THE RING OF ARITHMETICAL FUNCTIONS WITH UNITARY CONVOLUTION: DIVISORIAL AND TOPOLOGICAL PROPERTIES.

JAN SNELLMAN

Abstract. We study \((A, +, \oplus)\), the ring of arithmetical functions with unitary convolution, giving an isomorphism between \((A, +, \oplus)\) and a generalized power series ring on infinitely many variables, similar to the isomorphism of Cashwell-Everett \([4]\) between the ring \((A, +, \cdot)\) of arithmetical functions with Dirichlet convolution and the power series ring \(\mathbb{C}[[x_1, x_2, x_3, \ldots]]\) on countably many variables. We topologize it with respect to a natural norm, and show that all ideals are quasi-finite. Some elementary results on factorization into atoms are obtained. We prove the existence of an abundance of non-associate regular non-units.

1. Introduction

The ring of arithmetical functions with Dirichlet convolution, which we’ll denote by \((A, +, \cdot)\), is the set of all functions \(\mathbb{N}^+ \to \mathbb{C}\), where \(\mathbb{N}^+\) denotes the positive integers. It is given the structure of a commutative \(\mathbb{C}\)-algebra by component-wise addition and multiplication by scalars, and by the Dirichlet convolution

\[
f \cdot g(k) = \sum_{r|k} f(r)g(k/r).
\]

(1)

Then, the multiplicative unit is the function \(e_1\) with \(e_1(1) = 1\) and \(e_1(k) = 0\) for \(k > 1\), and the additive unit is the zero function \(0\).

Cashwell-Everett \([4]\) showed that \((A, +, \cdot)\) is a UFD using the isomorphism

\[
(A, +, \cdot) \simeq \mathbb{C}[[x_1, x_2, x_3, \ldots]],
\]

(2)

where each \(x_i\) corresponds to the function which is 1 on the \(i\)'th prime number, and 0 otherwise.

Schwab and Silberberg \([10]\) topologised \((A, +, \cdot)\) by means of the norm

\[
|f| = \frac{1}{\min \{ k|f(k) \neq 0 \}}
\]

(3)

They noted that this norm is an ultra-metric, and that \(((A, +, \cdot), |\cdot|)\) is a valued ring, i.e. that

1. \(|0| = 0\) and \(|f| > 0\) for \(f \neq 0\),
2. \(|f - g| \leq \max \{ |f|, |g| \}\),
3. \(|fg| = |f||g|\).

They showed that \((A, |\cdot|)\) is complete, and that each ideal is quasi-finite, which means that there exists a sequence \((e_k)_{k=1}^\infty\), with \(|e_k| \to 0\), such that every element in the ideal can be written as a convergent sum \(\sum_{k=1}^\infty c_k e_k\), with \(c_k \in A\).

In this article, we treat instead \((A, +, \oplus)\), the ring of all arithmetical functions with unitary convolution. This ring has been studied by several authors, such as Vaidyanathaswamy \([7]\), Cohen \([8]\), and Yocom \([13]\).
We topologise $\mathcal{A}$ in the same way as Schwab and Silberberg \cite{1}, so that $(\mathcal{A}, +, \oplus)$ becomes a normed ring (but, in contrast to $(\mathcal{A}, +, \cdot)$, not a valued ring). We show that all ideals in $(\mathcal{A}, +, \oplus)$ are quasi-finite.

We show that $(\mathcal{A}, +, \oplus)$ is isomorphic to a monomial quotient of a power series ring on countably many variables. It is présimplifiable and atomic, and there is a bound on the lengths of factorizations of a given element. We give a sufficient condition for nilpotency, and prove the existence of plenty of regular non-units.

Finally, we show that the set of arithmetical functions supported on square-free integers is a retract of $(\mathcal{A}, +, \oplus)$.

2. The ring of arithmetical functions with unitary convolution

Let $p_i$ denote the $i$th prime number, and denote by $\mathcal{P}$ the set of prime numbers. Let $\mathcal{P}\mathcal{P}$ denote the set of prime powers. Let $\omega(r)$ denote the number of distinct prime factors of $r$, with $\omega(1) = 0$.

**Definition 2.1.** If $k, m$ are positive integers, we define their *unitary product* as

$$k \oplus m = \begin{cases} \text{gcd}(k, m) = 1 & k \cdot m \\ 0 & \text{otherwise} \end{cases}$$

If $k \oplus m = p$, then we write $k \mid p$ and say that $k$ is a *unitary divisor* of $p$.

The so-called *unitary convolution* was introduced by Vaidyanathaswamy \cite{11}, and was further studied Eckford Cohen \cite{5}.

**Definition 2.2.** $\mathcal{A} = \{f : \mathbb{N}^+ \to \mathbb{C}\}$, the set of complex-valued functions on the positive integers. We define the *unitary convolution* of $f, g \in \mathcal{A}$ as

$$(f \oplus g)(n) = \sum_{d \mid n} f(d)g(n/d)$$

and the addition as

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

The ring $(\mathcal{A}, +, \oplus)$ is called the *ring of arithmetic functions* with unitary convolution.

**Definition 2.3.** For each positive integer $k$, we define $e_k \in \mathcal{A}$ by

$$e_k(n) = \begin{cases} 1 & k = n \\ 0 & k \neq n \end{cases}$$

We also define $0$ as the zero function, and $1$ as the function which is constantly 1.

**Lemma 2.4.** $0$ is the additive unit of $\mathcal{A}$, and $e_1$ is the multiplicative unit. We have that

$$(e_k \oplus e_k \oplus \cdots \oplus e_k)(n) = \begin{cases} 1 & n = k_1k_2\cdots k_r \text{ and } \gcd(k_i, k_j) = 1 \text{ for } i \neq j \\ 0 & \text{otherwise} \end{cases}$$

hence

$$e_k \oplus e_k \oplus \cdots \oplus e_k = \begin{cases} e_k & \text{if } \gcd(k_i, k_j) = 1 \text{ for } i \neq j \\ 0 & \text{otherwise} \end{cases}$$

\footnote{In \cite{10}, 1 is denoted $e$, and $e_1$ denoted $e_0$.}
Proof. The first assertions are trivial. We have \[ (f_1 \oplus \cdots \oplus f_r)(n) = \sum_{a_1 \oplus \cdots \oplus a_r = n} f_1(a_1) \cdots f_r(a_r) \] (9)

Since
\[ e_{k_1}(a_1)e_{k_2}(a_2)\cdots e_{k_r}(a_r) = 1 \text{ iff } \forall i : k_i = a_i, \]
(7) follows. \qed

Lemma 2.5. Any \( e_n \) can be uniquely expressed as a square-free monomial in \( \{ e_k | k \in PP \} \).

Proof. By unique factorization, there is a unique way of writing \( n = p_{i_1}^{a_{i_1}} \cdots p_{i_r}^{a_{i_r}} \), and (8) gives that
\[ e_n = e_{p_{i_1}^{a_{i_1}}} \cdots e_{p_{i_r}^{a_{i_r}}}. \]
We define the support of \( f \) as
\[ \text{supp}(f) = \{ n \in \mathbb{N}^+ | f(n) \neq 0 \} \] (10)
We define the order of a non-zero element by
\[ \text{N}(f) = \min \text{supp}(f) \] (11)
We also define the norm of \( f \) as
\[ |f| = \text{N}(f)^{-1} \] (12)
and the degree as
\[ \text{D}(f) = \min \{ \omega(k) | k \in \text{supp}(f) \} \] (13)

By definition, the zero element has order infinity, norm 0, and degree -1.

Lemma 3.2. The value semigroup of \( (A, |\cdot|) \) is \( |A \setminus \{0\}| = \{ 1/k | k \in \mathbb{N}^+ \} \), a discrete subset of \( \mathbb{R}^+ \).

Lemma 3.3. Let \( f, g \in A \setminus \{0\} \). Let \( \text{N}(f) = i, \text{N}(g) = j \), so that \( f(i) \neq 0 \) but \( f(k) = 0 \) for all \( k < i \), and similarly for \( g \). We assume that \( i \leq j \). Then, the following hold:
(i) \( \text{N}(f-g) \geq \min \{ \text{N}(f), \text{N}(g) \} \).
(ii) \( \text{N}(cf) = \text{N}(f) \) for \( c \in \mathbb{C} \setminus \{0\} \).

\[ \text{In} \] [10] the term norm is used.
(iii) \( N(f) = 1 \) iff \( f \) is a unit.
(iv) \( N(f \cdot g) = N(f)N(g) \leq N(f \oplus g) \), with equality iff \( (i,j) = 1 \).
(v) \( N(f \oplus g) \geq \max \{N(f), N(g)\} \), with strict inequality iff both \( f \) and \( g \) are non-units.
(vi) \( D(f + g) \geq \min \{D(f), D(g)\} \).
(vii) \( D(f \cdot g) = D(f) + D(g) \).
(viii) \( D(f) = 0 \) if and only if \( f \) is a unit.
(ix) Suppose that \( f \oplus g \neq 0 \). Then
\[
D(f + g) \geq D(f) + D(g) \geq \max \{D(f), D(g)\}.
\]
with \( D(f) + D(g) \) a valued ring, and \( D(g) \) is a valued ring, as well as a faithfully normed, \( b \)-separable complete vector space over \( \mathbb{C} \).

Proposition 3.5. \( |\cdot| \) is an ultrametric function on \( A \), making \( (A, +, \oplus) \) a normed ring, as well as a faithfully normed complete vector space over \( \mathbb{C} \).

Lemma 3.6. If \( f \) is a unit, then \( 1 = |f^n| = |f|^n \) for all positive integers \( n \). If \( n \) is a non-unit, then \( |f^n| < |f|^n \) for all \( n > 1 \).

Theorem 3.7. Let \( f \in ((A, +, \oplus), |\cdot|), f \neq 0 \). Then the following are equivalent:
1. \( f \) is topologically nilpotent,
2. \( f \) is not power-multiplicative,
3. \( f \) is not multiplicative in the normed ring \( (A, +, \oplus), |\cdot|) \),
4. \( f \) is a non-unit,
5. $|f| < 1$.

**Proof.** Using [3, 1.2.2, Prop. 2], this follows from the previous Lemma, and the fact that for a unit $f$,

$$1 = |f^{-1}| = |f|^{-1}.$$ 

3.1. **A Schauder basis for $(\mathcal{A}, |\cdot|)$**.

**Definition 3.8.** Let $\mathcal{A}'$ denote the subset of $\mathcal{A}$ consisting of functions with finite support. We define a pairing

$$\mathcal{A} \times \mathcal{A}' \to \mathbb{C}$$

$$(f, g) = \sum_{k=1}^{\infty} f(k)g(k)$$  

**Theorem 3.9.** The set $\{e_k : k \in \mathbb{N}^+\}$ is an ordered orthogonal Schauder base in the normed vector space $(\mathcal{A}, |\cdot|)$. In other words, if $f \in \mathcal{A}$ then

$$f = \sum_{k=1}^{\infty} c_k e_k, \quad c_k \in \mathbb{C}$$

where

(i) $|e_k| \to 0$,

(ii) the infinite sum (15) converges w.r.t. the ultrametric topology,

(iii) the coefficients $c_k$ are uniquely determined by the fact that

$$\langle f, e_k \rangle = f(k) = c_k$$

(iv) $\max_{k \in \mathbb{N}^+} \{|c_k||e_k|\} = 1/j$.

The set $\{e_p : p \in \mathbb{P}\}$ generates a dense subalgebra of $(\mathcal{A}, +, |\cdot|)$.

**Proof.** It is proved in [3] that this set is a Schauder base in the topological vector space $(\mathcal{A}, |\cdot|)$. It also follows from [3] that the coefficients $c_k$ in (3.9) are given by $c_k = f(k)$.

It remains to prove orthogonality. With the above notation,

$$|f| = \left| \sum_{k=1}^{\infty} c_k e_k \right| = 1/j,$$

where $j$ is the smallest $k$ such that $c_k \neq 0$. Recalling that $\mathbb{C}$ is trivially normed, we have that

$$|c_k||e_k| = \begin{cases} |e_k| = 1/k & \text{if } c_k \neq 0 \\ 0 & \text{if } c_k = 0 \end{cases},$$

so $\max_{k \in \mathbb{N}^+} \{|c_k||e_k|\} = 1/j$, with $j$ as above, so (17) holds.

By Lemma 2.5 any $e_k$ can be written as a square-free monomial in the elements of $\{e_p : p \in \mathbb{P}\}$. The set $\{e_k : k \in \mathbb{N}^+\}$ is dense in $\mathcal{A}$, so $\{e_p : p \in \mathbb{P}\}$ generates a dense subalgebra.

Let $J \subset \mathfrak{m}$ denote the ideal generated by all $e_k$, $k > 1$.

**Lemma 3.10.** $J$ is not finitely generated.
Proof. If $J$ is finitely generated, then there is an $N$ such that $$J = (e_2, \ldots, e_N).$$

Let $L$ be a prime number, $L > N$. Since $e_L \in J$, we have that 

$$e_L = \sum_{k=2}^{N} f_k \oplus e_k, \quad f_k \in A.$$  

We write $f_k = \sum_{i=1}^{\infty} c_{ki} e_i$, so that

$$e_L = \sum_{k=2}^{N} \sum_{i=1}^{\infty} c_{i,k} e_i \oplus e_k = \sum_{k=2}^{N} \sum_{i=1}^{\infty} c_{i,k} e_i \oplus \sum_{k=2}^{N} \sum_{\gcd(i,k)=1}^{\infty} c_{i,k} e_{i,k}.$$  

But this is impossible, because we can not write $L = ik$ with $\gcd(i,k) = 1$ and $2 \leq i \leq N < L$. \[\square\]

**Definition 3.11.** An ideal $I \subset A$ is called quasi-finite if there exists a sequence $(g_k)_{k=1}^{\infty}$ in $I$ such that $|g_k| \to 0$ and such that every element $f \in I$ can be written (not necessarily uniquely) as a convergent sum 

$$f = \sum_{k=0}^{\infty} a_k \oplus g_k, \quad a_k \in A \quad (18)$$

**Lemma 3.12.** $m$ is quasi-finite.

**Proof.** By Theorem 3.9 the set $\{ e_k \mid k > 1 \}$ is a quasi-finite generating set for $m$. \[\square\]

Since all ideals are contained in $m$, it follows that any ideal containing $\{ e_k \mid k > 1 \}$ is quasi-finite. Furthermore, such an ideal has $m$ as its closure. In particular, $J$ is quasi-finite, but not closed.

**Theorem 3.13.** All (non-zero) ideals in $A$ are quasi-finite. In fact, given any subspace $I$ if we can find 

$$G(I) := (g_k)_{k=1}^{\infty} \quad (19)$$

such that for all $f \in I$, 

$$\exists c_1, c_2, c_3, \ldots \in \mathbb{C}, \quad f = \sum_{i=1}^{\infty} c_i g_i. \quad (20)$$

So all subspaces possesses a Schauder basis.

**Proof.** We construct $G(I)$ in the following way: for each 

$$k \in \{ N(f) \mid f \in I \setminus \{0\} \} =: N(I)$$

we choose a $g_k \in I$ with $N(g_k) = k$, and with $g_k(k) = 1$. In other words, we make sure that the “leading coefficient” is 1; this can always be achieved since the coefficients lie in a field. For $k \notin N(I)$ we put $g_k = 0$.

To show that this choice of elements satisfy (20), take any $f \in I$, and put $f_0 = f$. Then define recursively, as long as $f_i \neq 0$,

$$n_i := N(f_i)$$

$$\mathbb{C} \ni a_i := f_i(n_i)$$

$$A \ni f_{i+1} := f_i - a_i g_{n_i}$$

Of course, if $f_i = 0$, then we have expressed $f$ as a linear combination of 

$$g_{n_1}, \ldots, g_{n_{i-1}}.$$
and we are done. Otherwise, note that by induction \( f_i \in I_i \), so \( n_i \in N(I) \), hence \( g_{n_i} \neq 0 \). Thus \( N(f_{i+1}) > N(f_i) \), so \( |f_{i+1}| < |f_i| \), whence
\[
|f_0| > |f_1| > |f_2| > \cdots \to 0.
\]
But
\[
f_{i+1} = f - \sum_{j=1}^{i} a_j g_{n_j},
\]
so
\[
F_i := \sum_{j=1}^{i} a_j g_{n_j} \to f,
\]
which shows that \( \sum_{j=1}^{\infty} a_j g_j = f \).

4. A FUNDAMENTAL ISOMORPHISM

4.1. The monoid of separated monomials. Let
\[
Y = \left\{ y_i^{(j)} \bigg| i, j \in \mathbb{N}^+ \right\}
\]
be an infinite set of variables, in bijective correspondence with the integer lattice points in the first quadrant minus the axes. We call the subset
\[
Y_i = \left\{ y_i^{(j)} \bigg| j \in \mathbb{N}^+ \right\}
\]
the \( i \)'th column of \( Y \).

Let \( [Y] \) denote the free abelian monoid on \( Y \), and let \( M \) be the subset of separated monomials, i.e. monomials in which no two occurring variables come from the same column:
\[
M = \left\{ y_{i_1}^{(j_1)} y_{i_2}^{(j_1)} \cdots y_{i_r}^{(j_r)} \bigg| 1 \leq i_1 < i_2 < \cdots < i_r \right\}
\]
We regard \( M \) as a monoid-with-zero, so that the multiplication is given by
\[
m \oplus m' = \begin{cases} 
mm' & \text{if } mm' \in M \\
0 & \text{otherwise} 
\end{cases}
\]
Note that the zero is exterior to \( M \), i.e. \( 0 \not\in M \). The set \( M \cup \{0\} \) is a (non-cancellative) monoid if we define \( m \oplus 0 = 0 \) for all \( m \in M \).

Recall that \( \mathcal{P} \mathcal{P} \) denotes the set of prime powers. It follows from the fundamental theorem of arithmetic that any positive integer \( n \) can be uniquely written as a square-free product of prime powers. Hence we have that
\[
\Phi : Y \to \mathcal{P} \mathcal{P}
\]
\[
y_i^{(j)} \mapsto p_i^j
\]
is a bijection which can be extended to a bijection
\[
\Phi : M \to \mathbb{N}^+
\]
\[
y_{i_1}^{(j_1)} \cdots y_{i_r}^{(j_r)} \mapsto p_{i_1}^{j_1} \cdots p_{i_r}^{j_r}
\]
If we regard \( \mathbb{N}^+ \) as a monoid-with-zero with the operation \( \oplus \) of (4), then (26) is a monoid-with-zero isomorphism.
4.2. **The ring \( A \) as a generalized power series ring, and as a quotient of \( \mathbb{C}[[Y]] \).** Let \( R \) be the large power series ring on \( [Y] \), i.e. \( R = \mathbb{C}[[Y]] \) consists of all formal power series \( \sum c_\alpha y^\alpha \), where the sum is over all multi-sets \( \alpha \) on \( Y \).

Let \( S \) be the generalized monoid-with-zero ring on \( M \). By this, we mean that
\[
S \text{ is the set of all formal power series } \sum_{m \in M} c_m m \text{, with component-wise addition, and with multiplication }
\]
\[
\left( \sum_{m \in M} f(m) m \right) \oplus \left( \sum_{m \in M} g(m) m \right) = \left( \sum_{m \in M} h(m) m \right)
\]
\[
h(m) = (f \oplus g)(m) = \sum_{s \oplus t = m} f(s) g(t)
\]

Define
\[
\text{supp}(\sum_{m \in [Y]} c_m m) = \{ m \in Y | c_m \neq 0 \} \quad (29)
\]
\[
\text{supp}(\sum_{m \in M} c_m m) = \{ m \in M | c_m \neq 0 \} \quad (30)
\]

Let furthermore
\[
\mathcal{D} = \{ f \in R | \text{supp}(f) \cap M = \emptyset \} \quad (32)
\]

**Theorem 4.1.** \( S \) and \( \frac{R}{\mathcal{D}} \) and \( A \) are isomorphic as \( \mathbb{C} \)-algebras.

**Proof.** The bijection (27) induces a bijection between \( S \) and \( A \) which is an isomorphism because of the way multiplication is defined on \( S \). In detail, the isomorphism is defined by
\[
S \ni \sum_{m \in M} c_m m \mapsto f \in A
\]
\[
f(\Phi(m)) = c_m
\]

For the second part, consider the epimorphism
\[
\phi : R \to S
\]
\[
\phi \left( \sum_{m \in [Y]} c_m m \right) = \sum_{m \in M} c_m m
\]

Clearly, \( \ker(\phi) = \mathcal{D} \), hence \( S \cong \frac{R}{\mathcal{D}} \). \( \square \)

Let us exemplify this isomorphism by noting that \( e_n \), where \( n \) has the square-free factorization \( n = p_1^{a_1} \cdots p_r^{a_r} \), corresponds to the square-free monomial \( y_1^{(a_1)} \cdots y_r^{(a_r)} \), and that
\[
1 = \sum_{m \in M} m = \prod_{i=1}^{\infty} \left( 1 + \sum_{j=1}^{\infty} y_i^{(j)} \right) \quad (34)
\]

What does its inverse \( \mu^* \) correspond to?
**Definition 4.2.** For \( m \in \mathcal{M} \), we denote by \( D(m) \) the number of occurring variables in \( m \) (by definition, \( D(1) = 0 \) and \( D(0) = -\infty \)). For \( S \ni f = \sum_{m \in \mathcal{M}} c_m m \), we put

\[
D(f) = \min \{ D(m) \mid c_m \neq 0 \}
\]

Using the isomorphism between \( S \) and \( \mathcal{A} \), we define \( D(g) \) for any \( g \in \mathcal{A} \) by

\[
D(g) = \min \{ \omega(n) \mid f(n) \neq 0 \}
\]

It is known (see [10]) that \( \mu^*(r) = (-1)^{\omega(r)} \) \( (36) \)

We then have that \( \mu^* \) corresponds to

\[
1^{-1} = \frac{1}{\prod_{i=1}^{\infty} \left( 1 + \sum_{j=1}^{\infty} y_i^{(j)} \right)} = \prod_{i=1}^{\infty} \frac{1}{1 + \sum_{j=1}^{\infty} y_i^{(j)}} = \sum_{m \in \mathcal{M}} (-1)^{D(m)} m
\]

Recall that \( f \in \mathcal{A} \) is a multiplicative arithmetic function if \( f(nm) = f(n)f(m) \) whenever \( (n, m) = 1 \). Regarding \( f \) as an element of \( S \) we have that \( f \) is multiplicative if and only if it can be written as

\[
f = \prod_{i=1}^{\infty} \left( 1 + \sum_{j=1}^{\infty} c_{i,j} y_i^{(j)} \right)
\]

It is now easy to see that the multiplicative functions form a group under multiplication.

### 4.3. The continuous endomorphisms.

In [9], Schwab and Silberberg characterized all continuous endomorphisms of \( \Gamma \). We give the corresponding result for \( \mathcal{A} \):

**Theorem 4.3.** Every continuous endomorphism \( \theta \) of the \( \mathbb{C} \)-algebra \( S \cong \mathcal{A} \) is defined by

\[
\theta(y_i^{(j)}) = \gamma_{i,j}
\]

where

\[
\gamma_{i,j} \gamma_{i,k} = 0 \quad \text{for all } i, j, k
\]

and

\[
\gamma_{a_1(n), b_1(n)} \cdots \gamma_{a_r(n), b_r(n)} \to 0 \quad \text{as } n = p_{a_1(n)}^{b_1(n)} \cdots p_{a_r(n)}^{b_r(n)} \to \infty
\]

**Proof.** Recall that \( S \cong \mathcal{B} \), where \( \mathcal{B} = \mathbb{C}[[Y]] \) and \( \mathcal{D} \) is the closure of the ideal generated by all non-separated quadratic monomials \( y_i^{(j)} y_i^{(k)} \). Since the set of square-free monomials in the \( y_i^{(j)} \)'s form a Schauder base, any continuous \( \mathbb{C} \)-algebra endomorphism \( \theta \) of \( S \) is determined by its values on the \( y_i^{(j)} \)'s, and must fulfill (41). Since \( y_i^{(j)} y_i^{(k)} = 0 \) in \( S \), we must have that

\[
\theta(0) = \theta(y_i^{(j)} y_i^{(k)}) = \theta(y_i^{(j)}) \theta(y_i^{(k)}) = \gamma_{i,j} \gamma_{i,k} = 0.
\]
5. Nilpotent elements and zero divisors

**Definition 5.1.** For \( m \in \mathbb{N}^+ \), define the prime support of \( m \) as

\[
\text{psupp}(m) = \{ p \in \mathcal{P} | p | m \}
\]

and (when \( m > 1 \)) the leading prime as

\[
lp(m) = \min \text{psupp}(m)
\]

For \( n \in \mathbb{N}^+ \), put

\[
A^p = \{ k \in \mathbb{N}^+ | p_i | k \text{ but } p_i \nmid k \text{ for } i < n \} = \{ k \in \mathbb{N}^+ | lp(k) = p_n \}
\]

Then \( \mathbb{N}^+ \setminus \{1\} \) is a disjoint union

\[
\mathbb{N}^+ \setminus \{1\} = \bigsqcup_{i=1}^{\infty} A^i
\]

**Definition 5.2.** Let \( f \in \mathcal{A} \) be a non-unit. The canonical decomposition of \( f \) is the unique way of expressing \( f \) as a convergent sum

\[
f = \sum_{i=1}^{\infty} f_i, \quad f_i = \sum_{k \in A^i} f(k)e_k
\]

The element \( f \) is said to be of polynomial type if all but finitely many of the \( f_i \)'s are zero. In that case, the largest \( N \) such that \( f_N \neq 0 \) is called the filtration degree of \( f \).

**Lemma 5.3.**

\[
f_i = \sum_{j=1}^{\infty} e_{p_j^i} \oplus g_{i,j}, \quad r \leq i, \quad p_r | n \implies g_{i,j}(n) = 0.
\]

For any \( n \) there is at most one pair \((i, j)\) such that

\[
(e_{p_j^i} \oplus g_{i,j})(n) \neq 0.
\]

More precisely, if

\[
n = p_{i_1}^{j_1} \cdots p_{i_r}^{j_r}, \quad i_1 < \cdots < i_r,
\]

then \((e_{p_j^{i_1}} \oplus g_{i_1,j_1})(n)\) may be non-zero.

**Definition 5.4.** For \( k \in \mathbb{N} \), define

\[
I_k = \{ f \in \mathcal{A} | f(n) = 0 \text{ for every } n \text{ such that } (n, p_1p_2 \cdots p_k) = 1 \}
\]

**Lemma 5.5.** \( I_k \) is an ideal in \((\mathcal{A}, +, \oplus)\).

**Proof.** It is shown in [8] that the \( I_k \)'s form an ascending chain of ideals in \((\mathcal{A}, +, \cdot)\). They are also easily seen to be ideals in \((\mathcal{A}, +, \oplus)\): if

\[
f \in I_k, \quad g \in \mathcal{A} \text{ and } (n, p_1p_2 \cdots p_k) = 1
\]

then

\[
(f \oplus g)(n) = \sum_{d \mid n} f(d)g(n/d) = 0,
\]

since \((d, p_1p_2 \cdots p_k) = 1\) for any unitary divisor of \( n \).
Theorem 5.6. Let $N \in \mathbb{N}^+$, and let $f \in (\mathcal{A}, +, \oplus)$ be a non-unit. Then 

$$I_N = \text{ann}(e_{p_1 \cdots p_N})$$

$$= \{0\} \cup \{ f \in \mathcal{A} | f \text{ is of polynomial type and has filtration degree } N \}$$

$$= \mathcal{A} \{ e_{p^i} \mid a, i \in \mathbb{N}^+, i \leq N \}$$

where $\overline{AW}$ denotes the topological closure of the ideal generated by the set $W$.

Proof. If $f \in I_N$ then for all $k$

$$(f \oplus e_{p_1 \cdots p_N})(k) = \sum_{a \oplus p_1 \cdots p_N = k} f(a) e_{p_1 \cdots p_N} = \sum_{a \oplus p_1 \cdots p_N = k} f(a) = 0$$

(49)

so $f \in \text{ann}(e_{p_1 \cdots p_N})$. Conversely, if $f \in \text{ann}(e_{p_1 \cdots p_N})$ then $(f \oplus e_{p_1 \cdots p_N})(k) = 0$ for all $k$, hence if $(n, p_1 \cdots p_N) = 1$ then

$$0 = (f \oplus e_{p_1 \cdots p_N})(np_1 \cdots p_N) = f(n) e_{p_1 \cdots p_N} = f(n)$$

(50)

hence $f \in I_N$.

If $f \in I_N$ then for $j > N$ we get that $f_j = 0$, since

$$f_j(k) = \begin{cases} 
0 & \text{if } k \notin A^j \\
0 & \text{if } k \in A^j
\end{cases}$$

Hence $f = \sum_{i=1}^N f_i$. Conversely, if $f$ can be expressed thusly, then $f(k) = f_{j_1}(k) = 0$ for $k = p_1^{a_1} \cdots p_N^{a_N}$ with $N < j_1 < \cdots < j_r$.

The last equality follows from Theorem 3.9. □

Theorem 5.7. Let $f \in \mathcal{A}$ be a non-unit. The following are equivalent:

(i) $f$ is of polynomial type.

(ii) $f \in \bigcup_{k=0}^{\infty} I_k$.

(iii) There is a finite subset $Q \subset \mathcal{P}$ such that $f(k) = 0$ for all $k$ relatively prime to all $p \in Q$.

(iv) $f \in \bigcup_{N=1}^{\infty} \text{ann}(e_{p_1 p_2 \cdots p_N})$.

(v) $f$ is contained in the topological closure of the ideal generated by the set

$\{ e_{p^i} \mid a, i \in \mathbb{N}^+, i \leq N \}$.

If $f$ has finite support, then it is of polynomial type. If $f$ is of polynomial type, then it is nilpotent.

Proof. Clearly, a finitely supported $f$ is of polynomial type. The equivalence (i) $\iff$ (ii) $\iff$ (iii) $\iff$ (iv) follows from the previous theorem.

If $f$ is of polynomial type, say of filtration degree $N$, then

$$f = \sum_{i=1}^N f_i$$

(51)

and we see that if $f^{N+1}$ is the $N + 1$st unitary power of $f$, then $f^{N+1}$ is the linear combination of monomials in the $f_i$’s, and none of these monomials are square-free. Since $f_i \oplus f_i = 0$ for all $i$, we have that $f^{N+1} = 0$. So $f$ is nilpotent. □

Lemma 5.8. The elements of polynomial type forms an ideal.

Proof. By the previous theorem, this set can be expressed as

$$\bigcup_{n=1}^{\infty} I_n,$$

which is an ideal since each $I_n$ is. □
Question 5.9. Are all [nilpotent elements, zero divisors] of polynomial type? If one could prove that the zero divisors are precisely the elements of polynomial type, then by Lemma 2.3 it would follow that \( Z(A) \) is an ideal, and moreover a prime ideal, since the product of two regular elements is regular (in any commutative ring). Then one could conclude that \( (A, +, \oplus) \) has few zero divisors, hence is additively regular, hence is a Marot ring.

Theorem 5.10. \((A, +, \oplus)\) contains infinitely many non-associate regular non-units.

Proof. Step 1. We first show that there is at least one such element. Let \( f \in A \) denote the arithmetical function

\[
f(k) = \begin{cases} 1 & k \in PP \\ 0 & \text{otherwise} \end{cases}
\]

Then \( f \) is a non-unit, and using a result by Yocom [13, 8] we have that \( f \) is contained in a subring of \((A, +, \oplus)\) which is a discrete valuation ring isomorphic to \( \mathbb{C}[[t]] \), the power series ring in one indeterminate. This ring is a domain, so \( f \) is not nilpotent.

We claim that \( f \) is in fact regular. To show this, suppose that \( g(f) = 0 \), then

\[
0 = (f \oplus g)(2) = f(2)g(1) = g(1).
\]

For the case \( r = 1 \), we want to show that \( g(q^a) = 0 \) for all prime numbers \( q \). Choose three different prime powers \( q_1^a, q_2^a, \) and \( q_3^a \). Then

\[
0 = f \oplus g(q_1^a)q_1^{a+i} = f(q_1^a)g(q_1^{a+i}) + f(q_2^a)g(q_2^{a+i}) = g(q_1^{a+i}) + g(q_2^{a+i}),
\]

when \( i \neq j, i, j \in \{1, 2, 3\} \). In matrix notation, these three equations can be written as

\[
\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} g(q_1^{a_1}) \\ g(q_2^{a_2}) \\ g(q_3^{a_3}) \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}
\]

from which we conclude (since the determinant of the coefficient matrix is non-zero) that

\[
0 = g(q_1^{a_1}) = g(q_2^{a_2}) = g(q_3^{a_3}).
\]

Now for the general case, \( r > 1 \). We need to show that that

\[
g(q_1^{a_1} \cdots q_r^{a_r}) = 0
\]

whenever \( q_1^{a_1}, \ldots, q_r^{a_r} \) are pair-wise relatively prime prime powers.

Choose \( N \) pair-wise relatively prime prime powers \( q_1^{e_1}, \ldots, q_N^{e_N} \). For each \( r + 1 \)-subset \( q_{s_1}, \ldots, q_{s_{r+1}} \) of this set we get a homogeneous linear equation

\[
0 = f \oplus g(q_{s_1} \cdots q_{s_{r+1}}) = g(q_{s_2} \cdots q_{s_{r+1}}) + g(q_{s_3} q_{s_4} \cdots q_{s_{r+1}}) + \cdots + g(q_{s_1} \cdots q_{s_r})
\]

The matrix of the homogeneous linear equation system formed by all these equations is the incidence matrix of \( r \)-subsets (of a set of \( N \) elements) into \( r + 1 \)-subsets. It has full rank [12]. Since it consists of \( \binom{N}{r+1} \) equations and \( \binom{N}{r} \) variables, we get that for sufficiently large \( N \), the null-space is zero-dimensional, thus the homogeneous system has only the trivial solution. It follows, in particular, that (52) holds.

Thus, \( g(m) = 0 \) for all \( m \), so \( f \) is a regular element.

Step 2. We construct infinitely many different regular non-units. Consider the element \( f \), with

\[
\tilde{f}(k) = \begin{cases} c_k & k \in PP \\ 0 & \text{otherwise} \end{cases}
\]
and where the \( c_k \)'s are “sufficiently generic” non-zero complex numbers, then we claim that \( \tilde{f} \), too, is a regular non-unit. With \( g, m, r \) as before, we have that, for \( r = 0 \),

\[
0 = f \oplus g(p^a) = f(p^a)g(1) = c_{pr}g(1).
\]

We demand that \( c_{pr} \neq 0 \), then \( g(1) = 0 \).

For a general \( r \), we argue as follows: the incidence matrices that occurred before will be replaced with “generic” matrices whose elements are \( c_k \)'s or zeroes, and which specialize, when setting all \( c_k = 1 \), to full-rank matrices. They must therefore have full rank, and the proof goes through.

**Step 3.** Let \( g \) be a unit in \( \mathcal{A} \), and \( \tilde{f} \) as above. We claim that if \( g \oplus f \) is of the above form, i.e. supported on \( \mathcal{P} \mathcal{P} \), then \( g \) must be a constant. Hence there are infinitely many non-associate regular non-units of the above form.

To prove the claim, we argue exactly as before, using the fact that \( g \oplus \tilde{f} \) is supported on \( \mathcal{P} \mathcal{P} \). For \( m = q_1^{a_1} \cdots q_r^{a_r} \) as before, the case \( r = 0 \) yields nothing:

\[
0 = g \oplus \tilde{f}(1) = \tilde{f}(1)g(1) = 0g(1) = 0,
\]

neither does the case \( r = 1 \):

\[
w = g \oplus \tilde{f}(q^a) = \tilde{f}(q^a)g(1),
\]

so \( g(1) \) may be non-zero. But for \( r = 2 \) we get

\[
0 = g \oplus \tilde{f}(q_1^{a_1}q_2^{a_2}) = \tilde{f}(q_1^{a_1})g(q_2^{a_2}) + g(q_1^{a_1})\tilde{f}(q_2^{a_2}),
\]

and also

\[
0 = g \oplus \tilde{f}(q_2^{a_2}q_3^{a_3}) = \tilde{f}(q_2^{a_2})g(q_3^{a_3}) + g(q_2^{a_2})\tilde{f}(q_3^{a_3})
\]

\[
0 = g \oplus \tilde{f}(q_3^{a_3}q_1^{a_1}) = \tilde{f}(q_3^{a_3})g(q_1^{a_1}) + g(q_3^{a_3})\tilde{f}(q_1^{a_1})
\]

which means that

\[
\begin{bmatrix}
\tilde{f}(q_2^{a_2}) & \tilde{f}(q_1^{a_1}) & 0 \\
\tilde{f}(q_3^{a_3}) & 0 & \tilde{f}(q_1^{a_1}) \\
0 & \tilde{f}(q_3^{a_3}) & \tilde{f}(q_2^{a_2})
\end{bmatrix}
\begin{bmatrix}
g(q_1^{a_1}) \\
g(q_2^{a_2}) \\
g(q_3^{a_3})
\end{bmatrix} =
\begin{bmatrix}
0 \\
0 \\
0
\end{bmatrix}
\]

By our assumptions, the coefficient matrix is non-singular, so only the zero solution exists, hence \( g(q_1^{a_1}) = 0 \).

An analysis similar to what we did before shows that \( g(q_1^{a_1} \cdots q_r^{a_r}) = 0 \) for \( r > 1 \).

With the same method, one can easily show that the characteristic function on \( \mathcal{P} \) is regular.

6. Some simple results on factorisation

Cashwell-Everett \(^4\) showed that \( (\mathcal{A}, +, \cdot) \) is a UFD. We will briefly treat the factorisation properties of \( (\mathcal{A}, +, \oplus) \). Definitions and facts regarding factorisation in commutative rings with zero-divisors from the articles by Anderson and Valdes-Leon \(^1\) \(^2\) will be used.

First, we note that since \( (\mathcal{A}, +, \oplus) \) is quasi-local, it is présimplifiable, i.e. \( a \neq 0 \), \( a = r \oplus u \) implies that \( r \) is a unit. It follows that for \( a, b \in \mathcal{A} \), the following three conditions are equivalent:

1. \( a, b \) are associates, i.e. \( \mathcal{A} \oplus a = \mathcal{A} \oplus b \).
2. \( a, b \) are strong associates, i.e. \( a = u \oplus b \) for some unit \( u \).
3. \( a, b \) are very strong associates, i.e. \( \mathcal{A} \oplus a = \mathcal{A} \oplus b \) and either \( a = b = 0 \), or \( a \neq 0 \) and \( a = r \oplus b \implies r \in U(\mathcal{A}) \).

We say that \( a \in \mathcal{A} \) is irreducible, or an atom, if \( a = b \oplus c \) implies that \( a \) is associate with either \( b \) or \( c \).
Theorem 6.1. \( (\mathcal{A}, +, \oplus) \) is atomic, i.e. all non-units can be written as a product of finitely many atoms. In fact, \( (\mathcal{A}, +, \oplus) \) is a bounded factorial ring (BFR), i.e. there is a bound on the length of all factorisations of an element.

Proof. It follows from Lemma 3.3 that the non-unit \( f \) has a factorisation into at most \( D(f) \) atoms. \( \square \)

Example 6.2. We have that \( e_2 \oplus (e_{2^k} + e_3) = e_6 \) for all \( k \), hence \( e_6 \) has an infinite number of non-associate irreducible divisors, and infinitely many factorisations into atoms.

Example 6.3. The element \( h = e_{30} \) can be factored as \( e_2 \oplus e_3 \oplus e_5 \), or as \( (e_6 + e_{20}) \oplus (e_2 + e_5) \).

These examples show that \( (\mathcal{A}, +, \oplus) \) is neither a half-factorial ring, nor a finite factorisation ring, nor a weak finite factorisation ring, nor an atomic idf-ring.

7. THE SUBRING OF ARITHMETICAL FUNCTIONS SUPPORTED ON SQUARE-FREE INTEgers

Let \( \mathcal{SF} \subset \mathbb{N}^+ \) denote the set of square-free integers, and put

\[ \mathcal{C} = \{ f \in \mathcal{A} | \text{supp}(f) \subset \mathcal{SF} \} \]  

(54)

For any \( f \in \mathcal{A} \), denote by \( p(f) \in \mathcal{C} \) the restriction of \( f \) to \( \mathcal{SF} \).

Theorem 7.1. \( (\mathcal{C}, +, \oplus) \) is a subring of \( (\mathcal{A}, +, \oplus) \), and a closed \( \mathcal{C} \)-subalgebra with respect to the norm \( |\cdot| \). The map

\[ p : \mathcal{A} \rightarrow \mathcal{C}, \quad f \mapsto p(f) \]  

(55)

is a continuous \( \mathcal{C} \)-algebra epimorphism, and a retraction of the inclusion map \( \mathcal{C} \subset \mathcal{A} \).

Proof. Let \( f, g \in \mathcal{C} \). If \( n \in \mathbb{N}^+ \setminus \mathcal{SF} \) then \( (f + g)(n) = f(n) + g(n) = 0 \), and \( cf(n) = 0 \) for all \( c \in \mathcal{C} \). Since \( n \in \mathbb{N}^+ \setminus \mathcal{SF} \), there is at least on prime \( p \) such that \( p^2 | n \). If \( m \) is a unitary divisor of \( m \), then either \( m \) or \( n/m \) is divisible by \( p^2 \). Thus

\[ (f + g)(n) = \sum_{m || n} f(m)g(n/m) = 0. \]

If \( f_k \rightarrow f \) in \( \mathcal{A} \), and all \( f_k \in \mathcal{C} \), let \( n \in \text{supp}(f) \). Then there is an \( N \) such that \( f(n) = f_k(n) \) for all \( k \geq N \). But \( \text{supp}(f_k) \subset \mathcal{SF} \), so \( n \in \mathcal{SF} \). This shows that \( \mathcal{C} \) is a closed subalgebra of \( \mathcal{A} \).

It is clear that \( p(f + g) = p(f) + p(g) \) and that \( p(cf) = cp(f) \) for any \( c \in \mathcal{C} \). If \( n \) is not square-free, we have already showed that

\[ 0 = (p(f) \oplus p(g))(n) = p((f \oplus g))(n). \]

Suppose therefore that \( n \) is square-free. Then so is all its unitary divisors, hence

\[ p(f \oplus g)(n) = (f \oplus g)(n) = \sum_{m || n} f(m)g(n/m) = \sum_{m || n} p(f)(m)p(g)(n/m) = (p(f) \oplus p(g))(n). \]

We have that \( p(f) = f \) if and only if \( f \in \mathcal{C} \), hence \( p(p(f)) = p(f) \), so \( p \) is a retraction to the inclusion \( i : \mathcal{C} \rightarrow \mathcal{A} \). In other words, \( p \circ i = \text{id}_\mathcal{C} \). \( \square \)

Corollary 7.2. The multiplicative inverse of an element in \( \mathcal{C} \) lies in \( \mathcal{C} \).
Proof. If \( f \in \mathcal{E} \), \( f \oplus g = e_1 \) then
\[
e_1 = p(e_1) = p(f \oplus g) = p(f) \oplus p(g) = f \oplus p(g),
\]
hence \( g = p(g) \), so \( g \in \mathcal{E} \).

Alternatively, we can reason as follows. If \( f \) is a unit in \( \mathcal{E} \) then we can without loss of generality assume that \( f(1) = 1 \). By Theorem 3.7, \( g = -f + e_1 \) is topologically nilpotent, hence by Proposition 1.2.4 of [3] we have that the inverse of \( e_1 - g = f \) can be expressed as \( \sum_{i=0}^{\infty} g^i \). It is clear that \( g \), and every power of it, is supported on \( \mathbb{SQF} \), hence so is \( f^{-1} \).

Corollary 7.3. \((\mathcal{E}, +, \oplus)\) is semi-local.

Proof. The units consists of all \( f \in \mathcal{E} \) with \( f(1) \neq 0 \), and the non-units form the unique maximal ideal.

Remark 7.4. More generally, given any subset \( Q \subset \mathbb{N}^+ \), we get a retract of \((A, +, \oplus)\) when considering those arithmetical functions that are supported on the integers \( n = p_1^{a_1} \cdots p_r^{a_r} \) with \( a_i \in Q \cup \{0\} \). This property is unique for the unitary convolution, among all regular convolutions in the sense of Narkiewicz [3].

In particular, the set of arithmetical functions supported on the exponentially odd integers (those \( n \) for which all \( a_i \) are odd) forms a retract of \((A, +, \oplus)\). It follows that the inverse of such a function is of the same form.

Let \( T = \mathbb{C}[x_1, x_2, x_3, \ldots] \), the large power series ring on countably many variables, and let \( J \) denote the ideal of elements supported on non square-free monomials.

Theorem 7.5. \((\mathcal{E}, +, \oplus) \simeq T/J\). This algebra can also be described as the generalized power series ring on the monoid-with-zero whose elements are all finite subsets of a fixed countable set \( X \), with multiplication
\[
A \times B = \begin{cases} A \cup B & \text{if } A \cap B = \emptyset \\ 0 & \text{otherwise} \end{cases}.
\]

Proof. Define \( \eta \) by
\[
\eta : T \rightarrow A, \quad \eta\left( \sum_m c_m m \right) = \sum_{m \text{ square-free}} c_m e_m,
\]
where for a square-free monomial \( m = m_{i_1} \cdots m_{i_r} \) with \( 1 \leq i_1 < \cdots < i_r \) we put \( e_m = e_{p_{i_1} \cdots p_{i_r}} \). Then \( \eta(T) = \mathcal{E} \), \( \ker \eta = J \). It follows that \( \mathcal{E} \simeq T/J \).

References

[1] D. D. Anderson and Silvia Valdes-Leon. Factorization in commutative rings with zero divisors. Rocky Mountain J. Math., 26(2):439–480, 1996.

[2] D. D. Anderson and Silvia Valdes-Leon. Factorization in commutative rings with zero divisors. II. In Factorization in integral domains (Iowa City, IA, 1996), pages 197–219. Dekker, New York, 1997.

[3] S. Bosch, U. G"untzer, and R. Remmert. Non-Archimedean analysis. Springer-Verlag, Berlin, 1984. A systematic approach to rigid analytic geometry.

[4] E. D. Cashwell and C. J. Everett. The ring of number-theoretic functions. Pacific Journal of Mathematics, 9:975–985, 1959.

[5] Eckford Cohen. Arithmetical functions associated with the unitary divisors of an integer. Mathematische Zeitschrift.

[6] James A. Huckaba. Commutative rings with zero divisors. Marcel Dekker Inc., New York, 1988.

[7] W. Narkiewicz. On a class of arithmetical convolutions. Colloq. Math., 10:81–94, 1963.
[8] Emil D. Schwab and Gheorghe Silberberg. A note on some discrete valuation rings of arithmetical functions. *Archivum Mathematicum (Brno)*, 36:103–109, 2000.

[9] Emil D. Schwab and Gheorghe Silberberg. The valuated ring of the arithmetical functions as a power series ring. *Archivum Mathematicum (Brno)*, 37(1):77–80, 2001.

[10] R. Sivaramakrishnan. *Classical theory of arithmetic functions*, volume 126 of *Pure and applied mathematics*. Marcel Dekker, 1989.

[11] R. Vaidyanathaswamy. The theory of multiplicative arithmetic functions. *Trans. Amer. Math. Soc.*, 33(2):579–662, 1931.

[12] Richard M. Wilson. The necessary conditions for t-designs are sufficient for something. *Utilitas Mathematica*, 4:207–215, 1973.

[13] K. L. Yocom. Totally multiplicative functions in regular convolution rings. *Canad. Math. Bull.*, 16:119–128, 1973.

Department of Mathematics, Stockholm University, SE-10691 Stockholm, Sweden

E-mail address: jans@matematik.su.se