whose domain of definition is the positive integers. As will be seen later, it is sometimes advantageous to

allow the domain of arithmetic functions to be the non-negative integers.

The definition of arithmetic function that will be used in this dissertation, unless otherwise indicated, is the definition given by Gioia [11].

Definition 1.1. An arithmetic function is a function whose domain is the positive integers and whose range is a subset of the set of complex numbers  $\mathbb{C}$ .

There are many arithmetic functions. Examples include  $f(n) = 1$ ,  $f(n) = n$ ,  $f(n) = n!$ ,  $f(n) = n^2$ , etc. The most interesting arithmetic functions are those whose value depends on the form of its argument, not just on the size of its argument. Some of these include  $\varphi(n)$ , Euler's  $\varphi$ -function;  $\tau(n)$ , the number of positive divisors of  $n$ ;  $\sigma(n)$ , the sum of the positive divisors of  $n$ ; and  $\mu(n)$ , the Mobius inversion function. Some of the properties of these and other arithmetic functions will be seen later in this paper.

An attempt to document the history and development of arithmetic functions leads to certain difficulties. Dickson [8], the most comprehensive history of the theory of numbers prior to 1919, and other references on the subject give historical accounts of the development of specific arithmetic functions but fail to give an overall history of arithmetic functions. The following account borrows freely from the work of Dickson [8],

Of the four arithmetic functions named above,  $\tau(n)$ , the number of divisors of  $n$ , was the first to be systematically investigated. Cordan in 1537 and Michael Stifel in 1544 were able to evaluate  $\tau(n)$

with  $n$  the product of  $k$  distinct primes. Mersenne in 1644 was able to solve equations of the form  $\tau(n) = 60$ . Frans van Schooten in 1657 extended the work of Mersenne. John Kersey in 1673 was the first to discover formula (1) below. John Wallis in 1685 and Pierre Rémond de Montmort in 1713 duplicated the results of Kersey.

Shockley [18] presents the formula

$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1), \quad (1)$$

where  $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ ;  $p_i$ ,  $i = 1, 2, \dots, k$  distinct primes.

E. Waring in 1770 proved that if  $\tau(n)$  is odd then  $n$  is a perfect square. E. Lionnet (1868), T. L. Pujó (1872), and Emil Hain (1873) were able to prove the converse of this result. A. P. Minn (1883) and G. Fontené (1902) obtained results concerning minimal solutions to equations of the type Mersenne first investigated.

Shockley [18] gives the formula

$$\sigma(n) = \prod_{i=1}^k \frac{p_i^{a_i+1} - 1}{p_i - 1}, \quad (2)$$

where  $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ ;  $p_i$ 's distinct primes for  $i = 1, 2, \dots, k$ , as the evaluation of the function  $\sigma$ .

Rene Descartes in 1638 developed a formula like (2) above with  $n$  being a power of a prime. Descartes was also aware of the multiplicative nature of  $\sigma$ . Finally, in 1658, John Wallis developed formula (2). E. Waring in 1782 supplied a proof of formula (2). In 1901, L. Kronecker derived formulas (1) and (2) using infinite series and products.

Euler's  $\varphi$ -function,  $\varphi(n)$ , is defined to be the number of positive integers not exceeding  $n$  which are relatively prime to  $n$ , with  $\varphi(1) = 1$ . Leonhard Euler in 1760 investigated  $\varphi(n)$  and derived the formula

$$\varphi(n) = p_1^{a_1-1} (p_1-1) p_2^{a_2-1} (p_2-1) \cdots p_k^{a_k-1} (p_k-1), \quad (3)$$

where  $n = p_1^{a_1} \cdots p_k^{a_k}$ ;  $p_i$ 's distinct primes for  $i = 1, 2, \dots, k$ .

Euler was also aware of the multiplicative nature of  $\varphi$ . Euler did this work without using the notation  $\varphi(n)$ . It was C. F. Gauss who introduced the symbol  $\varphi(n)$  in 1801. Gauss was also able to prove the important result

$$\sum_{d|n} \varphi(d) = n.$$

There are several expressions for  $\varphi(n)$  that are equivalent to (3). A. L. Crelle (1832) expressed  $\varphi(n)$  in the form

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right), \quad (4)$$

where  $n = p_1^{a_1} \cdots p_k^{a_k}$  as above. The Euler  $\varphi$ -function has been investigated very thoroughly. The above results and many other results have been obtained in many different ways by many different mathematicians since Euler initiated the investigation.

A. F. Mobius in 1832 defined the function  $\mu(n)$  as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1 \text{ and } n \text{ is divisible by a square,} \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k; p_i \text{'s distinct primes for } i = 1, 2, \dots, k. \end{cases}$$

Möbius used his function in the inversion of series. E. Meissel in 1850 found the frequently stated result

$$\sum_{m=1}^n \mu(m) \left[ \frac{n}{m} \right] = 1 .$$

Three men, R. Dedekind, J. Liouville, and B. Merry, in 1857 were able to prove that if

$$F(n) = \sum_{d|n} f(d)$$

then

$$f(n) = F(n) - \sum F\left(\frac{n}{a}\right) + \sum F\left(\frac{n}{ab}\right) - \sum F\left(\frac{n}{abc}\right) + \dots , \quad (5)$$

where each summation extends over all quotients where the factors of every denominator is a combination of the distinct prime factors of  $n$  taken the indicated number of times.

E. Laguerre in 1863 expressed (5) in the form

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F(d) . \quad (6)$$

It is interesting to note that the development in Shockley [18] proceeds by defining the functions  $\nu$  and  $\mu$  as follows:

$$\begin{aligned} \nu(n) &= 1 \text{ for each positive integer } n, \\ \mu &= \nu^{-1} \text{ with respect to convolution product.} \end{aligned}$$

Shockley is then able to show formula (6) valid as well as prove that  $\mu$  is evaluated exactly as Möbius defined it.

In 1874 F. Mertens was able to prove the familiar result that if  $n > 1$  then

$$\sum_{d|n} \mu(d) = 0 .$$

This is a brief account of the history of the development of the functions  $\tau$ ,  $\sigma$ ,  $\varphi$  and  $\mu$ .

### Purpose

The purpose of this dissertation is to investigate some of the algebraic structures that can be imposed on the number-theoretic functions and to prove that some of the systems obtained are isomorphic. Chapter III will investigate the algebraic structures using rather elementary methods. The isomorphisms used in Chapter IV are rather ingenuous and the methods considerably more elaborate and complicated.

Chapter V will investigate the effect of convoluting powers of the Mobius function with some of the well known arithmetic functions. Chapters III and V will provide the teacher of an undergraduate course in number theory with topics that can be used for enrichment material, special projects, or club meetings. Chapter IV could serve the same ends with the more capable students.

## CHAPTER II

### PRELIMINARY CONCEPTS

The material in this dissertation assumes as a prerequisite an abstract algebra course and a beginning course in number theory, both on the undergraduate level. This chapter contains, for review and for later reference, a listing of some of the definitions and theorems of these two areas of mathematics that will be frequently used in the later chapters. The theory of the convolution product of arithmetic functions is included in only a few of the number theory books in use now so most of the theorems and results of that section will be proven. The theory of unitary product parallels the theory of convolution product, as Gautier [10] shows, so her results will merely be summarized here.

#### Abstract Algebra

Definition 2.1. A nonempty set of elements  $G$  is a group if and only if in  $G$  there is defined a binary operation, denoted by  $\cdot$ , such that:

- (1)  $a, b \in G$  implies that  $a \cdot b \in G$  (closure).
- (2)  $a, b, c \in G$  implies that  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$   
(associative).
- (3) There exists an element  $e \in G$  such that  
 $a \cdot e = a = e \cdot a$  for all  $a \in G$  (identity).

- (4) For every  $a \in G$  there exists an element  $a^{-1} \in G$  such that  $a \cdot a^{-1} = a^{-1} \cdot a = e$  (inverses).

Recall that  $g \in G$  means  $g$  is an element of  $G$ . The notation  $(G, \cdot)$  will be used to denote the set  $G$  under the operation  $\cdot$ .

Definition 2.2. A group  $G$  is said to be abelian (commutative) if for every  $a, b \in G$ ,  $a \cdot b = b \cdot a$ .

It is common practice, when it can cause no confusion, to write  $ab$  instead of  $a \cdot b$ .

Definition 2.3. A groupoid is a set together with a closed binary operation.

Definition 2.4. A semi-group is an associative groupoid.

Definition 2.5. A monoid is a semi-group with identity.

Definition 2.6. A ring  $R$  is a nonempty set  $R$ , together with two binary operations  $\cdot$  and  $+$  such that for all  $a, b, c \in R$ :

- (1)  $a + b \in R$ .
- (2)  $a + b = b + a$ .
- (3)  $(a + b) + c = a + (b + c)$ .
- (4) There is  $0$  in  $R$  such that  $a + 0 = 0 + a = a$ .
- (5) There is  $-a$  in  $R$  such that  $a + (-a) = (-a) + a = 0$ .
- (6)  $a \cdot b \in R$ .
- (7)  $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ .
- (8)  $a \cdot (b + c) = a \cdot b + a \cdot c$  and  $(b + c) \cdot a = b \cdot a + c \cdot a$   
(distributive laws).



The notation  $(R, +, \cdot)$  will be used to denote the ring  $R$  under the operations  $+$  and  $\cdot$ .

Definition 2.7. A non-associative ring is a ring in which property (7) above fails.

Definition 2.8. A commutative ring is a ring in which, for every  $a, b \in R$ ,  $a \cdot b = b \cdot a$ .

Definition 2.9. A ring with identity is a ring in which, there exists a unique identity element with respect to the operation  $\cdot$ .

Definition 2.10. If  $R$  is a commutative ring then  $d \in R$ ,  $d \neq 0$ , is said to be a zero-divisor if and only if there exists a  $b \in R$ ,  $b \neq 0$ , such that  $d \cdot b = 0$ .

Definition 2.11. A commutative ring with identity is an integral domain if and only if it has no zero-divisors.

Definition 2.12. A ring is a division ring if and only if its non-zero elements form a group under  $\cdot$ .

Definition 2.13. A field is a commutative division ring.

### Convolution Product of Arithmetic Functions

In Chapter I an arithmetic function was defined to be any function mapping the positive integers into a subset of the complex field  $C$ . Let  $A$  represent the set of all arithmetic functions. The operation of convolution product, to be defined below, places an interesting structure upon the set of arithmetic functions. The investigation of this structure will constitute a major proportion of this dissertation.

Very few elementary number theory texts discuss the convolution product of arithmetic functions. Shockley [18] is an exception. Most of the development of this section is taken from the text by Shockley.

Definition 2.14. Let  $f$  and  $g$  be arithmetic functions. The function  $f \circ g$ , the convolution product of  $f$  and  $g$ , is defined by

$$(f \circ g)(n) = \sum_{d|n} f(d) g(n/d).$$

Since multiplication and addition are well defined closed operations in the field  $C$ ,  $f \circ g$  is a well defined arithmetic function whenever  $f$  and  $g$  are. Thus, convolution product is a closed binary operation on  $A$ . Several of the basic properties of convolution product will now be developed.

Theorem 2.1. Convolution product is commutative.

Proof: Let  $f, g \in A$  and  $n$  a positive integer. As  $d$  ranges over the divisors of  $n$  so does  $t = n/d$ . Thus

$$(f \circ g)(n) = \sum_{d|n} f(d) g(t) = \sum_{d|n} g(t) f(d) = \sum_{t|n} g(t) f(d) = (g \circ f)(n).$$

Since  $n$  is arbitrary,  $f \circ g = g \circ f$  and convolution product is commutative.

The following result will be used repeatedly without reference in the work to follow. Its proof is a straightforward manipulation of finite sums and is supplied in detail by Shockley [18; 104].

Theorem 2.2. Let  $f, g \in A$  and  $m$  and  $n$  be positive integers.

Then

$$\sum_{\substack{d|m \\ D|n}} f(d) g(D) = \sum_{d|m} f(d) \sum_{D|n} g(D) .$$

Theorem 2.3. Convolution product is associative.

Proof: Let  $f, g, h \in \mathbf{A}$  and  $n$  a positive integer. Consider

$$\begin{aligned} [(f \circ g) \circ h](n) &= \sum_{d|n} (f \circ g)(d) h(n/d) = \sum_{d|n} \left[ \sum_{s|d} f(s) g(d/s) \right] h(n/d) \\ &= \sum_{\substack{d|n \\ s|d}} f(s) g(d/s) h(n/d) = \sum_{st|n} f(s) g(t) h(n/(st)) \end{aligned} \quad (1)$$

where  $d = st$ . Also,

$$\begin{aligned} [f \circ (g \circ h)](n) &= \sum_{d|n} f(d) (g \circ h)(n/d) = \sum_{d|n} f(d) \sum_{m|n/d} g(m) h(n/(dm)) \\ &= \sum_{\substack{d|n \\ m|n/d}} f(d) g(m) h(n/(dm)) \\ &= \sum_{dm|n} f(d) g(m) h(n/(dm)) . \end{aligned} \quad (2)$$

Note that the results in (1) and (2) agree exactly if the substitutions  $d = s$  and  $m = t$  are made. Since  $n$  is arbitrary,  $(f \circ g) \circ h = f \circ (g \circ h)$  and convolution product is associative. The previous results shows  $(\mathbf{A}, \circ)$  to be at least a commutative semi-group.

A very important type of arithmetic function is the multiplicative function. The special property of multiplicative functions makes possible certain manipulations with multiplicative functions that are not valid in general.

Definition 2.15. The arithmetic function  $f$  is multiplicative if and only if  $f(mn) = f(m)f(n)$  whenever  $(m, n) = 1$ .

Let  $M$  represent the set of all multiplicative arithmetic functions. The following result is cited by Cashwell and Everett [4],

Theorem 2.4. Let  $f \in M$ . Then there is a positive integer  $n$  such that  $f(n) \neq 0$  if and only if  $f(1) = 1$ .

Proof: If  $f \in M$ , then  $f(n) = f(1 \cdot n) = f(1) \cdot f(n)$  for each positive integer  $n$ , since  $(n, 1) = 1$ . Suppose there is a positive integer  $n$  such that  $f(n) \neq 0$ . Dividing by  $f(n)$  gives  $f(1) = 1$ . To prove the converse let  $n = 1$ .

There are many results involving multiplicative functions that could be investigated but only those pertaining to convolution product are needed for this paper. The next few results investigate the properties of convolution product on the set  $M$ . The first result shows  $M$  to be closed under convolution product.

Theorem 2.5. If  $f, g \in M$  then  $f \circ g \in M$ .

Proof: Let  $m$  and  $n$  be positive integers such that  $(m, n) = 1$ . Let  $x$  and  $y$  be integers such that  $xm + yn = 1$ . If  $d$  is any divisor of  $mn$  then  $d = st$  where  $s|m$  and  $t|n$ . Since  $s|m$  and  $t|n$  it follows that  $m = ks$  and  $n = jt$ . Making the obvious substitutions above gives  $xks + yjt = 1$ . This in turn shows that  $(s, t) = 1$  as well as  $(k, j) = 1$ . But  $k = m/s$  and  $j = n/t$ , therefore  $(m/s, n/t) = 1$ . The remainder of the proof will follow using the fact that  $f$  and  $g$  are multiplicative.

Thus,

$$\begin{aligned}
(f \circ g)(mn) &= \sum_{d|mn} f(d)g(mn/d) = \sum_{\substack{s|m \\ t|n}} f(st)g\left(\frac{mn}{st}\right) \\
&= \sum_{\substack{s|m \\ t|n}} f(s)g(m/s)f(t)g(n/t) = \sum_{s|m} f(s)g(m/s) \sum_{t|n} f(t)g(n/t) \\
&= (f \circ g)(m)(f \circ g)(n) .
\end{aligned}$$

Therefore,  $f \circ g \in M$  since it is multiplicative.

So far it has been shown that  $(A, \circ)$  and  $(M, \circ)$  are commutative semi-groups. The system  $(A, \circ)$  also contains an identity and the system  $(M, \circ)$  is a commutative group. To obtain these results it is necessary to define the following function.

Definition 2.16. The arithmetic function  $\varepsilon$  is defined as follows:

$$\varepsilon(1) = 1, \quad \text{and} \quad \varepsilon(n) = 0 \quad \text{if} \quad n > 1 .$$

Theorem 2.6. The function  $\varepsilon$  is the identity for convolution product.

Proof: Let  $f \in A$  and  $n$  a positive integer. Then

$$(f \circ \varepsilon)(n) = \sum_{d|n} f(d)\varepsilon(n/d) = f(n)\varepsilon(1) = f(n) .$$

The theorem follows since convolution product in  $A$  is commutative.

The existence of an identity for convolution product leads to the existence of inverses with respect to convolution product. The definition is standard.

Definition 2.17. The arithmetic functions  $f$  and  $g$  are inverses of each other with respect to convolution product if and only if  $f \circ g = \varepsilon$ .

The usual notation of  $f^{-1}$  for the inverse of  $f$  will be used.

The next theorem is important in that it characterizes those elements of  $A$  for which an inverse with respect to convolution product exists. It is also extremely useful in that its proof exhibits a method for computing the inverse of a given function when it exists.

Theorem 2.7. The arithmetic function  $f$  has an inverse if and only if  $f(1) \neq 0$ .

Proof: Suppose by way of contradiction that  $f$  has an inverse  $f^{-1}$  and that  $f(1) = 0$ . Then  $1 = \varepsilon(1) = (f \circ f^{-1})(1) = f(1) f^{-1}(1) = 0 \cdot f^{-1}(1) = 0$  since  $f^{-1}(1)$  is an element of the field  $C$ . But  $1 \neq 0$ , therefore  $f(1) \neq 0$ .

To prove the converse suppose  $f(1) \neq 0$  and define the function  $g$  inductively by

$$g(1) = \frac{1}{f(1)}, \quad \text{and} \quad g(n) = -\frac{1}{f(1)} \cdot \sum_{\substack{d|n \\ d < n}} g(d) f(n/d) \quad \text{if } n > 1. \quad (3)$$

Since convolution product is commutative it suffices to show that

$(g \circ f)(n) = \varepsilon(n)$  for each positive integer  $n$ . If  $n = 1$ ,

$(g \circ f)(1) = g(1) f(1) = 1 = \varepsilon(1)$ . If  $n > 1$ , then

$$\begin{aligned} (g \circ f)(n) &= \sum_{d|n} g(d) f(n/d) = \sum_{\substack{d|n \\ d < n}} g(d) f(n/d) + g(n) f(1) \\ &= \sum_{\substack{d|n \\ d < n}} g(d) f(n/d) + \left\{ -\frac{1}{f(1)} \cdot \sum_{\substack{d|n \\ d < n}} g(d) f(n/d) \right\} f(1) = 0 = \varepsilon(n). \end{aligned}$$

Thus  $g$  is the inverse of  $f$  and is so indicated by writing  $g = f^{-1}$ .

The equations given in (3) above define in a recursive fashion the inverse of any arithmetic function  $f$  for which  $f(1) \neq 0$ . Let  $B = \{f \in A \mid f(1) \neq 0\}$ . The previous results show that  $(B, \circ)$  is a commutative group. Davison [7] gives this result by saying that  $(B, \circ)$  is the group of units of  $(A, \circ)$ , where  $f \in A$  is a unit if and only if  $f^{-1}$  exists. All that remains to verify that  $(M, \circ)$  is a commutative group, is to show that the inverse of a multiplicative arithmetic function is multiplicative. That is precisely the content of the following theorem.

Theorem 2.8. If  $f \in M$ ,  $f$  not identically zero, then  $f^{-1}$  exists and  $f^{-1} \in M$ .

Proof: Since  $f \in M$  is not identically zero Theorem 2.4 implies that  $f(1) = 1$ . Thus, by Theorem 2.7,  $f^{-1}$  exists and is given by  $f^{-1}(1) = 1$  and

$$f^{-1}(n) = - \sum_{\substack{d \mid n \\ d < n}} f^{-1}(d) f(n/d) \quad \text{if } n > 1.$$

Now to show that  $f^{-1}$  is multiplicative. Proceeding by way of contradiction suppose that there exist positive integers  $a$  and  $b$  with  $(a, b) = 1$  such that  $f^{-1}(ab) \neq f^{-1}(a)f^{-1}(b)$ . Let  $H = \{ab \mid a, b \in \text{positive integers}, (a, b) = 1, \text{ and } f^{-1}(ab) \neq f^{-1}(a)f^{-1}(b)\}$ . By assumption  $H \neq \emptyset$ , thus the well-ordering principle implies that  $H$  contains a smallest element  $mn$ . Thus if  $c$  and  $d$  are relatively prime positive integers such that  $cd < mn$  then  $f^{-1}(cd) = f^{-1}(c)f^{-1}(d)$ . Note that neither of  $m$  nor  $n$  is equal to one for if  $m = 1$  then  $f^{-1}(mn) = f^{-1}(n) = 1 \cdot f^{-1}(n) = f^{-1}(m)f^{-1}(n)$ . But this is a contradiction to the well-ordering principle. A similar statement obviously holds if  $n = 1$ . Thus  $1 < m$  and  $1 < n$ .

Consider the quantity  $f^{-1}(m)f^{-1}(n) - f^{-1}(mn)$ . From (3) in the proof of Theorem 2.7,

$$f^{-1}(m)f^{-1}(n) - f^{-1}(mn) = f^{-1}(m)f^{-1}(n) + \sum_{\substack{d|mn \\ d < mn}} f^{-1}(d) f(mn/d).$$

As in the proof of Theorem 2.5 if  $d|mn$  then  $d = st$  where  $s|m$ ,  $t|n$ ,  $(s, t) = 1$ , and  $(m/s, n/t) = 1$ . Since  $d = st < mn$ ,  $f^{-1}(st) = f^{-1}(s)f^{-1}(t)$ .

Thus

$$\begin{aligned} f^{-1}(m)f^{-1}(n) - f^{-1}(mn) &= f^{-1}(m)f^{-1}(n) + \sum_{\substack{s|m \\ t|n \\ st < mn}} f^{-1}(st) f((mn)/(st)) \\ &= f^{-1}(m)f^{-1}(n) + \sum_{\substack{s|m \\ t|n \\ st < mn}} f^{-1}(s) f^{-1}(t) f(m/s) f(n/t). \end{aligned}$$

But  $f(1) = 1$ , thus

$$\begin{aligned} f^{-1}(m)f^{-1}(n) - f^{-1}(mn) &= f^{-1}(m)f(1)f^{-1}(n)f(1) + \sum_{\substack{s|m \\ t|n \\ st < mn}} f^{-1}(s) f(m/s) f^{-1}(t) f(n/t) \\ &= \sum_{\substack{s|m \\ t|n}} f^{-1}(s) f(m/s) f^{-1}(t) f(n/t) \\ &= \sum_{s|m} f^{-1}(s) f(m/s) \sum_{t|n} f^{-1}(t) f(n/t) \\ &= (f^{-1} \circ f)(m) (f^{-1} \circ f)(n) = \epsilon(m) \cdot \epsilon(n) = 0. \end{aligned}$$

The last equality follows since neither of  $m$  nor  $n$  is equal to one.



Thus  $f^{-1}(mn) = f^{-1}(m)f^{-1}(n)$ , which contradicts the choice of  $m$  and  $n$ , that is, the well-ordering principle. Therefore  $H = \varnothing$  and  $f^{-1} \in M$ . This completes the proof of the theorem.

The next theorem records several of the usual group theory type results.

- Theorem 2.9.
- (i) The identity  $\varepsilon$  is unique.
  - (ii) Let  $f \in B$ . Then  $f^{-1}$  is unique.
  - (iii)  $\varepsilon^{-1} = \varepsilon$ .
  - (iv) If  $f \in B$  then  $(f^{-1})^{-1} = f$ .
  - (v) If  $f, g \in B$  then  $(f \circ g)^{-1} = f^{-1} \circ g^{-1}$ .

Proof: (i) Suppose  $h$  is another identity with respect to convolution product. Then  $h = h \circ \varepsilon$  since  $\varepsilon$  is an identity. But  $h \circ \varepsilon = \varepsilon$  since  $h$  is an identity. Therefore  $h = \varepsilon$ .

(ii) Let  $f \in B$  and suppose  $f^{-1}$  and  $g$  are both inverses for  $f$ . Then  $f \circ f^{-1} = \varepsilon$  and  $f \circ g = \varepsilon$  which implies  $f \circ f^{-1} = f \circ g$ . Convoluting on the left on both sides with  $f^{-1}$  gives  $\varepsilon \circ f^{-1} = \varepsilon \circ g$ , that is  $f^{-1} = g$  and the inverse under convolution product is unique.

(iii) Note that  $\varepsilon = \varepsilon \circ \varepsilon^{-1}$  since  $\varepsilon$  and  $\varepsilon^{-1}$  are inverses. Also,  $\varepsilon \circ \varepsilon^{-1} = \varepsilon^{-1}$  since  $\varepsilon$  is an identity. Therefore  $\varepsilon = \varepsilon^{-1}$ .

(iv) The proof of this part follows from the chain of equalities  $(f^{-1})^{-1} = (f^{-1})^{-1} \circ \varepsilon = (f^{-1})^{-1} \circ (f^{-1} \circ f) = ((f^{-1})^{-1} \circ f^{-1}) \circ f = \varepsilon \circ f = f$ .

(v) If  $f, g \in B$  then  $f(1) \neq 0$  and  $g(1) \neq 0$ . Thus  $(f \circ g)(1) \neq 0$  and by Theorem 2.7  $(f \circ g)^{-1}$  exists. The proof follows since  $\varepsilon = \varepsilon \circ \varepsilon = (f \circ f^{-1}) \circ (g \circ g^{-1}) = f \circ (f^{-1} \circ g) \circ g^{-1} = f \circ (g \circ f^{-1}) \circ g^{-1} = (f \circ g) \circ (f^{-1} \circ g^{-1})$  implies that  $(f \circ g)^{-1} = f^{-1} \circ g^{-1}$ .

## The Möbius Inversion Function

A. F. Möbius in 1832 defined the Möbius function  $\mu(n)$  as follows:

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1 \text{ and } n \text{ is divisible by a square,} \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k; p_i \text{'s distinct primes for } i = 1, 2, \dots, k. \end{cases}$$

Möbius used his function in the inversion of series, that is, given that  $f$  and  $g$  are arithmetic functions related by the formula

$$f(n) = \sum_{d|n} g(d) \quad (4)$$

for each positive integer  $n$ , Möbius was able to invert this series expressing  $g$  as a function of  $f$ . His result, commonly called the Möbius inversion formula, is

$$g(n) = \sum_{d|n} f(d) \mu(n/d) \quad (\text{or } \sum_{d|n} \mu(d) f(n/d)) \quad (5)$$

for each positive integer  $n$ . Niven-Zuckerman [15] gives a thorough development of the Möbius function using this approach to the development of its properties. The development in this dissertation will follow the development of Shockley [18]. With this approach several of the key results of convolution product developed in the last section will be put to good use. The development begins by defining several important arithmetic functions.

Definition 2.18. The functions  $\nu$ ,  $\iota$ , and  $\mu$  are defined as follows:

$$\begin{aligned} \nu(n) &= 1 \text{ for each positive integer } n, \\ i(n) &= n \text{ for each positive integer } n, \\ \mu &= \nu^{-1} \text{ (with respect to convolution product)}. \end{aligned}$$

The equation in (4) above can now be expressed by

$$f(n) = \sum_{d|n} g(d) = \sum_{d|n} g(d) \nu(n/d) = (g \circ \nu)(n)$$

for each positive integer  $n$ . Thus  $f = g \circ \nu$ .

Convoluting on both sides by  $\nu^{-1} = \mu$  gives  $g = f \circ \mu$ . Thus

$$g(n) = \sum_{d|n} f(d) \mu(n/d)$$

for each positive integer  $n$ . But this is the Möbius inversion formula given in (5) above if it can be shown that the function  $\mu$  as defined in Definition 2.18 above is indeed the Möbius function. The following theorem will provide this result.

Theorem 2.10. The value of the function  $\mu$  as defined in Definition 2.18 is identical with the Möbius function.

Proof: From equation (3) of Theorem 2.7 it follows that

$\mu(1) = 1/\nu(1) = 1$ . Since the function  $\nu$  is multiplicative, Theorem 2.8 implies that  $\mu$ , the inverse of  $\nu$ , is also multiplicative. If  $p$  is a prime, equation (3) shows that

$$\mu(p) = - \sum_{\substack{d|p \\ d < p}} \mu(d) \nu\left(\frac{p}{d}\right) = -\mu(1) \nu(p) = -1.$$

If  $n = p_1 p_2 \cdots p_k$ ,  $p_i$  distinct primes, the multiplicative nature of  $\mu$  gives

$$\mu(n) = \mu(p_1) \mu(p_2) \cdots \mu(p_k) = (-1)^k$$

If  $n$  is divisible by a square then necessarily there is a prime  $p$  such that  $p^m | n$ ,  $p^{m+1} \nmid n$ , and  $m \geq 2$ . Thus  $n = p^m \cdot s$  where  $(p^m, s) = 1$ . Since  $\mu$  is multiplicative it follows that  $\mu(n) = \mu(p^m) \mu(s)$ . It suffices to show that  $\mu(p^m) = 0$  if  $m \geq 2$ . Using equation (3) again

$$\mu(p^2) = -\{\mu(1) \nu(p^2) + \mu(p) \nu(p)\} = -\{1 - 1\} = 0,$$

and

$$\mu(p^3) = -\{\mu(1) \nu(p^3) + \mu(p) \nu(p^2) + \mu(p^2) \nu(p)\} = -\{1 - 1 + 0\} = 0.$$

Proceeding by induction suppose that for  $2 \leq t < m$  it is true that  $\mu(p^t) = 0$ . Then

$$\begin{aligned} \mu(p^m) &= - \sum_{\substack{d | p^m \\ d < p^m}} \mu(d) \nu(p^m/d) \\ &= -\{\mu(1) \nu(p^m) + \mu(p) \nu(p^{m-1}) + \mu(p^2) \nu(p^{m-2}) + \dots + \mu(p^{m-1}) \nu(p)\} \\ &= -\{1 - 1 + 0 + 0 + \dots + 0\} = 0. \end{aligned}$$

This completes the proof of the theorem.

Chapter V will investigate some interesting results obtained by convoluting powers of the Möbius function with several of the well known number-theoretic functions. To facilitate the work in Chapter V some preliminary results will be developed here. The functions:  $\varphi(n)$ , Euler's  $\varphi$ -function;  $\tau(n)$ , the number of positive divisors of  $n$ ; and  $\sigma(n)$ , the sum of the positive divisors of  $n$ , are studied extensively in most any elementary number theory course. Their definitions and

evaluations are reviewed in the following definition and theorem.

Definition 2.19.

(a) If  $n$  is a positive integer then  $\varphi(n)$  is the number of positive integers less than or equal to  $n$  that are relatively prime to  $n$ .

(b) If  $n$  is a positive integer then  $\tau(n) = \sum_{d|n} 1$ .

(c) If  $n$  is a positive integer then  $\sigma(n) = \sum_{d|n} d$ .

Theorem 2.11.  $\varphi(1) = \tau(1) = \sigma(1) = 1$ . If  $n = \prod_{i=1}^k p_i^{s_i}$ , where the  $p_i$ 's are distinct primes, then

$$(a) \quad \varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right),$$

$$(b) \quad \tau(n) = \prod_{i=1}^k (s_i + 1),$$

$$(c) \quad \sigma(n) = \prod_{i=1}^k \frac{p_i^{s_i+1} - 1}{p_i - 1}.$$

It is well known that the functions  $\varphi$ ,  $\tau$ , and  $\sigma$  are multiplicative. Another result from elementary number theory that will be useful is the following theorem.

Theorem 2.12. If  $n$  is a positive integer then  $\sum_{d|n} \varphi(d) = n$ .

Other needed results are contained in the following theorems.

Theorem 2.13. The following relationships are valid:

$$(a) \quad \mu \circ \nu = \varepsilon, \quad (b) \quad \nu \circ \nu = \tau, \quad \text{and} \quad (c) \quad \iota \circ \nu = \sigma.$$

Proof: (a) The result is immediate since  $\nu^{-1} \circ \nu = \varepsilon$  and  $\mu = \nu^{-1}$ .

(b) By definition, for each positive integer  $n$ ,

$$\tau(n) = \sum_{d|n} 1 = \sum_{d|n} 1 \cdot 1 = \sum_{d|n} \nu(d) \nu(n/d) = (\nu \circ \nu)(n).$$

Therefore  $\tau = \nu \circ \nu$ .

(c) By definition, for each positive integer  $n$ ,

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} d \cdot 1 = \sum_{d|n} \iota(d) \nu(n/d) = (\iota \circ \nu)(n).$$

Therefore  $\sigma = \iota \circ \nu$ .

Theorem 2.14. (a) If  $n > 1$  then  $\sum_{d|n} \mu(d) = 0$ ,

$$(b) \varphi(n) = \sum_{d|n} d \mu(n/d).$$

$$(c) \sigma = \varphi \circ \tau.$$

Proof: (a)  $\sum_{d|n} \mu(d) = \sum_{d|n} \mu(d) \cdot 1 = \sum_{d|n} \mu(d) \nu(n/d) = (\mu \circ \nu)(n)$   
 $= \varepsilon(n) = 0$  if  $n > 1$ .

$$(b) \text{ Since } \iota(n) = n = \sum_{d|n} \varphi(d) = \sum_{d|n} \varphi(d) \cdot 1 = \sum_{d|n} \varphi(d) \nu(n/d)$$

for  $n$  a positive integer it follows that  $\iota = \varphi \circ \nu$ . Thus

$$\varphi = \iota \circ \nu^{-1} = \iota \circ \mu. \text{ Hence}$$

$$\varphi(n) = \sum_{d|n} \iota(d) \mu(n/d) = \sum_{d|n} d \mu(n/d).$$

(c) From the proof of (b),  $\varphi = \iota \circ \mu$ . From Theorem 2.13

$\tau = \nu \circ \nu$  and  $\sigma = \iota \circ \nu$ . Thus

$$\varphi \circ \tau = (\iota \circ \mu) \circ (\nu \circ \nu) = \iota \circ \varepsilon \circ \nu = \iota \circ \nu = \sigma.$$

Therefore  $\sigma = \varphi \circ \tau$ .

Other special properties of convolution product and of the Möbius function will be developed as they are needed.

### Unitary Product of Arithmetic Functions

The convolution product of two arithmetic functions is defined in terms of a summation over all of the positive divisors of a given positive integer. Thus if  $n$  is a positive integer the summation is taken over all  $d$ , and consequently  $n/d$ , such that  $d$  divides  $n$ . The unitary product of two arithmetic functions differs from their convolution product in that the summation is taken over only those divisors  $d$  of  $n$  for which  $d$  and  $n/d$  are relatively prime. These divisors are called unitary divisors of  $n$ . The theory of the unitary product of arithmetic functions is very similar to that of convolution product. Gautier [10] in a masters report investigates the properties of unitary divisors and the unitary product of arithmetic functions. Several of Gautier's key results will be stated now for future reference.

Definition 2.20. The positive integer  $d$  is a unitary divisor of a positive integer  $n$ , written  $d \parallel n$ , if and only if  $d$  is a divisor of  $n$  and  $(d, n/d) = 1$ .

Definition 2.21. Let  $f$  and  $g$  be arithmetic functions. The function  $f \# g$ , the unitary product of  $f$  and  $g$ , is defined by

$$(f \# g)(n) = \sum_{d \parallel n} f(d) g(n/d).$$

Theorem 2.15. Unitary product is commutative.

Theorem 2.16. Unitary product is associative.

Definition 2.22. Define the arithmetic function  $I(n)$  by  
 $I(n) = 1$  if  $n = 1$ , and  $I(n) = 0$  if  $n > 1$ .

Theorem 2.17.  $I$  is the identity for unitary product.

Definition 2.23. The arithmetic functions  $f$  and  $g$  are inverses of each other with respect to unitary product if and only if  $f \# g = I$ .  
 The notation  $f^{-1}$  is used to denote the inverse of  $f$ .

Theorem 2.18. If  $f$  is an arithmetic function such that  $f^{-1}$  exists, then it is unique.

Theorem 2.19. The arithmetic function  $f$  has an inverse if and only if  $f(1) \neq 0$ .

Theorem 2.20. If  $f$  and  $g$  are multiplicative functions, then so is  $f \# g$ .

Theorem 2.21.  $(B, \#)$  is a commutative group.

Theorem 2.22. If  $f \in M$ ,  $f$  not identically zero, then  $f^{-1}$  exists and  $f^{-1} \in M$ .

Theorem 2.23.  $(M, \#)$  is a subgroup of  $(B, \#)$ .



## CHAPTER III

### RINGS OF ARITHMETIC FUNCTIONS

The purpose of this chapter is to consider several of the many operations that can be defined on the set of arithmetic functions and to investigate the resulting algebraic structures.

#### Sum of Arithmetic Functions

The first operation to be considered on the set of arithmetic functions is that of sum.

Definition 3.1. Let  $f$  and  $g$  be arithmetic functions. The function  $f \oplus g$ , the sum of  $f$  and  $g$ , is defined by

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

Recall that an arithmetic function maps the positive integers (or non-negative integers) into a subset of the complex field  $C$ . Addition is well-defined and closed in the field  $C$  making  $f \oplus g$  a well-defined arithmetic function. A key result is the following theorem.

Theorem 3.1. The set  $A$  of all arithmetic functions is a commutative group under sum.

**Proof:** Certainly  $A$  is a nonempty set of elements and by the comment before the statement of Theorem 3.1  $\oplus$  is a closed binary operation. That  $\oplus$  is commutative and associative follows directly from the

commutativity and associativity of addition in the field  $C$ . The function  $\theta$  defined by  $\theta(n) = 0$  for each positive integer  $n$  is clearly the identity for  $\oplus$  since  $\oplus$  is commutative and for  $f \in A$  and  $n$  a positive integer,

$$(f \oplus \theta)(n) = f(n) + \theta(n) = f(n) + 0 = f(n).$$

The inverse of a function  $f$  is the function  $g$  given by  $g(n) = -f(n)$  for  $n$  a positive integer since  $\oplus$  is commutative and

$$(f \oplus g)(n) = f(n) + g(n) = f(n) - f(n) = 0 = \theta(n).$$

This completes the proof that  $(A, \oplus)$  is a commutative group. This result will be used several times in the remainder of this chapter.

### Ordinary Product of Arithmetic Functions

The ordinary product of two arithmetic functions is defined exactly as the words would seem to imply.

Definition 3.2. Let  $f$  and  $g$  be arithmetic functions. The function  $f * g$ , the ordinary product of  $f$  and  $g$ , is defined by

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

Theorem 3.2. The ordinary product of arithmetic functions is a well-defined closed binary operation that is commutative, associative, and for which there exists an identity which is unique. That is,  $(A, *)$  is a commutative monoid.

Proof: That the ordinary product of arithmetic functions is well-defined, closed, commutative, and associative follows directly from the

definition of the ordinary product of two functions and the fact that multiplication in a field has these properties. The function  $\nu$  defined by  $\nu(n) = 1$  for each positive integer  $n$  is an identity for  $A$  under  $*$  since  $*$  is commutative and  $(f * \nu)(n) = f(n) \nu(n) = f(n) \cdot 1 = f(n)$  for each  $f \in A$  and for each positive integer  $n$ .

To show  $\nu$  is unique suppose  $\nu_1 \neq \nu$  is another identity with respect to  $*$ . Then there is a positive integer  $m$  for which  $\nu_1(m) \neq 1 = \nu(m)$ . Let  $g$  be any arithmetic function such that  $g(m) \neq 0$ . Then  $g(m) \neq \nu_1(m) g(m) = (\nu_1 * g)(m)$ . But this contradicts the assumption that  $\nu_1$  is an identity with respect to  $*$ . Therefore,  $\nu$  is a unique identity for  $A$  under  $*$  and the theorem is proven.

Carlitz in [2] and [3] asserts that the algebraic system based upon the ordinary product and the sum of arithmetic functions is a commutative ring that has zero divisors. A slightly stronger result will be proven.

Theorem 3.3.  $(A, \oplus, *)$  is a commutative ring with unity that has zero divisors.

Proof: Using the results of Theorems 3.1 and 3.2 it is sufficient to show that ordinary product distributes over sum and to exhibit a zero divisor with respect to  $*$ .

Let  $f$ ,  $g$ , and  $h$  be arithmetic functions and  $n$  a positive integer. The definitions of  $*$  and of  $\oplus$  and the distributive property of multiplication over addition in a field give the following string of equalities:

$$\begin{aligned}
 [f * (g \oplus h)](n) &= f(n) [(g \oplus h)(n)] = f(n) [g(n) + h(n)] = f(n)g(n) + f(n)h(n) \\
 &= (f * g)(n) + (f * h)(n) = [(f * g) \oplus (f * h)](n) .
 \end{aligned}$$

This shows ordinary product to distribute over sum. Thus  $(A, \oplus, *)$  is a commutative ring with unity.

To see that  $(A, \oplus, *)$  has zero divisors consider the following two functions:

$$f(n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 0 & \text{if } n \text{ is even} \end{cases} ; \quad g(n) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 1 & \text{if } n \text{ is even} \end{cases} .$$

Let  $n$  be any positive integer. Then  $(f * g)(n) = f(n)g(n) = 0$  since one of  $f(n)$  or  $g(n)$  is zero. Thus  $f * g = \theta$  (the zero function) but neither of  $f$  or  $g$  is the zero function. Therefore,  $(A, \oplus, *)$  has zero divisors. Hence  $(A, \oplus, *)$  is a commutative ring with unity but not an integral domain.

Theorem 3.4.  $(A, \oplus, *)$  is not a division ring.

Proof: It suffices to show there exists a non-zero arithmetic function  $f$  that has no inverse with respect to  $*$ . Let  $f$  be defined by

$$f(n) = \begin{cases} 0 & \text{if } n = 5 \\ 1 & \text{if } n \neq 5 \end{cases} .$$

Certainly  $f$  is a non-zero function. It was shown above that the function  $\nu(n) = 1$ ,  $n$  a positive integer, is the identity with respect to  $*$ . By way of contradiction suppose there is a  $g \in A$  such that  $f * g = \nu$ . Then in particular

$$(f * g)(5) = f(5)g(5) = 0 \cdot g(5) = 0$$

and

$$(f * g)(5) = \nu(1) = 1.$$

But this is an obvious contradiction. Thus,  $(A, \oplus, *)$  is not a division ring.

Theorems 3.3 and 3.4 prove the following theorem.

Theorem 3.5.  $(A, \oplus, *)$  is at most a commutative ring with unity.

### Cauchy Product of Arithmetic Functions

In the definition of the Cauchy product of arithmetic functions the domain of the arithmetic functions is taken to be the non-negative integers. Note that the definition of the sum of two arithmetic functions and the statement of Theorem 3.1 remain meaningful and valid if the domain of the arithmetic functions is taken to be the non-negative integers.

Definition 3.3. Let  $f$  and  $g$  be arithmetic functions. The function  $f \& g$ , the Cauchy product of  $f$  and  $g$ , is defined by

$$(f \& g)(n) = \sum_{r=0}^n f(r) g(n-r).$$

Closure of addition and multiplication in the field  $C$  make  $\&$  a well-defined operation.

Carlitz [2] indicates the following result.

Theorem 3.6.  $(A, \oplus, \&)$  is an integral domain.

Proof: From the results of Theorem 3.1 and the statement preceding Theorem 3.6, it suffices to show that the Cauchy product is commutative, and associative, distributes over sum, has a unique multiplicative identity, and has no zero divisors.

Cauchy product is commutative since, for  $n$  a non-negative integer and  $f$  and  $g$  arithmetic functions, the field properties of  $\mathbb{C}$  and the definition of Cauchy product imply:

$$\begin{aligned} (f \& g)(n) &= \sum_{r=0}^n f(r) g(n-r) \\ &= f(0)g(n) + f(1)g(n-1) + \dots + f(n-1)g(1) + f(n)g(0) \\ &= g(0)f(n) + g(1)f(n-1) + \dots + g(n-1)f(1) + g(n)f(0) \\ &= \sum_{r=0}^n g(r)f(n-r) = (g \& f)(n). \end{aligned}$$

The associativity of Cauchy product is slightly more difficult but just as mechanical. For  $n$  a non-negative integer and  $f$ ,  $g$ , and  $h$  arithmetic functions:

$$\begin{aligned} [(f \& g) \& h](n) &= \sum_{r=0}^n (f \& g)(r) h(n-r) = \sum_{r=0}^n \left[ \sum_{j=0}^r f(j) g(r-j) \right] h(n-r) \\ &= f(0)g(0)h(n) + \\ &\quad f(0)g(1)h(n-1) + f(1)g(0)h(n-1) + \\ &\quad f(0)g(2)h(n-2) + f(1)g(1)h(n-2) + f(2)g(0)h(n-2) + \\ &\quad \quad \quad \vdots \\ &\quad \quad \quad \vdots \\ &\quad f(0)g(n-1)h(1) + f(1)g(n-2)h(1) + \dots + f(n-1)g(0)h(1) + \\ &\quad f(0)g(n)h(0) + f(1)g(n-1)h(0) + \dots + f(n-1)g(1)h(0) + f(n)g(0)h(0). \end{aligned}$$

Adding the above array by columns gives

$$\begin{aligned}
f(0) \left[ \sum_{j=0}^n g(j) h(n-j) \right] &+ f(1) \left[ \sum_{j=0}^{n-1} g(j) h(n-1-j) \right] + \dots + f(n-1) \left[ \sum_{j=0}^1 g(j) h(1-j) \right] \\
&+ f(n) g(0) h(0) \\
&= \sum_{r=0}^n f(r) \sum_{j=0}^{n-r} g(j) h(n-r-j) = \sum_{r=0}^n f(r) (g \& h)(n-r) \\
&= [f \& (g \& h)](n) .
\end{aligned}$$

The distributive property results from the following manipulation.

$$\begin{aligned}
[f \& (g \oplus h)](n) &= \sum_{r=0}^n f(r) (g \oplus h)(n-r) = \sum_{r=0}^n f(r) [g(n-r) + h(n-r)] \\
&= \sum_{r=0}^n [f(r) g(n-r) + f(r) h(n-r)] = \sum_{r=0}^n f(r) g(n-r) + \sum_{r=0}^n f(r) h(n-r) \\
&= (f \& g)(n) + (f \& h)(n) = [(f \& g) \oplus (f \& h)](n)
\end{aligned}$$

A multiplicative identity with respect to  $\&$  is the function  $\beta$  defined by  $\beta(n) = 1$  if  $n = 0$  and  $\beta(n) = 0$  if  $n \neq 0$ . Let  $n$  be a non-negative integer and  $f \in A$ , then:

$$\begin{aligned}
(f \& \beta)(n) &= \sum_{r=0}^n f(r) \beta(n-r) \\
&= f(0) \beta(n) + \dots + f(n) \beta(0) \\
&= 0 + \dots + 0 + f(n) \cdot 1 \\
&= f(n) .
\end{aligned}$$

Cauchy product was shown above to be commutative, thus  $f \& \beta = f \& \beta$  and  $\beta$  is an identity with respect to  $\&$ . By way of contradiction, suppose that  $\beta$  is not unique. Let  $\beta_1 \neq \beta$  be an identity with respect to  $\&$ . Let  $m$  be the smallest non-negative integer for

which  $\beta_1(m) \neq \beta(m)$ . Let  $\nu(n) = 1$  for  $n$  a non-negative integer. Then by assumption  $\beta_1 \& \nu = \nu = \beta \& \nu$ . In particular,

$$\begin{aligned} (\beta_1 \& \nu)(m) &= \sum_{r=0}^m \beta_1(r) \nu(m-r) \\ &= \beta_1(0) \cdot 1 + \dots + \beta_1(m) \cdot 1 = \beta_1(0) + \beta_1(m), \end{aligned}$$

and

$$\begin{aligned} (\beta \& \nu)(m) &= \sum_{r=0}^m \beta(r) \nu(m-r) \\ &= 1 \cdot 1 + 0 \cdot 1 + \dots + 0 \cdot 1 = 1. \end{aligned}$$

If  $m = 0$  then  $\beta_1(0) \neq 1$  and  $(\beta_1 \& \nu)(0) \neq 1$ , and this is a contradiction since  $\nu(0) = 1$ . If  $m > 0$  then  $\beta_1(0) = 1$ ,  $\beta_1(m) \neq 0$  and again  $(\beta_1 \& \nu)(m) \neq (\beta \& \nu)(m)$  is a contradiction. Thus  $\beta$  is the unique identity with respect to  $\&$ .

Suppose by way of contradiction that  $A$  contains zero divisors with respect to  $\&$ . Then, there exists  $f, g \in A$  such that  $f \neq \theta \neq g$  and  $f \& g = \theta$ . Let  $m, n$  be the smallest non-negative integers such that  $f(m) \neq 0$  and  $g(n) \neq 0$ . Consider:

$$\begin{aligned} (f \& g)(m+n) &= \sum_{r=0}^{m+n} f(r) g(m+n-r) \\ &= f(0) g(m+n) + \dots + f(r-1) g(m+n-r+1) + f(m) g(n) \\ &\quad + f(m+1) g(n-1) + \dots + f(m+n) g(0) \\ &= f(m) g(n), \end{aligned}$$

since all other terms have a zero factor. Further, neither factor of  $f(m) g(n)$  is zero. Therefore,  $f \& g \neq \theta$ , which contradicts the assumption that  $A$  contains zero divisors with respect to  $\&$ . This completes the



proof of Theorem 3.6. This proof also shows  $(A, \&)$  to be a commutative monoid with no zero divisors.

Theorem 3.7.  $(A, \oplus, \&)$  is not a division ring.

Proof: It suffices to exhibit a function  $f \in A$ ,  $f \neq \theta$ , for which there does not exist a function  $g \in A$  such that  $f \& g = \beta$ . Let  $f$  be defined by  $f(n) = 0$  if  $n = 0$  and  $f(n) = 5$  if  $n \neq 0$ . Note that  $f \neq \theta$ . Recall that  $\beta(n) = 1$  if  $n = 0$  and  $\beta(n) = 0$  if  $n \neq 0$ . Clearly no function  $g$  exists for which  $(f \& g)(0) = f(0)g(0) = 1 = \beta(1)$ . Therefore,  $(A, \oplus, \&)$  is not a division ring.

Theorems 3.6 and 3.7 show that  $(A, \oplus, \&)$  is at most an integral domain.

### Convolution Product of Arithmetic Functions

The convolution product of arithmetic functions was defined in Chapter II and many of the algebraic properties were indicated as well. The following result is well known and appears in Shockley [18], Carlitz [2] and [3], and Cashwell and Everett [4].

Theorem 3.8.  $(A, \oplus, \circ)$  is an integral domain.

Proof:  $(A, \oplus)$  is a commutative group by Theorem 3.1. Convolution product is closed, commutative, associative, and has a unique identity as was shown in Chapter II. Thus, it suffices to show that convolution product distributes over sum and that there are no zero divisors in  $A$  with respect to convolution product.

Let  $f, g$ , and  $h$  be arithmetic functions and  $n$  a positive integer. Consider

$$\begin{aligned}
[f \circ (g \oplus h)](n) &= \sum_{d|n} f(d) (g \oplus h)(n/d) \\
&= \sum_{d|n} f(d) [g(n/d) + h(n/d)] \\
&= \sum_{d|n} f(d) g(n/d) + \sum_{d|n} f(d) h(n/d) \\
&= (f \circ g)(n) + (f \circ h)(n) \\
&= [(f \circ g) \oplus (f \circ h)](n)
\end{aligned}$$

Thus convolution product distributes over sum.

Suppose by way of contradiction that  $A$  contains zero divisors with respect to convolution product. Then there exists  $f, g \in A$  such that  $f \neq \theta \neq g$  and  $f \circ g = \theta$ . Let  $m, n$  be the smallest positive integers such that  $f(m) \neq 0$  and  $g(n) \neq 0$ . Let  $d$  be a positive divisor of  $mn$ . If  $1 \leq d < m$ , then  $f(d) = 0$ , and, if  $m < d \leq mn$ ,  $g(mn/d) = 0$ . Therefore,

$$\begin{aligned}
(f \circ g)(mn) &= \sum_{d|mn} f(d) g(mn/d) \\
&= f(1)g(mn) + \dots + f(m)g(n) + \dots + f(mn)g(1) \\
&= f(m)g(n),
\end{aligned}$$

since all other terms have a zero factor. Further, neither factor of  $f(m)g(n)$  is zero. Therefore,  $f \circ g \neq \theta$ , which contradicts the assumption that  $A$  contains zero divisors with respect to convolution product. This completes the proof of Theorem 3.8. This proof also shows  $(A, \circ)$  to be a commutative monoid with no zero divisors.

Theorem 3.9.  $(A, \oplus, \circ)$  is not a division ring. Thus  $(A, \circ, \oplus)$  is at most an integral domain.

Proof: The function  $f(n)=0$  if  $n=1$  and  $f(n)=5$  if  $n \neq 1$  is a non-zero function in  $A$  which by Theorem 2.7 has no inverse with respect to convolution product. Thus  $(A, \oplus, \bullet)$  is not a division ring.

### Unitary Product of Arithmetic Functions

Many of the results of Gautier [10] were stated in Chapter II. The first two results, stated below as Theorem 3.10 and Theorem 3.11, were proven by Gautier. Gautier made no mention of the third result although she did develop the theory needed to prove it.

Recall that  $\#$  indicates unitary product.

Theorem 3.10.  $(A, \oplus, \#)$  is a commutative ring with identity.

Theorem 3.11.  $(A, \oplus, \#)$  is not an integral domain.

Proof: It suffices to exhibit zero divisors with respect to  $\#$ .

$$\text{Define: } f(n) = \begin{cases} 1 & \text{if } n=2 \\ 0 & \text{if } n \neq 2 \end{cases}; \quad g(n) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ 1 & \text{if } n \text{ is even.} \end{cases}$$

If  $n=2$ , then

$$\begin{aligned} (f \# g)(2) &= \sum_{d \parallel 2} f(d)g(2/d) = f(1)g(2) + f(2)g(1) \\ &= 0 \cdot 1 + 1 \cdot 0 = 0 = \theta(2). \end{aligned}$$

If  $n \neq 2$  then  $(f \# g)(n) = \sum_{d \parallel n} f(d)g(n/d)$ . If  $d$  is even then  $n/d$  must be odd by the definition of unitary divisor. But the definition of  $g$  implies that all terms with  $n/d$  odd will be zero. If  $d$  is odd then  $n/d$  may be odd or even. But if  $d$  is odd  $f(d)=0$  by the definition of  $f$  so all terms with  $d$  odd are also zero. Thus,  $(f \# g)(n)=0$  if  $n \neq 2$ .

Therefore,  $f$  and  $g$  are zero divisors with respect to  $\#$  since  $f\#g = \theta$  and  $f \neq \theta \neq g$ .

Theorem 3.12.  $(A, \oplus, \#)$  is not a division ring.

Proof: The function  $g$  in the proof of Theorem 3.11 is such that  $g \neq \theta$ . But  $g(1) = 0$  so by Theorem 2.19  $g^{-1}$  does not exist. Therefore,  $(A, \oplus, \#)$  is not a division ring.

Theorems 3.10, 3.11, and 3.12 prove that  $(A, \oplus, \#)$  is at most a commutative ring with identity.

### Pi Product of Arithmetic Functions

All of the products of arithmetic functions investigated up to this time have been both commutative and associative. Each of these operations when combined with the operation of sum produced at least a commutative ring. Numerous examples exist of non-commutative rings. One of the easiest to verify is the ring of  $2 \times 2$  matrices over the rationals [12;85]. The purpose of this section is to define a product of arithmetic functions that is associative but not commutative and to use this product to exhibit a ring of arithmetic functions that is not commutative.

Definition 3.4. Let  $f$  and  $g$  be arithmetic functions. The function  $f \pi g$ , the pi product of  $f$  and  $g$ , is defined by  $(f \pi g)(n) = f(1)g(n)$  for each positive integer  $n$ .

The corresponding field properties make the pi product of two arithmetic functions a well defined arithmetic function. The next three theorems exhibit the desired properties of pi product.

Theorem 3.13. Pi product has no identity.

Proof: Let  $f(n)=n$  and  $g(n)=1$  for each positive integer  $n$ . Suppose by way of contradiction that  $I$  is an identity for  $\pi$ . If  $(f \pi I)(1) = f(1) = 1$  then  $I(1) = 1$ . Also, if  $(f \pi I)(2) = f(2) = 2$  and  $(f \pi I)(2) = f(1)I(2) = I(2)$  then  $I(2) = 2$ . But  $(g \pi I)(2) = g(2) = 1$  only if  $I(2) = 1$ . But this is a contradiction to  $I$  being a well defined function.

Theorem 3.14. Pi product is not commutative.

Proof: Let  $f$  and  $g$  be defined as in the proof above and let  $n=2$ . Then  $(f \pi g)(2) = 1$  but  $(g \pi f)(2) = 2$ . Thus  $\pi$  is not commutative.

Theorem 3.15. Pi product is associative.

Proof: Let  $f, g$ , and  $h$  be arithmetic functions and  $n$  a positive integer. Then

$$\begin{aligned} [(f \pi g) \pi h](n) &= (f \pi g)(1)h(n) = [f(1)g(1)]h(n) = f(1)[g(1)h(n)] \\ &= f(1)(g \pi h)(n) = [f \pi (g \pi h)](n) \end{aligned}$$

and  $\pi$  is associative.

The preceding results show  $(A, \pi)$  to be a semi-group. Since pi product has no identity in the set of arithmetic functions it is impossible for  $(A, \oplus, \pi)$  to be a division ring or an integral domain and since pi product is not commutative  $(A, \oplus, \pi)$  can be at most a ring. The next theorem shows this much is indeed true.

Theorem 3.16.  $(A, \oplus, \pi)$  is at most a ring.

Proof: Considering the discussion above and the previous theorems on pi product and sum it is sufficient to verify that pi product distributes

over sum. Let  $f, g,$  and  $h$  be arithmetic functions and  $n$  a positive integer. Then

$$\begin{aligned} [f \pi (g \oplus h)](n) &= f(1) (g \oplus h) (n) = f(1) [g(n) + h(n)] \\ &= f(1) g(n) + f(1) h(n) = (f \pi g) (h) + (f \pi h) (n) \\ &= [(f \pi g) \oplus (f \pi h)](n) \end{aligned}$$

and the proof is complete.

The following result is included for completeness.

Theorem 3.17. If  $f$  and  $g$  are multiplicative functions then so is  $f \pi g$ .

Proof: Let  $m$  and  $n$  be positive integers such that  $(m, n) = 1$ . Recall that if  $f$  is multiplicative and not identically zero then  $f(1) = 1$ . Thus

$$\begin{aligned} (f \pi g) (mn) &= f(1) g(mn) = f(1) g(m) f(1) g(n) \\ &= (f \pi g) (m) (f \pi g) (n). \end{aligned}$$

Of course if  $f$  is identically zero so is  $f \pi g$  and a constant function is multiplicative.

### Delta Product of Arithmetic Functions

The usual definition of a ring includes an associative multiplication, however, it is possible to define a non-associative ring. [12; 84].

Definition 3.5. A non-associative ring is a ring in which the associative property of the multiplication in the ring fails to hold.

Shockley [18; 110] defines a binary operation on arithmetic functions, called the delta product for convenience, which produces a

commutative non-associative ring when combined with the operation of sum.

Definition 3.6. Let  $f$  and  $g$  be arithmetic functions. The function  $f \delta g$ , the delta product of  $f$  and  $g$ , is defined by

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

The delta product of two arithmetic functions is a well defined arithmetic function since multiplication and addition are well defined and closed operations in the field that is the range of the given functions. To see that there can be no identity function with respect to delta product consider the function  $f$  defined by  $f(n) = 5$  for every positive integer  $n$ . Assume by way of contradiction that the function  $h$  is an identity with respect to delta product. Then  $(f \delta h)(1) = f(1) = 5$  so  $h(1) = 1$ . Also,  $(f \delta h)(2) = f(1)h(1) + f(2)h(2) = f(2) = 5$  which implies  $h(2) = 0$ . But  $h$  is clearly not an identity with respect to delta product since it fails for the function  $g(1) = 0, g(n) = 2$  for  $n > 1$ , that is  $(g \delta h)(2) = 0 \cdot 1 + 2 \cdot 0 = 0 \neq 2 = g(2)$ . Since there is no identity for delta product the question as to the existence of inverses has no meaning. However, as the next theorem will show, delta product is commutative.

Theorem 3.18. If  $f$  and  $g$  are arithmetic functions then  $f \delta g = g \delta f$ .

Proof: Let  $n$  be a positive integer. Then

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

Although the next result is not needed to prove the main result of this section it is an interesting result and is included for completeness.

Theorem 3.19. If  $f$  and  $g$  are multiplicative functions then so is  $f \delta g$ .

Proof: Let  $m$  and  $n$  be positive integers such that  $(m, n) = 1$ . If  $d | mn$  then  $d = st$  where  $s | m$ ,  $t | n$ , and  $(s, t) = 1$ . Thus

$$\begin{aligned} (f \delta g)(mn) &= \sum_{st | mn} f(st)g(st) = \sum_{\substack{s | m \\ t | n}} f(s)f(t)g(s)g(t) \\ &= \sum_{s | m} f(s)g(s) \sum_{t | n} f(t)g(t) \\ &= (f \delta g)(m) (f \delta g)(n) . \end{aligned}$$

Theorem 3.20. Delta product is not associative.

Proof: Let  $n = 2$ ,  $f(n) = g(n) = n$  for each positive integer  $n$  and  $h(1) = 1$ ,  $h(n) = 0$  if  $n > 1$ . Consider the following computations.

$$\begin{aligned} [(f \delta g) \delta h](2) &= \sum_{d | 2} \left[ \sum_{e | d} f(e)g(e) \right] h(d) \\ &= f(1)g(1)h(1) + [f(1)g(1) + f(2)g(2)]h(2) \\ &= 1 + [1 + 4] \cdot 0 = 1 . \end{aligned}$$

$$\begin{aligned} [f \delta (g \delta h)](2) &= \sum_{d | 2} f(d) \left[ \sum_{e | d} g(e)h(e) \right] \\ &= f(1)g(1)h(1) + f(2)[g(1)h(1) + g(2)h(2)] \\ &= 1 + 2[1 + 0] = 3 . \end{aligned}$$

Thus, delta product is not associative.



It is possible to summarize the results so far by stating that  $(A, \delta)$  is a commutative groupoid. The next theorem is the major result of this section.

Theorem 3.21.  $(A, \oplus, \delta)$  is a commutative non-associative ring

Proof: The only property that has not been verified is the distributive property of delta product over sum. Let  $n$  be a positive integer and  $f, g,$  and  $h$  arithmetic functions. Then

$$\begin{aligned}
 [f \delta (g \oplus h)](n) &= \sum_{d|n} f(d) [(g \oplus h)(d)] \\
 &= \sum_{d|n} f(d) [g(d) + h(d)] = \sum_{d|n} f(d) g(d) + \sum_{d|n} f(d) h(d) \\
 &= \sum_{d|n} f(d) g(d) + \sum_{d|n} f(d) h(d) = (f \delta g)(n) + (f \delta h)(n) \\
 &= [(f \delta g) \oplus (f \delta h)](n) .
 \end{aligned}$$

This completes the proof of the theorem. Since delta product has no identity  $(A, \oplus, \delta)$  is at most a commutative non-associative ring.

CHAPTER IV  
OPERATORS ON ALGEBRAS OF  
ARITHMETIC FUNCTIONS

In Chapter I an arithmetic function was defined to be any function mapping the positive integers into a subset of the complex numbers  $C$ . That the subset of  $C$  can aid in the investigation of the algebraic properties of a set of arithmetic functions will become apparent in this chapter. The techniques used and the results found in this chapter are summarized in an article by Rearick [16].

In the first part of this chapter attention will be focused on the algebraic comparison of sets of real-valued functions, that is, taking the subset of  $C$  referred to above as the real numbers. Throughout this chapter let  $A$  stand for the set of all real-valued arithmetic function,  $P$  the set of all  $f \in A$  such that  $f(1) > 0$ , and  $M$  the set of all  $f \in A$  such that  $f$  is a multiplicative function. The operations to be considered on these sets are those of sum ( $\oplus$ ), convolution product ( $\circ$ ), and unitary product ( $\#$ ). Let  $B = \{f \in A \mid f(1) \neq 0\}$ . The proofs of the previous chapters can be used without change to show that  $(A, \oplus)$ ,  $(B, \circ)$ ,  $(B, \#)$ ,  $(M, \circ)$ , and  $(M, \#)$  are all groups. It is easy to show that  $(P, \circ)$  and  $(P, \#)$  are subgroups of  $(B, \circ)$  and  $(B, \#)$ , respectively.

The algebraic equivalence of the above groups is summarized in Theorem 4.3. Before stating this theorem several definitions and results follow.

Definition 4.1. A mapping  $\alpha$  from a group  $G$  into a group  $H$  is a homomorphism if and only if for all  $a, b \in G$ ,  $\alpha(ab) = \alpha(a)\alpha(b)$ .

Definition 4.2. The mapping  $\beta: M \rightarrow N$  is an onto mapping if and only if for each  $n \in N$  there exists  $m \in M$  such that  $\beta(m) = n$ .

Definition 4.3. The mapping  $\gamma: M \rightarrow N$  is a one-to-one mapping if and only if whenever  $\gamma(x) = \gamma(y)$  then  $x = y$ .

Definition 4.4. The mapping  $\alpha$  from a group  $G$  to a group  $H$  is an isomorphism if and only if  $\alpha$  is a one-to-one onto homomorphism.

Definition 4.5. Two groups  $G$  and  $H$  are said to be isomorphic if and only if there is an isomorphism mapping  $G$  to  $H$ .

Definition 4.6. A nonempty set  $V$  is said to be a vector space over a field  $F$  if and only if  $(V, +)$  is an abelian group, and for each  $a \in F$ ,  $v \in V$ , there is an element  $av \in V$  subject to:

$$(1) a(v+w) = av+aw$$

$$(2) (a+b)v = av+bv$$

$$(3) a(bv) = (ab)v$$

$$(4) 1v = v$$

for all  $a, b \in F$ ,  $v, w \in V$  (where  $1$  is the unit element of  $F$  under multiplication).

Theorem 4.1.  $A$  is a vector space over  $R$ , the field of real numbers.

Proof:  $(A, \oplus)$  is known to be an abelian group. The usual definition of a scalar times a function shows  $af$  to be an element of  $A$  whenever

$f \in A$  and  $a \in R$ , that is,  $(af)(n) = af(n)$  for  $n$  a positive integer. The remaining properties follow from the definitions. Thus,

$$a(f \oplus g)(n) = a(f(n) + g(n)) = af(n) + ag(n) = (af \oplus ag)(n) ;$$

$$(a + b)f(n) = af(n) + bf(n) = (af \oplus bf)(n) ;$$

$$a(bf)(n) = a(bf(n)) = (ab)f(n) ;$$

and  $1f(n) = f(n)$ , for  $n$  a positive integer.

Definition 4.7. A ring  $B$  is called an algebra over a field  $F$  if and only if  $B$  is a vector space over  $F$  such that for all  $a, b \in B$  and  $r \in F$ ,  $r(ab) = (ra)b = a(rb)$ . An algebra is commutative if the ring is commutative.

Theorem 4.2.  $(A, \oplus, \circ)$  is a commutative algebra over  $R$ .

This result will be indicated by  $(A, \oplus, \circ, \cdot)$ .

Proof: From the theorem above  $A$  is a vector space over  $R$ . Also,  $(A, \oplus, \circ)$  is known to be a commutative ring. To complete the proof let  $f, g \in A$ ,  $r \in R$ ,  $n$  a positive integer, and consider the following manipulations.

$$\begin{aligned} [r(f \circ g)](n) &= r[(f \circ g)(n)] = r \sum_{d|n} f(d)g(n/d) \\ &= \sum_{d|n} rf(d)g(n/d) = \sum_{d|n} (rf)(d)g(n/d) \\ &= [(rf) \circ g](n) . \end{aligned}$$

Also,

$$\begin{aligned}
[r(f \circ g)](n) &= \sum_{d|n} f(d) \operatorname{rg}(n/d) = \sum_{d|n} f(d) (\operatorname{rg})(n/d) \\
&= [f \circ (\operatorname{rg})](n) .
\end{aligned}$$

It is also true that  $(A, \oplus, \#, \cdot)$  is a commutative algebra over  $R$ . The proof of Theorem 4.2 provides the pattern as  $(A, \oplus, \#)$  is a commutative ring and the manipulations in the proof can be carried out equally well using unitary product instead of convolution product. This sets the pattern for the remainder of this chapter as most theorems and definitions will be stated using convolution product and followed by an indication of how similar results hold for unitary product. A key result of this chapter is the following theorem.

Theorem 4.3. The groups  $(P, \circ)$ ,  $(M, \circ)$ ,  $(P, \#)$ ,  $(M, \#)$ , and  $(A, \oplus)$  are all isomorphic.

The proof of this theorem depends upon finding the required isomorphisms. One of the isomorphisms turns out to be the logarithm operator  $L$  defined in the next section. An operator is a mapping from a subset of a set into the set.

#### The Logarithm Operator $L$

Instrumental in the proof of Theorem 4.3 is the logarithm operator  $L$  given by the following definition.

Definition 4.8. If  $f \in P$ , let

$$L f(n) = \sum_{d|n} f(d) f^{-1}(n/d) \log d \quad \text{if } n > 1,$$

and

$$L f(1) = \log f(1) .$$

Observe that  $f^{-1}$  is the inverse of  $f$  with respect to convolution product and that  $L$  maps the set  $P$  into the set  $A$ .

An example illustrating the logarithm operator will follow. Let  $f$  in Definition 4.8 be the number of divisors function  $\tau$ . Since  $\tau$  is multiplicative its function values are completely determined by its function values on prime powers. A theorem to follow will show  $L f(n) = 0$  whenever  $f$  is multiplicative and  $n$  is not a power of a prime. Assuming this to be known for the present, let  $p$  be an arbitrary but fixed prime. Recall that  $\tau(1) = 1$  and  $\tau(p^k) = k + 1$  if  $k > 0$ .

Theorem 2.7 provides the tools needed to compute  $\tau^{-1}$ . Adapting the first two equations in the proof of that theorem to the present situation the equations become:

$$\tau^{-1}(1) = 1/\tau(1) = 1,$$

and

$$\tau^{-1}(p^k) = - \sum_{s=0}^{k-1} \tau^{-1}(p^s) \tau(p^{k-s}) \quad \text{if } k > 0.$$

Thus,

$$\tau^{-1}(p) = -\tau^{-1}(1) \tau(p) = -2,$$

$$\tau^{-1}(p^2) = -[1 \cdot 3 + (-2) \cdot 2] = 1,$$

and

$$\tau^{-1}(p^3) = -[1 \cdot 4 + (-2) \cdot 3 + 1 \cdot 2] = 0.$$

Assume  $\tau^{-1}(p^s) = 0$  for  $3 \leq s < k$ . If  $s = k$  then

$$\begin{aligned} \tau^{-1}(p^k) &= - \sum_{s=0}^{k-1} \tau^{-1}(p^s) \tau(p^{k-s}) \\ &= - [1(k+1) - 2(k) + 1(k-1) + 0(k-2) + \dots + 0 \cdot 2] \\ &= 0. \end{aligned}$$

Using these results the computation of  $L\tau(p^k)$  follows from Definition 4.8. Thus,

$$L\tau(1) = \log \tau(1) = 0 ,$$

$$L\tau(p) = \tau(1)\tau^{-1}(1)\log 1 + \tau(p)\tau^{-1}(1)\log p = 2\log p ,$$

$$L\tau(p^2) = 0 + \tau(p)\tau^{-1}(p)\log p + \tau(p^2)\tau^{-1}(1)\log p^2 = 2\log p ,$$

and

$$L\tau(p^3) = 0 + 2 \cdot 1 \log p + 3(-2)\log p^2 + 4 \cdot 1 \log p^3 = 2\log p .$$

If  $k > 3$  then

$$\begin{aligned} L\tau(p^k) &= [0 + \tau(p)\tau^{-1}(p^{k-1})\log p + \tau(p^2)\tau^{-1}(p^{k-2})\log p^2 + \dots] \\ &\quad + \tau(p^{k-2})\tau^{-1}(p^2)\log p^{k-2} + \tau(p^{k-1})\tau^{-1}(p)\log p^{k-1} + \tau(p^k)\tau^{-1}(1)\log p^k \\ &= 0 + (k-1) \cdot 1 \cdot (k-2)\log p + k(-2)(k-1)\log p + (k+1) \cdot 1 \cdot k \log p \\ &= 2\log p . \end{aligned}$$

It should be noticed that the prime  $p$  used does not affect the manipulations above except that the same prime must be used throughout. Thus, the pattern above holds for all primes  $p$ .

It will be shown that  $L$  is an isomorphism. The next theorem shows  $L$  to have the logarithmic property which is also, considering the operations on  $P$  and  $A$ , the desired homomorphism property.

Theorem 4.4. For all  $f, g \in P$ ,  $L(f \circ g) = Lf \oplus Lg$ .

The proof of this theorem will be facilitated by an additional definition and two supporting lemmas.

Definition 4.9. Define the operator  $\lambda : A \rightarrow A$  by  $\lambda f(n) = f(n) \log n$ ,  $n$  a positive integer.

Lemma 4.1. If  $n > 1$ ,  $Lf(n) = (f^{-1} \circ \lambda f)(n)$  for each  $f \in A$ .

Proof: If  $n > 1$ ,

$$Lf(n) = \sum_{d|n} f(d) f^{-1}(n/d) \log d = \sum_{d|n} f^{-1}(n/d) \lambda f(d) = (f^{-1} \circ \lambda f)(n).$$

Lemma 4.2. If  $f, g \in A$  then  $\lambda(f \circ g) = g \circ \lambda f \oplus f \circ \lambda g$ .

Proof: Let  $n$  be a positive integer and  $K = (g \circ \lambda f \oplus f \circ \lambda g)(n)$ . Then,

$$\begin{aligned} K &= (g \circ \lambda f)(n) + (f \circ \lambda g)(n) \\ &= \sum_{d|n} g(d) \lambda f(n/d) + \sum_{d|n} f(d) \lambda g(n/d). \end{aligned}$$

By Definition 4.9,

$$K = \sum_{d|n} g(d) f(n/d) \log(n/d) + \sum_{d|n} f(d) g(n/d) \log(n/d).$$

Reversing the order of the first sum and algebraic manipulations give

$$\begin{aligned} K &= \sum_{d|n} f(d) g(n/d) \log d + \sum_{d|n} f(d) g(n/d) \log(n/d) \\ &= \sum_{d|n} f(d) g(n/d) (\log d + \log(n/d)) \\ &= \sum_{d|n} f(d) g(n/d) \log n. \end{aligned}$$

Using Definition 4.9 gives the desired result, that is,

$$K = (f \circ g)(n) \log n = \lambda(f \circ g)(n).$$

Now to prove Theorem 4.4. Let  $f$  and  $g$  be elements of  $P$ .

If  $n = 1$ , then



$$\begin{aligned} L(f \circ g)(1) &= \log (f \circ g)(1) = \log f(1) g(1) = \log f(1) + \log g(1) \\ &= Lf(1) + Lg(1) = (Lf \oplus Lg)(1) . \end{aligned}$$

Now let  $n > 1$ . By Lemma 4.2, it is true that

$$\lambda(f \circ g) = g \circ \lambda f \oplus f \circ \lambda g .$$

Taking the convolution product of both sides of this expression with  $f^{-1} \circ g^{-1}$ , recalling that  $(A, \oplus, \circ)$  is a commutative ring, the following expression is obtained:

$$(f \circ g)^{-1} \circ \lambda(f \circ g) = f^{-1} \circ \lambda f \oplus g^{-1} \circ \lambda g .$$

By Lemma 4.1 this expression reduces to the desired expression.

Thus,

$$L(f \circ g)(n) = (Lf \oplus Lg)(n) ,$$

which completes the proof of the theorem.

The next theorem will show that the operator  $L$  is also a one-to-one and onto mapping completing the proof that  $L$  is an isomorphism mapping  $P$  onto  $A$ .

Theorem 4.5. For each  $h \in A$  there is a unique  $f \in P$  such that  $h = Lf$ .

The following example will serve to illustrate the method of the proof. Let  $h \in A$  be such that  $h = Lf$  as given in the example following Definition 4.8. Thus  $h(1) = 0$ ,  $h(2) = 2 \log 2$ ,  $h(3) = 2 \log 3$ ,  $h(4) = 2 \log 2$ ,  $h(5) = 2 \log 5$ ,  $h(6) = 0$ ,  $h(7) = 2 \log 7$ ,  $h(8) = 2 \log 2$ ,  $h(9) = 2 \log 3$ , etc. By the theorem above it should be possible to show

that  $f = \tau$ . The following computations show that  $f$  and  $\tau$  do agree on the first few positive integers.

Define  $f(1) = \exp(h(1))$ . Then  $f(1) = e^0 = 1$ . Note  $f(1) = \tau(1)$ . Compute  $f^{-1}(1) = 1/f(1) = 1 = \tau^{-1}(1)$ . Now use Definition 4.8 to compute  $f(2)$ . This is possible since  $\log 1 = 0$  and  $f^{-1}(2)$ , although at present it is unknown, is some fixed real number. Thus,

$$h(2) = 2 \log 2 = Lf(2) = f(1)f^{-1}(2) \log 1 + f(2)f^{-1}(1) \log 2,$$

which implies that  $f(2) = 2 = \tau(2)$ . It is now possible to solve for  $f^{-1}(2)$ . Since  $0 = \varepsilon(2) = (f \circ f^{-1})(2)$ , the equation  $0 = f(1)f^{-1}(2) + f(2)f^{-1}(1)$  reveals that  $f^{-1}(2) = -2 = \tau^{-1}(2)$ .

Similar computations show  $f(n) = \tau(n) = 2$  and  $f^{-1}(n) = \tau^{-1}(n) = -2$  for  $n = 3$  and for  $n = 5$ . Let  $n = 4$ . Then

$$h(4) = 2 \log 2 = Lf(4) = f(1)f^{-1}(4) \log 1 + f(2)f^{-1}(2) \log 2 + f(4)f^{-1}(1) \log 4$$

which shows that  $f(4) = 3 = \tau(4)$ . Also, from  $0 = \varepsilon(4) = (f \circ f^{-1})(4)$ , it follows that  $f^{-1}(4) = 1 = \tau^{-1}(4)$ .

Let  $n = 6$ , which is not a power of a prime. Now

$$\begin{aligned} h(6) &= 0 = Lf(6) \\ &= f(1)f^{-1}(6) \log 1 + f(2)f^{-1}(3) \log 2 + f(3)f^{-1}(2) \log 3 + f(6)f^{-1}(1) \log 6. \end{aligned}$$

Since  $\log 1 = 0$  this equation leads to the desired conclusion that  $f(6) = 4 = \tau(6)$ . Also,  $0 = \varepsilon(6) = (f \circ f^{-1})(6)$  shows that

$$f^{-1}(6) = 4 = (-2)(-2) = \tau^{-1}(2)\tau^{-1}(3) = \tau^{-1}(6),$$

since  $\tau$  being multiplicative implies that  $\tau^{-1}$  is also multiplicative.

Certainly this process can be continued to find the value of  $f(n)$  for any positive integer  $n$ . Notice also that the process at each step involves solving a linear equation in  $f(n)$  with real coefficients. The solutions of such equations are unique. No claim is made that  $f(n) = \tau(n)$  for all positive integers  $n$ . The process shows how the theorem can be proven.

Proof of Theorem 4.5. Let  $h \in A$ . A function  $f \in P$  is defined inductively as follows. For  $n=1$  define  $f(1) = \exp(h(1))$ . Certainly  $f(1) > 0$  so  $f$  will be an element of  $P$ . Let  $n > 1$  and assume  $f(k)$  has been defined for all  $k < n$  so as to satisfy the conditions of the theorem. Then the values of  $f^{-1}(k)$  may be determined recursively for all  $k < n$  by solving the system

$$\sum_{d|k} f^{-1}(d) f(k/d) = \epsilon(k)$$

for the unknown  $f^{-1}(k)$  for  $k=1, 2, \dots, n-1$ . For  $k=n$ ,  $f(n)$  is defined by solving for  $f(n)$  in the equation

$$h(n) = \sum_{d|n} f(d) f^{-1}(n/d) \log d.$$

This is possible since  $h(n)$  is known as are  $f(d)$  and  $f^{-1}(n/d)$  for all  $d$  and  $n/d$  less than  $n$ . Although the value of  $f^{-1}(n)$  is not known this factor occurs when  $d=1$  and the term  $f(1) f^{-1}(n) \log 1$  vanishes since  $\log 1 = 0$ . Hence it is possible to solve for  $f(n)$ ,

The construction of  $f$  from  $h$  and the definition of  $L$  shows that  $Lf = h$ . That the  $f$  so constructed is unique follows from observing that at the  $n^{\text{th}}$  step  $f(n)$  is determined by a finite number of well

defined field operations, that is, solving a linear equation in  $f(n)$  for  $f(n)$ . This completes the proof of the theorem.

Theorems 4.4 and 4.5 show that the mapping  $L : (P, \circ) \rightarrow (A, \oplus)$  defined by  $L : f \rightarrow Lf$  is an isomorphism. Thus, one of the parts of Theorem 4.3 has been proven, namely  $(P, \circ) \approx (A, \oplus)$ .

The next parts of Theorem 4.3 that will be proven are to show that  $(M, \circ) \approx (A, \oplus)$  and  $(M, \circ) \approx (P, \circ)$ . Several lemmas and theorems will be needed to accomplish this end.

Lemma 4.3. Let  $f$  be an arithmetic function. The arithmetic function  $g$  defined by

$$g(1) = 1$$

$$g(n) = \prod_{p|n} f(p^r), \text{ where } p^r | n \text{ and } p^{r+1} \nmid n, \text{ for } n > 1,$$

is multiplicative.

Proof: Let  $m$  and  $n$  be positive integers such that  $(m, n) = 1$ . If

$$m = \prod_{i=1}^k p_i^{a_i} \quad \text{and} \quad n = \prod_{i=1}^d q_i^{b_i}$$

are the canonical factorizations of  $m$  and  $n$  respectively, then  $p_i \neq q_j$  for any  $i, j$  such that  $1 \leq i \leq k, 1 \leq j \leq d$ . Now

$$g(mn) = \prod_{p|mn} f(p^r) \quad \text{where} \quad p^r | mn, p^{r+1} \nmid mn.$$

Since  $(m, n) = 1$  this can be written as

$$g(mn) = \prod_{p|m} f(p^s) \prod_{q|n} f(q^t) \quad \text{where } p^s|m, p^{s+1} \nmid m, q^t|n, q^{t+1} \nmid n.$$

Therefore,  $g(mn) = g(m)g(n)$ , showing  $g$  to be multiplicative.

Theorem 4.6. A function  $f \in P$  is multiplicative if, and only if,  $Lf(n) = 0$  whenever  $n$  is not a power of a prime.

Proof: Let  $f \in P$  and assume  $f$  to be multiplicative. Thus  $f(1) = 1$ , so  $Lf(1) = 0$ . Let  $N$  be any integer greater than one which is not a power of a prime. Then  $N$  can be written as  $mn$  where  $m > 1$ ,  $n > 1$ , and  $(m, n) = 1$ . To prove the implication, it suffices to show that  $Lf(N) = 0$ . It is possible to write:

$$\begin{aligned} Lf(N) &= \sum_{d|mn} f(d) f^{-1}(mn/d) \log d \\ &= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2) f^{-1}(m/d_1) f^{-1}(n/d_2) (\log d_1 + \log d_2) \end{aligned}$$

where each divisor  $d$  of  $mn$  has been written uniquely as  $d = d_1 d_2$ ,  $d_1$  being a divisor of  $m$  and  $d_2$  a divisor of  $n$ . Note  $(d_1, d_2) = 1$  and  $(m/d_1, n/d_2) = 1$  since  $(m, n) = 1$ . Thus,

$$\begin{aligned} Lf(N) &= \sum_{d_1|m} \sum_{d_2|n} [f(d_1) f^{-1}(m/d_1) \log d_1 f(d_2) f^{-1}(n/d_2) \\ &\quad + f(d_2) f^{-1}(n/d_2) \log d_2 f(d_1) f^{-1}(m/d_1)] \\ &= \sum_{d_1|m} f(d_1) f^{-1}(m/d_1) \log d_1 \sum_{d_2|n} f(d_2) f^{-1}(n/d_2) \\ &\quad + \sum_{d_1|m} f(d_1) f^{-1}(m/d_1) \sum_{d_2|n} f(d_2) f^{-1}(n/d_2) \log d_2 \\ &= Lf(m) \varepsilon(n) + \varepsilon(m) Lf(n) = 0, \end{aligned}$$

since  $m, n > 1$  implies that  $\varepsilon(n) = \varepsilon(m) = 0$ .

To prove the converse, suppose  $Lf(n) = 0$  whenever  $n$  is not a power of a prime. Then  $Lf(1) = 0$ , so  $f(1) = 1$ . Define  $g(1) = 1$ , and for  $n > 1$ , let

$$g(n) = \prod_{p|n} f(p^r) \quad \text{where} \quad p^r | n, p^{r+1} \nmid n.$$

By Lemma 4.3,  $g$  is multiplicative. It will be shown that  $g = f$ . By the definition of  $g$ ,  $f$  and  $g$  agree on powers of a prime. The functions  $f^{-1}$  and  $g^{-1}$  (relative to convolution product) also agree on powers of prime. This follows since the values of  $f^{-1}$  and  $g^{-1}$  on powers of a prime depend only upon the values of  $f$  and  $g$  respectively on the powers of a prime as determined by the equations  $\varepsilon(p^k) = (f \circ f^{-1})(p^k)$  and  $\varepsilon(p^k) = (g \circ g^{-1})(p^k)$ . From the definition of  $L$  it follows that  $Lf$  and  $Lg$  agree on powers of a prime. Since  $g$  is multiplicative, the previous half of this theorem shows that  $Lg(n) = 0$  whenever  $n$  is not a power of a prime. But this is also true of  $Lf$  by assumption. Therefore,  $Lf(n) = Lg(n)$  for all positive integers  $n$ . Thus, by Theorem 4.5,  $f(n) = g(n)$  for each positive integer  $n$ . This completes the proof of the theorem.

Notice that Theorem 4.6 does not give any information about  $Lg(n)$  whenever  $g$  is multiplicative and  $n$  is a power of a prime. For example, the function  $f$  defined by  $f(1) = 1$ ,  $f(n) = 0$  if  $n > 1$  is a multiplicative function (it is really  $\varepsilon$ ) such that for positive  $k$  and  $p$  a prime,

$$Lf(p^k) = f(1)f^{-1}(p^k) \log 1 + f(p)f^{-1}(p^{k-1}) \log p + \dots + f(p^k)f^{-1}(1) \log p^k = 0.$$

This follows since each term contains a zero factor, either  $\log 1$  or  $f(p^t)$ ,  $1 \leq t \leq k$ . In the example used earlier, where  $f = \tau$ , it was found that  $Lf(p^k) = 2 \log p \neq 0$  for  $k > 0$ . Thus  $Lf(n)$  may or may not be zero for  $f$  multiplicative and  $n$  a power of a prime.

Definition 4.10. Let

$$D = \{h \in A \mid h = Lf, f \in P, h(n) = 0 \text{ if } n \text{ is not a prime power}\}.$$

Lemma 4.4.  $(D, \oplus)$  is a subgroup of  $(A, \oplus)$ .

Proof: Observe that  $D$  is a subset of  $A$ . The set  $D$  is not empty since  $D = L(M)$  and  $M \neq \emptyset$ . Let  $h, g \in D$  and  $n$  a positive integer that is not a power of a prime. Then  $(h \oplus g)(n) = h(n) + g(n) = 0 + 0 = 0$ . Hence  $h \oplus g \in D$  making  $D$  closed under sum. If  $h \in D$  then  $-h \in D$  since  $h(n) = 0$  implies  $-h(n) = 0$ . Thus  $-h \in D$  and  $D$  contains the inverse of each of its elements. Therefore,  $(D, \oplus)$  is a subgroup of  $(A, \oplus)$ .

Theorem 4.7.  $(P, \circ) \approx (A, \oplus)$ .

The proof of this result was given in the dialogue following the proof of Theorem 4.5. The result is recorded here for future reference.

Theorem 4.8.  $(M, \circ) \approx (D, \oplus)$ .

Proof: It was shown in an earlier chapter that  $(M, \circ)$  is a subgroup of  $(P, \circ)$ . Consider the restriction  $L'$  of  $L$  to  $M$ ,  $L': M \rightarrow A$ . The image of  $M$  under  $L'$  is  $L'(M)$ . Theorem 4.6 shows that  $L'(M) = D$ .

Therefore,  $(M, \circ) \approx (D, \oplus)$  since the restriction of an isomorphism is an isomorphism of the restricted domain with its image space.

Recall that the purpose of the present work is to show that  $(M, \circ) \approx (P, \circ)$  and  $(M, \circ) \approx (A, \oplus)$ . Two results have already been recorded, namely  $(P, \circ) \approx (A, \oplus)$  and  $(M, \circ) \approx (D, \oplus)$ . The missing link in the chain of isomorphisms is contained in

Theorem 4.9.  $(D, \oplus) \approx (A, \oplus)$ .

Proof: Consider the mapping  $\gamma : D \rightarrow A$  defined by  $\gamma(h) = H$  where  $H(n) = h(k_n)$ ,  $\{k_n\}$  being the sequence of powers of primes arranged in ascending order, that is,  $\{k_n\} = \{2, 3, 2^2, 5, 7, 2^3, 3^2, 11, 13, 2^4, \dots\}$ . Thus  $H(1) = h(2)$ ,  $H(4) = h(5)$ , and  $H(7) = h(3^2)$ . It suffices to show  $\gamma$  is an isomorphism.

Let  $h, g \in D$  and  $H, G \in A$  such that  $\gamma(h) = H$  and  $\gamma(g) = G$ . Also, let  $k_n \in \{k_n\}$ . Then,

$$\begin{aligned} \gamma(h \oplus g)(k_n) &= (H \oplus G)(n) = H(n) + G(n) \\ &= \gamma h(k_n) + \gamma g(k_n) = (\gamma h \oplus \gamma g)(k_n). \end{aligned}$$

Therefore,  $\gamma$  is a homomorphism.

Let  $H \in A$ . Define  $h \in A$  by

$$h(m) = \begin{cases} 0 & \text{if } m \neq p^s \text{ (not a power of a prime)} \\ H(n) & \text{if } m = k_n. \end{cases}$$

Claim  $h \in D$ . By Theorem 4.5 there exists a unique  $f \in P$  such that  $Lf = h$ . By definition,  $h(m) = 0$  if  $m$  is not a power of a prime. Thus, by Theorem 4.6,  $f$  is multiplicative. Therefore,  $Lf = h \in L(M) = D$  and  $\gamma$  is an onto mapping.



Suppose  $H, G \in A$  such that  $H = G$ . Also, suppose  $h, g \in D$  such that  $\gamma h = H$  and  $\gamma g = G$ . If  $H(n) = G(n)$  for each positive integer  $n$  then  $h(k_n) = g(k_n)$  for each  $k_n \in \{k_n\}$ , that is  $h$  and  $g$  agree on powers of primes. Now  $h, g \in D = L(M)$  so  $h(m) = 0 = g(m)$  whenever  $m$  is not a power of a prime. Therefore,  $h(n) = g(n)$  for each positive integer  $n$  and  $\gamma$  is seen to be a one-to-one mapping.

Thus  $\gamma: D \rightarrow A$  is an isomorphism. Consequently,  
 $(D, \oplus) \approx (A, \oplus)$ .

Theorem 4.10.  $(M, \circ) \approx (A, \oplus)$ .

Proof: Since being isomorphic to is an equivalence relation,  
 $(M, \circ) \approx (D, \oplus)$  and  $(D, \oplus) \approx (A, \oplus)$  implies that  $(M, \circ) \approx (A, \oplus)$ .

Theorem 4.11.  $(M, \circ) \approx (P, \circ)$ .

Proof: Since  $(M, \circ) \approx (A, \oplus)$  and  $(P, \circ) \approx (A, \oplus)$  it follows that  
 $(M, \circ) \approx (P, \circ)$ .

Theorems 4.5, 4.10, and 4.11 summarize three of the parts to be shown in the proof of Theorem 4.3. The technique used in this section with the logarithm operator  $L$  and convolution product can be paralleled completely with a slight change in the definition of the logarithm operator and a corresponding change to the unitary product. The results are listed below. The proofs are generally omitted since the proofs of this section will suffice if convolution product  $\sum_{d|n}$  is replaced by unitary product  $\sum'_{d||n}$  and some of the definitions are changed.

### The Logarithm Operator $L'$

In this section  $f^{-1}$  denotes the inverse of the function  $f$  relative to unitary product. Recall that the function  $\epsilon$  is the identity with respect to both unitary and convolution product. Thus  $f \# f^{-1} = \epsilon$ . The development begins with:

Definition 4.11. If  $f \in P$ , let

$$L'f(n) = \sum_{d \parallel n} f(d) f^{-1}(n/d) \log d \quad \text{if } n > 1,$$

and

$$L'f(1) = \log f(1).$$

By its definition the operator  $L'$  maps the set  $P$  into the set  $A$ . One goal is to show that  $L'$  is an isomorphism of the groups  $(P, \#)$  and  $(A, \oplus)$ . It is seen to be a homomorphism by:

Theorem 4.12. For all  $f, g \in P$ ,  $L'(f \# g) = L'f \oplus L'g$ .

Definition 4.12. Define the operator  $\lambda' : A \rightarrow A$  by  $\lambda'f(n) = f(n) \log n$ ,  $n$  a positive integer.

Lemma 4.5. If  $n > 1$ ,  $L'f(n) = (f^{-1} \# \lambda'f)(n)$  for each  $f \in A$ .

Lemma 4.6. If  $f, g \in A$  then  $\lambda'(f \# g) = g \# \lambda'f \oplus f \# \lambda'g$ .

Theorem 4.13. For each  $h \in A$  there is a unique  $f \in P$  such that  $h = L'f$ .

Lemma 4.3 need not be changed since it does not involve either of the logarithm operators nor does it involve convolution or unitary product of arithmetic functions.

To fortify the claim that the proofs of the results in this section parallel those of the previous section, a proof for the next theorem is included.

Theorem 4.14. A function  $f \in \mathcal{P}$  is multiplicative if, and only if,  $L'f(n) = 0$  whenever  $n$  is not a power of a prime.

Proof: Let  $f \in \mathcal{P}$  and assume  $f$  to be multiplicative. Thus  $f(1) = 1$ , so  $L'f(1) = 0$ . Let  $N$  be any integer greater than one which is not a power of a prime. Then  $N$  can be written as  $mn$  where  $m > 1$ ,  $n > 1$ , and  $(m, n) = 1$ . To prove the implication, it suffices to show that  $L'f(N) = 0$ . It is possible to write:

$$\begin{aligned} L'f(N) &= \sum_{d \parallel mn} f(d) f^{-1}(mn/d) \log d \\ &= \sum_{d_1 \parallel m} \sum_{d_2 \parallel n} f(d_1) f(d_2) f^{-1}(m/d_1) f^{-1}(n/d_2) (\log d_1 + \log d_2) \end{aligned}$$

where each unitary divisor  $d$  of  $mn$  has been written uniquely as  $d = d_1 d_2$ ,  $d_1$  being a divisor of  $m$  and  $d_2$  a divisor of  $n$ . Note  $(d_1, d_2) = 1$  and  $(m/d_1, n/d_2) = 1$  since  $(m, n) = 1$ . Certainly  $d_1 \parallel m$  and  $d_2 \parallel n$  since  $d \parallel mn$ . Thus,

$$\begin{aligned} L'f(N) &= \sum_{d_1 \parallel m} \sum_{d_2 \parallel n} [f(d_1) f^{-1}(m/d_1) \log d_1 f(d_2) f^{-1}(n/d_2) \\ &\quad + f(d_2) f^{-1}(n/d_2) \log d_2 f(d_1) f^{-1}(m/d_1)] \\ &= \sum_{d_1 \parallel m} f(d_1) f^{-1}(m/d_1) \log d_1 \sum_{d_2 \parallel n} f(d_2) f^{-1}(n/d_2) \\ &\quad + \sum_{d_1 \parallel m} f(d_1) f^{-1}(m/d_1) \sum_{d_2 \parallel n} f(d_2) f^{-1}(n/d_2) \log d_2 \end{aligned}$$

$$= L'f(m)\varepsilon(n) + \varepsilon(m)L'(n) = 0,$$

since  $m, n > 1$  implies that  $\varepsilon(n) = \varepsilon(m) = 0$ .

To prove the converse, suppose  $L'f(n) = 0$  whenever  $n$  is not a power of a prime. Then  $L'f(1) = 0$ , so  $f(1) = 1$ . Define  $g(1) = 1$ , and for  $n > 1$ , let

$$g(n) = \prod_{p|n} f(p^r) \quad \text{where } p^r | n, p^{r+1} \nmid n.$$

By Lemma 4.3,  $g$  is multiplicative. It will be shown that  $g = f$ . By the definition of  $g$ ,  $f$  and  $g$  agree on powers of a prime. The functions  $f^{-1}$  and  $g^{-1}$  (relative to unitary product) also agree on powers of a prime. This follows since the values of  $f^{-1}$  and  $g^{-1}$  on powers of a prime depend only upon the values of  $f$  and  $g$  respectively on the powers of a prime as determined by the equations  $\varepsilon(p^k) = (f \# f^{-1})(p^k)$  and  $\varepsilon(p^k) = (g \# g^{-1})(p^k)$ . From the definition of  $L'$  it follows that  $L'f$  and  $L'g$  agree on powers of a prime. Since  $g$  is multiplicative, the previous half of this theorem shows that  $L'g(n) = 0$  whenever  $n$  is not a power of a prime. But this is also true of  $L'f$  by assumption. Therefore,  $L'f(n) = L'g(n)$  for all positive integers  $n$ . Thus, by Theorem 4.13,  $f(n) = g(n)$  for each positive integer  $n$ . This completes the proof of the theorem.

Definition 4.13. Let

$$D' = \{h \in A \mid h = L'f, f \in P, h(n) = 0 \text{ if } n \text{ is not a power of a prime}\}.$$

Lemma 4.7.  $(D', \oplus)$  is a subgroup of  $(A, \oplus)$ .

Theorem 4.15.  $(P, \#) \approx (A, \oplus)$ .

Theorem 4. 16.  $(M, \#) \approx (D', \oplus)$ .

Theorem 4. 17.  $(D', \oplus) \approx (A, \oplus)$ .

Theorem 4. 18.  $(M, \#) \approx (A, \oplus)$ .

Theorem 4. 19.  $(M, \#) \approx (P, \#)$ .

The following results which complete the proof of Theorem 4. 3 easily follow from the previous results and the transitive property of the equivalence relation "is isomorphic to".

Corollary 4. 1.  $(P, \circ) \approx (P, \#)$ .

Corollary 4. 2.  $(P, \circ) \approx (M, \#)$ .

Corollary 4. 3.  $(M, \circ) \approx (P, \#)$ .

Corollary 4. 4.  $(M, \circ) \approx (M, \#)$ .

Corollary 4. 1 and Corollary 4. 4 show that it is no longer necessary to state and prove all results in terms of both the convolution and unitary products. Future results will be proven for convolution product only.

It is of interest mathematically to exhibit an isomorphism that proves  $(P, \circ) \approx (P, \#)$  directly. Let  $\alpha: (P, \circ) \rightarrow (P, \#)$  be defined by  $\alpha: f \rightarrow f'$ , for each  $f \in (P, \circ)$ , where  $f'$  is determined by the equation  $Lf = L'f'$ . Let  $f$  be an element of  $(P, \circ)$ . The operator  $L$  is an isomorphism mapping  $(P, \circ)$  to  $(A, \oplus)$ . Thus,  $Lf = h$  is a unique element of  $(A, \oplus)$ . By Theorem 4. 13 there is a unique element  $f' \in (P, \#)$  such that  $h = L'f'$ . Also,  $L'$  is an isomorphism mapping

$(P, \#)$  to  $(A, \oplus)$  making its inverse mapping an isomorphism from  $(A, \oplus)$  to  $(P, \#)$ . Hence,  $\alpha$ , being the composition of two isomorphisms, is also an isomorphism. This completes the direct proof of Corollary 4.1.

### The Exponential Operator $E$

The operator  $L$  maps the set  $P$  to the set  $A$ . Theorem 4.5 showed  $L$  to be a one-to-one onto mapping. Thus, the inverse mapping from  $A$  to  $P$  exists and is also one-to-one and onto. This inverse mapping is given the name  $E$  by the

Definition 4.14. If  $h \in A$ , let  $Eh$  be the unique element  $f$  of  $P$  such that  $h = Lf$ .

All one-to-one onto mappings and their inverses exhibit the first two properties of  $E$  recorded in the theorem below. The last two properties of  $E$  follow readily from the definitions and previous results.

Theorem 4.20. (a)  $L(Eh) = h$  for every  $h \in A$ .

(b)  $E(Lf) = f$  for every  $f \in P$ .

(c)  $E(f \oplus g) = Ef \circ Eg$  for every  $f, g \in A$ .

(d)  $E(\theta) = \varepsilon$  where  $\theta(n) = 0$  for  $n$  a

positive integer.

Proof of (c): Let  $f$  and  $g$  be arbitrary elements of  $A$  with  $f_1$  and  $g_1$  the corresponding elements of  $P$  as determined by Theorem 4.5, that is,  $f = Lf_1$  and  $g = Lg_1$ . Then  $E(f \oplus g) = E(Lf_1 \oplus Lg_1)$  by substitution. Theorem 4.4 yields  $E(f \oplus g) = E(L(f_1 \circ g_1))$ , and thus

$E(f \oplus g) = f_1 \circ g_1$  by property (b). But  $f_1 = Ef$  and  $g_1 = Eg$  by property (b), so  $E(f \oplus g) = EfoEg$  as was to be shown.

Proof of (d): Since  $\varepsilon(n) = 1$  if  $n = 1$  and is zero otherwise,  $L\varepsilon(n) = 0$  for all  $n$ . Thus  $L\varepsilon = \theta$  which implies, by Theorem 4.5 and property (b), that  $E(\theta) = \varepsilon$ .

### General Powers of Arithmetic Functions

The properties of the operators  $E$  and  $L$  developed so far show the similarity between these operators and the usual exponential and logarithm operators. Definition 4.15 allows for the natural extension of these properties as exhibited in Theorem 4.21.

Definition 4.15. If  $f \in P$ , and  $r$  is any real number, define  $f^r = E(rLf)$ .

Theorem 4.21. For real numbers  $r$  and  $s$  and arithmetic functions  $f$  and  $g$  the following statements are true:

$$(a) \quad (f^r)^s = f^{rs},$$

$$(b) \quad f^{r+s} = f^r \circ f^s,$$

and

$$(c) \quad (f \circ g)^r = f^r \circ g^r,$$

Proof: Definition 4.15 gives the result  $(f^r)^s = E(sLf^r) = E(sL(E(rLf)))$ . Theorem 4.20 simplifies this result to  $(f^r)^s = E(srLf)$ . The commutativity of multiplication in the reals and another application of Definition 4.15 changes this expression to the desired form proving part (a).

By Definition 4.15,  $f^{r+s} = E((r+s)Lf)$ . But  $A$  is a vector space over the reals so  $f^{r+s} = E(rLf \oplus sLf)$ . Theorem 4.20 and Definition

4.15 can be used to obtain  $f^{r+s} = E(rLf) \circ E(sLf) = f^r \circ f^s$ , proving part (b).

To prove part (c), Definition 4.15 is used to obtain  $(f \circ g)^r = E(rL(f \circ g))$ . Using Theorem 4.4 and a property of vector spaces,  $(f \circ g)^r = E(r(Lf \oplus Lg)) = E(rLf \oplus rLg)$ . Theorem 4.20 and Definition 4.15 reduce this expression to the desired form, that is,  $(f \circ g)^r = E(rLf) \circ E(rLg) = f^r \circ g^r$ .

It is possible to obtain some special results of the above theorem by suitable restrictions on the real number  $r$ . Two such results are recorded in:

Theorem 4.22.

(a) If  $r$  is a positive integer and  $f \in A$ , then

$$f^r = f \circ f \circ \dots \circ f, \text{ to } r \text{ factors.}$$

(b) If  $r = -1$ ,  $f \circ f^{-1} = \varepsilon$ , that is,  $f^{-1}$  is the inverse of  $f$  under convolution product.

Proof: If  $r$  is a positive integer then, by definition,  $f^r = E(rLf)$ .

Using a vector space property this can be written

$f^r = E(Lf \oplus Lf \oplus \dots \oplus Lf)$ , to  $r$  addends. An obvious extension of Theorem 4.4 and an application of Theorem 4.20 completes the proof of Part (a), that is,  $f^r = E(L(f \circ f \circ \dots \circ f)) = f \circ f \circ \dots \circ f$ , to  $r$  factors.

If  $r = -1$  Definition 4.15 implies that  $f \circ f^{-1} = E(Lf) \circ E(-Lf)$ .

Theorem 4.20 completes the proof of part (b), that is,

$$f \circ f^{-1} = E(Lf \oplus (-Lf)) = E(\theta) = \varepsilon.$$

The mapping  $\gamma: P \rightarrow A$  defined by  $\gamma(f) = f^r$ , where  $r$  is a non-zero real number, exhibits several interesting properties. These properties and a major result appear in the following theorem.



Theorem 4.23. If  $r$  is a real number and  $f \in P$ , then  $f^r \in P$ .

Proof: If  $r = 0$  then  $f^r = \varepsilon$  is an element of  $P$  since  $\varepsilon(1) = 1 > 0$ .  
 Let  $r$  be any non-zero real number. If  $f \in P$  then  $f(1) > 0$ . By definition,  $f^r = E(rLf)$  so  $Lf^r = rLf$  by Theorem 4.20. By the definition of  $L$ ,  $\log f^r(1) = Lf^r(1) = rLf(1) = r \log f(1)$ . Since  $f(1) > 0$ ,  $\log f(1)$  is a finite real number and the same is true of  $r \log f(1)$ . Thus  $\log f^r(1)$  is also a finite real number making  $f^r(1) > 0$ . Therefore,  $f^r \in P$ .

Theorem 4.24. Let  $r$  be a non-zero real number and  $f \in P$ .

The equation  $g^r = f$  is uniquely solvable for  $g$  and the solution is  $g = f^{1/r}$ .

Proof: By definition, if  $f = g^r$  then  $f = E(rLg)$ . Hence  $Lf = rLg$ . Since  $r \neq 0$  this equation can be written  $\frac{1}{r} Lf = Lg$ . But this equation implies that  $E(\frac{1}{r} Lf) = E(Lg)$ , and finally  $f^{1/r} = g$ . The uniqueness of the result is a consequence of Definition 4.14.

It was proven in Chapter II that the inverse of a multiplicative function relative to convolution product is again a multiplicative function; also, that the convolution product of two multiplicative functions is again a multiplicative function. It is not difficult to see from this that  $f^k$  is multiplicative if  $f$  is multiplicative and  $k$  is an integer. The next theorem extends this result to all real numbers  $k$ .

Theorem 4.25. If  $f \in M$ , then  $f^r \in M$  for every real number

$r$ .

Proof: By Theorem 4.6, if  $f \in M$  then  $Lf(n) = 0$  whenever  $n$  is not a power of a prime. But  $rLf(n) = 0$  whenever  $Lf(n) = 0$ . Now  $rLf = L(E(rLf))$ , so the function  $E(rLf) = f^r$  is multiplicative by Theorem 4.6.

A mapping is called an automorphism if it is an isomorphism mapping a group onto itself. One of the properties of the mapping  $\gamma$  defined prior to Theorem 4.23 is that  $\gamma$  is an automorphism of the group  $(P, \circ)$ .

Theorem 4.26. For each non-zero real number  $r$ , the mapping  $\gamma: P \rightarrow P$  defined by  $\gamma(f) = f^r$  is an automorphism of the group  $(P, \circ)$  which leaves invariant the subgroup  $(M, \circ)$ .

Proof: Theorem 4.24 shows the mapping  $\gamma$  to be one-to-one and onto with the proper domain and range while Theorem 4.25 shows the subgroup  $(M, \circ)$  to be left invariant by  $\gamma$ . It remains to be shown that  $\gamma$  is a homomorphism. Let  $f$  and  $g$  be elements of  $P$ . The following is a straight forward calculation using the properties developed to this point. Thus,

$$\begin{aligned} \gamma(f \circ g) &= (f \circ g)^r = E(rL(f \circ g)) \\ &= E(r(Lf \oplus Lg)) = E(rLf \oplus rLg) \\ &= E(rLf) \circ E(rLg) = f^r \circ g^r \\ &= \gamma(f) \circ \gamma(g), \end{aligned}$$

which shows  $\gamma$  to be a homomorphism. This completes the proof of the theorem.

### Trigonometric Operators

It has been pointed out that the operators  $L$  and  $E$  have properties quite similar to usual logarithm and exponential operators. Noting that the elementary hyperbolic trigonometric functions of analysis are defined in terms of the exponential operator it is natural to investigate the properties of the corresponding trigonometric operators defined in terms of the operator  $E$ . As it turns out, it is possible to prove all the identities corresponding to the usual hyperbolic trigonometric identities. As a fringe benefit of this investigation two operations will be defined on the set  $A$  and the resulting groups shown to be isomorphic to  $(A, \oplus)$ . The investigation is initiated by defining the operators  $S$ ,  $C$ , and  $T$  mapping  $A$  into  $A$  as follows:

Definition 4.16. If  $f \in A$ , let

$$Sf = \frac{1}{2} (Ef \ominus E(-f)) ,$$

$$Cf = \frac{1}{2} (Ef \oplus E(-f)) , \quad \text{and}$$

$$Tf = Sf \circ (Cf)^{-1} .$$

The symbol  $\ominus$  is interpreted as follows:  $f \ominus g = f \oplus (-g)$ . For  $f \in A$ , each of  $Ef$ ,  $E(-f)$ ,  $-E(f)$ , and  $-E(-f)$  are well defined arithmetic functions. Thus,  $Sf$  and  $Cf$  are also well defined arithmetic functions. For  $Tf$  to be well defined it suffices to show that  $(Cf)^{-1}$  exists for each  $f \in A$ . For  $f \in A$ ,  $Cf(1) = \frac{1}{2} (Ef(1) \oplus E(-f(1)))$ . Since  $f(1) = f(1) \cdot \log e = \log e^{f(1)} = L e^{f(1)}$ , it follows that  $Ef(1) = e^{f(1)}$ . Likewise  $E(-f(1)) = e^{-f(1)}$ . Thus,  $Cf(1) = \frac{1}{2} (e^{f(1)} + e^{-f(1)}) = \cosh f(1) > 0$ . Therefore,  $Cf \in P$  and hence,  $(Cf)^{-1}$  exists.

Many of the analogues of the hyperbolic trigonometric identities will be proven. Some of these identities will be used to prove the isomorphisms to follow. Most of the proofs of the identities follow from elementary manipulations.

Identity 4.1.  $Sf = -S(-f)$ , corresponding to  $\sinh x = -\sinh(-x)$ .

$$\begin{aligned} \text{Proof: } -S(-f) &= -\frac{1}{2} (E(-f) \ominus E(-(-f))) = \frac{1}{2} (-E(-f) \oplus E(f)) \\ &= \frac{1}{2} (E(f) \ominus E(-f)) = Sf . \end{aligned}$$

Identity 4.2.  $Cf = C(-f)$ , corresponding to  $\cosh x = \cosh(-x)$ .

$$\text{Proof: } C(-f) = \frac{1}{2} (E(-f) \oplus E(-(-f))) = \frac{1}{2} (E(f) \oplus E(-f)) = Cf .$$

Identity 4.3.  $Tf = -T(-f)$  corresponding to  $\tanh x = -\tanh(-x)$ .

$$\text{Proof: } -T(-f) = -[S(-f) \circ (C(-f))^{-1}] = -[Sf \circ (Cf)^{-1}] = Sf \circ (Cf)^{-1} = Tf .$$

Instrumental in the proof of many of the identities to follow is to recall that  $(A, \oplus, \circ)$  is a commutative ring with identity. In particular,  $\circ$  distributes over both  $\oplus$  and  $\ominus$ .

Identity 4.4.  $S(2f) = 2(Sf \circ Cf)$ , corresponding to  $\sinh 2x = 2 \sinh x \cdot \cosh x$ .

Proof:

$$\begin{aligned} 2(Sf \circ Cf) &= 2(Cf \circ Sf) = 2 \cdot \frac{1}{2} (Ef \oplus E(-f)) \circ \frac{1}{2} (Ef \ominus E(-f)) \\ &= \frac{1}{2} [Ef \circ Ef \ominus E(-f) \circ E(-f)] = \frac{1}{2} [E(f \oplus f) \ominus E(-f \oplus -f)] \\ &= \frac{1}{2} [E(2f) \ominus E(-2f)] = S(2f) . \end{aligned}$$

Identity 4.5.  $(Cf)^2 \ominus (Sf)^2 = \varepsilon$ , corresponding to  
 $\cosh^2 x - \sinh^2 x = 1$ .

$$\begin{aligned} \text{Proof: } (Cf)^2 \ominus (Sf)^2 &= \left\{ \frac{1}{2} [Ef \oplus E(-f)] \right\}^2 \ominus \left\{ \frac{1}{2} [Ef \ominus E(-f)] \right\}^2 \\ &= \frac{1}{4} [Ef \circ Ef \oplus 2Ef \circ E(-f) \oplus E(-f) \circ E(-f)] \\ &\ominus \frac{1}{4} [Ef \circ Ef \ominus 2Ef \circ E(-f) \oplus E(-f) \circ E(-f)] \\ &= E(f \oplus -f) = E(\theta) = \varepsilon . \end{aligned}$$

Identity 4.6.  $C(2f) = (Cf)^2 \oplus (Sf)^2$ , corresponding to  
 $\cosh(2x) = \cosh^2 x + \sinh^2 x$ .

$$\begin{aligned} \text{Proof: } (Cf)^2 \oplus (Sf)^2 &= \left\{ \frac{1}{2} [Ef \oplus E(-f)] \right\}^2 \oplus \left\{ \frac{1}{2} [Ef \ominus E(-f)] \right\}^2 \\ &= \frac{1}{4} [Ef \circ Ef \oplus 2Ef \circ E(-f) \oplus E(-f) \circ E(-f)] \\ &\oplus \frac{1}{4} [Ef \circ Ef \ominus 2Ef \circ E(-f) \oplus E(-f) \circ E(-f)] \\ &= \frac{1}{2} [E(f \oplus f) \oplus E(-f \oplus -f)] = C(2f) . \end{aligned}$$

Two other identities for  $C(2f)$  follow immediately from  
 Identities 4.5 and 4.6. They are given without proof.

Identity 4.7.  $C(2f) = 2(Sf)^2 \oplus \varepsilon$ , corresponding to  
 $\cosh 2x = 2 \sinh^2 x + 1$ .

Identity 4.8.  $C(2f) = 2(Cf)^2 \ominus \varepsilon$ , corresponding to  
 $\cosh 2x = 2 \cosh^2 x - 1$ .

Identity 4.9.  $T(2f) = 2Tf \circ (\varepsilon \oplus (Tf)^2)^{-1}$ , corresponding to  
 $\tanh 2x = 2 \tanh x \div (1 + \tanh^2 x)$ .

Proof:  $2Tf \circ (\varepsilon \oplus (Tf)^2)^{-1} = 2Tf \circ [\varepsilon \oplus (Sf \circ (Cf)^{-1})^2]^{-1}$

$$\begin{aligned}
&= 2Sf \circ (Cf)^{-1} \circ \{[(Cf)^2 \oplus (Sf)^2] \circ (Cf)^{-2}\}^{-1} \\
&= 2Sf \circ (Cf)^{-1} \circ [C(2f)]^{-1} \circ (Cf)^2 \\
&= 2Sf \circ Cf \circ [C(2f)]^{-1} \\
&= S(2f) \circ [C(2f)]^{-1} = T(2f) .
\end{aligned}$$

Identity 4.10.  $Sf \oplus ((Sf)^2 \oplus \varepsilon)^{1/2} = Ef$ , corresponding to  $\sinh x + (\sinh^2 x + 1)^{1/2} = \exp x$ .

Proof: The key step in the proof is the use of Identity 4.5. Thus,

$$\begin{aligned}
Sf \oplus ((Sf)^2 \oplus \varepsilon)^{1/2} &= Sf \oplus Cf \\
&= \frac{1}{2} [Ef \ominus E(-f)] \oplus \frac{1}{2} [Ef \oplus E(-f)] \\
&= Ef .
\end{aligned}$$

Identity 4.11.  $S(f \oplus g) = Sf \circ Cg \oplus Cf \circ Sg$ , corresponding to  $\sinh(x \pm y) = \sinh x \cdot \cosh y \pm \cosh x \cdot \sinh y$ .

Proof: The proof for  $\oplus$  is given. The proof for  $\ominus$  follows in a similar manner.

$$\begin{aligned}
Sf \circ Cg \oplus Cf \circ Sg &= \frac{1}{2} [Ef \ominus E(-f)] \circ \frac{1}{2} [Eg \oplus E(-g)] \\
&\oplus \frac{1}{2} [Ef \oplus E(-f)] \circ \frac{1}{2} [Eg \ominus E(-g)] \\
&= \frac{1}{4} [Ef \circ Eg \ominus E(-f) \circ Eg \oplus Ef \circ E(-g) \\
&\ominus E(-f) \circ E(-g) \oplus Ef \circ Eg \\
&\ominus Ef \circ E(-g) \oplus E(-f) \circ Eg \ominus E(-f) \circ E(-g)] \\
&= \frac{1}{2} [E(f \oplus g) \ominus E(-(f \oplus g))] = S(f \oplus g) .
\end{aligned}$$

Identity 4. 12.  $C(f \oplus g) = Cf \circ Cg \oplus Sf \circ Sg$  , corresponding to  $\cosh(x \pm y) = \cosh x \cdot \cosh y \pm \sinh x \cdot \sinh y$  .

Proof:

$$\begin{aligned}
 Cf \circ Cg \oplus Sf \circ Sg &= \frac{1}{2} [Ef \oplus E(-f)] \circ \frac{1}{2} [Eg \oplus E(-g)] \\
 &\oplus \frac{1}{2} [Ef \ominus E(-f)] \circ \frac{1}{2} [Eg \ominus E(-g)] \\
 &= \frac{1}{4} [Ef \circ Eg \oplus E(-f) \circ Eg \oplus Ef \circ E(-g) \oplus E(-f) \circ E(-g)] \\
 &\oplus [Ef \circ Eg \oplus E(-f) \circ Eg \oplus Ef \circ E(-g) \ominus E(-f) \circ E(-g)] \\
 &= \frac{1}{2} [E(f \oplus g) \oplus E(-(f \oplus g))] = C(f \oplus g) .
 \end{aligned}$$

The proof for  $\ominus$  follows in a similar manner.

Identity 4. 13.  $T(f \oplus g) = (Tf \oplus Tg) \circ (\varepsilon \oplus Tf \circ Tg)^{-1}$  , corresponding to  $\tanh(x \pm y) = (\tanh x \pm \tanh y) \div (1 \pm \tanh x \cdot \tanh y)$  .

Proof: The proof for  $\oplus$  is given. By the definition of T and Identities 4. 11 and 4. 12,

$$\begin{aligned}
 T(f \oplus g) &= S(f \oplus g) \circ [C(f \oplus g)]^{-1} \\
 &= [Sf \circ Cg \oplus Cf \circ Sg] \circ [Cf \circ Cg \oplus Sf \circ Sg]^{-1} .
 \end{aligned}$$

Convoluting this result with  $\varepsilon = (Cf)^{-1} \circ (Cg)^{-1} \circ [(Cf)^{-1} \circ (Cg)^{-1}]^{-1}$  gives the desired result,

$$T(f \oplus g) = (Tf \oplus Tg) \circ (\varepsilon \oplus Tf \circ Tg)^{-1} .$$

The proof for  $T(f \ominus g)$  is similar.

Identity 4. 14.  $S(\frac{1}{2} f) = [\frac{1}{2} (Cf \ominus \varepsilon)]^{1/2}$  , corresponding to  $\sinh(\frac{1}{2} x) = [\frac{1}{2} (\cosh x - 1)]^{1/2}$  .

$$\begin{aligned}
\text{Proof: } \frac{1}{2} (Cf \ominus \varepsilon) &= \frac{1}{2} \left[ \frac{1}{2} (Ef \oplus E(-f)) \ominus \varepsilon \right] = \frac{1}{4} [Ef \ominus 2E(\theta) \oplus E(-f)] \\
&= \frac{1}{4} [E(\frac{1}{2}f) \circ E(\frac{1}{2}f) \ominus 2E(\frac{1}{2}f) \circ E(-\frac{1}{2}f) \oplus E(-\frac{1}{2}f) \circ E(-\frac{1}{2}f)] \\
&= \frac{1}{2} [E(\frac{1}{2}f) \ominus E(-\frac{1}{2}f)] \circ \frac{1}{2} [E(\frac{1}{2}f) \ominus E(-\frac{1}{2}f)] = (S(\frac{1}{2}f))^2 .
\end{aligned}$$

Therefore,  $S(\frac{1}{2}f) = [\frac{1}{2}(Cf \ominus \varepsilon)]^{1/2}$ .

Identity 4.15.  $C(\frac{1}{2}f) = [\frac{1}{2}(Cf \oplus \varepsilon)]^{1/2}$ , corresponding to  $\cosh(\frac{1}{2}x) = [\frac{1}{2}(\cosh x + 1)]^{1/2}$ .

The proof of this identity follows the pattern used to prove Identity 4.14, hence, it is omitted.

Identity 4.16.  $T(\frac{1}{2}f) = (Cf \ominus \varepsilon) \circ (Sf)^{-1} = Sf \circ (Cf \oplus \varepsilon)^{-1}$ , corresponding to  $\tanh(\frac{1}{2}x) = (\cosh x - 1) \div \sinh x = \sinh x \div (\cosh x + 1)$ .

Proof: Since  $Cf$  and  $\varepsilon$  are elements of  $P$  it follows that  $(Cf \oplus \varepsilon)$  is also an element of  $P$ . Thus,  $(Cf \oplus \varepsilon)^{-1}$  exists for each  $f$  in  $A$ . Since  $Sf(1) = \frac{1}{2} [Ef(1) - E(-f(1))] = \frac{1}{2} (e^{f(1)} - e^{-f(1)}) = \sinh f(1) = 0$  if and only if  $f(1) = 0$ ,  $(Sf)^{-1}$  exists if and only if  $f(1) \neq 0$ . Thus, the middle expression of the identity is well defined for arithmetic functions  $f$  such that  $f(1) \neq 0$ . Assuming this restriction to be satisfied, the definition of  $T$  implies that  $T(\frac{1}{2}f) = S(\frac{1}{2}f) \circ (C(\frac{1}{2}f))^{-1}$ . Convoluting with  $\varepsilon = S(\frac{1}{2}f) \circ (S(\frac{1}{2}f))^{-1}$  gives the result

$$T(\frac{1}{2}f) = (S(\frac{1}{2}f))^2 \circ [S(\frac{1}{2}f) \circ C(\frac{1}{2}f)]^{-1} .$$

By using identity 4.4 and Identity 4.14 the desired result is obtained.

Thus,

$$T(\frac{1}{2}f) = \frac{1}{2}(Cf \ominus \varepsilon) \circ (\frac{1}{2}Sf)^{-1} = (Cf \ominus \varepsilon) \circ (Sf)^{-1} ,$$



proving the first result. The second result is proved in a similar manner. Using Identity 4.15,

$$\begin{aligned} T\left(\frac{1}{2}f\right) &= S\left(\frac{1}{2}f\right) \circ C\left(\frac{1}{2}f\right) \circ [C\left(\frac{1}{2}f\right)]^{-2} \\ &= \frac{1}{2}Sf \circ \left[\frac{1}{2}(Cf \oplus \varepsilon)\right]^{-1} \\ &= Sf \circ (Cf \oplus \varepsilon)^{-1} . \end{aligned}$$

Identity 4.17.  $Sf \oplus Sg = 2S\left(\frac{1}{2}(f \oplus g)\right) \circ C\left(\frac{1}{2}(f \oplus g)\right)$ , corresponding to  $\sinh x + \sinh y = 2 \sinh \frac{1}{2}(x+y) \cdot \cosh \frac{1}{2}(x-y)$ .

Proof:  $2S\left(\frac{1}{2}(f \oplus g)\right) \circ C\left(\frac{1}{2}(f \oplus g)\right) = 2 \cdot \frac{1}{2} [E\left(\frac{1}{2}(f \oplus g)\right) \ominus E\left(-\frac{1}{2}(f \oplus g)\right)]$

$$\begin{aligned} &\circ \frac{1}{2} [E\left(\frac{1}{2}(f \oplus g)\right) \oplus E\left(-\frac{1}{2}(f \oplus g)\right)] \\ &= \frac{1}{2} [Ef \oplus Eg \ominus E(-g) \ominus E(-f)] \\ &= \frac{1}{2} [Ef \ominus E(-f)] \oplus \frac{1}{2} [Eg \ominus E(-g)] \\ &= Sf \oplus Sg . \end{aligned}$$

The other three factorization identities can be proven in exactly the same manner. For this reason they are stated without proof.

Identity 4.18.  $Sf \ominus Sg = 2C\left(\frac{1}{2}(f \oplus g)\right) \circ S\left(\frac{1}{2}(f \oplus g)\right)$ , corresponding to  $\sinh x - \sinh y = 2 \cosh \frac{1}{2}(x-y) \cdot \sinh \frac{1}{2}(x-y)$ .

Identity 4.19.  $Cf \oplus Cg = 2C\left(\frac{1}{2}(f \oplus g)\right) \circ S\left(\frac{1}{2}(f \oplus g)\right)$ , corresponding to  $\sinh x - \sinh y = 2 \cosh \frac{1}{2}(x+y) \cdot \sinh \frac{1}{2}(x-y)$ .

Identity 4.20.  $Cf \ominus Cg = 2S\left(\frac{1}{2}(f \oplus g)\right) \circ S\left(\frac{1}{2}(f \oplus g)\right)$ , corresponding to  $\cosh x - \cosh y = 2 \sinh \frac{1}{2}(x+y) \cdot \sinh \frac{1}{2}(x-y)$ .

These twenty identities, although not exhausting the known hyperbolic trigonometric identities, illustrate that a complete analogy does exist between the operators  $S$ ,  $C$ , and  $T$  and the operators  $\sinh$ ,  $\cosh$ , and  $\tanh$ . The discovery of such analogies in mathematics frequently provide insight into the mathematical structure of one or both of the areas. In this particular case, some of the identities proven above will be instrumental in observing two additional structures that can be placed upon the set  $A$  of all arithmetic functions. The following lemmas will prove a major portion of the theorem describing the first of these two structures.

$$\underline{\text{Lemma 4.8.}} \quad S(f \oplus g) = Sf \circ ((Sg)^2 \oplus \epsilon)^{1/2} \oplus Sg \circ ((Sf)^2 \oplus \epsilon)^{1/2} .$$

Proof: By Identity 4.11,  $S(f \oplus g) = Sf \circ Cg \oplus Cf \circ Sg$ . Using Identity 4.5 it is easily seen that  $Cg = ((Sf)^2 \oplus \epsilon)^{1/2}$  and  $Cf = ((Sg)^2 \oplus \epsilon)^{1/2}$ .

Making these substitutions in Identity 4.11 and commuting about the second convolution gives the desired result.

$$\underline{\text{Lemma 4.9.}} \quad \text{If } Sf = Sg \text{ then } f = g .$$

Proof: From Identity 4.10,  $Sf \oplus ((Sf)^2 \oplus \epsilon)^{1/2} = Ef$ . Thus, if  $Sf = Sg$ , then  $Ef = Eg$ . Therefore, by Definition 4.14,  $f = g$ .

$$\underline{\text{Lemma 4.10.}} \quad Sf = h \text{ if } f = L(h \oplus (h^2 \oplus \epsilon)^{1/2}) .$$

Proof: Let  $g = h \oplus (h^2 \oplus \epsilon)^{1/2}$ . Using the definition of  $S$  and making the expected substitutions,

$$\begin{aligned} Sf &= \frac{1}{2}(Ef \ominus E(-f)) = \frac{1}{2}(E(Lg) \ominus E(-Lg)) \\ &= \frac{1}{2}(g \ominus g^{-1}) . \end{aligned}$$

This last equality follows from Definition 4.15 and Theorem 4.20. Convoluting with  $\varepsilon = g \circ g^{-1}$  this result can be written

$$Sf = \frac{1}{2}(g^2 \ominus \varepsilon) \circ g^{-1}.$$

Replacing  $g$  by the expression involving  $h$  above and simplifying the resulting expression gives the desired result. Thus,

$$\begin{aligned} Sf &= \frac{1}{2}[(h \oplus (h^2 \oplus \varepsilon)^{1/2}) \circ (h \oplus (h^2 \oplus \varepsilon)^{1/2}) \ominus \varepsilon] \circ g^{-1} \\ &= \frac{1}{2}[h^2 \oplus 2h \circ (h^2 \oplus \varepsilon)^{1/2} \oplus h^2 \oplus \varepsilon \ominus \varepsilon] \circ g^{-1} \\ &= \frac{1}{2}[2h \circ (h \oplus (h^2 \oplus \varepsilon)^{1/2})](h \oplus (h^2 \oplus \varepsilon)^{1/2})^{-1} \\ &= h. \end{aligned}$$

Recall that the operator  $L$  maps the set  $P$  to the set  $A$ . The proof will be completed by showing that for each  $h$  in  $A$ ,  $g = h \oplus (h^2 \oplus \varepsilon)^{1/2}$  is in  $P$ . Suppose  $h(1) = r$ , where  $r$  is a real number. Then  $g(1) = r + (r^2 + 1)^{1/2} > r + |r| \geq 0$ . Therefore,  $g$  is in  $P$ .

Mappings that are isomorphisms are powerful tools in proving the equivalence of algebraic structures. The method used previously herein has been to define a mapping from one group to another group, show it to be an isomorphism, and to conclude that the two groups are isomorphic. In contrast, if the set  $G$  is a group under a given operation and  $H$  is a set and  $f: G \rightarrow H$  is an isomorphism, then  $H$  is a group under the operation induced by the mapping  $f$  and the operation on  $G$ .

The next theorem uses a slight alteration of the second use of isomorphisms mentioned above. If  $G$  is a group under a given operation and  $H$  is a set with an operation defined on it and  $f: G \rightarrow H$  is an

isomorphism that preserves the given operations on  $G$  and  $H$ , then  $H$  is a group under its given operation.

Theorem 4.27. Let  $\square$  denote the binary operation on  $A$  defined by  $f \square g = f \circ (g^2 \oplus \epsilon)^{1/2} \oplus g \circ (f^2 \oplus \epsilon)^{1/2}$  for each  $f, g \in A$ . Then the system  $(A, \square)$  forms a group which is isomorphic to  $(A, \oplus)$ .

Proof: Let  $\beta: (A, \oplus) \rightarrow (A, \square)$  by  $\beta: f \rightarrow Sf$ . It will be shown that  $\beta$  is an isomorphism that preserves the operations  $\oplus$  and  $\square$ .

By the definition of  $S$ ,  $Sf \in A$  whenever  $f \in A$ . Thus, the domain and range of  $\beta$  are as they should be. By Lemma 4.9,  $\beta$  is a one-to-one mapping while, by Lemma 4.10,  $\beta$  maps  $A$  onto  $A$ . Let  $f, g \in A$ . By the definition of  $\beta$  and Lemma 4.8,

$$\beta(f \oplus g) = S(f \oplus g) = Sf \circ ((Sg)^2 \oplus \epsilon)^{1/2} \oplus Sg \circ ((Sf)^2 \oplus \epsilon)^{1/2}.$$

Now  $Sf$  and  $Sg$  are elements of  $A$ . By the definitions of  $\square$  and of  $\beta$  this result can be written

$$\beta(f \oplus g) = Sf \square Sg = \beta f \square \beta g.$$

Thus,  $\beta$  is an isomorphism. Noting that each element of  $A$  can be expressed as  $Sf$  where  $f$  is also an element of  $A$ , it is seen by Lemma 4.8 that the operation  $\square$  is identical with the operation induced by  $\beta$ . Therefore,  $(A, \oplus) \approx (A, \square)$ , and  $(A, \square)$  is a group.

It is not difficult to show directly that  $(A, \square)$  is a group. Since elements of  $(A, \square)$  may be represented by  $Sf, Sg$ , and  $Sh$ , where  $f, g$  and  $h$  are elements of  $(A, \oplus)$ , Lemma 4.8 immediately shows that

$$Sf \square Sg = S(f \oplus g).$$

Since  $f \oplus g \in A$  whenever  $f, g \in A$ , this equation shows  $(A, \square)$  to be closed. This same equation and the associativity of  $\oplus$  lead to an easy proof of the associativity of  $\square$ . This same equation can also be used to show that  $S\theta$  is the identity for  $\square$  and  $-Sf = S(-f)$  is the inverse of  $Sf$  in  $(A, \square)$ . Thus,  $(A, \square)$  is a group.

The operator  $T$ , like the operator  $S$ , leads to the definition of an operation  $\Delta$  on a subset of  $A$ . The theorem to follow will show this subset  $V$  with its operation  $\Delta$  isomorphic to  $(A, \oplus)$ . The lemmas preceding the theorem prove a major portion of it.

Lemma 4.11. If  $f \in A$ , then  $E(2f) = (\varepsilon \oplus Tf) \circ (\varepsilon \ominus Tf)^{-1}$ .

Proof: From a property of the operator  $E$  and the obvious identity  $Ef = Ef$  it follows that

$$E(2f) \circ E(-f) = Ef.$$

Since  $Cf \ominus Sf = E(-f)$  and  $Cf \oplus Sf = Ef$ , the last equation becomes

$$E(2f) \circ (Cf \ominus Sf) = Cf \oplus Sf.$$

Convolving both sides of this equation with  $(Cf)^{-1}$  and the resulting equation with  $(\varepsilon \ominus Tf)^{-1}$  gives the results:

$$E(2f) \circ (\varepsilon \ominus Sf \circ (Cf)^{-1}) = \varepsilon \oplus Sf \circ (Cf)^{-1},$$

and

$$E(2f) = (\varepsilon \oplus Tf) \circ (\varepsilon \ominus Tf)^{-1}, \text{ respectively.}$$

The existence of  $(\varepsilon \ominus Tf)^{-1}$  must be shown. Since  $Tf(1) = (\exp f(1) - \exp(-f(1))) / (\exp f(1) + \exp(-f(1))) = \tanh f(1)$ , and  $-1 < \tanh f(1) < 1$  for each  $f \in A$ , it follows that  $(\varepsilon \ominus Tf) \in P$ . Hence,

$(\epsilon \oplus Tf)^{-1}$  exists, This completes the proof of the lemma.

Definition 4.17. Let  $V = \{f \in A \mid -1 < f(1) < 1\}$ . Let  $\Delta$  be an operation on  $V$  defined by  $f \Delta g = (f \oplus g) \circ (\epsilon \oplus f \circ g)^{-1}$  for each  $f, g \in V$ .

To show that  $\Delta$  is a closed binary operation on  $V$  it must be shown that  $(\epsilon \oplus f \circ g) \in P$  and that  $f \Delta g \in V$  whenever  $f, g \in V$ . If  $f, g \in V$  then  $-1 < f(1) < 1$  and  $-1 < g(1) < 1$ . Since  $\epsilon(1) = 1$  it follows that  $(\epsilon \oplus f \circ g)(1) > 0$  and thus  $(\epsilon \oplus f \circ g) \in P$ . Showing  $f \Delta g \in V$  is equivalent to showing  $|x+y| < |1+xy|$  for all real numbers  $x$  and  $y$  such that  $|x| < 1$  and  $|y| < 1$ . There are four cases to consider.

If  $x \geq 0$  and  $y \geq 0$ , then  $|x+y| < |1+xy|$  if and only if  $x+y < 1+xy$ . But this is equivalent to the statement  $x(1-y)+y < 1$ . Since  $0 \leq y < 1$  and  $0 \leq x < 1$ , it follows that  $x(1-y)+y < 1-y+y = 1$ . This completes the proof if  $x$  and  $y$  are nonnegative.

If  $x < 0$  and  $y < 0$  let  $|x| = a$  and  $|y| = b$ . Then  $|x+y| < |1+xy|$  if and only if  $a+b < 1+ab$ . The proof follows exactly as in the first case.

If  $x \leq 0$  and  $y \geq 0$ , let  $|x| = a$ , and suppose  $|x| \leq |y|$ . Then  $|x+y| < |1+xy|$  if and only if  $y-a < 1-ay$ . Equivalently,  $y+a(y-1) < 1$ . But  $y-1 < 0$ , so  $y+a(y-1) \leq y < 1$ . The proof of the case where  $|y| \leq |x|$  is completely similar.

Since the statement to be proven is symmetric in  $x$  and  $y$ , the case  $y \leq 0$  and  $x \geq 0$  is included above. Thus,  $\Delta$  has been shown to be a closed binary operation on  $V$ . It is well defined since the operations of sum and convolution product are well defined on  $A$ .

Lemma 4.12.  $Tf = h$  if  $f = \frac{1}{2}L(\varepsilon \oplus h) \ominus \frac{1}{2}L(\varepsilon \ominus h)$ .

Proof: By the definitions of  $T$ ,  $S$ , and  $C$ , and the obvious substitution for  $f$ ,

$$\begin{aligned} Tf &= Sf \circ (Cf)^{-1} = \frac{1}{2}[Ef \ominus E(-f)] \circ \left\{ \frac{1}{2}[Ef \oplus E(-f)] \right\}^{-1} \\ &= \frac{1}{2} [E \{ \frac{1}{2} L(\varepsilon \oplus h) \ominus \frac{1}{2} L(\varepsilon \ominus h) \} \ominus E \{ \frac{1}{2} L(\varepsilon \ominus h) \oplus \frac{1}{2} L(\varepsilon \oplus h) \}] \\ &\circ \left\{ \frac{1}{2} [E \{ \frac{1}{2} L(\varepsilon \oplus h) \oplus \frac{1}{2} L(\varepsilon \ominus h) \} \oplus E \{ \frac{1}{2} L(\varepsilon \ominus h) \ominus \frac{1}{2} L(\varepsilon \oplus h) \}] \right\}^{-1}. \end{aligned}$$

Using Theorem 4.20 and Definition 4.15, this expression becomes

$$\begin{aligned} Tf &= \frac{1}{2} [E(\frac{1}{2}L(\varepsilon \oplus h)) \circ E(-\frac{1}{2}L(\varepsilon \ominus h)) \ominus E(\frac{1}{2}L(\varepsilon \ominus h)) \circ E(-\frac{1}{2}L(\varepsilon \oplus h))] \\ &\circ \left\{ \frac{1}{2} [E(\frac{1}{2}L(\varepsilon \oplus h)) \circ E(-\frac{1}{2}L(\varepsilon \ominus h)) \oplus E(\frac{1}{2}L(\varepsilon \ominus h)) \circ E(-\frac{1}{2}L(\varepsilon \oplus h))] \right\}^{-1} \\ &= \frac{1}{2} [(\varepsilon \oplus h)^{1/2} \circ (\varepsilon \ominus h)^{-1/2} \ominus (\varepsilon \ominus h)^{1/2} \circ (\varepsilon \oplus h)^{-1/2}] \\ &\circ \left\{ \frac{1}{2} [(\varepsilon \oplus h)^{1/2} \circ (\varepsilon \ominus h)^{-1/2} \oplus (\varepsilon \ominus h)^{1/2} \circ (\varepsilon \oplus h)^{-1/2}] \right\}^{-1}. \end{aligned}$$

Convoluting the right side of this expression with

$\varepsilon = (\varepsilon \oplus h)^{1/2} \circ (\varepsilon \ominus h)^{1/2} \circ (\varepsilon \oplus h)^{-1/2} \circ (\varepsilon \ominus h)^{-1/2}$ , the result is

$$\begin{aligned} Tf &= \frac{1}{2} [(\varepsilon \oplus h) \circ \varepsilon \ominus (\varepsilon \ominus h) \circ \varepsilon] \circ \left\{ \frac{1}{2} [(\varepsilon \oplus h) \circ \varepsilon \oplus (\varepsilon \ominus h) \circ \varepsilon] \right\}^{-1} \\ &= \frac{1}{2} [2h] \circ \left\{ \frac{1}{2} [2\varepsilon] \right\}^{-1} \\ &= h \circ \varepsilon^{-1} = h. \end{aligned}$$

Lemma 4.13. If  $Tf = Tg$ , then  $f = g$ .

Proof: If  $Tf = Tg$ , then  $(\varepsilon \oplus Tf) \circ (\varepsilon \ominus Tf)^{-1} = (\varepsilon \oplus Tg) \circ (\varepsilon \ominus Tg)^{-1}$ .

Thus, by Lemma 4.11,  $E(2f) = E(2g)$ . Definition 4.14 implies  $2f = 2g$ , whence  $f = g$ .

This section is concluded with Theorem 4.28.

Theorem 4.28. Let  $V$  and  $\Delta$  be defined as in Definition 4.17. Then the system  $(V, \Delta)$  forms a group which is isomorphic to  $(A, \oplus)$ .

Proof: Let  $\gamma: A \rightarrow V$  by  $\gamma: f \rightarrow Tf$ . It will be shown that  $\gamma(A) \subset V$  and that  $\gamma$  is an isomorphism of the group  $(A, \oplus)$  and the set  $V$  with the operation  $\Delta$  on  $V$  being preserved by  $\gamma$ .

Let  $f \in A$ . Since  $Sf(1) = \sinh f(1)$  and  $Cf(1) = \cosh f(1)$ ,  $Tf(1) = \tanh f(1)$ . Also,  $-1 < \tanh f(1) < 1$  for each  $f \in A$  by property of  $\tanh$ . Thus  $Tf \in V$  whenever  $f \in A$ . This shows that  $\gamma(A) \subset V$ .

For each  $h$  in  $V$  the function  $f = \frac{1}{2}L(\epsilon \oplus h) \ominus \frac{1}{2}L(\epsilon \ominus h)$  is an element of  $A$  which has the property, by Lemma 4.12, that  $Tf = h$ . Therefore,  $\gamma$  maps  $A$  onto  $V$ . By Lemma 4.13,  $\gamma$  is a one-to-one mapping.

Let  $f, g \in A$ . By the definition of  $\gamma$  and Identity 4.13,

$$\gamma(f \oplus g) = T(f \oplus g) = (Tf \oplus Tg) \circ (\epsilon \oplus Tf \circ Tg)^{-1}.$$

Now  $Tf$  and  $Tg$  are elements of  $V$ . By the definitions of  $\Delta$  and of  $\gamma$  this result can be written

$$\gamma(f \oplus g) = Tf \Delta Tg = \gamma(f) \Delta \gamma(g).$$

Thus,  $\gamma$  is an isomorphism. Since each element of  $V$  can be expressed as  $Tf$  where  $f$  is an element of  $A$ , it is seen by Identity 4.13 that the operation  $\Delta$  is identical with the operation induced by  $\gamma$ . Therefore,  $(A, \oplus) \approx (V, \Delta)$ , and  $(V, \Delta)$  is a group.

It is not difficult to show directly that  $(V, \Delta)$  is a group. Since elements of  $(V, \Delta)$  may be represented by  $Tf$ ,  $Tg$ , and  $Th$ ,



where  $f$ ,  $g$ , and  $h$  are elements of  $(A, \oplus)$ , Identity 4.13 can be used to show  $V$  closed and associative under  $\Delta$ . The identity for  $\Delta$  in  $V$  is  $T\theta$ , where  $\theta$  is the zero function. If  $Tf$  is an element of  $V$  then  $-Tf = T(-f)$  is the inverse of  $Tf$  in  $V$ .

### Extension to Complex Algebras

Some of the previous results of this chapter can be extended to the set of complex valued arithmetic functions. Several sets of arithmetic functions will be discussed in this section. For reference, they are recorded as:

Definition 4.18. The sets  $A'$ ,  $P'$ ,  $M'$ , and  $A_1$  are given by:

- (1)  $A' = \{f \mid f \text{ is a complex valued arithmetic function}\}$ ,
- (2)  $P' = \{f \in A' \mid f(1) \text{ is real and positive}\}$ ,
- (3)  $M' = \{f \in A' \mid f \text{ is multiplicative}\}$ ,
- (4)  $A_1 = \{f \in A' \mid f(1) \text{ is real}\}$ .

By Theorem 3.1,  $(A', \oplus)$  is a commutative group. Now  $A_1 \subset A'$ , and if  $f(1)$  and  $g(1)$  are real, then certainly  $-f(1)$  and  $(f \oplus g)(1)$  are also real. Thus,  $(A_1, \oplus)$  is a subgroup of  $(A', \oplus)$ . Hence,  $(A_1, \oplus)$  is a commutative group.

The systems  $(P', \circ)$ ,  $(P', \#)$ ,  $(M', \circ)$ , and  $(M', \#)$  have been shown to be commutative groups. For future reference, these results are included in a lemma.

Lemma 4.14. The systems  $(A', \oplus)$ ,  $(P', \circ)$ ,  $(P', \#)$ ,  $(M', \circ)$ ,  $(M', \#)$ , and  $(A_1, \oplus)$  are commutative groups.

The primary purpose of this section is to prove the

Theorem 4.29. The groups  $(P', \circ)$ ,  $(M', \circ)$ ,  $(P', \#)$ ,  $(M', \#)$ , and  $(A', \oplus)$  are all isomorphic to each other and to each of the groups  $(P, \circ)$ ,  $(M, \circ)$ ,  $(P, \#)$ ,  $(M, \#)$ ,  $(A, \oplus)$ ,  $(A, \square)$ , and  $(V, \Delta)$ .

The proof of this theorem will consist of basically two parts. The first part will show that the group  $(A, \oplus)$  is isomorphic to each of the first four groups named in the theorem. The second part of the proof will consist of showing the groups  $(A', \oplus)$ ,  $(A, \oplus)$ , and  $(A_1, \oplus)$  to be isomorphic to each other. The methods and the proofs used in proving Theorem 4.3 can be followed to prove the first part. The corresponding theorems and definitions needed to show  $(P', \circ)$ ,  $(M', \circ)$ , and  $(A_1, \oplus)$  isomorphic will be stated.

Theorem 4.30.  $A_1$  is a vector space over  $R$ , the field of real numbers. Also,  $(A_1, \oplus, \circ)$  is a commutative algebra over  $R$  denoted by  $(A_1, \oplus, \circ, \cdot)$ .

Definition 4.19. If  $f \in P'$ , let

$$L_1 f(n) = \sum_{d|n} f(d) f^{-1}(n/d) \log d \quad \text{if } n > 1,$$

and

$$L_1 f(1) = \log f(1),$$

Observe that for  $L_1: P' \rightarrow A_1$ ,  $f^{-1}$  denotes the inverse of  $f$  with respect to convolution product.

Theorem 4.31. For all  $f, g \in P'$ ,  $L_1(f \circ g) = L_1 f \oplus L_1 g$ .

The proof of this theorem will be facilitated by an additional definition and two supporting lemmas.

Definition 4.20. Define the operator  $\lambda: A_1 \rightarrow A_1$  by  $\lambda f(n) = f(n) \cdot \log n$ ,  $n$  a positive integer.

The proofs of the next few lemmas and theorems are analogous to those using the logarithm operator  $L$  and hence are omitted. The proof of Theorem 4.31 is included to fortify the analogy.

Lemma 4.15. If  $n > 1$ ,  $L_1 f(n) = (f^{-1} \circ \lambda f)(n)$  for each  $f \in A_1$ .

Lemma 4.16. If  $f, g \in A_1$ , then  $\lambda(f \circ g) = g \circ \lambda f \oplus f \circ \lambda g$ .

Now to prove Theorem 4.31. Let  $f$  and  $g$  be elements of  $P^1$ . If  $n = 1$ , then

$$\begin{aligned} L_1(f \circ g)(1) &= \log(f \circ g)(1) = \log f(1) g(1) \\ &= \log f(1) + \log g(1) \\ &= L_1 f(1) + L_1 g(1) = (L_1 f \oplus L_1 g)(1). \end{aligned}$$

Now let  $n > 1$ . By Lemma 4.16, it is true that

$$\lambda(f \circ g) = g \circ \lambda f \oplus f \circ \lambda g.$$

Taking the convolution product of both sides of this expression with  $f^{-1} \circ g^{-1}$ , recalling that  $(A_1, \oplus, \circ)$  is a commutative ring, the following expression is obtained:

$$(f \circ g)^{-1} \circ \lambda(f \circ g) = f^{-1} \circ \lambda f \oplus g^{-1} \circ \lambda g.$$

By Lemma 4.15 this expression reduces to the desired expression.

Thus,

$$L_1(f \circ g) = L_1 f \oplus L_1 g.$$

Theorem 4.32. For each  $h \in A_1$  there is a unique  $f \in P'$  such that  $h = L_1 f$ .

Theorem 4.33. A function  $f \in P'$  is multiplicative if, and only if,  $L_1 f(n) = 0$  whenever  $n$  is not a power of a prime.

Definition 4.21. Let

$$D_1 = \{h \in A_1 \mid h = L_1 f, f \in P', h(n) = 0 \text{ if } n \text{ is not a prime power}\}.$$

Lemma 4.17.  $(D_1, \oplus)$  is a subgroup of  $(A_1, \oplus)$ .

Theorem 4.34.  $(P', \circ) \approx (A_1, \oplus)$ .

Theorem 4.35.  $(M', \circ) \approx (D_1, \oplus)$ .

Theorem 4.36.  $(D_1, \oplus) \approx (A_1, \oplus)$ .

Theorem 4.37.  $(M', \circ) \approx (A_1, \oplus)$ .

Theorem 4.38.  $(M', \circ) \approx (P', \circ)$ .

The same sequence of theorems, definitions, and lemmas could be stated in terms of unitary product instead of convolution product. Their proofs would follow in a similar manner with only minor changes. Thus, the proof of the first part of Theorem 4.29 has been outlined. The second part of the proof of Theorem 4.29 will consist of two lemmas.

Lemma 4.18.  $(A, \oplus) \approx (A', \oplus)$ .

Proof: Let  $\alpha: A \rightarrow A'$  by  $\alpha f(n) = f(2n-1) + if(2n)$ , for each  $f \in A$  and each positive integer  $n$ . Notice that  $\alpha f \in A'$  whenever  $f \in A$ . The

function  $\alpha$  is certainly well defined since  $f$  is well defined and the image of  $f(n)$  is determined by well defined operations in the complex field. To prove the lemma it suffices to show that  $\alpha$  is an isomorphism.

To show  $\alpha$  is an onto map let  $g \in A'$ . Then  $g(n) = a_n + i b_n$ , where  $a_n$  and  $b_n$  are real numbers, for each positive integer  $n$ . Define inductively the function  $f$  by:  $f(1) = a_1$ ,  $f(2) = b_1$ ,  $f(3) = a_2$ ,  $f(4) = b_2$ , and in general,  $f(2n-1) = a_n$  and  $f(2n) = b_n$ , for each positive integer  $n$ . Certainly  $f \in A$ , and, by the definition of  $f$ ,  $\alpha f = g$ . Therefore,  $\alpha$  maps  $A$  onto  $A'$ .

To show  $\alpha$  is one-to-one, suppose  $\alpha f_1 = g_1$  and  $\alpha f_2 = g_2$ , where  $f_1 \neq f_2$ . Then there exists a positive integer  $n$  such that  $f_1(n) \neq f_2(n)$ . If  $n$  is odd then there exists a positive integer  $m$  such that  $n = 2m - 1$ . Hence,  $\text{Real}\{g_1(m)\} = f_1(2m-1) \neq f_2(2m-1) = \text{Real}\{g_2(m)\}$ . If  $n$  is even then there exists a positive integer  $k$  such that  $n = 2k$ . Hence,  $\text{Imag}\{g_1(k)\} = f_1(2k) \neq f_2(2k) = \text{Imag}\{g_2(k)\}$ . Therefore,  $\alpha$  is a one-to-one mapping.

To show  $\alpha$  is a homomorphism let  $f$  and  $g$  be elements of  $A$  and let  $n$  be a positive integer. By the definition of  $\alpha$ ,

$$\begin{aligned} \alpha(f \oplus g)(n) &= (f \oplus g)(2n-1) + i(f \oplus g)(2n) \\ &= f(2n-1) + g(2n-1) + i(f(2n) + g(2n)) \\ &= (f(2n-1) + i f(2n)) + (g(2n-1) + i g(2n)) \\ &= \alpha f(n) + \alpha g(n) \\ &= (\alpha f \oplus \alpha g)(n). \end{aligned}$$

Thus,  $\alpha$  is a homomorphism. Consequently,  $\alpha$  is an isomorphism and  $(A, \oplus) \approx (A', \oplus)$ .

Lemma 4.19.  $(A, \oplus) \approx (A_1, \oplus)$ .

Proof: Let  $\beta: A \rightarrow A_1$  by  $\beta f(1) = f(1)$ , and  $\beta f(n) = f(2n-2) + if(2n-1)$  if  $n > 1$ , for each  $f \in A$ . Since  $f(1)$  is real,  $\beta f \in A_1$  whenever  $f \in A$ . The function  $\beta$  is well defined since  $f$  is well defined and the image of  $f(n)$  is a well defined complex number for each positive integer  $n$ . To prove the lemma it suffices to show that  $\beta$  is an isomorphism.

To show  $\beta$  is an onto map let  $g \in A_1$ . Then  $g(1)$  is a real number and  $g(n) = a_n + ib_n$ , where  $a_n$  and  $b_n$  are real numbers, for each positive integer  $n > 1$ . Define inductively a function  $f$  by:  $f(1) = g(1)$ ,  $f(2) = a_2$ ,  $f(3) = b_2$ ,  $f(4) = a_3$ ,  $f(5) = b_3$ , and in general,  $f(2n-2) = a_n$  and  $f(2n-1) = b_n$  for each positive integer  $n > 1$ . Certainly  $f \in A$ , and by the definition of  $f$ ,  $\beta f = g$ . Therefore,  $\beta$  maps  $A$  onto  $A_1$ .

To show  $\beta$  is one-to-one, suppose  $\beta f_1 = g_1$  and  $\beta f_2 = g_2$ , where  $f_1 \neq f_2$ . Then there exists a positive integer  $n$  such that  $f_1(n) \neq f_2(n)$ . If  $n = 1$ , then  $g_1(1) \neq g_2(1)$ . If  $n > 1$  and  $n$  is odd then there exists a positive integer  $m$ ,  $m > 1$ , such that  $n = 2m - 1$ . In this case  $\text{Imag}\{g_1(m)\} = f_1(2m-1) \neq f_2(2m-1) = \text{Imag}\{g_2(m)\}$ . If  $n > 1$  and  $n$  is even then there exists a positive integer  $k$ ,  $k > 1$ , such that  $n = 2k - 2$  and  $\text{Real}\{g_1(k)\} = f_1(2k-2) \neq f_2(2k-2) = \text{Real}\{g_2(k)\}$ . Therefore,  $\beta$  is a one-to-one mapping.

To show  $\beta$  is a homomorphism let  $f$  and  $g$  be elements of  $A$  and let  $n$  be a positive integer. If  $n = 1$ , then

$$\begin{aligned} \beta(f \oplus g)(1) &= (f \oplus g)(1) = f(1) + g(1) \\ &= \beta f(1) + \beta g(1) = (\beta f \oplus \beta g)(1). \end{aligned}$$

If  $n > 1$ , then

$$\begin{aligned}
 \beta(f \oplus g)(n) &= (f \oplus g)(2n-2) + i(f \oplus g)(2n-1) \\
 &= f(2n-2) + if(2n-1) + g(2n-2) + ig(2n-1) \\
 &= \beta f(n) + \beta g(n) \\
 &= (\beta f \oplus \beta g)(n) .
 \end{aligned}$$

Thus,  $\beta$  is a homomorphism. Consequently,  $\beta$  is an isomorphism and  $(A, \oplus) \approx (A_1, \oplus)$ .

Several applications of the transitive property of the equivalence relation "is isomorphic to" completes the proof of Theorem 4.29.

## CHAPTER V

### CONVOLUTIONS WITH THE MOBIUS FUNCTION

This chapter will concern itself exclusively with the set  $M$  of multiplicative functions under convolution product. In a previous chapter  $(M, \circ)$  was shown to be a commutative group. Many interesting relationships are known to exist within the group of multiplicative functions. For example, in Chapter II the following relationships were established:  $\mu \circ \nu = \varepsilon$ ,  $\nu \circ \nu = \tau$ ,  $\iota \circ \nu = \sigma$ , and  $\tau \circ \varphi = \sigma$ .

This chapter will focus on some interesting results that are obtained by convoluting powers of the Mobius function with some of the well known multiplicative functions. For example,  $\mu^k \circ \varphi$  will be investigated. Here, if  $k > 0$ ,  $\mu^k$  represents the convolution  $\mu \circ \mu \circ \dots \circ \mu$  with  $k$  factors; if  $k < 0$ ,  $\mu^k$  represents the convolution  $\mu^{-1} \circ \mu^{-1} \circ \dots \circ \mu^{-1}$  with  $|k|$  factors; and  $\mu^0 = \varepsilon$ . Since all functions to be considered are multiplicative it will suffice to consider the argument to be of the form  $p^\alpha$ ,  $\alpha \geq 0$ ,  $p$  a prime.

Formulas for  $\mu^k \circ \varphi$ ,  $\mu^k \circ \sigma$ , and  $\mu^k \circ \iota$

The formulas developed in this section are stated in terms of the following notation:  $\{p^\alpha(1 - 1/p)^n\}$  denotes the expression obtained by expanding the binomial term, multiplying formally by  $p^\alpha$  and retaining only the terms having non-negative exponents. Thus, if  $n \geq 0$ ,



$$\{p^\alpha(1-1/p)^n\} = p^\alpha - \binom{n}{1} p^{\alpha-1} + \binom{n}{2} p^{\alpha-2} \dots + (-1)^\alpha \binom{n}{\alpha}$$

where  $\binom{n}{i}$  is the binomial coefficient and is zero if  $i > n$ . Also,

$$\{p^\alpha(1-1/p)^{-n}\} = p^\alpha + \binom{n}{1} p^{\alpha-1} + \binom{n+1}{2} p^{\alpha-2} + \dots + \binom{n+\alpha+1}{\alpha}.$$

Notice that the two expressions agree for  $n=0$ .

The following lemmas will be needed to prove the first major result of this section.

Lemma 5.1. If  $0 \leq i < k$ , then  $\binom{k}{i} + \binom{k}{i+1} = \binom{k+1}{i+1}$ .

Proof: If  $k=1$ , then  $i=0$  and  $\binom{1}{0} + \binom{1}{1} = 1+1 = 2 = \binom{2}{1}$ . Suppose that for  $0 \leq i < k < n$  the lemma is true. Let  $k=n$ . If  $i=0$ , then  $\binom{n}{0} + \binom{n}{1} = 1+n = \binom{n+1}{1}$ . Suppose the lemma is true for  $0 \leq i < j < n$ . Let  $i=j$ . Then

$$\begin{aligned} \binom{n}{j} + \binom{n}{j+1} &= \frac{n!}{j!(n-j)!} + \frac{n!}{(j+1)!(n-j-1)!} \\ &= \frac{(j+1)n!}{(j+1)!(n-j)!} + \frac{(n-j)n!}{(j+1)!(n-j)!} \\ &= \frac{(n+1)!}{(j+1)!(n-j)!} = \binom{n+1}{j+1}. \end{aligned}$$

This completes the proof.

Lemma 5.2. If  $k \geq 0$ ,

$$\{p^\alpha(1-1/p)^k\} - \{p^{\alpha-1}(1-1/p)^k\} = \{p^\alpha(1-1/p)^{k+1}\}.$$

Proof: Let  $k \geq 0$ . By the definition of the notation,

$$\{p^\alpha(1-1/p)^k\} = p^\alpha - \binom{k}{1} p^{\alpha-1} + \binom{k}{2} p^{\alpha-2} - \dots + (-1)^\alpha \binom{k}{\alpha}$$

and

$$\{p^{\alpha-1}(1-1/p)^k\} = p^{\alpha-1} - \binom{k}{1} p^{\alpha-2} + \binom{k}{2} p^{\alpha-3} - \dots + (-1)^{\alpha-1} \binom{k}{\alpha-1}.$$

Since  $\binom{k}{i} + \binom{k}{i+1} = \binom{k+1}{i+1}$  by Lemma 5.1, grouping like powers of  $p$  in the difference of the two expressions above yields

$$p^\alpha - \binom{k+1}{1} p^{\alpha-1} + \binom{k+1}{2} p^{\alpha-2} - \dots + (-1)^\alpha \binom{k+1}{\alpha} = \{p^\alpha(1-1/p)^{k+1}\}.$$

This completes the proof.

Lemma 5.3. Let  $n$  be any positive integer and  $k$  any non-negative integer. Then

$$\sum_{i=0}^k \binom{n+i-1}{i} = \binom{n+k}{k}.$$

Proof: The proof is by induction on  $n$ . Let  $n=1$ . The lemma is true for  $k=0$  since  $\binom{1-1}{0} = 1 = \binom{1+0}{0}$ . Suppose that the lemma is true for  $n=1$  and for  $0 \leq k < j$ . Let  $k=j$ . Then

$$\sum_{i=0}^j \binom{n+i-1}{i} = \sum_{i=0}^{j-1} \binom{n+i-1}{i} + \binom{n+j-1}{j}.$$

Using the induction hypothesis and then Lemma 5.1 the manipulation becomes

$$\sum_{i=0}^j \binom{n+i-1}{i} = \binom{n+j-1}{j-1} + \binom{n+j-1}{j} = \binom{n+j}{j},$$

completing this part of the induction.

Suppose that the lemma is true for  $1 \leq n < m$  and for all  $k \geq 0$ . Let  $n=m$ . If  $k=0$  the lemma follows since  $\binom{m-1}{0} = 1 = \binom{m+0}{0}$ . Suppose the lemma is true for  $n=m$  and  $0 \leq k < j$ . Let  $k=j$ . Then

$$\begin{aligned} \sum_{i=0}^j \binom{m+i-1}{i} &= \sum_{i=0}^{j-1} \binom{m+i-1}{i} + \binom{m+j-1}{j} \\ &= \binom{m+j-1}{j-1} + \binom{m+j-1}{j} = \binom{m+j}{j}, \end{aligned}$$

exactly as in the induction above. This completes the proof of the lemma.

Lemma 5.4. If  $\alpha$  and  $n$  are non-negative integers, then

$$\sum_{i=0}^{\alpha} \{p^i(1-1/p)^{-n}\} = \{p^{\alpha}(1-1/p)^{-n-1}\}.$$

Proof: By definition,

$$\{p^i(1-1/p)^{-n}\} = p^i + \binom{n}{1} p^{i-1} + \binom{n+1}{2} p^{i-1} + \dots + \binom{n+i-1}{i}.$$

Thus,

$$\begin{aligned} \sum_{i=0}^{\alpha} \{p^i(1-1/p)^{-n}\} &= p^{\alpha} + p^{\alpha-1} \left[ 1 + \binom{n}{1} \right] \\ &\quad + p^{\alpha-2} \left[ 1 + \binom{n}{1} + \binom{n+1}{2} \right] + \dots + \left[ \sum_{i=0}^{\alpha} \binom{n+i-1}{i} \right]. \end{aligned}$$

But  $\sum_{i=0}^k \binom{n+i-1}{i} = \binom{n+k}{k}$  by Lemma 5.3. Hence,

$$\begin{aligned} \sum_{i=0}^{\alpha} \{p^i(1-1/p)^{-n}\} &= p^{\alpha} + \binom{n+1}{1} p^{\alpha-1} + \binom{n+2}{2} p^{\alpha-2} + \dots + \binom{n+\alpha}{\alpha} \\ &= \{p^{\alpha}(1-1/p)^{-n-1}\}, \end{aligned}$$

which completes the proof.

The first of three major results of this section is contained in the following theorem.

Theorem 5.1. Let  $k$  be any integer,  $\alpha$  any non-negative integer, and  $p$  a prime. Then

$$(\mu^k \circ \varphi)(p^\alpha) = \{p^\alpha(1-1/p)^{k+1}\} .$$

Proof: The proof of the theorem is by induction on  $k$ . Since  $(\mu^k \circ \varphi)(1) = 1 = \{(1-1/p)^{k+1}\}$ , the theorem is verified for  $\alpha = 0$ . The consideration of  $\alpha > 0$  is divided into two cases.

Case I.  $k \geq 0$ . If  $k=0$ ,

$$(\mu^0 \circ \varphi)(p^\alpha) = \varphi(p^\alpha) = p^\alpha(1-1/p) = \{p^\alpha(1-1/p)\} .$$

Suppose  $k=1$ . Since  $\mu(p^i) = 0$  if  $i \geq 2$ ,

$$\begin{aligned} (\mu \circ \varphi)(p^\alpha) &= \varphi(p^\alpha) - \varphi(p^{\alpha-1}) \\ &= p^\alpha(1-1/p) - p^{\alpha-1}(1-1/p) \\ &= \{p^\alpha(1-1/p)\} - \{p^{\alpha-1}(1-1/p)\} \\ &= \{p^\alpha(1-1/p)^2\} , \end{aligned}$$

by Lemma 5.2. This verifies the lemma for  $k=0$  and  $k=1$ .

To complete the induction for  $k$  non-negative, assume that for  $1 \leq s < k$ ,  $(\mu^s \circ \varphi)(p^\alpha) = \{p^\alpha(1-1/p)^{s+1}\}$ . If  $s=k$ , then

$$\begin{aligned} (\mu^k \circ \varphi)(p^\alpha) &= [\mu \circ (\mu^{k-1} \circ \varphi)](p^\alpha) \\ &= (\mu^{k-1} \circ \varphi)(p^\alpha) - (\mu^{k-1} \circ \varphi)(p^{\alpha-1}) \\ &= \{p^\alpha(1-1/p)^k\} - \{p^{\alpha-1}(1-1/p)^k\} \end{aligned}$$

$$= \{p^\alpha (1-1/p)^{k+1}\}.$$

The last two equalities follow from the induction hypothesis and Lemma 5.2, respectively.

Case II,  $k < 0$ . Let  $k = -m$  where  $m > 0$ . Since  $\mu^{-1} = \nu$ , it follows that  $\mu^k = \mu^{-m} = \nu^m$ . Thus, it suffices to show that  $(\nu^m \circ \varphi)(p^\alpha) = \{p^\alpha (1-1/p)^{-m+1}\}$ . The proof is by induction on  $m$ .

First notice that

$$(\nu \circ f)(p^\alpha) = \sum_{d|p^\alpha} \nu(p^\alpha/d) f(d) = \sum_{i=0}^{\alpha} f(p^i).$$

Let  $m=1$ . Then

$$(\nu \circ \varphi)(p^\alpha) = \sum_{i=0}^{\alpha} \varphi(p^i) = p^\alpha = \{p^\alpha (1-1/p)^0\},$$

verifying the result for  $m=1$ .

Suppose that  $(\nu^s \circ \varphi)(p^\alpha) = \{p^\alpha (1-1/p)^{-s+1}\}$  for  $1 \leq s < m$ .

Let  $s=m$ . Then

$$\begin{aligned} (\nu^m \circ \varphi)(p^\alpha) &= [\nu \circ (\nu^{m-1} \circ \varphi)](p^\alpha) = \sum_{i=0}^{\alpha} (\nu^{m-1} \circ \varphi)(p^i) \\ &= \sum_{i=0}^{\alpha} \{p^i (1-1/p)^{-m+2}\} = \{p^\alpha (1-1/p)^{-m+1}\}. \end{aligned}$$

The last two equalities follow from the induction hypothesis and Lemma 5.4, respectively. This completes the proof of the theorem.

The remaining two major results of this section follow easily from the first result. Each is preceded by a lemma.

Lemma 5.5. If  $k$  is an integer then  $\mu^k \circ \sigma = \mu^{k-2} \circ \varphi$ .

Proof: Since  $\sigma = \tau \circ \varphi$  and  $\tau = \nu \circ \nu$ , it follows that  $\sigma = \nu \circ \nu \circ \varphi = \mu^{-2} \circ \varphi$ . Convoluting both sides with  $\mu^k$  gives the desired result, that is,  $\mu^k \circ \sigma = \mu^{k-2} \circ \varphi$ .

Corollary 5.1. Let  $k$  be any integer,  $\alpha$  any non-negative integer, and  $p$  a prime. Then

$$(\mu^k \circ \sigma)(p^\alpha) = \{p^\alpha (1-1/p)^{k-1}\}.$$

Proof: The proof follows immediately from Lemma 5.5 and Theorem 5.1. Hence,

$$(\mu^k \circ \sigma)(p^\alpha) = (\mu^{k-2} \circ \varphi)(p^\alpha) = \{p^\alpha (1-1/p)^{k-1}\}.$$

Lemma 5.6. If  $k$  is an integer then  $\mu^k \circ \iota = \mu^{k+1} \circ \sigma$ .

Proof: Since  $\iota \circ \nu = \sigma$  it follows that  $\iota = \mu \circ \sigma$ . Convoluting both sides with  $\mu^k$  gives the desired result, that is,  $\mu^k \circ \iota = \mu^{k+1} \circ \sigma$ .

Corollary 5.2. Let  $k$  be any integer,  $\alpha$  any non-negative integer, and  $p$  a prime. Then

$$(\mu^k \circ \iota)(p^\alpha) = \{p^\alpha (1-1/p)^k\}.$$

Proof: The proof follows immediately from Lemma 5.6 and Corollary 5.1. Hence,

$$(\mu^k \circ \iota)(p^\alpha) = (\mu^{k+1} \circ \sigma)(p^\alpha) = \{p^\alpha (1-1/p)^k\}.$$

Since the functions  $\mu^k \circ \varphi$ ,  $\mu^k \circ \sigma$ , and  $\mu^k \circ \iota$  are multiplicative, the formulas displayed in Theorem 5.1 and its corollaries define

completely the evaluations of these functions. The similarity in these formulas seem to suggest that the functions  $\varphi$ ,  $\sigma$ , and  $\iota$  can be placed together in some system of classification. As will be seen in the next section, the functions  $\tau$ ,  $\varepsilon$ , and  $\nu$  also behave in a similar manner to each other when convoluted with powers of  $\mu$ , a manner quite different from the functions  $\varphi$ ,  $\sigma$ , and  $\iota$ .

Formulas for  $\mu^k \circ \tau$ ,  $\mu^k \circ \varepsilon$ ,  $\mu^k \circ \nu$ , and  $\mu^k$

In this section formulas for the multiplicative functions  $\mu^k \circ \tau$ ,  $\mu^k \circ \varepsilon$ , and  $\mu^k \circ \nu$  will be developed. Since these functions are multiplicative it suffices to consider the argument to be a power of a prime. As will be seen, the formulas developed will depend only upon the value of  $k$  and the power to which the prime is raised. The prime itself will not appear in the evaluation.

A by-product of this investigation will be the construction of what is sometimes referred to as the negative Pascal triangle. The negative Pascal triangle contains the binomial coefficients in the expansion of  $(1 \pm x)^n$  for  $n$  an integer and  $x^2 < 1$ . The well known Pascal triangle is a subset of the negative Pascal triangle and hence will be produced in this section as well. All of this information will be contained in a table to appear later in this section.

The first result is contained in the

Theorem 5.2. Let  $k$  be any integer,  $\alpha$  any non-negative integer, and  $p$  a prime. Then

$$(\mu^k \circ \tau)(p^\alpha) = \binom{-k+1+\alpha}{\alpha}, \quad \text{if } k \leq 1, \quad \text{and}$$

$$(\mu^k \circ \tau)(p^\alpha) = (-1)^\alpha \binom{k-2}{\alpha}, \quad \text{if } k \geq 2.$$

Proof: The proof is by induction on  $k$ . Two cases are required.

Case I.  $k \geq 2$ . Since  $\nu \circ \nu = \tau$  it follows that  $\varepsilon = \mu^2 \circ \tau$ .

Thus, if  $\alpha = 0$  and  $k = 2$ ,

$$(\mu^k \circ \tau)(p^\alpha) = \varepsilon(1) = 1 = \binom{0}{0} = (-1)^\alpha \binom{k-2}{\alpha}.$$

Also, if  $\alpha > 0$  and  $k = 2$ ,

$$(\mu^k \circ \tau)(p^\alpha) = \varepsilon(p^\alpha) = 0 = \binom{0}{1} = (-1)^\alpha \binom{k-2}{\alpha}.$$

This verifies the second conclusion of the theorem for  $k = 2$ .

Suppose that the second conclusion of the theorem is valid for  $n$  such that  $2 \leq n < k$  and for all  $\alpha \geq 0$ . Thus,

$$(\mu^n \circ \tau)(p^\alpha) = (-1)^\alpha \binom{n-2}{\alpha}.$$

Let  $n = k$ . If  $\alpha = 0$ , then

$$(\mu^k \circ \tau)(1) = 1 = \binom{k-2}{0} = (-1)^\alpha \binom{k-2}{\alpha}.$$

Assume that  $(\mu^k \circ \tau)(p^j) = (-1)^j \binom{k-2}{j}$  for all  $j$  such that  $0 \leq j < \alpha$ .

Let  $j = \alpha$ . Then

$$\begin{aligned} (\mu^k \circ \tau)(p^\alpha) &= (\mu \circ (\mu^{k-1} \circ \tau))(p^\alpha) \\ &= \mu(1)(\mu^{k-1} \circ \tau)(p^\alpha) + \mu(p)(\mu^{k-1} \circ \tau)(p^{\alpha-1}) \\ &= 1 \cdot (-1)^\alpha \binom{k-3}{\alpha} + (-1)(-1)^{\alpha-1} \binom{k-3}{\alpha-1}, \end{aligned}$$

by the induction hypothesis. Algebraic manipulation and Lemma 5.1 change this result to the desired form. Thus,



$$\begin{aligned}
(\mu^k \circ \tau)(p^\alpha) &= (-1)^\alpha \left[ \binom{k-3}{\alpha} + \binom{k-3}{\alpha-1} \right] \\
&= (-1)^\alpha \binom{k-2}{\alpha},
\end{aligned}$$

which completes the induction and the proof of the theorem in the case where  $k \geq 2$ .

Case II.  $k \leq 1$ . Let  $k=1$ . Since  $\nu \circ \nu = \tau$  it follows that  $\nu = \mu \circ \tau$ . Thus, if  $\alpha \geq 0$ ,

$$(\mu^k \circ \tau)(p^\alpha) = \nu(p^\alpha) = 1 = \binom{\alpha}{\alpha} = \binom{-k+1+\alpha}{\alpha}.$$

This verifies the first conclusion of the theorem for  $k=1$ .

Although it is not essential to the induction to follow, the case for  $k=0$  does more clearly illustrate the formula being established and for this reason it is included. It does make the induction slightly easier to state. If  $k=0$ ,

$$(\mu^k \circ \tau)(p^\alpha) = \tau(p^\alpha) = \alpha + 1 = \binom{\alpha+1}{\alpha} = \binom{-k+1+\alpha}{\alpha}.$$

This verifies the formula for  $k=0$ .

Assume that for  $\alpha \geq 0$  and  $k = -t$ , where  $0 \leq t < m$ ,

$$(\mu^k \circ \tau)(p^\alpha) = \binom{-k+1+\alpha}{\alpha}.$$

Let  $t=m$ . Also let  $f = \mu^{-m+1} \circ \tau$ . If  $\alpha = 0$ ,

$$\begin{aligned}
(\mu^{-m} \circ \tau)(p^\alpha) &= (\mu \circ f)(1) = \mu(1) f(1) \\
&= 1 \cdot \binom{(m-1)+1+0}{0} = \binom{m}{0} \\
&= 1 = \binom{m+1}{0} = \binom{m+1+\alpha}{\alpha}.
\end{aligned}$$

Assume that for  $0 \leq j < \alpha$  and  $0 \leq t \leq m$ ,

$$(\mu^{-t} \circ \tau)(p^j) = \binom{t+1+j}{j}.$$

Let  $j = \alpha$ . Also, let  $g = \mu^{-t+1} \circ \tau$ . Then

$$\begin{aligned} (\mu^{-t} \circ \tau)(p^\alpha) &= (\nu \circ g)(p^\alpha) \\ &= \nu(1)g(p^\alpha) + \nu(p)g(p^{\alpha-1}) + \dots + \nu(p^\alpha)g(1) \\ &= \nu(1)g(p^\alpha) + \sum_{i=1}^{\alpha} \nu(p^i)g(p^{\alpha-i}) \\ &= \nu(1)g(p^\alpha) + \sum_{i=0}^{\alpha-1} \nu(p^i)g(p^{\alpha-1-i}) \\ &= \nu(1)g(p^\alpha) + (\nu \circ g)(p^{\alpha-1}) \\ &= 1 \cdot \binom{t-1+1+\alpha}{\alpha} + (\mu^{-t} \circ \tau)(p^{\alpha-1}) \\ &= \binom{t+\alpha}{\alpha} + \binom{t+1+\alpha-1}{\alpha-1} \\ &= \binom{t+1+\alpha}{\alpha}. \end{aligned}$$

This completes the induction and the proof of the theorem.

The formulas for the other two functions follow easily and are contained in the corollaries below.

Lemma 5.7. If  $k$  is an integer then  $\mu^k \circ \varepsilon = \mu^{k+2} \circ \tau$ .

Proof: Since  $\nu \circ \nu = \tau$  it follows that  $\varepsilon = \mu^2 \circ \tau$ . Convoluting both sides with  $\mu^k$  gives  $\mu^k \circ \varepsilon = \mu^{k+2} \circ \tau$ .

Corollary 5.3. Let  $k$  be any integer,  $\alpha$  any non-negative integer, and  $p$  a prime. Then

$$(\mu^k \circ \varepsilon)(p^\alpha) = \binom{-k-1+\alpha}{\alpha}, \text{ if } k \leq -1, \text{ and}$$

$$(\mu^k \circ \varepsilon)(p^\alpha) = (-1)^\alpha \binom{k}{\alpha}, \text{ if } k \geq 0.$$

Proof: The proof follows from Lemma 5.7 and Theorem 5.2. If  $k \leq -1$ , then

$$(\mu^k \circ \varepsilon)(p^\alpha) = (\mu^{k+2} \circ \tau)(p^\alpha) = \binom{-k-2+1+\alpha}{\alpha} = \binom{-k-1+\alpha}{\alpha}.$$

Also, if  $k \geq 0$ ,

$$(\mu^k \circ \varepsilon)(p^\alpha) = (\mu^{k+2} \circ \tau)(p^\alpha) = (-1)^\alpha \binom{k+2-2}{\alpha} = (-1)^\alpha \binom{k}{\alpha}.$$

Lemma 5.8. If  $k$  is an integer then  $\mu^k \circ \nu = \mu^{k-1} \circ \varepsilon$ .

Proof: Since  $\mu \circ \nu = \varepsilon$ , convoluting both sides with  $\mu^{k-1}$  gives the desired result.

Corollary 5.4. Let  $k$  be any integer,  $\alpha$  any non-negative integer, and  $p$  a prime. Then

$$(\mu^k \circ \nu)(p^\alpha) = \binom{-k+\alpha}{\alpha}, \text{ if } k \leq 0, \text{ and}$$

$$(\mu^k \circ \nu)(p^\alpha) = (-1)^\alpha \binom{k-1}{\alpha}, \text{ if } k \geq 1.$$

Proof: The proof follows from Lemma 5.8 and Corollary 5.3. If  $k \leq 0$ , then

$$(\mu^k \circ \nu)(p^\alpha) = (\mu^{k-1} \circ \varepsilon)(p^\alpha) = \binom{-k+1-1+\alpha}{\alpha} = \binom{-k+\alpha}{\alpha}.$$

Also, if  $k \geq 1$ ,

$$(\mu^k \circ \nu)(p^\alpha) = (\mu^{k-1} \circ \varepsilon)(p^\alpha) = (-1)^\alpha \binom{k-1}{\alpha}.$$

Since  $\mu^k \circ \varepsilon = \mu^k$  for each integer  $k$ , Corollary 5.3 implies

Corollary 5.5. Let  $k$  be any integer,  $\alpha$  any non-negative integer, and  $p$  a prime. Then

$$\mu^k(p^\alpha) = \binom{-k-1+\alpha}{\alpha}, \text{ if } k \leq -1, \text{ and}$$

$$\mu^k(p^\alpha) = (-1)^\alpha \binom{k}{\alpha}, \text{ if } k \geq 0.$$

Table I contains function values of  $(\mu^k \circ \varepsilon)(p^\alpha)$  for  $p$  an arbitrary but fixed prime,  $k$  an integer, and  $\alpha$  a non-negative integer. For a given  $\alpha$  and  $k$ , the entry in the table corresponding to these values will be recognized as the  $(\alpha+1)^{\text{st}}$  coefficient in the expansion of  $(1-x)^k$ , where  $x^2 < 1$ . For example, the seventh coefficient in the expansion of  $(1-x)^{-4}$  is given by  $(\mu^{-4} \circ \varepsilon)(p^6) = 84$ . Also, the fourth coefficient in the expansion of  $(1-x)^6$  is given by  $(\mu^6 \circ \varepsilon)(p^3) = -20$ .

Lemma 5.1 suggests an algorithm by which the entire table may be produced from the first column and any row, in particular, the row corresponding to  $k=0$ . Since  $(1-x)^0 = 1$  for each  $x$  such that  $x^2 < 1$ , the coefficients for  $(1-x)^0$  are  $1, 0, 0, 0, \dots$ . Equivalently, the entries in the row corresponding to  $k=0$  are  $1, 0, 0, 0, \dots$ . Also, for any integer  $k$ , the first coefficient in the expansion of  $(1-x)^k$  is one. Therefore, the column corresponding to  $\alpha=0$  is necessarily an infinite column of ones.

For convenience, let the entry in the table corresponding to  $k=k'$  and  $\alpha=\alpha'$  be denoted by  $(k', \alpha')$ . Thus,  $(-3, 6) = 28$  and

TABLE I  
A PORTION OF THE NEGATIVE  
PASCAL TRIANGLE

| $k \backslash \alpha$ | 0 | 1  | 2  | 3   | 4   | 5   | 6    | 7    | 8    | 9     | 10    |
|-----------------------|---|----|----|-----|-----|-----|------|------|------|-------|-------|
| -8                    | 1 | 8  | 36 | 120 | 330 | 792 | 1716 | 3432 | 6435 | 11440 | 19448 |
| -7                    | 1 | 7  | 28 | 84  | 210 | 462 | 924  | 1716 | 3003 | 5005  | 8008  |
| -6                    | 1 | 6  | 21 | 56  | 126 | 252 | 462  | 792  | 1287 | 2002  | 3003  |
| -5                    | 1 | 5  | 15 | 35  | 70  | 126 | 210  | 330  | 495  | 715   | 1001  |
| -4                    | 1 | 4  | 10 | 20  | 35  | 56  | 84   | 120  | 165  | 220   | 286   |
| -3                    | 1 | 3  | 6  | 10  | 15  | 21  | 28   | 36   | 45   | 55    | 66    |
| -2                    | 1 | 2  | 3  | 4   | 5   | 6   | 7    | 8    | 9    | 10    | 11    |
| -1                    | 1 | 1  | 1  | 1   | 1   | 1   | 1    | 1    | 1    | 1     | 1     |
| 0                     | 1 | 0  | 0  | 0   | 0   | 0   | 0    | 0    | 0    | 0     | 0     |
| 1                     | 1 | -1 | 0  | 0   | 0   | 0   | 0    | 0    | 0    | 0     | 0     |
| 2                     | 1 | -2 | 1  | 0   | 0   | 0   | 0    | 0    | 0    | 0     | 0     |
| 3                     | 1 | -3 | 3  | -1  | 0   | 0   | 0    | 0    | 0    | 0     | 0     |
| 4                     | 1 | -4 | 6  | -4  | 1   | 0   | 0    | 0    | 0    | 0     | 0     |
| 5                     | 1 | -5 | 10 | -10 | 5   | -1  | 0    | 0    | 0    | 0     | 0     |
| 6                     | 1 | -6 | 15 | -20 | 15  | -6  | 1    | 0    | 0    | 0     | 0     |
| 7                     | 1 | -7 | 21 | -35 | 35  | -21 | 7    | -1   | 0    | 0     | 0     |
| 8                     | 1 | -8 | 28 | -56 | 70  | -56 | 28   | -8   | 1    | 0     | 0     |

$(4, 1) = -4$ . Using this notation, Lemma 5.1 implies that  $(k-1, \alpha) + (k, \alpha+1) = (k-1, \alpha+1)$ , for  $k$  an integer and  $\alpha$  a non-negative integer. Geometrically within the table this means that, given any entry in the table, the sum of that entry and the entry that is diagonally below it and to its right is equal to the entry that is immediately to the right of the given entry. Since  $1+0 = 1$ , the "1's" in the row corresponding to  $k = -1$  are easily generated. Also, since  $1+1 = 2$ ,  $2+1 = 3$ ,  $3+1 = 4$ , ..., the entries in the row corresponding to  $k = -2$  can be generated from the row below it. Continuing in this manner the entries in the rows corresponding to  $k = -3, -4, -5, \dots$  can be generated.

The entries for the rows corresponding to  $k = 1, 2, 3, \dots$  can be generated by the same pattern. The problem becomes one of finding the missing addend. Since  $1+(-1) = 0$ ,  $0+0 = 0$ ,  $0+0 = 0, \dots$ , the entries in the row corresponding to  $k = 1$  are  $1, -1, 0, 0, 0, \dots$ . Also, since  $1+(-2) = -1$ ,  $-1+1 = 0$ , and  $0+0 = 0$ , the entries in the row corresponding to  $k = 2$  are  $1, -2, 1, 0, 0, 0, \dots$ . In a similar manner the rest of the rows can be generated.

This table will be called the negative Pascal triangle. The rows above the row corresponding to  $k = 0$ , when taken as a single block of numbers and rotated in the clockwise direction through an angle of 135 degrees, take on the following configuration:

$$\begin{array}{cccccc}
 & & & & & 1 \\
 & & & & & 1 & 1 \\
 & & & & 1 & 2 & 1 \\
 & & & 1 & 3 & 3 & 1 \\
 & & 1 & 4 & 6 & 4 & 1 \\
 1 & 5 & 10 & 10 & 5 & 1 \\
 \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
 \end{array}$$

The student of high school algebra will recognize this triangular array of numbers as the Pascal triangle. The  $n^{\text{th}}$  row of the Pascal triangle contains the binomial coefficients of the expansion of  $(a+b)^{n-1}$ , for  $n$  a positive integer.

This same property can be attributed to the entries in the upper half of Table I. Let  $k$  be non-positive and fixed. The entries on the diagonal line passing through  $k$  with a slope of  $-1$  with the horizontal are the binomial coefficients in the expansion of  $(a+b)^{-k-2}$ . For example, when  $k = -6$ , the coefficients of  $(a+b)^4$  are 1, 4, 6, 4, and 1.

A closer look at the bottom half of Table I shows that, with concern given to convergence, this same property can be attributed to those entries in the bottom half of the table. Thus, the entries on the diagonal line passing through  $k$  with a slope of  $-1$  with the horizontal are the binomial coefficients in the expansion of  $(1+x)^{-k-2}$ ,  $x^2 < 1$ . For example, when  $k = 2$ , the coefficients of  $(1+x)^{-4}$  are 1, -4, 10, -20, 35, -56, . . . .

These last few paragraphs following Corollary 5.5 are intended to describe the properties of and the relationships to be found in Table I. A comparison of the evaluation of  $(\mu^k \circ \epsilon)(p^\alpha)$  given by Corollary 5.3 and the binomial coefficients as displayed on page 370 of the C. R. C. Standard Mathematical Tables, Twelfth Edition [6], proves the implications made here concerning the entries in the table being specific coefficients of certain binomial expansions.

## CHAPTER VI

### SUMMARY AND CONCLUSIONS

A brief history of the development of the theory of algebraic structure as well as an account of the discovery of some of the more common arithmetic functions was included in the first chapter. The second chapter continued with the development of background information. The definition of an arithmetic function was formalized as any function mapping the positive integers into a subset of the complex field  $C$ . Essential definitions, a development of basic properties of the convolution product and unitary product, and a review of the more common arithmetic functions comprised the content of Chapter II.

Chapter III investigated the algebraic structures obtained by defining an addition and several different multiplications on the set  $A$  of arithmetic functions. It was shown that the system  $(A, \oplus)$ , the set of arithmetic functions under sum, is a commutative group. The system  $(A, *)$ , the set of arithmetic functions under ordinary product, was shown to be a commutative monoid. Thus,  $(A, \oplus, *)$  is a commutative ring with unity. However, it is not an integral domain nor is it a division ring.

The system  $(A, \&)$ , the set of arithmetic functions under Cauchy product, is a commutative monoid with no zero divisors. Thus,  $(A, \oplus, \&)$  is an integral domain; however, it is not a division ring. The system  $(A, \circ)$ , the set of arithmetic functions under convolution



product, is a commutative monoid with no zero divisors. Hence,  $(A, \oplus, \circ)$  is an integral domain; however, it is not a division ring. The system  $(A, \#)$ , the set of arithmetic functions under unitary product, is a commutative monoid. This makes  $(A, \oplus, \#)$  a commutative ring with identity. The system is not an integral domain nor is it a division ring.

The pi product  $(\pi)$  and the delta product  $(\delta)$  of arithmetic functions were introduced in order to show examples of rings that are "minimal" in some sense. Pi product is an associative, non-commutative operation that has no identity. Thus, the system  $(A, \oplus, \pi)$  is a ring and it is at most a ring. Delta product is a commutative, non-associative operation that has no identity. Thus, the system  $(A, \oplus, \delta)$  is a commutative non-associative ring and at most a commutative non-associative ring.

In Chapter IV, the set  $A$  was defined to be the set of all real-valued arithmetic functions,  $M$  the set of all multiplicative real-valued functions, and  $P$  the set of all  $f \in A$  such that  $f(1) > 0$ . Also,  $A'$  was defined to be the set of all complex valued arithmetic functions,  $P'$  the set of all  $f \in A'$  such that  $f(1)$  is real and positive, and  $M'$  the set of multiplicative functions in  $A'$ . The main conclusion of the chapter is proving that all of the following groups are isomorphic to each other:  $(P', \circ)$ ,  $(M', \circ)$ ,  $(P', \#)$ ,  $(M', \#)$ ,  $(A', \oplus)$ ,  $(P, \circ)$ ,  $(M, \circ)$ ,  $(P, \#)$ ,  $(M, \#)$ ,  $(A, \oplus)$ ,  $(A, \square)$ , and  $(V, \Delta)$ . The machinery needed to prove these results included a logarithm operator  $L$ , and exponential operator  $E$ , and the trigonometric operators  $S$ ,  $C$ , and  $T$ . These operators were shown to have properties analogous to the logarithm function, the exponential function, and the hyperbolic functions  $\sinh$ ,  $\cosh$ , and

$\tanh$ , respectively. The logarithm operator  $L$  was also shown to provide the following characterization of a multiplicative function: The function  $f \in P$  is multiplicative if and only if  $Lf(n) = 0$  whenever  $n$  is not a power of a prime,

In Chapter V formulas were developed for each of the multiplicative functions  $\mu^k \circ \varphi$ ,  $\mu^k \circ \sigma$ ,  $\mu^k \circ \iota$ ,  $\mu^k \circ \tau$ ,  $\mu^k \circ \varepsilon$ ,  $\mu^k \circ \nu$ , and  $u^k$ , for  $k$  an integer. The first three of these functions have evaluations that are quite similar to each other. This is also true of the last four functions, however, the evaluations of the two sets of functions are quite different. The function  $\mu^k$ , indeed the last four functions listed above, can be used to produce the binomial coefficients. The construction of the negative Pascal triangle was an unexpected result of this investigation.

#### Other Results

The search for the results stated and proven in Chapter V led to the discovery of several additional interesting results. Most are stated in this section without proof in an effort both to diminish the bulk of this work as well as to provide the reader with the opportunity to use his own means to prove these results should this be to the reader's liking. The reader should keep in mind that the theory of Chapter IV, and, in particular, the theory associated with the logarithm operator  $L$ , can be used advantageously in proving some of the results to follow.

Lemma 6.1.

$$\varphi^{-1}(p^\alpha) = \begin{cases} 1 & \text{if } \alpha = 0, \\ 1-p & \text{if } \alpha \geq 1. \end{cases}$$

Recall that by Theorem 4.6 if  $f$  is a multiplicative function then  $Lf(n) = 0$  whenever  $n$  is not a power of a prime. For this reason it

suffices to state the following results using the argument  $n$  to be a power of a prime. In the results to follow,  $p$  is an arbitrary but fixed prime,  $k$  is an integer, and  $\alpha$  is a positive integer. If  $\alpha = 0$ ,  $p^\alpha = 1$ , and  $f(p^\alpha) = 1$  whenever  $f$  is multiplicative. In this case  $Lf(p^\alpha) = \log f(1) = 0$ .

The following theorem is readily established by induction on  $\alpha$ . This result holds for  $\alpha$  a non-negative integer.

Theorem 6.1.  $L\varphi(p^\alpha) = (p^\alpha - 1) \log p$ .

The next result was proven in the proof of Theorem 4.20. It is included in this section for completeness.

Theorem 6.2.  $L\varepsilon = 0$

Corollary 6.1.  $L\varphi^k(p^\alpha) = k(p^\alpha - 1) \log p$ .

Note for example that  $L\varphi^{-1}(p^\alpha) = (1 - p^\alpha) \log p$ .

In the case of the next theorem, and the other theorems of this type to follow, the reader may find it beneficial to prove the result for the case  $k = 1$  and then use the identity  $Lf^k = kLf$  for  $k \neq 0$ . If  $k = 0$ , Theorem 6.2 is useful.

Theorem 6.3.  $L\mu^k(p^\alpha) = -k \log p$ .

Corollary 6.2.  $L\nu^k(p^\alpha) = k \log p$ .

Theorem 6.4.  $L(\mu^k \circ \varphi)(p^\alpha) = (p^\alpha - k - 1) \log p$ .

Theorem 6.5.  $L(\mu^k \circ \varepsilon)(p^\alpha) = -k \log p$ .

Theorem 6.6.  $L(\mu^k \circ \nu)(p^\alpha) = (1 - k) \log p$ .

Theorem 6.7.  $L\tau^k(p^\alpha) = 2k \log p$ .

Corollary 6.3.  $L(\mu^k \circ \tau)(p^\alpha) = (2-k) \log p$ .

Theorem 6.8.  $L\sigma^k(p^\alpha) = k(p^\alpha + 1) \log p$ .

Corollary 6.4.  $L(\mu^k \circ \sigma)(p^\alpha) = (p^\alpha + 1 - k) \log p$ .

Theorem 6.9.  $L\iota^k(p^\alpha) = kp^\alpha \log p$ .

Corollary 6.5.  $L(\mu^k \circ \iota)(p^\alpha) = (p^\alpha - k) \log p$ .

Theorem 6.10. The infinite set of functions

$$H = \{\mu^k, \mu^k \circ \tau, \mu^k \circ \varepsilon, \mu^k \circ \nu \mid k \text{ is an integer}\}$$

is a cyclic group under convolution product. The function  $\mu$  generates  $H$ .

Theorem 6.11. The infinite sets of functions

$$K = \{\mu^k \circ \varphi, \mu^k \circ \sigma, \mu^k \circ \iota \mid k \text{ is an integer}\}$$

is not closed under convolution product.

Proof: Since the functions  $\mu^k \circ \varphi$ ,  $\mu^k \circ \sigma$ , and  $\mu^k \circ \iota$  differ only by a power of  $\mu$ , it suffices to consider the set  $K' = \{\mu^k \circ \iota \mid k \text{ is an integer}\}$ . Let  $k$  and  $j$  be integers and  $\alpha$  a positive integer. From Corollary 6.5 it follows that

$$[(\mu^k \circ \iota) \circ (\mu^j \circ \iota)](p^\alpha) = (\mu^{k+j-p^\alpha} \circ \iota)(p^\alpha).$$

Since the exponent of  $\mu$  depends upon  $\alpha$ ,  $\mu^{k+j-p^\alpha} \circ \iota$  cannot be a unique element of  $K'$  for all  $\alpha$ . This proves Theorem 6.11.

This proof does show that for a fixed  $\alpha$  the convolution product of two elements of  $K'$  at  $p^\alpha$  can be found by evaluating another element of  $K'$  at  $p^\alpha$ . This does show that the set  $K'$  (and hence  $K$ ) is "closed" in a manner that is highly dependent upon the choice of  $\alpha$ .

Some interesting patterns can be observed when comparing the evaluations of the functions in the sets  $H$  and  $K$  as derived in Chapter V and those of the operator  $L$  on these functions as stated above. For example,  $(\mu^k \circ \sigma)(p^\alpha) = \{p^\alpha(1-1/p)^{k-1}\}$ , while  $L(\mu^k \circ \sigma)(p^\alpha) = (p^\alpha)^{-k+1} \log p$  for  $\alpha \geq 1$ . Also,  $(\mu^k \circ \tau)(p^\alpha) = \binom{-k+1+\alpha}{\alpha}$  if  $k \leq 1$ , and equals  $(-1)^\alpha \binom{k-2}{\alpha}$  if  $k \geq 2$ , while  $L(\mu^k \circ \tau)(p^\alpha) = (2-k) \log p$  if  $\alpha \geq 1$ . The pattern is found by observing the coefficient of  $\log p$  in each case.

On the first page of Chapter V several identities were mentioned. These included  $\nu \circ \nu = \tau$ ,  $\iota \circ \nu = \sigma$ , and  $\tau \circ \phi = \sigma$ . Corollary 6.2 and Theorem 6.7 verify the first of these. Theorem 6.9, Corollary 6.2, and Theorem 6.8 verify the second. The third is verified by Theorems 6.7, 6.1, and 6.8.

#### Ideas for Continued Study

The well-behaved results of the previous section give hope that much more can be said about a comparison of the formulas for evaluating functions in  $M$  ( $P$  seems to be too large a set to start with) and their resultant formulas in the image space of the isomorphism  $L$ . Just this brief exposure assures one that it is much easier to do the analysis in the image space. Can one characterize all functions by the form of their evaluations in  $L(M)$ ? Should this be possible then a technique needs to be developed for taking a given function in  $L(M)$

and determining its pre-image in the set  $M$ . That is, given  $f \in L(M)$  what does  $E(f)$  look like? The method used in the proof of Theorem 4.5 is of no computational value since the function must be recognized by its function values.

Rearick [17], in an article that is a follow-up to the article that supplied the basis for Chapter IV, develops power series representations of arithmetic functions and certain operators. Perhaps this approach could help to answer the questions raised above. The article seems to be of sufficient length to provide the nucleus of another study.

## BIBLIOGRAPHY

1. Barnes, Wilfred E., Introduction To Abstract Algebra, D. C. Heath and Company, Boston, 1963.
2. Carlitz, L., "Arithmetic Functions in an Unusual Setting," American Mathematical Monthly, Vol. 73, Part 1, 1966, pp. 582-590.
3. Carlitz, L., "Rings of Arithmetic Functions," Pacific Journal of Mathematics, Vol. 14, No. 4 (Winter, 1964), pp. 1165-1171.
4. Cashwell, E. D., and C. J. Everett, "The Ring of Number-Theoretic Functions," Pacific Journal of Mathematics, Vol. 9 (Winter, 1959), pp. 975-985.
5. Courant, Richard and Herbert Robbins, What Is Mathematics?, Oxford University Press, London, 1941.
6. C. R. C. Standard Mathematical Tables, Twelfth Edition, Chemical Rubber Publishing Company, Cleveland, Ohio, 1959.
7. Davison, T. M. K., "On Arithmetic Convolutions," Canadian Mathematical Bulletin, Vol. 9, 1966, pp. 287-296.
8. Dickson, Leonard Eugene, History Of The Theory Of Numbers, Volume I, Carnegie Institution of Washington, Washington, D. C., 1919.
9. Eves, Howard and Carroll V. Newsom, An Introduction To The Foundations And Fundamental Concepts Of Mathematics, Rinehart and Company, Inc., New York, 1958.
10. Gautier, Gloria Jane, "Unitary Divisors and Associated Number-Theoretic Functions," Oklahoma State University, Master of Science Thesis, 1970.
11. Gioia, Anthony A., The Theory of Numbers: An Introduction, Markham Publishing Company, Chicago, 1970.
12. Herstein, I. N., Topics In Algebra, Blaisdell Publishing Company, Waltham, Massachusetts, 1964.
13. LeVeque, William Judson, Topics In Number Theory, Volume I, Addison-Wesley Publishing Company, Inc., Reading, Massachusetts, 1956.

14. Long, Calvin T., Elementary Introduction To Number Theory, D. C. Heath and Company, Boston, 1965.
15. Niven, Ivan and Herbert S. Zuckerman, An Introduction to the Theory of Numbers, John Wiley and Sons, Inc., New York, 1966.
16. Rearick, David, "Operators on Algebras of Arithmetic Functions," Duke Mathematical Journal, Vol. 35, 1968, pp. 761-766.
17. Rearick, David, "The Trigonometry of Numbers," Duke Mathematical Journal, Vol. 35, 1968, pp. 767-776.
18. Shockley, James E., Introduction To Number Theory, Holt, Rinehart and Winston, Inc., New York, 1967.
19. Warner, Seth, Modern Algebra, Volume I, Prentice-Hall, Inc., Englewood Cliffs, N. J., 1965.



VITA 2

Thomas Ray Hamel

Candidate for the Degree of

Doctor of Education

Thesis: SELECTED ALGEBRAIC STRUCTURES OF NUMBER-  
THEORETIC FUNCTIONS

Major Field: Higher Education

Biographical:

Personal Data: Born in Hays, Kansas, September 26, 1939, the son of Harry W. and Nona E. Hamel.

Education: Started school at West Plainville Country School, Plainville, Kansas; graduated from Zurich Grade School, Zurich, Kansas, in 1953; graduated from Palco Rural School, Palco, Kansas, in 1957; received the Bachelor of Science degree from Fort Hays Kansas State College in May, 1961, with a major in chemistry; attended Kansas State University, Manhattan, Kansas, during the summers of 1963 and 1964; attended Kansas State Teachers College, Emporia, Kansas, during the summers of 1966 and 1967; received the Master of Arts degree from Kansas State Teachers College with a major in mathematics in August, 1967; attended the University of Oklahoma, Norman, Oklahoma, from June, 1968, to May, 1969; completed requirements for the Doctor of Education degree at Oklahoma State University in July, 1971.

Professional Experience: Taught secondary school mathematics at Harrison Junior High School and Great Bend High School, Great Bend, Kansas, the year 1961-62; taught junior high mathematics at Harrison Junior High School, Great Bend, Kansas, from 1962 to 1966; taught high school mathematics at Great Bend High School, Great Bend, Kansas, from 1966 to 1968; graduate assistant in Department of Mathematics, University of Oklahoma, Norman, Oklahoma, the year 1968-1969; graduate assistant in Department of Mathematics, Oklahoma State University, Stillwater, Oklahoma, 1969-1971.