Rings of arithmetic functions with regular convolution

Elin Gawell

9th September 2005

Abstract

This work deals with regular convolutions and the structure of the rings of artihmetic functions where a regular convolution is the multiplication.

In chapter 1 one finds definitions necessary for the report. In section 1.2 the *regular convolution* is defined. The section contains Narkewicz' classification of regular convolutions.

Chapter 2 treats the restriction to the subring $\Gamma[V] = \{f : \mathbb{N}^+ \to \mathbb{C} | f(n) = 0, n \notin V\}$ and describe how these parts can be joined together to the whole ring. The idea behind this work was that it might be easier to study the subrings and then use the results to describe the whole ring.

The purpose of chapter 3 is to find possible regular convolutions. To do this we consider the progressions as *incidence algebras*. The main result of this chapter is the discovery of the *ternary convolution*, which is then described in chapter 4.

In chapter 4 one also finds an explicit formulae for the inverse of invertible elements in the ring with ternary convolution. This formulae accually work regardless of choice of regular convolution.

The main result of chapter 5 is that there exist only one regular convolution on the ring $\Gamma[W]$, where W is the square-free integers. We also state the conjecture that all zero divisors and nilpotent elements in $\Gamma[W]$ are of polynomial type.

Chapter 6 deals with the restrictions to $[n]$. We describe the ring as a monomial ring and study the the monomial ideals a bit further.

Contents

Chapter 1

Introduction and preliminaries

1.1 Definitions

Let $\mathbb{N}$ and $\mathbb{N}^+$ denote the non-negative respectively the positive integers. We denote the i'th prime number by p_i, and the set of all prime numbers by $\mathbb{P}$. The set of prime powers is denoted by $\mathbb{PP}$. Let the $\mathbb{C}$-vector space, with coordinatewise addition and scalar multiplication, of arithmetic functions $f : \mathbb{N}^+ \to \mathbb{C}$ be denoted Γ.

Definition 1.1. Let $f \in \Gamma \setminus \{0\}$. Define the *support* of f as

$$\operatorname{supp}(f) = \{n \in \mathbb{N}^+ | f(n) \neq 0\} \tag{1.1}$$

Define the *order* of a non-zero element by

$$\operatorname{ord}(f) = \min \operatorname{supp}(f) \tag{1.2}$$

Define the *norm* of f as

$$|f| = \frac{1}{\operatorname{ord}(f)} \tag{1.3}$$

By definition the zero element has order infinity and norm 0. This is an ultra-norm on Γ.

If we give $\mathbb{C}$ the trivial norm, by for $c \in \mathbb{C}$

$$|c| = \begin{cases} 1 & c \neq 0 \\ 0 & c = 0 \end{cases}$$

then Γ becomes a normed vector space over $\mathbb{C}$.

Definition 1.2. For $m \in \mathbb{N}^+$, define the *prime support* of m as

$$\operatorname{psupp}(m) = \{p \in \mathbb{P} \mid p|m\}$$

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

$$\mathrm{lp}(m) = \min \mathrm{psupp}(m)$$

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

$$\mathbb{N}^{|n|} = \{k \in \mathbb{N}^+ | \mathrm{lp}(k) = p_n\}$$

Definition 1.3. For any $n \in \mathbb{N}^+$ we let e_n be the characteristic function on $\{n\}$, i.e.

$$e_n(k) = \begin{cases} 1 & k = n \\ 0 & \text{otherwise} \end{cases}$$

It is clear that any $f \in \Gamma$ be be written as

$$f = \sum_{n=1}^{\infty} f(n) e_n \tag{1.4}$$

This sum is convergent with respect to the norm.

Definition 1.4. Let $f \in \Gamma$ be a non-unit. The *canonical decomposition* of f is the unique way of expressing f as a convergent sum

$$f = \sum_{i=1}^{\infty} f_i, \quad f_i = \sum_{k \in \mathbb{N}^{|i|}} f(k) e_k$$

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.

Definition 1.5. An arithmetic function f is *multiplicative* if $f(n)f(m) = f(mn)$ for $(m, n) = 1$

1.2 Regular convolutions

The term *regular convolution* was introduced by Narkiewicz in [1], 1963.

Definition 1.6. A convolution, $*_A$, is defined by

$$f *_A g(n) = \sum_{d \in A(n)} f(d) g(\frac{n}{d}) \tag{1.5}$$

where $A(n)$ is a set of divisors to the natural number n.

In [1] Narkiewicz states and proves the following propositions, which all have to apply if the convolution is regular.

Proposition 1.7. *The convolution $*_A$ is associative if and only if the following two conditions are equivalent:*

(a)

$$d \in A(m),\ m \in A(n)$$

(b)

$$d \in A(n),\ \frac{m}{d} \in A(\frac{n}{d})$$

Proposition 1.8. *The convolution $*_A$ is commutative if and only if $d \in A(n)$ implies that $\frac{n}{d} \in A(n)$.*

Proposition 1.9. *The convolution $*_A$ has a unit element if and only if for every n, $\{1, n\} \subset A(n)$.*

Definition 1.10. A convolution is *multiplicative* if from the multiplicativity of the factors follows the multiplicativity of the convolution product, i.e. if f and g are multiplicative, then so is $f * g$.

Proposition 1.11. *The convolution defined by (1.5) is multiplicative if and only if $A(mn) = A(m) \times A(n)$, for $(m, n) = 1$. (Here $B \times C$ denote the set of all integers which can be represented in the form bc, $b \in B, c \in C$)*

Definition 1.12. A convolution, $*_A$ is *regular* if the ring of arithmetic functions with ordinary addition and this convolution as multiplication is

- commutative
- associative
- has a unit element
- preserve multiplicativity
- the inverse function of $f(n) \equiv 1$ shall take only the values 0 and -1 for prime powers

The most well-known examples of regular convolutions is the Dirichlet convolution (where $A(n)$ is the set of all divisors of n) and the unitary convolution (where $A(n) = \{d|\ d|n \text{ and } (d, \frac{n}{d}) = 1\}$).

In [1] Narkiewicz also proves the following theorem

Theorem 1.13. *A convolution defined by (1.5) is regular if and only if there is a family $\{\pi_p | p \in \mathbb{P}\}$ of partitions of $\mathbb{N}^+$ into (finite or infinite) arithmetic progressions, such that*

$$p_1^{a_1} \cdots p_r^{a_r} \in A(p_1^{b_1} \cdots p_r^{b_r})$$

if and only if

$$(a_1, \ldots, a_r) \leq (b_1, \ldots, b_r)$$

and for all $1 \leq i \leq r$, either $a_i = 0$ or a_i and b_i belong to the same progression in the partition π_i.

The two extremal cases are the Dirichlet convolution, where all partitions have only one (infinite) block, and unitary convolution, where all blocks have size 1.

Definition 1.14. p^a is called a primitive prime power (with respect to the convolution) if a is the first number in some progression in π_p.

Proposition 1.15. *With $*$ as multiplication Γ becomes a normed $\mathbb{C}$-algebra.*

Proof Take $f, g \in \Gamma$. Let $\mathrm{ord}(f) = k$ and $\mathrm{ord}(g) = l$. Then $f = \sum_{n=k}^{\infty} f(n)e_n$ and $g = \sum_{n=l}^{\infty} g(n)e_n$, $f(k) \neq 0, G(l) \neq 0$. But then it is clear that

$$f *_A g = f(k)g(l)e_{kl} + \text{terms of higher order}$$

and hence $|f *_A g| = \frac{1}{kl} \leq \frac{1}{k}\frac{1}{l} = |f||g|$.

Chapter 2

Restrictions

Definition 2.1. For $V \subset \mathbb{N}^+$, we let $\Gamma[V]$ be the closed subvector space of Γ consisting of functions $f : \mathbb{N}^+ \to \mathbb{C}$ with support in V. Suppose that $1 \in V$. If A gives a regular convolution product $*_A$ on Γ, we use this to make $\Gamma_A[V]$ a topological algebra by

$$f * g(n) = \begin{cases} f *_A g(n) & \text{if } n \in V \\ 0 & \text{otherwise} \end{cases} \tag{2.1}$$

Theorem 2.2. *If*

$$V_1 \subset V_2 \subset V_3 \subset \cdots \subset W \subset \mathbb{N}^+, \quad \bigcup V_i = W$$

then there are natural continuous $\mathbb{C}$-linear epimorphisms

$$\Gamma[V_1] \leftarrow \Gamma[V_2] \leftarrow \Gamma[V_3] \leftarrow \cdots \leftarrow \Gamma[W] \leftarrow \Gamma, \tag{2.2}$$

and

$$\lim_{\leftarrow} \Gamma[V_i] \cong \Gamma[W] \tag{2.3}$$

Proof Use the notation in (1.4), i.e

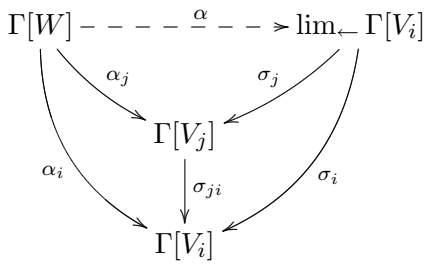
$$f = \sum_{n=1}^{\infty} f(n) e_n$$

The natural homomorphisms

$$\sigma_{ji} : \Gamma[V_j] \to \Gamma[V_i] \qquad i \leq j$$

maps $\sum_{n \in V_j} f(n) e_n$ to $\sum_{n \in V_i} f(n) e_n$. These are clearly epimorphisms.

Now we can draw the following diagram:



The elements in $\lim_{\leftarrow} \Gamma[V_i]$ are of the form $(f_1, f_2, f_3, \dots)$ with $f_i \in \Gamma[V_i]$ and $\sigma_{ji}(f_j) = f_i$. Define

$$\sigma_i : \lim_{\leftarrow} \Gamma[V_i] \to \Gamma[V_i]$$

σ_i maps $(f_0, f_1, f_2, \dots) \in \lim_{\leftarrow} \Gamma[V_i]$ to $f_i \in \Gamma[V_i]$. This gives that $\sigma_i = \sigma_{ji} \circ \sigma_j$ Define

$$\alpha_i : \Gamma[W] \to \Gamma[V_i]$$

like σ_{ji}, i.e. maps $f = \sum_{n=0}^{\infty} f(n)e_n$ to $\sum_{n \in V_i} f(n)e_n$. Then, if $i \leq j$, $\alpha_i = \sigma_{ji} \circ \alpha_j$.
This induces a homomorphism $\alpha : \Gamma[W] \to \lim_{\leftarrow} \Gamma[V_i]$ such that the diagram commutes. α maps $f_W \in \Gamma[W]$ to $f = (f_1, f_2, f_3, \dots) \in \lim_{\leftarrow} \Gamma[V_i]$. α is clearly injective, since the only function that maps to 0 is the 0-function. To show that α is also surjective, take $f \in \lim_{\leftarrow} \Gamma[V_i]$. $f = (f_1, f_2, f_3, \dots)$ with $f_i \in V_i$ and $\sigma_{ji}(f_j) = f_i$ $i < j$, We want to show that this $f \in \lim_{\leftarrow} \Gamma[V_i]$ corresponds to a unique $f_W \in \Gamma[W]$. Since $f_W \in \Gamma[W]$ is determined by it's values on W, take $w \in W$. Since $\cup V_j = W$ and $V_1 \subset V_2 \subset \dots$, $w \in V_j$ for j large enough. Take this j and define $f_W(w) = f_j(w)$. If $k > j$ then $f_k(w) = f_j(w)$ since $\sigma_{kj}(f_k) = f_j$. Hence f_W is well-defined. From this construction follows that $\alpha_i(f_W) = f_i$. Hence α is surjective.

Proposition 2.3. *Let $p \in \mathbb{P}$ and let $B_1, B_2 \in \pi_p$; let $B_i' = \{ p^j | j \in B_i \}$. Then the following hold:*

(a) $\Gamma[B_i'] \cong \mathbb{C}[[x]]$ *if B_i' is infinite, and* $\Gamma[B_i'] \cong \frac{\mathbb{C}[x]}{x^\ell}$ *if B_i' has ℓ elements.*

(b) *If $B_1 \neq B_2$ then $\Gamma[B_1' \cup B_2'] \cong \Gamma[B_1'] \times_{\mathbb{C}} \Gamma[B_2']$, where $R \times_{\mathbb{C}} S$ is the* fibre product *of the augmented $\mathbb{C}$-algebras R and S, i.e. the the pullback of the diagram $R \to \mathbb{C} \leftarrow S$.*

(c) $\Gamma[\{p^i | i \geq 0\}] \cong \lim_{\leftarrow}(\times_{\mathbb{C}} \Gamma[B_j'])$, *the inverse limit over n of the fibre products of the first n (which per definition is isomorphic to the infinite fiber product $\times_{\mathbb{C}(B_j \in \pi_p)}$)$\Gamma[B_j']$)*

Proof

(a) $B_i \in \pi_p$ means that $B_i = \{0, a, 2a, \dots\}$, or $B_i = \{0, a, 2a, \dots, ra\}$, for some a. Thus $p^j \in B_i'$ implies that $j = ka$ for some $k \in \mathbb{N}$. Another way of expressing the same thing would be to say that $p^j = (p^a)^k$ for some $k \in \mathbb{N}$. $\Gamma[B_i']$ is then the vector space with basis $\{e_{p^j} | j \in B_i\}$.
First let B_i be infinite. Define

$$\varphi : \Gamma[B_i'] \to \mathbb{C}[[x]]$$

$$e_{p^j} \mapsto x^{\frac{j}{a}}$$

This is a homomorphism since $j, l \in B_i$ and B_i infinite implies that $e_{p^j} * e_{p^m} = e_{p^{j+m}}$ and $\varphi(e_{p^{j+m}}) = x^{\frac{j+m}{a}} = x^{\frac{j}{a}} x^{\frac{m}{a}} = \varphi(e_{p^j})\varphi(e_{p^m})$. It is well defined, and since the only thing that maps to 0 is 0, it's injective. Since B_i is infinite for any $k \in \mathbb{N}$ there exists a $j \in B_i$ such that $j = ka$, i.e. for any x^k there exists a function e_{p^j} such that $\varphi(e_{p^j}) = x^{\frac{j}{a}} = x^k$. Thus φ is surjective, and hence an isomorphism. So in this case $\Gamma[B_i'] \cong \mathbb{C}[[x]]$.

Now let B_i' be finite with ℓ elements. Then $\Gamma[B_i']$ has a basis $\{e_1, e_{p^a}, e_{p^{2a}}, \dots, e_{p^{(\ell-1)a}}\}$. Now define the following homomorphism

$$\varphi : \Gamma[B_i'] \to \frac{\mathbb{C}[x]}{x^\ell}$$

$$e_{p^j} \mapsto x^{\frac{j}{a}}$$

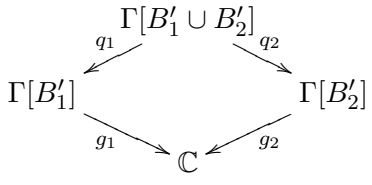
If $j, m \in B_i$, but $j + m \notin B_i$, i.e. $j + m \geq \ell a$, then $e_{p^j} * e_{p^m} = 0$, so in order to make φ well defined, $\varphi(e_{p^j})\varphi(e_{p^m}) = 0$. Assume $j+m = \ell a+n$. Since $\varphi(e_{p^j})\varphi(e_{p^m}) = x^{\frac{j}{a}} x^{\frac{m}{a}} = x^{\frac{j+m}{a}} = x^{\frac{\ell a+n}{a}} = x^\ell x^{\frac{n}{a}} = 0 \cdot x^{\frac{n}{a}} = 0$, φ is well defined and as above we get that $\Gamma[B_i'] \cong \frac{\mathbb{C}[x]}{x^\ell}$.

(b) Define

$$g_1 : \Gamma[B_1'] \to \mathbb{C}$$

$$f \mapsto f(1)$$

Define g_2 analogous. $g_1(e_{p^i} * e_{p^j}) = g_1(e_{p^{i+j}}) = e_{p^{i+j}}(1) = 0 = e_{p^i}(1)e_{p^j}(1)$ if $i + j \in B_1, i + j \neq 0$ and $g_1(e_{p^i} * e_{p^j}) = g_1(0) = 0$ if $i + j \notin B_1$. If $i + j = 0$ then $i = j = 0$ and $g_1(e_{p^0} * e_{p^0}) = g_1(e_1 * e_1) = g_1(e_1) = e_1(1) = 1 = 1 \cdot 1 = g_1(e_1)g_1(e_1)$. Thus g_1 and g_2 are well defined epimorphisms.
We can now draw the following commutative diagram:



q_1 and q_2 are defined in the natural way:

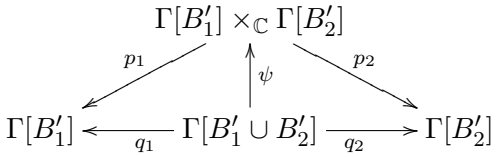
$$q_1(\sum_{n\in B_1'\cup B_2'} f(n)e_n) = \sum_{n\in B_1'} f(n)e_n$$

We have a homomorphism

$$p_1 : \Gamma[B_1'] \times_{\mathbb{C}} \Gamma[B_2'] \to \Gamma[B_1']$$

$$(f_1, f_2) \mapsto f_1$$

We also have a homomorphism p_2 defined analogous to p_1. This gives the induced homomorphism ψ in the following diagram:



ψ is defined in the following way:

$$\psi(\sum_{n\in B_1'\cup B_2'} f(n)e_n) = (\sum_{n\in B_1'} f(n)e_n, \sum_{n\in B_2'} f(n)e_n)$$

ψ is injective since $\psi(f) = (0,0)$ implies that f lacks support in both B_1' and B_2', and hence it lacks support in $B_1' \cup B_2'$. To show that ψ is surjective, take $(f_1, f_2) \in \Gamma[B_1'] \times_{\mathbb{C}} \Gamma[B_2']$. Since every $f \in \Gamma[B_1' \cup B_2']$ is uniquely determined by the values it takes on $B_1' \cup B_2'$, take $w \in B_1' \cup B_2'$. Then there are three possibilities, $w \in B_1'$, $w \in B_2'$ or $w = 1$. If $w \in B_1'$, let $f(w) = f_1(w)$, if $w \in B_2'$, let $f(w) = f_2(w)$, if $w = 1$ then, since the diagram commutes $f_1(1) = f_2(1)$ and to let $f(1) = f_1(1) = f_2(1)$ will therefore be well-defined. Hence this f exists and is unique, hence ψ is surjective.

$$\therefore \Gamma[B_1' \cup B_2'] \cong \Gamma[B_1'] \times_{\mathbb{C}} \Gamma[B_2']$$

(c) Define the following homomorphisms

$$\alpha_j : \Gamma[\{p^i | i \geq 0\}] \to \Gamma[B_1'] \times_{\mathbb{C}} \cdots \times_{\mathbb{C}} \Gamma[B_j']$$

α_j is defined in the same way as ψ. i.e. it maps e_{p^k} to the vector with e_{p^k}:s on positions $n_1, n_2, \ldots, n_m$ if e_{p^k} has support in $\Gamma[B'_{n_1}], \Gamma[B'_{n_2}], \ldots,$ $\Gamma[B'_{n_m}]$ and 0 on all other positions. α_j is clearly an epimorphism.

$$\sigma_j : \varprojlim(\times_{\mathbb{C}}\Gamma[B_j']) \to \Gamma[B_1'] \times_{\mathbb{C}} \cdots \times_{\mathbb{C}} \Gamma[B_j']$$

σ_j maps $(f_1, (f_k)_{k=1}^2, (f_k)_{k=1}^3, \dots)$ to $(f_k)_{k=1}^j$.

$$\sigma_{ji} : \Gamma[B_1'] \times_{\mathbb{C}} \cdots \times_{\mathbb{C}} \Gamma[B_j'] \to \Gamma[B_1'] \times_{\mathbb{C}} \cdots \times_{\mathbb{C}} \Gamma[B_i'], \quad i \leq j$$

σ_{ji} maps $(f_1, f_2, \dots, f_i, \dots, f_j)$ to $(f_1, f_2, \dots, f_i)$. These induce a homomorphism

$$\alpha : \Gamma[\{p^i | i \geq 0\}] \to \lim_{\leftarrow}(\times_{\mathbb{C}} \Gamma[B_j'])$$

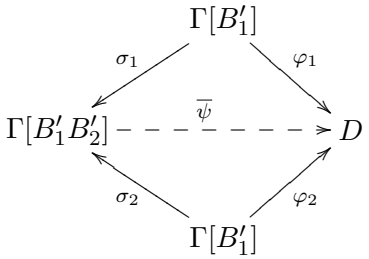
α takes an element $f' \in \Gamma[\{p^i | i \geq 0\}]$ to $(\alpha_1(f'), \alpha_2(f'), \dots)$. It's obvious that α is injective, and since all α_j:s are epimorphisms, α is also surjective.

$$\therefore \Gamma[\{p^i | i \geq 0\}] \cong \lim_{\leftarrow}(\times_{\mathbb{C}} \Gamma[B_j'])$$

Proposition 2.4. *Let $p, q \in \mathbb{P}, p \neq q$. Let $1 \in B_1' \subset \{p^i | i \geq 0\}$, $1 \in B_2' \subset \{q^i | i \geq 0\}$. Then*

$$\Gamma[B_1' B_2'] \cong \Gamma[B_1'] \widehat{\otimes}_{\mathbb{C}} \Gamma[B_2']$$

as $\mathbb{C}$-algebras, i.e. $\Gamma[B_1' B_2']$ solves the following universal problem,



where $\varphi_i : \Gamma[B_i'] \to D, i = 1, 2$ are bounded $\mathbb{C}$-algebra homomorphisms into a complete $\mathbb{C}$-algebra D and $\sigma_i : \Gamma[B_i'] \to \Gamma[B_1' B_2'], i = 1, 2$, are bounded $\mathbb{C}$-algebra homomorphisms.

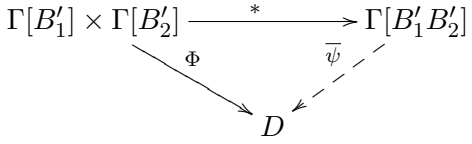
If both $\Gamma[B_1']$ and $\Gamma[B_2']$ are finite, the complete tensor product can be replaced by ordinary tensor product over $\mathbb{C}$.

Proof Define

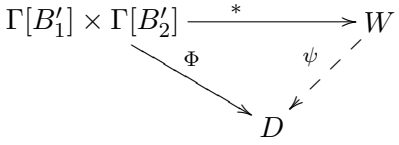
$$\sigma_i : \Gamma[B_i'] \to \Gamma[B_1' B_2'], \qquad \sum_{j \in B_i'} c_j e_j \mapsto \sum_{j \in B_i'} c_j e_j, \quad i = 1, 2$$

These are obviously bounded $\mathbb{C}$-algebra homomorphisms. $\Gamma[B_1' B_2']$ is obviously a complete $\mathbb{C}$-algebra. In order to verify the universal property for $\Gamma[B_1' B_2']$, let Φ denote the $\mathbb{C}$-bilinear map $\Phi : \Gamma[B_1'] \times \Gamma[B_2'] \to D, (f_1, f_2) \mapsto \varphi_1(f_1)\varphi_2(f_2)$, which is bounded by $|\varphi_1||\varphi_2|$. If one can prove that this induces a unique bounded $\mathbb{C}$-algebra homomorphism $\overline{\psi}$ such that the following

diagram commutes, then this $\overline{\psi}$ will also make the diagram in the proposition commutative.



$*$ denotes multiplication, i.e. the convolution. It must be verified that $*$ is bilinear and bounded. The bilinearity follows from the fact that $*$ is a regular convolution, and hence it's associative and distributive. That $*$ is bounded is verified by an easy calculation.
Now, let $W \subset \Gamma[B_1'B_2']$ be the set of all elements on the form $\sum_{i=0}^{M}\sum_{j=0}^{N} c_{ij}e_{p^iq^j} \in \Gamma[B_1'B_2']$ where M, N are finite. Then we have the following diagram



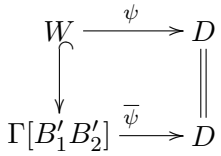
Then it is clear that $\psi(f), f \in W$ is determined by the values of ψ of the $e_{p^iq^j}$'s. We have that

$$\Phi(e_{p^i}, e_{p^j}) = \varphi_1(e_{p^i})\varphi_2(e_{p^j})$$

and since the diagram has to be commutative we have that

$$\psi(e_{p^iq^j}) = \varphi_1(e_{p^i})\varphi_2(e_{p^j})$$

But since $\overline{W} = \Gamma[B_1'B_2']$ we can apply proposition 6 from chapter 1.1.7 in [2] which say that there exist a unique $\overline{\psi}$ such that this diagram commutes



Hence $\Gamma[B_1'B_2']$ solves the universal problem and hence

$$\Gamma[B_1'B_2'] \cong \Gamma[B_1']\widehat{\otimes}_{\mathbb{C}}\Gamma[B_2']$$

If $\Gamma[B_1']$ and $\Gamma[B_2']$ are finite just skip the last step in the proof and it is clear that $\Gamma[B_1'B_2'] \cong \Gamma[B_1'] \otimes_{\mathbb{C}} \Gamma[B_2']$.

Proposition 2.5. *Let* $\Gamma_i = \Gamma[\{p_i^j | j \geq 0\}]$. *Then*

$$\Gamma \cong \varprojlim_{n \to \infty} \Gamma_1\widehat{\otimes}_{\mathbb{C}} \ldots \widehat{\otimes}_{\mathbb{C}}\Gamma_n$$

Proof Let $\Gamma_{1\ldots k} = \Gamma[\{p_1^{j_1}, \ldots p_k^{j_k}\}]$. Then by putting $B_i' = \{p_i^j | j \geq 0\}$ and use induction on proposition 2.4 we get that $\Gamma_{1\ldots k} \cong \Gamma_1\widehat{\otimes}_{\mathbb{C}} \ldots \widehat{\otimes}_{\mathbb{C}}\Gamma_k$. But now we can apply theorem 2.2 which gives the result.

Chapter 3

Incidence algebras

Assume that A gives a regular convolution, and that $W \subset \mathbb{N}^+$ contains 1. Define a partial order $\leq = \leq_A$ on W by $m \leq_A n$ iff $m \in A(n)$. Then $W = (W, \leq_A)$ is a locally finite poset, so we can define its *incidence algebra* $I(W)$, which consists of all $\mathbb{C}$-valued functions on closed intervals in W, with pointwise addition and multiplication of scalars, and with the convolution product

$$f * g([a,b]) = \sum_{a \leq c \leq b} f([a,c])g([c,b]) \tag{3.1}$$

It is given the topology of pointwise convergence.

The *reduced incidence algebra* $\mathrm{Red}(W)$ of W consists of the subalgebra of functions which take the same value on equivalent intervals, where $[a,b]$ and $[c,d]$ are considered equivalent if $b/a = d/c$.

Theorem 3.1. *As a topological* $\mathbb{C}$*-algebra,* $\mathrm{Red}(W)$ *is isomorphic to* $\Gamma[W]$.

Proof

$$\mathrm{Red}(W) = \{f \in I(W, \mathbb{C}) | f(x_1, y_1) = f(x_2, y_2) \text{ if } \frac{y_1}{x_1} = \frac{y_2}{x_2}\}$$

Then $\mathrm{Red}(W)$ is the reduced incidence algebra of W over $\mathbb{C}$. The mapping $\varphi : \mathrm{Red}(W) \to \Gamma[W]$ such that

$$f \mapsto \sum_{n=1}^{\infty} f(1,n)e_n$$

is a bijection. Then, if $f, g \in \mathrm{Red}(W)$

$$(f \cdot g)(1,n) = \sum_{d \in A(n)} f(1,d)g(d,n) = \sum_{d \in A(n)} f(1,d)g(1,\frac{n}{d})$$

and if

$$\Big(\sum_{n=1}^{\infty} a_n e_n\Big) * \Big(\sum_{n=1}^{\infty} b_n e_n\Big) = \sum_{n=1}^{\infty} c_n e_n$$

then

$$c_n e_n = \sum_{d \in A_n} a_d e_d * b_{\frac{n}{d}} e_{\frac{n}{d}} = \sum_{d \in A_n} a_d b_{\frac{n}{d}} e_n$$

which implies $c_n = \sum_{d \in A_n} a_n b_{\frac{n}{d}}$. This shows that multiplication in $\mathrm{Red}(W)$ corresponds to multiplication in $\Gamma[W]$. It follows that $\mathrm{Red}(W)$ is isomorphic to $\Gamma[W]$.

Definition 3.2. $\oplus$ is an operation on posets defined as follows. $P \oplus Q$ has $P \cup Q$ as a subset. $u \leq v$ iff either

- $u, v \in P$ and $u \leq v$ in P, or
- $u, v \in Q$ and $u \leq v$ in Q, or
- $u \in P, v \in Q$.

Definition 3.3. A subset B of a partially ordered set is a *chain* if for any $u, v \in B$, either $u \leq v$ or $v \leq u$.

Definition 3.4. A *wedge of chains* is a set of chains $\{C_i |\ i \in I\}$ with an element w such that $w \leq u$ for all $u \in C_i$.

We give a counterpart to Proposition 2.3:

Proposition 3.5. *Let $p \in \mathbb{P}$ and let $B_1, B_2 \in \pi_p$; let $B_i' = \left\{ p^j \middle| j \in B_i \right\}$. Partially order B_i' and $B_1' \cup B_2'$ as above. Let $\mathbb{N}$ denote the natural numbers with their natural order, and $[n]$ the induced subposet on $\{1, 2, \ldots, n\}$. Then the following hold:*

(a) *$B_i' \cong \mathbb{N}$ if B_i' is infinite, and $\cong [\ell]$ if B_i' has ℓ elements.*

(b) *If $B_1' \neq B_2'$ then*

$$B_1' \cup B_2' \cong [1] \oplus \left[(B_1' \setminus \{1\}) + (B_2' \setminus \{1\}) \right]$$

i.e. the Hasse diagram of $B_1' \cup B_2'$ is obtained by placing the diagrams of B_1' and B_2' next to each other, then identifying the two elements corresponding to 1.

(c) *$\left\{ p^i \middle| i \geq 0 \right\}$ is a wedge of chains, one for each block $B_i \in \pi_p$, joined together with the element 1 as the minimum.*

(d) *There is at most one infinite chain, and if there is an infinite chain, there is a common bound of the lengths of the other chains.*

Proof

(a) Let B_i' be infinite. Since $B_i \in \pi_p$, $B_i' = \{1, p^a, p^{2a}, \dots\}$. Define

$$\varphi : B_i' \to \mathbb{N}$$

$$p^{ra} \mapsto r + 1$$

This is obviously a poset isomorphism.

Let B_i' be finite. Now $B_i' = \{1, p^a, \dots, p^{(\ell-1)a}\}$. Define

$$\varphi : B_i' \to [\ell]$$

$$p^{ra} \mapsto r + 1$$

Also an obvious poset isomorphism.

(b) $[1] \oplus (B_1' \setminus \{1\} + B_2' \setminus \{1\})$ is the poset with subset $B_1' \cup B_2'$, and $u \leq v$ iff either

- $u = 1$, or
- $u, v \in B_1'$ and $u \leq v$,
- $u, v \in B_2'$ and $u \leq v$.

Define

$$\psi : B_1' \cup B_2' \to [1] \oplus [(B_1' \setminus \{1\}) + (B_2' \setminus \{1\})]$$

$$B_1 \cup B_2 \ni p^{ra} \mapsto p^{ra} \in [1] \oplus [(B_1' \setminus \{1\}) + (B_2' \setminus \{1\})]$$

It is obvious from the above that the inverse of this bijective homomorphism preserves the order. Hence it's an poset isomorphism.

(c) Follows from theorem 2 in [1].

(d) Assume that the diagram has two infinite chains, B_1' and B_2'. Then

$$B_1 = \{0, a, 2a, \dots\}$$

$$B_2 = \{0, b, 2b, \dots\}$$

But since $ba = ab$ and $ba \in B_1$, $ab \in B_2$ we have a contradiction.

Assume that the diagram has one infinite chain, say B_1'. Let $B_1 = \{0, a, 2a, \dots\}$. Then the common bound of length of the other chains have to be a because if a chain, B_i', has length $a + 1$ then $B_i = \{0, b, 2b, \dots, ab\}$ and then it would intersect B_1.

Proposition 3.6. *If all chains in a Hasse diagram of posets $\{p^i | i \geq 0\}$ have the same length, then the length have to be 2, 3 or the diagram will be composed of only one infinite chain.*

Proof We already know the existence of a convolution with all chains of length 2, namely the unitary convolution. Therefore this proof considers only wedges with chains of length > 2.
The case with only one infinite chain is the well-known Dirichlet convolution so the rest of the proof only deals with finite chains.
Let all chains be of length $r > 2$. Then the chains is constructed as follows

$$\begin{aligned}
&\{0, 1, 2, \ldots, r-1\} \\
&\{0, r, 2r, \ldots, (r-1)r\} \\
&\{0, r+1, 2(r+1), \ldots, (r-1)(r+1)\} \\
&\ldots \\
&\{0, s, 2s, \ldots, rs\} \\
&\ldots
\end{aligned}$$

where s is the first number not in any previous chain.
Assume r is even, then $r > 3$, so there exists chains with r and $r+2$ as first non-zero element. r and $r+2$ is even and hence we can factor out 2 and their least common multiple will be $\frac{r(r+2)}{2}$. But since both $\frac{r}{2}$ and $\frac{r+2}{2} = \frac{r}{2} + 1$ is $\leq r-1$ the least common multiple will be in both chains and hence the only wedge of chains where all chains are of the same even length is the unitary case.

Now assume $r \neq 3$ is odd. Consider $r+1$ and $r+3$. There exists chains with $r+1$ and $r+3$ as first non-zero element. The least common multiple of $r+1$ and $r+3$ is $\frac{(r+1)(r+3)}{2}$. Since both $\frac{r+1}{2}$ and $\frac{r+3}{2}$ is $\leq r-1$ the least common multiple will be in both chains and hence there exist no diagram with all chains of ha same odd length > 3.

When $r = 3$ the chains will be:

$$\begin{aligned}
&\{0, 1, 2\} \\
&\{0, 3, 6\} \\
&\{0, 4, 8\} \\
&\{0, 5, 10\} \\
&\{0, 9, 18\} \\
&\ldots
\end{aligned}$$

It is clear that this chains will never intersect, because if we continue to take the next number not in any previous chain, say s, then $2s$ will clearly not be in any previous chain. Because of the fundamental theorem of arithmetic $2s \neq 2t$ if $s \neq t$.

Proposition 3.7. *All diagrams, except for the one with just one chain of infinite length (i.e. the Dirichlet convolution), must contain infinitely many chains of length* 2 *or* 3.

Proof Assume that the diagram does not contain any chains of length 2 or 3. Let the chain containing 1 have length r. r is finite, since otherwise we

Figure 3.1: Posets of Dirirchlet, unitary and ternary convolution, restricted to a powers of a single prime

have the Dirichlet case and moreover $r \geq 4$, since the diagram doesn't have chains of length 2 or 3. Then we will have the chains

$$\begin{aligned}
&\{0, 1, \ldots, r-1\} \\
&\{0, r, \ldots, sr\} \\
&\{0, r+1, \ldots, t(r+1)\} \\
&\{0, r+2, \ldots, u(r+2)\} \\
&\{0, r+3, \ldots, v(r+3)\} \\
&\ldots
\end{aligned}$$

with $s, t, u, v \geq 3$. But then it follows from the proof of proposition 3.6 that two chains have some element in common, which is a contradiction. In the same way we can assume that there is only finitely many chains of length 2 and 3. Then there exist a number, r, such that $\{0, r, 2r\}$ is the last chain of length 3 and there exist a number s such that $\{0, s\}$ is the last chain of length 2. Take the largest number of r and s. Now we can apply the same argument as above and get a contradiction.

Proposition 3.8. *Let $p, q \in \mathbb{P}$, $p \neq q$. Let $1 \in B_1 \subset \left\{ p^i \middle| i \geq 0 \right\}$, $1 \in B_2 \subset \left\{ q^i \middle| i \geq 0 \right\}$. Then*

$$B_1 B_2 \cong B_1 \times B_2,$$

where the $\times$ denotes the Cartesian product of the posets B_1 and B_2.

Proof The order in $B_1 B_2$ is defined as usual, i.e. $p^a q^b \geq p^r q^s$ iff $p^a \geq p^r$ and $q^b \geq q^s$. The same order is used in $B_1 \times B_2$, i.e. $(p^a, q^b) \geq (p^r, q^s)$ iff $p^a \geq p^r$ and $q^b \geq q^s$. Define

$$\varphi : B_1 B_2 \to B_1 \times B_2$$

$$p^r q^s \mapsto (p^r, q^s)$$

Since $\varphi(p^a) = (p^a, 1)$, φ is a homomorphism since multiplication in $B_1 \times B_2$ is componentwise multiplication. This makes φ a bijection. We can also define the inverse to φ

$$\varphi^{-1}((p^r, q^s)) = p^r q^s$$

The inverse is well-defined and $(p^r, q^s) \leq (p^n, q^m)$ implies that $\varphi((p^r, q^s)) = p^r q^s \leq p^n q^m = \varphi((p^n, q^m))$ according to the definition of order above. Hence φ is an order preserving bijection whose inverse is order preserving and hence it's a poset isomorphism.

$$\therefore B_1 B_2 \cong B_1 \times B_2$$

Proposition 3.9. *The poset $(\mathbb{N}^+, \leq_A)$ is isomorphic to the infinite direct product of the posets $(\left\{ p_i^j \middle| j \geq 0 \right\}, \leq_A)$. Then $(\mathbb{N}^+, \leq_A)$ is isomorphic to S. If $n \in \mathbb{N}^+$, then the interval $[1, n]$ is isomorphic to a product of finitely many finite chains.*

Proof Let $n \in \mathbb{N}^+$ have the prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ Define

$$\varphi : (\mathbb{N}^+, \leq_A) \to (\{p_1^j | j \geq 0\} \times \{p_2^j | j \geq 0\} \times \ldots, \leq_A)$$

φ map n to the vector with $p_i^{a_i}$ on the i:th places and 0 on all others. This is clearly a bijection. The inverse of φ then exists and

$$(p_1^{a_1}, p_2^{a_2}, \ldots) \geq (p_1^{b_1}, p_2^{b_2}, \ldots)$$

implies $a_i \geq b_i$ for all $i \in \mathbb{N}$. Hence

$$\varphi^{-1}((p_1^{a_1}, p_2^{a_2}, \ldots)) = p_1^{a_1} p_2^{a_2} \cdots \geq p_1^{b_1} p_2^{b_2} \cdots = \varphi^{-1}((p_1^{b_1}, p_2^{b_2}, \ldots))$$

Hence φ is a poset isomorphism and $(\mathbb{N}^+, \leq_A) \cong (\{p_1^j | j \geq 0\} \times \{p_2^j | j \geq 0\} \times \ldots, \leq_A)$

If $1 \leq n \in \mathbb{N}$ then either n is prime or there exists a largest prime number $p_k \leq n$. For each prime p_i there exists a unique number $l_i \in \mathbb{N}$ such that $p_i^{l_i}$ is the largest power of p_i less then or equal to n. Then as above we can define a mapping

$$\varphi : ([1, n], \leq_A) \to (\{p_1^j | 0 \leq j \leq l_1\} \times \cdots \times \{p_k^j | 0 \leq j \leq l_k\}, \leq_A)$$

This mapping is a poset isomorphism according to the above. The number of chains is clearly finite and all $\{p_i^j | 0 \leq j \leq l_i\}$ are clearly finite chains.

Let $1 \in W \subset \mathbb{N}^+$. We define the *zeta function* of $\Gamma[W]$ to be $\zeta = \sum_{n \in W} e_n \in \Gamma[W]$, and let the *Möbius function* be its multiplicative inverse $\mu = \zeta^{-1}$.

Theorem 3.10. *$\mu(p_1^{a_1} \cdots p_r^{a_r})$ is $(-1)^r$ if all $p_i^{a_i}$ are primitive, 0 otherwise.*

Proof Let p^a be primitive. Then

$$\mu * \zeta(p^a) = \sum_{d \in A(p^a)} \mu(d)\zeta(\frac{p^a}{d}) = \sum_{d \in A(p^a)} \mu(d) = \mu(1) + \mu(p^a) = 1 + \mu(p^a) = 0$$

which implies that $\mu(p^a) = -1$ if p^a is primitive. Then, if $p^a | p^{2a}$,

$$\mu * \zeta(p^{2a}) = \sum_{d \in A(p^{2a})} \mu(d) = \mu(1) + \mu(p^a) + \mu(p^{2a}) = 1 - 1 + \mu(p^{2a}) = 0$$

It follows by induction that $\mu(p^b) = 0$ if p^b non-primitive.

Let $n = p_1^{a_1} p_2^{a_2}$ where both $p_1^{a_1}$ and $p_2^{a_2}$ are primitive. Then

$$\sum_{d \in A(n)} \mu(d) = \mu(1) + \mu(p_1^{a_1}) + \mu(p_2^{a_2}) + \mu(p_1^{a_1} p_2^{a_2}) =$$

$$= 1 - 1 - 1 + \mu(p_1^{a_1} p_2^{a_2}) = 0$$

Hence $\mu(p_1^{a_1} p_2^{a_2}) = 1 = (-1)^2$. Assume that $\mu(p_1^{a_1} \cdots p_{r-1}^{a_{r-1}}) = (-1)^{r-1}$ if all $p_i^{a_i}$ are primitive. Let $n = p_1^{a_i} \cdots p_r^{a_r}$ where all $p_i^{a_i}$ are primitive. Then

$$\sum_{d \in A(n)} \mu(d) = \sum_{i=1}^{r-1} \binom{r}{i} (-1)^i + \mu(p_1^{a_1} \cdots p_r^{a_r}) = 0$$

Hence $\mu(p_1^{a_i} \cdots p_r^{a_r}) = (-1)^r$ if all $p_i^{a_i}$ are primitive.

Let $n = p_1^{2b} p_2^a$ where p_1^{2b} is non-primitive and p_2^a, p_1^b is primitive. Then

$$\sum_{d \in A(n)} \mu(d) = \mu(1) + \mu(p_2^a) + \mu(p_1^b) + \mu(p_1^{2b}) + \mu(p_1^b p_2^a) + \mu(p_1^{2b} p_2^a) =$$

$$= 1 - 1 - 1 + 0 + 1 + \mu(p_1^{2b} p_2^a) = 0$$

which implies that $\mu(p_1^{2b} p_2^a) = 0$. Induction over the number of factors gives that $\mu(p_1^{a_i} \cdots p_r^{a_r}) = 0$ if one of the $p_i^{a_i}$s is non-primitive. Moreover induction over the number of non-primitive factors then shows that $\mu(p_1^{a_i} \cdots p_r^{a_r}) = 0$ if some of the $p_i^{a_i}$s are non-primitive.

Chapter 4

Ternary convolution

In proposition 3.6 we concluded that the unitary convolution and the Dirichlet convolution both have the property that a Hasse digram of posets $\{p^i | i \geq 0\}$ has the property that all wedges of chains had the same length. The proposition said that there were only one more convolution with this property. We call this convolution *ternary convolution*. Since both Dirichlet convolution and unitary convolution is well-known it might be interesting to look into this ternary convolution and see what can be said about it. The ring of arithmetic functions with ternary convolution is obviously isomorphic to the complete tensor product of countably many copies of $\frac{\mathbb{C}[x]}{(x^3)}$.

Proposition 4.1. *A prime power p^a is primitive if either a is odd or $a = 2^\alpha b$ where b is odd and α is even.*

Proof Ternary convolution is determined by the progressions $\{0, 1, 2\}$, $\{0, 3, 6\}, \{0, 4, 8\}, \ldots, \{0, s, 2s\}, \ldots$, where s is the next number not in any previous chain. The primitive prime powers are p^n where n is the first non-zero element in some chain. The third element in every chain is divisible by 2, hence all p^a with a odd are primitive. Hence if $a = 2b$ with b odd, then p^a is non-primitive. This gives that $p^{2^2 b}$ must be primitive, since $2^2 b$ can't be the third number in any chain (because if it were the third number then $2b$ would be primitive). Continuation in this way gives the result.

Corollary 4.2. *The proportion of a such that p^a is primitive in the interval $[1, l]$ is near $\frac{2}{3}$ for large l.*

Proof In a large interval near $\frac{1}{2}$ of the numbers are odd. It is also clear that near $\frac{1}{4}$ is divisible by 4. This discussion leads to the following formulae

$$\frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \frac{1}{16} - \frac{1}{32} + \cdots = \frac{1}{2} + \sum_{n=2}^{\infty} \big(-\frac{1}{2}\big)^k$$

Since when we add all numbers divisible by 4, we also get those divisible by 8, which don't give primitive powers of a prime, so therefore we have to subtract these, and so on. Developing the sum above gives that the number of a such that p^a is primitive is $\frac{2}{3}$ in an interval large enough.

In [3] Schinzel formulate a formulae for the inverse function to an invertible function f under unitary convolution. Here we do the same thing for the ternary convolution. The formulae we give actually works for every regular convolution, the tricky part is just to factor n into primitive elements. In proposition 4.3 we show that this can be done under the ternary convolution, but it is easy to realize that n can be factored into primitive elements in a unique way with respect to any regular convolution.

Proposition 4.3. *Any number $n \in \mathbb{N}$ has a unique factorization into primitive elements.*

Proof Every $n \in \mathbb{N}$ has a unique prime factorization, $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Then if $p_i^{a_i}$ is non-primitive one can write $p_i^{a_i} = p_i^{\frac{a_i}{2}} p_i^{\frac{a_i}{2}}$ where $p_i^{\frac{a_i}{2}}$ must be primitive. Hence it follows that n can be written as a product of primitive elements in a unique way.

Definition 4.4. For a number $n \in \mathbb{N}$ let $\upsilon(n)$ be the number of primitive prime powers counted with multiplicity in the factorization of n.

Proposition 4.5. *If $f(1) = 1$ the inverse function of f exists and is given by the formulae*

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

$$f^{-1}(n) = \sum_{k=1}^{\upsilon(n)} (-1)^k \sum_{\substack{d_1 \cdots d_k = n \\ d_i \in A(n),\, d_i > 1}} \prod_{i=1}^{k} f(d_i) \qquad \text{for } n > 1$$

Proof The formulae is obviously true for $n = 1$, thus let $n > 1$. Then we have

$$f * f^{-1}(n) = \sum_{d \in A(n)} f(d) f^{-1}(\frac{n}{d}) = f^{-1}(n) + \sum_{\substack{d \in A(n) \\ 1 < d < n}} f(d) f^{-1}(\frac{n}{d}) + f(n) =$$

$$= \sum_{k=1}^{\upsilon(n)} (-1)^k \sum_{\substack{d_1 \cdots d_k = n \\ d_i \in A(n),\, d_i > 1}} \prod_{i=1}^{k} f(d_i) +$$

$$\sum_{\substack{d \in A(n) \\ 1 < d < n}} f(d) \sum_{k=1}^{\upsilon(\frac{n}{d})} (-1)^k \sum_{\substack{d_1 \cdots d_k = \frac{n}{d} \\ d_i \in A(\frac{n}{d}),\, d_i > 1}} \prod_{i=1}^{k} f(d_i) + f(n) = 0$$

since

$$\sum_{\substack{d \in A(n) \\ 1 < d < n}} f(d) \sum_{k=1}^{v(\frac{n}{d})} (-1)^k \sum_{\substack{d_1 \cdots d_k = \frac{n}{d} \\ d_i \in A(\frac{n}{d}),\, d_i > 1}} \prod_{i=1}^{k} f(d_i) + f(n) = -\sum_{k=1}^{v(n)} (-1)^k \sum_{\substack{d_1 \cdots d_k = n \\ d_i \in A(n),\, d_i > 1}} \prod_{i=1}^{k} f(d_i)$$

One of the questions that we hoped to be able to answer about this ring was what are the nilpotent elements and the zero divisors in the ring. This work isn't finished yet, but a result on the way is proposition 4.9. To get there we need a few lemmas.

Lemma 4.6. *1. If p^a is primitive, then $e_{p^a} * e_{p^a} = e_{p^{2a}}$*

2. If p^a is non-primitive, then $e_{p^a} * e_{p^a} = 0$

3. If $a \neq b$, then $e_{p^a} * e_{p^b} = 0$

Proof

1.
$$e_{p^a} * e_{p^a}(p^{2a}) = \sum_{\substack{d_1 d_2 = p^{2a} \\ d_i \in A(p^{2a})}} e_{p^a}(d_1) e_{p^a}(d_2) =$$

$$= e_{p^a}(p^{2a}) e_{p^a}(1) + e_{p^a}(p^a) e_{p^a}(p^a) + e_{p^a}(1) e_{p^a}(p^{2a}) = 0 + 1 + 0 = 1$$

2.
$$e_{p^a} * e_{p^a}(p^{2a}) = \sum_{\substack{d_1 d_2 = p^{2a} \\ d_i \in A(p^{2a})}} e_{p^a}(d_1) e_{p^a}(d_2) =$$

$$= e_{p^a}(p^{2a}) e_{p^a}(1) + e_{p^a}(1) e_{p^a}(p^{2a}) = 0$$

3. If $a \neq b$ then p^{ab} is either primitive or non-primitive. If p^{ab} is primitive, then
$$e_{p^a} * e_{p^b}(p^{ab}) = \sum_{\substack{d_1 d_2 = p^{ab} \\ d_i \in A(p^{ab})}} e_{p^a}(d_1) e_{p^b}(d_2) =$$

$$= e_{p^a}(p^{ab}) e_{p^b}(1) + e_{p^a}(1) e_{p^b}(p^{ab}) = 0$$

it follows from the calculations above that $e_{p^a} * e_{p^b} = 0$. If p^{ab} is non-primitive then $p^{ab} = (p^{\frac{ab}{2}})^2$ where $p^{\frac{ab}{2}}$ is primitive. Hence

$$e_{p^a} * e_{p^b}(p^{ab}) = e_{p^a}(p^{ab}) e_{p^{2a}}(1) + e_{p^a}(p^{\frac{ab}{2}}) e_{p^{2a}}(p^{\frac{ab}{2}}) + e_{p^a}(1) e_{p^{2a}}(p^{\frac{ab}{2}}) = 0$$

Lemma 4.7. *If $n = p_1^{a_1} \cdots p_k^{a_k}$ were all p_i are distinct primes, then*

$$e_n = e_{p_1^{a_1}} * \cdots * e_{p_k^{a_k}}$$

Proof One can factor $p_1^{a_1}\cdots p_k^{a_k}$ into it's primitive parts, so $p_1^{a_1}\cdots p_k^{a_k} = q_1^{b_1}\cdots q_l^{b_l}$. If $p_i^{a_i}$ is non-primitive, then $e_{p_i^{a_i}} = e_{p_i^{\frac{a_i}{2}}} * e_{p_i^{\frac{a_i}{2}}}$ since

$$e_{p_i^{\frac{a_i}{2}}} * e_{p_i^{\frac{a_i}{2}}}(p_i^{a_i}) = \sum_{d\in A(p_i^{a_i})} e_{p_i^{\frac{a_i}{2}}}(d) e_{p_i^{\frac{a_i}{2}}}(\frac{n}{d}) = 1$$

Hence

$$e_{p_1^{a_1}} * \cdots * e_{p_k^{a_k}}(n) = e_{q_1^{b_1}} * \cdots * e_{q_l^{b_l}}(n) = \sum_{d_1\cdots d_l = n} e_{q_1^{b_1}}(d_1)\cdots e_{q_l^{b_l}}(d_l) = 1$$

Lemma 4.8. *Let $n = p_1^{a_1}\cdots p_k^{a_k}$ and $m = q_1^{b_1}\cdots q_l^{b_l}$, where p_i and q_i are primes. Then*

$$e_m * e_n = \begin{cases} 0 & \text{if for some } i,j, p_i = q_j \text{ and } a_i \neq b_j \text{ or } p_i^{a_i} \text{ non-primitive} \\ e_{mn} & \text{otherwise} \end{cases}$$

Proof This follows directly from Lemma 4.7, the commutativity of the ring and the properties of the regular three convolution, since if $p_i = q_j$ and $a_i \neq b_j$ for some i, j, then clearly

$$e_n * e_m = \cdots * e_{p_i^{a_i}} * \cdots * e_{p_i^{b_j}} * \cdots = \cdots * 0 * \cdots = 0$$

On the other had if $a_i = b_i$ but $p_i^{a_i}$ non-primitive, then

$$e_n * e_m = \cdots * e_{p_i^{a_i}} * \cdots * e_{p_i^{a_i}} * \cdots = \cdots * 0 * \cdots = 0$$

Proposition 4.9. *In the ring with three-convolution, all elements of polynomial type are nilpotent.*

Proof Lemma 4.8 gives that $(e_n)^3 = 0$ for all n. Hence, since $k \in \mathbb{N}^{|i|}$ implies that $p_i|k$ and Lemma 4.6 then gives

$$(f_i)^3 = \left(\sum_{k\in\mathbb{N}^{|i|}} f(k)e_k\right)^3 = 0$$

If an element is of polynomial type then $f = \sum_{i=1}^{\infty} f_i$ with all but finitely many of the f_i's are zero. So, because of the above and the pigeonhole principle,

$$f^{(2N+1)} = \left(\sum_{i=1}^{N} f_i\right)^{2N+1} = 0$$

Hence all elements of polynomial type are nilpotent.

Corollary 4.10. *All elements of polynomial type are zero divisors in the ring with ternary convolution.*

Proof Let f be of polynomial type. Proposition 4.9 gives that $f^m = 0$ for some $m > 1$. Hence $f * f^{m-1} = f^{m-1} * f = 0$ and hence f i s a zero divisor.

Question 4.11. *Are all zero divisors of polynomial type?*

Chapter 5

Restrictions to square-free integers

If W consists of the square-free integers, then the ring $\Gamma[W]$ is isomorphic to the completion of the group ring to the direct sum of countably many $\mathbb{Z}/2\mathbb{Z}$. An alternative description would be to view the ring as the completion of the free vector space on finite subsets of $\mathbb{N}$ with the multiplication

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

Theorem 5.1. *Let W consist of the square-free integers. Then there is only one regular convolution on $\Gamma[W]$.*

Proof If $p \in \mathbb{P}$ then, by Proposition 1.9, $A(p) = \{1, p\}$. By Proposition 1.11, if $p, q \in \mathbb{P}$ then $A(pq) = \{1, p, q, pq\}$. Induction gives that if n is square-free, then $A(n) = \{1, p \in \mathbb{P} \text{ such that } p|n;\ p, q \in \mathbb{P} \text{ such that } pq|n;\ \ldots;\ n\}$. Hence Definition 2.1 implies that any convolution on $\Gamma[W]$ is defined as

$$e_m * e_n = \begin{cases} e_{mn} & \text{if } mn \text{ square-free} \\ 0 & \text{otherwise} \end{cases}$$

But this is a unique definition and hence there exist only one regular convolution on $\Gamma[W]$. mn squarefree implies that there exist no $p \in \mathbb{P}$ such that $p|m$ and $p|n$, i.e. $(m, n) = 1$.

Corollary 5.2. *The convolution on $\Gamma[W]$ can be viewed as the unitary convolution on the square-free integers.*

This means that the ring $\Gamma[W]$ share many properties with the ring Γ with unitary convolution. For example all elements of polynomial type are nilpotent.

Conjecture 5.3. *All zero divisors and nilpotent elements in $\Gamma[W]$ are of polynomial type.*

Chapter 6

Restrictions to $[n]$

Let A be some regular convolution, and let $W \subset \mathbb{N}^+$ be a finite subset closed under taking A-divisors. We will be mostly interseted in the case $W = [n] = \{1, 2, \ldots, n\}$.

The ring $\Gamma[W]$ is a monomial ring, i.e. a quotient of a polynomial ring (on finitely many variables) with a monomial ideal.

Henceforth we assume A fixed and suppress it from notations. Let $\mathbb{PP}[W]$ be the primitive prime powers in W.

Theorem 6.1. $\Gamma[W] = \frac{\mathbb{C}[\{ e_q | q \in \mathbb{PP}[W] \}]}{I_W + J_W}$, *where* I_W, J_W *are monomial ideals, and where* $I_W = I \cap \{ e_q | q \in \mathbb{PP}[W] \}$, *where* I *is the defining ideal of* $\Gamma = \frac{\mathbb{C}[[e_q]]}{I}$.

Proof It is clear that $\frac{\mathbb{C}[\{e_q | q \in \mathbb{PP}[W]\}]}{I_W}$ is a subvector space of $\frac{\mathbb{C}[[e_q]]}{I}$. Define

$$\varphi : \frac{\mathbb{C}[\{e_q | q \in \mathbb{PP}[W]\}]}{I_W} \to \Gamma[W]$$

such that

$$\varphi(e_n) = \begin{cases} e_n & \text{if } e_n \in \Gamma[W] \\ 0 & \text{otherwise} \end{cases}$$

This is a homomorphism, since if $e_m, e_n \in \Gamma[W], e_{mn} \notin \Gamma[W]$ then $0 = \varphi(e_{mn}) = \varphi(e_m) * \varphi(e_n) = e_m * e_n = 0$. $\mathrm{Ker}(\varphi)$ is clearly a monomial ideal. Then $J_W = \mathrm{Ker}(\varphi)$ so

$$\Gamma[W] = \frac{\mathbb{C}[\{e_q | q \in \mathbb{PP}[W]\}]}{I_W + J_W}$$

Equivalently, W is identified with $\{ e_w | w \in W \}$ and is regarded as a multicomplex on $\mathbb{PP}[W]$, and $\Gamma[W]$ as the multicomplex ring on W.

Definition 6.2. A *facet* of W is an element which is maximal w.r.t $\leq_A$.

Definition 6.3. The *socle* of a homogeneous quotient $R = \mathbb{C}[x_1, \ldots, x_r]/I$ is the set

$$\mathbf{soc}(R) = \{f \in R | fg = 0 \text{ for all } g \in \boldsymbol{m}\},$$

where $\boldsymbol{m} = (x_1, \ldots, x_r)$ is the unique graded maximal ideal in R.

Lemma 6.4. *The socle is a graded ideal.*

Proof It is obvious that the socle is an ideal. Any $f \in R$ can be decomposed into homogenous components, $f = f_1 + f_2 + \cdots + f_d$. Take $f \in \mathbf{soc}(R)$, then since $fg = 0$ for all $g \in \boldsymbol{m}$ we have that $(f_1 + \cdots + f_d)x_i = f_1x_i + \cdots + f_dx_i = 0$ for all i. This implies that $f_jx_i = 0$ for all $1 \leq j \leq d$, since $f_1x_i, \ldots, f_dx_i$ are all homogenous of different degrees or 0.

It is obvious that any $f = f_1 + \cdots + f_d$ such that $f_n \in \mathbf{soc}(R), 1 \leq n \leq d$ is in $\mathbf{soc}(R)$. Hence the socle is a graded ideal.

Lemma 6.5. *The element $e_w \in \Gamma[W]$ is in the socle iff $w \in W$ is a facet. These elements span the socle as a vector space.*

Proof $n \leq m$ if and only if $e_m = e_n * e_p$ for some $p \in W$. Hence w is a facet if and only if for all $v \in W \setminus \{1\}$, $e_v * e_w \neq e_k, k \in W$, i.e. $e_v * e_w = 0$ for all $v \in W \setminus \{1\}$. Hence w facet implies $e_w \in \mathbf{soc}(\Gamma[W])$.

Assume $e_w \in \mathbf{soc}(\Gamma[W])$. $\boldsymbol{m}$ is generated by $\{e_v | \ v \in \mathbb{PP}[W]\}$, which means that it is also generated by the set $\{e_v | \ v \in W \setminus \{1\}\}$. Then, for all $v \in W \setminus \{1\}$, $e_w * e_v = 0$. Hence either $vw \notin W$ or $w \notin A(vw)$. In both cases we have that $e_v * e_w \notin \Gamma[W]$. Hence w is a facet.

That these elements then span the socle as a vector space is obvious.

Lemma 6.6. *For any $w \in W$, let JJ_w be the ideal in $S = \frac{\mathbb{C}[\{e_q | \ q \in \mathbb{PP}[W]\}]}{I_W}$ generated by the set $\{ e_v \in \Gamma[W] | v \not\leq w \}$. Then the ideal J_W is the intersection of all ideals JJ_w when w ranges over all facets, in S.*

Proof The ideal $\bigcap_{w \text{ facet}} JJ_w$ is generated by all e_q such that $q \not\leq w$ for any facet w. An equivalent formulation would be to say that the ideal is generated by e_q such that $q \notin W$.

Example 6.7. $W = [10]$. If A is Dirichlet then $\mathbb{PP}[W] = \{2, 3, 5, 7\}$, W is the multicomplex $\{e_2, e_3, e_2^2, e_5, e_2e_3, e_7, e_2^3, e_3^2, e_2e_5\}$, and so the multicomplex ring is

$$\Gamma[W] = \frac{\mathbb{C}[e_2, e_3, e_5, e_7]}{(e_2^4, e_2^3e_3, e_2^2e_5, e_2e_7, e_3^3, e_3e_5, e_3e_7, e_5^2, e_5e_7, e_7^2)}.$$

There is no I_W since $I = (0)$. The facets are $10, 9, 8, 7, 6$ with corresponding ideals $JJ_{10} = (e_3, e_2^2, e_7)$, $JJ_9 = e_2, e_5, e_7)$, $JJ_8 = (e_3, e_5, e_2e_3, e_7)$, $JJ_7 = (e_2, e_3, e_5)$, $JJ_6 = (e_2^2, e_5, e_7, e_3^2)$.

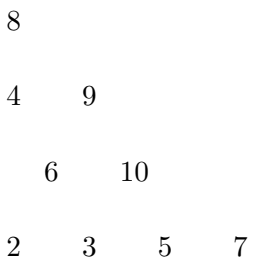


Figure 6.1: $W = 10$, Dirichlet convolution

Example 6.8. If A is unitary convolution, $W = [10]$, then $\mathbb{PP}[W] = \{2, 3, 4, 5, 7, 8, 9\}$, W is the multicomplex $\{e_2, e_3, e_4, e_5, e_2e_3, e_7, e_8, e_9, e_2e_5\}$,

$$I_W = (e_2^2, e_2e_4, e_2e_8, e_3^2, e_3e_9, e_4^2, e_4e_8, e_5^2, e_7^2, e_8^2, e_9^2),$$

the restriction of I to this ring, and

$$J_W = (e_2e_7, e_2e_9, e_3e_5, e_3e_7, e_3e_8, e_4e_5, \\ e_4e_7, e_4e_9, e_5e_7, e_5e_8, e_5e_9, e_7e_8, e_7e_9, e_8e_9).$$

The facets are $10, 9, 8, 7, 6, 4$, with corresponding ideals $JJ_{10} = (e_3, e_4, e_7, e_8, e_9)$,$JJ_9 = (e_2, e_3, e_4, e_5, e_7, e_8)$, $JJ_8 = (e_2, e_3, e_4, e_5, e_7, e_9)$,$JJ_7 = (e_2, e_3, e_4, e_5, e_8, e_9)$, $JJ_6 = (e_4, e_5, e_7, e_8, e_9)$, $JJ_4 = (e_2, e_3, e_5, e_7, e_8, e_9)$.

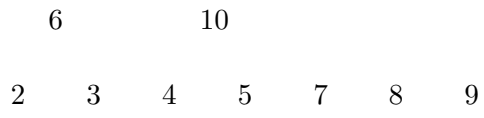


Figure 6.2: $W = 10$, unitary convolution

Example 6.9. If A is ternary convolution, $W = [10]$, then $\mathbb{PP}[W] = \{2, 3, 5, 7, 8\}$, W is the multicomplex $\{e_2, e_3, e_2^2, e_5, e_2e_3, e_7, e_8, e_3^2, e_2e_5\}$,

$$I_W = (e_2^3, e_3^3, e_2e_8)$$

and

$$J_W = (e_2^2e_3, e_2e_7, e_3e_5, e_2e_3^2, e_2^2e_5, e_3e_7, e_3e_8, e_5^2, e_5e_7, e_2e_3e_7, e_7e_8, e_2e_5e_7)$$

The facets are $10, 9, 8, 7, 6, 4$, with corresponding ideals $JJ_{10} = (e_3, e_2^2, e_7, e_8, e_3^2)$, $JJ_9 = (e_2, e_5, e_2e_3, e_7, e_8)$, $JJ_8 = (e_2, e_3, e_5, e_7)$, $JJ_7 = (e_2, e_3, e_5, e_8)$, $JJ_6 = (e_2^2, e_5, e_7, e_8, e_3^2, e_2e_5)$, $JJ_4 = (e_3, e_5, e_2e_3, e_7, e_8, e_2e_5)$

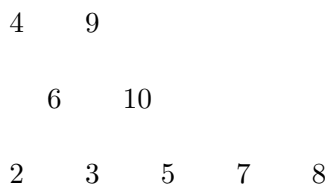


Figure 6.3: $W = 10$, ternary convolution

Bibliography

[1] W. Narkiewicz. On a class of arithmetical convolutions. *Colloquium Mathematicum*, 10(1):81–94, 1963.

[2] S. Bosch, U. Günter, and R. Remmert. *Non-Archimedean Analysis.* Springer-Verlag, 1984.

[3] A. Schinzel. A property of the unitary convolution. *Colloquium Mathematicum*, 78(1):93–96, 1998.