A Study of Some Dickson Nearrings

Giordano Gallina and Fiorenza Morini

Dipartimento di Matematica e Informatica
Università di Parma - Italy
Parco Area delle Scienze 53/A, 43124 Parma, Italy

Abstract

We generalize a factor nearring of Dickson nearrings of formal power series.

Mathematics Subject Classification: 16Y30, 13F25

Keywords: Nearring, Dickson nearring, coupling map, composition ring, formal power series ring

1 Introduction

All nearrings of this article are left nearrings, that is in which the product is distributive on the left with respect to the sum. According to [4], given a ring \([R; +, \cdot]\), a coupling map for \(R\) is a function \(\varphi : R \to \text{End}[R; +, \cdot] (a \to \varphi_a)\) such that \(\varphi_0\) is the null endomorphism, while, for any \(a, b \in R\), \(\varphi_a \circ \varphi_b = \varphi_{a \varphi_a(b)}\). If \(\varphi\) is a coupling map for \(R\), the nearring coupled with \(R\) by \(\varphi\) ([4, page 155]) is the structure \([R; +, \circ]\), where \(\circ\) is given by \(a \circ b = a \varphi_a(b)\) (which implies \(\varphi_{a \circ b} = \varphi_a \circ \varphi_b\)). This last structure can be denoted by \(R^\varphi\), and it is said to be a Dickson nearring. In this paper, we start from a ring \(A\) without zero divisors, endowed with an injective endomorphism \(\rho\), and we consider the ring of formal power series \(A[[X, \rho]]\)\(^{(1)}\). We suppose that \(\varphi\) is a suitable coupling map for \(A\) (with \(A^\varphi = [A; +, \circ]\)) and we extend \(\varphi\) to a coupling map \(V\) for \(A[[X, \rho]]\), according to [7] and [8, page 136]. In this paper, we study ideals in \(A[[X, \rho]]^V\); besides, if \(J\) is the ideal generated by \(X^2\), we show that a weakening of hypothesis onto \(\rho\), in

\(^{(1)}\)See also [8, pages 260-261].
$A[[X, \rho]]^V/J$, leads to nearrings introduced in [3]. Consequently, we concentrate our attention on the set $G_\varphi$ of endomorphisms $\gamma$ of $[A^* = A\backslash\{0\}; \circ]$ such that, for every $a \in A^*$, $\varphi_a = \varphi_\gamma(a)$. A congruential equation gives us aid to characterize the elements of $G_\varphi$ in the finite case (Theorem 3.1). Moreover, we describe a method to identify various elements of $G_\varphi$, in cases in which $A$ is a polynomial integral domain over a field. For further generalities on the theory of nearrings, we refer to the treatises [1, 2, 5, 6, 8].

2 On ideals of Dickson nearrings

Let $A$ be a ring without zero divisors, with identity 1, and let $\rho$ be an injective endomorphism of $A$ such that $\rho(1) = 1$. We consider the ring $H = A[[X, \rho]]$, whose elements are formal power series with coefficients in $A$, where addition and multiplication are defined by

$$
\left( \sum_{i \in \mathbb{N}_0} X^i a_i \right) + \left( \sum_{i \in \mathbb{N}_0} X^i b_i \right) = \sum_{i \in \mathbb{N}_0} X^i (a_i + b_i)
$$

$$
\left( \sum_{i \in \mathbb{N}_0} X^i a_i \right) \cdot \left( \sum_{i \in \mathbb{N}_0} X^i b_i \right) = \sum_{k \in \mathbb{N}_0} X^k c_k
$$

with $c_k = \sum_{i+j=k} \rho^i(a_i)b_j$.

Let $\varphi$ be a coupling map for $A$, such that $\forall a \in A^* \varphi_a$ is injective. For any $f = \sum_{i \in \mathbb{N}_0} X^i a_i$ of $H^* = H\backslash\{0\}$, we put $\sigma(f) = \min\{i | a_i \neq 0\}$, $\varepsilon(f) = a_{\sigma(f)}$.

If $\delta$ is an endomorphism of $A$ we denote by $\delta$ the function $H \to H$ defined as follows

$$
\delta \left( \sum_{i \in \mathbb{N}_0} X^i a_i \right) = \sum_{i \in \mathbb{N}_0} X^i \delta(a_i)
$$

Suppose that $\forall a \in A \varphi_a \circ \rho = \rho \circ \varphi_a$ and that $\forall a \in A^* \varphi_{\rho(a)} = \varphi_a$. We call $V$ the coupling map for $H$ ([7]) such that $V_0$ is the null endomorphism, while $V_f = \overline{\varphi}_f(f)$ for every $f \in H^*$. Put $H^V = [H; +, \circ_1]$. The polynomial ring $H' = A[X, \rho] = \{\sum_{i \in \mathbb{N}_0} X^i a_i | a_i \neq 0 \text{ for a finite number of } i \in \mathbb{N}_0\}$ is a subring of $H$. For $f = \sum_{i \in \mathbb{N}_0} X^i a_i \in H'^* \text{ put } \deg f = \max\{i | a_i \neq 0\}$, $\varepsilon'(f) = a_{\deg f}$.

We call $V'$ the coupling map for $H'$ such that $V'_0$ is the null endomorphism, while $V'_f = \overline{\varphi}_f^\ast(f)$ for every $f \in H'^*$. We put $H'^{V'} = [H'; +, \circ_2]$.

**Theorem 2.1.** If $A^\rho$ is a proper nearfield (non-skew-field), then $H'^{V'}$ is a nearring without proper right ideals.

---

(2) For us, $\mathbb{N}_0$ is the set of natural numbers, $\mathbb{N}$ is that of natural numbers 0 excepted and $\mathbb{Z}$ is that of relative integers.
Proof. Let \( I \) be a non-null right ideal of \( H^{V'} \). We consider \( f \in I \setminus \{0\} \). If \( f \) is constant it is immediate that \( I = H^{V'} \). Let now \( \deg f \geq 1 \). Put \( a = \varepsilon(f) \) and \( g = f \circ_a a^{-1} \), \( g \) belongs to \( I \) and it is monic. Since \( A^f \) is a proper nearfield, there are \( b,c \in A^* \) with \( \varphi_b(c) \neq c \). We define \( h = (b + g) \circ_a c - b \circ_a c \), which belongs to \( I \), since \( I \) is a right ideal. From the fact \( b + g \) is monic, \( V_{b+g} \) is equal to the identity map on \( H' \), so \( h = bc + gc - b\varphi_b(c) = b(c - \varphi_b(c)) + gc \), where now the products are calculated in the ring \( H' \). Because of \( h \in I \) and \( gc = g \circ_a c \in I \), we have \( b(c - \varphi_b(c)) \in I \); therefore \( I \) contains a non null element of \( A \). Then \( I = H^{V'} \). \( \square \)

Theorem 2.2. For any \( n \in \mathbb{N}_0 \), \( X^n \cdot H \) is an ideal of \( H^V \).

Proof. For an \( r \in \mathbb{N} \), we put \( I = X^r \cdot H \). Obviously, \( I \) is a left ideal. Let \( f \in I \setminus \{0\} \), \( g, h \in H^* \). Put \( u = (g + f) \circ_0 h - g \circ_0 h, \sigma(g) = s, \sigma(f) = t, \varepsilon(g) = b \). If \( s < t \), then \( \varepsilon(g + f) = \varepsilon(g) = b, (g + f) \circ_0 h = (g + f) \cdot V_{g+f}(h) = (g + f) \varphi_b(h), g \circ_0 h = g V_0(h) = g \varphi_b(h) \), hence \( u \) is equal to \( f \cdot \varphi_b(h) \), which belongs to \( I \). If \( t \leq s \), since \( r \leq t \), we have \( r \leq t \leq s \), so \( u \in I \). \( \square \)

Theorem 2.3. If \( A^f \) is a proper nearfield, the unique non null ideals and the unique non null right ideals of \( H^{V'} \) are the \( X^n \cdot H \), \( n \in \mathbb{N}_0 \).

Proof. Let \( I \) be a non null right ideal of \( H^V \). We take an \( f \in I \), \( f \neq 0 \), with \( \sigma(f) = r \) the smallest possible. let \( b,a \) non null elements of \( A \), such that \( b \neq 0, \varphi_{b+a} \neq \varphi_b \) (they exist since \( A^f \) is a proper nearfield). Put \( c = \varepsilon(f), g = f \circ_0 c^{-1} \circ_1 a \). We have \( g \in I \), \( \varepsilon(g) = a, \sigma(g) = r \). We consider \( d \in A \) such that \( \varphi_{b+a}(d) \neq \varphi_b(d) \). Define \( h = (X^r b + d) \circ_1 d - (X^r b) \circ_0 d \). Since \( I \) is a right ideal, \( h \in I \), and we have \( h = (X^r b + g) \varphi_{b+a}(d) - (X^r b) \varphi_b(d) \). Put \( w = h - g \circ_1 (\varphi_{b+a}^{-1}(\varphi_{b+a}(d))) = h - g \cdot \varphi_{b+a}(d) \). Because \( g, h \in I \), \( w \) lies in \( I \), and \( w = h - g \cdot \varphi_{b+a}(d) = (X^r b + g) \varphi_{b+a}(d) - (X^r b) \varphi_b(d) - g \cdot \varphi_{b+a}(d) = X^r b(\varphi_{b+a}(d) - \varphi_b(d)) \). The element \( w \) is distinct from \( 0 \), since \( \varphi_{b+a}(d) - \varphi_b(d) \neq 0 \) and \( b \neq 0 \). We call \( e \) the non null coefficient of \( w \). We have \( w \circ_0 e^{-1} \in I \), that is \( X^r \in I \). Then \( X^r \circ_1 H = X^r \cdot H \subseteq I \). But there exists no \( l \in I \setminus \{0\} \) with \( \sigma(l) < r \); therefore the last inclusion can be replaced by an equality. \( \square \)

3 On a factor nearring of \( H^V \)

3.1 A possible change of the operation \( \circ_1 \)

We put \( A^f = [A; +, 0] \). Let \( J \) be the ideal of \( H^V \), \( J = X^2 \circ_1 H = X^2 \cdot H \). In order to analyze the operation \( \circ_1 \) defined onto \( H^V / J \), let \( f = \sum_{i \in \mathbb{N}_0} X^i a_i \in H, g = \sum_{i \in \mathbb{N}_0} X^i b_i \in H \). We distinguish the two cases in which \( a_0 \neq 0 \), and \( a_0 = 0 \). If \( a_0 \neq 0 \), then \( (f + J) \circ_1 (g + J) = (a_0 + X a_1 + J) \circ_1 (b_0 + X b_1 + J) =\)

(3) According to [7], we denote by \( a^{-1} \) the inverse of \( a \) in the nearfield \( A^f \).
= ((a_0 + Xa_1) \circ_1 (b_0 + Xb_1)) + J = ((a_0 + Xa_1) \cdot V_{a_0 + Xa_1}(b_0 + Xb_1)) + J =
= ((a_0 + Xa_1) \varphi_{a_0}(b_0 + Xb_1)) + J = ((a_0 + Xa_1) \cdot (\varphi_{a_0}(b_0) + X \varphi_{a_0}(b_1))) + J =
= a_0 \circ b_0 + X(a_1 \varphi_{a_0}(b_0) + \rho(a_0) \varphi_{a_0}(b_1)) + J.

If \(a_0 = 0\), then \((f + J) \circ_1 (g + J) = (Xa_1 + J) \circ_1 (b_0 + Xb_1 + J) = X(a_1 \varphi_{a_1}(b_0)) + J =
= X(a_1 \circ b_0) + J.

We can summarize these facts as follows. The nearring \(H^V/J\) is isomorphic to \([A \times A; +, \circ_1]\), where now the operations + and \(\circ_1\), on \(A \times A\), are defined in the next manner. For \((a_0, a_1), (b_0, b_1) \in A \times A\)

\[(a_0, a_1) + (b_0, b_1) = (a_0 + b_0, a_1 + b_1)\]  \hspace{1cm} (1)

besides, if \(a_0 \neq 0\), then

\[(a_0, a_1) \circ_1 (b_0, b_1) = (a_0 \circ b_0, a_1 \varphi_{a_0}(b_0) + \rho(a_0) \varphi_{a_0}(b_1))\]  \hspace{1cm} (2)

while, if \(a_0 = 0\), then

\[(0, a_1) \circ_1 (b_0, b_1) = (0, a_1 \circ b_0)\]  \hspace{1cm} (3)

Now we try to reduce the hypotheses onto \(\rho\), requiring that \(\rho\) satisfies only the subsequent conditions (a), (b).

(a) \(\rho\) is an endomorphism of \([A^*, \circ]\);\]

(b) \(\forall a \in A^* \varphi_a = \varphi_{\rho(a)}\).

We call \(G_{\varphi}\) the set of \(\rho\) verifying (a), (b). Thus, if \(\rho \in G_{\varphi}\), then \(A \times A\), with operations + and \(\circ_1\) defined by (1),(2),(3), is a nearring. The demonstration of this is already contained in [3].

### 3.2 On the finite case

In this subsection, we strictly follow notations of [8, pages 168,169]. We suppose here that \(A\) is a finite field \(F = F_q^n\), so that \(F^\varphi\) is a nearfield, and \(\varphi\) has fixed field \(P_{\varphi} = F_q\). We recall that, for \(\xi \in F\) and \(k \in \mathbb{Z}\), \(\xi^k\) means the \(k\)-th power of \(\xi\), calculated in \(F^\varphi\). By Theorem 1.1 of [8, page 168],

\[\left(\left(F^\varphi\right)^* \simeq G_{q,n} = G_p < x, y | x^m = 1, y^n = x^t, yxy^{-1} = x^q >\right)\]

where \(m = q^{a-1}/n\), \(t = m/q-1\), and there exist \(a, b \in (F^\varphi)^*\) such that \([(F^\varphi)^*; \circ]\) is generated by \(\{a, b\}^{(5)}\), and the function \(\{x, y\} \rightarrow (F^\varphi)^*\), which sends \(x\) to \(a\) and \(y\) to \(b\), is extendible to an isomorphism of \(G_{q,n}\) onto \((F^\varphi)^*\). We have \(a^{n+1} = 1, b^n = a^t, b \circ a \circ b^{-1} = a^2\).

\[\text{(4)}\text{Not necessarily commuting with every } \varphi_a, a \in A.\]

\[\text{(5)}\text{In which } b \text{ is equal to a generator } w \text{ of } [F^*; :], \text{ while } a = w^n.\]
Theorem 3.1. A function \( f \) from \((F^\varphi)^*\) to \((F^\varphi)^*\) belongs to \(G_\varphi\) if and only if \( f \) is (natural) prolongation\(^{(6)}\) of a function \( h : \{a, b\} \to (F^\varphi)^* \) with \( h(a) = a^2\), \( h(b) = a^2 \circ b (= a^b) \), where \( r, s \in \mathbb{Z} \) are such that

\[
s \cdot q^n - 1 \equiv \frac{q^n - 1}{n(q - 1)}(1 - r) \equiv 0 \mod \frac{q^n - 1}{n}.
\]

Proof. An endomorphism of \([(F^\varphi)^*; \circ]\) is uniquely determined by the way in which it operates onto \( a \) and \( b \). From Theorem 1.1 of [8, page 168], the kernel \( U \) of the homomorphism \((F^\varphi)^* \to \text{Aut} F, c \to \varphi_c\), is a (normal) cyclic subgroup of \((F^\varphi)^*\) generated by \( a \). Therefore, an \( f \in \text{End}[(F^\varphi)^*; \circ] \) is such that \( f \in G_\varphi \) if and only if \( f(a) \in U \), \( f(b) \in U \circ b = U \cdot b \), namely if and only if \( f(a) \) is a power of \( a \) and \( f(b) \) is of the form \( a^z \circ b = a^z \cdot b \).

Conversely, let \( h \) be a function \( h : \{a, b\} \to (F^\varphi)^* \) such that \( h(a) = a^2 \), \( h(b) = a^s \circ b \) for \( r, s \in \mathbb{Z} \). We put \( a_1 = h(a), b_1 = h(b) \). The function \( h \) is extendable to an endomorphism of \( G_\varphi \), if and only if \( a_1 \) and \( b_1 \) verify the defining relations of \( G_{q,n} \), that is, if and only if

\[
a_1^m = 1, \quad b_1^m = a_1^t, \quad b_1 \circ a_1 \circ b_1^{-1} = a_1^q.
\]

We have:

\[
a_1^m = (a^2)^m = (a^m)^2 = 1;
\]

\[
b_1 \circ a_1 \circ b_1^{-1} = a^2 \circ b \circ a^2 \circ b^{-1} \circ a^{-s} = a^z \circ a^{rs} \circ a^{-s} = a^{zq} = (a^z)^q = a_1^q.
\]

We observe that, for every \( k \in \mathbb{N} \), \( b^k \circ a^z \circ b^{-k} = (b^k \circ a \circ b^{-k})^z = a^{zk} \cdot b_1^k \),

\[
\text{that is } b_1^k \circ a^z = a^{zk} \cdot b_1^k = a^{zk} \cdot b_1^k.
\]

Hence \( b_1^m = a^{zq} \circ b_1 \circ a^{zq} \circ b_1 \circ \ldots \circ a^{zq} \circ b_1 = a^{zq + q^2 + q^3 + \ldots + q^{n-1}} \cdot b_1^n = a^{z \cdot \frac{q^{n-1} - 1}{q - 1}} \cdot a^t = a^{s \cdot \frac{q^{n-1} - 1}{q - 1} + t}\).

Moreover \( a_1^t = a^t \).

Therefore \( b_1^m = a_1^t \) if and only if \( s \cdot \frac{q^n - 1}{q - 1} + t \cdot (1 - r) \equiv 0 \mod m \).

\( \square \)

3.3 When \( A \) is an integral polynomial domain

In this subsection, let \( B \) be a (commutative) field, and we suppose that \( A \) is the ordinary gaussian polynomial domain \( B[Y] \), in one indeterminate \( Y \). We denote by \( T \) an automorphism of \( B[Y] \) verifying one of the two following conditions, \((\alpha)\) or \((\beta)\).

\((\alpha)\) There exists an automorphism \( S \) of \( B \), of finite order, such that \( T = S^{(7)} \).

\((\beta)\) The characteristic of \( B \) is a prime number, and \( T \) is the automorphism of \( B[Y], T : f(Y) \to f(Y + a) \) where \( a \) is a fixed element of \( B^* \).

\(^{(6)}\)That is \( \forall u, v \in \mathbb{Z} \) \( f(a^2 b^2) = h(a)^2 h(b)^2 \).

\(^{(7)}\)As usual, we call \( S \) the natural extension of \( S \) to \( B[Y] \) (defined by \( S(b_0 + Y b_1 + \ldots + Y^n b_n) = S(b_0) + Y S(b_1) + \ldots + Y^n S(b_n) \)).
Suppose that \( \varphi \) is a coupling map for \( A = B[Y] \) such that \( \varphi_0 \) is the null endomorphism, while \( \varphi_f = T^{\deg f} \) for \( f \neq 0, f \in A \). We will determine various elements of \( G_\varphi \).

Let \( L \) be the subgroup generated by \( T \) in \( \text{Aut } A \), and let \( r \in \mathbb{N} \) be the cardinality of \( L \). We call \( P \) the set of all orbits of \( L \) constituted by monic irreducible polynomials\(^8\). For any \( M \in P \), fix an \( f_M \in M \). Put \( \Lambda = \{ f_M | M \in P \} \). We define a function \( \rho : A^* \to A^* \) initially onto \( \Lambda \). For \( f_M \in \Lambda \), let \( \rho(f_M) = h_M \), where \( h_M \) is a non null polynomial of \( A \), with \( \deg h_M \equiv \deg f_M \), and besides, if \( d_1, d_2 \) are the cardinalities of the orbits of \( L \) represented by \( f_M, h_M \) respectively, we suppose that \( d_2 \) divides \( d_1 \). Then \( \frac{d_1}{d_2} \) divides \( \frac{r}{d_2} \). We define now \( \rho \) on the set of all monic irreducible polynomials of \( A \). If \( v(Y) \) is a monic irreducible polynomial of \( A \), then there exists an \( M \in P \) such that \( v(Y) \in M \). Therefore \( v(Y) = T^k(f_M) \) for a \( k \in \mathbb{N} \). Put \( \rho(v(Y)) = T^k(h_M) = T^k(\rho(f_M)) \), that is, definitively,

\[
\rho(T^k(f_M)) = T^k(\rho(f_M))
\]  

(4)

We prove that this has meaning. The stabilizer of \( f_M \) in \( L \) is a subgroup \( H_1 \) of \( L \) of order \( \frac{r}{d_1} \), and the stabilizer of \( h_M \) in \( L \) is a subgroup \( H_2 \) of order \( \frac{r}{d_2} \) (where \( d_1, d_2 \) are the cardinalities of the orbits of \( L \) represented by \( f_M, h_M \) respectively). Since \( \frac{d_1}{d_2} \) divides \( \frac{r}{d_2} \), and \( L \) is a finite cyclic, \( H_1 \) is contained in \( H_2 \). Now, if \( T^k(f_M) = T^{k'}(f_M) \), then \( T^{k-k'}(f_M) = f_M \), which implies \( T^{k-k'} \in H_1 \), hence \( T^{k-k'} \in H_2 \), so \( T^{k-k'}(h_M) = h_M \), i.e. \( T^k(h_M) = T^{k'}(h_M) \). In this way, \( \rho \) is defined on the set of all monic irreducible polynomials. We try to define \( \rho \) on the whole \( A^* \) in the subsequent manner. We say that \( \rho \) sends any non null constant polynomial to itself. Besides, for every \( h(Y) \in A^* \), \( \deg h(Y) \geq 1 \), write \( h(Y) \) as

\[
h(Y) = a v_1(Y)^{m_1} v_2(Y)^{m_2} \ldots v_s(Y)^{m_s}
\]
in which \( a \in B^* \), \( v_1(Y), v_2(Y), \ldots, v_s(Y) \) are monic irreducible two by two distinct and the \( m_i \) are in \( \mathbb{N}_0 \). Then we define

\[
\rho(h(Y)) = \alpha \rho(v_1(Y))^{m_1} \rho(v_2(Y))^{m_2} \ldots \rho(v_s(Y))^{m_s}
\]

**Lemma 3.2.** The function \( \rho \) preserves the product \( \cdot \) defined onto \( A^* \), and \( \rho \) commutes with \( T \).

**Proof.** Banally, if \( g_1, g_2 \in A^* \), then \( \rho(g_1 \cdot g_2) = \rho(g_1) \cdot \rho(g_2) \). It is also obvious that, if \( b \in A^* \) is constant, \( \rho(T(b)) = T(\rho(b)) \). We demonstrate now that, for \( \pi \) monic irreducible, \( \rho(T(\pi)) = T(\rho(\pi)) \). Let \( v(Y) \in A \) be monic irreducible. Then there exists an \( f_M \in \Lambda \) and a \( k \in \mathbb{N} \) such that \( v(Y) = T^k(f_M) \). Because of (4), we have

\[
\rho(T(v(Y))) = \rho(T^{k+1}(f_M)) = T^{k+1}(\rho(f_M)) = T(T^k(\rho(f_M))) = T(\rho(T^k(f_M))) = T(\rho(v(Y))).
\]

More in general, if \( h(Y) \in A^* \) is of positive degree, we write \( h(Y) \),

\(^8\)We call that \( T \) sends monic polynomials to monic polynomials.
as before, in the form $h(Y) = av_1(Y)^{m_1}v_2(Y)^{m_2}\ldots v_s(Y)^{m_s}$. By preceding part of the demonstration, for any $1 \leq i \leq s$, $T(\rho(v_i(Y))) = \rho(T(v_i(Y)))$. Then, if we bear in mind the definition of $\rho$,

$$
\rho(T(h(Y))) = \rho(T(av_1(Y)^{m_1}v_2(Y)^{m_2}\ldots v_s(Y)^{m_s})) = \rho(T(a)T(v_1(Y))^{m_1}T(v_2(Y))^{m_2}\ldots T(v_s(Y))^{m_s}) = T(a)\rho(T(v_1(Y)))^{m_1}\rho(T(v_2(Y)))^{m_2}\ldots \rho(T(v_s(Y)))^{m_s} = T(a\rho(v_1(Y)))^{m_1}\rho(v_2(Y))^{m_2}\ldots \rho(v_s(Y))^{m_s}) = T(\rho(\rho(a\rho(v_1(Y))^{m_1}v_2(Y))^{m_2}\ldots v_s(Y)^{m_s})) = T(\rho(h(Y)))
$$

□

Lemma 3.3. For any $f \in A^*$

$$
\deg f \equiv_r \deg \rho(f)
$$

Proof. The assertion is obvious if $f$ is constant. Let $v(Y) \in A^*$ be monic irreducible. Then $v(Y) = T^k(f_M)$ for an $f_M \in \Lambda$ and a $k \in \mathbb{N}$. We can write, by (4),

$$
\deg \rho(v(Y)) = \deg(\rho(T^k(f_M))) = \deg(T^k(\rho(f_M))) = \deg(\rho(f_M)) \equiv_r \deg f_M = \deg T^k(f_M) = \deg v(Y)
$$

More in general, let $h(Y) \in A^*$ have positive degree, and we write, as above, $h(Y)$ in the form

$$
h(Y) = av_1(Y)^{m_1}v_2(Y)^{m_2}\ldots v_s(Y)^{m_s}
$$

We observe that, by previous demonstration, for $1 \leq i \leq s$,

$$
\deg v_i(Y) \equiv_r \deg \rho(v_i(Y))
$$

Hence

$$
\deg h(Y) = m_1 \deg v_1(Y) + \ldots + m_s \deg v_s(Y) \equiv_r m_1 \deg \rho(v_1(Y)) + \ldots + m_s \deg \rho(v_s(Y)) = \deg(a\rho(v_1(Y))^{m_1}\ldots \rho(v_s(Y))^{m_s}) = \deg(\rho(a\rho(v_1(Y))^{m_1}\ldots v_s(Y)^{m_s})) = \deg \rho(h(Y))
$$

□

Corollary 3.4. For any $f \in A^*$

$$
T^{\deg f} = T^{\deg \rho(f)} \text{ and } \varphi_f = \varphi_{\rho(f)}
$$
We recall that we have put $A^\circ = [A; +, \circ]$.

**Lemma 3.5.** The function $\rho$ is an endomorphism of $[A^*; \circ]$.

**Proof.** We take $f, g \in A^*$. By Lemma 3.2 and Corollary 3.4,

$$
\begin{align*}
\rho(f \circ g) &= \rho(f \varphi_f(g)) = \rho(f \cdot T^{\text{deg}f}(g)) = \\
&= \rho(f) \cdot \rho(T^{\text{deg}f}(g)) = \rho(f) \cdot T^{\text{deg}f}(\rho(g)) = \\
&= \rho(f) \cdot T^{\text{deg}f}(\rho(g)) = \rho(f) \cdot \varphi_{\rho(f)}(\rho(g)) = \\
&= \rho(f) \circ \rho(g)
\end{align*}
$$

Therefore, we can conclude with the following theorem.

**Theorem 3.6.** The function $\rho$ is an element of $G_{\varphi}$.

**Proof.** The assertion holds from Lemma 3.5 and Corollary 3.4.

References


Received: July 2, 2015; Published: September 9, 2015