Multivariate Polynomial maps

Noncommutative and non-associative structures,

braces and applications.

Malte, March 2018

Part of this talk is extracted from a few joint works with T.Y. Lam, A. Ozturk, J. Delenclos.

.

I) Noncommutative Polynomial maps in one variable .

a) Skew polynomial rings.

b) Pseudo-linear maps and polynomial maps.

c) Counting the number of roots.

d) Wedderburn polynomials and Symmetric functions.

II) **Iterated Ore extensons.**

a) Evaluation(s).

b) Good points.

III) **Free Ore extensions.**

a) Definitions.

b) Generalized PLT.

c) Product formula.

d) VDM matrices, P-independence, P-bases.

e) Closed subsets.

.

1 Noncommutative Polynomial map in one variable.

a) **Skew polynomial rings.**

A a ring, $\sigma \in End(K)$, δ a σ-derivation:

$$\delta \in End(K,+) \qquad \delta(ab) = \sigma(a)\delta(b) + \delta(a)b, \ \forall a, b \in K.$$

Define a ring $R := A[t;\sigma,\delta]$; Polynomials $f(t) = \sum_{i=0}^{n} a_i t^i \in R$.

Degree and addition are defined as usual, the product is based on:

$$\forall a \in A, \quad ta = \sigma(a)t + \delta(a).$$

Exemples 1.1. 1) If $\sigma = id.$ and $\delta = 0$ we get back the usual polynomial ring $A[x]$.

2) $R = \mathbb{C}[t;\sigma]$ where σ is the complex conjugation. If $x \in \mathbb{C}$ is such that $\sigma(x)x = 1$ then

$$t^2 - 1 = (t + \sigma(x))(t - x)$$

. On the other hand $t^2 + 1$ is central and irreducible in R.

b) **Pseudo-linear maps and polynomial maps**

Definitions 1.2. A a ring, σ an endomorphism of A and δ a σ-derivation of A. Let V be a left A-module.

a) An additive map $T : V \longrightarrow V$ such that, for $\alpha \in A$ and $v \in V$,

$$T(\alpha v) = \sigma(\alpha)T(v) + \delta(\alpha)v.$$

is called a (σ, δ) pseudo-linear transformation (or a (σ, δ)-PLT, for short).

b) For $f(t) \in R = A[t; \sigma, \delta]$ and $a \in A$, we define $f(a)$ to be the only element in A such that $f(t) - f(a) \in R(t - a)$.

If $R = A[t; \sigma, \delta]$ and ${}_RM$ is a left R module. we have

$$t.(am) = (ta).m = \sigma(a)t.m + \delta(a).m$$

For $a \in A$ and $m \in M$. Hence $t.$ is a (σ, δ)-PLT defined on M. This leads to

$${}_RM \longleftrightarrow {}_AM + PLT$$

.

<u>Examples</u>: For $a \in A$, $T_a : A \to A$ defined by $T_a(x) = \sigma(x)a + \delta(x)$ is a PLT. In particular, $T_0 = \delta, T_1 = \sigma + \delta$ are PLT.
What is the module defined by T_a ? This is $R/R(t - a)$. From this it easy to check that

$$\forall f(t) \in A[t; \sigma, \delta] \; \forall a \in A, \;\; f(a) = f(T_a)(1)$$

In case $A = K$ is a division ring, for $f(t), g(t) \in A[t; \sigma, \delta]$ and $a \in K$ if $g(a) \neq 0$ we have

$$fg(a) = f(a^{g(a)})g(a).$$

where for $0 \neq c \in K$ $a^c = \sigma(c)ac^{-1} + \delta(c)c^{-1}$.

If A is not a division ring ?

In general when $T \in End(M,+)$ The map $\varphi : R \longrightarrow End(M,+)$ given by

$$\varphi(\sum_{i=0}^{n} a_i t^i) = \sum_{i=0}^{n} a_i T^i.$$

is a ring homomorphism.

In particular, in the case of the evaluation at $a \in A$ this leads to

$$fg(a) = (f(T_a) \circ g(T_a))(1) = f(T_a)(g(a))$$

c) **Counting the roots**

Let $A = K$ be a division ring, we define

$$E(f,a) := \ker f(T_a) = \{0 \neq b \in K \mid f(a^b) = 0\} \cup \{0\}$$

<u>Facts and notations</u>

$a \in K$, $R = K[t;\sigma,\delta]$.

1) $\Delta(a) := \{a^c = \sigma(c)ac^{-1} + \delta(c)c^{-1} \mid 0 \neq c \in K\}$.

2) T_a defines a left R-module structure on K via $f(t).x = f(T_a)(x)$.

3) In fact, ${}_RK \cong R/R(t-a)$ as left R-module.

4) ${}_RK_S$ where $S = End_R({}_RK) \cong End_R(R/R(t-a))$, a division ring. isomorphic to the division ring $C(a) := \{0 \neq x \in K \mid a^x = a\} \cup \{0\}$.

5) For any $a \in K$ and $f(t) \in R = K[t;S,D]$, $\ker f(T_a)$ is a right vector space on the division ring $C(a)$.

Theorem 1.3. *Let $f(t) \in R = K[t;S,D]$ be of degree n. We have*

(a) The roots of $f(t)$ belong to at most n conjugacy classes, say

$\Delta(a_1), \ldots, \Delta(a_r)$; $r \leq n$ (Gordon Motzkin in "classical" case).

(b) $\sum_{i=1}^{r} dim_{C_i} \ker f(T_{a_i}) \leq n$.

For any $f(t) \in R = K[t; S, D]$ we thus "compute" the number of roots by adding the dimensions of the vector spaces consisting of "exponents" of roots in the different conjugacy classes...

Theorem 1.4. *let p be a prime number, $\mathbb{F}_q$ a finite field with $q = p^n$ elements, θ the Frobenius automorphism ($\theta(x) = x^p$). Then:*

a) There are p distinct θ-classes of conjugation in $\mathbb{F}_q$.

b) $0 \neq a \in \mathbb{F}_q$ we have $C^\theta(a) = \mathbb{F}_p$ and $C^\theta(0) = \mathbb{F}_q$.

(c) $R = \mathbb{F}_q[t;\theta]$, $t - a$ for $a \in \mathbb{F}_q$ is

$$G(t) := [t - a \,|\, a \in \mathbb{F}_q]_l = t^{(p-1)n+1} - t$$

. We have $RG(t) = G(t)R$.

The polynomial $G(t)$ in the above theorem is a Wedderburn polynomial...

d) **Wedderburn polynomials and symmetric functions**

Definitions 1.5. 1. (a) A monic polynomial $p(t) \in R = K[t; S, D]$ is a Wedderburn polynomial if we have equality in the "counting roots formula".

(b) For $a_1, \ldots, a_n \in K$ the matrix

$$V_n^{S,D}(a_1, \ldots, a_n) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ T_{a_1}(1) & T_{a_2}(1) & \ldots & T_{a_n}(1) \\ \ldots & \ldots & \ldots & \ldots \\ T_{a_1}^{n-1}(1) & T_{a_1}^{n-1}(1) & \ldots & T_{a_1}^{n-1}(1) \end{pmatrix}$$

Theorem 1.6. *Let $f(t) \in R = K[t; S, D]$ be a monic polynomial of degree n. The following are equivalent:*

(a) $f(t)$ is a Wedderburn polynomial.

(b) There exist n elements $a_1, \ldots, a_n \in K$ such that
$f(t) = [t - a_1, \ldots, t - a_n]_l$ where $[g, h]_l$ stands for LLCM of g, h.

(c) There exist n elements $a_1, \ldots, a_n \in K$ such that

$$S(V)C_f V^{-1} + D(V)V^{-1} = Diag(a_1, \ldots, a_n)$$

Where C_f is the companion matrix of f and $V = V(a_1, \ldots, a_n)$

(d) Every quadratic factor of f is a Wedderburn polynomial.

Example

Construction of Wedderburn polynomials: Let $a, b \in K$ be two different elements in K.

$$f(t) := [t - a, t - b]_l = (t - b^{b-a})(t - a) = (t - a^{a-b})(t - b).$$

Assume now that $c \in K$ is such that $f(c) \neq 0$ then:

$$g(t) := [t - a, t - b, t - c]_l = (t - c^{f(c)})f(t).$$

Wedderburn polynomials can be used to develop noncommuative symmetric functions.

2 Iterated Ore extensions

a) **Evaluation**

Consider $f(t_1,t_2) \in R = A[t_1;\sigma_1,\delta_1][t_2;\sigma_2;\delta_2]$ and $a = (a_1,a_2) \in A^2$. Considering $f(t_1,t_2)$ as an element of $R_1[t_2,\sigma_2,\delta_2]$, where $R_1 = A[t_1;\sigma_1;\delta_1]$, we can evaluate $f(t_1,b) \in R_1 = A[t_1;\sigma_1,\delta_1$. and this polynomial can then be evaluated in a. In other words we must evaluate at a the remainder of the division of $f(t_1,t_2)$ by $t_2 - b$ in $R_1[t_2;\sigma_2,\delta_2]$. This leads to the following definition:

Definition 2.1. Let $R_1 := A[t_1;\sigma_1,\delta_1]$ be an Ore extension and σ_2,δ_2 an endomorphism and a σ_2-derivation of R_1 respectively. We assume that $\sigma_2(A) \subseteq A$ and $\delta_2(A) \subseteq A$. For $(a,b) \in A^2$ and $f(t_1,t_2) \in A[t_1;\sigma_1,\delta_1][t_2;\sigma_2,\delta - 2]$, we define $f(a,b)$ to be the unique element in A representing $f(t_1,t_2)$ in $R/(R_1(t_1-a)+R(t_2-b))$.

Exemples 2.2. 1. Let us compute $(t_1t_2)(a,b)$. We have $t_1t_2 = t_1(t_2-b)+t_1b = t_1(t_2-b)+\sigma_1(b)t_1+\delta_1(b)$. This leads to $(t_1t_2)(a,b) = \sigma_1(b)a+\delta_1(b)$.

2. $(t_2t_1)(a,b) = (\sigma_2(t_1)t_2+\delta_2(t_1))(a,b) = (\sigma_2(t_1)(b)+\delta_2(t_1))(a)$.

Notations 1. 1. Let $A,\sigma_1,\sigma_2,\delta_1,\delta_2$ be as above. We put, for $x \in A$, $T_a^1(x) = \sigma_1(x)a+\delta_1(x)$ and $T_a^2(x) = \sigma_2(x)a+\delta_2(a)$.

2. For $(a,b) \in A^2$ we put $I_1 = R_1(t_1-a)+R(t_2-b)$ and $I := R(t_1-a)+R(t_2-b)$. Of course we have $I_1 \subseteq I \subseteq R$.

It sems reasonable to require that $(t_2(t_1-a))(a,b) = 0$ for any $b \in A$. This leads to the requirement that $t_2(t_1-a) \in I_1$.

b) **Good points**

Theorem 2.3. *With the above notations, the following are equivalent:*

1. $I_1 = I$;
2. $R(t_1 - a) \subseteq I_1$;
3. $I \neq R$;
4. $t_2(t_1 - a) \in I_1$;
5. $\sigma_2(t_1 - a)b + \delta_2(t_1 - a) \in R_1(t_1 - a)$;
6. $(t_2 t_1)(a, b) = \sigma_2(a)b + \delta_2(a)$;
7. *the map* $\psi : R = K[t_1; \sigma_1, \delta_1][t_2; \sigma_2, \delta_2] \longrightarrow End(K, +)$ *defined by* $\psi(f(t_1, t_2)) = f(T_a^1, T_b^2)$ *is a ring homomorphism;*
8. $\forall f, g \in R,\ (fg)(a, b) = (f(T_a^1, T_b^2) \circ g(T_a^1, T_b^2))(1)$.

Definition 2.4. A point $(a, b) \in A^2$ will be called a good point if one of the equivalent statements of the above theorem holds.

Notice that the last statement of this theorem is the required analogue of the "product formula".

Exemples 2.5. 1. In the classical case ($\sigma_1 = \sigma_2 = id_K$ and $\delta_1 = \delta_2 = 0$), every point $(a, b) \in K^2$ is good.

2. If K is a division ring $\sigma_1 = id_K,\ \delta_1 = 0$ and $\sigma_2 = id, \delta_2 = d/dt_1$, we have for any $a, b \in K,\ (t_2 - b)(t_1 - a) = (t_1 - a)(t_2 - b) + 1$. This shows that in this case there are **no good points**.

3 Free Ore extensions

a) **Definitions**

We follow U. Martinez-Peñas and F.R. Kschischang: "Evaluation and interpolation over multivariate skew polynomial rings".

A a ring, $\sigma : A \longrightarrow M_n(A)$ a ring morphism and an additive map $\delta : A \longrightarrow \mathbb{A}^n$ such that

$$\delta(ab) = \sigma(a)\delta(b) + \delta(a)b$$

$R = A\langle t_1, \dots, t_n\rangle / I$. where I is the ideal generated by the following relations

$$\forall a \in A, \; t_i a = \sum_{j=1}^{n} \sigma_{ij}(a) t_j + \delta_i(a)$$

writing $\mathbf{t}$ for the column vector $(t_1, \dots, t_n)^t$ we have the following commutation rule

$$\forall a \in A, \quad \mathbf{t}a = \sigma(a)\mathbf{t} + \delta(a)$$

For $f \in R$ and $\mathbf{a} = (a_1, \dots, a_n) \in A^n$, $f(\mathbf{a})$ is the (unique) element of A representing f modulo $\sum_i R(t_i - a_i)$.

Example

$n = 2$ and $a, b \in A^2$,

$$(t_1 t_2)(a, b) = \sigma_{11}(b)a + \sigma_{12}(b)b + \delta_1(b)$$

$$(t_2 t_1)(a, b) = \sigma_{21}(a)a + \sigma_{22}(a)b + \delta_2(a)$$

. b) **Generalized PLT**

$R = A[t_1, \dots, t_n\,; (\sigma), (\delta)], \quad {}_A M$ a left A-module .

A GPLT T is a set of additive maps $T_1, \dots, T_n$: $T_i : M \longrightarrow M$ such that

$$\forall a \in A,\ \forall m \in M,\ \forall 1 \leq i \leq n\ \ T_i(am) = \sum_{j=1}^{n} \sigma_{ij}(a)T_j(m) + \delta_i(a)m$$

As earlier:

$$_RM \longleftrightarrow {}_AM + GPLT$$

<u>Example</u> $\mathbf{a} = (a_1, \dots, a_n) \in A^n$ Define $T_{\mathbf{a}} = (T_1, \dots, T_n)$ by

$$T_i(x) = \sum_{j=1}^{n} \sigma_{ij}(x)a_j + \delta_i(x)$$

We have, as in case $n = 1$,

There is a ring homomorphism $\varphi : R \longrightarrow End(M, +)$ such that $\varphi(t_i) = T_i$.

As in the case when $n = 1$, for $f(\mathbf{t}) \in R$ and $\mathbf{a} = (a_1, \dots, a_n)$

$$f(\mathbf{a}) = f(T_{\mathbf{a}})(1).$$

This leads to a product formula that can be expressed as follows

$$f, g \in R\ \ (fg)(\mathbf{a}) = f(T_{\mathbf{a}})(g(\mathbf{a})).$$

If $A = K$ is supposed to be a division ring, we have for $F, G \in R$ and $\mathbf{a} \in \mathbb{F}^n$ we have that either $G(\mathbf{a}) = \mathbf{0}$ and then also $FG(a) = 0$ or $G(\mathbf{a}) = \mathbf{c} \neq \mathbf{0}$ and then

$$(FG)(\mathbf{a}) = \mathbf{F}(\mathbf{a^c})\mathbf{G}(\mathbf{a}).$$

where $\mathbf{a}^c = \sigma(c)\mathbf{a}c^{-1} + \delta(c)c^{-1}$

Example

For $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$. One can check that the following polynomials annihilates both $\mathbf{a}$ and $\mathbf{b}$:

$$(t_1 - \sum_{i=1}^{n} \sigma_{1i}(b_1 - a_1)b_i + \delta_1(b_1 - a_1))(t_1 - a_1)$$

$$(t_2 - \sum_{i=1}^{n} \sigma_{2i}(b_1 - a_1)b_i + \delta_2(b_1 - a_1))(t_1 - a_1)$$

Facts

- Classical correspondance between subsets of K^n and polynomials annihilating these subsets holds here...
- Lagrange interpolation holds....
- One can divide K^n into conjugacy classes and look for zeros of polynomial inside a class. These leads to a vector space just as $E(f, a) = \ker(f(T_{\mathbf{a}}))$ (as in the case $n = 1$).

c) **P-independence, P-Basis**

This notions are quite similar to the one in case $n = 1$. Briefly

- A subset of $E \subset K^n$ is said to be P independent if for any $a \in E$ there exists a polynomial annihilating $E\{a\}$ that doesn't annihilates a.
- A subset $E \subset K^n$ is closed if the set of common zeros of the polynomials that annihilate E is equal to E.
- A P-basis of a closed set C is a P idependent subset of C such that its closure is C.

Many questions

- Can we "count the roots" ?

- Analogue of left common multiples (i.e. generators of intersection of principal left ideals)?

- Analogues of Wedderburn polynomials ?

- In case $A = \mathbb{F}_q$ is a finite field can we imagine a similar situation as in the case $n = 1$?

- Ring structure of R and its quotient? (remark suppose $A = K$ is a division ring and $\Lambda \subset K^n$ is such that $\Lambda^c \subset \Lambda$, then $I(\Lambda) := \{f \in R \mid f(\Lambda) = 0\}$ is a two sided ideals)

.

Thank you (very Malte)!

.