A STUDY OF NORMED DIVISION DOMAINS AND THEIR ANALOGUES WITH APPLICATIONS TO NUMBER THEORY

Thesis Submitted to the University of Calicut
in partial fulfilment of the requirements
for the award of the degree of

DOCTOR OF PHILOSOPHY
IN MATHEMATICS

By

RAJENDRAN VALIAVEETIL

DEPARTMENT OF MATHEMATICS

UNIVERSITY OF CALICUT

OCTOBER 1996

R. SIVARAMAKRISHNAN,
Professor of Mathematics (retired)
UNIVERSITY OF CALICUT

3rd October 1996

C E R T I F I C A T E

This is to certify that the dissertation entitled :

A STUDY OF NORMED DIVISION DOMAINS AND THEIR ANALOGUES WITH APPPLICATIONS TO NUMBER THEOREY

is a bonafide record of the investigations written by Sri Rajendran Valiaveetil in partial fulfilment of the requirements for the award of the Degree of Doctor of Philosophy in Mathematics and that it has been carried out under my supervision and guidance.

Also certified that he has not taken up sizeable quantities of material from any printed publication. Whenever results are quoted, they have been duly acknowledged.

It is further certified that this dissertation or any part thereof has not been presented to any other university/institution for the award of a research degree Diploma or title.

R. SIVARAMAKRISHNAN

D E C L A R A T I O N

I, Rajendran Valiaveetil do hereby declare that the dissertation entitled :

A STUDY OF NORMED DIVISION DOMAINS AND THEIR ANALOGUES WITH APPLICATIONS TO NUMBER THEORY

is a bonafide record of investigation done by me under the supervision and guidance of Dr. R. Sivaramakrishnan. I also declare that this has not been previously formed the basis for the award of any degree diploma, associateship, fellowship other similar title or recognition.

Department of Mathematics
UNIVERSITY OF CALICUT
Dated 3 October 1996.

RAJENDRAN VALIAVEETIL

A C K N O W L E D G E M E N T S

It is a matter of great pleasure for me to express my heart-felt gratitude to my supervising teacher Dr. R. Sivaramakrishnan for his stimulating guidance, constant encouragement and sincere cooperation. Without his creative approach and tremendous help it would not have been possible for me to shape this dissertation in its present form.

I am grateful to Dr. V. Krishnakumar, Head of the Department of Mathematics, University of Calicut for his helpful advice and for providing the facilities in the department to carry out the research work. My sincere thanks are also due to the other members of the faculty of Mathematics for all the couragement given to me while making academic discussions with them. I also place on record my thanks to Prof. K. Balagangadharan, Visiting Professor with whom I had fruitful discussions.

I wish to thank my colleagues in the Department of Mathematics, P.S.M.O. College, Tirurangadi for their assistance and words of goodwill during the period of my research. I am also indebted and grateful to the former Principals Prof. K. Ahammed Kutty, Dr. T. Mohammed and Prof. P. Abdul Latheef and the present Principal

Prof. P. Abdul Azeez. I take this opportunity to express my sincere thanks to Janab C.H.Kunhahamed Haji, the Manager of P.S.M.O. College for permitting to register for part-time research and to the authorities of the University of Calicut for enrolment as a part-time research scholar.

I would also like to express my gratitude to my wife and children for the troubles and pains they have taken during my frequent absence from home in connection with the academic work of a prolonged nature.

Finally my sincere thanks go to Miss M. Sujaya 'Megha Xerox and Computers', Thokkottu, Mangalore for the excellent job of typing.

Dated 3 October 1996 Rajendran Valiaveetil

CONTENTS

INTRODUCTION

Rajendran Valiaveetil “A study of normed division domains and their analogues with applications to number theory” Thesis. Department of Mathematics , University of Calicut, 1996

INTRODUCTION

It was E. Kummer (1810-1893) who introduced the notion of rings and ideals while studying the structure and properties of cyclotomic fields. The contributions of R. Dedekind (1831-1916) and Emmy Noether (1882-1935) to the development of the theory of rings and ideals are well-known. It may be remarked that we find examples of commutative rings with unity outside the realm of algebraic numbers such as convolution rings of arithmetic functions. The motivation for this dissertation is from the idea of the so-called *normed division domains* introduced by Solomon W. Golomb in [17] where an algebraic structure endowed with a norm is considered.

Definition : A nonempty set S with a *partial order* $\le$ which is *reflexive* and *transitive* together with a norm N which maps S into the set $\mathbb{Z}^{+}$ of positive integers is called a *normed division domain* written NDD if

(i) whenever $\alpha \le \beta$ for $\alpha, \beta \in S$, $N(\alpha) | N(\beta)$ and

(ii) if $N(u) = 1$ for $u \in S$, then $u \le \alpha$ for all α in S.

Among other things S.W. Golomb [17], considers the set S of all nonzero Gaussian intergers as an NDD with the customary notion of divisibility as the *partial order* and with the usual *norm* : $N(a + bi) = a^2 + b^2$, $a + bi \in S$.

Noting that the norm N on S is *multiplicative* in the sense that $N(\alpha\beta) = N(\alpha)\,N(\beta)$, we make the following :

Definition : Let R be an integral domain with unity. A *multiplicative norm* N on R is a function $N : R \longrightarrow \tilde{\mathbb{Z}}$, the set of nonnegative integers satisfying the following properties :

(i) $N(\alpha) = 0$ if and only if $\alpha = 0$

(ii) $N(\alpha\beta) = N(\alpha)\,N(\beta)$ for all α,β in R.

An integral domain endowed with a *multiplicative norm* is called a *multiplicatively normed domain*, abbreviated MND. (In [16], J.B. Fraleigh also mentions about the multiplicative norm).

The theme of the dissertation is about certain properties of mutlipicatively normed domains and their analogues with reference to situations arising in convolution rings of arithmetic functions. A brief survey of the contents of the dissertation is given below.

In Chapter 1, we develop the notion of a *multiplicatively normed domain*, obbreviated MND. We confine ourselves to those MND's R in which $N(u) = 1$ for $u \in R$ if and only if u is a *unit* in R. in Theorem 1 we obtain a sufficient condition for $a \in R$ to be *irreducible* in R. We observe that if R is an MND, then *factorization into irreducibles is possible* in R in the sense that *every* *nonzero nonunit* in R is a *finite product of irreducibles* in R. From examples in [31] and [37] we see that factorization into irreducibles need not be unique so that an MND need not be a *unique factorization domain* (UFD). In theorem 5, we establish that an MND is a UFD if and only if it is a GCD domain. It is shown in Theorem 6 that the ring R[x] of polynomials in one indeterminate x over an MND R is also an MND. Further we note that if R is an MND so is the ring R[[x]] of formal power series over R.

We begin Chapter 2, by examining the nature of the principal ideal J generated by the irreducible element $1+\sqrt{-5}$ in the ring $R = \mathbb{Z}[\sqrt{-5}]$. It is known [2] that J is *maximal* in the set of *proper principal ideals* of R. However J is not a *prime ideal* of R as $1 + \sqrt{-5}$ is not a *prime element* in R. We observe that J coincides with the ideal Q of R where

$$Q = \{a + b\sqrt{-5} : a - b \equiv 0 \pmod 6\}$$

Next we consider the ring $\mathbb{Z}[\sqrt{-p}]$, where p is a prime $\equiv 2 \pmod 3$ and we see that

$$Q = \{a + b\sqrt{-p} : a-b \equiv 0 \pmod 6\}$$

is an ideal of $\mathbb{Z}[\sqrt{-p}]$. In theorem 8, it is shown that Q has a very nice property that whenever $\alpha\beta \in Q$ with $\alpha, \beta \in \mathbb{Z}[\sqrt{-p}]$ and $\alpha \notin Q$, then either β or 2β or $3\beta \in Q$. This leads us to the following :

Definition : Let R be a commutative ring with unity. A proper ideal Q of R is called a *quasi-prime ideal* if whenever $\alpha\beta \in Q$ with $\alpha,\beta \in R$, there exists a positive integer k such that either $k\alpha \in Q$ or $k\beta \in Q$.

We call a commutative ring R with unity having a nonempty subset T of zero divisors of finite additive order a *quasi-integral domain* if whenever $\alpha,\beta \in R$ with $\alpha\beta = 0$ either $\alpha \in T$ or $\beta \in T$. Then we arrive at the following characterization of a *quasi-prime* ideal in Theorem 9 : Let R be a commutative ring with unity. Suppose that Q is a proper ideal of R which is not a *prime ideal.* Then Q is a *quasi-prime ideal* if and only if R/Q is a *quasi-integral domain*.

We remark that there is a notion of a *quasi-ideal* in a semigroup or a ring introduced by O. Steinfeld [36]. However our definition of *a quasi-prime ideal* is not related to Steinfeld's definition.

In Chapter 3, we go to the ring of arithmetic functions. By an arithmetic function we mean a map $f : \mathbb{Z}^+ \longrightarrow \mathbb{C}$ or $f : \tilde{\mathbb{Z}} \longrightarrow \mathbb{C}$ where $\mathbb{Z}^+(\tilde{\mathbb{Z}})$ denotes the set of positive integers (the set of nonnegative integers) and $\mathbb{C}$ denotes the field of complex numbers. We denote the set of all arithmetic functions with *domain* $\mathbb{Z}^+$ by $\mathcal{A}$. If $f,g \in \mathcal{A}$ we define their *natural sum* and their Dirichlet *convolution* or *product*, respectively by

$$(f + g)(r) = f(r) + g(r) \qquad r \geq 1$$

$$(f.g)(r) = \sum_{d \mid r} f(d)\, g(r/d) \qquad r \geq 1.$$

With respect to these operations, $\mathcal{A}$ becomes a commutative ring with unity. Introducing the norm $N(f)$ of $0 \neq f \in \mathcal{A}$ as the least positive integer n such that $f(n) \neq 0$ and setting $N(0) = 0$, Cashwell and Everett [5] have shown that $\mathcal{A}$ is indeed a UFD. With respect to this norm $\mathcal{A}$ is an MND. Further we see that $\mathcal{A}$ has a unique maximal ideal (Theorem 10). In Theorem 11, we realise $\mathcal{A}$ as a *subdirect sum* of the rings $\mathcal{A}/I_p$, where I_p is the principal ideal generated by *the prime* $x_p \in \mathcal{A}$ defined by

$$x_p(r) = \begin{cases} 1, & r = p \\ 0, & \text{otherwise} \end{cases}$$

Let f be a nonzero element of $\mathcal{A}$. Let I_f be the ideal which is *maximal* in the family of ideals of $\mathcal{A}$ which excludes f. $\mathcal{A}$ *is isomorphic to* the *subdirect sum* of the *subdirectly irreducible* rings $\mathcal{A}/I_f$. In the last section of the Chapter, we exhibit a *strictly descending chain of ideals* in $\mathcal{A}$, thereby showing that $\mathcal{A}$ is not *Artinian* (Theorem 13). We note that this can be also deduced from the fact that *the only integral domains that satisfy descending chain condition are fields* ([2], p.226).

In Chapter 4 , we look at the MND $\mathcal{A}$ of arithmetic functions from the point of view of its structure as a *vector space* over $\mathbb{C}$. It is interesting to note that certain arithmetical identities follow as a consequence of some linear operators on $\mathcal{A}$. Theorem 14 shows that the map $T : \mathcal{A} \longrightarrow \mathcal{A}$ defined by

$$(T(f))\ (r) = \sum_{d|r} f((a,r)),\quad f \in \mathcal{A},\quad r \geq 1.$$

where (a,r) denotes the g.c.d. of a and r, is a *bijective norm-preserving* linear operator. Next, we consider the linear operator $T_1 : \mathcal{A} \longrightarrow \mathcal{A}$ defined by

$$(T_1(f))\ (r) = \sum_{d|r} f((d,\ r/d))$$

and prove that (Theorem 15) T_1 satisfies the identity

$$(T_1(f))\ (r) = \sum_{k^2|r} f(k)\ 2^{\omega(r/k^2)}$$

where $\omega(r)$ denotes the number of *distinct* prime factors of r. From the above we deduce

$$\sum_{d|r}(d\ ,\ r/d) = \sum_{k^2|r} k\ \ 2^{\omega(r/k^2)}$$

an identity due to Daniel I.A. Cohen [6]. Analogous to the linear operator T_1, we have another linear operator $T_2 : \mathcal{A} \longrightarrow \mathcal{A}$ defined by

$$(T_2(f))(r) = \sum_{d \mid r} f([d, r/d]), \quad f \in \mathcal{A}, \quad r \geq 1.$$

where $[d, r/d]$ denotes the l.c.m of d and r/d. It is established in Theorem 16 that T_2 satisfies the identity

$$(T_2(f))(r) = \sum_{k^2 \mid r} f(r/k)\, 2^{\omega(r/k^2)}$$

It is deduced that

$$\sum_{d \mid r} [d, r/d] = \sum_{k^2 \mid r} (r/k)\, 2^{\omega(r/k^2)}$$

We further observe that T_1 *preserves norm* if and only f is a *unit* in $\mathcal{A}$ (Theorem 17) whereas T_2 is *norm -preserving* (Theorem 18). We also have a linear operator L on $\mathcal{A}$ obtained via l.c.m. convolution :

$$(L(f))(r) = \sum_{\substack{1 \leq a \leq r \\ [a,b] = r}} f(a), \quad f \in \mathcal{A}$$

where a is the first coordinate of the ordered pair (a,b) such that [a,b] = r. It is proved in Theorem 19 that L is *norm-preserving* and if F = f.e, where e(r) =1, r ≥ 1, then L is given by

$$(L(f))\ (r) = \sum_{t \mid r} F(t)\ d(t)\ \mu(r/t)$$

where μ is the Möbius function.

It is established in Theorem 20, that the operator L defined above has the property that if $f = c\mu$, then $L(f) = f$ where $c \in \mathbb{C}$ and μ is the Möbius Function. Conversely if $L(f) = f$ for $f \in \mathcal{A}$, then $f = c\mu$ where $c = f(1)$.

In Chapter 5, we consider some commutative rings with unity in the context of arithmetic functions and having divisors of zero. First we extend the definition of a multiplicative norm *to any commutative ring with unity.*

Definition : Let R be a commutative ring with unity. A *multiplicative norm* N on R is a function N from R into the set $\tilde{\mathbb{R}}$ of non negative real numbers such that

(i) $N(0) = 0$

(ii) $N(\alpha\beta) = N(\alpha)\ N(\beta)$ for all $\alpha, \beta \in R$.

R is called a *multiplicatively normed ring*, abbreviated MNR if there is defined a *multiplicative norm* on it. As a first example (not from the set of arithmetic functions), we consider the ring of real valued continuous functions defined on the closed interval $[0,1]$. The second example is the Lucas ring $\mathfrak{B}$ of arithmetic functions defined on $\tilde{\mathbb{Z}}$, the set of nonnegative integers, introduced by L. Carlitz

[4] which is described as follows :

Let p be specified prime. Writing

$$r = r_o + r_1 p + r_2 p^2 + \ldots\ldots \qquad (0 \le r_j < p)$$

$$k = k_o + k_1 p + k_2 p^2 + \ldots. \qquad (0 \le k_j < p)$$

one notes that

$$\binom{r}{k} \equiv \binom{r_o}{k_o} \binom{r_1}{k_1} \ldots\ldots \pmod{p}$$

From the above, we deduce that the binomial coefficient $\binom{r}{k}$ is prime to p if and only if

$$0 \le k_j \le r_j \qquad (j = 0,1,2\ldots\ldots).$$

For f, g $\in \mathfrak{B}$ the Lucas product h = f * g of f and g is given by

$$h(r) = \sum_{k=0}^{r}{}' \; f(k)\; g(r-k)$$

where Σ' is restricted to those k for which $p \nmid \binom{r}{k}$.

With respect to the *natural sum* and *Lucas product* $\mathfrak{B}$ is a commutative ring with unity. Defining $N(f) = |f(0)|$, $f \in \mathfrak{B}$, it follows that $\mathfrak{B}$ is an MNR. In this connection we also prove that $\mathfrak{B}$ is indeed a local ring (Theorem 21). Further it is observed that the ring of arithmetic functions with respect to unitary convolution also serves as an example of an MNR.

The concluding chapter of the dissertation is about a finite dimensional algebra drawn from a class of functions, which are periodic (mod r) ($r \geq 1$) and which satisfy

$$f(n) = f((n,r))$$

where f is complex valued . The precise definition is given below :

Let F be a field of characteristic zero containing the r^{th} roots of unity where r is an arbitrary but fixed positive integer. Following Eckford Cohen [7], $f : \mathbb{Z} \longrightarrow F$ is called an (r, F) arithmetic function if

$$f(n) = f(m) \text{ whenever } n \equiv m \pmod{r}.$$

We denote the set of (r, F) arithmetic functions by $\mathcal{A}_r(F)$. $f \in \mathcal{A}_r(F)$ is called an even function of n (mod r) or briefly an even function (mod r) if

$$f(n) = f((n,r))$$

Where (n,r) stands for the g.c.d of n and r. Taking $F = \mathbb{C}$ the field of complex numbers, Eckford Cohen has made a detailed study of properties of even functions (mod r) in [7], [8], [9] [10] [11] and [14]. In the case $F = \mathbb{C}$ We denote the set of even functions (mod r) by $\mathcal{B}_r(\mathbb{C})$. Some structural properties of $\mathcal{B}_r(\mathbb{C})$ are also studied by P. Haukkanen and R. Sivaramankrishnan (see [19]).

The Ramanujan's sum C(n,r) is given by

$$C(n.r) = \sum_{\substack{h \pmod r \\ (h,\ r) = 1}} \exp\ (2\pi inh/r)$$

where the summation is over a residue system (mod r). C(n,r) is an even function (mod r). It is known [8] that $f \in \mathcal{B}_r(\mathbb{C})$ has the unique finite Fourier representation

$$f(n) = \sum_{d \mid r} \alpha(d)\ C\ (n,d)$$

where the Fourier coefficients $\alpha(d)$ are given by

$$\alpha(d) = (1/r) \sum_{d \mid r} f(r/\delta)\ C\ (r/d,\ \delta)$$

It is known [26], that $\mathcal{B}_r(\mathbb{C})$ is a vector space of dimension d(r), the number of divisors of r, with an orthonormal basis

$$\{ (r\phi\ (d))^{-1}\ C(n,d)\ :\ d \mid r \}$$

where ϕ is the Euler ϕ - function, with respect to the inner product :

$$<f,g> = \sum_{a \pmod r} f(a)\ \overline{g(a)}$$

$\overline{g(a)}$ being the complex conjugate of g(a).

In Theorem 24, it is shown that $\mathscr{B}_r(\mathbb{C})$ is an MNR with the norm N defined by

$$N(f) = r \min_{d} \{|\alpha(d)|\}, \quad f \in \mathscr{B}_r(\mathbb{C})$$

where the minimum is taken over the divisors d of r and $\alpha(d)$, $d|r$ are Fourier coefficients of f.

In [9], a subset of completely even functions (mod r) of $\mathscr{B}_r(\mathbb{C})$ is considered. $f \in \mathscr{B}_r(\mathbb{C})$ is called a completely even function (mod r) if there exists an arithmetic function F such that

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

We observe that the function B(n,r) [34] defined by

$$B(n,r) = \sum_{\substack{h \pmod r \\ (h,r) = \text{a square}}} \exp(2\pi ihn/r)$$

is such that

$$\lambda(r)\ B(n,r) = \sum_{d|(n,r)} d\ \lambda\ (d)$$

where $\lambda(r) = (-1)^{\Omega(r)}$, $\Omega(r)$ being the *total* number of prime factors of r (*each counted according to its multiplicity*). So $\lambda(r)$ B(n,r) is completely even (mod r). In Theorem 25, we establish the orthogonal property of B(n,r) :

If t_1, t_2 are square-free divisors of r,

$$\sum_{n \equiv a+b \pmod{r}} B(a, r/t_1)\, B(b, r/t_2) = \begin{cases} r\, B(n, r/t), & \text{if } t_1 = t_2 = t \\ 0, & \text{if } t_1 \neq t_2 \end{cases}$$

Using this we assert that the set $V_r(\mathbb{C})$ of completely even functions (mod r) forms a subspace of $\mathcal{B}_r(\mathbb{C})$ having dimension $2^{\omega(r)}$, the number of square-free divisors of r. $V_r(\mathbb{C})$ has an orthonormal basis

$$\{\lambda(r/t)\ (rb(r/t))^{-1/2}\ B(n, r/t) : t \text{ a square-free divisor of } r\}$$

where $b(r) = B(0,r)$. We mention that $\mathcal{B}_r(\mathbb{C})$ has also another subspace $W_r(\mathbb{C})$ of unitary functions (mod r) and having the same dimension $2^{\omega(r)}$, (see [13]).

A note on a generalization of the nil radical of an ideal namely the k-fold nil radical of an ideal($k \geq 1$) is added in the Appendix as the result relating to the ring rational integers was obtained while working in the area of commutative rings with unity.

Most of the preliminary results needed in the dissertation are mentioned and duly acknowledged as and where required. Some well-known theorems used in the dissertation are numbered with *. All unexplained notions related to number theory may be found in [1], [29], and those related to algebra in [2], [16] and [21].

While concluding, we wish to remark that the dissertation makes a humble attempt to throw more light on the properties of certain algebraic structures arising in the context of algebraic numbers and rings of arithmetic functions under various convolution operations.

MULTIPLICATIVELY NORMED DOMAINS

Rajendran Valiaveetil “A study of normed division domains and their analogues with applications to number theory” Thesis. Department of Mathematics , University of Calicut, 1996

CHAPTER 1

MULTIPLICATIVELY NORMED DOMAINS

We begin with a 'restricted' partially ordered set $(S, \leq)$ where the relation $\leq$ is reflexive as well as transitive. That is $\alpha \leq \alpha$ for all α in S; if $\alpha \leq \beta$ and $\beta \leq \gamma$ then $\alpha \leq \gamma$ for all α, β, γ in S.

Following Solomon W. Golomb [17], we give

1.0.1 Definition ([17]). Let $(S, \leq)$ be a restricted partially ordered set and N be a function which maps S into the set $\mathbb{Z}^+$ of positive integers such that if $\alpha \leq \beta$ for α and β in S, then $N(\alpha)|N(\beta)$, and if $N(u) = 1$ for u in S, then $u \leq \alpha$ for all α in S. Then $D = (S, \leq, N)$ is called a *normed division domain*, abbreviated NDD.

1.0.2 Definition ([17]) . If $N(u) = 1$ for an element u in an NDD, then u is called a *unit* in that NDD.

1.0.3 Example ([17]) . Let $S = \mathbb{Z}[i]\backslash\{0\}$, the non zero Gaussian integers. S with the usual notion of divisibility and with the usual norm N given by $N(a+bi) = a^2+b^2$ for a+bi in S, is an NDD.

Let T be the subset of S consisting of rational integers, with the standard divisibility and with the same norm : $N(a) = N(a+0i) = a^2$. Then $(T, \leq, N)$ is also an NDD.

1.0.4 Example ([17]). Let S be the set of all finite groups, and for $G \in S$, define $N(G)$ = order of G; define $H \leq G$ for $H, G \in S$ if and only if H is isomorphic to a subgroup of G. Then $D = (S, \leq, N)$ is an NDD.

1.0.5 Example. Let $\mathcal{O}$ be the ring of integers of a number field K of degree n. Let S be the set of all non zero ideals of $\mathcal{O}$ and define $I \leq J$ if and only if $J \subseteq I$ for I, $J \in S$. With the standard definition of norm of an ideal of $\mathcal{O}$ ([37], p. 125) as $N(I)$ = order of the quotient ring $\mathcal{O}/I$, $(S, \leq, N)$ is an NDD.

1.0.6 Example. Let $S = F[x]\setminus\{0\}$, the set of all non zero polynomials in a single indeterminate x over a field F. Define $f(x) \leq g(x)$ if and only if $\deg f(x) \leq \deg g(x)$ and also define $N((f(x)) = 2^{\deg f(x)}$ for $f(x), g(x) \in S$. Then $(S, \leq, N)$ in an NDD.

We observe that the norms in the examples (1.0.3), (1.0.5) and (1.0.6) are *multiplicative*, that is $N(\alpha\beta) = N(\alpha)\, N(\beta)$ for all α, β in S. The purpose of this Chapter is to study certain integral domains that have a norm which is multiplicative. These are called *mutliplicatively normed domains*, abbreviated MND and such domains are examined for unique factorization property of elements . The corresponding rings of polynomials and field of quotients are also considered.

1.1 MULTIPLICATIVELY NORMED DOMAINS

Throughout what follows by an *integral domain* we mean *a commutative ring with unity* 1 *and having no zero divisors.* We begin with the following :

1.1.1 Definition. Let R be an integral domain. A *multiplicative norm* N on R is a function mapping R into the non-negative integers $\tilde{\mathbb{Z}}$ such that

(i) $N(\alpha) = 0$ if and only if $\alpha = 0$

(ii) $N(\alpha\beta) = N(\alpha)\ N(\beta)$ for all $\alpha, \beta \in R$.

An integral domain R with a *multiplicative norm* on it is called *multiplicatively normed domain* , abbreviated MND.

In ([16], p. 311) J.B. Fraleigh also mentions about the multiplicative norm.

1.1.2 Example. Let R be an integral domain. Define $N : R \longrightarrow \tilde{\mathbb{Z}}$ by

$$N(\alpha) = \begin{cases} 1, & \text{if } 0 \neq \alpha \in R \\ 0, & \text{if } \alpha = 0 \end{cases}$$

Then R is an MND.

1.1.3 Example : Let $R = \mathbb{Z}[\sqrt{d}\,] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$, where $d \neq 1$ is a square-free integer, that is an integer not divisible by the square of any positive integer > 1. Define N on R by $N(a + b\sqrt{d}) = |a^2 - db^2|$. Then N is a *multiplicative norm* on R. In particular $R = \mathbb{Z}[\sqrt{-5}]$ with $N(a+b\sqrt{-5}) = a^2 + 5b^2$ is an MND.

1.1.4 Example. The ring $\mathcal{O}$ of integers of any number field K of degree n is an MND with norm N defined by

$N(x) = |x_1 x_2 \ldots x_n|$, $x \in \mathcal{O}$ where $x_1, x_2, \ldots, x_n$ are the roots of the field polynomial of x over K, ([37], p. 54).

1.1.5 Example . Let F be a field and F[x] be the ring of polynomials over F in a single indeterminate x. Then F[x] is an integral domain. Define $N : F[x] \longrightarrow \tilde{\mathbb{Z}}$ by

$$N(f(x)) = 2^{\deg f(x)}, \quad f(x) \in F[x]$$

Then N is a *multiplicative norm* on F[x]

Let R be an MND, with norm N. Then $N(1) = 1$. Also if $u \in R$ is a unit then $N(u) = 1$. *But in general the converse is not true.* For example in (1.1.2) we see that $N(a)=1$ for every $0 \neq a \in R$. In (1.1.4) and (1.1.5) we note that *$N(u) = 1$ if and only if* u is a unit in the integral domain under consideration.

1.2 DIVISIBILITY

In this section we consider only those *multiplicatively normed domains,* R with multiplicative norm N such that $N(u) = 1$ for $u \in R$ *if and only if* u *is a unit in R* . In this case we prove that R is a unique factorization domain if and only if R is a GCD domain.

1.2.1 Definition ([2], p. 90) . Let $a, b \in R$, $a \neq 0$. We say that a *divides* b or *a is a divisor* of b written $a|b$ if there exists some $c \in R$ such that $b = ac$. In case a *does not divide* b we shall write $a \nmid b$.

For $a \in R$, we write

$$\langle a\rangle = \{ra : r \in R\}$$

for the principal ideal of R generated by a. We note that $a|b$ if and only if $\langle b\rangle \subseteq \langle a\rangle$.

Two elements $0 \neq a$, $0 \neq b \in R$ are called *associates* of each other if $a|b$ and $b|a$. Further a and b are associates if and only if $a = ub$ for some unit u in R. Also $\langle a\rangle = \langle b\rangle$ if and only if a and b are associates.

1.2.2 Definition ([2], p. 97) . A *nonzero nonunit* $a \in R$ is said to be *irreducible* if $a = bc$, then either b or c is a unit.

A *nonzero nonunit* $a \in R$ is said to be *prime* if $a|bc$ $(b, c \in R)$, then either $a|b$ or $a|c$.

A prime is always irreducible but not conversely ([2], p 97).

Theorem 1. Let R be an MND with norm N. A sufficient condition for an element $a \in R$ to be *an irreducible* of R is that N(a) is *a rational prime.*

Proof : Let $a \in R$ be such that $N(a) = p$, where p is a rational prime. If $a = bc$ then $p = N(a) = N(b)\ N(c)$. Then either $N(b) = 1$ or $N(c) = 1$, that is either b or c is a unit in R. Therefore a must be an irreducible element of R. □

Theorem 2 . Let R be an MND. An element $a \in R$ is an irreducible element of R if and only if there is no element $b \in R$ which is irreducible and which is such that $b|a$ and $N(b) < N(a)$.

Proof : If there is an irreducible element $b \in R$ such that $b|a$ and $N(b) < N(a)$, then there exist some $c \in R$ with $a = bc$ where $N(b) > 1$ and $N(c) > 1$. Hence a cannot be irreducible in R.

To prove the converse, suppose that $N(a) > 1$ and a is not an irreducible element of R. We must show that there exists a proper divisor b of a such that b is an irreducible element in R. We proceed by induction on $N(a)$. If $N(a) = 2$, the smallest possible norm for an irreducible, then a must be irreducible by Theorem 1. Assume that the result is true for all elements of R whose norms are less than or equal to n where $n \geq 2$. Let $\alpha \in R$ be such that $N(\alpha) = n+1$. Then either α is irreducible or it has a divisor β such that $2 \leq N(\beta) < n+1$. By induction hypothesis either β is an irreducible in which case there is nothing to prove or β has an irreducible divisor γ with $2 \leq N(\gamma) < N(\beta) \leq n$. In this situation, since $\gamma | \beta$ and $\beta | \alpha$ and as the relation *divides* is transitive we get $\gamma | \alpha$ and γ is an irreducible divisor of α with $1 < N(\gamma) < N(\alpha)$. □

Let us recall a few definitions :

1.2.3 Definition ([2], p. 92) . Let $a_1, a_2, \ldots, a_n$ be nonzero elements in an integral domain R. An element $d \in R$ is called a *greatest common divisor*, abbreviated g.c.d of $a_1, a_2, \ldots, a_n$ if

(i) $d | a_i$ for $i = 1, 2, \ldots, n$

(ii) $c | a_i$ for $i = 1, 2, \ldots, n$ implies that $c | d$.

The g.c.d of $a_1, a_2, \ldots, a_n \in R$ is *unique whenever it exists, upto arbitrary unit factors.* In a principal ideal domain any finite set of nonzero elements $a_1, a_2, \ldots, a_n$ has a g.c.d ([2], p. 93) .

1.2.4 Definition ([23], p. 84) . A GCD *domain* is an integral domain in which each pair of nonzero elements has a g.c.d.

1.2.5 Definition [23], p. 90). A commutative ring R with unity is said to satisfy the *ascending chain condition on principal ideals* (ACCP) if for any ascending chain of principal ideals

$$<a_o> \subseteq <a_1> \subseteq \ldots \subseteq <a_n> \subseteq \ldots$$

there exists an integer m (depending on the chain such that $<a_n> = <a_m>$ for all $n \geq m$.

1.2.6 Definition ([2], p. 100) . An integral domain R is called a *unique factorization domain*, abbreviated UFD if the following conditions are satisfied :

i) every element of R that is neither zero nor a unit can be factored into a finite product of irreducible elements in R.

ii) if $p_1 p_2 \ldots p_r$ and $q_1 q_2 \ldots q_s$ are twofactorizations of an element $a \in R$ into irreducibles, then $r = s$ and the q_j can be renumbered so that p_i and q_i are associates.

We also need the following :

Theorem 3^*. ([23], p. 91) . Let R be an integral domain . The following conditions are equivalent :

(i) Every nonzero nonunit of R is a product of primes.

(ii) R is a UFD.

(iii) R is a GCD domain in which ACCP is satisfied.

The proof is omitted (cf [23], pp 91-92) .

The theorem asserts that UFD's are precisely GCD domains in which ACCP is satisfied.

Now we shall prove that, in an MND factorization into irreducibles is possible.

1.2.7 Lemma . Let R be an MND. Then every nonzero non unit of R has a factorization into a finite product of irreducibles in R.

Proof. Let R be an MND with norm N. Then $N(ab) = N(a)\ N(b)$ for al $a, b \in R$. Also by our convention $N(u) = 1$ for $u \in R$ if and only if u is a unit in R. Let $a \in R$ be any nonzero, nonunit. We prove the theorem by induction on N(a). If a is not already irreducible, then we can write $a = bc$ with $N(b) < N(a)$ and $N(c) < N(a)$. By induction hypothesis both b and c can be factored into products of irreducibles and hence a is also a product of irreducibles. □

Theorem 4 . Any MND R satisfies ACCP.

Proof : By Lemma 1.2.7, any nonzero nonunit in R can be expressed as a finite product of irreducibles . Also if $a, b \in R$ and $b \neq 0$ then $\langle a\rangle \subseteq \langle b\rangle$ if and only if $b|a$. So it follows that R satisfies ACCP. □

Theorem 5 . An MND is a UFD if and only if it is a GCD domain .

Proof : Suppose that R is an MND which is a UFD. By Theorem 3*, R must be a GCD domain.

Conversely suppose that R is an MND which is a GCD domain. By Theorem 4, R satisfies ACCP also. So R is a GCD domain in which ACCP is satisfied. By Theorem 3*, R is UFD. □

The following example illustrates the significance of Theorem 5. We note that $6 \in \mathbb{Z}[\sqrt{-5}]$ has two nontrivial factorizations into irreducibles :

$$6 = 2.3 = (1 + \sqrt{-5})\ (1-\sqrt{-5})$$

Indeed, since 2 is not an associate of $1+\sqrt{-5}$ or $1-\sqrt{-5}$ it follows that the above two factorizations of 6 are distinct and hence $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, (see [31] or [37]).

Next, consider the elements 6 and $3(1+\sqrt{-5})$ in $\mathbb{Z}[\sqrt{-5}]$. The common factors are 1, 3, and $1+\sqrt{-5}$. But none of these factors is divisible by the others. So the g.c.d of 6 and $3(1+\sqrt{-5})$ fails to exist. The failure of the UFD property in $\mathbb{Z}[\sqrt{-5}]$ is due to the fact that $\mathbb{Z}[\sqrt{-5}$ is not a GCD domain though it satisfies ACCP.

1.2.8. Definition. Let R be a commutative ring with unity. An ideal $P \neq R$ is called a *prime ideal* if whenever $ab \in P$ with $a, b \in R$, either $a \in P$ or $b \in P$.

It is known that p is a prime element in an integral domain R if and only if the principal ideal $\langle p \rangle \neq R$ is prime. We note that $1+\sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$ is irreducible but not prime. So the principal ideal $\langle 1+\sqrt{-5} \rangle$ in $\mathbb{Z}[\sqrt{-5}]$ is not a prime ideal. So the natural question is : what type of ideal is the principal ideal generated by $1 + \sqrt{-5}$? This will be investigated in Chapter 2.

1.3 RING OF POLYNOMIALS OVER AN MND

If R is an MND, we look at the ring R[x] of polynomials over R in a single indeterminate x.

Theorem 6. If R is an MND then so is R[x] .

Proof : It is known that if R is an integral domain then so is R[x]. Let $f(x) = a_0 + a_1x + \ldots + a_n x^n, n = \deg f(x) \geq 0$,

$a_i \in R$ $(i = 0, 1, 2, ..., n)$. Let the norm on R be N. Then define $N(f(x) = N(a_n)$. If $g(x) = b_o + b_1 x + ..., + b_m x^m$, $m = \deg g(x) \geq 0$, $b_i \in R$ $(i = 0, 1, ..., m)$. then $N(g(x)) = N(b_m)$. Since $f(x)\ g(x)$ is a polynomial of degree $n+m$ with the largest coefficient $a_n\ b_m$, we have

$N(f\ g) = N(a_n\ b_m) = N(a_n)\ N(b_m) = N(f)\ N(g)$ So $R[x]$ is an MND.

Remark : It also easily follows that if R is an MND, then so is the ring R[[x]] of formal power series with coefficients in R.

1.4 THE FIELD OF QUOTIENTS OF AN MND

We first give the notion of a field with valuation. Let G be an ordered abelian group with an element O adjoined : $V = G \cup \{0\}$, disjoint in which we define $00=0$ and $g>0$, $0g=0=g0$ for all $g \in G$. Following Jacobson [22], one has

1.4.1. Definition ([22],p. 556) . If F is a field and V is an ordered abelian group with 0 adjoined then we define a V-valuation of F to be a function $\Phi : F \longrightarrow V$ such that

(i) $\Phi(a) = 0$ if and only if $a = 0$

(ii) $\Phi(ab) = \Phi(a)\ \Phi(b)$

(iii) $\Phi(a+b) \leq \max\ (\Phi(a),\ \Phi(b))$

We need to extend the above definition to integral domains. If R is an integral domain and V an ordered abelian group with 0 adjoined, then a V-valuation of R is a function $\Phi : R \longrightarrow V$ satisfying conditions (i) — (iii) of Definition 1.4.1. We recall ([22], p. 557) that if R is an integral domain and Φ a V-valuation on R, then Φ has a unique extension to a V-valuation on the field of quotients F of R.

In the case of an MND, the norm does not satify condition (iii) of definition 1.4.1, is general . Therefore an MND is not capable of consideration as a domain with valuation using the norm.

IDEALS IN A MULTIPLICATIVELY NORMED DOMAIN

Rajendran Valiaveetil “A study of normed division domains and their analogues with applications to number theory” Thesis. Department of Mathematics , University of Calicut, 1996

CHAPTER 2

IDEALS IN A MULTIPLICATIVELY NORMED DOMAIN

We examine the nature of a principal ideal in an MND. In particular, we consider the principal ideal J generated by the irreducible element $1 + \sqrt{-5}$ in $\mathbb{Z}[\sqrt{-5}]$. That is,

$$J = < 1 + \sqrt{-5} >$$

$$= \{(a+b\sqrt{-5})(1 + \sqrt{-5}) : a, b \in \mathbb{Z}\}$$

It is known ([2], p. 98) that J is maximal in the set of proper principal ideals of $\mathbb{Z}[\sqrt{-5}]$. However, that is not needed here.

Let Q denotes the ideal in $\mathbb{Z}[\sqrt{-5}]$ defined by

$$Q = \{(a+b\sqrt{-5} : a-b \equiv 0 \pmod 6)\}$$

2.0.1 Lemma . $J = Q$

Proof : Let $x + y\sqrt{-5} \in J$. Then there exist $a, b \in \mathbb{Z}$ such that

$$x + y\sqrt{-5} = (a + b\sqrt{-5})(1 + \sqrt{-5})$$

or

$$x + y\sqrt{-5} = (a-5b) + (a+b)\sqrt{-5}$$

or

$$x = a-5b \quad \text{and} \quad y = a+b$$

Therefore, $y-x = 6b$ and $x + 5b = 6a$

This shows that if $x+y\sqrt{-5} \in J$, then $x-y \equiv 0 \pmod 6$ and hence $x + y\sqrt{-5} \in Q$. Thus $J \subseteq Q$

To prove the reverse inclusion we proceed as follows : Suppose $r + s\sqrt{-5} \in Q$. Then $r - s \equiv 0 \pmod 6$. We claim that there exist integers a, b such that

$$r + s\sqrt{-5} = (a + b\sqrt{-5})(1+\sqrt{-5}) \text{ where } r-s \equiv 0 \pmod 6$$

That is, given r, s with $r-s \equiv 0 \pmod 6$ solutions a, b in integers exist for the simultaneous equations in x, y :

$$x - 5y = r$$

$$x + y = s$$

Let $r-s = 6k$, where k is an integer. Them $6y = s-r = -6k$ or $y = -k = \frac{1}{6}(s-r)$.

$$\text{Then } x = 5y + r = \frac{5}{6}(s-r) + r = \frac{5s + r}{6} = \frac{6s + (r-s)}{6}$$

$$= s + \frac{1}{6}(r-s)$$

So there exist solution for the above simultaneous equations :

$$a = s + \frac{1}{6}(r-s)\ ,\ b = \frac{1}{6}(s-r)$$

This proves that $Q \subseteq J$ and so the proof follows. □

Remark : Since $1 + \sqrt{-5}$ is not prime in $\mathbb{Z}[\sqrt{-5}]$ $<1+\sqrt{-5}>$ is not a prime ideal of $\mathbb{Z}[\sqrt{-5}]$.

2.1 THE MND $\mathbb{Z}[\sqrt{-p}]$

We now go to a general setting by replacing 5 by an odd prime p, arbitrary but fixed such that $p \equiv 2 \pmod 3$. For each such p, $\mathbb{Z}[\sqrt{-p}] = \{a+b\sqrt{-p} : a, b \in \mathbb{Z}\}$ is an integral domain in which factorization of a nonzero nonunit into irreducibles is not always unique . For example it is known that $\mathbb{Z}[\sqrt{-11}]$ is a UFD, whereas $\mathbb{Z}[\sqrt{-23}]$ is not a UFD ([37],p. 93)

We define

$$M_2 = \{ a + b\sqrt{-p} \quad : a-b \equiv 0 \pmod 2)$$

$$M_3 = \{ a + b\sqrt{-p} \quad : a-b \equiv 0 \pmod 3)$$

Theorem 7 . M_2 and M_3 are maximal ideals of $\mathbb{Z}[\sqrt{-p}]$.

Proof : Let us write $R = \mathbb{Z}[\sqrt{-p}\,]$. It is easy to see that M_2 is a subgroup of $(R, +)$.

Let $\alpha = a + b\sqrt{-p} \in R$ and $\beta = c+d\sqrt{-p} \in M_2$

Then $c-d \equiv 0 \pmod 2$.

Also $\alpha\beta = (ac-bdp) + (bc + ad)\sqrt{-p}$

For $\alpha\beta$ to belong to M_2, we must have

$$(ac-bd\,p) - (bc-ad) \equiv 0 \pmod 2.$$

As p is odd, $p \equiv -1 \pmod 2$ and therefore

$$(ac-bdp) - (bc-ad) \equiv (a-b)(c-d) \pmod 2 \equiv 0 \pmod 2$$

since $c-d \equiv o \pmod 2$.

Thus M_2 is an ideal of R.

Further if $\alpha = a + b\sqrt{-p}$ is any element of R that does not belong to M_2, that is $a-b \equiv 1 \pmod 2$, we can write

$$1 = \alpha + (1-a+b\sqrt{-p})$$

which expresses 1 as a sum of α and an element of M_2. So any ideal of R containing M_2 and α contains 1, and therefore it is the whole of R. Thus M_2 is a maximal ideal of R.

Next, we consider M_3. Clearly M_3 is an additive subgroup of R. If $\alpha = a+b\sqrt{-p} \in R$ and $\beta = c + d\sqrt{-p} \in M_3$, then $c-d \equiv 0 \pmod 3$. For $\alpha\beta$ to belong to M_3, we must have

$$(ac - bd\,p) - (bc+ad) \equiv 0 \pmod 3.$$

Since $p \equiv 2 \pmod 3$ and $c-d \equiv 0 \pmod 2$, we have

$$\begin{aligned}(ac-bdp) - (bc+ad) &\equiv (ac-2bd) - (bc+ad) \pmod 3\\ &\equiv (ac-bd) - (bc+ad) \pmod 3\\ &\equiv (a-b)(c-d) \pmod 3\\ &\equiv 0 \pmod 3\end{aligned}$$

Thus $\alpha\beta \in M_3$ and hence M_3 is an ideal of R.

Finally if $\alpha \in R$ but $\alpha \notin M_3$, then we can write

$$1 = \begin{cases} \alpha + (1-a-b\sqrt{-p}, & \text{if } a-b \equiv 1 \pmod 3) \\ 2\alpha + (1-2a-2b\sqrt{-p}, & \text{if } a-b \equiv 2 \pmod 3) \end{cases}$$

which expresses 1 in terms of α and an element of M_3. So it follows that M_3 is also a maximal ideal of R. □

Remark : We observe that

$$M_2 \cap M_3 = \{a+b\sqrt{-p} : a-b \equiv 0 \pmod 6)\}$$

Let us denote this ideal by Q.

Theorem 8 . The ideal Q of R is such that whenever $\alpha\beta \in Q$ and $\alpha \notin Q$ (for $\alpha, \beta \in R$) we have $\beta \in Q$ or $2\beta \in Q$ or $3\beta \in Q$.

Proof : For $\alpha, \beta \in R$ given by $\alpha = a+b\sqrt{-p}$, $\beta = c+d\sqrt{-p}$ with $\alpha\beta \in Q$, one has

$$(ac-bdp) - (bc + ad) \equiv 0 \pmod 6)$$

As $p \equiv 2 \pmod 3$, we have $p \equiv 5 \pmod 6$ and so the above congruence implies that

(2.1.1) $$(a-b)\ (c-d) \equiv 0\ (\text{mod } 6.$$

Now assume $\alpha \notin Q$. Then $a-b \not\equiv 0 \pmod 6$. Three cases arise :

Case(i) $a-b$ is not divisible by the primes 2 and 3.

Then (2.1.1.) implies that $c-d \equiv 0 \pmod 6$ so that $\beta \in Q$.

Case(ii). $a-b$ is divisible by 2 but not by 3.

Then (2.1.1.) implies that $c-d \equiv 0 \pmod 3$ which implies that $2(c-d) \equiv 0 \pmod 6$ showing that $2\beta \in Q$.

Case(iii). $a-b$ is divisible by 3 but not by 2.

Then $c-d \equiv 0 \pmod 2$ so that $3(c-d) \equiv 0 \pmod 6$ implying that $3\beta \in Q$. □

2.2 QUASI-PRIME IDEALS

Theorem 8 leads to the notion of a *quasi-prime ideal* defined as follows :

2.2.1 Definition . Let R be a commutative ring with unity. A proper ideal Q of R is called a *quasi-prime ideal* if there exists a positive integer k such that whenever $\alpha\beta \in Q$ with $\alpha, \beta \in R$, either $k\alpha \in Q$ or $k\beta \in Q$.

We note that the positive integer k depends on the product $\alpha\beta \in Q$. It is obvious that every prime ideal of R is a quasi-prime ideal. Theorem 8 shows that is $R = \mathbb{Z}[\sqrt{-p}\,]$, p, a prime, $p \equiv 2 \pmod 3$, then $Q = \{a+b\sqrt{-p} \equiv 0 \pmod 6)\}$ is a quasi-prime ideal.

Consider $R = \mathbb{Z}[\sqrt{-p}\,]$, $p \equiv 2 \pmod 3$ as an MND, with the norm $N(a+b\sqrt{-p}) = a^2+pb^2$. Then every ideal of R is a quasi-prime ideal. For, let Q be any ideal of R. Let $\alpha\beta \in Q$ where $\alpha, \beta \in R$. If $\alpha=a+b\sqrt{-p}$, write $\bar{\alpha} = a-b\sqrt{-p} \in R$ and by the definition of an ideal $\bar{\alpha}\,(\alpha\beta) \in Q$ implying $(a^2 + pb^2)\,\beta \in Q$ or $N(\alpha)\,\beta \in Q$ and so Q is a quasi-prime ideal.

More generally if R is any MND with a norm N satisfying $\alpha | N(\alpha)$ for every $0 \neq \alpha \in R$, then every ideal of R is quasi-prime.

In particular $<1 + \sqrt{-5}>$ is a quasi-prime ideal of $\mathbb{Z}[\sqrt{-5}]$. Since $1+\sqrt{-5}$ is not a prime element, we have already mentioned that $<1+\sqrt{-5}>$ is not a prime ideal.

We proceed to characterize quasi-prime ideals . The motivation is from the structure of the quotient ring $\frac{\mathbb{Z}[\sqrt{-5}]}{<1+\sqrt{-5}>}$. Since $<1+\sqrt{-5}>$ is proper ideal of $\mathbb{Z}[\sqrt{-5}]$ and it is not a prime ideal, the quotient ring is not an integral domain .

Let R be a commutative ring with unity and having divisors of zero. The zero divisors of R can be put into two disjoint subsets T and F such that

(i) T contains those zero divisors which are *torsion elements* in (R, +). That is each zero divisor belonging to T is of *finite order* .

(ii) F contains those zero divisors which are *torsion-free elements* in (R, +).

If R is of finite characteristic n (>0) and has zero divisors, *then all the zero divisors* of R are torsion elements. In particular, the zero divisors of $\mathbb{Z}_n$ (n composite) are of finite additive order.

Let R be any commutative ring with unity of characteristic zero and having zero divisors. Then the set $S = R \times \mathbb{Z}_n$ where n is composite , is a commutative ring with unity with respect to addition and multiplication defined by

$$(r, a) + (s, b) = (r + s, a +_n b)$$
$$(r, a) \quad (s, b \quad = (rs, a \; x_n \; b)$$

where $+_n$ and x_n denote the addition and multiplication modulo n. S has zero divisors that are either torsion elements or torsion-free elements.

2.2.2 Definition . Let R be a commutative ring with unity and possessing a non empty subset T of zero divisors which are torsion elements in (R, +). R is called *a quasi-integral domain* if whenever $\alpha, \beta \in R$ with $\alpha\beta = 0$, either $\alpha \in T$ or $\beta \in T$.

For example, $\mathbb{Z}_n$(n composite) is a quasi-integral domain.

Theorem 9. Let R be a commutative ring with unity. Suppose that Q is a proper ideal of R which is not a prime ideal. Then Q is a *quasi-prime ideal* if and only if R/Q is a *quasi-integral domain.*

Proof : Suppose that Q is a quasi-prime ideal of R. Assume that $(a+Q)(b+Q) = Q$; $a,b \in R$. Then one has $ab \in Q$, which by the definition of a quasi-prime ideal implies that there is a positive integer k such that $ka \in Q$ or $kb \in Q$. This in turns implies that either $a + Q$ or $b + Q$ is a torsion element in the additive group of R/Q. Hence R/Q is a quasi-integral domain.

Conversely assume that R/Q is a quasi-integral domain. Suppose that $ab \in Q$, with $a,b \in R$.

Then $Q = ab + Q = (a + Q)(b + Q)$. So there exists a positive integer k such that $k(a + Q) = Q$ or $k(b + Q) = Q$, that is such that $ka \in Q$ or $kb \in Q$. Hence Q is a quasi-prime ideal. □

Remark : There is a notion of a quasi-ideal of a semigroup or a ring introduced by O. Steinfeld and studied extensively by himself and others. A systematic survey of the most important results of quasi-ideals in semigroups and rings is contained in the monograph authored by

O. Steinfeld (see [36]). The notion of a quasi-prime ideal is not related to that of a quasi-ideal and is new as far as we know. There is also a notion of a quasi-field introduced by P. Kesava Menon (see [25] in 1963.

THE DIRICHLET ALGEBRA OF ARITHMETIC FUNCTIONS

Rajendran Valiaveetil "A study of normed division domains and their analogues with applications to number theory" Thesis. Department of Mathematics , University of Calicut, 1996

CHAPTER 3

THE DIRICHLET ALGEBRA OF ARITHMETIC FUNCTIONS

By an arithmetic function we mean a complex-valued function defined for all positive integers. We denote the set of positive integers by $\mathbb{Z}^+$, the field of complex numbers by $\mathbb{C}$ and he set of all arithmetic functions by $\mathcal{A}$. For f, $g \in \mathcal{A}$, we define their sum (sometimes called natural sum) and *Dirichlet convolution or product* by

(3.0.1) $$(f+g)(r) = f(r) + g(r), \quad r \geq 1$$

(3.0.2) $$(f.g)(r) = \sum_{d \mid r} f(d)\, g(r/d), \quad r \geq 1$$

where the summation is over the divisors d of r. It can be easily verified that $(\mathcal{A}, +, .)$ is a commutative ring with unity e_o defined by

(3.0.3) $$e_o(r) = \begin{cases} 1 & \text{for } r = 1 \\ 0 & \text{for } r \neq 1 \end{cases}$$

It is known ([35], p.30) that $\mathcal{A}$ is infact a UFD . An algebraic study of the ring $\mathcal{A}$ has also been made by H.N. Shapiro in [32].

(3.0.4) LEMMA . $(\mathcal{A},+,.)$ is an MND.

Proof : Following E.D. Cashwell and C.J. Everett [5], we define the norm N(f) of $0 \neq f \in \mathcal{A}$ to be the least positive integer n such that $f(n) \neq 0$; if f is the zero function define $N(f) = N(0) = 0$.

Let $f, g \in \mathcal{A}$, both non zero. Suppose $N(f)=m$ and $N(g)=n$. We may assume that $m \leq n$.

Then $(f.g)(r) = 0$ for all $r \in \mathbb{Z}^+$ with $r<mn$.

Also $(f.g)(mn) = f(m)\, g(n) + f(n)\, g(m)$

$$= \begin{cases} 2\, f(m)\, g(m), & m = n \\ f(m)\, g(n), & m < n \end{cases}$$

so that $(f.g)(mn) \neq 0$.

$$\text{Thus } N(f.g) = mn = N(f)\, N(g).$$

Since $N(0) = 0$, we have $N(fg) = N(f)\, N(g)$ for all $f, g \in \mathcal{A}$. Thus $\mathcal{A}$ is an MND. □

Remark : It is known that an arithmetic function f possesses a Dirichlet inverse if and only if $f(1) \neq 0$ ([35], p. 6) Thus $f \in \mathcal{A}$ is a unit if and only if $N(f) = 1$.

Now consider the MND $\mathcal{A}$. For $f \in \mathcal{A}$ and $\alpha \in \mathbb{C}$ define

$$(\alpha f)(r) = \alpha f(r) \text{ for all } r \in \mathbb{Z}^+.$$

Then it follows that with repect to the sum defined by (3.0.1) and the scalar multiplication defined above $\mathcal{A}$ is an infinite dimensional vector space over $\mathbb{C}$. Thus $\mathcal{A}$ is indeed an algebra over $\mathbb{C}$ with identity e_0 defined by(3.0.3).

We call it the *Dirichlet algebra* $\mathscr{A}$ over $\mathbb{C}$. The purpose of this chapter is to study the *ring structure* of $\mathscr{A}$.

3.1 THE MND $\mathscr{A}$

We recall the definition of a *local ring* :

3.1.1 Definition ([27], p. 33) . A commutative ring with unity is called a *local ring* if it has exactly one maximal ideal.

3.1.2 Lemma : Let R be a commutative ring with unity If ϕ is a homomorphism of the ring R onto a field, then ker ϕ is a maximal ideal of R.

Proof is omitted.

Theorem 10. $\mathscr{A}$ is a *local ring.*

Proof : Define $\phi : \mathscr{A} \longrightarrow \mathbb{C}$ by

$$\phi(f) = f(1), \quad f \in \mathscr{A}.$$

For $f, g \in \mathscr{A}$

$$\phi(f+g) = (f+g)(1) = f(1) + g(1)$$

$$\phi(fg) = (f.g)(1) = f(1)\, g(1)$$

So $\phi : \mathscr{A} \longrightarrow \mathbb{C}$ is a homomorphism. Further ϕ is onto since given $c \in \mathbb{C}$, we have the preimage of c defined by

$$f(r) = \begin{cases} c, & r = 1 \\ 0, & \text{otherwise} \end{cases}$$

Then by Lemma 3.1.2, ker Φ is a maximal ideal of $\mathcal{A}$. Since $f \in \mathcal{A}$ is a unit if and only if $f(1) \neq 0$, we see that ker Φ consists of all the nonunits in $\mathcal{A}$. Now any proper ideal of $\mathcal{A}$ consists of nonunits and hence contained in ker Φ. So ker Φ is the only maximal ideal of $\mathcal{A}$. Thus $\mathcal{A}$ is a *local ring.*

Next, we consider decomposition of $\mathcal{A}$. We need the following :

3.1.3 Definition ([2], p. 201) . Let $\{R_i\}$ be a family of rings indexed by some set I. The *complete direct sum* of the rings R_i denoted by $\Sigma \oplus R_i$ consists of all functions a defined on the index set I subject to the condition that for each element $i \in I$ the functional value a(i) lies in R_i. That is

$$\Sigma \oplus R_i = \{a \mid a : I \longrightarrow \cup R_i \text{ and } a(i) \in R_i\}$$

The rings R_i are called the component rings of the sum $\Sigma \oplus R_i$.

With respect to addition and multiplication defined by componentwise, $\Sigma \oplus R_i$ becomes a ring. The zero element of $\Sigma \oplus R_i$ is the function $0 : I \longrightarrow \cup R_i$ defined by $0(i) = 0$ for all $i \in I$. If $I = \mathbb{Z}^+$, then $\Sigma \oplus R_i$ may be viewed as the set of all infinite sequences $(a_1, a_2, \ldots, a_n, \ldots)$ such that $a_i \in R_i$ for each $i \in I$.

A special subring of the complete direct sum $\Sigma \oplus R_i$ is the *subdirect sum* :

3.1.4 Definition ([2], p. 206) . A subring S of the complete direct sum $\Sigma \oplus R_i$ is said to be *subdirect sum of* the rings, written $S = \Sigma^s \oplus R_i$ if the induced projection $\pi_i | S : S \longrightarrow R_i$ is an onto mapping for each i. The subdirect sum is *nontrivial* if none of the mappings $\pi_i | S$ is *one to one* (hence S is not isomorphic to any R_i).

3.1.5 Lemma ([2], p. 206) . A ring R is isomorphic to a subdirect sum of rings R_i if and only if there exists an isomorphism $f : R \longrightarrow \Sigma \oplus R_i$ such that for each i, the composite $\pi_i \cdot f$ is a homomorphism of R onto R_i.

3.1.6 Lemma ([2], p.207). A ring R is isomorphic to a subdirect sum of rings R_i if and only if R contains a collection of ideals $\{I_i\}$ such that $R/I_i \approx R_i$ and $\cap I_i = \{0\}$.

For the proof of the above two Lemmas, see D.M. Burton ([2], pp. 206-207).

In the context of the ring $\mathcal{A}$, we have an infinite number of primes (cf, [20], p. 103) x_p in $\mathcal{A}$ given by

$$x_p\ (r) = \begin{cases} 1, & r = p \\ 0, & \text{otherwise} \end{cases}$$

for each prime $p \in \mathbb{Z}^+$. For fixed prime p, $N(x_p) = p$. Let I_p denote the principal ideal, generated by x_p.

Denote the quotient ring $\mathcal{A}/I_p$ by Q_p.

Theorem 11 : The ring $\mathcal{A}$ is a *subdirect sum* of the rings Q_p, where p runs through the primes in $\mathbb{Z}^+$.

Proof. The proof follows from Lemma 3.1.5. by observing that $\{I_p\}$ is a collection of ideals and $\bigcap_p I_p = \{0\}$. □

Remark: The subdirect sum $\sum_p^s \oplus Q_p$ is nontrivial since $I_p \neq \langle 0 \rangle$ for all p.

3.1.7. Definition ([2], p. 211) A ring R is said to be *subdirectly irreducibe* if in any representation of R as a subdiect sum of rings R_i, *at least* one of the associated homomorphisms of R onto R_i is actually an isomorphism. Otherwise R is said to be *reducible*.

We observe that $\mathcal{A}$ has a set a nonzero ideals I_p with zero intersection. A theorem of Birkhoff ([2], p 212) states that every commutative ring R with unity is isomorphic to subdirect sum of subdirectly irreducible rings. In particular $\mathscr{A}$ also possesses this property.

Theorem 12* : Let f be a nonzero element of $\mathscr{A}$. Let I_f be the ideal which is maximal in the family of ideals of $\mathscr{A}$ which excludes f. Then $\mathscr{A}$ is isomorphic to the subdirect sum of the subdirectly irreducible rings $\mathscr{A}/I_f$.

Proof : The proof follows in the same lines as the proof of Birkhoff's theorem ([2], p.212). □

3.2 CHAINS OF IDEALS IN $\mathscr{A}$.

We need the following definitions :

3.2.1 Definition ([2], p. 223) . Let R be a commutative ring with unity. R is said to satisfy the *descending chain condition* for ideals if, given any descending chain of ideals of R,

$$I_1 \supseteq I_2 \supseteq \ldots\ldots \supseteq I_n \supseteq \ldots\ldots,$$

there exists an integer n such that $I_n = I_{n+1} = I_{n+2} = \ldots$

If R satisfies descending chain condition for ideals then R is said to be *Artinian* .

3.2.2 Definition ([2], p. 81) . Let R be a commutative ring with unity. An ideal I of R is called *primary* if the conditions $ab \in I$ and $a \notin I$ together imply that $b^n \in I$ for some positive integer n.

3.2.3 Lemma : Let $I_k = \{ f \in \mathcal{A} : N(f) \geq k \} \cup \{0\}$.
Then I_k is a primary ideal for $k \geq 1$.

Proof : It is easy to see that I_k is an ideal of $\mathcal{A}$ for each $k \geq 1$. Let $f, g \in I_k$. If $f \neq 0$,

then $N(fg) \geq k$ or $N(f)\, N(g) \geq k$. Suppose that $N(f) = t$, a positive integer such that $t < k$ and that $f \notin I_k$ then $N(g) \geq k/t$ so that we have $N(g) \geq [k/t] + 1$ since $N(g)$ is an integer, where $[x]$ is the greatest integer not exceeding x. If $[k/t] + 1 = s < k$, then there exists a positive integer m such that $s^m \geq k$. Then $N(g^m) = N(g)^m \geq s^m \geq k$ so that $g^m \in I_k$. Thus I_k is a primary ideal of $\mathcal{A}$. □

Theorem 13 . $\mathcal{A}$ is not *Artinian*.

Proof : From Lemma 3.2.3 we have a strictly descending chain of ideals of $\mathcal{A}$:

$$I_1 \supsetneqq I_2 \supsetneqq I_3 \supsetneqq \cdots$$

So $\mathcal{A}$ is not Artinian.

Remark : We know that *the only integral domains that satisfy descending chain condition are fields* ([2], p. 226) This can be seen as follows :

Let R be an integral domain. Let $0 \neq a \in R$. Since R satisfies descending chain condition, the chain

$$\langle a\rangle \supseteq \langle a^2\rangle \supseteq \ldots\ldots, \text{ must terminate.}$$

So there exist $n \in \mathbb{Z}^+$ such that $\langle a^n\rangle = \langle a^{n+1}\rangle$.

Then there exist $b \in R$ such that $a^n = ba^{n+1}$, using the cancellation law, we get $1 = ba$. This shows that every nonzero element of R has an inverse in R and hence R is a field.

Since $\mathcal{A}$ is an integral domain and it is not a field it follows from the above observation that $\mathcal{A}$ is not Artinian.

CERTAIN NORM PRESERVING LINEAR OPERATORS AND ARITHMETICAL IDENTITIES

Rajendran Valiaveetil “A study of normed division domains and their analogues with applications to number theory” Thesis. Department of Mathematics , University of Calicut, 1996

CHAPTER 4

CERTAIN NORM-PRESERVING LINEAR OPERATORS AND ARITHMETICAL IDENTITIES

In this chapter, we look at the multiplicatively normed domain $\mathscr{A}$ of arithmetic functions from the point of view of its structure as a vector space over $\mathbb{C}$, the field of complex numbers . It is interesting to note that certain arithmetical identities follow as a consequence of some linear operators. In this connection, we point out that certain transformations of arithmetic functions have been considered in various situations different from the present context by L. Carlitz and M.V. Subbarao [4], P.Haukkanen and R. Sivaramakrishnan [18], P. Kesava Menon [24], David Rearick [30].

4.1 A NORM-PRESERVNG LINEAR OPERATOR

We recall the following :

4.1.1 Definition . Let V be a vector space over the field F. A map $L: V \longrightarrow V$ is called a linear operator on V if

$$\text{(i) } L(u+v) = L(u) + L(v) \text{ for all } u, v \in V$$

$$\text{(ii) } L(cu) = c\,L(u) \text{ for all } u \in V,\ c \in F$$

If R is a multiplicatively normed algebra over $\mathbb{C}$, we say that the map $L : R \longrightarrow R$ is norm-preserving if

$$N(L(v)) = N(v) \quad \text{for all } v \in R$$

where $N(v)$ is the norm of $v \in R$.

For $f \in \mathcal{A}$, we define

$$(4.1.2) \qquad (T(f))(r) = \sum_{a=1}^{r} f((a, r)), \qquad r \geq 1$$

where (a,r) denotes the g.c.d of a and r.

By Cesaro's identity [15] whenever $f \in \mathcal{A}$

$$(4.1.3. \qquad \sum_{a=1}^{r} f((a, r)) = \sum_{d \mid r} f(d) \quad \phi(r/d)$$

Where ϕ denotes the Euler ϕ - function.

(4.1.2) and (4.1.3) imply that

$$T(f) = f.\phi$$

Theorem 14. $T : \mathcal{A} \longrightarrow \mathcal{A}$ defined by (4.1.2) is a *bijective norm-preserving linear operator* on $\mathcal{A}$.

Proof : When T is defined by (4.1.2), we have

$$T(f) = f.\phi$$

Where ϕ is the Euler ϕ - function. Since $\mathcal{A}$ is an integral domains it follows that T is one-to-one. Also given $f \in \mathcal{A}$ there exist $f = \phi^{-1} \in \mathcal{A}$ such that

$$T(f.\phi^{-1}) = f$$

so that T is onto.

For $f, g \in \mathcal{A}$

$$T(f+g) = (f+g).\Phi = f.\Phi + g.\Phi = T(f) + T(g)$$

and if $c \in \mathbb{C}$

$$T(cf) = (cf).\Phi = c(f.\Phi) = c\,T(f)$$

Thus T is a linear operator on $\mathcal{A}$.

Finally, for $f \in \mathcal{A}$,

$$N(T(f)) = N(f.\Phi) = N(f)\,N(\Phi) = N(f)1 = N(f)$$

so that T is norm-preserving also. □

Remark : $T^{-1} : \mathcal{A} \longrightarrow \mathcal{A}$ is define byd $T^{-1}(f) = f.\Phi^{-1}$.

But

$$\Phi^{-1}(r) = \sum_{d \mid r} d\,\mu(d)$$

where μ is the Möbius function defined by

$$(4.1.4)\quad \mu(r) = \begin{cases} 1, & r = 1 \\ 0, & \text{if there is a prime } p \text{ such that } p^2 \mid r \\ (-1)^s, & \text{if } r = p_1 p_2 \ldots . p_s,\ p_i \neq p_j \text{ primes} \end{cases}$$

Writing $F(r) = \sum_{d \mid r} f(d)$, we get

$$(4.1.5)\qquad (T^{-1}(f))\,(r) = \sum_{d \mid r} d\, F\,(r/d)\,\mu\,(d)$$

For, $T^{-1}(f) = f.\Phi^{-1} = f.(I^{-1}.e)$ where $I(r) = r$, $r \geq 1$ and $e(r)=1$, $r \geq 1$, and so

$$T^{-1}(f) = (f.e).\ I^{-1} = F\ .\ I^{-1} = F.(I\mu)$$

Hence we obtain (4.1.5).

4.2 TWO LINEAR OPERATORS

We define two linear operators T_1 and T_2 on $\mathcal{A}$ as follows :

For $f \in \mathcal{A}$,

$$(4.2.1) \qquad (T_1(f))(r) = \sum_{d|r} f((d,\ r/d))$$

and

$$(4.2.2) \qquad (T_2(f))(r) = \sum_{d|r} f([d,\ r/d])$$

where $(d,\ r/d)$ and $[d,\ r/d]$ denote the g.c.d and l.c.m of d and r/d, respectively. It can be easily verfied that T_1 and T_2 are linear operators on $\mathcal{A}$.

Theorem 15 . $T_1 : \mathcal{A} \longrightarrow \mathcal{A}$ defined by (4.2.1) satisfies the identity

$$(4.2.3) \qquad (T_1(f))(r) = \sum_{k^2|r} f(k)\ 2^{\omega(r/k^2)}$$

where $\omega(r)$ denotes the number of distinct prime factors of r.

Proof : If t denotes the number of distinct prime factors of r, the number of ways of expressing r as the product of two coprime factors is 2^{t-1}. Suppose $d|r$ and $(d, r/d) = k$ Then $d = kd_1$, $r/d = kd_2$ where $(d_1, d_2) = 1$.

Further $r = k^2 d_1 d_2$ and so $k^2|r$. Thus if $(d, r/d) = k$ we have $k^2|r$.

Conversely if $k^2|r$ and $r = k^2 s$, s can be factored into two coprime factors s_1, s_2 in $2^{\omega(s)-1}$ ways. For each of these ways

$$r = k^2 s_1 s_2 = (ks_1)(ks_2) = d\,(r/d) \text{ with } d = ks, \text{ and } r/d = ks_2$$

Therefore for each k satisfying $k^2|r$, there exist $2^{\omega(s)-1}$ pairs of divisors of d, r/d such that $(d, r/d) = k$. Thus the total number of such divisors is $2.2^{\omega(s)-1} = 2^{\omega(s)}$, where $s = r/k^2$. Now consider the set $\{d_1 = 1, d_2, \ldots, d_n = r\}$ of divisors of r written in ascending order of magnitude. This set is partitioned into mutually disjoint classes.

$$C_1, C_2, \ldots\ldots, C_m$$

such that the class C_k contains those divisor d of r for which $(d, r/d) = k$, if $k^2|r$. The number of elements in the class, C_k is $2^{\omega(r/k^2)}$. We note that C_k is empty if $k^2 \nmid r$. We also note that if d(r) denotes the number of divisors of r, then

$$d(r) = \sum_{k^2 | r} 2^{\omega(r/k^2)}$$

Further $f((d,r/d))$ will occur as $f(k)$ for each d belonging to the class C_k and there are $2^{\omega(r/k^2)}$ elements in C_k. Thus the effect of T_1 on f is as given in (4.2.3) . □

From Theorem 15, we deduce

(4.2.4) Corollary (Daniel I.A. Cohen) (see [6]).

$$\sum_{d|r} (d, r/d) = \sum_{k^2|r} k\, 2^{\omega(r/k^2)}$$

Proof : Take $f(r) = r$ in (4.2.1) and (4.2.3). □

Theorem 16 : $T_2 : \mathcal{A} \longrightarrow \mathcal{A}$ defined by (4.2.2) satisfies the identity

(4.2.6) $$(T_2(f)(r) = \sum_{k^2|r} f(r/k)\, 2^{\omega(r/k^2)}$$

Proof : The proof follows as that of Theorem 15 since we have

$$\left[d, r/d\right] = r\,(d, r/d)^{-1}.$$ □

4.2.7 Corollary .

$$\sum_{d|r} [d, r/d] = \sum_{k^2|r} (r/k) \quad 2^{\omega(r/k^2)}$$

Proof : Take $f(r) = 1$ in (4.2.2) and (4.2.6) . □

Next, we look at the operators T_1 and T_2 more closely. Let $r = s^2 t$, where t is the greatest square-free divisor of r. By Theorem 15,

$$(T_1(f))(r) = \sum_{k|s} f(k)\ 2^{\omega((s^2/k^2)t)}$$

as the square divisors of r are those which divide s.

Moreover $\omega((s^2/k^2)t) = \omega(s^2/k^2) + \omega(t')$ where t' is the greatest square-free divisor of r such that $(t', r/t') = 1$

Therefore since $\omega(s^2/k^2) = \omega(s/k)$, we get

$$(4.2.8) \qquad (T_1(f))\ (r) = 2^{\omega(t')} \sum_{k|s} f(k)\ 2^{\omega(s/k)}$$

One notes from (4.2.8) that if $N(f) = m$, then $N(T_1(f)) = m^2$ For if $m' < m^2$, $m' = u^2 v$ where v is the greatest square-free divisor of m' and $u^2 < m^2$ or $u < m$. This yields

$$(T_1(f))\ (m') = 2^{\omega(v)} \sum_{k|u} f(k)\ 2^{\omega(u/k^2)} = 0$$

Now

$$(T_1(f))\ (m^2) = \sum_{k \mid m} f(k)\ 2^{\omega(m^2/k^2)} = f(m) \neq 0$$

Theorem 17 . The operator T_1 defined by (4.1.1) has the property that $N(T_1(f)) = N(f)$ if and only if f is a unit in $\mathcal{A}$.

Proof : If $N(f) = m$, then we have $N(T_1(f)) = m^2$. Thus $N(T_1(f)) = N(f)$ if and only if $N(f) = 1$, that is if and only if f is a unit in $\mathcal{A}$. □

Analogous to (4.2.8) we get using theorem 16,

(4.2.9) $$(T_2\ (f))\ (r) = 2^{\omega(t')} \sum_{k \mid s} f(r/k)\ 2^{\omega(s/k)}$$

Where $r = s^2 t$ and t' is the greatest square-free divisor of r such that $(t', r/t') = 1$.

Theorem 18 . The operator $T_2 : \mathcal{A} \longrightarrow \mathcal{A}$ defined in (4.2.2) is norm-preserving.

Proof : If $N(f) = m$, then by (4.2.9) for $1 \leq a < m$, we have

$$(T_2(f))\ (a) = 2^{\omega(b')} \sum_{k \mid s} f(a/k)\ 2^{\omega(s/k)}$$

Where $a = s^2 b$ and b' is the greatest square-free divisor of a such that $(b', a/b') = 1$. As $f(a/k) = 0$ for $1 \le k \le s$,

$$(T_2(f))\ (a) = 0 \text{ for } 1 \le a < m$$

It follows that m is the least positive integer such that

$$(T_2(f))\ (m) \ne 0.$$

and therefore $$N(T_2(f)) = m = N(f)\ . \qquad \square$$

4.3 A LINEAR OPERATOR VIA L.C.M. CONVOLUTION

4.3.1 Definition : For f, g $\in \mathcal{A}$, the l.c.m. convolution of f and g denoted by [f,g] is defined by

$$[f,\ g]\ (r) = \sum_{[a,b]\ =\ r} f(a)\ g(b)$$

Where the summation is over all ordered pairs of positive integers a, b such that [a, b] = r.

A connection between l.c.m. convolution and Dirichlet convolution is given by

(4.3.2) $$[f,\ g].\ e = (f.e)\ (g.e)$$

where $e\ (r) = 1,\quad r \ge 1$. (4.3.2) is due to Von Sterneck [15] and fg denote the natural product of f and g :

$$(f\ g)\ (r) = f(r)\ g(r),\ r \geq 1.$$

We introduce an operator $L : \mathcal{A} \longrightarrow \mathcal{A}$ given by

$$(L(f))\ (r) = \sum_{\substack{1 \leq a \leq r \\ [a,b] = r}} f(a)$$

where a is the first coordinate of the ordered pair (a, b) with [a, b] = r.

We note that

$$(4.3.3) \qquad L(f) = [f,e]$$

Theorem 19 . If $f \in \mathcal{A}$ is such that $F = f.e$, then

$$(4.3.4) \qquad (L(f))\ (r) = \sum_{t \mid r} F(t)\ d(t)\ \mu\ (r/t),$$

where μ is the Möbius function and $L : \mathcal{A} \longrightarrow \mathcal{A}$ is a norm-preserving linear operator.

Proof : In terms of l.c.m convolution

$$L(f) = [f,\ e]$$

By Von Sterneck's formula (4.3.2), we have

$$L(f).e = (f.e)\ (e.e)$$

But $(e.e)\ (r) = d(r)$, the number of divisors of r.

Since $F = f.e$, we get

$$(4.3.5) \qquad L(f).\ e = Fd$$

Since the Dirichlet inverse of e is μ, (4.3.5) implies

$$L(f) = Fd.\mu$$

and therefore (4.3.4) follows .

Now it can be easily verified that $L : \mathcal{A} \longrightarrow \mathcal{A}$ is a linear operator. Also,

$$N(L(f)) = N(Fd)\ N(\mu) = N(Fd)1 = N(Fd)$$
$$= N(F) \text{ as } d(r) \neq 0,\ r \geq 1$$
$$= N(f.e) = N(f)\ N(e) = N(f) \text{ as } N(e) = 1$$

Thus L is norm-preserving. □

Remark 1 : It is interesting to observe that in the case of the Möbius function μ,

(4.3.6) $$L(\mu) = \mu$$

For, $L(\mu).e = (\mu.e)\ (e.e) = e_o d = e_o$

So $L(\mu)$ is the Dirichlet inverse of μ and hence $L(\mu) = \mu$

Remark 2. In the case of Euler Φ-function, we obtain

(4.3.7) $$(L(\Phi))\ (r) = \sum_{t \mid r} t\ d(t)\ \mu\ (r/t)$$

The details of simplifications are omitted.

Theorem 20. If L is the linear operator on $\mathcal{A}$ defined by (4.3.4) and if $f = c\mu$, where $c \in \mathbb{C}$ and μ is the Möbius function, then $L(f) = f$. Conversely if $L(f) = f$, $f \in \mathcal{A}$, them $f = c\mu$ where $c = f(1)$.

Proof : The first part of the statement follows from the linearity of L and from Remark 1.

Next suppose that $L(f) = f$, $f \in \mathcal{A}$

Then $Fd.\mu = f$ or $Fd = f.e = F$

so that $F(d-e) = 0$

Since $d(r) \neq e(r)$ for $r > 1$, this implies that $F(r) = 0$ $r \geq 2$. So we may define $F(1) = c$ for some $c \in \mathbb{C}$. Then $f(1) = F(1) = c$. Thus

$$F(r) = \begin{cases} c & r = 1 \\ 0 & r > 1 \end{cases}$$

So

$$f.e = c.e_o$$

Since μ is the Dirichlet inverse of e, this implies $f = c\mu$. $\square$

CERTAIN MULTIPLICATIVELY NORMED RINGS

Rajendran Valiaveetil "A study of normed division domains and their analogues with applications to number theory" Thesis. Department of Mathematics , University of Calicut, 1996

CHAPTER 5

CERTAIN MULTIPLICATIVELY NORMED RINGS

From now on we turn to commutative rings with unity and *having divisors of zero*. We extend the definition of the multiplicative norm *to any commutative ring with unity*.

Definition : Let R be a commutative ring with unity. A multiplicative norm N on R is a function N from R into the set $\tilde{\mathbb{R}}$ of non negative real numbers such that .

(i) $N(0) = 0$

(ii) $N(\alpha\beta) = N(\alpha)\, N(\beta)$ for all $\alpha, \beta \in R$.

R is called a *multiplicatively normed ring,* abbreviated MNR if there is defined a multiplicative norm on it.

If $\alpha \in R$ is a divisor of zero, then there exists $0 \neq \beta \in R$ such that $\alpha\beta = 0$ so that

$$0=N(0) = N(\alpha\beta) = N(\alpha)\, N(\beta)$$

implying either $N(\alpha) = 0$ or $N(\beta) = 0$.

5.1 THE RING $\mathscr{C}([0,1])$

Consider the set $\mathscr{C}([0,1])$ of all real valued continuous functions defined on the closed interval $[0,1]$. If $f, g \in \mathscr{C}([0,1])$, define the sum and product by

$$(f+g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)\, g(x) \quad \text{for all}$$

$x \in [0,1]$.

Then $\mathscr{C}([0,1])$ is a commutative ring with unity, the unity being the constant function 1 defined by $1(x) = 1$ for all $x \in [0,1]$. It can be seen that $\mathscr{C}([0,1])$ has divisors of zero and that if $0 \neq f$, $0 \neq g \in \mathscr{C}[0,1]$ with $fg = 0$ then either $f(0) = 0$ or $g(0) = 0$. For $f \in \mathscr{C}([0,1])$ define norm of f by $N(f) = |f(0)|$. Then N is a multiplicative norm on $\mathscr{C}([0,1])$.

5.2 THE LUCAS RING OF ARITHMETIC FUNCTIONS

A more interesting example of an MNR is the Lucas ring of arithmetic functions introduced by L. Carlitz, [3], described below :

Let F be an arbitrary but fixed field and $\mathfrak{B}$ denote the set of all arithmetic functions defined on the set of nonnegative integers into F. As usual, we define the sum f+g of $f, g \in \mathfrak{B}$ by

$$(f+g)(r) = f(r) + g(r), \quad r=0,1,2.....$$

The Lucas product $f * g$ of $f, g \in \mathscr{B}$ is defined as follows.

Let p be a fixed prime in $\mathbb{Z}^+$. Writing ,

$$r = r_o + r_1 p + r_2 p^2 + \ldots\ldots \qquad (0 \le r_j < p)$$
$$k = k_o + k_1 p + k_2 p^2 + \ldots\ldots \qquad (0 \le k_j < p)$$

then

$$\binom{r}{k} \equiv \binom{r_o}{k_o} \binom{r_1}{k_1} \ldots \pmod p$$

In particular the binomial coefficient $\binom{r}{k}$ is prime to p if and only if

$$0 \le k_j \le r_j \quad (r = 0,1,2,\ldots)$$

Now define $f * g$ by

$$(5.2.1) \qquad (f * g)(r) = \sum_{k=0}^{r}{}' f(k)\, g(r-k)$$

where Σ' is restricted to those k with $p \nmid \binom{r}{k}$.

It can be seen that $(\mathscr{B}, +, *)$ is a commutative ring with unity. The zero element and the unity are respectively the functions defined by

$$z(r) = 0 \qquad r = 0,1,2,\ldots.$$

$$u(r) = \begin{cases} 1 & r = 0 \\ 0 & r > 0 \end{cases}$$

For $f \in \mathcal{B}$, define norm of f by $N(f) = |f(0)|$. Then $\mathcal{B}$ is an MNR.

Let us closely examine the elements of $\mathcal{B}$. A function $f \in \mathcal{B}$ is called singular if $f(0) = 0$; otherwise f is called nonsingular. It can be deduced that $f \in \mathcal{B}$ is invertible if and only if $N(f) \neq 0$. We now prove

Theorem 21. $(\mathcal{B}, +, *)$ is a local ring.

Proof . Let S be the set of all singular elements in $\mathcal{B}$.

For $f, g \in S$, $f - g \in S$ as

$$(f-g)(0) = f(0) - g(0) = 0-0 = 0$$

Next, let $h \in \mathcal{B}$, $f \in S$.

Then $(h * f)(0) = h(0)\, f(0) = 0$ as $f \in S$.

Thus $h * f \in S$. So S is an ideal of $\mathcal{B}$. But S is the set of all non units in $\mathcal{B}$. So it follows that S is the unique maximal ideal of $\mathcal{B}$. Hence $\mathcal{B}$ is a local ring. □

Remark : If we consider the field F to be of positive characteristic, then f is a zero divisor if and only if it is singular [3]. So in this case $f \in \mathcal{B}$ is a zero divisor if and only if $N(f) = 0$.

5.3 THE UNITARY CONVOLUTION RING

Let r be a fixed positive integer. A divisor d of r is called a unitary divisor of r if $(d, r/d) = 1$, where (x, y) denotes the g.c.d of x and y.

Let $\mathcal{A}$ be the set of all arithmetic functions defined on $\mathbb{Z}^+$. For $f, g \in \mathcal{A}$, define the unitary convolution of f and g denoted by $f \oplus g$ as

$$(5.3.1) \qquad f \oplus g\,(r) = \sum_{d \| r} f(d)\, g(r/d)$$

where $d \| r$ means that d runs through the unitary divisors of r. With respect the usual addition and the product defined by (5.3.1), $(\mathcal{A}, +, \oplus)$ is a commutative ring with unity e_o and having zero divisors. ([35], p. 9), where e_o is the function defined by

$$(5.3.2) \qquad e_o\,(r) = \begin{cases} 1 & r = 1 \\ 0 & \text{otherwise} \end{cases}$$

For $f \in \mathcal{A}$, define norm of f by

$$N(f) = |f(1)|$$

Them it follows that $(\mathcal{A}, +, \oplus)$ is an MNR. Also we observe that $f \in \mathcal{A}$ has an inverse (with respect to unitary convolution) if and only if $N(f) \neq 0$.

THE CAUCHY ALGEBRA OF EVEN FUNCTIONS (MOD r)

Rajendran Valiaveetil "A study of normed division domains and their analogues with applications to number theory" Thesis. Department of Mathematics , University of Calicut, 1996

CHAPTER 6

THE CAUCHY ALGEBRA OF EVEN FUNCTIONS (MOD r)

In chapter 3 we considered the Dirichlet algebra of arithmetic functions which is infinite dimensional over $\mathbb{C}$. We now turn over to the case of a *finite dimensional algebra* via Cauchy convolution discussed below : The terminology is due to Eckford Cohen ([7]).

6.0.1 Definition ([35], p. 326) . Let r be an arbitrary but fixed positve integer and F a field of characteristic zero containing r^{th} roots of unity. A function $f : \mathbb{Z} \longrightarrow F$ is called an (r, F) arithmetic function if

$$f(n) = f(m) \text{ whenever } n \equiv m \pmod{r}.$$

6.0.2 Definition ([35], p. 326) . An arithmetic function f is said to be periodic with period r if

$$f(n) = f(n+\lambda r), \ \lambda \in \mathbb{Z}.$$

We call f a periodic function (mod r) .

An (r, F) arithmetic function is clearly a periodic function (mod r). We denote the set of all (r, F) arithmetic functions by $\mathcal{A}_r(F)$.

The Cauchy product of f and $g \in \mathcal{A}_r(F)$ is defined by

$$(f \odot g)(n) = \sum_{n \equiv a+b \pmod r} f(a)\, g(b)$$

where a and b range over the elements of a complete residue system (mod r) such that $n \equiv a+b \pmod r$. The set $\mathcal{A}_r(F)$ forms a commutative ring relative to ordinary addition and Cauchy multiplication . The function u_o defined by

$$u_o(n) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod r \\ 0 & \text{otherwise} \end{cases}$$

serves as the identity under Cauchy multiplication.

6.0.3 Definition ([35], p. 335) . $f \in \mathcal{A}_r(F)$ is said to be an even function of n (mod r) or briefly an even function (mod r) if

$$f(n) = f((n, r))$$

where (n,r) denotes the g.c.d. of n and r.

We consider the case $F = \mathbb{C}$, the field of complex numbers. Then the set $\mathcal{B}_r(\mathbb{C})$ of even functions (mod r) is a subset of the set $\mathcal{A}_r(\mathbb{C})$ of $(r, \mathbb{C})$ arithmetic functions. The properties of $\mathcal{B}_r(\mathbb{C})$ have been studied extensively by E. Cohen in a series of papers ([7], [8] [9] [10], [11] and [14]), P. Haukkanen and R. Sivaramakrishnan in ([19]). The purpose of this chapter is to point out certain properties of $\mathcal{B}_r(\mathbb{C})$ relevant to the main theme of this work , as a multiplicatively normed ring.

6.1 THE MNR $\mathfrak{B}_r$ ($\mathbb{C}$)

We recall that the Ramanujan's sum is defined by

$$(6.1.1.)\qquad C(n,\ r) = \sum_{\substack{h \ (\mathrm{mod}\ r) \\ (h,r)=1}} \exp\,(2\pi i h n/r)$$

Where h runs through a reduced residue system (mod r).

We also need the orthogonal property of C(n,r) in the following two forms :

$$(6.1.2)\qquad \sum_{n \equiv a+b \ (\mathrm{mod}\ r)} C(a,d_1)\ C(b,\ d_2) = \begin{cases} r\ C\ (n,\ d), \text{ if } d_1 = d_2 = d \\ 0, \quad \text{otherwise} \end{cases}$$

$$(6.1.3)\qquad \sum_{t \mid r} C\ (r/t,\ d_1)\ C\ (r/d_2, t) = \begin{cases} r, \quad \text{if } d_1 = d_2 \\ 0, \quad d_1 \neq d_2 \end{cases}$$

where d_1, d_2 are divisors of r.

Further , the following result

$$(6.1.4)\qquad \phi\ (d_1)\ C\ (r/d_1,\ d_2) = \phi(d_2)\ C\ (r/d_2,\ d_1)$$

where ϕ is the Euler ϕ-function; d_1, d_2 are divisors of r is also needed.

We first prove two important theorems, due to E. Cohen

Theorem 22* ([35], p. 335) . If $f \in \mathfrak{B}_r(\mathbb{C})$, then f has the representation

$$(6.1.5) \qquad f(n) = \sum_{d|r} \alpha(d)\, C\,(n, d)$$

where the coefficients $\alpha(d)$ are uniquely determined by

$$(6.1.6) \qquad \alpha(d) = (1/r) \sum_{\delta|r} f\,(r/\delta)\, C(r/d, \delta)$$

or equivalently by

$$(6.1.7) \qquad \alpha(d) = (r\Phi(d))^{-1} \sum_{j=1}^{r} f(j)\, C(j, d)$$

Where $C(n, r)$denotes the Ramanujan sum defined by (6.1.1) .

Proof : ([35], p.336) : If f has the representation given by (6.1.5), then

$$\sum_{d|r} \alpha(d)\, C(n,d) = (1/r) \sum_{\delta|r} f\,(r/\delta) \sum_{d|r} C\,(n,d)\, C\,(r/d, \delta)$$

Since $C\,(n, r)$ is an even function (mod r), we have $C(n,d) = C(s,d)$, where $s = (n, r)$. Therefore

$$\sum_{d|r} \alpha(d) C(n,d) = (1/r) \sum_{\delta|r} f\,(r/\delta) \sum_{d|r} C\,(s,d)\, C\,(r/d, \delta)$$

By the orthogonal property of $C(n,r)$ in the form (6.1.3) we have

$$\sum_{d|r} C(s,d)\, C(r/d, \delta) = \begin{cases} r & \text{if } r/s = \delta \\ 0 & \text{otherwise} \end{cases}$$

So

$$\sum_{d|r} \alpha(d)\, C(n,d) = (1/r) \sum_{\delta|r} f(r/\delta)\, \eta(s, \delta)$$

Where

$$\eta(s, \delta) = \begin{cases} r & \text{if } r = s\,\delta \\ 0 & \text{otherwise} \end{cases}$$

Thus

$$\sum_{d|r} \alpha(d)\, C(n,d) = f(s) = f(n) \text{ as } s = (n,r).$$

This proves (6.1.5)

Since $C(n,r) \in \mathcal{B}_r(\mathbb{C})$, the functions f given by (6.1.5) belong to $\mathcal{B}_r(\mathbb{C})$. Now the set $\{ r^{-1} C(n, d) : d|r\}$ forms a linearly independent set. For suppose

$$g(n) = \sum_{\delta|r} a_\delta\, C(n,\delta) = 0,\ a_\delta \in \mathbb{C} \text{ and } C(n,\delta) \neq 0 \text{ for } \delta|r.$$

Let d be a fixed divisor of r. Then taking $h(n) = C(n,d)$ and using the orthogonal property of $C(n,r)$ in the form (6.1.2.) we obtain

$$(h \odot g)(n) = \sum_{n \equiv a+b \pmod r} h(a)\, g(b)$$

$$= \sum_{n \equiv a+b \pmod r} C(a,d) \sum_{\delta | r} a_\delta\, C(b, \delta)$$

$$= \sum_{\delta | r} a_\delta \,) \sum_{n \equiv a+b \pmod r} C(a, d)\, C(b, \delta)$$

$$\begin{cases} r\, a_d\, C(n,d) & \text{if } \delta = d \\ 0 & \text{otherwise} \end{cases}$$

Hence $g(n) = 0$ implies $a_d = 0$ for each $d|r$. Thus the representation (6.1.5) of f is unique.

To obtain the expression for $\alpha(d)$ given in (6.1.6) we note that a residue system (mod r) could be replaced by a residue system $z = (r/\delta)\, x$, $\delta | r$, $(x, \delta) = 1$, by the class division of integers (mod r)

Therefore

$$(6.1.8) \qquad (r\phi\, (d))^{-1} \sum_{j=1}^{r} f(j)\, C(j,d)$$

$$= (r\, \phi(d))^{-1} \sum_{\delta | r} f(rx/\delta)\, C(rx/\delta,\, d)$$

Since $f(n)$ and $C(n,r)$ are is $\mathcal{B}_r(\mathbb{C})$, we get

$$(r\phi(d))^{-1} \sum_{\delta | r} \sum_{x \pmod \delta} f(rx/\delta)\, C(rx/\delta,\, d)$$

$$= (r\ \Phi\ (d))^{-1} \sum_{\delta | r} f(r/\delta)\ C(r/\delta,\ d)\ \Phi\ (\delta)$$

$$= (r\Phi(d))^{-1} \sum_{\delta | r} f(r/\delta)\ C(r/d,\ \delta)\ \Phi(d) \quad \text{, by (6.1.4)}$$

$$= r^{-1} \sum_{\delta | r} f(r/\delta)\ C(r/d,\ \delta)$$

$$= \alpha(d)$$

Now (6.1.8) implies that

$$\alpha(d) = (r\Phi(d))^{-1} \sum_{j=1}^{r} f(j)\ C(j,d). \qquad \Box$$

Remark : The coefficients $\alpha(d)$ occuring in the expansion (6.1.5) of $f(n)$ are called the Fourier coefficients of f.

Theorem 23* [[35], p. 338) . Let $f,\ g \in \mathcal{B}_r\ (\mathbb{C})$ with Fourier coefficients $\alpha(d)$ and $\beta(d)$ respectively. The Cauchy product $f \odot g$ of f and g is given by

$$(6.1.9\ ) \quad (f \odot g)\ (n) = r \sum_{d | r} \alpha(d)\ \beta(d)\ C(n,d)$$

Proof ([35] p. 338) : We have

$$f(n) = \sum_{d_1 | r} \alpha(d_1)\ C(n,d_1)$$

and

$$g(n) = \sum_{d_2 | r} \beta(d_2)\ C\ (n,d_2)$$

By definition

$$(f \odot g)(n) = \sum_{n \equiv a+b \pmod r} f(a)\, g(b)$$

$$= \sum_{d_1 | r, d_2 | r} \alpha(d_1)\, \beta(d_2) \sum_{n \equiv a+b \pmod r} C(a, d_1)\, C(b, d_2)$$

$$= r \sum_{d | r} \alpha(d)\, \beta(d)\, C(n,d),$$ by the orthogonal property (6.1.2) of $C(n,r)$.

With respect to pointwise addition and Cauchy multiplication $\mathscr{B}_r(\mathbb{C})$ is a commutative ring with unity u_o defined by

$$u_o(n) = \begin{cases} 1, & \text{if } n \equiv o \pmod r \\ 0, & \text{otherwise} \end{cases}$$

Further if define multiplication by scalar by

$$(cf)(r) = cf(r), \quad c \in \mathbb{C}, \; f \in \mathscr{B}_r(\mathbb{C})$$

it follows that $\mathscr{B}_r(\mathbb{C})$ is also a vector space over $\mathbb{C}$. Thus $\mathscr{B}_r(\mathbb{C})$ is indeed an algebra are $\mathbb{C}$, we call it the Cauchy algebra of even function (mod r) In fact $\mathscr{B}_r(\mathbb{C})$ is a finite dimensional complex vector space of dimension $d(r)$ (cf, [26], p. 194). Also $\mathscr{B}_r(\mathbb{C})$ is a Hilbert space with respect to the inner product

$$\langle f,g\rangle = \sum_{a \pmod r} f(a)\, \overline{g(a)}$$

where $\overline{g(a)}$ denotes the complex conjugate of $g(a)$

and

$$\{ (r\, \Phi(d))^{-1/2} C(n,d) : d \mid r) \}$$

is an orthonormal basis for $\mathcal{B}_r(\mathbb{C})$ ([19]), Theorem 5).

Theorem 24 : $\mathcal{B}_r(\mathbb{C})$ is an MNR.

Proof : Define $N : \mathcal{B}_r(\mathbb{C}) \longrightarrow \tilde{\mathbb{R}}$ by

$$N(f) = r \min_d \{ |\alpha(d)| \}$$

where the minimum is taken over the divisors of d of r and $\alpha(d)$, $d \mid r$ are the Fourier coefficients of f. If $g \in \mathcal{B}_r(\mathbb{C})$ with Fourier coefficients $\beta(d)$, $d \mid r$.

then $$N(g) = r \min_d \{ | (\beta(d) | \}$$

By (6.1.9), the Fourier coefficients of $f \odot g$ are $r\, \alpha(d)\, \beta(d)$, so that we have

$$N(f \odot g) = r \min_d \{ r |\alpha(d)| \beta(d) | \}$$

$$= r \min_d \{ |\alpha(d)| \}\ r \min_d \{ |\beta(d)| \}$$

$$= N(f)\ N(g)$$

Remark 1 Since u_o has the representation

$$u_o(n) = \sum_{d|r} r^{-1} C(n,d)$$

We have

$$N(u_o) = r \min_d \{r^{-1}\} = 1$$

Remark 2 Since

$$C(n,r) = \sum_{d|r} e_o(r/d)\, C(n,d)$$

$$N(C) = r \min_d \{|e_o(r/d)|\} = 0$$

as $e_o(r) = 1$ when $r = 1$ and is zero for $r \geq 2$.

6.2 SOME LINEAR OPERATORS ON $\mathcal{B}_r(\mathbb{C})$

We consider some mappings on the algebra $\mathcal{B}_r(\mathbb{C})$. Among the norm-preserving algebra homomorphisms on $\mathcal{B}_r(\mathbb{C})$ we have the identity homomorphism $I : \mathcal{B}_r(\mathbb{C}) \longrightarrow \mathcal{B}_r(\mathbb{C})$ given by $I(f) = f$ and the conjugation map

$\bar{I} : \mathcal{B}_r(\mathbb{C}) \longrightarrow \mathcal{B}_r(\mathbb{C})$ given by $\bar{I}(f) = \bar{f}$ where $\bar{f}$ is defined by

$$\bar{f}(n) = \sum_{d|r} \overline{\alpha(d)}\, C(n,d)$$

$\overline{\alpha(d)}$ being the complex conjugate of the Fourier coefficient $\alpha(d)$ of f.

We now proceed to discuss a linear operator on the vector space $\mathcal{B}_r(\mathbb{C})$ obtained by via the following analogue of $C(n,r)$, (see, [12]). As in [34] we write

$$(6.2.1) \qquad B(n,r) = \sum_{\substack{h \ (\mathrm{mod}\ r) \\ (h,r) = \text{ a square}}} \exp\ (2\pi inh/r)$$

where the summation is over a residue system h (mod r) such that (h, r) is a square.

We recall that an arithmetic function f is said to be mutliplicative if $f(mn) = f(m)\ f(n)$ whenever $(m,n) = 1$. f is said to be completely multiplicative if $f(mn) = f(m)\ f(n)$ for all $m, n \in \mathbb{Z}^{+}$.

Following the terminology of E. Cohen [8], $f \in \mathfrak{X}_r(\mathbb{C})$ is said to be completely even (mod r) if there exist some arithmetic function F such that

$$f(n) = \sum_{d \mid (n,r)} F(d)$$

Let $\Omega(r)$ denotes the *total* number of prime factors of r, *each factor being counted according to its multiplicity* The function defined by $\lambda(r) = (-1)^{\Omega(r)}$, $r = 1,2,3\ldots$ is called the Liouville's function and it is completely multiplicative. Then $\mathcal{B}(n,r)$ has the representation

$$(6.2.2) \qquad B(n,r) = \sum_{d \mid (n,r)} \lambda(r/d)\ d = \lambda\ (r/g)\ b(g)$$

where $g = (n,r)$ and $b(r) = B(0,r)$.

Since λ is completely multiplicative, one has

$$(6.2.3) \quad \lambda(r)\ B(n,r)=\lambda(r)\ b(g)=\lambda(g) \sum_{d\mid g} \lambda(g/d)\ d = \sum_{d\mid g} d\ \lambda(d)$$

This shows that $\lambda(r)\ B(n,r)$ is a completely even function (mod r). In § 6.3. we will see that the set of all completely even functions (mod r) forms a subspace of $\mathcal{B}_r(\mathbb{C})$ having dimension $2^{\omega(r)}$, the number of square-free divisors of r.

It is known [34] that

$$(6.2.4) \qquad B(n,r) = \sum_{dD^2 = r} C(n,d)$$

so that $B(n,r)$ has a representation of the form

$$B(n,r) = \sum_{d\mid r} \in (r/d)\ C(n,d)$$

where

$$(6.2.5) \qquad \in (r) = \begin{cases} 1, & \text{if } r \text{ is a perfect square} \\ 0, & \text{otherwise} \end{cases}$$

Therefore

$$(f \odot B)\ (r) = r \sum_{d\mid r} \alpha(d) \in(r/d)\ C(n,d)$$

Where $\alpha(d)$, are the Fourier coefficients of f. So we get

$$r^{-1}\ (B \odot f)\ (r) = \sum_{\substack{d\mid r \\ dD^2=r}} \alpha(d)\ C(n,d)$$

Let us now define $T : \mathcal{B}_r(\mathbb{C}) \longrightarrow \mathcal{B}_r(\mathbb{C})$ by

$$T(f) = r^{-1} B \odot f$$

Then T is a linear operator on $\mathcal{B}_r(\mathbb{C})$, but T is not norm-preserving as $N(B) = 0$.

6.3 THE SUBSPACE OF COMPLETELY EVEN FUNCTIONS (MOD r)

Analogous to the orthogonal property of the Ramanujan's sum $C(n,r)$, we have for $B(n,r)$

Theorem 25. If t_1 and t_2 are square-free divisors of r

$$(6.3.1)\qquad \sum_{n \equiv a+b \pmod r} B(a, r/t_1)\, B(b, r/t_2) = \begin{cases} r\, B(n, r/t) & \text{if } t_1 = t_2 = t \\ 0 & \text{if } t_1 \neq t_2 \end{cases}$$

Proof : Using (6.2.4) we have

$$\sum_{n \equiv a+b \pmod r} B(a, r/t), B(b, r/t_2) = \sum_{n \equiv a+b \pmod r} \Big(\sum_{d_1 D_1^2 = r/t_1} C(a,d_1)\Big) \Big(\sum_{d_2 D_2^2 = r/t_2} C(b, d_2)\Big)$$

$$= \sum_{\substack{d_1 D_1^2 = r/t_1 \\ d_2 D_2^2 = r/t_2}} \sum_{n \equiv a+b \pmod r} C(a,d_1)\, C(b,d_2)$$

Using the orthogonal property of $C(n,r)$ the inner sum can be simplified further. If $d_1 = d_2 = d$, it reduces to $r\, C(n,d)$ and is zero if $d_1 \neq d_2$ When $d_1 = d_2 = d$ we have $dD_1^2 = r/t_1$, $dD_2^2 = r/t_2$ and so $t_1 D_1^2 = t_2 D_2^2$. But t_1 and t_2 are square-free

If $t_1 \neq t_2$ either t_1 or t_2 has a prime factor not occuring in the other. If t_1 has a prime factor p_1 not occuring in t_2, this prime factor will have to occur in D_2^2 and in that case D_2^2 will cease to be a square. Similarly if t_2 has a prime factor p_2 not occurring in t_1 the it will spoil the square nature of D_1^2. So $d_1=d_2$ will imply that $t_1=t_2=t$ (say). But then $D_1^2 = D_2^2 = D^2$ (say)

Therefore the sum simplifies to

$$\begin{cases} r \sum\limits_{dD^2=r/t} C(n,d) & \text{if } t_1 = t_2 = t \\ 0, & \text{otherwise} \end{cases}$$

(6.2.4) now yields the required result. □

Next we note that $B(a,r) = B(-a,r)$. For it $(h,r) = x^2$ with $1 \leq h \leq r$, $(r-h, r)$ also equal to x^2. Taking $n=0$, in (6.3.1) we obtain :

6.3.2 Corollary . If t_1 and t_2 are square-free divisors of r, then

$$\sum_{a \pmod r} B(a, r/t_1)\, B(a, r/t_2) = \begin{cases} r\, b(r/t) & \text{if } t_1=t_2=t \\ 0 & \text{otherwise} \end{cases}$$

We now state

Theorem 26. The set $V_r(\mathbb{C})$ of completely even functions (mod r) forms a subspace of $\mathscr{B}_r(\mathbb{C})$ having dimension $2^{\omega(r)}$ the number of square-free divisors of r. $V_r(\mathbb{C})$ has an orthonormal basis

$$\{\lambda(r/t)\ (r\ b(r/t))^{-1/2}\ B(n,r/t) : t \text{ a square-free divisor of } r\}$$

Proof : The proof follows along the same lines as that of the proof of Theorem 5 of [19]or the proof of Theorem 2.1 of Chapter 7 of [26].

We mention that Cohen [13] considered the unitary analogue $C^*(n,r)$ of $C(n,r)$ and obtained another subspace $W_r(\mathbb{C})$ of $\mathscr{B}_r(\mathbb{C})$ of dimension $2^{\omega(r)}$, the number of square-free divisors of r.

APPENDIX

k-FOLD NIL RADICAL OF AN IDEAL

Let R be a commutative ring with unity and I be an ideal of R. We recall that the *nil radical* of I denoted by $\sqrt{I}$ is given by

$$\sqrt{I} = \{r \in R : r^n \in I \text{ for some } n \in \mathbb{Z}^+ \text{ where } n \text{ depends on } r\}$$

Let k be an arbitrary but fixed positive integer. We define the k-fold nil radical of I to be the set

$$\sqrt{I_k} = \{ r \in R : kr^n \in I \text{ for some } n \in \mathbb{Z}^+ \text{ depending on } r\}$$

We observe that $\sqrt{I_k}$ is an ideal of the ring R. For, if a and b are elements of $\sqrt{I_k}$, then there exist suitably chosen integers m, $n \in \mathbb{Z}^+$ such that

$$ka^m \in I, \; kb^n \in I$$

Since every term in the binomial expansion of $(a-b)^{m+n}$ contains either a^m or b^n as a factor, it follows that $k(a-b)^{m+n} \in I$ and therefore $a-b \in \sqrt{I_k}$.

Further if $a \in \sqrt{I_k}$ and $r \in R$ we have $r\,k\,a^m \in I$ and

$k(ra)^m = kr^m a^m = r^{m-1}\,(rka^m) \in I$ so that $ra \in \sqrt{I_k}$

Also, if $a \in \sqrt{I}$, there exists an integer $s \in \mathbb{Z}^+$ such that $a^s \in I$. Then,

$$a^s + a^s + \ldots\ldots k \text{ times} = ka^s \in I$$

or $a \in \sqrt{I_k}$. Thus $\sqrt{I_k}$ is an ideal of R containing I.

Now we obtain the k- fold nil radical of an ideal <m> in the ring $\mathbb{Z}$ of integers.

Theorem . Let $\mathbb{Z}$ denote the ring of integers. Suppose I = <m> be the ideal generated by $m \in \mathbb{Z}^+$. For fixed positive integer k, the k-fold nil radical of I is the ideal generated by the product of the distinct prime factors of m/g where g = (k,m).

Proof : We write

$$m = p_1^{\alpha_1}\ p_2^{\alpha_2}\ \ldots\ p_s^{\alpha_s}\ q_1^{\beta_1}\ q_2^{\beta_2} \ldots\ q_t^{\beta_t}$$

where , p_i, q_r (i = 1,2,....,s ; r = 1,2,....,t) are distinct primes and

$$k = p_1^{\gamma_1}\ p_2^{\gamma_2}\ \ldots\ p_s^{\gamma_s}\ r_1^{\delta_1}\ r_2^{\delta_2} \ldots\ r_l^{\delta_l}$$

where, r_1, r_2,....,r_l are distinct primes not contained in m.

If $\epsilon_i = \min_i \{\alpha_i, \gamma_i\}$,

$$(k,m) = g = p_1^{\epsilon_1} p_2^{\epsilon_2} \ldots\ p_s^{\epsilon_s}$$

Suppose $p_1, p_2, \ldots\ p_\nu$ are such that $\alpha_i > \gamma_i$ $(i = 1,2\ldots,\nu)$ Then, (A.1) $\quad m/g = p_1^{\alpha_1-\gamma_1} \; p_2^{\alpha_2-\gamma_2} \ldots p_\nu^{\alpha_\nu-\gamma_\nu} \; q_1^{\beta_1} \; q_2^{\beta_2} \ldots q_t^{\beta_t}$

Writing $I = \langle m \rangle$, let $a \in \sqrt{I_k}$

Then, there exists $\lambda \geq 1$ such that $k\, a^\lambda \in I$.

or $k\, a^\lambda$ is a multiple of m. or $(k/g)\, a^\lambda$ is a multiple of m/g

But $(k/g, m/g) = 1$ Therefore, a^λ is a multiple of m/g.

As $\lambda \geq 1$, a is a multiple of the product of the prime factors in m/g.

or $\quad a \in J$ Where

(A.2) $\quad J = \langle p_1 p_2 \ldots p_\nu \; q_1 \; q_2 \ldots q_t \rangle$

This shows that

$$\sqrt{I_k} \subseteq J$$

Next suppose $x \in J$.

Then x is a multiple of $p_1 p_2 \ldots p_\nu q_1 q_2 \ldots q_t$

Setting $\alpha = \max\{\alpha_1-\gamma_1, \alpha_2-\gamma_2, \ldots, \alpha_\nu-\gamma_\nu\}$

$$\beta = \max\{\beta_1, \beta_2, \ldots, \beta_t\}$$

and writing $\Delta = \max\{\alpha, \beta\}$ one gets

$$x^\Delta \text{ is a multiple of } m/g.$$

Therefore, $k\, x^\Delta$ is a multiple of $k\,(m/g) = (k/g)\, m$

But k/g is an integer. So $k\, x^\Delta$ is a multiple of m

or $\quad k\, x^\Delta \in I$. This implies that $x \in \sqrt{I_k}$ or

(A.3) $\quad J \subseteq \sqrt{I_k}$

From (A.2) and (A.3) we get $J = \sqrt{I_k}$ and J is the ideal generated by the product of the prime factors of m/g.

Corollary : The nil radical of $\langle m \rangle$ in $\mathbb{Z}$ is the ideal generated by the product of the prime factors of m, as $(k, m) = 1$ for $k = 1$. (see [2]).

REFERENCES

[1] T.M. Apostol : Introduction to Analytic NumberTheory, Narosa Pub. House, New Delhi (1980).

[2] D.M. Burton : A First Course in Rings and Ideals, Addison Wesley Pub. Co. (1970).

[3] L. Carlitz: Arithmetical Functions in an Unusual Setting, Amer. Math. Monthly 73 (1966) 582-590.

[4] L. Carlitz and M.V. Subbarao : Transformations of Arithmetic Functions, Duke Math. J. 40 (1973) 949-958.

[5] E.D. Cashwell and C.J. Everett : The ring of Number-Theoretic Functions, Pac. J. Math. 9 (1959) 975-985.

[6] Daniel I.A. Cohen : Problem No 5290, Amer. Math Monthly 72 (1965) p. 555.

[7] E. Cohen : Rings of Arithmetic Functions, Duke Math. J. 19 (1952) 115-129.

[8] ―――――― : A class of Arithmetic Functions, Proc. Nat. Acad. Sci., 41 (1955) 939-944.

[9] ―――――― : Representations of Even Functions (Mod r) I, Arithmetical Identities, Duke Math. J 25(1958) 401-422.

[10] ―――――― : Representations of Even Functions (Mod r) II, Cauchy Products, Duke Math. J. 26 (1959) 165-182.

[11] ―――――― : Representations of Even Functions (Mod r) III, Special Topics , Duke Math. J. 26 (1959) 491-500.

[12] ―――――― : Arithmetical Functions Associated with the Unitary Divisors of an Integer, Math. Z. 74 (1960) 66-80.

[13] ―――――― : Unitary Functions (Mod r) Duke. Math. J. 28 (1961) 475-486.

[14] ―――――― : Arithmetical Notes VIII. Some Classes of Even Functions (Mod r), Collect. Math. 16 (1964) 81-87.

[15] L.E. Dickson : History of the Theory of Numbers, Vol I, Cheisea Pub. Co. N.Y. (1952) .

[16] J.B. Fraleigh : A First Course in Abstract Algebra, Third Edition, Addison Wesley Pub. Co. (1982).

[17] S.W. Golomb : Normed Division Domains, Amer. Math. Monthly, 88 (1981) 680-686.

[18] P. Haukkanen and R. Sivaramakrishnan Arithmetic Functions is an Algebraic Setting, Tsukuba J. Math., 15 (1991) 227-234.

[19] ―――――― : Cauchy Multiplication and Periodic Functions (Mod r), Collect. Math. 42 (1991) 33-44.

[20] E.H. Hlawka, J. Schoibengeier, R. Taschner : Geometric and Analytic Number Theory, Universi Text, Springer-Verlag, Berlin (1991).

[21] N. Jacobson : Basic Algebra , Vol I, Hindustan Pub. Co. Delhi, (1983).

[22] ———— : Basic Algebra, Vol II, Hindustan Pub. Co. Delhi (1983).

[23] G. Karpilovsky : Commutative Group Algebras, Monographs and Text Books in Pure and Applied Mathematics No. 78 Marcel Dekker, Inc. N.Y. (1983).

[24] P. Kesava Menon : Transformationsof Arithmetic Functions J. Ind. Math. Soc. 6 (1942) 143-152.

[25] ———— : A Class of Quasi-fields having Isomorphic Additive and Multiplicative Groups, J. Ind. Math. Soc. 27 (1963) 71-90.

[26] J. Knopfmacher : Abstract Analytic Number Theory North Holland, (1975).

[27] J. Lambek : Lectures on Rings and Modules, Blaisdell Pub. Co. Waltham (1966).

[28] N. J. Lord : Simultaneous Complements in Finite Dimensional Vector Spaces, Amer. Math. Monthly, 92 (1985) 492-493.

[29] P.J. McCarthy : Introduction to Arithemtic Functions, Universi Text, Springer-Verlag (1986).

[30] D. Rearick : Operators on Algebras of Arithmetic Functions , Duke Math. J. 35 (1968) 761-766.

[31] P. Samuel : Unique Factorization, Amer. Math. Monthly, 78 (1968) 945-952.

[32] H.N. Shapiro : On the Convolution Ring of Arithmetic Functions, Communications on Pure and Applied Math. 25 (1972) 287-336.

[33] G.F. Simmons : Introduction to Topology and Modern Analysis, McGraw Hill, Kogakusha Ltd. (1963).

[34] R. Sivaramakrishnan : Square-reduced System (Mod r) and Related Arithmetic Functions, Canad. Math. Bull. 22 (1979) 207-220.

[35] ―――――― : Classical Theory of Arithmetic Functions, Monographs and Text Books in Pure and Applied Mathematics No.126, Marcel Dekker Inc, N.Y. (1989).

[36] O. Steinfeld : Quasi-ideals in Rings and Semigroups Disquitiones Mathematicae Hungaricae No. 10 Akademiai Kiado, Budapest (1978).

[37] I.N. Stewart and D.O. Tall : Algebraic Number Theory, Second Edition, Chapman and Hall, London (1987).

POST-SCRIPT

The material presented in this dissertation is a humble attempt to study the structural properties of rings via the norm-functions. We saw in the background the proof of the

Theorem : The Dirichlet Algebra $\mathcal{A}$ of arithmetic funcitions possesses the UFD property for its non-zero non-unit elements which was proved by ED Cashwell and C.J. Everett [2] in 1959. This was achieved by them by defining the norm of an arithmetic function f as the least positive integer a for which $f(a) \neq 0$. An alternate direct proof of the UFD property was attempted. However, it turned out that it needed to be a GCD domain as ACCP holds in the ring. David Rearick [4] kindly sent us his finding that $\mathcal{A}$ is an interpolation algebra in the sense that if given any two functions f and of such that $g \neq 0$ there exists a pair of functions $q, r \in \mathcal{A}$ such that $f = g.q + r$ where r takes the value zero on all multiples of $N(g)$ when N denotes the norm. He also pointed out that $\mathcal{A}$ as an interpolation algebra becomes a local ring.

In Chapter 3, it is shown that an integral domain R which is multiplicatively normed and if $u \in R$ is such that u is a unit if and only if $N(u) = 1$, becomes a UFD provided R is a GCD domain. It will be nice if the Dirichlet algebra of arithmetic functions is shown to be a GCD domain, though it is an interpolation algebra. In a sense, $\mathcal{A}$ is 'semi-Eulidean'.

Extending the definition of an MND to any commutative ring with unity and having divisors of zero, we have examined the structure of the Lucas ring $\mathfrak{B}$ of arithmetic functions in Chapter 5. A conjecture of Carlitz [1] states that every zero divisor in $\mathfrak{B}$ is nilpotent. It is believed that the problem is still open.

The Cauchy algebra $\mathfrak{B}_r(\mathbb{C})$ of even functions (mod r) gives an interesting example of a finite - dimensional algebra which is multiplicatively normed. Two particular subspaces $V_r(\mathbb{C})$ and $W_r(\mathbb{C})$ of $\mathfrak{B}_r(\mathbb{C})$ of have the same dimension $2^{\omega(r)}$. By a theorem of N.J. Lord [3] there exists a common complement to both the subspaces $V_r(\mathbb{C})$ and $W_r(\mathbb{C})$. It is worthwhile attempting to find out the common complement. This is not considered in Chapter 6.

In short, this post script is meant to point out that there is scope for further research in these directions.

REFERENCES

1. L. Carlitz : Arithmetical Functions is an Unusual Setting · Amer. Math. Monthly 73 (1966) 582-590.
2. E.D. Cashwell and C.J. Everett : The Ring of Number-theoretic Functions Duke Math. J. 9 (1959) 975-985.
3. N.J. Lord : Simultaneous Complements in Finite-Dimensional Vector Spaces, Amer. Math. Monthly 92 (1985) 492-493.
4. David Rearick : Interpolation Algebras, (1965) (unpublished, private communication)