ROMANIAN JOURNAL OF MATHEMATICS AND COMPUTER SCIENCE, 2013, VOLUME 3, ISSUE 2, p.155-159

DISCRETE CONVOLUTION RINGS

HORST BRUNOTTE

Abstract. The notion of a discrete convolution ring is introduced. Some examples and results on zero-divisors and units of this class of rings are presented.

1. Introduction

Convolutions play important roles in many different areas of mathematics, e.g., functional analysis, probability theory, group theory, number theory or measure theory. Here we focus on purely algebraic aspects. In this context we mention that the notion of a convolution algebra appeared for instance in [3, 4, 1, 5].

The approach of [3] was generalized by M. El Bachraoui [2]; his work on convolution structures was motivated and inspired by algebraic logic. From another point of view a more general concept was pursued by S. Veldsman by defining convolution types. More specifically, he investigated radical theoretic properties of rings originating from apparently widely different ring constructions and suggested a new grouping of seemingly disparate ring constructions. To this end he introduced the notion of convolution rings in a very general algebraic setting and showed that many important ring constructions can be covered under this umbrella [6]. Furthermore, he investigated the influence of the convolution type on the corresponding convolution ring. In a subsequent paper S. Veldsman [7] defined a more specialized convolution type, namely an arithmetic convolution type thereby providing a unified treatment of many rings which have been called arithmetic.

In this short note we introduce the notion of a discrete convolution type which turns out to be a slight generalization of an arithmetic convolution type. Closely following the work of S. Veldsman we construct discrete convolution rings and present some examples and results on zero-divisors and units of this class of rings.

2. Definition and examples of arithmetic convolution rings

We introduce the following notion which essentially goes back to [7, 6] and refer the reader to [6] for a detailed discussion of the meaning and consequences of the properties listed below. In the following formal definition it is convenient to regard ρ as the convolution rule, I as the index set and T as the subset of trivial elements of I.

Definition 1. Let I be a non-empty subset of the set $\mathbb{Z}$ of rational integers, $\mathcal{S}$ a subset[1] of $\mathcal{P}(I)$ with $\mathcal{S} \neq \{I\}$ and $\rho : I \to \mathcal{P}(I \times I)$ and $\tau : I \times I \to \mathbb{Z}$ be mappings. The quadruple $\mathcal{T} = (I, \mathcal{S}, \rho, \tau)$ is called a discrete convolution type if it enjoys the following properties.

(C1) For all $S_1, S_2 \in \mathcal{S}$ there is an $S \in \mathcal{S}$ such that $S \subseteq S_1 \cap S_2$.

(C2) For all $S_1, S_2 \in \mathcal{S}$ there is an $S \in \mathcal{S}$ with the following property: For all $s \in S$ the relation $(i, j) \in \rho(s)$ implies either $i \in S_1$ or $j \in S_2$.

(C3) For all $i \in I$ we have $0 < \operatorname{Card} \rho(i) < \infty$ and

$$(r, s) \in \rho(i) \iff (s, r) \in \rho(i) \qquad (r, s \in I).$$

(C4) For all $i, j \in I$ we have $\tau(i, j) = \tau(j, i)$.

Date: October 3, 2013.

2010 *Mathematics Subject Classification.* 16S99, 13F99, 13F20, 13F25.

Key words and phrases. convolution, convolution rings, polynomial rings.

[1] $\mathcal{P}(X)$ denotes the set of all subsets of the set X.

(C5) For all $i \in I$, $(r,s) \in \rho(i)$ and $(p,q) \in \rho(r)$ there exists a unique $u \in I$ such that $(p,u) \in \rho(i)$, $(q,s) \in \rho(u)$ and

$$\tau(r,s)\tau(p,q) = \tau(p,u)\tau(q,s).$$

(C6) For all $i \in I$, $(p,q) \in \rho(i)$ we have $q = i$ provided p belongs to the set

$$T = \{t \in I \,:\, (t,t) \in \rho(t) \text{ and } \tau(t,j) = 1 \text{ for all } j \in I\}\ .$$

(C7) For every $i \in I$ there is a unique $t \in T$ such that $(t,i) \in \rho(i)$.

(C8) There is some $S \in \mathcal{S}$ such that $T \subseteq I \setminus S$.

We recall some straightforward observations from [6].

Remark 2. (i) Note that $T, \mathcal{S} \neq \emptyset$ in view of (C7) and (C8), respectively.

(ii) If $\emptyset \in \mathcal{S}$ then (C1), (C2) and (C8) are trivially satisfied.

(iii) If $T = I$ then $\tau = 1$.

(iv) Let $\tau = 1$, i.e., we have $\tau(i,j) = 1$ for all $i,j \in I$. This trivially implies

$$T = \{t \in I \,:\, (t,t) \in \rho(t)\}\ .$$

(v) Every discrete convolution type is a convolution type on $\mathbb{Z}$-algebras in the sense of [6, Definition 1.1].

(vi) Let (X,σ) be an arithmetic convolution type such that X contains a non-empty subset T as defined in [7, Section 2]. Then $(X, \{\emptyset\}, \sigma, 1)$ is a discrete convolution type.

In the remainder of this note we let $\mathcal{T} = (I, \mathcal{S}, \rho, \tau)$ be a discrete convolution type and R be a unital ring[2], i.e., we assume that R has a multiplicative identity element $1 \neq 0$. Following [6] we set

$$C(R,\mathcal{T}) = \{f : I \to R \,:\ \text{ there exists some } S \in \mathcal{S} \text{ such that } f(s) = 0 \text{ for all } s \in S\}$$

and define two operations on $C(R,\mathcal{T})$. For $f,g \in C(R,\mathcal{T})$ and $i \in I$ we set

$$(f+g)(i) = f(i) + g(i)\,,$$
$$(f \bullet g)(i) = \sum_{(s,t)\in\rho(i)} \tau(s,t) f(s) g(t)\,.$$

Proposition 3. (i) *$(C(R,\mathcal{T}), +, \bullet)$ is a unital ring with multiplicative identity element ι_1 where we define the mapping $\iota_r : I \to R$ by*

$$\iota_r(i) = \begin{cases} r & (i \in T) \\ 0 & (i \notin T) \end{cases}$$

for $r \in R$.

(ii) *The mapping $\iota : R \to C(R,\mathcal{T})$ given by $\iota(r) = \iota_r$ defines a ring monomorphism.*

(iii) *If R is commutative then $C(R,\mathcal{T})$ is commutative.*

Proof. (i), (ii) Clear by [6, Section 1].
(iii) Clear by [6, Proposition 1.4]. □

Based on these observations we call $C(R,\mathcal{T})$ the discrete convolution ring of type $\mathcal{T}$ over R; moreover, we regard R as a subring of $C(R,\mathcal{T})$ and identify r and ι_r. In view of Remark 2 (vi) this notion is a slight generalization of an arithmetic convolution ring (see [7] for the definition). Clearly, if I has cardinality 1 then $\mathcal{S} = \{\emptyset\}$ and $\tau = 1$, and $C(R,\mathcal{T})$ and R coincide. Thus we recall that any unital ring can be seen as an arithmetic convolution ring (see [7]).

Example 4. (i) As shown in [6, Section 2] direct products, polynomials, power series and Laurent series are examples of discrete convolution rings with $\tau = 1$.

[2]All rings in this note are associative.

ROMANIAN JOURNAL OF MATHEMATICS AND COMPUTER SCIENCE, 2013, VOLUME 3, ISSUE 2, p.155-159

(ii) The necklace rings [6, Section 2] are examples of discrete convolution rings of type $(\mathbb{N}_{>0}, \{\emptyset\}, \rho, \tau)$ with

$$\rho(i) = \{(k,\ell) \in \mathbb{N}_{>0} \times \mathbb{N}_{>0} \ : \ \operatorname{lcm}(k,\ell) = i\}$$

and $\tau(i,j) = \gcd(i,j)$ for $i,j \in \mathbb{N}_{>0}$. Here lcm and gcd denote the least common multiple and the greatest common divisor, respectively.

3. Zero-divisors and units in arithmetic convolution rings

Similarly as shown in [7, Section 3] for arithmetic convolutions rings $C(R,\mathcal{T})$ can have zero-divisors irrespective of whether R has or has not.

Proposition 5. *$C(R,\mathcal{T})$ has non-zero zero-divisors if one of the following two conditions is satisfied.*

(i) *There exist $p,q \in I$ such that $(p,q) \notin \rho(i)$ for every $i \in I$.*
(ii) *There exists an element $p \in I \setminus T$ such that $\tau(p,p) = 1$, $(p,p) \in \rho(p)$ and $(p,p) \notin \rho(i)$ for every $i \in I$.*

Proof. (i) Similarly as in the proof of [7, Proposition 2] we define the non-zero mappings

$$f(x) = \begin{cases} 1, & \text{if } x = p, \\ 0, & \text{otherwise} \end{cases} \qquad \text{and} \qquad g(x) = \begin{cases} 1, & \text{if } x = q, \\ 0, & \text{otherwise} \end{cases} \qquad (x \in I)$$

and check $f \bullet g = 0$.
(ii) The proof of [7, Proposition 2] can be copied. □

Analogously as in [7, Section 3] we introduce conditions on the discrete convolution type aiming at excluding zero-divisors in $C(R,\mathcal{T})$ which do not belong to R.

Definition 6. (i) We say that $\mathcal{T}$ fulfills the lower bound requirement if $I \setminus T$ has a lower bound in $\mathbb{Z}$ provided that $I \neq T$.
(ii) We say that $\mathcal{T}$ has the complementary ordering property if for all $i \in I$ and all $(r,s),(u,v) \in \rho(i)$ we have

$$r \leq u \iff s \geq v\,.$$

Remark 7. [7, Section 3] Suppose that $\mathcal{T}$ has the complementary ordering property.

(i) Let $i \in I$ and $(r,s),(u,v) \in \rho(i)$ such that $r < u$. Then we have $s > v$.
(ii) The second condition mentioned in Proposition 5 is not satisfied. More precisely, there does not exist an element $p \in I \setminus T$ such that

$$(p,p) \in \rho(p) \setminus \bigcup_{i \in I} \rho(i)\,.$$

We extend the notion of a well-behaved convolution type introduced in [7, Section 3] to our settings here.

Definition 8. [7, Section 3] $\mathcal{T}$ is called well-behaved if it satisfies the following three properties.

(i) $\mathcal{T}$ fulfills the lower bound requirement.
(ii) $\mathcal{T}$ has the complementary ordering property.
(iii) For all $i,j \in I$ there exists some $k \in I$ such that $(i,j) \in \rho(k)$.

Remark 9. [7, Section 3] Let $\mathcal{T}$ be well-behaved. Then $\operatorname{Card} T = 1$, i.e., I has exactly one trivial element. Moreover, none of the two conditions mentioned in Proposition 5 is satisfied.

As explained in [7] a well-behaved convolution type imposes a strong algebraic structure on the set I. We formulate the result [7, Proposition 7] as follows.

ROMANIAN JOURNAL OF MATHEMATICS AND COMPUTER SCIENCE, 2013, VOLUME 3, ISSUE 2, p.155-159

Proposition 10. *Let $\mathcal{T}$ be a well-behaved discrete convolution type. For any $i, j \in I$ there is a unique $k \in I$ such that $(i, j) \in \rho(k)$; in this case we write $k = i * j$. Moreover, $(I, *)$ is a commutative cancellative semigroup with the unique trivial element as identity. For all $i, j, k \in I$ the relation $i < j$ implies $i * k < j * k$. If $\operatorname{Card} I > 1$ then I is infinite.*

Proof. The proofs of [7, Lemma 6 and Proposition 7] hold under our prerequisites. □

The proof of [7, Proposition 4] extends to our settings in a straightforward manner and we record the result as follows.

Theorem 11. *Suppose that $\mathcal{T}$ is a well-behaved discrete convolution type, R has characteristic zero and $\tau(r, s) \neq 0$ for all $r, s \in I$. Then $C(R, \mathcal{T})$ has zero-divisors if and only if R has zero-divisors.*

In [7, Section 4] conditions were formulated which guarantee that $C(R, \mathcal{T})$ has more units than R. We extend this criterion to our settings here.

Theorem 12. *Let R be commutative and assume that $\mathcal{T}$ satisfies the lower bound requirement and the following two conditions.*

(i) *For all $t \in T$ we have $\rho(t) = \{(t, t)\}$.*
(ii) *Let $i, j, k \in I$ and $(i, j) \in \rho(k)$. If $i \notin T$ then $j < k$.*

Then $f \in C(R, \mathcal{T})$ is a unit if and only if $f(t)$ is a unit in R for all $t \in T$.

Proof. For the convenience of the reader we give an adapted version of the proof of [7, Proposition 5]. Note that $C(R, \mathcal{T})$ is commutative by Proposition 3.

Let $f \in C(R, \mathcal{T})$ be a unit and $g \in C(R, \mathcal{T})$ such that $f \bullet g = \iota_1$. Then we have

$$1 = \iota_1(t) = (f \bullet g)(t) = \tau(t, t) f(t) g(t) = f(t) g(t) \,,$$

thus $f(t)$ is a unit in R.

Conversely, let $f(t)$ be a unit in R for all $t \in T$ and put

$$g(t) := (f(t))^{-1} \qquad (t \in T). \tag{1}$$

If $T = I$ then in view of the properties of τ and condition (i) above $g : I \to R$ is a map with the required properties, and we are done.

Therefore, we now assume $T \neq I$. The lower bound requirement yields an element

$$m := \min(I \setminus T) \,,$$

and we now define $g(n)$ for $n \geq m$ by induction. By (C7) there is a unique $t \in T$ such that $(t, m) \in \rho(m)$, by (1) we can set

$$g(m) := -(f(t))^{-1} f(m) g(t) \,.$$

Clearly, $t \neq m$. We observe

$$\rho(m) = \{(t, m), (m, t)\} \,. \tag{2}$$

Indeed, assume $(r, s) \in \rho(m)$ such that $(r, s) \neq (t, m), (m, t)$. Again using (C7) we find $s \notin T$, hence $r < m$ by (C3) and condition (ii) above. But then $r \in T$ which implies the contradiction $s = m$ and $r = t$. From (2) and the properties of τ we infer

$$\begin{aligned} (f \bullet g)(m) &= \tau(t, m) f(t) g(m) + \tau(m, t) f(m) g(t) \\ &= -f(t)(f(t))^{-1} f(m) g(t) + f(m) g(t) \\ &= 0 \;=\; \iota_1(m) \;=\; (g \bullet f)(m) \,. \end{aligned}$$

Now we suppose that $g(i)$ has been defined for $m \leq i < n$. If $n \in T$ we are done by (1), therefore let $n \notin T$. Using (C7) we find some $t \in T$ such that we can write $\rho(m) = \{(r_1, s_1), \ldots, (r_k, s_k)\}$ with $k \geq 2$ and $r_1 = t,\ s_1 = n,\ r_2 = n$ and $s_2 = t$; here we use $n \neq t$. Condition (ii) above ensures that for $\ell > 2$ we have $r_\ell,\ s_\ell < n$, thus $g(r_\ell)$ and $g(s_\ell)$ are defined. It is easy to check that

$$g(n) := -(f(t))^{-1} \sum_{\ell=2}^{k} \tau(r_\ell, s_\ell) f(r_\ell) g(s_\ell)$$

satisfies

$$(f \bullet g)(n) = (g \bullet f)(n) = 0 = \iota_1(n) \ .$$

□

Specializing to well-behaved convolution types yields a characterization of units in discrete convolution rings.

Corollary 13. *Let R be commutative and assume that $\mathcal{T}$ is well-behaved. Then $f \in C(R, \mathcal{T})$ is a unit if and only if $f(t)$ is a unit in R for all $t \in T$.*

Proof. As already mentioned above [7, Lemma 6] holds under our prerequisites. Therefore the assertion follows from the Theorem. □

Analogously as in [7, Section 4] we remark that the Inversion Principle can be applied in discrete convolution rings. Let $u \in C(R, \mathcal{T})$ be a unit with inverse v and $g \in C(R, \mathcal{T})$. Setting $f = g \bullet u$ we can state: For every $i \in I$ we have

$$f(i) = \sum_{(r,s)\in\rho(i)} \tau(r,s) g(r) u(s)$$

if and only if for every $i \in I$ we have

$$g(i) = \sum_{(r,s)\in\rho(i)} \tau(r,s) f(r) v(s) \ .$$

Acknowledgement. The author is indebted to S. Veldsman for kindly sending him the paper [8].

References

[1] M. Aguiar and S. Mahajan, *Hopf monoids in the category of species*. Preprint, 2012.
[2] M. El Bachraoui, *Convolution over Lie and Jordan algebras*, Contrib. Discrete Math., 1 (2006), pp. 106–126 (electronic).
[3] R. S. Pierce, *Associative algebras*, vol. 88 of Graduate Texts in Mathematics, Springer-Verlag, New York, 1982. Studies in the History of Modern Science, 9.
[4] H.-E. Porst, *Dual adjunctions between algebras and coalgebras*, Arab. J. Sci. Eng. Sect. C Theme Issues, 33 (2008), pp. 407–411.
[5] D. Rosso, *Convolution algebras and applications to representation theory*. Preprint, 2012.
[6] S. Veldsman, *Convolution rings*, Algebra Colloq., 13 (2006), pp. 211–238.
[7] ———, *Arithmetic convolution rings*, Int. J. Algebra, 5 (2011), pp. 771–791.
[8] ———, *Factorization in arithmetic convolution rings*. Preprint, 2012.

Haus-Endt-Strasse 88, D-40593 Düsseldorf, GERMANY
E-mail address: brunoth@web.de