Polynomial near-rings

Stefan Veldsman
Near-ring conference, Vorau (Austria, July 2009)

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

1 Introduction

The study of polynomials, in one form or another, is probably one of the oldest entities studied in mathematics. From ancient times, through the middle ages, the renaissance and moden times, polynomial functions and related topics played a central role in the development of mathematics in most cultures. The Hindus knew how to solve quadratics in 600 BC, and the Babylonians by then had developed considerable skill at algebraic manipulation and were using special cases of the quadratic formula. Symbolic algebra as we know it today, developed in Arabia between 600 and 1000 AD. They were solving cubic equations and, in the work of Al-Khowarizmi (c. 825), they were starting to identify geometric magnitudes with numbers. These led to formulas for areas, volume, etc. By Descarte's time (1596 - 1658), analytic geometry was well understood, so that the computational power of algebra and the intuitive power of geometry could each enhance the other.

Subsequently the theory of equations attracted the attention of the best mathematicians. Euler (1707 - 1783) and Lagrange (1736 - 1813) considered the problem of finding a general formula, analogous to the quadratic formula, for the roots of any polynomial of degree 5. Their work led to the epoch making discoveries of Abel (1802 - 1829) and Galois (1811 - 1832), who brought groups into the picture.

The general study of curves and surfaces obtained as the graphs of polynomials is known as algebraic geometry. Invariant theory, which dates from the time of Cayley (1821 - 1895) and Sylvester (1814 - 1897), is the study of which properties of a curve or surface remain invariant under certain transformations related to polynomials. And I hardly need to mention the hype and influence of elliptic curves and related topics during the last two decades.

Heinrich Hertz (1857 - 1894), the well-known German physicist from Hamburg, said of polynomials:

"One cannot escape the feeling that these mathematical formulae have an independent existence and an intelligence of their own, that they are wiser than we are, wiser even than their discoverers, that we get more out of them than was originally put into them."

(By the way, Hertz knew both Arabic and Sanskrit.)

Polynomials functions did not escape the formalism which became part and parcel of mathematics in the twentieth century. This formal approach to polynomials is the basis of the book of Lausch and Nobauer, (H. LAUSCH and W. NÖBAUER. *Algebra of Polynomials*. North Holland, Amsterdam, 1973), 36 years ago. A polynomial over a given algebraic structure is just a free algebra in which expressions are reduced by the rules of the variety in which considerations are taking place. As such, polynomials over near-rings are well-defined algebraic entities, but rather akward to deal with; even to such an extent the very little, if any at all, were published on this topic.

About 25 years ago, a refreshing new look at what should constitute a matrix near-ring, also led to a model for polynomial near-rings. This proposed model for polynomial near-rings was suggested by Andries van der Walt, but it it was Scott Bagley who took up the idea and set the ball rolling. Apart from his contributions there were a few others, but the cupboard remains embarrassingly bare.

In my talk today, I will briefly survey what has been done. Following that, I will discuss relationships between polynomial near-rings and matrix near-rings and finally, I want to say something about substitutions and polynomial functions - the aim, of course, is to characterize those near-rings for which the polynomial functions are exactly representative of all the self-maps on the near-ring.

I need to start with two warnings:

Firstly, near-rings of polynomials should not be confused with polynomial near-rings. Typically, a near-ring of polynomials is a set of polynomials over a (commutative) ring (with identity) which is a near-ring with respect to the usual addition and composition of ring polynomials. These near-rings have been studied extensively and their theory and applications can be found in the books by Pilz and Clay. A polynomial near-ring, on the other hand, is a near-ring of polynomials in the universal algebraic sense, see for example Lausch and Nöbauer. I will discuss polynomial near-rings in this latter sense, following the model proposed by van der Walt.

Secondly, the theory of polynomial near-rings is still in its infancy; many of the concepts and tools are certainly not yet well-established. Much of what has been done and what I will talk about today may well not stand the test of time. Moreover, the words of Thomas Huxley (1825 - 1895), the well-known English biologist and supporter of Darwin's theory of evolution, often rings true here:

"The great tradegy of science - the slaying of beautiful hypothesis by ugly fact."

What then are polynomial near-rings?

Let N be a 0-symmetric near-ring with identity and let 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. With respect to the usual left and right scalar multiplication, N^k is a unital two-sided faithful $N-N$-bigroup. What is meant by this, is that there are mappings $N \times N^k \to N^k$ and $N^k \times N \to N^k$, given by $n\alpha = n(\alpha_1, \alpha_2, \alpha_3, ...) = (n\alpha_1, n\alpha_2, n\alpha_3, ...)$ and $\alpha n = (\alpha_1, \alpha_2, \alpha_3, ...)n = (\alpha_1 n, \alpha_2 n, \alpha_3 n, ...)$ respectively such that $(n+m)\alpha = n\alpha + m\alpha, (\alpha+\beta)n = \alpha n + \beta n, (nm)\alpha = n(m\alpha), \alpha(nm) = (\alpha n)m$ and $(n\alpha)m = n(\alpha m)$ for all $\alpha, \beta \in N^k$ and $n, m \in N$. All actions are unital and N^k is two-sided faithful, i.e. $nN^k = 0$ implies $n = 0$ and $N^k n = 0$ implies $n = 0$.

As is well-known, $M_N(N^k) := \{f \in M_0(N^k) \mid f(\alpha n) = f(\alpha)n$ for all $\alpha \in N^k, n \in N\}$ is a subnear-ring of $M_0(N^k)$. By the left-faithfulness, N can be embedded in $M_N(N^k)$ via $\eta : N \to M_N(N^k)$ defined by $\eta(a) := \eta_a, \eta_a(\alpha) := a\alpha$ for all $\alpha \in N^k$. We identify $a \in N$ with η_a in $M_N(N^k)$ and note that the identity map on N^k is then the identity of N.

Any $u \in M_N(N^k) - N$ will be called an *indeterminate*. A *commuting indeterminate* is an indeterminate which is an $N-N$-homomorphism, i.e. $u(n\alpha) = nu(\alpha)$, $u(\alpha n) = u(\alpha)n$ and $u(\alpha+\beta) = u(\alpha)+u(\beta)$ for all $\alpha, \beta \in N^k$ and $n \in N$. For an indeterminate u, let $[N, N^k, u]$ be the subnear-ring of $M_N(N^k)$ generated by $N \cup \{u\}$.

Let $k = \omega$ and define $x : N^\omega \to N^\omega$ by $x(\alpha_1, \alpha_2, \alpha_3, ...) = (0, \alpha_1, \alpha_2, \alpha_3, ...)$ - the so called right shift function. Then $x \in M_N(N^\omega) - N$ is a commuting indeterminate and the near-ring $[N, N^\omega, x]$ is called the *polynomial near-ring over* N. As is to be expected, this near-ring will be denoted by $N[x]$.

2 Overview of existing results

As mentioned above, Scott Bagley was the first to study polynomial near-rings as defined above:

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

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

The major thrust here was to establish the tools to work with polynomial near-rings and to investigate the structure and transfer of ideals between N and $N[x]$. For example, if I is a left ideal of N, $I^* := \{f \in N[x] \mid f(N^\omega) \subseteq I\}$ is an ideal of $N[x]$ and when I is an ideal of N, then $N[x]/I^* \cong (N/I)[x]$.

The next contributions came from Mark Farag:

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

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

Again much emphasis were on investigations of the ideal structure of $N[x]$. In addition, he showed that polynomial near-rings do not satisfy the dcc on ideals and that it has no minimal ideals. It is significant to mention that there is no Euclidean algorithm to assist in these proofs. He also gave some generalizations of polynomial near-rings, including twisted polynomial near-rings.

Both Bagley and Farag, as well as Lee

⊙ Enoch K.S. LEE. Theory of polynomial near-rings. *Comm. Algebra* **32** (2004), 1619-1635);

develop many properties of polynomial near-rings modulo an ideal called sym_0; this is the ideal of $N[x]$ generated by $\{a(b_0 + b_1x + ... + b_nx^n) - ab_{\sigma(n)}x^{\sigma(n)} - ... - ab_{\sigma(0)}x^{\sigma(0)} \mid a, b_i \in N$ and σ is a permutation on $\{1, 2, 3, ..., n\}$ for $n = 0, 1, 2, ...\}$. Any $f \in N[x]$ then satisfies $f \equiv f_0 + f_1x + ... + f_nx^n \bmod sym_0$ for some $n \geq 0, f_i \in N$. Moreover, modulo this ideal of symbolically zero polynomials, the product and sum of near-ring polynomials are the same as for the polynomials over a ring. This, to me at least, removes much of the fun and significance of working with near-ring polynomials. Ons should rather establish tools to work with proper near-ring polynomials.

The degree of a near-ring polynomial seems to be problematic. Bagley defines it as follows:

For $0 \neq f \in N[x]$, $\deg(f) := \max\{|f(\alpha)| - |\alpha| \mid \alpha \in N^\omega$ has finite support$\}$ where for any $\beta \in N^\omega$ with finite support, $|\beta| := \min\{m \in \mathbb{N} \mid \beta_i = 0$ for all $i > m\}$. When $f = 0$, it has degree 0 by definition. It is shown that every polynomial has some degree and that a number of the familiar properties of the degree of ring polynomials also hold for the near-ring polynomials. In general, it is not always obvious what the degree of a polynomial is, and often it is not just straightforward to calculate it. For example, provided a does not distribute over $b+c$, we have $f := a(b+cx) - acx - ab$ is a polynomial of degree 0

There is one more paper dealing with polynomial near-rings:

⊙ Enoch K.S. LEE and Nico J. GROENEWALD. Polynomial near-rings in k indeterminates. *Bull. Austral. Math. Soc.* **70** (2004), 441-449;

show that one may iterate the near-ring polynomial construction and that the order in which it is done is not important: $(N[x])[y] \cong (N[y])[x]$.

At the last near-ring conference in Linz (2007), I described certain homomorphic images of polynomial near-rings. For example, if $N[x]$ is the polynomial near-ring over a near-field N and the ideal generated by the polynomial x^2+1 in $N[x]$ is denoted by $\langle x^2+1 \rangle$, then $N/\langle x^2+1 \rangle \cong [N, N^2, y]$ where $y \in M_N(N^2) - N$ is a commuting indeterminate with $y^2 + 1 = 0$. These results appeared in :

⊙ S. VELDSMAN. Homomorphic images of polynomial near-rings, *Contr. Algebra and Geometry* **50** (2009), 119-142.

We will return to these results again at a later stage. First we look at the relationship between polynomial near-rings and matrix near-rings.

3 Polynomial near-rings and matrix near-rings

From our early training in linear algebra, we know that there are many fruitful connections between matrices and polynomials and the one can hardly be studied without the other. I next want to show that some of these relationships extend to the near-ring case. In fact, since in the near-ring case both matrices and polynomials are functions, these relationships are actually more natural.

For a ring R, let $\mathbb{M}_\omega(R)$ denote the ring of $\omega \times \omega$ row finite matrices over the ring R. Then the polynomial ring $R[x]$ can be embedded in $\mathbb{M}_\omega(R)$ by $\psi : R[x] \hookrightarrow \mathbb{M}_\omega(R)$ defined by

$$\psi(f_0 + f_1x + f_2x^2 + ... + f_nx^n) = \begin{bmatrix} f_0 & f_1 & f_2 & ... & f_n & 0 & 0 & ... \\ 0 & f_0 & f_1 & f_2 & ... & f_n & 0 & ... \\ 0 & 0 & f_0 & f_1 & f_2 & ... & f_n & ... \\ : & : & : & : & : & : & : & : .. \end{bmatrix}.$$

Then $R[x] \cong \psi(R[x])$ and the latter is a subring of $\mathbb{M}_\omega(R)$. This is a very special subring; for example, if R is a commutative ring then $\psi(R[x])$ is a commutative subring of the very non-commutative ring $\mathbb{M}_\omega(R)$. Within $\mathbb{M}_\omega(R)$ it is possible to identify this subring. Let F be the matrix

$$F = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & ... \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & ... \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & ... \\ : & : & : & : & : & : & : & : .. \end{bmatrix}.$$

Then it can be shown that $\psi(R[x]) = C(F)$ where $C(F)$ is the centralizer of F in $\mathbb{M}_\omega(R)$, i.e. $C(F) = \{A \in \mathbb{M}_\omega(R) \mid FA = AF\}$. In fact, it can be shown that $R[x] \cong \psi(R[x]) = C(F) = R[F]$ where the latter denotes the subring $R[F] = \{f(F) \mid f(x) \in R[x]\}$.

How much of this is true for near-rings? Well, we first need a near-ring analogue of the row finite matrices. This has already been provided by Johan Meyer in his PhD thesis:

⊙ J.H. MEYER. *Matrix near-rings*, Ph.D. thesis, University of Stellenbosch, 1986;

For the near-ring N, let $\mathbb{M}_\omega(N)$ be the subnear-ring of $M_N(N^\omega)$ generated by $\{f_j^a \mid a = (a_1, a_2, a_3, ...) \in N^\omega, j = (j_1, j_2, j_3, ...) \in \mathbb{N}^\omega\}$ where $f_j^a : N^\omega \to N^\omega$ is the function defined by $f_j^a(\alpha_1, \alpha_2, \alpha_3, ...) = (a_1\alpha_{j_1}, a_2\alpha_{j_2}, a_3\alpha_{j_3}, ...)$ for all $(\alpha_1, \alpha_2, \alpha_3, ...) \in N^\omega$. If you want, you may think of f_j^a as the $\omega \times \omega$ matrix with 0 everywhere except in the i-th row and j_i -th column there is an a_i. Clearly $N \hookrightarrow \mathbb{M}_\omega(N)$ via $a \mapsto f_j^a$ where $a = (a, a, a, ...)$ and $j = (1, 2, 3, ...)$.

Another preliminary, is: Recall that for the polynomial near-ring $N[x]$ we have used the right shift function $x(\alpha_1, \alpha_2, \alpha_3, ...) = (0, \alpha_1, \alpha_2, \alpha_3, ...)$ as the commuting indeterminate. One could equally well have used the left shift function $\overline{x}(\alpha_1, \alpha_2, \alpha_3, ...) = (\alpha_2, \alpha_3, ...)$ for it can be shown that

$N[x] \cong N[\overline{x}]$. If we insist on writing function arguments on the right then, especially when we work with matrices as functions, it is more natural to use the left shift function. And this is what we will do from now one: $N[x]$ will be the polynomial near-ring with x the left shift function.

Now both $N[x]$ and $\mathbb{M}_\omega(N)$ are subnear-rings of $M_N(N^\omega)$ which contains N, so the inclusion $N[x]$ will follow if we can show that $N \cup \{x\} \subseteq \mathbb{M}_\omega(N)$, i.e. we need $x \in \mathbb{M}_\omega(N)$. But this is clear since $x = f^1_j$ where $1 = (1, 1, 1, ...)$ and $j = (2, 3, 4, ...)$. Moreover, as is the case for rings, it can be shown that $N[x] = C(x)$ where $C(x) = \{g \in \mathbb{M}_\omega(R) \mid gx = xg\}$.

As motivation for the next corresponcence, we again return to the civilized world of rings. Let R be a comutative ring with identity and let $h(x) = x^k - h_{k-1}x^{k-1} - ... - h_1x - h_0$ be a monic polynomial of degree k over R. Then

$$\begin{aligned} \tfrac{R[x]}{\langle h(x)\rangle} &\cong \{a_1 + a_2y + a_3y^2 + ... + a_ky^{k-1} \mid a_i \in R, y^k = \sum_{i=0}^{k-1} h_iy^i\} \\ &\cong \mathbb{M}_k(R, h) \end{aligned}$$

where a matrix in $\mathbb{M}_k(R, h)$ is of the form $[a_{ij}]_{k\times k}$ with $a_{1j} = a_j$ for $j = 1, 2, 3, ..., k$ and $a_{ij} = a_{i-1,j-1} + h_{j-1}a_{i-1,k}$ for $i = 2, 3, ..., k$ and $j = 1, 2, 3, ..., k\}$. Here we take $a_{i0} = 0$.

I suspect this latter representation of the polynomial quotient ring as a matrix ring is well-know, but apart from one or two concrete examples in abstract algebra text books (usually the one that leads to the circulant matrices), I have not seen it or even a reference to a general result anywhere.

For illustrative purposes, a simple example will do: Let

$h(x) = x^3 - 2x^2 + x - 3 \in \mathbb{Z}[x]$.

Then $h_2 = 2, h_1 = -1$ and $h_0 = 3$.

Moreover,

$\frac{\mathbb{Z}[x]}{\langle h(x)\rangle} \cong \{a + by + cy^2 \mid a, b, c \in R, y^3 = 2y^2 - y + 3\} \cong \mathbb{M}_3(\mathbb{Z}, h)$ and a typical element of this matrix ring is

$$\begin{bmatrix} a & b & c \\ 3c & a - c & b + 2c \\ 3(b + 2c) & -b + c & a + b + 4c \end{bmatrix}.$$

Working with the matrices rather than the polynomials have the advantage that products of elements can be directly calculated; there are no reductions necessary as is the case when dealing with the polynomials.

Again $\mathbb{M}_k(R,h)$ is a very special subring of the ring of all $k \times k$ matrices over A - it is, for example, a commutative ring of matrices. Again the question arises which subrings S of $\mathbb{M}_k(R)$ will be such a quotient of a polynomial near-ring. The answer is given by:

A subring S of $\mathbb{M}_k(R)$ is of the form $\mathbb{M}_k(R,h)$ for some polynomial $h(x) = x^k - h_{k-1}x^{k-1} - ... - h_1x - h_0 \in R[x]$ if and only if $S = C(E)$ where $C(E)$ denotes the centralizer of the matrix E in

$$\mathbb{M}_k(R) \text{ and } E = \begin{bmatrix} 0 & 1 & 0 & 0 & . & . & . & 0 \\ 0 & 0 & 1 & 0 & . & . & . & 0 \\ 0 & 0 & 0 & 1 & 0 & . & . & 0 \\ : & : & : & : & : & : & : & : .. \\ 0 & 0 & 0 & 0 & . & . & . & 1 \\ h_0 & h_1 & . & . & . & . & . & h_{k-1} \end{bmatrix} \text{ for some } h_i \in$$

R. The matrix E is, of course, just the companion matrix of the polynomial $h(x)$.

Again we ask how much of this is true for near-rings? To start with, a nice canonical description of the quotient of a polynomial near-ring determined by the ideal generated by a polynomial is not always available. At the previous near-ring conference, I showed that in some cases it is possible to give a nice description of such quotients.

In order to do this, and also for later use, we need to fix a canonical representation of near-ring polynomials. Contrary to the ring case, we do not have a normal form for near-ring polynomials. So we will just have to do the best we can.

It can be shown that $N[x] = \bigcup_{n=1}^{\infty} \mathcal{A}_n$ where

$$\mathcal{A}_1 = \{a_1x^{n_1} + a_2x^{n_2} + ... + a_tx^{n_t} \mid a_i \in N, n_i \geq 0, t \geq 1\}.$$

If $\mathcal{A}_n$ has been defined for $n \geq 1$, then

$$\mathcal{A}_{n+1} = \{ \sum_{i=1}^{finite} a_iw_i \mid a_i \in N, w_i \in \mathcal{A}_n\}.$$

We will write polynomials in the form given by the elements of the classes $\mathcal{A}_n$ above. Moreover, we always write x as far to the right as possible (but not as a common factor on the right) and the constants as far to the left as possible. For example

$$ax(b + x^2c)dx = a(bd + cdx^2)x^2 = a(bdx^2 + cdx^4)$$

but the last is the canonical representation.

The *level of a polynomial* is the smallest $n \geq 1$ for which it is in $\mathcal{A}_n$ and its *height* is the biggest exponent of x. But note that for a given polynomial, these notions are not uniquly determined! Both these depend on the particular representation chosen for the poynomial. It could well happen that $f(x) = x^2 - bx = d(b - x)$ - both are canonical representations of $f(x)$ but with different levels as well as different heights. So, the level and the height of a polynomial is always associated with the particular representation chosen for it.

Let $h(x) = x^k - p(x)$ where $k \geq 2$ and $p(x)$ is a polynomial with a representation of height $k-1$. Subject to some conditions on the polynomial $p(x)$, which is not important here, it has been shown that $\frac{N[x]}{\langle h(x)\rangle} \cong [N, N^k, y]$ where $y : N^k \to N^k$ is a commuting indeterminate with $y^k = p(y)$ in $[N, N^k, y]$. Our interest is now on the near-ring $[N, N^k, y]$. Recall that it is the subnear-ring of $M_N(N^k)$ generated by $N \cup \{y\}$. But we know that $\mathbb{M}_k(N)$, the $k \times k$ matrix near-ring over N, is also a subnear-ring of $M_N(N^k)$, namely the subnear-ring generated by $\{f_{ij}^a \mid a \in N, 1 \leq i, j \leq n\}$ where $f_{ij}^a : N^k \to N^k$ is the function defined by $f_{ij}^a(\alpha_1, \alpha_2, ..., \alpha_k) = (0, 0, ..., a\alpha_j, 0, ..., 0)$ with $a\alpha_j$ in the i-position. Again, like for the ring case, it can be shown that

$\frac{N[x]}{\langle h(x)\rangle} \cong [N, N^k, y] \subseteq \mathbb{M}_k(N)$; in fact, $\frac{N[x]}{\langle h(x)\rangle} \cong [N, N^k, y] = C(y) = \{f \in \mathbb{M}_k(N) \mid fy = yf\}$, the centralizer subnear-ring of y in $\mathbb{M}_k(N)$.

This then brings us to our last topic:

4 Substitution and polynomial functions

As we well know, whenever one leaves a comforting commutative environment, substitutions in polynomials are problematic. And near-ring polynomials are no exception.

For substitution in near-ring polynomials, we should always have the polynomial in the canonical form before we do any substitution. For rings, this would mean right substitution. Just to remind you of the problems we can expect with substitution, let $f(x) = (x - a)(x - b) \in N[x]$, take N to be a near-field. If one is required to find the $t \in N$ for which $f(t) = 0$ and due care is not taken, one's first reaction will be to argue that $f(t) = 0 \Leftrightarrow (t - a)(t - b) = 0$ from which $t = a$ or $t = b$ follows since N is a near-field. This is of course not the case - for substitution the polynomial

$f(x)$ must be in canonical form. This means $f(x) = (x-a)(x-b) = x(x-b) - a(x-b) = x^2 - bx - a(x-b)$ and the last form is the canonical form. Then $f(a) = a^2 - ba - a(a-b)$ which need not be 0; even if N is a ring.

A more serious challenge will be what to make of the following: Let $f(x) = d(x-a) - d(b-a) + d(b-x) \in N[x]$. Here we take arbitrary distinct elements a, b, d from N; just ensure that d does not distributive over $b-a$. Then $f(x)$ is a near-ring polynomial of degree 1 in the sense of Bagley, or of height 1 in my terminology, but it has two arbitrary distinct zeros a and b. And we may even take N to be a finite near-field!

Or, let $f(x) = a(b+x) - ax - ab \in N[x]$. Then $f(x)$ has height 1, degree 0 and two zeros $x = 0$ and $x = -b$. Even a simple linear equation like $a(b+x) = c + dx$ may not have a solution when N is a finite near-field; i.e. a polynomial like $g(x) = a(b+x) + c + dx$ may not have a solution over a near-field.

In other words, in stark contrast to the ring case, the only rule that tells us how many zeros to expect for a near-ring polynomial over a near-field, says that it may have no zeros or it may have some zeros.

Let me remind you of some of the well-known results when dealing with commutative rings:

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

(2) If R is an integral domain, then any polynomial of degree n over R can have at most n roots in R.

(3) If we discard commutativity, and let D be a division ring, it has been shown 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.

So, as we return to near-rings, the above should serve as a warning that we are about to enter highly insecure territory. With our agreement on a cannonical form for a near-ring polynomial, substitution is well-defined operation.

Or is it really?

As mentioned, a near-ring polynomial $f(x)$ may have many different representations, for example $f(x) = x^2 - bx = d(b-x)$. For a substitution $f(a)$, which representation should we choose? Fortunately it can be shown

that it does not matter - they will all give the same element in N which means that $f(a)$ is indeed well-defined.

With any near-ring polynomial $f(x)$ we thus associate a uniquly determined function $\overline{f} : N \to N$ defined by $\overline{f}(a) = f(a)$ where the latter means we replace all occurences of x with a. This substitution is well-behaved with respect to addition, in the sense that if $h(x) = f(x) + g(x)$, then $h(a) = f(a) + g(a)$. But this is not the case with products and composition: If $h(x) = f(x)g(x)$, then we need not have $h(a) = f(a)g(a)$ and if $h(x) = f(g(x))$, also $h(a)$ need not coincide with $f(g(a))$. There are some tools that do facilitate the process of substitutions in products and compositions. I will mention some of them for you:

(1) For $a \in N$ and $f(x) \in N[x], f(a) = 0$ if and only if $f(x) \in \langle x - a]$ (and this is as good as it gets).

(2) Let $f(x) \in N[x]$ and let $\langle f(x)]$ be the left ideal of $N[x]$ generated by $f(x)$. If $f(a) = 0$ for some $a \in N$ and $g(x) \in \langle f(x)]$, then $g(a) = 0$.

A number of related tools are:

(3) We do have some division algorithm: If $h(x) = x^k - p(x) \in N[x]$ where $p(x)$ has height $\leq k-1$, then for any $f(x) \in N[x], f(x) = h_1(x) + r(x)$ where $h_1(x) \in \langle h(x)]$ and $r(x)$ has height $\leq k-1$. But, as we have seen above, the fact that $r(x)$ has height $\leq k-1$ says nothing about the number of zeros it may have; even if N is a finite near-field.

(4) Let L be a left ideal of N and let $f(x) \in N[x]$. If $c \in L$, then $f(c) - f(0) \in L$. If L is an ideal of N, then $b - c \in L$ implies $f(b) - f(c) \in L$.

(5) Let $a \in N$. Then $\langle a] = \{p(a) \mid p(x) \in N[x], p(0) = 0\}$.

(6) A non-zero element b of N is called a *generalized unit* in N if there is a polynomial $p(x) \in N[x]$ with $p(0) = 0$ and $p(b) = 1$.

In a ring R with an identity, $0 \neq b \in R$ is a generalized unit if and only if b has a left inverse. For near-rings one can show:

(7) Let N be a 0-symmetric near-ring with identity. Then every non-zero element of N is a generalized unit if and only if N has no non-trivial left ideals.

We use $\mathcal{P}(N)$ and $\mathcal{M}(N)$ to denote the set of all near-ring polynomial functions and the set of all self-maps of N respectively. A rather pleasing result is the following:

(8) Let N be a 0-symmetric near-ring with identity. If $\mathcal{P}(N) = \mathcal{M}(N)$, then N is a finite near-field.

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 (not necessarily commutative and not necessarily with identity), we know: For the ring R, $\mathcal{P}(R) = \mathcal{M}(R)$ if and only if R is either the trivial ring of order 1 or 2, or for some n and some finite field F, $R = \mathbb{M}_n(F)$. I should mention, 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 (J.V. Brawley and L. Carlitz, A characterization of the $n \times n$ matrices over a finite field, *American Mathematical Monthly* **80** (1973), 670 - 672).

What the situation is concerning the converse of (8) above is not clear. The difficulty is that in the near-ring case, even for finite near-fields, one do not have the interpolation results of Lagrange or Newton available. In particular, the problem is constructing near-ring polynomials with prescibed zeros. Well, this is not entirely true. I will show you that one can construct near-ring polynomials with any desired zeros. The problem is that in general one cannot be sure that these are the only zeros.

Let N be a near-field and let $a_0, a_1, a_2, ..., a_k$ be distinct elements from the near-field N. Inductively we will define polynomials with zero a_0; with zeros a_0, a_1; with zeros a_0, a_1, a_2; etc.

Clearly $f_0(x) = x - a_0$ is a near-ring polynomial with unique zero a_0.

We next define a sequence of elements in N as follows:

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

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

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

Then $f_1(x) = (x - v(a_1, a_0))f_0(x)$ is a near-ring polynomial with both a_0 and a_1 as zeros. To verify this, we must first write $f_1(x)$ in canonical form before we do the substitution. Thus:

$$
\begin{aligned}
f_1(x) &= (x - v(a_1, a_0))f_0(x) \\
&= (x - v(a_1, a_0))(x - a_0) \\
&= x(x - a_0) - v(a_1, a_0)(x - a_0) \\
&= x^2 - a_0x - v(a_1, a_0)(x - a_0).
\end{aligned}
$$

Clearly $f_1(a_0) = 0$ and

$f_1(a_1) = a_1^2 - a_0a_1 - v(a_1, a_0)(a_1 - a_0) = (a_1 - a_0)a_1 - (a_1 - a_0)a_1(a_1 - a_0)^{-1}(a_1 - a_0) = 0.$

By abuse of notation, for the obvious advantage of direct substitution, we note that $f_1(x)$ can be written as:

$$
\begin{aligned}
f_1(x) &= x^2 - a_0x - v(a_1, a_0)(x - a_0) \\
&= (x - a_0)x - v(a_1, a_0)(x - a_0) \\
&= ((x - a_0)x(x - a_0)^{-1} - v(a_1, a_0))(x - a_0) \\
&= (v(x, a_0) - v(a_1, a_0))(x - a_0)
\end{aligned}
$$

where $v(x, a) = (x - a)x(x - a)^{-1}$. This should not be thought of as a "polynomial" in x; it is just a covenient notation and when x is replaced by $b \in N$, say, then that is exactly what we do.

The benefit of this representation of $f_1(x)$ is that direct substitution is valid without first writing the polynomial in canonical form, i.e., for any $b \in N$, we have $f_1(b) = (v(b, a_0) - v(a_1, a_0))(b - a_0)$. Then

$f_1(b) = 0 \Leftrightarrow (v(b, a_0) - v(a_1, a_0))(b - a_0) = 0 \Leftrightarrow b = a_0$ or $v(b, a_0) = v(a_1, a_0)$. This last equality holds if $b = a_1$, but not necessarily only if for there may well be other $b's$ with $v(b, a_0) = v(a_1, a_0)$. We note that such $b's$ must be conjugates of a_1 (but not just any conjugate).

It is worth empasizing this point with an example: Let N be the near-field on $GF(3^2) = \{a + bt \mid a, b = 0, 1, 2\}$. Then $f(x) = (v(x, t) - v(2 + t, t))(x - t)$ has zeros $2 + t, t$ and $1 + 2t$ since $v(1 + 2t, t) = v(2 + t, t)$. On the other hand, $g(x) = (v(x, 2 + t))(x - (2 + t))$ has zeros $2 + t$, t and $2t$ since $v(2t, 2+t) = v(t, 2+t)$. Moreover, $h(x) = t(x-(2+t))-t(t-(2+t))+t(t-x)$ has zeros $2 + t, t$ and $1 + t$.

Let us return to our construction and let $f_2(x) = (x - v(a_2, a_1, a_0))f_1(x)$.

which can be written as

$f_2(x) = (v(x, a_1, a_0) - v(a_2, a_1, a_0))(v(x, a_0) - v(a_1, a_0))(x - a_0)$.

As in the previous case, we have direct substitution since for any $b \in N$,

$f_2(b) = (v(b, a_1, a_0) - v(a_2, a_1, a_0))(v(b, a_0) - v(a_1, a_0))(b - a_0)$

Then $f_2(x)$ has zeros a_0, a_1 and a_2. Continuing in this way, we can get a near-ring polynomial with zeros $a_0, a_1, a_2, ..., a_k$ but we cannot be assured that these are the only zeros. For example, for $f(x) = (v(x, a_0) - v(a_1, a_0))(x - a_0)$ we know a_0 and a_1 are zeros, but there well could be an $b \in N$, b not equal to either a_0 nor a_1 with $v(b, a_0) = v(a_1, a_0)$. When we have commutativity available, then $v(a, b) = (a - b)a(a - b)^{-1} = a$ and we are on a well-trodden path. But we do not have this in general, so we conclude with:

Let N be a finite near-field with $v(a, c) \neq v(b, c)$ for all distinct elements a, b, c in N. Then $\mathcal{P}(N) = \mathcal{M}(N)$.

I suspect that this assumption will actually force N to be a finite field, i.e. we will get the result: 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 field. But we have to remember the words of Stephen Hawkins (1942 -), the well-known British theoretical physicist:

"One is always a long way from solving a problem until one actually has the answer."

5 References

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

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

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

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

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

[6] H. LAUSCH and W. NÖBAUER. *Algebra of Polynomials*. North Holland, Amsterdam, 1973.
[7] Enoch K.S. LEE. Theory of polynomial near-rings. *Comm. Algebra* **32** (2004), 1619-1635.
[8] Enoch K.S. LEE and Nico J. GROENEWALD. Polynomial near-rings in k indeterminates. *Bull. Austral. Math. Soc.* **70** (2004), 441-449.
[9] L.R. le RICHE, J.D.P. MELDRUM and A.P.J. van der WALT. On group near-rings. *Arch. Math.* **52** (1989), 132-139.
[10] J.D.P. MELDRUM and A.P.J. van der WALT. Matrix near-rings. *Arch. Math.* **47** (1986), 312-319.
[11] J.H. MEYER. *Matrix near-rings*, Ph.D. thesis, University of Stellenbosch, 1986.
[12] W. Keith NICHOLSON. *Abstract Algebra*. PWS Publishing Company, USA, 1993.
[13] G. PILZ. *Near-rings*. North Holland, Amsterdam, 1983.
[14] S. VELDSMAN. Homomorphic images of polynomial near-rings, *Contr. Algebra and Geometry*.**50** (2009), 119-142.