Arithmetic Convolution Rings

Stefan Veldsman

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

Abstract. Arithmetic convolution rings provide a general and unified treatment of many rings that have been called arithmetic; the best known examples are rings of complex valued functions with domain in the set of non-negative integers and multiplication the Cauchy product or the Dirichlet product. The emphasis here is on factorization and related properties of such rings which necessitates prior results on the existence of zero-divisors and units in arithmetic convolution rings.

Mathematics Subject Classification: Primary 16S99; Secondary 13F15, 13F25

Keywords: arithmetic convolution ring; arithmetic ring; Cauchy product; Dirichlet product

1. Introduction

Earlier the notions convolution type and convolution ring have been defined [7]. In itself, a convolution type is independent of any algebraic considerations, but a convolution type can be imposed on a ring which will result in a new ring, called the corresponding convolution ring. There are many different convolution types. One type, when imposed on a ring may yield a matrix ring; another type may yield a polynomial ring, etc. The reasons for doing this were two-fold. In the first place, it provides a convenient tool to describe and investigate that which is common for many different ring constructions. For example (see [8]), the general radical theory of convolution rings is a convenient tool to describe the radical theory of polynomial rings, matrix rings, incidence algebras, etc. Secondly, and this is also our purpose here, it enables one to separate the construction method from the base ring and enables one to isolate what it is in the construction method that determines certain algebraic properties of the constructed ring. As a trivial example, a polynomial ring over a commutative ring is always commutative, but a matrix ring over a commutative ring need not be commutative and the reason for this difference is to
be found in the construction method. Both these aspects will be demonstrated here by studying arithmetic convolution rings. This is a generalization of the well-known arithmetic rings and our emphasis will be on factorization and related properties in such rings. In particular, this general approach will unify many common results between the arithmetic ring with the Cauchy product and the one with the Dirichlet product but it will also show that the essential difference between them is in the number of ”prime elements” in the associated index sets (Proposition 16 and the ensuing remarks). In preparation for this, we will initially need results on the existence or not of zero-divisors and units in such arithmetic convolution rings.

2. Definitions and Examples

For the definition of a general convolution type, see [7]. Here we will only consider the more restricted arithmetic convolution type \( T \). This is a pair \( T = (X, \sigma) \) with \( X \) and \( \sigma \) the parameters of the convolution type. \( X \) is a non-empty set of of integers, called the index set and for every \( x \in X \), \( \sigma(x) \) is a non-empty, finite and symmetric subset of \( X \times X \) called the convolution rule. By the symmetry of \( \sigma \) is understood that \((s,t) \in \sigma(x)\) if and only if \((t,s) \in \sigma(x)\). Let \( A \) be a ring and let \( C(A,T) = \{ f \mid f : X \to A \text{ a function} \}. \) On the set \( C(A,T) \) define two operations, componentwise addition and convolution product respectively by: For \( f, g \in C(A,T) \) and \( x \in X \), let \((f+g)(x) = f(x) + g(x)\) and let \((fg)(x) = \sum_{(s,t)\in \sigma(x)} f(s)g(t)\). In general \( C(A,T) \) need not be a ring with respect to these operations since the product need not be associative. To ensure associativity, we assume:

(A) 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 \((q,t) \in \sigma(v)\).

Then \( C(A,T) \) is a ring, called the arithmetic convolution ring of type \( T \) over \( A \). When the convolution type under discussion is clear, we will write \( C(A) \) for \( C(A,T) \). The ring \( A \) is often called the base ring. In general, one could have vastly contrasting properties between \( A \) and \( C(A) \). To ensure at least some relationship between the rings \( A \) and \( C(A) \), we need to impose a further condition on the convolution type to ensure that \( A \) can be embedded into \( C(A) \). This is achieved by assuming the existence of certain trivial elements in \( X \). We suppose that \( X \) contains a non-empty subset \( T \) 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 \((t,t) \in \sigma(x)\).

(T3) If \((p,q) \in \sigma(x)\) and \( p \in T \), then \( q = x \).

By the symmetry of \( \sigma \), necessarily also \((x,t) \in \sigma(x)\) holds if \((t,x) \in \sigma(x)\) (cf. (T2)) and \((p,q) \in \sigma(x)\) and \( q \in T \) implies \( p = x \) (cf. (T3)). Subject to the existence of such a subset \( T \) in \( X \), every ring \( A \) can be embedded as a subring in \( C(A) \) via the map \( \iota : A \to C(A) \) defined by
\[ \iota(a) = \iota_a : X \to A \text{ with } \iota_a(x) = \begin{cases} a \text{ if } x \in T \\ 0 \text{ if } x \notin T. \end{cases} \]

We usually identify \( a \in A \) with \( \iota_a \). This embedding is well-behaved in the sense that if \( A \) has an identity 1, then \( \iota_1 \) is the identity of \( C(A) \). The class of trivial elements \( T \) is uniquely defined. If \( x \in X \) is such that \( \sigma(x) = \{(x, x)\} \), then \( x \in T \), but in general, for \( t \in T \), \( \sigma(t) \) may contain elements other than \( (t, t) \). When \( T = X \), then \( \sigma(x) = \{(x, x)\} \) for all \( x \in X \). When \( X \) has cardinality 1, then \( C(A) \) coincides with \( A \). For later use, note that because \( \sigma \) is symmetric, \( C(A) \) will be a commutative ring if and only if \( A \) is a commutative ring.

**Example 1.** The first four examples below are well-known and their properties have been studied in many papers.

(i) **Direct Product.** Let \( X \) be any non-empty subset of the integers. Let \( \sigma(x) = \{(x, x)\} \) for all \( x \in X \). Then \( T = X \) and in this case \( (fg)(x) = f(x)g(x) \). Hence the convolution ring \( C(A) \) coincides with the direct product \( A^X \) of \(|X|\) copies of the ring \( A \).

(ii) **Cauchy Product.** Let \( X = \mathbb{Z}_0^+ := \{0, 1, 2, 3, \ldots \} \) 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 \( (fg)(n) = \sum_{i+j=n} f(i)g(j) \). This convolution ring \( C(A) \) is just the ring \( A[[x]] \) of formal power series over \( A \) in the commuting indeterminate \( x \).

(iii) **Lucas Product.** This is a restricted version of the Cauchy Product. Let \( p \) be any fixed prime. Then any integer \( a \geq 0 \) can be written as \( a = a_0 + a_1p + a_2p^2 + \ldots \) where for each \( a_i \), \( 0 \leq a_i < p \). Let \( \sigma(n) = \{(r, s) \mid r, s \in \mathbb{Z}_0^+, r + s = n \text{ and for all } i \geq 0, r_i \leq n_i \} \) for each \( n \in \mathbb{Z}_0^+ \). Then \( T = \{0\} \).

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

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

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

(vii) **Unitary Convolution.** This is a variant of the Dirichlet product (see [5]). Let \( X = \mathbb{Z}^+ \) and for each \( n \in X \), let \( \sigma(n) = \{(r, s) \mid r, s \in \mathbb{Z}^+, rs = n \text{ and } \gcd(r, s) = 1\} \). Here \( T = \{1\} \).

(viii) **Necklace Product.** Let \( X = \mathbb{Z}^+ \) and let \( \sigma(n) = \{(i, j) \mid i, j \in \mathbb{Z}^+, \lcm(i, j) = n\} \) for all \( n \in \mathbb{Z}^+ \). Let \( T = \{1\} \). The terminology used here for this product is strictly speaking not really correct. Necklace rings have been defined and studied in [6] where the necklace product was actually defined.
by \((fg)(n) = \sum_{\text{lcm}(r,s)=n} \gcd(r,s)f(r)g(s)\) while here the product is given by \((fg)(n) = \sum_{\text{lcm}(r,s)=n} f(r)g(s)\).

(ix) **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 \(n \geq 0\). Here \(T = \{0\}\).

(x) **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 \(n \geq 1\). Let \(T = \{1\}\).

(xi) **Extended Cauchy Product.** Let \(X = \mathbb{Z}\), \(\sigma(x) = \{(r,s) \mid r + s = x, rs \geq 0\}\) for all \(x \in X\). Here \(T = \{0\}\).

3. **Zero-divisors**

Since \(A\) is a subring of \(C(A)\), any zero-divisor of \(A\) will be a zero-divisor in \(C(A)\). But \(C(A)\) may have zero-divisors irrespective of whether \(A\) has or not; this being a consequence of the construction method. Here we identify two such cases. We also want to know under which conditions on the parameters of the convolution type the only zero-divisors in \(C(A)\) are those already present in \(A\).

**Proposition 2.** Suppose the convolution type \(T\) 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 \(A \neq 0\).

**Proof.** Suppose the existence of \(p\) and \(q\) as in \((ZD1)\). Let \(0 \neq a \in A\) and define \(f,g : X \to A\) by

\[
f(x) = \begin{cases} 
a & \text{if } x = u \\
0 & \text{otherwise}
\end{cases}
\quad \text{and} \quad
g(x) = \begin{cases} 
a & \text{if } x = v \\
0 & \text{otherwise}
\end{cases}
\]

Then \(f \neq 0, g \neq 0\) but \(fg = 0\). \(\square\)

**Proposition 3.** Suppose the convolution type \(T\) 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 \(A \neq 0\).

**Proof.** Suppose the existence of \(p \in X\) as in \((ZD2)\). By \((T2)\) there is a \(t \in T\) with \((p,t) \in \sigma(p)\) and \((t,p) \in \sigma(p)\). Choose \(0 \neq a \in A\) and define \(f,g : X \to A\) by

\[
f(x) = \begin{cases} 
a & \text{if } x = t \\
-a & \text{if } x = p \\
0 & \text{otherwise}
\end{cases}
\quad \text{and} \quad
g(x) = \begin{cases} 
-a & \text{if } x = p \\
0 & \text{otherwise}
\end{cases}
\]

Then \(f \neq 0, g \neq 0\) and it can be verified that \(fg = 0\). \(\square\)
Convolution types satisfying any one of the conditions above will always force the corresponding convolution rings to have nonzero zero-divisors, irrespective of any properties that the ring $A$ may have. To ensure that zero-divisors in a convolution ring can only come from $A$ (if there are any), the following requirement on the convolution type will suffice:

An arithmetic convolution type is called well-behaved $(WB)$ if it satisfies:

(WB1) For every $r, s \in X$, there exists $y \in X$ with $(r, s) \in \sigma(y)$ (i.e. condition $(ZD1)$ is not satisfied).

(WB2) $T$ 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) $T$ fulfils the Lower Bound Requirement: If $T \neq X$, then $X - T$ has a lower bound in $\mathbb{Z}$.

We will see below that a well-behaved arithmetic convolution type actually imposes a strong algebraic structure on the index set; but now we just mention the following properties of such a type $T$. Firstly, $X$ has exactly one trivial element. Indeed, the existence of at least one follows from the assumption that $T \neq \emptyset$ and if $t_1$ and $t_2$ are two elements of $T$, then condition (WB1) gives an $s \in X$ with $(t_1, t_2) \in \sigma(s)$. By condition (T3) and the symmetry of $\sigma$ we get $t_1 = s = t_2$. We also note that by (WB2), if $(r, s), (u, v) \in \sigma(x)$ with $r < u$, then $s > v$. (WB2) also implies that condition (ZD2) does not hold.

**Proposition 4.** Let $T$ be a well-behaved arithmetic convolution type. Then $C(A)$ will have zero-divisors if and only if the ring $A$ has zero-divisors. Consequently $C(A)$ is an integral domain if and only if $A$ is an integral domain.

**Proof.** If $X$ has cardinality 1, the statement follows; suppose that $|X| \geq 2$. The necessity is clear; suppose $C(A)$ has nonzero zero-divisors, say $f, g$ are nonzero elements of $C(A)$ with $fg = 0$. By the assumptions, $\{t\} = T \subset X$ and $X$ has a lower bound in $\mathbb{Z}$. Let $F$ and $G$ be the support of $f$ and $g$ respectively in $X$. Both $F$ and $G$ are non-empty; hence $r := \min F \in X$ and $s := \min G \in X$ exist. Choose $y \in X$ with $(r, s) \in \sigma(y)$. Then $f(r) \neq 0 \neq g(s)$ but $f(r)g(s) = 0$. Indeed, for any $(p, q) \in \sigma(y)$, if $p < r$, then $f(p) = 0$ and if $p > r$, then by (WB2) $q < s$ and so $g(q) = 0$. If $p = r$, then by (WB2), $q = s$ and so $0 = (fg)(y) = \sum_{(p,q) \in \sigma(y)} f(p)g(q) = f(r)g(s)$.

The Cauchy product, Dirichlet product and Prime power product are examples of well-behaved arithmetic convolution types; the Direct product, Lucas product and Quasi-regular product satisfy $(ZD1)$ and the Necklace product and the Quasi-regular product satisfy $(ZD2)$.

### 4. Units and Inversion Theorems

For a ring $A$ with identity, any unit of $A$ will be a unit in $C(A)$. But in general, the ring $C(A)$ is much "larger" than $A$; so it is plausible to expect
more units in $C(A)$. To ensure the existence of such units in $C(A)$, certain conditions on the convolution type have to be imposed. A convolution type satisfies condition $(U)$ if it satisfies the following three requirements:

(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 (= WB3)), i.e. if $T \neq X$, then $X - T$ has a lower bound in $\mathbb{Z}$.

It will be shown below that any well-behaved arithmetic convolution type satisfies condition $(U)$. The converse is not true: the direct product convolution type satisfies condition $(U)$, but is, as was seen before, not well-behaved. The next result confirms the well-known characterization of the units in the power series rings and in the rings with the Dirichlet product. What is interesting however, is that the requirement for the existence of units in these rings is the same as that for the existence of units in a direct product.

**Proposition 5.** For an arithmetical convolution type which satisfies condition $(U)$ and a commutative ring $A$ with identity, $f \in C(A)$ is a unit if and only if $f(t)$ is a unit in $A$ for all $t \in T$.

**Proof.** Let $f$ be a unit in $C(A)$ with inverse $g$. Then $fg = \iota_1 = gf$ and for any $t \in T$, $f(t)g(t) = 1 = g(t)f(t)$. Hence $f(t)$ is a unit in $A$. Conversely, suppose $f \in C(A)$ with $f(t)$ a unit in $A$ for all $t \in T$. Define a function $g : X \to A$ as follows: For each $t \in T$, let $g(t) = (f(t))^{-1}$. If $T = X$ we are done; suppose thus $T \subset X$. By (U3), $m = \min X - T$ exists. For any $r \in X$, if $r < m$, then $r \in T$. By condition (T2) there is a $t_m \in T$ such that $(m, t_m) \in \sigma(m)$. Then $\sigma(m) = \{ (m, t_m), (t_m, m) \}$. Indeed, note firstly that $m \neq t_m$. Let $(r, s) \in \sigma(m)$ with $(r, s) \neq (m, t_m)$ and $(r, s) \neq (t_m, m)$. This means $s \notin T$. By (U2) we get $r < m$ and hence $r \in T$. But then $s = m$ which contradicts $(r, s) \neq (t_m, m)$. Hence $\sigma(m) = \{ (m, t_m), (t_m, m) \}$. Let $g(m) = -(f(t))^{-1}f(m)g(t_m)$. Let $n > m$ and suppose $g(i)$ has been defined for all $m \leq i < n$. We may assume $n \in X - T$. Now $\sigma(n) = \{ (r_1, s_1), (r_2, s_2), ..., (r_k, s_k) \}$ for some $k \geq 2$. We know that $k \geq 2$, for if $\sigma(n) = \{ (r, s) \}$, then we get the contradiction $(n, t_n) = (r, s) = (n, t_n)$. Let us assume $(r_1, s_1) = (t_n, n)$ and $(r_2, s_2) = (n, t_n)$. By (U2) we know that $r_j, s_j < n$ for all $j = 3, 4, ..., k$. Let $g(n) = -(f(t_n))^{-1} \sum_{j=2}^{k} f(r_j)g(s_j)$. Then $g$ is well-defined and it can be verified that $fg = \iota_1 = gf$.  

A simple observation but with many useful applications, is the Inversion Principle. This is especially the case for the Dirichlet product where it forms the basis of the so-called inversion theorems.

**Inversion Principle.** Let $A$ be a commutative ring with identity. Let $u \in C(A)$ be 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 \( x \in X \), \( g(x) = \sum_{(r,s) \in \sigma(x)} f(r)w(s) \).

We conclude this section with some examples. 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, since 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 \( x \).

The Dirichlet product convolution type satisfies condition (U) and if \( u \in C(A) \) is a unit with inverse \( w \), then for all \( f, g \in C(A) \), \( f(n) = \sum_{d|n} g(n)u(\frac{n}{d}) \) for all \( n \geq 1 \) if and only if \( g(n) = \sum_{d|n} f(n)w(\frac{n}{d}) \) 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:

\[
    f(n) = \sum_{d|n} g(d) \text{ for all } n \geq 1 \text{ if and only if } g(n) = \sum_{d|n} f(d)w(\frac{n}{d}) \text{ for all } n \geq 1.
\]

Both the Lucas product convolution type as well as the Cauchy product convolution types satisfy condition (U). We give another application of the Inversion Principle for the Cauchy product. 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 \( \binom{k}{n} = \begin{cases} 
    \frac{k(k-1)...(k-(n-1))}{n!} & \text{if } n \geq 1 \\
    1 & \text{if } n = 0
    \end{cases} \), 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 \( n \geq 0 \).
identity can also be proven directly by using the Vandermonde Convolution

Formula \( \sum_{i=0}^{n} \binom{r}{i} \binom{s}{n-i} = \binom{r+s}{n} \) for \( r, s, n \geq 0 \).

5. Well-behaved arithmetic convolution types

In this section, we will show that the index set of a well-behaved arithmetic convolution type, as defined in Section 3, has a very specific algebraic structure.

For the main result, we need some preliminaries:

Lemma 6. Let \( T = (X, \sigma) \) be a well-behaved arithmetic convolution type. Then:

(i) \( X \) has a minimal element which is the unique trivial element \( t \).
(ii) If \( (r, s) \in \sigma(x) \) for \( x \in X \), then \( r, s \leq x \).
(iii) If \( (r, s) \in \sigma(r) \) for some \( r \in X \), then \( s = t \).
(iv) If \( (r, r) \in \sigma(s) \) for some \( s \in X \), then either \( r = s = t \) or \( r < s \).
(v) For \( (r, s) \in \sigma(x) \), any two of \( r, s \) or \( x \) determines the third uniquely.
(vi) \( T \) satisfies condition \((U)\).

Proof. We already know that \( T = \{ t \} \) and this will often be used without any further mention.

(i) If \( X = T \), the statement is clear; suppose thus \( |X| \geq 2 \). By (WB3), we know that \( X - T \) has a minimal element, say \( m \). Thus \( m \leq t \). By (WB1), there is a \( y \in X \) with \( (m, m) \in \sigma(y) \). By (T2) we also know \( (y, t) \in \sigma(y) \).

From (WB3), since \( m \leq y \), we then have \( m \geq t \), i.e. \( m = t \).

(ii) From \( (r, s) \in \sigma(x) \), \( (x, t) \in \sigma(x) \), \( s \geq t \) and (WB2) we get \( r \leq x \).

(iii) Let \( (r, s) \in \sigma(r) \) for some \( r \in X \). Together with \( (r, t) \in \sigma(r) \) and (WB2) it follows that \( s = t \).

(iv) By (ii) above, \( (r, r) \in \sigma(s) \) implies \( r \leq s \). If \( r = s \), then by (iii) we have \( r = s = t \); otherwise \( r < s \).

(v) Let \( (r, s) \in \sigma(x) \). If also \( (u, s) \in \sigma(x) \), then immediately by (WB2) \( r = u \) follows. Suppose also \( (r, s) \in \sigma(y) \) for some \( y \in X \). By (WB1) there is a \( c \in X \) with \( (x, y) \in \sigma(c) \). Apply condition \((A)\) to \( (x, y) \in \sigma(c) \) and \( (r, s) \in \sigma(x) \) to get a unique \( v \in X \) with \( (r, v) \in \sigma(c) \) and \( (s, y) \in \sigma(v) \). Likewise, using \( (y, x) \in \sigma(c) \) and \( (r, s) \in \sigma(y) \) there is a unique \( u \in X \) with \( (r, u) \in \sigma(c) \) and \( (s, x) \in \sigma(u) \). Then \( (r, v) \in \sigma(c) \) and \( (r, u) \in \sigma(c) \). As we have just seen, this means \( u = v \). Thus \( (s, y) \in \sigma(v) \) and \( (s, x) \in \sigma(u) = \sigma(v) \) gives \( x = y \) by the first part.

(vi) \((U1)\) follows from (i) and (ii); \((U2)\) follows from (ii) and (iii). \( \square \)

Proposition 7. Let \( T = (X, \sigma) \) be a well-behaved arithmetic convolution type. Then \( T = \{ t \} \) and for any \( x, y \in X \), there exists a unique \( z \in X \) with \( (x, y) \in \sigma(z) \); write \( z = x*y \). Moreover, \( (X, *) \) is a commutative semigroup with identity \( t \); it is cancellative (\( a*x = a*y \) implies \( x = y \)), torsion-free (\( nx = ny \) implies \( x = y \)).
\[ x = y, \ n \geq 1 \] and monotone with respect to the usual order on \( \mathbb{Z} \) (for all \( x, y, a \in X, x < y \) implies \( x*a < y*a \)). When \( T \neq X \), then \( X \) must necessarily be infinite.

In the formulation of the proposition, \( nx \) for \( n \in \mathbb{Z}^+ \) and \( x \in X \), means \( nx = x*x*...*x, n \) times (but note that towards the end of Section 6 it will be written as \( x^n \) for the obvious notational advantages there).

**Proof.** That \( (X, \ast) \) is a commutative semigroup with identity \( t \) follows from Lemma 6(v), condition (A), the symmetry of \( \sigma \) and the definition of the class \( T \). The cancellative property also follows from (v) above. Suppose \( x, y, a \in X \) with \( x < y \). We show \( x \ast a < y \ast a \). Let \( x \ast a = u \) and \( y \ast a = v \). Using the associativity and commutativity of the operation \( \ast \), we get \( x \ast v = y \ast u \). By (WB2) \( x \ast a = u < v = y \ast a \). Next we show that \( nx = ny \) implies \( x = y \), \( n \geq 1 \), by induction on \( n \). For \( n = 2 \) with \( x \ast x = y \ast y \), \( x < y \) implies, by (WB2), that \( x > y \); a contradiction. Hence \( x = y \). Let \( n \geq 2 \) and suppose the statement is true for \( n \). Suppose \( (n + 1)x = (n + 1)y \). Then \( nx \ast x = ny \ast y \). If \( x < y \), then the monotonicity already proven gives \( nx < ny \). By (WB2) we then get the contradiction \( x > y \). Thus \( x = y \).

Finally, suppose \( T \neq X \) and \( X \) is finite, say \( X = \{m_0 = t, m_1, ..., m_k\} \), \( k \geq 1 \), with \( m_0 < m_1 < ... < m_k \). By (WB1) there is a \( y \in X \) with \( (m_{k-1}, m_k) \in \sigma(y) \).

Since \( m_k \leq y \) (by Lemma 6(ii)), we must have \( y = m_k \). In view of Lemma 6(iii), this means \( m_{k-1} = m_0 \). Thus \( X = \{m_0, m_1\} \). Again, by (WB1), there is a \( z \in X \) with \( (m_1, m_1) \in \sigma(z) \) from which \( m_1 = z \) follows. Thus \( m_0 = m_1 \) which contradicts \( T \neq X \); hence \( X \) must be infinite.

It should be mentioned here that in general for \( T \) a well-behaved arithmetic convolution type, \( C(A, T) \) 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.

The identity \( t \) is the only unit in the semigroup \( (X, \ast) \). In view of the algebraic structure on the index set, it is possible to define divisibility and all the associated notions in the usual way: For \( x, y \in X \), we say \( x \) divides \( y \) in \( X \), written as \( x \mid y \), if there is a \( z \in X \) with \( y = x \ast z \). Care should be taken with this notation. When we write \( x \mid y \) it is as defined here with respect to the operation \( \ast \) and if we want divisibility of integers in the usual sense, it will explicitly be stated. An element \( p \in X \) is called \( \sigma \)-irreducible if \( p \notin T \) and \( |\sigma(p)| = 2 \), i.e. \( \sigma(p) = \{(p, t), (t, p)\} \); \( p \) is called \( \sigma \)-prime if \( p \notin T \) and whenever \( p \mid a \ast b \), then \( p \mid a \) or \( p \mid b \). Any \( \sigma \)-prime element of \( X \) is also \( \sigma \)-irreducible, but not conversely. It can also be shown that every chain of distinct elements \( a_1, a_2, a_3, ... \) in \( X \) with \( a_{i+1} \mid a_i \) for all \( i \) must terminate. As is then well known, if it is assumed that every \( \sigma \)-irreducible element of \( X \) is
also σ-prime, then every \( x \in X, x \neq t \), has a unique factorization (up to order) as \( x = p_1 * p_2 * p_3 * \ldots * p_k \) for \( \sigma \)-irreducibles \( p_1, p_2, p_3, \ldots, p_k, k \geq 1 \), in \( X \).

From the above we know that a well-behaved arithmetic convolution type \( \mathcal{T} = (X, \sigma) \) either has an infinite index set or an index set with precisely one element. We fix the notation for \( X \) as \( X = \{m_0, m_1, m_2, \ldots \} \) with \( t = m_0 < m_1 < m_2 < \ldots \). Of course, it may happen that \( X = \{m_0\} \). In general the elements of \( \sigma(x) \) are not known. What we do know is that for all \( x \in X - T \), \( \sigma(x) \) contains at least the two elements \((x, t)\) and \((t, x)\), \( \sigma(m_0) = \{(m_0, m_0)\} \) and \( \sigma(m_1) = \{(m_0, m_1), (m_1, m_0)\} \). This means, whenever \(|X| \geq 2\), that \( X \) has at least one \( \sigma \)-irreducible element namely \( m_1 \).

On occasion, the following partition of \( X \) with \(|X| \geq 2\) will be useful. For \( k \geq 1 \), choose \( m_k \in X \) fixed and let \( X_k = \{x \in X \mid m_k \mid x\} \). Then \( m_k \in X_k \) since \( m_k * t = m_k, m_k \leq x \) for all \( x \in X_k \) and \( t \in \overline{X_k} := X - X_k \). We will take \( X_k = \{s_1, s_2, s_3, \ldots \} \) and \( \overline{X_k} = \{r_1, r_2, r_3, \ldots \} \) with \( m_k = s_1 < s_2 < s_3 < \ldots \) and \( t = r_1 < r_2 < r_3 < \ldots \). For any \((u, v) \in \sigma(r_i)\) with \( r_i \in \overline{X_k} \), also \( u \) and \( v \) must be in \( \overline{X_k} \). Indeed, if, for example \( u \in X_k \), then \( m_k \mid u \) and \( u \mid r_i \) which gives the contradiction \( m_k \mid r_i \). In view of this, \( \mathcal{T}_k := (X_k, \sigma_k) \) is an arithmetical convolution type where \( \sigma_k(r_i) = \sigma(r_i) \) for all \( r_i \in \overline{X_k} \). If \( \mathcal{T} = (X, \sigma) \) is a well-behaved arithmetic convolution type, then the arithmetical convolution type \( \mathcal{T}_k := (X_k, \sigma_k) \) will satisfy conditions (WB2) and (WB3) but it need not be well-behaved. For example, let \( X = \mathbb{Z}_0^+ \) and \( \sigma(n) = \{(i, j) \mid i + j = n\} \) for the Cauchy product convolution type. Choose any \( k \geq 2 \). Then \( X_k = \{k, k+1, k+2, \ldots \} \) with \( \overline{X_k} = \{0, 1, 2, \ldots, k-1\} \) and there is no \( u \in \overline{X_k} \) with \((k-1, k-1) \in \sigma_k(u) \); hence (WB1) is not satisfied. Exactly when \( \mathcal{T}_k \) will be well-behaved, is given by the next result.

**Proposition 8.** For a well-behaved arithmetic convolution type \( \mathcal{T} = (X, \sigma) \) and \( \mathcal{T}_k := (X_k, \sigma_k) \) as defined above, \( \mathcal{T}_k \) is well-behaved if and only if \( m_k \) is a \( \sigma \)-prime element of \( X \).

**Proof.** Suppose \( \mathcal{T}_k \) is well-behaved and \( m_k \) is not \( \sigma \)-prime in \( X \). This means there are \( a, b \in X \) such that \( m_k \mid a \cdot b \) but \( m_k \nmid a \) and \( m_k \nmid b \). Then both \( a \) and \( b \) are in \( X_k \) and since, by assumption, \( \mathcal{T}_k \) is well-behaved, there is an \( u \in X_k \) with \( a \cdot b = u \). But this contradicts \( m_k \mid a \cdot b \).

Suppose \( m_k \) is \( \sigma \)-prime. Let \( u, v \in \overline{X_k} \). Since \( \mathcal{T} \) is well-behaved, there is a \( w \in X \) with \((u, v) \in \sigma(w)\). If \( w \in X_k \), then \( m_k \mid u \cdot v \) and so \( m_k \mid u \) or \( m_k \mid v \); both not possible. Hence \( x \in \overline{X_k} \) and we may conclude that \( \mathcal{T}_k \) is well-behaved. \( \square \)

For a well-behaved arithmetic convolution type \( \mathcal{T} = (X, \sigma) \), \( m_k \in X \) fixed with \( k \geq 1 \) and a ring \( A \), let \( C_k(A) \) denote the convolution ring \( C_k(A, \mathcal{T}_k) \). The mapping \( \pi_k : C(A) \rightarrow C_k(A) \) defined by \( \pi_k(f) = f_k \) where \( f_k \) denotes the restriction of \( f \) to \( \overline{X_k} \), is a surjective ring homomorphism with \( \ker \pi_k = \{f \in C(A) \mid f(r_i) = 0 \text{ for all } r_i \in \overline{X_k}\} \). This ideal will be described by a mapping \( e_k \) defined as follows. Let \( A \) be a ring with identity and let \( k \geq 0 \).
Define \( e_k : X \rightarrow A \) by \( e_k(x) = \begin{cases} 1 & \text{if } x = m_k \\ 0 & \text{otherwise} \end{cases} \). When \( k = 0 \), \( e_0 \) is the identity \( e_0 = \iota_1 \) in \( C(A) \). It can be verified that if \( m_i \ast m_j = m_k \), then \( e_i e_j = e_k \) in \( C(A) \). Moreover, for any \( f \in C(A) \) and \( x \in X \),

\[
(e_k f)(x) = \begin{cases} f(s) & \text{if } m_k \ast s = x \\ 0 & \text{otherwise} \end{cases}
\]

**Proposition 9.** Let \( T = (X, \sigma) \) be a well-behaved arithmetic convolution type, let \( k \geq 1 \) and let \( A \) be a commutative ring with identity. Let \( g \in C(A) \). Then \( g(r_i) = 0 \) for all \( r_i \in \overline{X}_k \) if and only if \( e_k \mid g \) in the ring \( C(A) \).

**Proof.** If \( g = he_k \) for some \( h \in C(A) \), then for any \( r_i \in \overline{X}_k \), \( g(r_i) = \sum_{(r,s) \in \sigma(r_i)} h(r)e_k(s) = 0 \). The reason for this last equality is that for all \( (r,s) \in \sigma(r_i) \), both \( r \) and \( s \) are in \( \overline{X}_k \) and \( m_k \in X_k \). Conversely, suppose \( g(r_i) = 0 \) for all \( r_i \in \overline{X}_k \). For every \( s_i \in X_k \) there is a unique \( u_i \in X \) such that \( m_k \ast u_i = s_i \). Since any \( x \in X \) determines such an \( s_i \) by \( s_i = m_k \ast x \), we have that \( X = \{ u \mid m_k \ast u = s \} \) and the function \( h : X \rightarrow A \) with \( h(u_i) = g(s_i) \) is well-defined. We show \( e_k h = g : \) For any \( r_i \in \overline{X}_k \), \( (e_k h)(r_i) = 0 = g(r_i) \). For \( s_i \in X_k \), \( (e_k h)(s_i) = \sum_{(r,s) \in \sigma(s_i)} e_k(r)h(s) = e_k(m_k)h(u_i) = 1g(s_i) = g(s_i) \). Thus \( e_k h = g \) as required. \( \square \)

**Corollary 10.** Let \( T = (X, \sigma) \) be a well-behaved arithmetic convolution type, let \( k \geq 1 \) and let \( A \) be a commutative ring with identity. Then \( \ker \pi_k = \langle e_k \rangle \) where the latter denotes the ideal in \( C(A) \) generated by \( e_k \).

Another result that will be useful later, gives a relationship between \( \sigma \)-prime elements in \( X \) and prime elements in \( C(A) \). It should be mentioned that whenever we consider \( m_k \in X, k \geq 1 \) or an \( X_k \) without specifying the cardinality of \( X \), we implicitly assume that \( X \) has cardinality greater than \( 1 \).

**Proposition 11.** Let \( T = (X, \sigma) \) be a well-behaved arithmetic convolution type and let \( A \) be an integral domain. If \( m_k, k \geq 1 \), is a \( \sigma \)-prime element in \( X \), then \( e_k \) is a prime element of the ring \( C(A) \).

**Proof.** Let \( m_k \) be a \( \sigma \)-prime element in \( X \). Since \( e_k(m_0) = 0 \), \( e_k \) is not a unit in \( C(A) \). Let \( f, g \in C(A) \) with \( e_k \mid fg \) in \( C(A) \), say \( fg = e_k h \) for some \( h \in C(A) \). If \( g(r_i) = 0 \) for all \( r_i \in \overline{X}_k \), then by Proposition 9 \( e_k \mid g \) and we are done; suppose thus \( g(r_i) \neq 0 \) for some \( r_i \). Choose \( r_i \in \overline{X}_k \) minimal with respect to \( g(r_i) \neq 0 \). Then \( g(m_0) = g(r_1) = g(r_2) = \ldots = g(r_{l-1}) = 0 \) (recall that we took \( r_1 = m_0 \)). We will show \( f(r_i) = 0 \) for all \( r_i \in \overline{X}_k \) from which \( e_k \mid f \) will follow (Proposition 9). For any \( x \in X \),
\[
\sum_{(r, s) \in \sigma(x)} f(r)g(s) = (fg)(x) \\
= (e_k h)(x) \\
= \begin{cases} 
  h(s) & \text{if } (r, s) \in \sigma(x), r = m_k \\
  0 & \text{otherwise} \\
  h(u_i) & \text{if } x = s_i, m_k \cdot u_i = s_i \\
  0 & \text{otherwise} 
\end{cases}
\]

Hence \(0 = (fg)(r_t) = f(m_0)g(r_t) + \sum \{ f(r)g(s) \mid (r, s) \in \sigma(r_t), r \neq m_0 \} \).

For \((r, s) \in \sigma(r_t), r \neq m_0\), we have \(s < r_t\) and \(s = r_i\) for some \(r_i \in \overline{X_k}\). Hence \(g(s) = 0\) and thus \(f(m_0)g(r_t) = 0\). Since \(A\) is an integral domain, \(f(r_i) = f(m_0) = 0\) follows. Let \(n \geq 2\) and suppose \(f(r_1) = f(r_2) = \ldots = f(r_{n-1}) = 0\).

We show also \(f(r_n) = 0\). Let \(r_n \cdot r_t = x\). Since \(m_k\) is \(\sigma\)-prime, \(x \in \overline{X_k}\) (cf. Proposition 8), say \(x = r_j\). Now \(0 = (fg)(r_j) = \sum_{(r, s) \in \sigma(r_j)} f(r)g(s) = f(m_0)g(r_j) + \sum \{ f(r)g(s) \mid (r, s) \in \sigma(r_j), m_1 \leq r < r_n, r_j \geq s > r_t \} + f(r_n)g(r_t) + \sum \{ f(r)g(s) \mid (r, s) \in \sigma(r_j), r_n < r \leq r_j, m_0 \leq s < r_t \} + f(r_j)g(m_0)\).

For \((r, s) \in \sigma(r_j)\). Then both \(r\) and \(s\) are in \(\overline{X_k}\). For \(m_0 \leq r < r_n\), we have \(f(r) = 0\) since each such \(r\) is of the form \(r = r_i < r_n\) for some \(r_i \in \overline{X_k}\). For \(r_1 \leq s < r_t\), we have \(g(s) = 0\) since \(s = r_j \in \overline{X_k}\) for some \(j\). Hence \(f(r_n)g(r_t) = 0\). But \(g(r_i) \neq 0\), so \(f(r_n) = 0\). We thus conclude that \(f(r_i) = 0\) for all \(r_i \in \overline{X_k}\).

6. Factorization

Next we discuss factorization and related matters in arithmetic convolution rings. Our results will give a unified treatment of many results that have been proved separately for, especially, the Cauchy Product and the Dirichlet Product. Factorization is usually considered in integral domains; so to ensure that \(C(A)\) is an integral domain whenever \(A\) is, we henceforth assume that \(T\) is a well-behaved arithmetic convolution type. Throughout this section, unless mentioned otherwise, \(A\) will be an integral domain. The first few results show some of the interaction between prime and irreducible elements in \(A\) and \(C(A)\).

Proposition 12. Let \(T\) 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 \(f(m_0)\) irreducible in \(A\), then \(f\) is irreducible in \(C(A)\).

Proof. (i) If \(b\) is irreducible in \(A\), then \(b \neq 0\) and it is not a unit in \(A\) and subsequently also not in \(C(A)\). Suppose \(b = fg\) for some \(f, g \in C(A)\) with \(f\) and \(g\) non-units in \(C(A)\). Then \(f(m_0)\) and \(g(m_0)\) are non-units in \(A\) with \(b = (fg)(m_0) = f(m_0)g(m_0)\); a contradiction.
(ii) Let $b$ be prime in $A$. Let $f, g \in C(A)$ with $b | fg$, say $fg = bh$ for some $h \in C(A)$. Suppose $b \nmid g$. For every $x \in X, bh(x) = \sum_{(r,s)\in \sigma(x)} b(r)h(s) = (bh)(x) = (fg)(x) = \sum_{(r,s)\in \sigma(x)} f(r)g(s)$. Let $G = \{x \in X \mid b$ does not divide $g(x)\}$. If $G = \emptyset$, then $b | g(x)$ in $A$ for all $x \in X$; say $g(x) = bw_x$ for $w_x \in A$. Define $w : X \to A$ by $w(x) = w_x$ for all $x \in X$. Then $w \in C(A)$ and $g = bw$, i.e. $b | g$; a contradiction. Thus $G \neq \emptyset$. Let $m = \min G$. Now $(fg)(m) = f(m_0)g(m) + \sum\{f(r)g(s) \mid (r,s) \in \sigma(m), r \neq m_0\}$. Since $b | fg$ and $b | g(s)$ for all $(r,s) \in \sigma(m), r \neq m_0$ by the definition of $m$, it follows that $b | f(m_0)$. Let $k \geq 0$ and suppose $b | f(m_i)$ for $i = 0, 1, 2, ..., k - 1$. We show $b | f(m_k)$. Let $m_t = m_k*m$. Then $bh(m_t) = f(m_k)g(m) + \sum\{f(r)g(s) \mid (r,s) \in \sigma(m_t), r < m_k\} + \sum\{f(r)g(s) \mid (r,s) \in \sigma(m_t), r > m_k\}$. If $(r,s) \in \sigma(m_t)$ and $r < m_k$, then $b | f(r)$ while if $r > m_k$, then $s < m$ and so $b | g(s)$. Hence $b | f(m_k)g(m)$ and thus $b | f(m_k)$. We conclude that $b | f(x)$ for all $x \in X$ and thus $b | f$.

(iii) Since $f(m_0)$ is irreducible in $A$, it is not a unit in $A$ and so $f$ is not a unit in $C(A)$. Suppose $f = gh$ for some $g, h \in C(A)$. Then $f(m_0) = g(m_0)h(m_0)$ and so one of $g(m_0)$ or $h(m_0)$ must be a unit in $A$. This means either $g$ or $h$ must be a unit in $C(A)$.

The converse of (iii) is not true; for an example see [1].

**Proposition 13.** Let $T$ be a well-behaved arithmetic convolution type and let $A$ be an integral domain. Let $f \in C(A)$ with $f(m_0) = ab$ where $a$ and $b$ are non-units in $A$ with $aA + bA = A$. Then $f$ is reducible in $C(A)$.

**Proof.** We define two non-units $g$ and $h$ in $C(A)$ with $f = gh$. Let $g(m_0) = a$ and $h(m_0) = b$. This will ensure that $g$ and $h$ will not be units in $C(A)$. Since $f(m_1) \in A = aA + bA$, choose $h(m_1), g(m_1) \in A$ with $f(m_1) = ah(m_1) + bg(m_1)$. Then $f(m_1) = \sum g(r)h(s)$ since $\sigma(m_1) = \{(m_0,m_1),(m_1,m_0)\}$. Note that if $(r,s) \in \sigma(m_2)$ with $r \neq m_0$ and $s \neq m_0$, then $r = m_1 = s$. Thus $f(m_2) - \sum\{g(r)h(s) \mid (r,s) \in \sigma(m_2), r \neq m_0, s \neq m_0\} \in A = aA + bA$ makes sense (even though the sum could be empty) and we can choose $h(m_2), g(m_2) \in A$ with $f(m_2) - \sum\{g(r)h(s) \mid (r,s) \in \sigma(m_2), r \neq m_0, s \neq m_0\} = ah(m_2) + bg(m_2)$. Then $f(m_2) = \sum g(r)h(s)$. Suppose $g(m_i), h(m_i)$ have been defined for $i = 0, 1, 2, ..., k$ with $f(m_k) = \sum g(r)h(s)$. As above, choose $h(m_{k+1}), g(m_{k+1}) \in A$ with $f(m_{k+1}) - \sum\{g(r)h(s) \mid (r,s) \in \sigma(m_k), r \neq m_0, s \neq m_0\} = ah(m_{k+1}) + bg(m_{k+1})$. Then $f(m_{k+1}) = \sum g(r)h(s)$. We conclude that $b | f(x)$ for all $x \in X$ and thus $b | f$.

The converse of (iii) is not true; for an example see [1].

**Proposition 13.** Let $T$ be a well-behaved arithmetic convolution type and let $A$ be an integral domain. Let $f \in C(A)$ with $f(m_0) = ab$ where $a$ and $b$ are non-units in $A$ with $aA + bA = A$. Then $f$ is reducible in $C(A)$.

**Proof.** We define two non-units $g$ and $h$ in $C(A)$ with $f = gh$. Let $g(m_0) = a$ and $h(m_0) = b$. This will ensure that $g$ and $h$ will not be units in $C(A)$. Since $f(m_1) \in A = aA + bA$, choose $h(m_1), g(m_1) \in A$ with $f(m_1) = ah(m_1) + bg(m_1)$. Then $f(m_1) = \sum g(r)h(s)$ since $\sigma(m_1) = \{(m_0,m_1),(m_1,m_0)\}$. Note that if $(r,s) \in \sigma(m_2)$ with $r \neq m_0$ and $s \neq m_0$, then $r = m_1 = s$. Thus $f(m_2) - \sum\{g(r)h(s) \mid (r,s) \in \sigma(m_2), r \neq m_0, s \neq m_0\} \in A = aA + bA$ makes sense (even though the sum could be empty) and we can choose $h(m_2), g(m_2) \in A$ with $f(m_2) - \sum\{g(r)h(s) \mid (r,s) \in \sigma(m_2), r \neq m_0, s \neq m_0\} = ah(m_2) + bg(m_2)$. Then $f(m_2) = \sum g(r)h(s)$. Suppose $g(m_i), h(m_i)$ have been defined for $i = 0, 1, 2, ..., k$ with $f(m_k) = \sum g(r)h(s)$. As above, choose $h(m_{k+1}), g(m_{k+1}) \in A$ with $f(m_{k+1}) - \sum\{g(r)h(s) \mid (r,s) \in \sigma(m_k), r \neq m_0, s \neq m_0\} = ah(m_{k+1}) + bg(m_{k+1})$. Then $f(m_{k+1}) = \sum g(r)h(s)$. We conclude that $b | f(x)$ for all $x \in X$ and thus $b | f$.
\[ m_0, s \neq m_0 \} = ah(m_{k+1}) + bg(m_{k+1}). \] Then \[ f(m_{k+1}) = \sum_{(r,s) \in \sigma(m_{k+1})} g(r)h(s). \]

By induction the result follows. \[ \square \]

In an integral domain \( A \) with \( a, b \in A \), an element \( d \) is called a greatest common divisor (gcd) of \( a \) and \( b \) if \( d \mid a \) and \( d \mid b \) and whenever \( c \mid a \) and \( c \mid b \) for some \( c \in A \), then \( c \mid d \). In a unique factorization domain (UFD), a gcd of \( a \) an \( b \) will always exist and it is unique up to associates. In such a case, \( a \) and \( b \) are called relatively prime if the gcd of \( a \) and \( b \) is 1. Clearly, if \( aA + bA = A \), then \( a \) and \( b \) are relatively prime and in a principal ideal domain (PID), \( aA + bA = A \) if and only if \( a \) and \( b \) are relatively prime.

Recall, for a field \( A \), 0 \( \neq f \in C(A) \) is a unit if and only if \( f(m_0) \neq 0 \). Hence, if \( 0 \neq g \in C(A) \) is a non-unit and \( X \) contains a \( \sigma \)-irreducible element \( m \) with \( g(m) \neq 0 \), then \( g \) is irreducible in \( C(A) \). If not, then \( g = fh \) for non-units \( f \) and \( h \) in \( C(A) \). This means \( f(m_0) = 0 = h(m_0) \). But \( 0 \neq g(m) = f(m)h(m_0) + f(m_0)h(m) = 0 \); a contradiction.

**Proposition 14.** Let \( T \) be a well-behaved arithmetic convolution type and let \( A \) be an integral domain. Let \( f \in C(A) \) with \( f(m_0) = b^k \) where \( b \in A \) is prime and \( k \geq 1 \). If \( b \nmid f(m_1) \), then \( f \) is irreducible in \( C(A) \).

**Proof.** For \( k = 1 \) the result follows from Proposition 12(iii); suppose thus \( k \geq 2 \). If \( f = gh \) for two non-units \( g, h \in C(A) \), then \( b^k = g(m_0)h(m_0) \) and so \( b \mid g(m_0) \) or \( b \mid h(m_0) \). Suppose \( b \mid g(m_0) \). Choose \( r \geq 1 \) maximal with respect to \( g(m_0) = b^r u \) with \( u \in A \) and \( b \nmid u \). Now \( r < k \), for if \( r \geq k \), then \( b^k = b^r uh(m_0) \). Then \( 1 = (b^{k-r}u)h(m_0) \) which makes \( h(m_0) \) and then also \( h \) a unit. Hence \( r < k \) and so \( b \mid h(m_0) \). Suppose thus \( h(m_0) = b^rv \) with \( v \in A \), \( b \nmid v \) and \( r + s = k \), say \( r \leq s \). Then \( b^k = g(m_0)h(m_0) = b^kuv \) and \( u \) and \( v \) units in \( A \) follow. Now \( f(m_1) = g(m_1)h(m_0) + g(m_0)h(m_1) = b^r(g(m_1)b^{s-r}v + uh(m_1)) \) which contradicts \( b \nmid f(m_1) \). Hence \( f \) is irreducible. \[ \square \]

**Proposition 15.** Let \( T \) be a well-behaved arithmetic convolution type and let \( A \) be an integral domain. If \( A \) has acc on principal ideals, then so does \( C(A) \).

**Proof.** For \( |X| = 1 \) the result is clear; suppose \( |X| \geq 2 \). Let \( \langle f_1 \rangle \subseteq \langle f_2 \rangle \subseteq \ldots \) be an ascending chain of principal ideals in \( C(A) \). Then for every \( i < j \), there exists a \( g_{i,j} \in C(A) \) with \( f_i = f_j g_{i,j} \). If \( f_i = 0 \) for all \( i \geq 1 \), we are done; suppose thus \( f_n(m_k) \neq 0 \) for some \( k \geq 0, n \geq 1 \). Choose \( k \geq 0 \) minimal with respect to \( f_j(m_0) = f_j(m_1) = \ldots = f_j(m_{k-1}) = 0 \) for all \( j \geq 1 \) but with \( f_i(m_k) \neq 0 \) for some \( i \geq 1 \). Let \( n \) be minimal amongst these \( i \). Thus also \( f_1(m_k) = f_2(m_k) = \ldots = f_{n-1}(m_k) = 0 \).

Since \( f_i(m_k) = \sum_{(r,s) \in \sigma(m_k)} f_{i+1}(r)g_{i,i+1}(s) = f_{i+1}(m_k)g_{i,i+1}(m_0) \), because \( f_j(r) = 0 \) for all \( j \geq 1 \) and \( r < m_k \), we have an ascending chain of principal ideals \( \langle f_1(m_k) \rangle \subseteq \langle f_2(m_k) \rangle \subseteq \ldots \) in \( A \). By the assumption on \( A \), there is a \( t \geq 1 \) with \( \langle f_{t+p}(m_k) \rangle = \langle f_t(m_k) \rangle \) for all \( p \geq 0 \). Note that \( t \geq n \), for
if $t < n$, then $f_t(m_k) = 0$ and so $f_{t+p}(m_k) = 0$ for all $p \geq 0$, i.e. also $f_n(m_k) = 0$; a contradiction. Hence $t \geq n$ which also means $f_t(m_k) \neq 0$.

For all $p \geq 0$, there is a $u_p \in A$ with $f_{t+p}(m_k) = f_t(m_k)u_p$. But $f_t(m_k) = (f_{t+p}g_{t,t+p})(m_k) = f_{t+p}(m_k)g_{t,t+p}(m_0)$ because $f_j(r) = 0$ for all $r < m_k$ and $j \geq 1$. Thus $f_t(m_k) = f_{t+p}(m_k)u_p g_{t,t+p}(m_0)$ from which $g_{t,t+p}(m_0)$ a unit in $A$ and thus $g_{t,t+p}$ a unit in $C(A)$ follow. Since $f_t = f_{t+p}g_{t,t+p}$ for all $p \geq 0$, we conclude that $\langle f_t \rangle = \langle f_{t+1} \rangle = \langle f_{t+2} \rangle = \ldots$.

Let $E = \{e_k \mid m_k \in X \text{ is } \sigma\text{-prime}\}$ and let $\mathcal{E} = \{\epsilon \mid \epsilon \text{ is a finite product of elements from } E\}$. The set $E$ could be finite, even empty, but it could also be infinite. If $E \neq \emptyset$, let $A[[E]]$ denote the ring of formal power series over $A$ in the commuting indeterminates $e_k \in E$. A typical element of $A[[E]]$ is of the form $f = \sum_{i=0}^{\infty} f_i \epsilon_i$ where $f_i \in A$, $\epsilon_i \in \mathcal{E}$ for $i \geq 1$ and $\epsilon_0 = 1$. Then:

**Proposition 16.** Let $T$ be a well-behaved arithmetic convolution type and let $A$ be an integral domain. Suppose every $\sigma$-irreducible element in $X$ is $\sigma$-prime and that $X$ has at least one $\sigma$-irreducible element. Then $C(A) \cong A[[E]]$.

**Proof.** Recall from Section 3 that, in view of the assumptions on the index set, every $m \in X$ has a unique factorization (up to order) as $m = p_1 \ast p_2 \ast \ldots \ast p_{k_m}$ for some $\sigma$-primes $p_i$. Let $\epsilon(m) = e_{p_1}e_{p_2} \ldots e_{p_{k_m}}$ for each $m \in X$ where $e_{p_i} \in E$. Note that $\epsilon(m \ast n) = \epsilon(m)\epsilon(n)$ for all $m, n \in X$. Define $\theta : C(A) \to A[[E]]$ by $\theta(f) = \sum_{m \in X} f(m)\epsilon(m)$ for each $f \in C(A)$. It can be verified that $\theta$ is well-defined, injective, surjective and preserves addition. Also, for $f, g \in C(A)$:

$$\theta(fg) = \sum_{m \in X} (fg)(m)\epsilon(m)$$

$$= \sum_{i=0}^{\infty} \sum_{r \ast s = m_i} f(r)g(s)\epsilon(m_i)$$

$$= \sum_{i=0}^{\infty} \sum_{r \ast s = m_i} f(r)g(s)\epsilon(r_i)\epsilon(s_i) \text{ since } \epsilon(m_i) = \epsilon(r_i)\epsilon(s_i)$$

$$= \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} f(m_i)g(m_j)\epsilon(m_i)\epsilon(m_j)$$

$$= \left( \sum_{i=0}^{\infty} f(m_i)\epsilon(m_i) \right) \left( \sum_{j=0}^{\infty} g(m_j)\epsilon(m_j) \right)$$

$$= \theta(f)\theta(g)$$

as required. □

The Cauchy Product has only one $\sigma$-prime (namely 1) and $C(A) \cong A[[x]]$. The Dirichlet Product has infinitely many $\sigma$-primes (the prime numbers are exactly the $\sigma$-primes) and $C(A) \cong A[[x_1, x_2, x_3, \ldots]]$; both these are well-known
Lemma 17. Let $\mathcal{T} = (X, \sigma)$ be a well-behaved arithmetic convolution type.

(i) Suppose the index set $X$ has a unique $\sigma$-irreducible element. Then it must also be $\sigma$-prime.

(ii) Suppose $m_k \in X$ is $\sigma$-prime. If $|X_k| = 1$, then $m_k$ is the only $\sigma$-irreducible element in $X$.

Proof. (i) Suppose $X$ contains a unique $\sigma$-irreducible which must $m_1$. We show that it is $\sigma$-prime: Suppose $m_1 \mid m_i \cdot m_j$. If $i = 0$ or $i = 1$, then $m_1 \mid m_j$ or $m_1 \mid m_i$ and we are done; suppose thus $i > 1$. Then $m_i$ is not $\sigma$-irreducible, say $m_i = m_r \cdot m_s$ for some $0 < r, s$. Hence both $m_r$ and $m_s$ are strictly less than $m_i$. If one of them is $\sigma$-irreducible, i.e. coincides with $m_1$, we are done; suppose thus $m_r$ is not $\sigma$-irreducible. The $m_r$ has a non-trivial factorization $m_r = m_u \cdot m_v$ with both $m_u$ and $m_v$ strictly less than $m_r$. We may repeat the previous argument. This process cannot be repeated indefinitely since $X$ has a lower bound; hence we conclude that $m_1$ is $\sigma$-prime.

(ii) Let $m_k \in X$ be $\sigma$-prime with $|X_k| = 1$. Then $X_k = \{m_0\}$ and $X = X - \{m_0\}$ which means $m_k \mid m$ for all $m_0 \neq m \in X$. Let $q \in X$ be any $\sigma$-irreducible. Then $q \neq t$ and $m_k \mid q$. Thus $q = m_k \cdot m$ for some $m \in X$. Since $q$ is $\sigma$-irreducible, this means $m = m_0$ and so $q = m_k$. \hfill \Box

Proposition 18. 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 $\sigma$-irreducible element.

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

Proof. Suppose $C(A)$ is a principal ideal domain. Firstly we show that $X$ has a unique $\sigma$-irreducible element. We already know that $\sigma(m_1) = \{(m_0, m_1), (m_1, m_0)\}$; suppose there is an $m_k \in X, k > 1$, with $\sigma(m_k) = \{(m_0, m_k), (m_k, m_0)\}$. For the mappings $e_1$ and $e_k$, consider the ideal $I = e_1C(A) + e_kC(A)$ of $C(A)$. By assumption there are $f, g, h \in C(A)$ such that $\langle h \rangle = I$, $e_k = hf$ and $e_1 = hg$. Also $h = e_1v + e_kv$ for some $u, v \in C(A)$. Since $k > 1$, $h(m_0) = 0$. Then $1 = e_k(m_k) = h(m_k)f(m_0) + h(m_0)f(m_k) = h(m_k)f(m_0)$ and so both $h(m_k)$ and $f(m_0)$ are non-zero. But $0 = e_k(m_1) = h(m_1)f(m_0) + h(m_0)f(m_1) = h(m_1)f(m_0)$ and so $h(m_1) = 0$. Thus $1 = e_1(m_1) = h(m_1)g(m_0) + h(m_0)g(m_1) = 0$; a contradiction. Hence $X$ has a unique $\sigma$-irreducible element $m_1$. Let $0 \neq a \in A$. We show $a$ is an unit. Let $I = \{f \in C(A) \mid f(m_0) \in aA\}$. Then $I$ is a non-zero ideal of $C(A)$ since $e_1 \in I$. By assumption, $I = \langle h \rangle$ for some $0 \neq h \in C(A)$. Since $h \in I$, $h(m_0) = au$ for some $u \in A$. Also $n_0(m_0) = a \in aA$.
and so $\iota_0 = hg$ for some $g \in C(A)$. Then $a = h(m_0)g(m_0) = \text{aug}(m_0)$. Hence $g(m_0)$ is a unit in $A$ and so $g$ is an unit in $C(A)$. Choose $f \in C(A)$ with $e_1 = hf$. Then $0 = e_1(m_0) = h(m_0)f(m_0) = \text{aug}(m_0)$ and thus $f(m_0) = 0$. Then $1 = e_1(m_1) = h(m_1)f(m_0) + h(m_0)f(m_1) = \text{aug}(m_1)$ and $a$ a unit follows.

$(ii) \Rightarrow (iii)$ follows from Proposition 16 and Lemma 17. $(iii) \Rightarrow (i)$ is part of the folklore of ring theory.

It is well-known that if $A$ is a PID, then $A[[x]]$ is a UFD. In view of the above result, this means that for a PID $A$ and a well-behaved arithmetic convolution type $T$ for which the index set has at least two elements and a unique $\sigma$-irreducible element, $C(A) \cong A[[x]]$ is a UFD. We know that in general if $A$ is a UFD, then $C(A)$ need not be a UFD - Samuel [4] has shown that $R[[x]]$ is not necessarily a UFD when $R$ is one. For the Dirichlet product, we know that there are infinitely many $\sigma$-primes, hence in this case $C(A)$ is never a PID.

For our final results, we retain the assumption that $T$ is a well-behaved arithmetic convolution type and choose $p \in X$ a $\sigma$-prime element. We recall both $X_p$ and $\overline{X}_p$ are non-empty, containing $p$ and $m_0$ respectively. Here, as may have been noted already, we deviate slightly from our earlier notation: taking $p = m_k$ and rather write $X_p, \overline{X}_p, e_p$, etc. in stead of $X_k, \overline{X}_k, e_k$, etc.

respectively. Using the usual arguments, it can be shown that any $m \in X$ can be written as $m = p^n \ast u$ for some $u \in X, p \nmid u$ and $n \geq 0$. Here $p^n$ means $p \ast p \ast \ldots \ast p$, $n$ times for $n \geq 1$ and $p^0 = m_0$. It can then be verified that $e_p(n) = \begin{cases} 1 & \text{if } m = p^n \\ 0 & \text{otherwise} \end{cases}$.

If we let $T_p := (\overline{X}_p, \sigma_p)$ where $\sigma_p(x) = \sigma(x)$ for all $x \in \overline{X}_p$, then $T_p$ is also a well-behaved arithmetic convolution type (Proposition 8); 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 $g \in C_p(A), f \in C(A)$. Moreover, any $f \in C(A)$ can be written as $f = \overline{f}^* + (f - \overline{f}^*)$ with $f - \overline{f}^* \in \ker \pi_p$ and $\overline{f}^* \in (0 : X_p)C(A) := \{h \in C(A) \mid h(x) = 0 \text{ for all } x \in X_p\}$.

**Proposition 19.** Let $T$ be a well-behaved arithmetic convolution type. Let $p \in X$ be a $\sigma$-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 $I = (f_1, f_2, \ldots, f_n)$, then $I_p = (\overline{f}_1, \overline{f}_2, \ldots, \overline{f}_n)$ and if $I_p = (g_1, g_2, \ldots, g_n)$, then
Thus, if we write $\langle g_1^*, g_2^*, \ldots, g_n^*, e_p \rangle$ if $e_p \in I$
\[ I = \begin{cases} 
\langle g_1^*, g_2^*, \ldots, g_n^*, e_p \rangle & \text{if } e_p \in I \\
\langle f_1, f_2, \ldots, f_n \rangle & \text{if } e_p \notin I \text{ and } f_i \in I \text{ with } \pi_p(f_i) = g_i.
\end{cases} \]

Proof. Since $\pi_p$ is surjective, the sufficiency is well-known. Suppose thus $I_p = \langle g_1, g_2, \ldots, g_n \rangle$, $g_i \in I_p = \pi_p(I) \subseteq C_p(A)$, say $g_i = \pi_p(f_i) = \overline{f_i}$ for some $f_i \in I$.

Suppose firstly $e_p \in I$. For any $g_i^*, \pi_p(f_i - g_i^*) = 0$; hence $f_i - g_i^* \in \ker \pi_p = \langle e_p \rangle \subseteq I$. Thus $g_i^* \in I$ and $\langle g_1^*, g_2^*, \ldots, g_n^*, e_p \rangle \subseteq I$ follows. On the other hand, any $f \in I$ can be written as $f = \overline{f} + (f - \overline{f})$ with $f - \overline{f} \in \ker \pi_p = \langle e_p \rangle$.

Then $\overline{f} = \overline{f} = \pi_p(\overline{f'}) = \pi_p(f) \in I_p$ and so $\overline{f} = \sum_{i=1}^n h_i g_i$ for some $h_i \in C_p(A)$.

From this it follows that $\overline{f} = \sum_{i=1}^n h_i g_i^*$ and so $f \in \langle g_1^*, g_2^*, \ldots, g_n^*, e_p \rangle$. We thus conclude that $I = \langle g_1^*, g_2^*, \ldots, g_n^*, e_p \rangle$ when $e_p \notin I$.

Suppose now $e_p \notin I$. Clearly $\langle f_1, f_2, \ldots, f_n \rangle \subseteq I$. For the converse inclusion, we first show that if $h \in I$, then $h = \sum r_i f_i + h_1 e_p$ for some $r_i \in C(A), h_1 \in \ker \pi_p = \langle e_p \rangle$.

For $h \in I$, $h = \overline{h} + (h - \overline{h})$ with $h - \overline{h} \in \ker \pi_p = \langle e_p \rangle$. Then $\overline{h} = \pi_p(\overline{h}) = \pi_p(h) \in I_p = \langle g_1, g_2, \ldots, g_n \rangle$, say $\overline{h} = \sum r'_i g_i$ for some $r'_i \in C_p(A)$. Choose $r_i \in C(A)$ with $\pi_p(r_i) = r'_i$. Then $\pi_p(\overline{h}) = \overline{h} = \pi_p(\sum_{i=1}^n r_i f_i)$, i.e. $\overline{h} - \sum_{i=1}^n r_i f_i \in \ker \pi_p$, say $\overline{h} - \sum_{i=1}^n r_i f_i = h_1 \notin \ker \pi_p$. Then $h_1 + (h - \overline{h}) \in \ker \pi_p = \langle e_p \rangle$, say $h_1 + h - \overline{h} = h_1 e_p$ for $h_1 \in C(A)$. Hence $h = \sum_{i=1}^n r_i f_i + h_1 e_p$. Since $h$ and $f_i$ are all in $I$, also $h_1 e_p \in I$. The ideal $I$ is prime with $e_p \notin I$, hence $h = \sum_{i=1}^n r_i f_i + h_1 e_p$ with $h_1 \in I$ as claimed.

For $h_1 \in I$, we may repeat this process to get $h_1 = \sum_{i=1}^n r^{(1)}_i f_i + h_2 e_p$, $h_2 \in I$.

Thus, if we write $r^{(0)}_i$ for $r_i$, we get $h = \sum_{i=1}^n (r^{(0)}_i + r^{(1)}_i e_p) f_i + h_2 e_p^2$. Continue in this way to get for any $t \geq 0$,

$$h = \sum_{i=1}^n (r^{(0)}_i + r^{(1)}_i e_p + \ldots + r^{(t)}_i e_p) f_i + h_{t+1} e_p^{t+1}.$$ Define a function $k_i : X \to A$ as follows: For $w \in X$, we know $w = p^{n_w} * m_w$ with $n_w \geq 0$ and $m_w \in \overline{X_p}$; let $k_i(w) = (r^{(0)}_i + r^{(1)}_i e_p + \ldots + r^{(n_w)}_i e_p)(w)$. Then $k_i \in C(A)$ and to conclude
the proof, we show \( h = \sum_{i=1}^{n} k_i f_i \). Let \( m \in X \), say \( m = p^t \ast s \) with \( s \in X_p \). Note that for any \( u, v \in X \) with \( m = u \ast v \), neither of \( u \) or \( v \) can be equal to \( p^{t+1} \); hence \( (h_{t+1}e_{p}^{t+1})(u) = 0 \). Thus
\[
\begin{align*}
    h(m) &= \left( \sum_{i=1}^{n} (r_i(0) + r_i(1) e_p + \ldots + r_i(t) e_p^t) f_i \right)(m) + (h_{t+1}e_{p}^{t+1})(m) \\
    &= \left( \sum_{i=1}^{n} (r_i(0) + r_i(1) e_p + \ldots + r_i(t) e_p^t) f_i \right)(m) \\
    &= \sum_{i=1}^{n} \sum_{m=u \ast v} (r_i(0) + r_i(1) e_p + \ldots + r_i(t) e_p^t)(u)f_i(v).
\end{align*}
\]

On the other hand, for any \( m = u \ast v \), \( u \) will be of the form \( u = p^j \ast w \) with \( 0 \leq j \leq t \) and \( w \in X_p \). This means \( k_i(u) = (r_i(0) + r_i(1) e_p + \ldots + r_i(t) e_p^t)(u) \). Since \( (h_{j+1}e_{p}^{j+1})(u) = (h_{j+2}e_{p}^{j+2})(u) = \ldots = (h_t e_{p}^{t})(u) = 0 \), \( k_i(u) = (r_i(0) + r_i(1) e_p + \ldots + r_i(t) e_p^t)(u) \) from which
\[
\begin{align*}
    \left( \sum_{i=1}^{n} k_i f_i \right)(m) &= \sum_{i=1}^{n} (k_i f_i)(m) \\
    &= \sum_{i=1}^{n} \sum_{m=u \ast v} k_i(u)f_i(v). \tag*{□}
\end{align*}
\]

For the Cauchy Product, there is a unique \( \sigma \)-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 \( I_1 := \{ a \in A \mid a = f(0) \text{ for some } f \in A[[x]] \} \) is a finitely generated ideal of \( A \). We conclude with a number of corollaries. The first uses a well-known theorem from Cohen. Both these quoted ring theory results can be found, for example, in Watkins [9].

**Corollary 20.** Let \( T \) be a well-behaved arithmetic convolution type. Let \( p \in X \) be a \( \sigma \)-prime element. For an integral domain \( A \), \( C_p(A) \) noetherian implies \( C(A) \) noetherian.

**Proof.** Let \( I \) be a prime ideal of \( C(A) \). Then \( I_p \) is finitely generated by assumption and by the previous result \( I \) is finitely generated. Thus \( C(A) \) is noetherian. \( \Box \)

**Corollary 21.** Let \( T \) be a well-behaved arithmetic convolution type. Let \( p \in X \) be a \( \sigma \)-prime element. If \( C_p(A) \) is a principal ideal domain, then \( C(A) \) is a unique factorization domain.

**Proof.** Let \( I \) be a prime ideal of \( C(A) \). If \( e_p \in I \), then \( I \) contains a prime element and we are done. Suppose \( e_p \notin I \). We know \( I_p \) is an ideal in \( C_p(A) \) and so \( I_p = \langle g \rangle \) for some \( g \in C_p(A) \). But then \( I = \langle f \rangle \) (by Proposition 19)
where $f \in C(A)$ with $\pi_p(f) = g$. Since $I$ is a prime ideal, we know $f$ is a prime element and we are done.

Corollary 20 may be called the arithmetic convolution ring version of the Hilbert Basis Theorem. For polynomial rings, its converse was given by Gilmer [2]; we conclude with the arithmetic convolution version.

**Proposition 22.** 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.

**Proof.** Let $C(A)$ be noetherian. Since $I$ an ideal of $A$ implies $C(I)$ an ideal of $C(A)$, it easily follows that $A$ is noetherian. Since $A$ is noetherian, to show that $A$ has an identity, it is sufficient to show that for any $b \in A$, also $b \in Ab$ holds. For each $i \geq 0$, define a function $f_i : X \to A$ by

$$f_i(x) = \begin{cases} b & \text{if } x = m_i \\ 0 & \text{otherwise} \end{cases}.$$  Then $\langle f_0 \rangle \subseteq \langle f_0, f_1 \rangle \subseteq \langle f_0, f_1, f_2 \rangle \subseteq \ldots$ is an ascending chain of ideals of $C(A)$. Since $C(A)$ is noetherian, there is an $n \geq 1$ such that $f_{n+1} \in \langle f_0, f_1, \ldots, f_n \rangle$. Thus $f_{n+1} = \sum_{i=0}^{n} g_i f_i + \sum_{i=0}^{n} k_i f_i$ for some $g_i \in C(A)$ and $k_i \in \mathbb{Z}$. Then

$$b = f_{n+1}(m_{n+1})$$

$$= \sum_{i=0}^{n} \sum_{r \in \sigma(m_{n+1})} \{g_i(r)f_i(s) | (r, s) \in \sigma(m_{n+1})\} + \sum_{i=0}^{n} \{k_i f_i(m_{n+1})\}$$

$$= \sum_{i=0}^{n} \sum_{r \in \sigma(m_{n+1})} \{g_i(r)b | (r, m_i) \in \sigma(m_{n+1})\}$$

$$+ \sum_{i=0}^{n} \sum_{s \neq m_i} \{g_i(r)(s) | (r, m_i) \in \sigma(m_{n+1})\} + 0$$

$$= \sum_{i=0}^{n} \{g_i(r)b | (r, m_i) \in \sigma(m_{n+1})\}$$

(this sum has at least one term since $(m_{n+1}, m_0) \in \sigma(m_{n+1})$)

$$= ab \text{ where } a = \sum_{i=0}^{n} \{g_i(r) | (r, m_i) \in \sigma(m_{n+1})\}$$

**Acknowledgement.** Financial support through grant IG/SCI/DOMS/11/04 from Sultan Qaboos University is hereby kindly acknowledged.

**References**


*Received: February, 2011*