**Mathematica Pannonica**
**23**/1 (2012), 45–64

# NEAR-RINGS OF POLYNOMIAL FUNCTIONS

Stefan **Veldsman**

*Dept. Mathematics, Sultan Qaboos University, Sultanate of Oman*

**Dedicated to the memory of Andries P. J. van der Walt**

*Received*: December 2010

*MSC 2010*: 16 Y 30

*Keywords*: Near-ring, near-ring polynomial, near-ring polynomial function.

**Abstract:** Associated with a near-ring polynomial is the usual polynomial function obtained by substitution. Some rules and properties for this substitution are established and the question for which near-rings the only self-maps are polynomial functions is investigated.

## 1. Introduction

The study of polynomial near-rings has been rekindled by a model proposed by Andries van der Walt. This model is based on a functional approach to near-ring polynomials and is much more tractable than the traditional universal algebraic approach. Here we continue these investigations; firstly to set the scene for substitutions into near-ring polynomials and secondly, to the subsequent problem of the relationship between all the self-maps on a near-ring and the polynomial maps. It will be seen that in many cases the situation here is quite different from that of rings. We start with a brief recollection of the required notions.

Near-rings of polynomials should not be confused with polynomial near-rings. The former is a set of polynomials over a ring (typically, commutative with identity) which is a near-ring with respect to the usual

*E-mail address:* veldsman@squ.edu.om

addition and composition of polynomials. These near-rings have been studied extensively and their theory and applications can be found in the books by Pilz [13] and Clay [4].

A polynomial near-ring, on the other hand, is a near-ring of polynomials with coefficients from a near-ring in the universal algebraic sense, see for example Lausch and Nöbauer [8], where the coefficients are from a near-ring. These polynomials are much more awkward to deal with and apart from the more general universal algebraic considerations, not much work has been done in this area. We will study near-ring polynomials using the model proposed by Andries van der Walt and which was motivated by the functional approach to matrix near-rings [12] and group near-rings [11]. The initial investigations were done by Bagley [1, 2] and taken further by Farag [5, 6], Lee [9], Lee and Groenewald [10] and Veldsman [14, 15, 16]. In this model, polynomials are regarded as functions and the indeterminate, which is also a function, is a commuting indeterminate. The polynomial near-rings in this sense are thus more restricted but much better behaved and easier to deal with than those prescribed by the universal algebraic approach mentioned above.

## 2. Definitions

All near-rings, usually denoted by $N$, will be right distributive, 0-symmetric and with identity 1. As usual, $A \lhd N$ means $A$ is an ideal of the near-ring $N$. Let $(G, +)$ be a group. $G$ is called an $N-N-bigroup$ if there are mappings $N \times G \to G$ and $G \times N \to G$ such that, if we write the images by juxtaposition, then $(n+m)g = ng+mg$, $(g+h)n = = gn + hn$, $(nm)g = n(mg)$, $g(nm) = (gn)m$ and $(ng)m = n(gm)$ for all $g, h \in G$ and $n, m \in N$. We suppose that all actions are unital and that $G$ is left-faithful, i.e. $(0 : G)_N := \{n \in N \mid nG = 0\} = 0$. The set $M_N(G) := \{f \in M_0(G) \mid f(gn) = f(g)n \text{ for all } g \in G, n \in N\}$ is a subnear-ring of $M_0(G)$ where $M_0(G)$ denotes the near-ring of all 0 preserving functions from $G$ to $G$ with respect to pointwise addition and composition. By the left-faithfulness, $N$ can be embedded in $M_N(G)$ via $\eta : N \to M_N(G)$ defined by $\eta(a) := \eta_a, \eta_a(g) := ag$ for all $g \in G$. We identify $a \in N$ with $\eta_a$ in $M_N(G)$ and note that the identity map on $G$ is then the identity of $N$.

We work mostly with the following bigroup: Let $N$ be a 0-symmetric near-ring with identity and let $G := N^k$ be the direct sum of $k$ copies of $(N,+)$ where $k \in \mathbb{N}$, $\mathbb{N}$ is the set of positive integers, or $k = \omega$, the first limit ordinal. By $\pi_i : N^k \to N$ we will denote the $i$-th projection map. With respect to the usual left and right scalar multiplication, $N^k$ is a unital left-faithful $N - N$-bigroup.

Any $u \in M_N(G) - N$ will be called an *indeterminate*. A *commuting indeterminate* is an indeterminate which is an $N - N$-homomorphism, i.e. $u(ng) = nu(g)$, $u(gn) = u(g)n$ and $u(g+h) = u(g) + u(h)$ for all $g, h \in G$ and $n \in N$. For an indeterminate $u$, let $[N, G, u]$ be the subnear-ring of $M_N(G)$ generated by $N \cup \{u\}$. If $u$ is a commuting indeterminate, then it can be shown that $u$ commutes with all the elements in $[N, G, u]$ (and is hence a distributive element of $[N, G, u]$). More properties of indeterminates can be found in [14]; we recall only the following:

**Proposition 2.1.** *Let $u \in M_N(G)$ be a commuting indeterminate. Then*

$$[N, G, u] = \bigcup_{n=1}^{+\infty} \mathcal{A}_n \quad \text{where} \quad \mathcal{A}_1 = \{au^n \mid a \in N, n \geq 0\} \qquad \textit{and}$$

$$\mathcal{A}_{n+1} = \left\{ \sum_{i=1}^{m} a_i w_i \mid m \geq 1, a_i \in N, w_i \in \mathcal{A}_n \right\} \quad \textit{for} \quad n \geq 1.$$

The elements of $[N, G, u]$ will usually be denoted by small letters $f, g, h, \ldots$ without any reference to the indeterminate $u$. Any element of $[N, G, u]$ is in one of the $\mathcal{A}_n$'s and we will always write an element from $[N, G, u]$ in the form as specified for $\mathcal{A}_n$'s elements as above. This will be our canonical representation of the elements of $[N, G, u]$; but note that this representation of an element in $[N, G, u]$ need not be unique.

The mapping $x : N^\omega \to N^\omega$ defined by

$$x(\alpha_1, \alpha_2, \alpha_3, \ldots) = (\alpha_2, \alpha_3, \alpha_4, \alpha_5, \ldots)$$

is called the *left shift function*. It is a commuting indeterminate in $M_N(N^\omega)$. The *polynomial near-ring* $N[x]$ is defined as $[N, N^\omega, x]$. Note that $x$ commutes with all the elements of $N[x]$ and is thus a distributive element of $N[x]$. By definition, $N[x]$ is always 0-symmetric. Originally a polynomial near-ring was defined by using the right shift function $x^* : N^\omega \to N^\omega$ given by $x^*(\alpha_1, \alpha_2, \alpha_3, \ldots) = (0, \alpha_1, \alpha_2, \alpha_3, \alpha_4, \ldots)$. This does not really matter, since in [15] it was shown that $[N, N^\omega, x] \cong$ $\cong [N, N^\omega, x^*]$.

In proving statements about elements of $[N, G, u]$ for $u$ a commuting indeterminate, we usually use one of the following two inductive arguments. Firstly, show that any $au^n$, $a \in N, n \geq 0$, has the desired property.

Then suppose that both $f, g \in [N, G, u]$ have the property and show that $f + g$ and $fg$ also satisfy the property. One may then conclude that all the elements of $[N, G, u]$ have this property. The second argument is based on Prop. 2.1. Any $f \in [N, G, u]$ is in one of the classes $\mathcal{A}_n$; the *level* of $f$ is the smallest $n \geq 1$ for which $f \in \mathcal{A}_n$. The proof that the elements of $[N, G, u]$ have a certain property is then by induction on the level of $f$.

From [15, 16] we recall: Because $x$ is a commuting indeterminate, $xf = fx$ for all $f \in N[x]$. This means that if $f(\alpha_1, \alpha_2, \alpha_3, ...) = = (\beta_1, \beta_2, \beta_3, ...)$, then $f(\alpha_2, \alpha_3, \alpha_4, ...) = (\beta_2, \beta_3, \beta_4, ...)$. With any $f \in N[x]$ we associate a function $F : N^\omega \to N$ defined by $F(\alpha_1, \alpha_2, \alpha_3, \dots) = = \pi_1(f(\alpha_1, \alpha_2, \alpha_3, ...))$ for all $(\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega$. This function $F$ is uniquely determined by $f$ and it completely describes the polynomial $f$ since for every $i \geq 1$ and $\alpha = (\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega$, $F(\alpha_i, \alpha_{i+1}, \alpha_{i+2}, ...) = = \pi_i(f(\alpha_1, \alpha_2, \alpha_3, ...))$. Furthermore, there exists an integer $k \geq 1$ such that for all $\alpha = (\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega$,

$$\pi_1(f(\alpha_1, \alpha_2, \alpha_3, ...)) = \pi_1(f(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k, 0, 0, 0, ...)).$$

Let $k_f$ be the minimum amongst all such $k$. This $k_f$ is uniquely determined by $f$ and is independent of the representation chosen for $f$. The *height* of $f$ is then defined as follows: If $f = 0$, let the height of $f$ be $-\infty$ and if $f \neq 0$, define the height of $f$ to be $k_f - 1$. For $f, g \in N[x]$, it has been shown that $\text{height}(f+g) \leq \max\{\text{height}(f), \text{height}(g)\}$ and $\text{height}(fg) \leq \leq \text{height}(f) + \text{height}(g)$. If $f \in N[x]$ with $\text{height}(f) = 0$, then $f = b$ for some $b \in N$. Indeed, let $F$ be the function associated with $f$ and let $b = F(1, 0, 0, ...)$. Then $F(\alpha_1, \alpha_2, \alpha_3, ...) = F(\alpha_1, 0, 0, ...) = F(1, 0, 0, ...)\alpha_1 = = b\alpha_1$ and for any $i \geq 1$, $\pi_i(f(\alpha_1, \alpha_2, \alpha_3, ...)) = F(\alpha_i, \alpha_{i+1}, \alpha_{i+2}, ...) = = F(\alpha_i, 0, 0, ...) = b\alpha_i$. Thus $f = b \in N$. The following, from [16], will be useful:

**Lemma 2.2.** *Let $f \in N[x]$ with associated function $F$. If there is a $k \geq 0$ such that*

(i) *$F(\alpha_1, \alpha_2, \alpha_3, ...) = F(\alpha_1, \alpha_2, ..., \alpha_{k+1}, 0, 0, ...)$ for all $(\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega$ and*

(ii) *there are $\gamma_{k+1}, \gamma_{k+2}, \gamma_{k+3}, ... \in N^\omega$ such that*
$$F(0, ..., 0, \gamma_{k+1}, \gamma_{k+2}, \gamma_{k+3}, ...) \neq 0 \quad \textit{with} \quad \gamma_{k+1} \quad \textit{in position } k+1,$$
*then height$(f) = k$.*

It can easily be verified that if $f \in N[x]$ with $\text{height}(f) = k$, then $height(fx) = k+1$ and $\text{height}(af) = k$ where $a \in N$ is not a zero-divisor in $N$.

For $k, m \in \mathbb{N} \cup \{\omega\}$, let $M_N(N^k, N^m) := \{g \mid g : N^k \to N^m$ is a function such that for all $a \in N$ and $\alpha \in N^k$, $g(\alpha a) = g(\alpha)a\}$. With respect to pointwise addition and the canonical product $(ag)(t) = ag(t)$, $M_N(N^k, N^m)$ is an $N$-group. However, there is not a canonical way to turn it into a near-ring (of course, for certain choices of $k$ and $m$ there are). The next result, which was proved in [16], shows that $M_N(N^\omega, N)$ can be made into a near-ring with respect to a certain multiplication that contains an isomorphic copy of $N[x]$. But note that $M_N(N^\omega, N)$ can be a near-ring with respect to other (non-trivial) multiplications as well.

**Proposition 2.3.** *$M_N(N^\omega, N)$ is a near-ring with respect to pointwise addition and for $F, G \in M_N(N^\omega, N)$, the product $FG$ is defined by $(FG)(\alpha) := F(G(\alpha_1, \alpha_2, \alpha_3, ...), G(\alpha_2, \alpha_3, \alpha_4, ...), G(\alpha_3, \alpha_4, \alpha_5, ...), ...)$ for all $\alpha = (\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega$. The mapping $\gamma : N[x] \to M_N(N^\omega, N)$ defined by $\gamma(f) = F$ is an injective homomorphism.*

If $f, g \in N[x]$ with associated functions $F$ and $G$ respectively, then we need to know the associated functions of $f + g$ and $fg$ in terms of $F$ and $G$. For $f + g$ it is $F + G$. For any $\alpha = (\alpha_1, \alpha_2, \alpha_3, ...) \in$ $\in N^\omega$, suppose $g(\alpha_1, \alpha_2, \alpha_3, ...) = (\beta_1, \beta_2, \beta_3, ...)$. Then $\beta_i = \pi_i(g(\alpha)) =$ $= G(\alpha_i, \alpha_{i+1}, \alpha_{i+2}, ...)$ and the associated function of $fg$ is $FG$ where

$$\begin{aligned}(FG)(\alpha) &= F(G(\alpha_1, \alpha_2, \alpha_3, ...), G(\alpha_2, \alpha_3, \alpha_4, ...), G(\alpha_3, \alpha_4, \alpha_5, ...), ...) = \\ &= F(\pi_1(g(\alpha)), \pi_2(g(\alpha)), \pi_3(g(\alpha)), ...) = \\ &= F(\beta_1, \beta_2, \beta_3, ...).\end{aligned}$$

We will also need substitution in near-ring polynomials. This is addressed in the next section.

## 3. Substitutions

Whenever one leaves a comforting commutative environment, substitutions in polynomials need due care. Near-ring polynomials are no exception in this regard and will present many unexpected twists and turns.

For $k, m, n, l \in \mathbb{N} \cup \{\omega\}$ and $F \in M_N(N^k, N)$, choose $k$ elements $u_1, u_2, u_3, ... \in M_N(N^m, N^n)$. Define a function $F(u_1, u_2, u_3, ...) : N^m \to N^n$ as follows: For any $\alpha \in N^m$ and $i = 1, 2, 3, ..., n$, $\pi_i(F(u_1, u_2, u_3, ...)(\alpha)) =$

$= F(\pi_i(u_1(\alpha)), \pi_i(u_2(\alpha)), \pi_i(u_3(\alpha)), ...)$. The following property will often be used, mostly without any further recall.

**Lemma 3.1.** *For $k, m, n, l \in \mathbb{N} \cup \{\omega\}$ and $F \in M_N(N^k, N)$, choose $k$ elements $u_1, u_2, u_3, ... \in M_N(N^m, N^n)$ and let $g \in M_N(N^l, N^m)$.*

*Then $F(u_1 g, u_2 g, u_3 g, ...) = F(u_1, u_2, u_3, ...)g$.*

**Proof.** Let $\alpha \in N^l$. For any $i = 1, 2, 3, ..., n$,

$$\begin{aligned}&\pi_i(F(u_1 g, u_2 g, u_3 g, ...)(\alpha)) = \\ &= F(\pi_i(u_1(g(\alpha))), \pi_i(u_2((g(\alpha))), \pi_i(u_3((g(\alpha))), ...) = \\ &= \pi_i(F(u_1, u_2, u_3, ...)(g(\alpha))). \qquad \Diamond\end{aligned}$$

Let $f \in N[x]$ with associated function $F$. Let $u \in M_N(N^n, N^m)$, $n, m \in \mathbb{N} \cup \{\omega\}$. Define $\overline{f}(u) \in M_N(N^n, N^m)$ by $\overline{f}(u) = F(1, u, u^2, u^3, ...)$ where $F(1, u, u^2, u^3, ...) : N^n \to N^m$ is the function as defined above. Note that for $f \in N[x]$ with associated function $F$, $f = F(1, x, x^2, x^3, ...)$. Indeed, for any $\alpha = (\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega$ and $i \geq 1$,

$$\begin{aligned}\pi_i(F(1, x, x^2, x^3, ...)(\alpha_1, \alpha_2, \alpha_3, ...)) &= F(\pi_i(\alpha), \pi_i(x(\alpha)), \pi_i(x^2(\alpha)), ...) = \\ &= F(\alpha_i, \alpha_{i+1}, \alpha_{i+2}, ...) = \pi_i(f(\alpha_1, \alpha_2, \alpha_3, ...)).\end{aligned}$$

Substitution is well-defined and it does not depend on any particular representation of the polynomial. In the passing it may be mentioned that this functional approach to polynomials over near-rings with identity can be applied to rings which lends itself to a well-defined theory of substitution in polynomials over not necessarily commutative rings.

A particular substitution which will be of importance here is the following. For $F \in M_N(N^k, N)$ and $a \in N$, $(1, a, a^2, a^3, ...) \in N^\omega$ and $F(1, a, a^2, a^3, ...) \in N$ is well-defined. On the other hand, any $a \in N$ is identified with the function $a : N^\omega \to N^\omega$ defined by $a(\alpha_1, \alpha_2, \alpha_3, ...) = = (a\alpha_1, a\alpha_2, a\alpha_3, ...)$ in $N[x]$. Thus, $F(1, a, a^2, a^3, ...) : N^\omega \to N^\omega$ is given by

$$\begin{aligned}&\pi_i(F(1, a, a^2, a^3, ...)(\alpha)) = F(\pi_i(\alpha), \pi_i(a(\alpha)), \pi_i(a^2(\alpha)), ...) = \\ &= F(\alpha_i, a\alpha_i, a^2\alpha_i, ...) = F(1, a, a^2, a^3, ...)\alpha_i \text{ for all } i.\end{aligned}$$

This means $F(1, a, a^2, a^3, ...)$ is a constant, i.e. an element from $N$ in $N[x]$ which is in perfect harmony with the former meaning. Let $f \in \in N[x]$ with associated function $F$ and let $a \in N$. Define $\overline{f}(a)$ by $\overline{f}(a) = = F(1, a, a^2, a^3, ...)$. Note that

$$\overline{f}(a) = F(1, a, a^2, a^3, ...) = \pi_1(f(1, a, a^2, a^3, ...)) = \beta_1$$

where $f(1, a, a^2, a^3, ...) = (\beta_1, \beta_2, \beta_3, ...)$. Thus $\beta_i = \pi_i(f(1, a, a^2, a^3, ...)) = = F(a^{i-1}, a^i, a^{i+1}, ...) = F(1, a, a^2, a^3, ...)a^{i-1} = \beta_1 a^{i-1}$. We conclude that

$$f(1,a,a^2,a^3,...) = (\beta_1,\beta_2,\beta_3,...) = (\beta_1,\beta_1 a,\beta_1 a^2,\beta_1 a^3,...) = \\ = (\overline{f}(a),\overline{f}(a)a,\overline{f}(a)a^2,\overline{f}(a)a^3,...).$$

Remember that $N[x]$ is 0-symmetric (i.e. for all $f \in N[x]$, $f0 = 0$), but note that $\overline{f}(0) = F(1,0,0,...)$ need not be 0. However, $F(0,0,0,...) = 0$ and if $f$ has height $k$,

$$\begin{aligned} & f = 0 \text{ (zero function) } \Leftrightarrow \\ & \quad \Leftrightarrow f(\alpha_1,\alpha_2,\alpha_3,...) = 0 \text{ (zero in } N^\omega) \text{ for all } \alpha_1,\alpha_2,\alpha_3,... \in N \Leftrightarrow \\ & \quad \Leftrightarrow F(\alpha_1,\alpha_2,...,\alpha_{k+1},0,0,...) = 0 \\ & \qquad \text{(zero in } N) \text{ for all } \alpha_1,\alpha_2,...,\alpha_{k+1} \in N \Longrightarrow \\ & \quad \Longrightarrow \overline{f}(a) = 0 \text{ for all } a \in N. \end{aligned}$$

The converse of this last implication does not hold in general: Consider $f = x + x^2 \in \mathbb{Z}_2[x]$. Clearly $f \neq 0$ (for example, $f(1,1,0,0,0,...) = = (1,0,0,0,...) \neq 0$) but $\overline{f}(0) = 0 = \overline{f}(1)$.

The substitution $\overline{f}(a)$ gives rise to a function $\sigma_a : N[x] \to N$ defined by $\sigma_a(f) = \overline{f}(a)$ for all $f \in N[x]$. Both $N[x]$ and $N$ are (left) $N$-groups and it can be shown that $\sigma_a$ is a surjective $N$-group homomorphism which is the identity on $N$. In general $\sigma_a(fg)$ and $\sigma_a(fb)$ need not coincide with $\sigma_a(f)\sigma_a(g)$ and $\sigma_a(f)b$ respectively for $f,g \in N[x]$ and $b \in N$. What all this means is that $\overline{(f+g)}(a) = \overline{f}(a) + \overline{g}(a)$ and $\overline{bf}(a) = b\overline{f}(a)$ but $\overline{(fg)}(a)$ need not coincide with $\overline{f}(a)\overline{g}(a)$ and $\overline{(fb)}(a)$ need not coincide with $\overline{f}(a)b$ for $b \in N$. We need to know what $\overline{(fg)}(a)$ is. By definition,

$$\begin{aligned} \overline{(fg)}(a) &= (FG)(1,a,a^2,a^3,...) = \\ &= F(G(1,a,a^2,a^3,...),G(a,a^2,a^3,...),G(a^2,a^3,...),...) = \\ &= F(G(1,a,a^2,a^3,...),G(1,a,a^2,a^3,...)a,G(1,a,a^2,a^3,...)a^2,...) = \\ &= F(\overline{g}(a),\overline{g}(a)a,\overline{g}(a)a^2,...). \end{aligned}$$

If $\overline{g}(a)a = a\overline{g}(a)$, then

$$\begin{aligned} \overline{(fg)}(a) &= F(\overline{g}(a),\overline{g}(a)a,\overline{g}(a)a^2,...) = \\ &= F(\overline{g}(a),a\overline{g}(a),a^2\overline{g}(a),...) = \\ &= F(1,a,a^2,a^3,...)\overline{g}(a) = \\ &= \overline{f}(a)\overline{g}(a) \end{aligned}$$

but in general it need not be the case.

The composition of two near-ring polynomials will be required. This, to be defined below, may well be somewhat confusing. Recall that $N \cup \{x\} \subseteq N[x] = [N, N^\omega, x]$ and the latter is the subnear-ring of

$M_N(N^\omega)$ generated by $N \cup \{x\}$. The near-ring multiplication in the near-ring $M_N(N^\omega)$ is the composition of mappings, i.e. if $f, g \in M_N(N^\omega)$, then $fg$ is actually the usual composition of $f$ and $g$, i.e. $(fg)(\alpha) = f(g(\alpha))$. For example, if $f, g \in N[x]$, say $f = a(b+cx)+dx^3$ and $g = r + sx^2$, then the product of $f$ and $g$ in $N[x]$ is the composition of the two functions $f$ and $g$ in $M_N(N^\omega)$ which gives $fg = (a(b+cx)+dx^3)(r+sx^2) = = a(b(r+sx^2)+c(rx+sx^3))+d(rx^3+sx^5)$. That this look just like the product of polynomials of rings, is due to the magic of the mapping $x$. What will be meant by the composition of two near-ring polynomials, will be a binary operation that looks like the composition of two polynomials (by substitution) and should not be confused with the product in $M_N(N^\omega)$ (and $N[x]$).

For $f, g \in N[x]$, define $f \circ g$ by $f \circ g := F(1, g, g^2, ...)$ where $F$ is the associated function of $f$, i.e $f \circ g = \overline{f}(g)$. This is a well-defined operation and the result is again a polynomial in $N[x]$. For example, for $f = a(b+cx)+dx^3$ and $g = r+sx^2$ as above,

$$f \circ g = a(b + c(r+sx^2)) + d[r\{r(r+sx^2)+s(rx^2+sx^6)\}+ \\ + s\{r(rx^2+sx^4)+s(rx^4+sx^6)\}].$$

Again we need to know the associated function of $f \circ g$ in terms of the functions $F$ and $G$ and we need to know $\overline{(fog)}(a)$. For the latter, we know that in general it will not be $\overline{f}(\overline{g}(a))$. Let $h = f \circ g$ with associated function $H$. For any $\alpha \in N^\omega$,

$$H(\alpha) = \pi_1(f \circ g(\alpha)) = \pi_1(F(1, g, g^2, ...)(\alpha)) = \\ = F(\pi_1(\alpha), \pi_1(g(\alpha)), \pi_1(g^2(\alpha)), ...) = F(\alpha_1, G(\alpha), G^2(\alpha), G^3(\alpha), ...).$$

Thus $H = F(G^0, G, G^2, G^3, ...)$ if we use the analogy $G^n(\alpha) = \pi_1(g^n(\alpha))$ for $n \geq 0$ with $g^0 = 1$. The powers of $G$ can be expressed as follows:

$$G^2(\alpha) = G(G(\alpha_1, \alpha_2, \alpha_3, ...), G(\alpha_2, \alpha_3, \alpha_4, ...), G(\alpha_3, \alpha_4, \alpha_5, ...), ...) = \\ = G(G(\alpha), G(x(\alpha)), G(x^2(\alpha)), ...), \text{ i.e. } G^2 = G(G, Gx, Gx^2, ...).$$

In general, $G^{n+1} = G(G^n, G^n x, G^n x^2, ...)$. For $a \in N$, we get

$$\overline{(fog)}(a) = H(1, a, a^2, a^3, ...) = \\ = F(1, G(1, a, a^2, a^3, ...), G^2(1, a, a^2, a^3, ...), G^3(1, a, a^2, a^3, ...), ...) = \\ = F(1, \overline{g}(a), G(\overline{g}(a), \overline{g}(a)a, \overline{g}(a)a^2, \overline{g}(a)a^3, ...), ...),$$

where the last dots do not indicate a necessarily repeating patern; these powers $G^n(1, a, a^2, a^3, ...)$ will each have to be calculated.

We will not pursue this matter here, but the algebraic structure of $(N[x], +, \cdot, \circ)$ can be investigated as a natural near-ring analogue of a composition ring $(R[x], +, \cdot, \circ)$.

To see the properties of substitution in near-ring polynomials in context, we recall a few of the salient properties of polynomials over commutative rings:

(1) For a ring polynomial $f$, we have: $\overline{f}(a) = 0$ if and only if $x - a$ is a factor of $f$.

(2) If $R$ is an integral domain, then any polynomial of degree $n$ over $R$ can have at most $n$ roots in $R$. If we discard commutativity and let $D$ be a division ring, it is known that any polynomial of degree $n$ over $D$ can have either one zero from each of at most $n$ conjugacy classes in $D$ or it will have an infinite number of zeros.

A few examples will indicate some of the exceptional behaviour of substitution in near-ring polynomials. Let $f = (x-a)(x-b) = x^2 - bx - -a(x-b) \in N[x]$, take $N$ to be any near-field. To find a $t \in N$ for which $\overline{f}(t) = 0$, the first reaction is to argue that $\overline{f}(t) = 0 \Leftrightarrow (t-a)(t-b) = 0$ from which $t = a$ or $t = b$ follows since $N$ is a near-field. This is of course not the case - $\overline{f}(t) = F(1, t, t^2, t^3, ...) = t^2 - bt - a(t-b)$ which is 0 when $t = b$, but when $t = a$, this need not be the case (even if $N$ is a non-commutative ring). Another example to highlight the unusual behavior of near-ring polynomials is the following: Let $f = d(x-a) - d(b-a) + +d(b-x) \in N[x]$. Here we take arbitrary distinct elements $a, b, d$ from a near-field $N$; just ensure that $d$ does not distributive over $b - a$. Then $f$ is a non-zero near-ring polynomial of height 1 and it has at least two arbitrary distinct zeros $a$ and $b$. Moreover, even a simple linear equation like $a(b+x) = c + dx$ over a near-field $N$ may not have a solution in $N$ (see Example 4.7 below). It was already mentioned that $\overline{fg}(a)$ need not coincide with $\overline{f}(a)\overline{g}(a)$; neither does $\overline{f}(a) = 0$ imply $\overline{fg}(a) = 0$ and $\overline{f \circ g}(t)$ and $\overline{f}(\overline{g}(t))$ are in general different. Even though substitution is not well-behaved with respect to products and composition of near-ring polynomials, there are some special cases which do facilitate matters. We give some of these and start with:

**Proposition 3.2.** *Let $f \in N[x]$ with height $m$ and associated function $F$. Let $g \in N[x]$ and $a \in N$. Then:*

(i) $fg = F(g, gx, gx^2, ...)$ *and*

(ii) $\overline{fg}(a) = F(\overline{g}(a), \overline{g}(a)a, \overline{g}(a)a^2, ...)$.

**Proof.** By Lemma 3.1 and the commutativity of $x$, we get

$$fg = F(1, x, x^2, x^3, ...)g = F(g, gx, gx^2, ...).$$

The second statement has already been verified above. $\Diamond$

A number of applications of this result are worth recording:

**Corollary 3.3.** *Let $f, g \in N[x]$ with $a \in N$ such that $\overline{g}(a) = 0$. Then $\overline{fg}(a) = 0$ and $\overline{g^n}(a) = 0$ for all $n \geq 1$.*

**Corollary 3.4.** *For $f \in N[x]$ and $a \in N$, $\overline{fx}(a) = \overline{f}(a)a$.*

**Proof.** For $x$, the associated function $X$ is given by $X(\alpha_1, \alpha_2, \alpha_3, ...) = = \alpha_2$. Thus $\overline{x}(a) = X(1, a, a^2, a^3, ...) = a$ and

$$\overline{fx}(a) = F(\overline{x}(a), \overline{x}(a)a, \overline{x}(a)a^2, ...) =$$
$$= F(a, a^2, a^3, ...) = F(1, a, a^2, a^3, ...)a = \overline{f}(a)a. \qquad \Diamond$$

Another application is the following: Let $e \in N$ be a central idempotent, i.e. $e^2 = e$ and $ae = ea$ for all $a \in N$. Define $\gamma_e \colon N[x] \to N$ by $\gamma_e(f) = = \overline{f}(e)$ for all $f \in N[x]$. Clearly $\gamma_e$ preserves addition and for $f, g \in N[x]$, $\gamma_e(fg) = F(\overline{g}(e), \overline{g}(e)e, ..., \overline{g}(e)e^m) = F(1, e, e^2, ..., e^m)\overline{g}(e) = \overline{f}(e)\overline{g}(e) = = \gamma_e(f)\gamma_e(g)$. Thus $\gamma_e$ is a near-ring homomorphism and it is surjective. Two special cases are for $e = 0$ and $e = 1$ which gives respectively $\frac{N[x]}{\ker \gamma_0} \cong N \cong \frac{N[x]}{\ker \gamma_1}$; note $\ker \gamma_0 = \{f \in N[x] \mid \overline{f}(0) = F(1, 0, 0, ...) = 0\}$.

**Proposition 3.5.** *Let $f, g \in N[x]$. If $f$ has height $k \leq 1$, then $\overline{f \circ g}(a) = = \overline{f}(\overline{g}(a))$ for all $a \in N$.*

**Proof.** Let $f, g \in N[x]$ with $h = f \circ g$ and associated functions $F, G$ and $H$. For any $\alpha \in N^\omega$,

$$H(\alpha) = F(\alpha_1, G(\alpha), G^2(\alpha), G^3(\alpha), ...) = F(\alpha_1, G(\alpha), 0, 0, ...)$$

since $f$ has height $\leq 1$. Thus

$$\overline{(f \circ g)}(a) = H(1, a, a^2, a^3, ...) = F(1, \overline{g}(a), 0, 0, ...) =$$
$$= F(1, \overline{g}(a), (\overline{g}(a))^2, (\overline{g}(a))^3, ...) = \overline{f}(\overline{g}(a)). \qquad \Diamond$$

**Proposition 3.6.** *Let $f, g \in N[x]$ with $\overline{f}(0) = 0$ and for some $a \in N$, $\overline{g}(a) = 0$. Then $\overline{f \circ g}(a) = 0$.*

**Proof.** Let $f, g \in N[x]$ with $\overline{f}(0) = 0$ and $\overline{g}(a) = 0$ for some $a \in N$. As seen earlier,

$$\overline{(fog)}(a) = H(1, a, a^2, a^3, ...) =$$
$$= F(1, G(1, a, a^2, a^3, ...), G^2(1, a, a^2, a^3, ...), G^3(1, a, a^2, a^3, ...), ...),$$

$G(1, a, a^2, a^3, ...) = \overline{g}(a) = 0$ and

$$G^2(1, a, a^2, a^3, ...) = G(\overline{g}(a), \overline{g}(a)a, \overline{g}(a)a^2, \overline{g}(a)a^3, ...) = 0.$$

Thus $G^n(1,a,a^2,a^3,...)=0$ for all $n\geq 1$; so $\overline{(fog)}(a)=H(1,a,a^2,a^3,...) = = F(1,0,0,...) = \overline{f}(0) = 0$. ◊

For a near-ring $S$ and $u \in S$, we will use $\langle u]$ (resp. $\langle u\rangle$) to denote the left ideal (resp. ideal) of $S$ generated by $u$. It can be shown that $\langle u] = \bigcup\limits_{n=0}^{+\infty} \mathcal{L}_n$ where $\mathcal{L}_0 = \{u\}$ and for $n \geq 0$, if $\mathcal{L}_0, \mathcal{L}_1, ..., \mathcal{L}_{2n}$ have been defined, let $\mathcal{L}_{2n+1} = \{a(w+b) - ab \mid a, b \in S, w \in \mathcal{L}_{2n}\}$ and $\mathcal{L}_{2n+2} = = \left\{\sum\limits_i^{\text{finite}} (a_i \pm w - a_i \mid a_i \in S, w \in \mathcal{L}_{2n+1}\right\}$. For near-ring polynomials we have a weak form of the Division Algorithm [16]:

**Proposition 3.7.** *Suppose $h \in N[x]$ has the form $h = x^k - p$ where $k \geq 2$ and $p \in N[x]$ has height $\leq k-1$. Then for any $f \in N[x], f = h_1 + r$ where $h_1 \in \langle h]$ and $r \in N[x]$ with $r = 0$ or $r$ has height $\leq k-1$.*

**Proposition 3.8.** *Let $f \in N[x]$ and let $g \in \langle f]$. If $a \in N$ and $\overline{f}(a) = 0$, then $\overline{g}(a) = 0$.*

**Proof.** Let $f, g$ and $a$ be as in the statement. We know $g \in \mathcal{L}_n$ for some $n \geq 0$ where $\langle f] = \bigcup\limits_{n=0}^{+\infty} \mathcal{L}_n$ as defined above. We proceed by induction on $n$. If $n = 0$, then $g = f$ and we are done. If $n = 1$, $g = h(f+w) - hw$ for some $h, w \in N[x]$. Let $G, H, F$ and $W$ be the functions associated with $g, h, f$ and $w$ respectively. Now

$$\begin{aligned}&\overline{g}(a) = H(F(1,a,a^2,a^3,...) + W(1,a,a^2,a^3,...),\\ &F(a,a^2,a^3,...) + W(a,a^2,a^3,...), F(a^2,a^3,...) + W(a^2,a^3,...),...) -\\ &\qquad - H(W(1,a,a^2,a^3,...), W(a,a^2,a^3,...), F(a^2,a^3,...),...) = 0\end{aligned}$$

since

$$F(a^i, a^{i+1}, a^{i+2}, a^{i+3}, ...) = F(1,a,a^2,a^3,...)a^i = \overline{f}(a)a^i = 0$$

for $i = 0,1,2,....$ For $n = 2$, we know $g$ is of the form $g = \sum\limits_i^{\text{finite}} (h_i \pm f_i - h_i)$ where $h_i \in N[x]$ and $f_i \in \mathcal{L}_1$. By the previous step we know that $\overline{f}_i(a) = 0$ for all $i$ and so $\overline{g}(a) = \sum\limits_i^{\text{finite}} (\overline{h_i}(a) \pm \overline{f_i}(a) - \overline{h_i}(a)) = 0$. For the inductive step, we may proceed as above and show that if the statement is true for all $g \in \mathcal{L}_{2n}$, then it is also true for $g \in \mathcal{L}_{2n+1}$ and $g \in \mathcal{L}_{2n+2}$. We thus conclude that for any $g \in \langle f]$, $\overline{g}(a) = 0$. ◊

**Corollary 3.9.** *Let $f \in N[x]$. If $\overline{f}(a) = 0$ for some $a \in N$, then $\langle f] \cap N = 0$.*

**Proof.** Let $g \in \langle f] \cap N$, say $g = b$ where $b \in N$ and $\overline{f}(a) = 0$ for some $a \in N$. By the previous proposition, $b = \overline{g}(a) = 0$. $\Diamond$

**Proposition 3.10.** *Let $f \in N[x]$ and let $a \in N$. Then $\overline{f}(a) = 0$ if and only if $f \in \langle x - a]$ where $\langle x - a]$ denotes the left ideal in $N[x]$ generated by $x - a$.*

**Proof.** If $f \in \langle x - a]$, then $\overline{f}(a) = 0$ follows from Prop. 3.7. Suppose thus $\overline{f}(a) = 0$. By the Division Algorithm (3.7), $f = h + r$ where $h \in \langle x - a]$ and $r \in N[x]$ with $r = 0$ or $r$ has height $< 1$. This means $r \in N$ and $0 = \overline{f}(a) = \overline{h}(a) + r = r$. Hence $f = h \in \langle x - a]$. $\Diamond$

**Corollary 3.11.** *Let $f \in N[x]$ and let $a \in N$. Then $f - \overline{f}(a) \in \langle x - a]$.*

As for rings, when $f \in N[x]$ is divided by $h = x - a, a \in N$, then the remainder is $\overline{f}(a)$. Indeed, by the Division Algorithm, $f = g + r$ for some $g, r \in N[x]$ with $g \in \langle h]$ and $r = 0$ or $0 \neq r \in N$. Since $g \in \langle h]$, we have $\overline{f}(a) = \overline{g}(a) + r = r$.

Any $f \in N[x]$ determines a function $\overline{f} \colon N \to N$ defined by $a \mapsto \overline{f}(a)$. As is to be expected from the theory of polynomials in general, these maps are compatible (cf. 7.121 in Pilz [13]):

**Proposition 3.12.** *Let $I \lhd N, f \in N[x]$ and $a, b \in N$. If $a - b \in I$, then $\overline{f}(a) - \overline{f}(b) \in I$.*

**Proof.** Note firstly that for $a - b \in I$, $c \in N$ and any $n \geq 1$, always $ca^n - cb^n \in I$. This follows by an inductive argument since $ca^n - cb^n = = ca^{n-1}((a - b) + b) - ca^{n-1}b + (ca^{n-1} - cb^{n-1})b$. The proof can then be completed by induction on the level of $f$. $\Diamond$

Likewise, by using induction, it can be proved that

**Proposition 3.13.** *Let $I$ be a left ideal of $N$ and let $f \in N[x]$. If $a \in I$, then $\overline{f}(a) - \overline{f}(0) \in I$.*

Because of the way substitution with near-ring polynomials over a commuting indeterminate $x$ is defined here, the next result is slightly different from its universal algebraic counterpart (see Pilz [13], 7.123).

**Proposition 3.14.** *For any $a \in N$, $\langle a] = \{\overline{f}(a) \mid f \in N[x], \overline{f}(0) = 0\}$.*

**Proof.** Let $B = \{\overline{f}(a) \mid f \in N[x], \overline{f}(0) = 0\}$. We show that $B$ is a left ideal of $N$ for which $a \in B \subseteq \langle a]$. Firstly, $a = \overline{g}(a)$ for $g = = x \in N[x]$ and if $f \in N[x]$ with $\overline{f}(0) = 0$ we have $\overline{f}(a) \in \langle a]$. For $f, g \in N[x], \overline{f}(a) - \overline{g}(a) = \overline{(f - g)}(a) \in B$ and for any $b \in N$, $b + f - b \in \in N[x]$ and $b + \overline{f}(a) - b = \overline{(b + f - b)}(a) \in B$. Lastly, for $b, c \in N$, $b(\overline{f}(a) + c) - bc = \overline{(b(f + c) - bc)}(a) \in B$. $\Diamond$

This result is useful in that it connects elements of a near-ring with left ideals via polynomials. What this means is that if some property of elements in a near-ring can be defined in terms of polynomials, it provides a way to connect this to ideals; a connection that is often quite elusive in near-ring theory. We give one example. A nonzero element $b$ in a near-ring $N$ is called a *generalized unit* if there is a $g \in N[x]$ such that $\overline{g}(b) = 1$ and $\overline{g}(0) = 0$. If $N$ is a ring, then $b$ is a generalized unit if and only if $b$ has a left inverse. Thus, a ring $R$ is a division ring if and only if $R$ has an identity and every nonzero element is a generalized unit. Using the proposition above, it can be shown that a near-ring $N$ has no non-trivial left ideals if and only if every nonzero element of $N$ is a generalized unit. It can also be mentioned that the $g \in N[x]$ which makes $b$ a generalized unit can be chosen, without any loss of generality, of height 1. Indeed, if $g$ has height $m \geq 2$ and associated function $G$, we may regard $G$ as a function $G : N^{m+1} \to N$. Let $f$ be the polynomial defined by $f := G(1, x, bx, b^2x, ..., b^{m-1}x)$. Then $f \in N[x]$, $\overline{f}(0) = G(1, 0, 0, ..., 0) = = \overline{g}(0) = 0$ and $\overline{f}(b) = G(1, b, b^2, b^3, ..., b^m) = \overline{g}(b) = 1$. We show $f$ has height 1. Let $F$ be the function associated with $f$. For any $\alpha = = (\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega$, $F(\alpha_1, \alpha_2, \alpha_3, ...) = \pi_1(G(1, b, b^2, b^3, ..., b^m)(\alpha)) = = G(\alpha_1, \alpha_2, b\alpha_2, b^2\alpha_2, ..., b^{m-1}\alpha_2) = F(\alpha_1, \alpha_2, 0, 0, ...)$. Thus $f$ has height $\leq 1$. If its height is 0, then $f = a \in N$ for some $a \neq 0$. Then $a = \pi_1(a(1, 0, 0, ...)) = \pi_1(f(1, 0, 0, ...)) = F(1, 0, 0, ...) = \overline{f}(0) = 0$; a contradiction. Thus $height(f) = 1$.

## 4. Polynomial functions

Any $f \in N[x]$ determines a function $\overline{f} : N \to N$ defined by $a \mapsto \overline{f}(a)$. This function is called a *polynomial function* and the set of all polynomial functions of $N$ will be denoted by $\mathcal{P}(N)$. It is clearly contained in the set $\mathcal{M}(N)$ of all functions from $N$ to $N$ and it is of some importance to know if or when the equality will hold. For a commutative ring $R$ with identity, we know $\mathcal{P}(R) = \mathcal{M}(R)$ if and only if $R$ is a finite field. For arbitrary rings $R$, not necessarily commutative and not necessarily with identity, it is known that the set of all polynomial functions on $R$ coincides with $\mathcal{M}(R)$ if and only if $R$ is either the trivial ring of order 1 or 2, or for some $n$ and some finite field $F$, $R = \mathbb{M}_n(F)$, cf. [3]. It should be mentioned that in this result, polynomial means generalized polynomial in the sense that the indeterminate is not commuting and one has to cater for different terms like $ax$ and $xa$. We will show that for a 0-symmetric near-ring $N$, $\mathcal{P}(N) = \mathcal{M}(N)$ if and only if $N$ is a finite near-field.

For universal algebras, it is known that if the set of polynomial functions coincides with the set of all functions, then the algebra must necessarily be simple and finite [8]. The near-ring polynomial functions considered here are more restrictive since we are dealing with a commuting indeterminate and we cannot directly use this result.

We start by discussing some other ways in which near-ring polynomial functions can be viewed and also look at a few related issues. The set $\mathcal{M}(N)$ is a near-ring with respect to pointwise addition and composition and is different to and should not be confused with the near-ring $N^N$ which denotes the direct sum of $|N|$ copies of $N$. Both these near-rings contains $N$ as a subnear-ring: in $\mathcal{M}(N)$ an element $a \in N$ is regarded as the function $a : N \to N$ defined by $a(t) = at$ for all $t \in N$ and in $N^N$, $a : N \to N$ is the constant function $a(t) = a$ for all $t \in N$. The underlying groups of these two near-rings coincide and can be turned into an $N$-group with respect to the canonical product provided by the mentioned embeddings. In both cases, this lead to $af : N \to N$ defined by $(af)(t) = af(t)$ for all $t, a \in N$ and $f \in (\mathcal{M}(N), +) = (N^N, +)$; hence as $N$-groups we also have $(\mathcal{M}(N), +) = (N^N, +)$. For $n \geq 1$, let $u^n : N \to N$ denote the function $u^n(t) = t^n$ for all $t \in N$. Let $\mathcal{B} = \{u^n \mid n \geq 1\} \cup N$ and let $\overline{\mathcal{B}}$ be the $N$-subgroup of $N^N$ generated by $\mathcal{B}$. It can then be shown that $\mathcal{B} \subseteq \mathcal{P}(N) \subseteq \overline{\mathcal{B}}$. Indeed, $u^n$ coincides with the polynomial function $\overline{f}$ for $f = x^n \in N[x]$. The second inclusion can easily be shown by induction on the level of the polynomials $f \in N[x]$. Since $\mathcal{P}(N)$ is an $N$-subgroup of $N^N$, we conclude that $\mathcal{P}(N) = \overline{\mathcal{B}}$.

Let $\mathcal{P}_{UA}(N)$ denote the polynomial functions on the near-ring $N$ in the universal algebraic sense. This means $\mathcal{P}_{UA}(N)$ is the subnear-ring of the near-ring $N^N$ generated by $N \cup \{1_N\}$ where $1_N : N \to N$ denotes the identity function on $N$. In the canonical way, $\mathcal{P}_{UA}(N)$ is an $N$-subgroup of $N^N$ which contains $\mathcal{B}$. Hence $\mathcal{P}(N) = \overline{\mathcal{B}} \subseteq \mathcal{P}_{UA}(N)$ follows and in general the latter inclusion is strict as was mentioned above.

For the near-ring $N$, let $\Omega = \Omega_N := \{\eta_a \mid a \in N\}$ where $\eta_a : N \to N$ is the function $\eta_a(t) = at$ for all $t \in N$. Every $\eta_a$ can be regarded as a unary operation on $N$ and $N^\Omega := (N, +, \Omega)$ is an $\Omega$-group. Let $\mathcal{P}_\Omega(N^\Omega)$ denote the polynomial functions of $N^\Omega$ in the universal algebraic sense (i.e. the $\Omega$-subgroup of $(N^\Omega)^{N^\Omega}$ generated by $N \cup \{1_{N^\Omega}\}$). Since

$N \cup \{1_{N^\Omega}\} \subseteq \mathcal{P}(N)$ and $\mathcal{P}(N)$ is an $\Omega$-subgroup of $(N^\Omega)^{N^\Omega}$, $\mathcal{P}_\Omega(N^\Omega) \subseteq$ $\subseteq \mathcal{P}(N)$ follows.

Substitution in polynomials, as was defined in the previous section, can be looked at differently as we now describe: Let $k \geq 1$ and let $G = N^{N^k}$. Embed $N$ in $G$ by treating $a \in N$ as a constant function. With $\Omega$ as above, $G^\Omega := (G, +, \Omega)$ is an $\Omega$-group where the unary operation $\eta_a : G \to G$ is defined by $(\eta_a g)(\alpha) = ag(\alpha)$ for $g \in G$ and $\alpha \in N^k$. Let $\mathcal{P}_k(N)$ be the $\Omega$-subgroup of $G^\Omega$ generated by $N \cup \{\pi_1, \pi_2, ..., \pi_k\}$ where $\pi_i : N^k \to N$ is the $i$-th projection. This means $\mathcal{P}_k(N)$ consists of all the $k$-place polynomial functions in the universal algebraic sense. For $f \in N[x]$ with associated polynomial function $\overline{f}$, we show there is a $k \geq 1$ and $p \in \mathcal{P}_k(N)$ such that $\overline{f}(t) = p(t, t^2, ..., t^k)$ for all $t \in N$. Let $k$ be the height of $0 \neq f \in N[x]$. Thus $k + 1 = \min\{n \mid n \geq 1$ and $F(\alpha) = \pi_1(f(\alpha_1, \alpha_2, ..., \alpha_n, 0, 0, 0, ...)$ for all $\alpha = (\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega\}$. If $F$ is the associated function of the polynomial $f$, we may thus regard $F$ as a function $F : N^{k+1} \to N$ since $F(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k, \alpha_{k+1}, \alpha_{k+2}, ...) =$ $= F(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k, \alpha_{k+1}, \beta_{k+2}, \beta_{k+3}, ...)$ for all $\alpha = (\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega$ and $\beta_{k+2}, \beta_{k+3}, ... \in N$. If we let $p : N^k \to N$ be defined by

$$p(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k) := F(1, \alpha_1, \alpha_2, \alpha_3, ..., \alpha_k)$$

for all $(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k) \in N^k$, it can be shown that $\overline{f}(t) = p(t, t^2, ..., t^k)$ for all $t \in N$ and $p \in \mathcal{P}_k(N)$. The latter membership follows by an inductive argument on the level of the polynomial $f$.

**Proposition 4.1.** *Let $N$ be a 0-symmetric near-ring with identity. Then $\mathcal{P}(N) = \mathcal{M}(N)$ if and only if $N$ is a finite near-field.*

**Proof.** Suppose $\mathcal{P}(N) = \mathcal{M}(N)$. If $\mathcal{P}_{UA}(N)$ denotes the set of all polynomial functions over the near-ring $N$ in the universal algebraic sense, then $|\mathcal{P}_{UA}(N)| \geq |\mathcal{P}(N)| = |\mathcal{M}(N)|$ (cf. [8],§11.3). Thus $N$ must be finite and simple. Next we show that $N$ has no nonzero proper left ideals. If $I$ is a nonzero proper left ideal of $N$, choose $0 \neq a \in I$ and $b \in N - I$. Define the function $g : N \to N$ by

$$g(t) = \begin{cases} b \text{ if } t \neq 0 \\ 0 \text{ if } t = 0. \end{cases}$$

Then $g(a) - g(0) = b \notin I$ and by Prop. 3.12 $g$ cannot be a polynomial function. Hence $N$ has no non-trivial left ideals and thus also no nonzero left zero divisors (since for any $c \in N$, the left annihilator $(0 : c)_N :=$ $:= \{n \in N \mid nc = 0\}$ is a left ideal of $N$). Because $N$ is finite, this means every nonzero element has a left inverse and so $N$ is a finite near-field.

For the converse, suppose $N$ is a finite (0-symmetric) near-field. If $N$ happens to be a field, we are done. Suppose thus $N$ is a proper near-field; say $a(b+c) \neq ab + ac$ for some $a, b, c \in N$. Let $\Omega = \{\eta_d \mid d \in N\}$ be as above. Then the $\Omega$-group $N^{\Omega} = (N, +, \Omega)$ is simple. Now $p := \eta_a x = ax$ is a unary polynomial over $N^{\Omega}$ with $p(0) = 0$ but $p$ is not a group homomorphism $(p(b+c) \neq p(b) + p(c))$. This means the $\Omega$-group $N^{\Omega}$ is polynomially complete, i.e. $\mathcal{P}_{\Omega}(N^{\Omega}) = N^N$ (see, for example, [7]). Since $\mathcal{P}_{\Omega}(N^{\Omega}) \subseteq \mathcal{P}(N) \subseteq N^N$, we may conclude that $\mathcal{P}(N) = \mathcal{M}(N)$. $\Diamond$

Next we describe a method of constructing a polynomial over a near-field with (at least) a given number of zeros. For a near-field $N$ and $b_i \in N, i \geq 0$, define a sequence $v(b_1, b_0), v(b_2, b_1, b_0), v(b_3, b_2, b_1, b_0), ...$ of elements in $N$ by:

$$v(b_1, b_0) = \begin{cases} (b_1 - b_0)b_1(b_1 - b_0)^{-1} \text{ if } b_1 \neq b_0 \\ b_1 \text{ otherwise} \end{cases}$$

and if $v(b_n, b_{n-1}, ..., b_1, b_0)$ has been defined for any $n+1$ arguments $b_n, b_{n-1}, ..., b_1, b_0 \in N, n \geq 1$, let

$$v(b_{n+1}, b_n, ..., b_1, b_0) = v(v(b_{n+1}, b_{n-1}, ..., b_1, b_0), v(b_n, b_{n-1}, ..., b_1, b_0)).$$

By abuse of notation, we also write $v(x, b) = (x - b)x(x - b)^{-1}$ (and as above also for $v(x, b_n, ..., b_1, b_0)$), but it should be emphasized that this is just a convenient notation and these expressions are certainly not polynomials. When $N$ is commutative, then $v(b_n, b_{n-1}, ..., b_1, b_0) = b_n$ for any $n \geq 1$.

In the proof below, we often use Cor. 3.3 to facilitate the substitution.

**Proposition 4.2.** *Let $N$ be a near-field and let $a_0, a_1, a_2, ..., a_n$ be elements from $N$. Then*

$$g := (v(x, a_{n-1}, ..., a_1, a_0) - v(a_n, a_{n-1}, ..., a_1, a_0))(v(x, a_{n-2}, ..., a_1, a_0) - \\ - v(a_{n-1}, ..., a_1, a_0))...(v(x, a_0) - v(a_1, a_0))(x - a_0)$$

*is a near-ring polynomial of height $n+1$ over $N$. For any $b \in N$,*

$$\overline{g}(b) = (v(b, a_{n-1}, ..., a_1, a_0) - v(a_n, a_{n-1}, ..., a_1, a_0))(v(b, a_{n-2}, ..., a_1, a_0) - \\ - v(a_{n-1}, ..., a_1, a_0))...(v(b, a_0) - v(a_1, a_0))(b - a_0).$$

*Moreover, $\overline{g}(b) = 0$ if and only if $x = a_0$ or $v(b, a_0) = v(a_1, a_0)$ or ... or $v(b, a_{n-1}, ..., a_1, a_0) = v(a_n, a_{n-1}, ..., a_1, a_0)$.*

**Proof** (by induction on $n \geq 0$). Clearly $g_0 := x - a_0$ is a near-ring polynomial of height 1, $\overline{g_0}(b) = b - a_0$ and $g_0$ has unique zero $a_0$. Note that $v(x, a_0)g_0 = g_0x$ and for any $b \in N, v(b, a_0)\overline{g_0}(b) = \overline{g_0}(b)b$. Let $g_1 := (v(x, a_0) - v(a_1, a_0))g_0$. Then $g_1 = g_0x - v(a_1, a_0)g_0$ is a near-ring polynomial of height 2 over $N$ and $\overline{g_1}(b) = \overline{g_0}(b)b - v(a_1, a_0)\overline{g_0}(b) =$ $= (v(b, a_0) - v(a_1, a_0))\overline{g_0}(b) = (v(b, a_0) - v(a_1, a_0))(b - a_0)$. Thus $\overline{g_1}(b) = 0$ if and only if $v(b, a_0) = v(a_1, a_0)$ or $b = a_0$. Note that $v(x, a_1, a_0)g_1 = g_1x$ and for each $b \in N$, $v(b, a_1, a_0)\overline{g_1}(b) = \overline{g_1}(b)b$. Suppose the near-ring polynomials $g_0, g_1, ..., g_{n-1}$ have been defined where:

(i) $g_i$ has height $i + 1$ for $i = 0, 1, 2, ..., n - 1$.

(ii) for each $b \in N$,

$$\overline{g_{n-1}}(b) = (v(b, a_{n-2}, ..., a_1, a_0) - v(a_{n-1}, a_{n-2}, ..., a_1, a_0))$$

$$(v(b, a_{n-3}, ..., a_1, a_0) - v(a_{n-2}, ..., a_1, a_0))...(v(b, a_0) - v(a_1, a_0))(b - a_0),$$

(iii) $\overline{g_{n-1}}(b) = 0$ if and only if

$$v(b, a_{n-2}, ..., a_1, a_0) = v(a_{n-1}, a_{n-2}, ..., a_1, a_0) \text{ or}$$
$$v(b, a_{n-3}, ..., a_1, a_0) = v(a_{n-2}, ..., a_1, a_0) \text{ or ... or}$$
$$v(b, a_0) = v(a_1, a_0) \text{ or } b = a_0,$$

(iv) $v(x, a_{n-1}, a_{n-2}, ..., a_1, a_0)g_{n-1} = g_{n-1}x$ and

(v) $v(b, a_{n-1}, a_{n-2}, ..., a_1, a_0)\overline{g_{n-1}}(b) = \overline{g_{n-1}}(b)b$.

Let $g_n := (v(x, a_{n-1}, ..., a_1, a_0) - v(a_n, a_{n-1}, ..., a_1, a_0))g_{n-1}$. Then

$$g_n = v(x, a_{n-1}, ..., a_1, a_0)g_{n-1} - v(a_n, a_{n-1}, ..., a_1, a_0)g_{n-1} =$$
$$= g_{n-1}x - v(a_n, a_{n-1}, ..., a_1, a_0)g_{n-1}.$$

For any $b \in N$,

$$\overline{g_n}(b) = \overline{g_{n-1}}(b)b - v(a_n, a_{n-1}, ..., a_1, a_0)\overline{g_{n-1}}(b) =$$
$$= (v(b, a_{n-1}, ..., a_1, a_0) - v(a_n, a_{n-1}, ..., a_1, a_0))\overline{g_{n-1}}(b)$$

as required. Also, $g_n$ has height $n + 1$ the last statement about the zeros of the polynomial $g_n$ follows since $N$ has no nonzero zero-divisors. $\Diamond$

The result above ensures that $g$ has zeros $a_0, a_1, a_2, ..., a_n$, but they need not be the only ones. For example, $v(b, a_0) = v(a_1, a_0)$ may hold for $b$ other than $b = a_1$ as can be seen in Example 4.5 below. When $N$ is a field, the polynomial $g$ above reduces to the familiar

$$g := (x - a_n)(x - a_{n-1})...(x - a_1)(x - a_0).$$

The next result is striking in its simplicity and is hardly worth singling out, but this belies its significance. It shows that if there are enough non-distributivity in a near-ring, near-ring polynomials of height 1 and any finite number of zeros can be constructed (even over a near-field).

**Lemma 4.3.** *Let $N$ be a near-ring with $f, g \in N[x]$, both of height $\leq k$ for some $k \geq 1$. Suppose $f$ and $g$ have zeros $a_1, a_2, ..., a_n$ and $b_1, b_2, ..., b_m$ in $N$ respectively. If there is $d \in N$ such that $d$ does not distribute over $f+g$, then $h := df - d(g+f) + dg$ is a non-zero near-ring polynomial of height $\leq k$ over $N$. Each of $a_1, a_2, ..., a_n, b_1, b_2, ..., b_m$ is a zero for $h$ (and there could be other zeroes as well).*

The last result, before we conclude with an example, has an exact counterpart for rings (see [17]). The proof below uses the same idea, but is slightly more involved.

**Proposition 4.4.** *Let $N$ be a $0$-symmetric near-ring with identity. Suppose every nonzero $f \in N[x]$ has at most a finite number of zeros in $N$. Then $N$ is finite or $N$ has no nonzero zero-divisors.*

**Proof.** If $N$ is finite, we are done; suppose $N$ is infinite. Choose $a, b \in N$ with $ba = 0$ and both $a$ and $b$ nonzero. Let $\theta : N \to N$ be the group homomorphism defined by $\theta(t) = tb$ for all $t \in N$. Since $N$ is infinite, either $\ker\theta$ or $\operatorname{Im}\theta$ must be infinite.

Suppose $\ker\theta$ is infinite. Then there is an infinite sequence $t_1, t_2, t_3, ...$ of distinct elements of $N$ such that $t_i b = 0$ for all $i$. If the sequence $bt_1, bt_2, bt_3, ...$ has infinitely many distinct terms, then $f := x^2$ is a nonzero polynomial in $N[x]$ with an infinite number of zeros in $N$; a contradiction. Thus there is some $k \geq 1$ such that $bt_k = bt_{k+1} = bt_{k+2} = ....$ Let $f := bt_k - bx$. Then $f \in N[x]$ and it is not zero. Indeed, if it is zero, then for all $a_1, a_2, a_3, ... \in N, 0 = f(a_1, a_2, a_3, ...) = (bt_k a_1 - ba_2, bt_k a_2 - ba_3, ...)$. For $a_1 = 0$ and $a_2 = 1$ we get the contradiction $b = 0$. Hence $f$ is nonzero and it has infinitely many distinct zeros $t_k, t_{k+1}, t_{k+2}, ...$; again a contradiction.

Suppose thus $\operatorname{Im}\theta = Nb$ is infinite, say $t_1 b, t_2 b, t_3 b, ...$ is an infinite sequence of distinct elements from $Nb$. If the sequence $at_1 b, at_2 b, at_3 b, ...$ has infinitely many distinct terms, the nonzero polynomial $f := x^2$ has infinitely many distinct zeros. If not, there is some $k \geq 1$ with $at_k b = $ $= at_{k+1} b = at_{k+2} b = ....$ Since $a \neq 0$, it can be shown that $f :=$ $:= at_k b - ax$ is a non-zero polynomial with infinitely many distinct zeros $t_k b, t_{k+1} b, t_{k+2} b, ...$ which again contradicts our assumption. We conclude that $a = 0$ or $b = 0$. $\Diamond$

**Example 4.5.** Let $N$ be the Dickson near-field on $GF(3^2)$. This means $N = \{a + bt \mid a, b = 0, 1, 2\}$ with addition $(a + bt) + (c + dt) =$ $= (a + c) + (b + d)t$ (modulo 3). The multiplication is given in the table below in which all the products $s0 = 0 = u0$ for all $s, u \in N$ have been omitted:

| | $1$ | $2$ | $t$ | $2t$ | $1+t$ | $1+2t$ | $2+t$ | $2+2t$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $2$ | $t$ | $2t$ | $1+t$ | $1+2t$ | $2+t$ | $2+2t$ |
| $2$ | $2$ | $1$ | $2t$ | $t$ | $2+2t$ | $2+t$ | $1+2t$ | $1+t$ |
| $t$ | $t$ | $2t$ | $2$ | $1$ | $1+2t$ | $2+2t$ | $1+t$ | $2+t$ |
| $2t$ | $2t$ | $t$ | $1$ | $2$ | $2+t$ | $1+t$ | $2+2t$ | $1+2t$ |
| $1+t$ | $1+t$ | $2+2t$ | $2+t$ | $1+2t$ | $2$ | $t$ | $2t$ | $1$ |
| $1+2t$ | $1+2t$ | $2+t$ | $1+t$ | $2+2t$ | $2t$ | $2$ | $1$ | $t$ |
| $2+t$ | $2+t$ | $1+2t$ | $2+2t$ | $1+t$ | $t$ | $1$ | $2$ | $2t$ |
| $2+2t$ | $2+2t$ | $1+t$ | $1+2t$ | $2+t$ | $1$ | $2t$ | $t$ | $2$ |

The following can be verified:

(1) $v(1+2t, t) = 2+t = v(2+t, t)$ but $1+2t \neq 2+t$.

(2) The polynomial $h = t(1+t+x) + t + (1+t)x$ has no zeros in $N$.

(3) Using Lemma 4.3 (repeatedly), we will construct a non-zero polynomial $f$ of height 1 over $N$ which has as zeros all the elements of $N$ except $2+2t$.

$f_1 := t(1+2x) + 2t + tx$ is a non-zero polynomial ($\overline{f_1}(t) = 1+t$) of height 1 and has zeros $0, 1$ and $2$.

$f_2 := t(2t+2x) + 1 + t(x+2t)$ is a non-zero polynomial ($\overline{f_2}(1) = 2$) of height 1 and has zeros $0, t$ and $2t$.

Thus, $f_3 := tf_1 + 2t(f_1 + f_2) + tf_2$ is a non-zero polynomial ($\overline{f_3}(1+t) = t$) of height 1 and with zeros $0, 1, 2, t$ and $2t$.

$f_4 := t(x+2+2t) + 2t + t(2+t+2x)$ is a non-zero polynomial ($\overline{f_4}(0) = t$) of height 1 and with zeros $0, 1+t$ and $2+t$.

$f_5 := tf_4 + 2t(f_4 + x + 2 + t) + t(x+2+t)$ is a non-zero polynomial ($\overline{f_5}(0) = 1$) of height 1 and with zeros $1+t, 2+t$ and $1+2t$.

Thus, $f := tf_3 + 2t(f_3 + f_5) + tf_5$ is a polynomial of height 1 with all elements of $N$ as zeros except $2+2t$ since $\overline{f}(2+2t) = 2 \neq 0$.

**Acknowledgements.** Thanks are due to the unknown referee for suggesting the inclusion of the alternative and related polynomial functions described at the beginning of Sec. 4 and also for the proof of the converse of Prop. 4.1.

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

## References

[1] BAGLEY, S.: *Polynomial near-rings, distributor ideals and $J_2$ ideals of generalized centralizer near-rings*, Doctoral dissertation, Texas A&M University, 1993.

[2] BAGLEY, S.: Polynomial near-rings: Polynomials with coefficients from a near-ring, in: *Nearrings, Nearfields and Loops* (Editors: Saad, Thomsen), Kluwer Academic Publishers, Netherlands, 1997, 179–190.

[3] BRAWLEY, J. V. and CARLITZ, L.: A characterization of the $n \times n$ matrices over a finite field, *Amer. Math. Monthly* **80** (1973), 670–672.

[4] CLAY, J. R.: *Nearrings: Geneses and Applications*, Oxford Science Publications, New York, 1992.

[5] FARAG, M.: *On the structure of polynomial near-rings*, Doctoral dissertation, Texas A&M University, 1999.

[6] FARAG, M.: A new generalization of the center of a near-ring with applications to polynomial near-rings, *Comm. Algebra* **29** (2001), 2377–2387.

[7] KAARLI, K. and PIXLEY, A. F.: *Polynomial completeness in algebraic systems*, Chapman and Hall/CRC, 2001.

[8] LAUSCH, H. and NÖBAUER, W.: *Algebra of Polynomials*, North Holland, Amsterdam, 1973.

[9] LEE, E. K. S.: Theory of polynomial near-rings, *Comm. Algebra* **32** (2004), 1619–1635.

[10] LEE, E. K. S. and GROENEWALD, N. J.: Polynomial near-rings in $k$ indeterminates, *Bull. Austral. Math. Soc.* **70** (2004), 441–449.

[11] LE RICHE, L. R., MELDRUM, J. D. P. and VAN DER WALT, A. P. J.: On group near-rings, *Arch. Math.* **52** (1989), 132–139.

[12] MELDRUM, J. D. P. and VAN DER WALT, A. P. J.: Matrix near-rings, *Arch. Math.* **47** (1986), 312–319.

[13] PILZ, G.: *Near-rings*, North Holland, Amsterdam, 1983.

[14] VELDSMAN, S.: Homomorphic images of polynomial near-rings, *Contr. Algebra and Geometry* **50** (2009), 119–142.

[15] VELDSMAN, S.: Polynomial and matrix near-rings, *Arabian Journal for Science and Engineering* **36** (2011), 1039–1046.

[16] VELDSMAN, S.: Polynomial and matrix near-rings, II, *Southeast Asian Bull. Math.* To appear.

[17] Problem E 2098, *Amer. Math. Monthly* **76** (1969), 561–562.