ARCHIVUM MATHEMATICUM (BRNO)
Tomus 40 (2004), 161 – 179

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

JAN SNELLMAN

Abstract. We study $(\mathcal{A}, +, \oplus)$, the ring of arithmetical functions with unitary convolution, giving an isomorphism between $(\mathcal{A}, +, \oplus)$ and a generalized power series ring on infinitely many variables, similar to the isomorphism of Cashwell-Everett [4] between the ring $(\mathcal{A}, +, \cdot)$ of arithmetical functions with *Dirichlet convolution* and the power series ring $\mathbb{C}[\![x_1, x_2, x_3, \dots]\!]$ 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 $(\mathcal{A}, +, \cdot)$, 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

$$f \cdot g(k) = \sum_{r|k} f(r)g(k/r)\,. \tag{1}$$

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 $\mathbf{0}$.

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

$$(\mathcal{A}, +, \cdot) \simeq \mathbb{C}[\![x_1, x_2, x_3, \dots]\!]\,, \tag{2}$$

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

2000 *Mathematics Subject Classification*: 11A25, 13J05, 13F25.
Key words and phrases: unitary convolution, Schauder Basis, factorization into atoms, zero divisors.
Received January 28, 2002.

Schwab and Silberberg [9] topologised $(\mathcal{A}, +, \cdot)$ by means of the norm

$$|f| = \frac{1}{\min \{ \, k \mid f(k) \neq 0 \, \}} \, . \tag{3}$$

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

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

They showed that $(\mathcal{A}, |\cdot|)$ 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 $\sum_{k=1} c_k e_k$, with $c_k \in \mathcal{A}$.

In this article, we treat instead $(\mathcal{A}, +, \oplus)$, the ring of all arithmetical functions with unitary convolution. This ring has been studied by several authors, such as Vaidyanathaswamy [11], Cohen [5], and Yocom [13].

We topologise $\mathcal{A}$ in the same way as Schwab and Silberberg [9], 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

We denote the integers by $\mathbb{Z}$, the non-negative integers by $\mathbb{N}$, and the positive integers by $\mathbb{N}^+$. Let p_i be the i'th prime number. Denote by $\mathcal{P}$ the set of prime numbers, and by $\mathcal{PP}$ the set of prime powers. The integer 1 is not a prime, nor a prime power. Let $\omega(r)$ be 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

$$k \oplus m = \begin{cases} km & \gcd(k, m) = 1 \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

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

The so-called *unitary convolution* was introduced by Vaidyanathaswamy [11], and was further studied Eckford Cohen [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

$$(f \oplus g)(n) = \sum_{\substack{m \oplus p = n \\ m,n \geq 1}} f(m)g(n) = \sum_{d \| n} f(d)g(n/d) \tag{5}$$

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

$$e_k(n) = \begin{cases} 1 & k = n \\ 0 & k \neq n \end{cases} \tag{6}$$

We also define[1] $\mathbf{0}$ as the zero function, and $\mathbf{1}$ as the function which is constantly 1.

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

$$(e_{k_1} \oplus e_{k_2} \oplus \cdots \oplus e_{k_r})(n) = \begin{cases} 1 & n = k_1 k_2 \cdots k_r \quad \textit{and} \quad \gcd(k_i, k_j) = 1 \\ & \qquad\qquad\qquad\qquad \textit{for} \quad i \neq j \\ 0 & \textit{otherwise} \end{cases} \tag{7}$$

hence

$$e_{k_1} \oplus e_{k_2} \oplus \cdots \oplus e_{k_r} = \begin{cases} e_{k_1 k_2 \cdots k_r} & \textit{if} \quad \gcd(k_i, k_j) = 1 \quad \textit{for} \quad i \neq j \\ 0 & \textit{otherwise} \end{cases} \tag{8}$$

Proof. The first assertions are trivial. We have [10] that for $f_1, \ldots, f_r \in \mathcal{A}$,

$$(f_1 \oplus \cdots \oplus f_r)(n) = \sum_{a_1 \oplus \cdots \oplus a_r = n} f_1(a_1) \cdots f_r(a_r) \tag{9}$$

Since

$$e_{k_1}(a_1) e_{k_2}(a_2) \cdots e_{k_r}(a_r) = 1 \quad \text{iff} \quad \forall i : k_i = a_i\,,$$

(7) follows. □

Lemma 2.5. *For $n \in \mathbb{N}^+$, e_n can be uniquely expressed as a square-free monomial in $\{\, e_k \mid k \in \mathcal{PP} \,\}$ (we use the convention that the empty product corresponds to the multiplicative unit e_1).*

Proof. By unique factorization, there is a unique way of writing $n = p_{i_1}^{a_1} \cdots p_{i_r}^{a_r}$, and (8) gives that

$$e_n = e_{p_{i_1}^{a_1} \cdots p_{i_r}^{a_r}} = e_{p_{i_1}^{a_1}} \oplus \cdots \oplus e_{p_{i_r}^{a_r}}\,. \qquad \square$$

Theorem 2.6. *$(\mathcal{A}, +, \oplus)$ is a quasi-local, non-noetherian commutative ring having divisors of zero. The units $U(\mathcal{A})$ consists of those f such that $f(1) \neq 0$.*

[1] In [10], $\mathbf{1}$ is denoted e, and e_1 denoted e_0.

Proof. It is shown in [10] that $(\mathcal{A}, +, \oplus)$ is a commutative ring, having zero-divisors, and that the units consists of those f such that $f(1) \neq 0$. If $f(1) = 0$ then

$$(f \oplus g)(1) = f(1)g(1) = 0 .$$

Hence the non-units form an ideal $\mathfrak{m}$, which is then the unique maximal ideal.

We will show (Lemma 3.10) that $\mathfrak{m}$ contains an ideal (the ideal generated by all e_k, for $k > 1$) which is not finitely generated, so $\mathcal{A}$ is non-noetherian. □

3. A topology on $\mathcal{A}$

The results of this section are inspired by [9], were the authors studied the ring of arithmetical functions under Dirichlet convolution. We'll use the notations of [3]. We regard $\mathbb{C}$ as trivially normed.

Definition 3.1. Let $f \in \mathcal{A} \setminus \{\mathbf{0}\}$. We define the *support* of f as

$$\operatorname{supp}(f) = \left\{ n \in \mathbb{N}^+ \mid f(n) \neq 0 \right\} . \tag{10}$$

We define the *order*[2] of a non-zero element by

$$\mathrm{N}(f) = \min \operatorname{supp}(f) . \tag{11}$$

We also define the *norm* of f as

$$|f| = \mathrm{N}(f)^{-1} \tag{12}$$

and the *degree* as

$$\mathrm{D}(f) = \min \left\{ \omega(k) \mid k \in \operatorname{supp}(f) \right\} . \tag{13}$$

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

Lemma 3.2. *The value semigroup of $(\mathcal{A}, |\cdot|)$ is*

$$|\mathcal{A} \setminus \{\mathbf{0}\}| = \left\{ 1/k \mid k \in \mathbb{N}^+ \right\} ,$$

a discrete subset of $\mathbb{R}^+$.

Lemma 3.3. *Let $f, g \in \mathcal{A} \setminus \{\mathbf{0}\}$. Let $\mathrm{N}(f) = i$, $\mathrm{N}(g) = j$, so that $f(i) \neq 0$ but $f(k) = 0$ for all $k < i$, and similarly for g. Then, the following hold:*

(i) $\mathrm{N}(f - g) \geq \min \{\mathrm{N}(f), \mathrm{N}(g)\}$.
(ii) $\mathrm{N}(cf) = \mathrm{N}(f)$ *for* $c \in \mathbb{C} \setminus \{0\}$.
(iii) $\mathrm{N}(f) = 1$ *iff f is a unit.*
(iv) $\mathrm{N}(f \cdot g) = \mathrm{N}(f)\mathrm{N}(g) \leq \mathrm{N}(f \oplus g)$, *with equality iff* $\gcd(i, j) = 1$.
(v) $\mathrm{N}(f \oplus g) \geq \max \{\mathrm{N}(f), \mathrm{N}(g)\}$, *with strict inequality iff both f and g are non-units.*
(vi) $\mathrm{D}(f + g) \geq \min \{\mathrm{D}(f), \mathrm{D}(g)\}$.
(vii) $\mathrm{D}(f) = 0$ *if and only if f is a unit.*
(viii) $\mathrm{D}(f \oplus g) \geq \mathrm{D}(f) + \mathrm{D}(g) \geq \max \{\mathrm{D}(f) , \mathrm{D}(g)\}$,
with $\mathrm{D}(f) + \mathrm{D}(g) > \max \{\mathrm{D}(f), \mathrm{D}(g)\}$ *if f, g are non-units.*

[2] In [10] the term *norm* is used.

Proof. (i), (ii), and (iii) are trivial, and (iv) is proved in [10].

If $\omega(s) < \min\{\mathrm{D}(f), \mathrm{D}(g)\}$ then

$$s \notin \operatorname{supp}(f) \cup \operatorname{supp}(g),$$

so

$$(f+g)(s) = f(s) + g(s) = 0.$$

This proves (vi). Since f is a unit iff $f(1) \neq 0$, (vii) follows.

For any a in the support of f and any b in the support of g, such that $a \oplus b \neq 0$, we have that

$$\omega(a \oplus b) = \omega(a) + \omega(b) \geq \mathrm{D}(f) + \mathrm{D}(g).$$

This proves the first inequality of (viii). Using (vii) the other assertion follows.

(v) is proved similarly. □

Corollary 3.4. $|f \oplus g| \leq |f||g| = |f \cdot g|$.

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

Proof. $((\mathcal{A}, +, \cdot), |\cdot|)$ is a valuated ring, and a faithfully normed complete vector space over $\mathbb{C}$ [9]. It is also separable with respect to bounded maps [3, Corollary 2.2.3]. So $(\mathcal{A}, +)$ is a normed group, hence Corollary 3.4 shows that $(\mathcal{A}, +, \oplus)$ is a normed ring. □

Note that, unlike $((\mathcal{A}, +, \cdot), |\cdot|)$, the normed ring $((\mathcal{A}, +, \oplus), |\cdot|)$ is not a valued ring, since

$$|e_2 \oplus e_2| = |\mathbf{0}| = 0 < |e_2|^2 = 1/4.$$

In fact, defining f^n to be the n'th unitary power of n, we have that

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 $n > 1$.*

Proof. The first assertion is trivial, so suppose that f is a non-unit. From Corollary 3.4 we have that $|f^n| \leq |f|^n$. If $|f| = 1/k$, $k > 1$, i.e. $f(k) \neq 0$ but $f(j) = 0$ for $j < k$, then $f^2(k^2) = 0$ since $\gcd(k, k) = k > 1$. It follows that $\left|f^2\right| > |f|^2$, from which the result follows. □

Recall that in a normed ring, a non-zero element f is called

- *topologically nilpotent* if $f^n \to 0$,
- *power-multiplicative* if $|f^n| = |f|^n$ for all n,
- *multiplicative* if $|fg| = |f||g|$ for all g in the ring.

Theorem 3.7. *Let $f \in ((\mathcal{A}, +, \oplus), |\cdot|)$, $f \neq \mathbf{0}$. Then the following are equivalent:*

(1) *f is topologically nilpotent,*

(2) *f is not power-multiplicative,*

(3) *f is not multiplicative*[3] *in the normed ring $(\mathcal{A}, +, \oplus), |\cdot|)$,*

[3]This is not the same concept as multiplicativity for arithmetical functions, i.e. that $f(nm) = f(n)f(m)$ whenever $\gcd(n, m) = 1$. However, since the latter kind of elements satisfy $f(1) = 1$, they are units, and hence multiplicative in the normed-ring sense.

(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,

$$1 = \left|f^{-1}\right| = |f|^{-1} . \qquad \square$$

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

$$\begin{aligned} &\mathcal{A} \times \mathcal{A}' \to \mathbb{C} \\ &\langle f, g \rangle = \sum_{k=1}^{\infty} f(k)g(k) \end{aligned} \tag{14}$$

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

$$f = \sum_{k=1}^{\infty} c_k e_k \, , \qquad c_k \in \mathbb{C} \tag{15}$$

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*

$$\langle f, e_k \rangle = f(k) = c_k \tag{16}$$

(iv)

$$\max_{k \in \mathbb{N}^+} \{|c_k||e_k|\} = \left| \sum_{k=1}^{\infty} c_k e_k \right| . \tag{17}$$

The set $\{e_1\} \cup \{ e_p \mid p \in \mathcal{PP} \}$ generates a dense subalgebra of $((\mathcal{A}, +, \oplus), |\cdot|)$.

Proof. It is proved in [9] that this set is a Schauder base in the topological vector space $(\mathcal{A}, |\cdot|)$. It also follows from [9] 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 $\{\, e_p \mid p \in \mathcal{PP}\,\}$. The set $\{\, e_k \mid k \in \mathbb{N}^+\,\}$ is dense in $\mathcal{A}$, so $\{\, e_p \mid p \in \mathcal{PP}\,\}$ 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. The following proof was provided by the anonymous referee. Consider the following ideal I in $\mathcal{A}$:

$$I = \{f \in \mathcal{A} \mid f(1) = 0\,,\ \forall\, p \in \mathcal{P} :\ f(p) = 0\}\,.$$

Then the units of $\mathcal{A}/I$ are precisely the elements of the form $g + I$, where $g \in \mathcal{A}$, $g(1) \neq 0$. Moreover, for any $f, g \in \mathcal{A}$ such that $f(1) = a \in \mathbb{C}$, $g(1) = 0$, we have $(f + I) \oplus (g + I) = (ag) + I = a(g + I)$. Assume that J is finitely generated ideal, say $J = (b_1, \dots, b_r)$. Then $b_1(1) = \cdots = b_r(1) = 0$ and any element of J is of the form $\sum_{i=1}^r f_i \oplus b_i$ for suitable $f_1, \dots f_r \in \mathcal{A}$. We have

$$\left(\sum_{i=1}^r f_i \oplus b_i\right) + I = \sum_{i=1}^r (f_i + I) \oplus (b_i + I) = \sum_{i=1}^r a_i(b_i + I)\,,$$

where $a_i = f_i(1) \in \mathbb{C}$, which belongs to the finitely dimensional linear subspace of $\mathcal{A}/I$ generated by $b_1 + I, \dots, b_r + I$. This is a contradiction with the fact that the linear subspace of $\mathcal{A}/I$ generated by $e_k + I$, $k > 1$, is of infinite dimension. □

Definition 3.11. An ideal $I \subset \mathcal{A}$ 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

$$f = \sum_{k=1}^\infty a_k \oplus g_k\,, \qquad a_k \in \mathcal{A}\,. \tag{18}$$

Lemma 3.12. *$\mathfrak{m}$ is quasi-finite.*

Proof. By Theorem 3.9 the set $\{\, e_k \mid k > 1\,\}$ is a quasi-finite generating set for $\mathfrak{m}$. □

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

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

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

such that for all $f \in I$,

$$\exists c_1, c_2, c_3, \dots \in \mathbb{C}\,, \qquad f = \sum_{i=1}^\infty c_i g_i\,. \tag{20}$$

So all subspaces possesses a Schauder basis.

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

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

we choose a $g_k \in I$ with $\mathrm{N}(g_k) = k$, 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 $g_k = \mathbf{0}$.

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 $f_i \neq \mathbf{0}$,

$$\begin{aligned} n_i &:= N(f_i)\,, \\ \mathbb{C} \ni a_i &:= f_i(n_i)\,, \\ \mathcal{A} \ni f_{i+1} &:= f_i - a_i g_{n_i}\,. \end{aligned}$$

Of course, if $f_i = \mathbf{0}$, 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 $f_i \in I$, so $n_i \in N(I)$, hence $g_{n_i} \neq 0$. Thus $\mathrm{N}(f_{i+1}) > \mathrm{N}(f_i)$, 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

$$Y = \left\{ y_i^{(j)} \mid i, j \in \mathbb{N}^+ \right\} \tag{21}$$

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

$$Y_i = \left\{ y_i^{(j)} \mid j \in \mathbb{N}^+ \right\} \tag{22}$$

the *i'th column* of Y.

Let $[Y]$ denote the free abelian monoid on Y, and let $\mathcal{M}$ be the subset of *separated monomials*, i.e. monomials in which no two occurring variables come from the same column:

$$\mathcal{M} = \left\{ y_{i_1}^{(j_1)} y_{i_2}^{(j_2)} \cdots y_{i_r}^{(j_r)} \mid 1 \leq i_i < i_2 < \cdots i_r \right\}. \tag{23}$$

We regard $\mathcal{M}$ as a monoid-with-zero, so that the multiplication is given by

$$m \oplus m' = \begin{cases} mm' & mm' \in \mathcal{M} \\ 0 & \text{otherwise} \end{cases} \tag{24}$$

Note that the zero is exterior to $\mathcal{M}$, i.e. $0 \notin \mathcal{M}$. The set $\mathcal{M} \cup \{0\}$ is a (non-cancellative) monoid if we define $m \oplus 0 = 0$ for all $m \in \mathcal{M}$.

Recall that $\mathcal{PP}$ 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

$$\begin{aligned} \Phi : Y &\to \mathcal{PP}\,, \\ y_i^{(j)} &\mapsto p_i^j \end{aligned} \tag{25}$$

is a bijection which can be extended to a bijection

$$\begin{aligned} \Phi : \mathcal{M} &\to \mathbb{N}^+\,, \\ 1 &\mapsto 1\,, \\ y_{i_1}^{(j_1)} \cdots y_{i_r}^{(j_r)} &\mapsto p_{i_1}^{j_1} \cdots p_{i_r}^{j_r}\,. \end{aligned} \tag{26}$$

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 $\mathcal{A}$ 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. $R = C[\![Y]\!]$ consists of all formal power series $\sum c_{\boldsymbol{\alpha}} \boldsymbol{y}^{\boldsymbol{\alpha}}$, where the sum is over all multi-sets $\boldsymbol{\alpha}$ on Y.

Let S be the generalized monoid-with-zero ring on $\mathcal{M}$. By this, we mean that S is the set of all formal power series

$$\sum_{m \in \mathcal{M}} f(m)m\,, \qquad f(m) \in \mathbb{C} \tag{27}$$

with component-wise addition, and with multiplication

$$\begin{aligned} \left(\sum_{m \in \mathcal{M}} f(m)m\right) \oplus \left(\sum_{m \in \mathcal{M}} g(m)m\right) = \left(\sum_{m \in \mathcal{M}} h(m)m\right)\,, \\ h(m) = (f \oplus g)(m) = \sum_{s \oplus t = m} f(s)g(t)\,. \end{aligned} \tag{28}$$

Define

$$\operatorname{supp}(\sum_{m \in [Y]} c_m m) = \{\, m \in [Y] \mid c_m \neq 0 \,\}\,, \tag{29}$$

$$\operatorname{supp}(\sum_{m \in \mathcal{M}} c_m m) = \{\, m \in \mathcal{M} \mid c_m \neq 0 \,\}\,. \tag{30}$$

Let furthermore

$$\mathfrak{D} = \{\, f \in R \mid \operatorname{supp}(f) \cap \mathcal{M} = \emptyset \,\}\,. \tag{31}$$

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

Proof. The bijection (26) induces a bijection between S and $\mathcal{A}$ which is an isomorphism because of the way multiplication is defined on S. In detail, the isomorphism is defined by

$$\begin{aligned} S \ni \sum_{m \in \mathcal{M}} c_m m &\mapsto f \in \mathcal{A}\,, \\ f(\Phi(m)) &= c_m\,. \end{aligned} \tag{32}$$

For the second part, consider the epimorphism

$$\begin{gathered} \phi : R \to S\,, \\ \phi\left(\sum_{m \in [Y]} c_m m\right) = \sum_{m \in \mathcal{M}} c_m m\,. \end{gathered}$$

Clearly, $\ker(\phi) = \mathfrak{D}$, hence $S \simeq \frac{R}{\ker(\phi)} = \frac{R}{\mathfrak{D}}$. □

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

$$\mathbf{1} = \sum_{m \in \mathcal{M}} m = \prod_{i=1}^{\infty} \left(1 + \sum_{j=1}^{\infty} y_i^{(j)}\right)\,. \tag{33}$$

What does its inverse μ^* correspond to?

Definition 4.2. For $m \in \mathcal{M}$, we denote by $\omega(m)$ the number of occurring variables in m (by definition, $\omega(1) = 0$). For

$$S \ni f = \sum_{m \in \mathcal{M}} c_m m$$

we put

$$\mathrm{D}(f) = \min\{\, \omega(m) \mid c_m \neq 0 \,\} \tag{34}$$

if $f \neq 0$ and $D(\mathbf{0}) = \infty$. Then $\omega(\Phi(m)) = \omega(m)$, and if f and g correspond to each other via the isomorphism (32), then $\mathrm{D}(f) = \mathrm{D}(g)$.

It is known (see [10]) that

$$\mu^*(r) = (-1)^{\omega(r)}\,. \tag{35}$$

We then have that μ^* corresponds to

$$\mathbf{1}^{-1} = \frac{1}{\prod_{i=1}^{\infty}\left(1 + \sum_{j=1}^{\infty} y_i^{(j)}\right)} = \prod_{i=1}^{\infty} \frac{1}{1 + \sum_{j=1}^{\infty} y_i^{(j)}} = \sum_{m \in \mathcal{M}} (-1)^{\omega(m)} m\,. \tag{36}$$

Recall that $f \in \mathcal{A}$ is a *multiplicative* arithmetic function if $f(nm) = f(n)f(m)$ whenever $\gcd(n, m) = 1$. Regarding $f \neq \mathbf{0}$ as an element of S we have that f is multiplicative if and only if it can be written as

$$f = \prod_{i=1}^{\infty} \left(1 + \sum_{j=1}^{\infty} c_{i,j} y_i^{(j)} \right) . \tag{37}$$

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 $(\mathcal{A}, +, \cdot)$, the ring of arithmetical functions with Dirichlet convolution. We give the corresponding result for $\mathcal{A} = (\mathcal{A}, +, \oplus)$:

Theorem 4.3. *Every continuous endomorphism θ of the $\mathbb{C}$-algebra $S \simeq \mathcal{A}$ is defined by*

$$\theta(y_i^{(j)}) = \gamma_{i,j} , \tag{38}$$

where

$$\gamma_{i,j}\gamma_{i,k} = 0 \qquad \textit{for all} \quad i, j, k \tag{39}$$

and

$$\gamma_{a_1(n),b_1(n)} \cdots \gamma_{a_r(n),b_r(n)} \to 0 \qquad \textit{as} \quad n = p_{a_1(n)}^{b_1(n)} \cdots p_{a_r(n)}^{b_r(n)} \to \infty . \tag{40}$$

Proof. Recall that $S \simeq \frac{R}{\mathfrak{D}}$, where $R = \mathbb{C}[\![Y]\!]$ and $\mathfrak{D}$ 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 of S, any continuous C--algebra endomorphism θ of S is determined by its values on the $y_i^{(j)}$'s, and must fulfill (40). Since $y_i^{(j)} y_i^{(k)} = 0$ in S, we must have that

$$\theta(0) = \theta(y_i^{(j)} y_i^{(k)}) = \theta(y_i^{(j)})\theta(y_i^{(k)}) = \gamma_{i,j}\gamma_{i,k} = 0 . \qquad \square$$

5. Nilpotent elements and zero divisors

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

$$\operatorname{psupp}(m) = \{ p \in \mathcal{P} \mid p \mid m \} \tag{41}$$

and (when $m > 1$) the *leading prime* as

$$\operatorname{lp}(m) = \min \operatorname{psupp}(m) . \tag{42}$$

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

$$A^{(n)} = \left\{ k \in \mathbb{N}^+ \mid p_n \mid k \text{ but } p_i \nmid k \text{ for } i < n \right\} = \left\{ k \in \mathbb{N}^+ \mid \operatorname{lp}(k) = p_n \right\} . \tag{43}$$

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

$$\mathbb{N}^+ \setminus \{1\} = \bigsqcup_{i=1}^{\infty} A^{(i)} . \tag{44}$$

Definition 5.2. If $f \in \mathcal{A}$ is a non-unit, then the *canonical decomposition* of f is the unique way of expressing f as a convergent sum

$$f = \sum_{i=1}^{\infty} f_i, \quad f_i = \sum_{k \in A^{(i)}} f(k) e_k \,. \tag{45}$$

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 $f_N \neq \mathbf{0}$ is called the *filtration degree* of f.

Lemma 5.3. *If $f \in \mathcal{A}$ is a non-unit with canonical decomposition* (45), *then*

$$f_i = \sum_{j=1}^{\infty} e_{p_i^j} \oplus g_{i,j} \,, \tag{46}$$

where $r \leq i$, $p_r \mid n$ implies that $g_{i,j}(n) = 0$. For any n there is at most one pair (i, j) such that

$$\left(e_{p_i^j} \oplus g_{i,j} \right)(n) \neq 0 \,.$$

More precisely, if

$$n = p_{i_1}^{j_1} \cdots p_{i_r}^{j_r} \,, \qquad i_1 < \cdots < i_r \,,$$

then $\left(e_{p_a^b} \oplus g_{a,b} \right)(n)$ may be non-zero only for $a = i_1$, $b = j_1$.

Definition 5.4. For $k \in \mathbb{N}$, define

$$I_k = \{\, f \in \mathcal{A} \mid f(n) = 0 \;\text{ for every } n \text{ such that } \gcd(n, p_1 p_2 \cdots p_k) = 1 \,\} \,. \tag{47}$$

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

$$f \in I_k,\, g \in \mathcal{A} \quad \text{and} \quad \gcd(n, p_1 p_2 \cdots p_k) = 1$$

then

$$(f \oplus g)(n) = \sum_{d \| n} f(d) g(n/d) = 0 \,,$$

since $\gcd(d, p_1 p_2 \cdots p_k) = 1$ for any unitary divisor of n. □

For any $h \in \mathcal{A}$, the *annihilator* $\operatorname{ann}(h) \subset \mathcal{A}$ is the ideal consisting of all elements $g \in \mathcal{A}$ such that $gh = \mathbf{0}$.

Theorem 5.6. *Let $N \in \mathbb{N}^+$, then*

$$\begin{aligned} I_N &= \operatorname{ann}(e_{p_1 \cdots p_N}) \\ &= \{\mathbf{0}\} \cup \{ f \in \mathcal{A} \mid f \textit{ is a non-unit of polynomial type} \\ &\qquad\qquad \textit{and has filtration degree at most } N \} \\ &= \overline{\mathcal{A} \left\{ e_{p_i^a} \mid a, i \in \mathbb{N}^+,\, i \leq N \right\}} \,, \end{aligned}$$

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

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

$$
\begin{aligned}
(f \oplus e_{p_1 \cdots p_N})(k) &= \sum_{a \oplus p_1 \cdots p_N = k} f(a) e_{p_1 \cdots p_N}(p_1 \cdots p_N) \\
&= \sum_{a \oplus p_1 \cdots p_N = k} f(a) = 0\,, \qquad (48)
\end{aligned}
$$

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

$$
0 = (f \oplus e_{p_1 \cdots p_N})(np_1 \cdots p_N) = f(n) e_{p_1 \cdots p_N}(p_1 \cdots p_N) = f(n) \qquad (49)
$$

hence $f \in I_N$.

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

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

Hence $f = \sum_{i=1}^{N} f_i$. Conversely, if f can be expressed in this way, then $f(k) = f_{j_1}(k) = 0$ for $k = p_{j_1}^{a_1} \cdots p_{j_r}^{a_r}$ 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) *$f \in \bigcup_{N=1}^{\infty} \operatorname{ann}(e_{p_1 p_2 \cdots p_N})$.*

(v) *There is a positive integer N such that f is contained in the topological closure of the ideal generated by the set*

$$
\left\{ e_{p_i^a} \;\middle|\; a, i \in \mathbb{N}^+,\, i \leq N \right\}.
$$

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) $\iff$ (v) follows from the previous theorem.

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

$$
f = \sum_{i=1}^{N} f_i \qquad (50)
$$

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 is square-free. Since $f_i \oplus f_i = \mathbf{0}$ for all i, we have that $f^{N+1} = \mathbf{0}$. 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 I_n form an ascending chain of ideals. $\square$

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 5.8 it would follow that $Z(\mathcal{A})$ 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* [6] *that $(\mathcal{A}, +, \oplus)$ has* few zero divisors*, hence is* additively regular*, hence is a* Marot ring*.*

Theorem 5.10. $(\mathcal{A}, +, \oplus)$ *contains infinitely many non-associate regular non-units.*

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

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

Then f is a non-unit, and using a result by Yocom [13, 8] we have that f is contained in a subring of $(\mathcal{A}, +, \oplus)$ which is a discrete valuation ring isomorphic to $\mathbb{C}\llbracket t \rrbracket$, 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 $g \in \mathcal{A}$, $f \oplus g = \mathbf{0}$. We will show that $g = \mathbf{0}$.

Any positive integer m can be written $m = q_1^{a_1} \cdots q_r^{a_r}$, where the q_i are distinct prime numbers. If $r = 0$, then $m = 1$, and $g(1) = 0$, since

$$0 = (f \oplus g)(2) = f(2)g(1) = g(1)\,.$$

For the case $r = 1$, we want to show that $g(q^a) = 0$ for all prime numbers q. Choose three different prime powers $q_1^{a_1}$, $q_2^{a_2}$, and $q_3^{a_3}$. Then

$$0 = f \oplus g(q_i^{a_i} q_j^{a_j}) = f(q_i^{a_i})g(q_j^{a_j}) + f(q_j^{a_j})g(q_i^{a_i}) = g(q_j^{a_j}) + g(q_i^{a_i})\,,$$

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

$$g(q_1^{a_1} \cdots q_r^{a_r}) = 0 \tag{51}$$

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 $q_1^{a_1}, \dots, q_N^{a_N}$. For each $r+1$-subset $q_{s_1}, \dots, q_{s_{r+1}}$ of this set we get a homogeneous linear equation

$$\begin{aligned} 0 &= f \oplus g(q_{s_1} \dots q_{s_{r+1}}) \\ &= g(q_{s_2} \cdots q_{s_{r+1}}) + g(q_{s_1} q_{s_3} \cdots q_{s_{r+1}}) + \cdots + g(q_{s_1} \cdots g_{s_r}) \,. \end{aligned} \tag{52}$$

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 (51) 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 $\tilde{f}$, with

$$\tilde{f}(k) = \begin{cases} c_k & k \in \mathcal{PP} \\ 0 & \text{otherwise} \end{cases}$$

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 $r = 0$,

$$0 = f \oplus g(p^a) = f(p^a) g(1) = c_{p^a} g(1) \,.$$

We demand that $c_{p^a} \neq 0$, 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 $\mathcal{PP}$, 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 $\mathcal{PP}$. For $m = q_1^{a_1} \cdots q_r^{a_r}$ as before, the case $r = 0$ yields nothing:

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

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

$$\begin{aligned} 0 &= g \oplus \tilde{f}(q_1^{a_1} q_3^{a_3}) = \tilde{f}(q_1^{a_1}) g(q_3^{a_3}) + g(q_1^{a_1}) \tilde{f}(q_3^{a_3}) \,, \\ 0 &= g \oplus \tilde{f}(q_2^{a_2} q_3^{a_3}) = \tilde{f}(q_2^{a_2}) g(q_3^{a_3}) + g(q_1^{a_1}) \tilde{f}(q_3^{a_3}) \,, \end{aligned}$$

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. $a \neq \mathbf{0}$, $a = r \oplus a$ 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 $a = b = \mathbf{0}$, or $a \neq \mathbf{0}$ 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 $\mathrm{D}(f)$ atoms. □

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 $\mathcal{SQF} \subset \mathbb{N}^+$ denote the set of square-free integers, and put

$$\mathfrak{C} = \{ f \in \mathcal{A} \mid \operatorname{supp}(f) \subset \mathcal{SQF} \} \,. \tag{53}$$

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

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

$$\begin{aligned} p : \mathcal{A} &\to \mathfrak{C}\,, \\ f &\mapsto p(f) \end{aligned} \tag{54}$$

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

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

$$(f \oplus g)(n) = \sum_{m \| n} f(m) g(n/m) = 0\,.$$

If $f_k \to f$ in $\mathcal{A}$, and all $f_k \in \mathfrak{C}$, let $n \in \operatorname{supp}(f)$. Then there is an N such that $f(n) = f_k(n)$ for all $k \geq N$. But $\operatorname{supp}(f_k) \subset \mathcal{SQF}$, so $n \in \mathcal{SQF}$. This shows that $\mathfrak{C}$ 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 $c \in \mathbb{C}$. 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

$$\begin{aligned} p(f \oplus g)(n) = (f \oplus g)(n) &= \sum_{m \| n} f(m) g(n/m) \\ &= \sum_{m \| n} p(f)(m) p(g)(n/m) = (p(f) \oplus p(g))(n)\,. \end{aligned}$$

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

Corollary 7.2. *The multiplicative inverse of an element in $\mathfrak{C}$ lies in $\mathfrak{C}$.*

Proof. If $f \in \mathfrak{C}$, $f \oplus g = e_1$ then

$$e_1 = p(e_1) = p(f \oplus g) = p(f) \oplus p(g) = f \oplus p(g)\,,$$

hence $g = p(g)$, so $g \in \mathfrak{C}$.

Alternatively, we can reason as follows. If f is a unit in $\mathfrak{C}$ 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 $\mathcal{SQF}$, hence so is f^{-1}. $\square$

Corollary 7.3. $(\mathfrak{C}, +, \oplus)$ *is semi-local.*

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

Remark 7.4. More generally, given any subset $Q \subset \mathbb{N}^+$, we get a retract of $(\mathcal{A}, +, \oplus)$ 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 [7].

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 $(\mathcal{A}, +, \oplus)$. 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. $(\mathfrak{C}, +, \oplus) \simeq T/J$. *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*

$$A \times B = \begin{cases} A \cup B & \text{if } A \cap B = \emptyset \\ 0 & \text{otherwise} \end{cases} \tag{55}$$

Proof. Define η by

$$\begin{aligned} &\eta : T \to \mathcal{A} \\ &\eta\Big(\sum_m c_m m\Big) = \sum_{m \text{ square-free}} c_m e_m\,, \end{aligned} \tag{56}$$

where for a square-free monomial $m = x_{i_1} \cdots x_{i_r}$ with $1 \leq i_1 < \cdots < i_r$ we put $e_m = e_{p_{i_1} \cdots p_{i_r}}$. Then $\eta(T) = \mathfrak{C}$, $\ker \eta = J$. It follows that $\mathfrak{C} \simeq T/J$. $\square$

Acknowledgement. I am grateful to the anonymous referee for suggesting several corrections and improvements, and for the proof of Lemma 3.10.

References

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

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

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

[4] Cashwell, E. D. and Everett, C. J., *The ring of number-theorethic functions*, Pacific J. Math. **9** (1959), 975–985.

[5] Cohen, E., *Arithmetical functions associated with the unitary divisors of an integer*, Math. Z. **74** (1960), 66–80.

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

[7] Narkiewicz, W., *On a class of arithmetical convolutions*, Colloq. Math. **10** (1963), 81–94.

[8] Schwab, E. D. and Silberberg, G., *A note on some discrete valuation rings of arithmetical functions*, Arch. Math. (Brno) **36** (2000), 103–109.

[9] Schwab, E. D. and Silberberg, G., *The valuated ring of the arithmetical functions as a power series ring*, Arch. Math. (Brno) **37**(1) (2001), 77–80.

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

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

[12] Wilson, R. M. *The necessary conditions for t-designs are sufficient for something*, Util. Math. **4** (1973), 207–215.

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

Department of Mathematics, Stockholm University
SE-10691 Stockholm, Sweden
E-mail: Jan.Snellman@math.su.se