Factorizations in Ore Extensions

Denison Conference, Columbus, Ohio, May 2012

The content of this talk is extracted from a few joint works with

T.Y. Lam, A. Ozturk, J. Delenclos.

A) Counting roots.

a) Skew polynomial rings.

b) Roots of polynomials and kernel of operators.

c) Counting the number of roots.

d) Wedderburn polynomials and their factorizations.

B) **Factorizations.**

a) Fully reducible polynomials and their characterizations.

b) Factorizations of fully reducible polynomials.

C)**Application.**

Factorizations in $\mathbb{F}_q[x;\theta]$.

.

1 A) Counting roots.

a)Skew polynomial rings.

K a division ring, $S \in End(K)$, D a S-derivation:

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

For $a \in K$, L_a left multiplication by a.
In $End(K,+)$, we then have : $D \circ L_a = L_{S(a)} \circ D + L_{D(a)}$.
Define a ring $R := K[t; S, D]$; 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:

$$\forall a \in K, \quad ta = S(a)t + D(a).$$

Exemples 1.1. 1) If $S = id.$ and $D = 0$ we get back the usual polynomial ring $K[x]$.

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

$$t^2 - 1 = (t + S(x))(t - x)$$

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

3) $R = \mathbb{Q}(x)[t; id., \frac{d}{dx}]$. $tx - xt = 1$; for any $q(x) \in \mathbb{Q}[x]$ the polynomial $(t - q(x))^n$ has distinct roots...

4) K a field, $q \in K \setminus \{0\}$ and $S \in End_K(K[x])$ defined by $S(x) = qx$. $R = K[x][y; S]$. Commutation rule: $yx = qxy$.

Facts

a) Ore (1933): $R = K[t; S, D]$ is a left principal ideal domain.

b) Ore (1933): $R = K[t; S, D]$ is a unique factorization domain:

If $f(t) = p_1(t) \dots p_n(t) = q_1(t) \dots q_m(t),\ p_i(t), q_i(t)$ irreducible then $m = n$ and there exists $\sigma \in \mathcal{S}_n$ such that,

$$\text{For } 1 \leq i \leq n, \qquad \frac{R}{Rq_i} \cong \frac{R}{Rp_{\sigma(i)}}$$

b) Roots and kernels

The map $\varphi_0 : R \longrightarrow End(K, +), \circ$ defined by

$$\varphi_0(\sum_{i=0}^{n} a_i t^i) = \sum_{i=0}^{n} a_i D^i$$

is a ring homomorphism.

More generally, for $a \in K$, $T_a \in End(K, +)$ is defined by

$$T_a(x) = S(x)a + D(x) \quad \forall x \in K.$$

Examples: $T_0 = D,\ T_1 = S + D$.

The map $\varphi_a : R \longrightarrow End(K, +)$ given by

$$\varphi_a(\sum_{i=0}^{n} a_i t^i) = \sum_{i=0}^{n} a_i T_a^i.$$

is a ring homomorphism.

For $a \in K$ and $f(t) \in R$ there exist $q(t) \in R, c \in K$ such that $f(t) = q(t)(t - a) + c$. c is called the (right) evaluation of $f(t)$ at a. We write $c = f(a)$. We say a is a (right) root of $f(t)$ if $f(a) = 0$.

Link between $\ker f(T_a)$ and (right) roots of $f(t)$?

Theorem 1.2. *(a)* $f(T_a)(1) = f(a)$*.*

(b) For $f, g \in R$*,* $fg(a) = f(T_a)(g(a))$*.*

(c) For $a, b \in K$ *with* $b \neq 0$*, we have* $(t-c)b = S(b)(t-a)$ *where* $c := S(b)ab^{-1} + D(b)b^{-1}$*. This will be* **denoted** $c = a^b$**)**

(d) For $b \neq 0$*,* $(f(t)b)(a) = f(a^b)b$*.*

(e) For $b \neq 0$*,* $f(T_a)(b) = f(a^b)b$*.*

(f) If $g(a) \neq 0$*, we have* $fg(a) = f(a^{g(a)})g(a)$*.*

Proof. (a) From $p(t) = q(t)(t-a) + p(a)$ we get
$p(T_a) = q(T_a)(T_a - L_a) + L_{p(a)}$. Since $(T_a - L_a)(1) = 0$, this gives (a)
(b) $fg(a) = fg(T_a)(1) = f(T_a)(g(T_a)(1)) = f(T_a)(g(a))$.
(c) $(t-c)b = tb - cb = tb - S(b)a - D(b) = S(b)(t-a)$.
(d) Write $f(t) = q(t)(t-a^b) + f(a^b)$ and
$f(t)b = q(t)S(b)(t-a) + f(a^b)b$.
(e) For $b \neq 0$, $f(a^b)b = (f(t)b)(a) = (f(T_a) \circ L_b)(1) = f(T_a)(b)$
(f) This is clear from (b) and (e). □

We define

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

.

c) Counting roots

Facts and notations

$a \in K$, $R = K[t; S, D]$.

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

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

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

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

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

d) Wedderburn polynomials and their factorizations

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

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

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.

Exemple 1.7. 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:

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

Remarques 1.8.

(b) Wedderburn polynomials can be used to develop noncommuative symmetric functions.

(b) **Question**: Is every left V-domain a right V-domain?
Can we use $R = K[t; S, D]$ to construct such an example?
One necessary condition for R to be a right V domain is that every monic polynomial is Wedderburn... (-,T.Y.Lam, S.K.Jain)

(c) Matrices $A \in M_n(K)$ that are (S, D)-diagonalizable are can be characterized by Wedderburn polynomials ($S \in Aut(K)$.)

How can we build all the linear factorizations of a Wedderburn polynomial?

Theorem 1.9. *Let $f \in R$ be a Wedderburn polynomial and $V(f)$ the set of his right roots.*

(a) Assume that $V(f) \subseteq \Delta(a)$, then the linear factorizations are in bijection with the complete flags of right $C(a)$-vector spaces in $E(f, a)$.

(b) Assume that $V(f) \subseteq \bigcup_{i=1}^{r} \Delta(a_i)$ then the linear factorizations of f are in bijection with the "shuffle complete flags" of $\bigcup_{i=1}^{r} E(f, a_i)$.

Since a polynomial which is linearly factorizable is a product of Wedderburn polynomials we can use the above factorizations to get factorizations of such polynomials.

Exemple 1.10. Let us describe all the factorizations of $f = [t - a^x, t - a]_l$. These factorizations are in bijection with the complete flags in the two dimensional vector space $E(f, a) = C + xC$ where $C := C^{S,D}(a)$. The flags are of the form $0 \neq yC \subset E(f, a)$. Apart from the flag $0 \subset xC \subset E(f, a)$, they are given by $0 \subset (1 + x\beta)C \subset E(f, a)$, where $\beta \in C^{S,D}(a)$. Hence we get the following factorizations $f = (t - a^{a-a^x})(t - a^x)$ and $(t - a^{a-\gamma})(t - a^{1+x\beta})$, where $\gamma = a - a^{1+x\beta}$.

2 B) Fully reducible polynomials and their factorizations.

a) Fully reducible polynomials

Definitions 2.1. (a) A monic polynomial $f \in R = K[t; S; D]$ is fully reducible if there exist irreducible polynomials $p_1, \dots, p_n$ such that $Rf = \bigcap_{i=1}^n Rp_i$.

(b) $p, q \in R$ are conjugate iff $R/Rp \cong R/Rq$.

Theorem 2.2. *Let $f \in R$ be a monic polynomial of degree l. Then the following are equivalent:*

(i) f is fully reducible.

(ii) There exist monic irreducible polynomials $p_1 \dots, p_n$ such that $Rf = \cap_{i=1}^n Rp_i$ is an irredundant intersection.

(iii) There exist monic irreducible polynomials $p_1 \dots p_n \in R$ and an invertible matrix $V \in M_l(K)$ such that

$$C_f V = S(V) diag(C_{p_1} \dots, C_{p_n}) + D(V).$$

where $C_f, C_{p_1}, \dots, C_{p_n}$ denote companion matrices.

(iv) $R = R/Rf$ is semisimple.

.

b) Factorizations of fully reducible polynomials.

Definitions 2.3. (a) Let p be an irreducible monic polynomial of degree n.

$$t. : \ R/RP \longrightarrow R/Rp : g + Rp \mapsto tg + Rp$$

$$T_p : K^n \longrightarrow K^n : v \mapsto S(v)C_p + D(v)$$

Where C_p denotes the companion matrix of p.

(b) Get a left R-module structure on K^n: $f(t).v = f(T_p)(v)$.

${}_RK^n_{S_p}$ where $S_p := End_R(K^n) \cong End_R(R/Rp)$ is a division ring.

For $f(t) \in R$, $f(T_p) \in End(K^n, +)$ is right S_p-linear.

Define $V(f) = \{p \in R \,|\, p \text{ is irreducible and } f \in Rp\}$

(c) Two monic polynomials $p, q \in R$ are conjugate if $R/Rp \cong R/Rq$.

(d) For $f(t) \in R$, $E(f,p) := \{q \in R \,|\, q \in V(f) \text{ and } R/RP \cong R/Rq\}$.

Theorem 2.4. *Let $f(t) \in R$ of degree n;*

(a) $V(f)$ intersects at most n conjugacy classes say $\Delta(p_1), \dots, \Delta(p_n)$.

(b) $\sum_{i=1}^{n} dim_{S_i} \ker f(T_{P_i}) \leq n$, where $S_i := End(R/Rp_i)$.

(c) The equality occurs in (b) if and only if f is fully reducible.

As for the Wedderburn polynomials, one can get all the factorizations of a fully reducible polynomial by looking at flags in the and shuffles of flags in the different $\ker f(T_p)$ where $p(t) \in V(f)$.

.

3 C) Application

a)**Factorizations in $\mathbb{F}_q[t;\theta]$.**

Aim: reduce factorization in $\mathbb{F}_q[t;\theta]$ to factorisation in $\mathbb{F}_q[x]$

Definitions 3.1. p a prime number,
(a)$i \geq 1$, put $[i] := \frac{p^i-1}{p-1} = p^{i-1} + p^{i-2} + \cdots + 1$ and put $[0] = 0$.
(b) $q = p^n$. define $\mathbb{F}_q[x^{\square}] \subset \mathbb{F}_q[x]$ by:

$$\mathbb{F}_q[x^{\square}] := \{\sum_{i\geq 0} \alpha_i x^{[i]} \in \mathbb{F}_q[x]\}$$

Elements of $\mathbb{F}_q[x^{\square}]$ are called $[p]$-polynomials.

Extend θ to $F_q[x]$ via $\theta(x) = x^p$ i.e. $\theta(g) = g^p$ for $g \in F_q[x]$.

Let us consider $R := F_q[t;\theta] \subset S := F_q[x][t;\theta]$.

For $f \in R := \mathbb{F}_q[t;\theta] \subset \mathbb{F}_q[x][t;\theta]$
We may evaluate f in x.

Theorem 3.2. *Let $f(t) = \sum_{i=0}^n a_i t^i \in R := \mathbb{F}_q[t;\theta] \subset S := \mathbb{F}_q[x][t;\theta]$. We have:*

1) for every $b \in \mathbb{F}_q$, $f(b) = \sum_{i=0}^n a_i b^{[i]}$.

2) $f^{\square}(x) = \sum_{i=0}^n a_i x^{[i]} \in \mathbb{F}_q[x^{\square}]$.

3) $\{f^{\square} | f \in R = \mathbb{F}_q[t;\theta]\} = \mathbb{F}_q[x^{\square}]$.

4) For $i \geq 0$ and $h(x) \in \mathbb{F}_q[x]$ we have $T_x^i(h) = h^{p^i} x^{[i]}$.

5) If $g(t) \in S = F_q[x][t;\theta]$ et $h(x) \in \mathbb{F}_q[x]$ $g(T_x)(h(x)) \in \mathbb{F}_q[x]h(x)$.

6) For $h(t) \in R = \mathbb{F}_q[t;\theta]$, $f(t) \in Rh(t)$ iff $f^{\square}(x) \in \mathbb{F}_q[x]h^{\square}(x)$.

Corollaire 3.3. *$f(t) \in \mathbb{F}_q[t;\theta]$ is irrducible iff the corresponding p-polynomial $f^{\square}$ does not have non trivial factors in $\mathbb{F}_q[x^{\square}]$.*

Method

Let $f(t) \in R := \mathbb{F}_q[t;\theta]$.

Step 1 Compute $f^{\square}$ and check if $f^{\square}$ has a factor in $\mathbb{F}_q[x^{\square}]$. If no then $f(t)$ is irreducible R.

Step 2 If $f^{\square}(x) = q(x)h^{\square}(x)$ for some polynomial $h(t)$ then $h(t)$ divides $f(t)$ and write $f(t) = g(t)h(t)$. Come back to step 1 replacing $f(t)$ by $g(t)$.

Example

Consider $f(t) = t^4 + (a+1)t^3 + a^2t^2 + (1+a)t + 1 \in \mathbb{F}_4[t;\theta]$. its associated polynomial is $x^{15} + (a+1)x^7 + (a+1)x^3 + (1+a)x + 1 \in \mathbb{F}_4[x]$. We may factorize it as:

$$(x^{12}+ax^{10}+x^9+(a+1)x^8+(a+1)x^5+(a+1)x^4+x^3+ax^2+x+1)(x^3+ax+1)$$

This last factor is a $[p]$-polynomial that corresponds to $t^2 + at + 1 \in \mathbb{F}_4[t;\theta]$. Since $x^3 + ax + 1$ is irreducible in $\mathbb{F}_4[x]$, we have $t^2 + at + 1$ is irreducible as well in $\mathbb{F}_4[t;\theta]$. We conclude that $f(t) = (t^2 + t + 1)(t^2 + at + 1)$ is a decomposition of $f(t)$ in irreducible factors in $\mathbb{F}_4[t;\theta]$.

.

THANK YOU ALL

THANK YOU LAM

Very happy birthday !