Factorization in Arithmetic Convolution Rings

Stefan Veldsman

veldsman@squ.edu.om
Sultan Qaboos University, Muscat, Sultanate of Oman

1. Introduction

An arithmetic convolution ring is a special case of the more general convolution rings. Convolution rings were introduced in [7] as a general ring construction for mainly two reasons:

(1) It provides a convenient tool to describe and investigate that which is common for many different ring constructions.

(2) It enables one to isolate properties of the construction method that determine algebraic properties of the constructed ring.

Both these will be demonstrated here by studying arithmetic rings under the guise of arithmetic convolution rings. Recall, arithmetic rings are rings of complex valued functions with domain in the set of non-negative integers and multiplication typically given by the Cauchy product or the Dirichlet product.

2. Definitions

An *arithmetic convolution type* $\mathcal{T}$ is a pair $\mathcal{T} = (X, \sigma)$ where the parameters X and σ satisfy:

- X a non-empty set of integers and
- for every $x \in X$, $\emptyset \neq \sigma(x)$ finite and symmetric subset of $X \times X$.

For a ring A, let $C(A, \mathcal{T}) = \{f \mid f : X \to A \text{ a function}\}$ with two operations:

- componentwise addition, $(f + g)(x) = f(x) + g(x)$ and
- convolution product, $(fg)(x) = \sum_{(s,t)\in\sigma(x)} f(s)g(t)$

For the product to be associative, it is assumed that:

For all $x \in X, (s, t) \in \sigma(x)$ and $(p, q) \in \sigma(s)$, there exists a unique $v \in X$ with $(p, v) \in \sigma(x)$ and $(q, t) \in \sigma(v)$.

$C(A, \mathcal{T})$ is a ring; called the *arithmetic convolution ring of type* $\mathcal{T}$ *over* A; usually denoted by $C(A)$.

In general there need not be any strong relationship between A and $C(A)$. To ensure that at least A can be embedded into $C(A)$, suppose

that X contains a non-empty subset T (the set of *trivial elements)* which satisfies the following three conditions:

(T1) For all $t \in T$, $(t,t) \in \sigma(t)$.
(T2) For every $x \in X$, there exists unique $t = t_x \in T$ such that $(t,x) \in \sigma(x)$.
(T3) If $(p,q) \in \sigma(x)$ and $p \in T$, then $q = x$.

Then $\iota : A \to C(A)$ defined by $\iota(a) = \iota_a : X \to A$ with $\iota_a(x) = \begin{cases} a \text{ if } x \in T \\ 0 \text{ if } x \notin T \end{cases}$ is an embedding of A into $C(A)$.

3. Examples

(1) **Direct Product.** $\emptyset \neq X \subseteq \mathbb{Z}$ ($\mathbb{Z}$ the set of the integers). Let $\sigma(x) = \{(x,x)\}$ for all $x \in X$. Then $T = X$, $(fg)(x) = f(x)g(x)$. $C(A)$ is the direct product A^X of $|X|$-copies of the ring A.

(2) **Cauchy Product**. $X = \mathbb{Z}_0^+ := \{0,1,2,3,...\ \}$ and $\sigma(n) = \{(i,j) \mid i,j \in \mathbb{Z}_0^+, i+j = n\}$ for each $n \in \mathbb{Z}_0^+$. Then $T = \{0\}$ and $(fg)(n) = \sum_{i+j=n} f(i)g(j)$. $C(A)$ is the ring $A[[x]]$ of formal power series over A in the commuting indeterminate x.

(3) **Lucas Product.** $X = \mathbb{Z}_0^+$. Let p be any fixed prime. Then any integer $a \geq 0$ can be written as $a = a_0 + a_1 p + a_2 p^2 + ...$ where for each a_i, $0 \leq a_i < p$. Let $\sigma(n) = \{(r,s) \mid r,s \in \mathbb{Z}_0^+, r+s = n$ and for all $i \geq 0$, $r_i \leq n_i\}$ for each $n \in \mathbb{Z}_0^+$. Then $T = \{0\}$.

(4) **Dirichlet Product.** $X = \mathbb{Z}^+$ and for each $n \in X$, let $\sigma(n) = \{(r,s) \mid r,s \in \mathbb{Z}^+, rs = n\}$. Then $T = \{1\}$ and $(fg)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$.

(5) **Extended Dirichlet Product.** $X = \mathbb{Z} - \{0\}$ and for every $n \in X$, let $\sigma(n) = \{(r,s) \mid rs = n\}$. Then $T = \{1\}$ and $\sigma(1) = \{(1,1),(-1,-1)\}$.

(6) **Prime Power Product.** Let $p_1, p_2, ..., p_k$ be k distinct primes, $k \geq 1$. Let $X = \{p_1^{n_1} p_2^{n_2} ... p_k^{n_k} \mid n_i \geq 0\}$. For each $n \in X$, let $\sigma(n) = \{(r,s) \mid r,s \in X, rs = n\}$ and let $T = \{1\}$.

(7) **Unitary Convolution.** Let $X = \mathbb{Z}^+$ and for each $n \in X$, let $\sigma(n) = \{(r,s) \mid r,s \in \mathbb{Z}^+, rs = n$ and $\gcd(r,s) = 1\}$. Then $T = \{1\}$.

(8) **Necklace Product.** Let $X = \mathbb{Z}^+$ and let $\sigma(n) = \{(i,j) \mid i,j \in \mathbb{Z}^+, \operatorname{lcm}(i,j) = n\}$ for all $n \in \mathbb{Z}^+$. Then $T = \{1\}$ and $(fg)(n) = \sum_{\operatorname{lcm}(r,s)=n} f(r)g(s)$.

(9) **Quasi-regular Product.** Let $X = \mathbb{Z}_0^+$ and let $\sigma(n) = \{(i,j) \mid 0 \leq i,j \leq n, i+j-ij = n\}$ for each $n \geq 0$. Then $T = \{0\}$.

(10) **Full product.** Let $X = \mathbb{Z}^+$ and let $\sigma(n) = \{(i,j) \mid (i = n \text{ and } 1 \leq j \leq n) \text{ or } (j = n \text{ and } 1 \leq i \leq n)\}$ for all $n \geq 1$. Then $T = \{1\}$.

4. Zero-divisors

Any zero-divisor of A will be a zero-divisor of $C(A)$, but zero-divisors in $C(A)$ may also exclusively come from properties of the convolution parameters:

PROPOSITION 1. *Suppose the convolution type $\mathcal{T}$ satisfies condition*

$(ZD1)$: *There exists $p, q \in X$ such that for all $x \in X$, $(p,q) \notin \sigma(x)$.*

Then $C(A)$ will have nonzero zero-divisors for any ring $A \neq 0$.

PROPOSITION 2. *Suppose the convolution type $\mathcal{T}$ satisfies condition*

$(ZD2)$: *There exists $p \in X - T$ such that $(p,p) \in \sigma(p)$ and for all $x \in X - \{p\}, (p,p) \notin \sigma(x)$.*

Then $C(A)$ will have nonzero zero-divisors for any ring $A \neq 0$.

An arithmetic convolution type is called *well-behaved* if it satisfies:

(WB1) For every $r, s \in X$, there exists $y \in X$ with $(r,s) \in \sigma(y)$.

(WB2) $\mathcal{T}$ has the *Complementary Ordering Property*, i.e., for all $x \in X$ and for all $(r,s),(u,v) \in \sigma(x)$, $r \leq u \Leftrightarrow s \geq v$.

(WB3) $\mathcal{T}$ fulfils the *Lower Bound Requirement*: If $T \neq X$, then $X - T$ has a lower bound in $\mathbb{Z}$.

PROPOSITION 3. *Let $\mathcal{T}$ be a well-behaved arithmetic convolution type. Then $C(A)$ will have zero-divisors if and only if the ring A has zero-divisors. Thus, for such convolution types, $C(A)$ is an integral domain if and only if A is an integral domain.*

Examples of well-behaved arithmetic convolution types are: the Cauchy product, the Dirichlet product and the prime power product.

5. Units and Inversion Theorems

Any unit in A will be a unit in $C(A)$, but in general $C(A)$ is much larger than A and may contain more units. To help identifying units in $C(A)$, a convolution type is said to satisfy condition (U) if the following three requirements are fulfilled:

(U1) For all $t \in T$, $\sigma(t) = \{(t,t)\}$.

(U2) For all $x \in X$ and for all $(r,s) \in \sigma(x)$, if $r \notin T$, then $s < x$.

(U3) Lower Bound Requirement, i.e. if $T \neq X$, then $X - T$ has a lower bound in $\mathbb{Z}$.

PROPOSITION 4. *For an arithmetical convolution type which satisfies condition (U) and a commutative ring A with identity, $f \in C(A)$ is a unit in $C(A)$ if and only if $f(t)$ is a unit in A for all $t \in T$.*

A simple observation but with many applications is the Inversion Principle. This is especially the case for the Dirichlet product where it forms the basis of the well-known inversion theorems:

Inversion Principle. Let A be a commutative ring with identity. Let $u \in C(A)$ be a unit with inverse w. For any $f, g \in C(A)$, $f = gu$ if and only if $g = fw$. Hence, for each $x \in X$, $f(x) = \sum_{(r,s)\in\sigma(x)} g(r)u(s)$ if and only if for each $x \in X, g(x) = \sum_{(r,s)\in\sigma(x)} f(r)w(s)$.

Examples:

(1) The **direct product** convolution type satisfies condition (U) and $f : X \to A$ is a unit if and only if $f(x)$ is a unit for all $x \in X$. Inversion theorems are not interesting here: the product is not "convoluted" enough: if u is a unit in A^X with inverse u^{-1}, then for any $f, g \in A^X$, $f(x) = g(x)u(x)$ for all x if and only if $g(x) = f(x)u^{-1}(x) = f(x)(u(x))^{-1}$ for all x.

(2) The **Dirichlet product** convolution type satisfies condition (U) and if $u \in C(A)$ is a unit with inverse w, then for all $f, g \in C(A)$, $f(n) = \sum_{d|n} g(d)u(\frac{n}{d})$ for all $n \geq 1$ if and only if $g(n) = \sum_{d|n} f(d)w(\frac{n}{d})$ for all $n \geq 1$. In particular, if we take $X = \mathbb{Z}^+$, $A = \mathbb{C}$ and $u(n) = 1$ for all $n \geq 1$, then u is a unit with inverse

$$w(n) = \begin{cases} 1 \text{ if } n = 1 \\ (-1)^k \text{ if } n \text{ has } k \text{ different primes in its prime factorization} \\ 0 \text{ otherwise} \end{cases}.$$

This is just the Möbius function and we have the well-known Möbius Inversion Formula: $f(n) = \sum_{d|n} g(d)$ for all $n \geq 1$ if and only if $g(n) = \sum_{d|n} f(d)w(\frac{n}{d})$ for all $n \geq 1$.

(3) The **Cauchy product** convolution types satisfies condition (U). An application of the Inversion Principle for the Cauchy product is: Let $A = \mathbb{C}$ and let $k \neq 0$ be a fixed real number.

Let $u := (1+x)^k = \sum_{n=0}^{+\infty} \binom{k}{n} x^n$ where $\binom{k}{n} = \begin{cases} \frac{k(k-1)\ldots(k-(n-1))}{n!} \text{ if } n \geq 1 \\ 1 \text{ if } n = 0 \end{cases}$,

i.e.

$u(n) = \binom{k}{n}$ for all $n \geq 0$. Then u is a unit in $C(A)$ with inverse $w = (1+x)^{-k} = \sum_{n=0}^{+\infty} \binom{-k}{n} x^n$, i.e. $w(n) = \binom{-k}{n}$ for all $n \geq 0$. Let $g(n) = 1$ for all $n \geq 0$. For $f = gu$ we get $f(n) = \sum_{i=0}^{n} \binom{k}{n-i}$ and then $g = fw$ by the Inversion Principle which leads to the identity $1 = \sum_{i=0}^{n} \sum_{j=0}^{i} \binom{k}{i-j} \binom{-k}{n-i}$ for all $n \geq 0$.

(4) Any well-behaved arithmetic convolution type satisfies condition (U).

6. Well-behaved arithmetic convolution types

PROPOSITION 5. *Let $\mathcal{T} = (X, \sigma)$ be a well-behaved arithmetic convolution type. Then:*

(i) $T = \{t\}$.

(ii) For any $x, y \in X$, there exists a unique $z \in X$ with $(x, y) \in \sigma(z)$; write $z = x * y$

(iii) $(X, *)$ is a commutative semigroup with identity t.

(iv) The identity t is the only unit in the semigroup $(X, *)$.

(v) $(X, *)$ is cancellative ($a * x = a * y$ implies $x = y$)

(vi) $(X, *)$ is torsion-free ($nx = ny$ implies $x = y$, $n \geq 1$).

(vii) $(X, *)$ is monotone with respect to the usual order on $\mathbb{Z}$ (for all $x, y, a \in X, x < y$ implies $x * a < y * a$).

(viii) When $T \neq X$, then X must necessarily be infinite.

In general, for $\mathcal{T}$ a well-behaved arithmetic convolution type, $C(A, \mathcal{T})$ is not the same as the semigroup ring $A[X]$ since the latter only consists of functions with finite support. The generalized power series rings studied by Ribenboim in many papers, see for example [3], is more restrictive than the general arithmetic convolution rings while a well-behaved arithmetic convolution ring is a special case of a generalized power series ring but with much sharper results.

7. Factorization

Discussions about factorization usually start with the notions prime and irreducibility; here it is no exception.

Suppose that $\mathcal{T} = (X, \sigma)$ is a well-behaved arithmetic convolution type with $T = \{t\}$. We fix some terminology:

- For $x, y \in X$, x *σ-divides* y in X if there is a $z \in X$ with $y = x * z$.
- $p \in X$ is *σ-irreducible* if $p \notin T$ and $|\sigma(p)| = 2$, i.e. $\sigma(p) = \{(p, t), (t, p)\}$.

• $p \in X$ is *σ-prime* if $p \notin T$ and whenever p σ-divides $a * b$, then p σ-divides a or p σ-divides b.

• For $m \in X$, define $e_m : X \to A$ by $e_m(x) = \begin{cases} 1 \text{ if } x = m \\ 0 \text{ otherwise} \end{cases}$.

PROPOSITION 6. *Let $\mathcal{T} = (X, \sigma)$ be a well-behaved arithmetic convolution type and let A be an integral domain. If $p \in X$ is σ-prime, then e_p is a prime element of the ring $C(A)$.*

PROPOSITION 7. *Let $\mathcal{T}$ be a well-behaved arithmetic convolution type and let A be an integral domain. Let $b \in A$. Then:*

(i) If b is irreducible in A, then b is also irreducible in $C(A)$.

(ii) If b is prime in A, then b is also a prime element in $C(A)$.

(iii) If $f \in C(A)$ with $f(t)$ irreducible in A, then f is irreducible in $C(A)$.

PROPOSITION 8. *Let $\mathcal{T}$ be a well-behaved arithmetic convolution type and let A be an integral domain. Let $f \in C(A)$ with $f(t) = ab$ where a and b are non-units in A with $aA+bA = A$. Then f is reducible in $C(A)$.*

PROPOSITION 9. *Let $\mathcal{T}$ be a well-behaved arithmetic convolution type and let A be an integral domain. If A has acc on principal ideals, then so does $C(A)$.*

Let $E := \{e_p \mid p \in X \text{ is } \sigma\text{-prime}\}$. If $E \neq \emptyset$, let $A[[E]]$ denote the ring of formal power series over A in the commuting indeterminates $e_p \in E$.

PROPOSITION 10. *Let $\mathcal{T}$ be a well-behaved arithmetic convolution type and let A be an integral domain. Suppose every σ-irreducible element in X is σ-prime and X has at least one σ-irreducible element. Then $C(A) \cong A[[E]]$.*

Examples:

(1) The Cauchy Product has only one σ-prime (namely 1) and $C(A) \cong A[[x]]$.

(2) The Dirichlet Product has infinitely many σ-primes (the prime numbers are exactly the σ-primes) and $C(A) \cong A[[x_1, x_2, x_3, ...]]$.

(3) For the Prime Power Product determined by the primes $p_1, p_2, p_3, ..., p_k$, these are exactly also all the σ-primes and $C(A) \cong A[[x_1, x_2, x_3, ..., x_k]]$.

PROPOSITION 11. *For a well-behaved arithmetic convolution type $\mathcal{T}$ with cardinality of the index set at least 2 and an integral domain A, the following are equivalent:*

(i) $C(A)$ is a principal ideal domain.

(ii) A is a field and X has a unique σ-irreducible element.

(iii) A is a field and $C(A) \cong A[[x]]$.

For our final results, we need : Choose $p \in X$, let $\overline{X_p} := \{x \in X \mid p$ does not σ-divide $x\}$ and $\sigma_p(r) = \sigma(r)$ for all $r \in \overline{X_p}$. Then:

PROPOSITION 12. *For a well-behaved arithmetic convolution type $\mathcal{T} = (X, \sigma)$ and $\mathcal{T}_p := (\overline{X_p}, \sigma_p)$, $\mathcal{T}_p$ is a well-behaved arithmetic convolution type if and only if p is a σ-prime element of X.*

In this case, for a ring A, the corresponding convolution ring is denoted by $C_p(A)$. The function $\pi_p : C(A) \to C_p(A)$, defined by $\pi_p(f) = \overline{f}$ where $\overline{f}$ is the restriction of f to $\overline{X_p}$, is a surjective homomorphism with $\ker \pi_p$ the ideal of $C(A)$ generated by e_p. With any $g \in C_p(A)$ we associate an element $g^* : X \to A$ of $C(A)$ defined by $g^*(x) = \begin{cases} g(x) \text{ if } x \in \overline{X_p} \\ 0 \text{ otherwise} \end{cases}$. Then $\pi_p(g^*) = \overline{g^*} = g$ and $\pi_p(f) = \pi_p(\overline{f}^*)$ for all $g \in C_p(A), f \in C(A)$.

PROPOSITION 13. *Let $\mathcal{T}$ be a well-behaved arithmetic convolution type. Let $p \in X$ be a σ-prime element and let I be a prime ideal of $C(A)$. Then $I_p := \pi_p(I)$ is an ideal of $C_p(A)$. Moreover, I is finitely generated in $C(A)$ if and only if I_p is finitely generated in $C_p(A)$. In particular, if $I = \langle f_1, f_2, ..., f_n \rangle$, then $I_p = \langle \overline{f_1}, \overline{f_2}, ..., \overline{f_n} \rangle$ and if $I_p = \langle g_1, g_2, ..., g_n \rangle$, then*

$$I = \begin{cases} \langle g_1^*, g_2^*, ..., g_n^*, e_p \rangle \text{ if } e_p \in I \\ \langle f_1, f_2, ..., f_n \rangle \text{ if } e_p \notin I \text{ and } f_i \in I \text{ with } \pi_p(f_i) = g_i. \end{cases}$$

For the Cauchy Product, there is a unique σ-prime and $C(A) \cong A[[x]]$. The above theorem is then just the well-known result of Kaplansky that a prime ideal I of $A[[x]]$ is finitely generated if and only if $I_1 := \{a \in A \mid a = f(0)$ for some $f \in I\}$ is a finitely generated ideal of A.

COROLLARY 14. *(Arithmetic convolution ring version of the Hilbert Basis Theorem) Let $\mathcal{T}$ be a well-behaved arithmetic convolution type. Let $p \in X$ be a σ-prime element. For an integral domain A, $C_p(A)$ noetherian implies $C(A)$ noetherian.*

COROLLARY 15. *Let $\mathcal{T}$ be a well-behaved arithmetic convolution type. Let $p \in X$ be a σ-prime element. If $C_p(A)$ is a principal ideal domain, then $C(A)$ is a unique factorization domain.*

For polynomial rings, the converse of the Hilbert Basis Theorem was given by Gilmer [2]; we conclude with the arithmetic convolution ring version.

PROPOSITION 16. *Let $\mathcal{T}$ be a well-behaved arithmetic convolution type with cardinality of the index set greater than one. Let A be a commutative ring. Then $C(A)$ noetherian implies A noetherian and A must have an identity.*

References

[1] BIRMAJER, Daniel and Juan B. GILL. Arithmetic in the ring of formal power series with integer coefficients, *Amer. Math. Monthly* **115** (2008), 541-549.

[2] GILMER, R.W. If $R[X]$ is Noetherian, R contains an identity, *Amer. Math. Monthly* **74**(1967), 70

[3] RIBENBOIM, Paulo. Rings of generalized Power Series II: Units and Zero-Divisors, *J. Algebra* **168** (1994), 71-89.

[4] SAMUEL, Pierre. On unique factorization domains, *Illinois J. Math.* **5** (1961), 1-17.

[5] VAIDYANATHASWAMY, R. The theory of multiplicative arithmetic functions, *Trans. Amer. Math. Soc.* **33** (2) (1931), 579-662.

[6] VARADARAJAN, K. and K. WEHRHAHN. Aperiodic rings, necklace rings and Witt vectors, *Advances in Math.* **81** (1990), 1-29.

[7] VELDSMAN, S. Convolution Rings, *Alg. Coll.* **13**(2) (2006), 211-238.

[8] VELDSMAN, S. The radical theory of convolution rings, *Bull. Acad. Stiinte Repub. Mold. Mat.* **44**(1) (2004), 98-115.

[9] WATKINS, John J. *Topics in commutative ring theory.* Princeton University Press, USA, 2007.