INSTITUTE OF MATHEMATICS
of the
Polish Academy of Sciences

ul. Śniadeckich 8, P.O.B. 21, 00-956 Warszawa 10, Poland http://www.impan.pl

IM PAN Preprint 722 (2010)

Tomasz Maszczyk

On Splitting Polynomials in Noncommutative Extensions

Presented by Piotr M. Hajac

Published as manuscript

Received 05 May 2010

ON SPLITTING POLYNOMIALS IN NONCOMMUTATIVE EXTENSIONS

TOMASZ MASZCZYK†

ABSTRACT. We prove that for every splitting of a polynomial $f(X) \in K[X]$ into linear factors in a K-algebra A, any cyclic permutation of linear factors gives the same result and all roots of linear factors are roots of that polynomial. We use it to identify moding out $A[X]/(f(X))$ by the left ideal generated by a linear factor with the right substitution of its root. With a splitting we associate a distributive law between monads and prove that any splitting of a separable polynomial in the center $Z(A)$ does not admit formal deformations in A with a nontrivial distributive law.

1. Introduction. Let $f(X) = f_n X^n + f_{n-1}X^{n-1} + \cdots + f_0 \in A[X]$ be a polynomial with coefficients in a commutative unital ring A. Suppose there is given a splitting of $f(X)$ in $A[X]$

$$f(X) = f_n(X - a_1)\cdots(X - a_n). \tag{1}$$

Then by the substitution homomorphism argument one sees that all a_k's are roots of $f(X)$ and by commutativity of $A[X]$ any permutation of them defines the same splitting. Therefore the problem of splitting of a given polynomial reduces to the problem of finding the set of its roots. This fact is fundamental for Galois theory and algebraic geometry.

In the case of noncommutative coefficients of a given polynomial the situation is much worse. First of all, a given splitting does not reduce to the set of elements a_k, since we cannot permute linear factors because of noncommutativity of $A[X]$. Moreover, if $a \in A$ is not central in A then the substitution homomorphism of rings

$$\mathbb{Z}[X] \to A, \quad X \mapsto a \tag{2}$$

does not extend to a homomorphism of A-algebras

$$A[X] \to A, \quad X \mapsto a, \tag{3}$$

because X is central in $A[X]$. This means that one can not use the substitution A-algebra homomorphism argument to prove that elements $a_1, \ldots, a_n$ appearing in the decomposition

$$f(X) = f_n(X - a_1)\cdots(X - a_n) \tag{4}$$

are roots of $f(X)$. The problem of such splittings in terms of relationships between coefficients of a given polynomial with a generic set of its (left or right) roots and elements a_k (so called pseudoroots) was related to quadratic algebras with structure encoded by graphs in [1][3][2][5]. However, these relationships are

†The author was partially supported by KBN grants N201 1770 33 and 115/E-343/SPB/6.PR UE/DIE 50/2005-2008.

Mathematics Subject Classification (2000): 13P05, 16U80, 15A30.

much more complicated than in the commutative case and make sense only if some elements of the algebra are invertible.

The interest for splitting polynomials in noncommutative algebras started in 1921 when Wedderburn proved [6] that any minimal polynomial $f(X) \in K[X]$ of an element of a central division algebra A algebraic over the center K of A splits in $A[X]$ into linear factors which can be permuted cyclically and every pseudoroot appearing in this splitting is a root of $f(X)$. This fact was very helpful in determining the structure of division algebras of small order [6] and found many other applications (see e.g. [4] for references).

We start this paper from an observation that under the assumption that coefficients (which do not have to commute one with each other) commute with pseudoroots (which do not have to commute one with each other) the situation is much closer to the commutative case. We show that then pseudoroots are roots and any cyclic permutation of them gives the same splitting. This means that instead of finite sets of commutative roots (ordered n-tuples up to all permutations) we obtain finite cyclically ordered sets (ordered n-tuples up to all cyclic permutations) of noncommutative roots. We give examples of such splittings, beyond the context of division rings, where in spite of cyclic symmetry, transposition of any two consequtive linear factors is impossible. It does not seem that this elementary fact could be derived from the known theory of splitting polynomials in noncommutative algebras (Gelfand-Retakh-Wilson [3]). The reason is that the condition of commutativity between coefficients and pseudoroots is a closed condition while the general theory works for generic elements. We will see in examples that the above elementary fact is true even if differences of pseudoroots are non-invertible or even nilpotent.

Next, we apply this observation to construct a canonical map $A \otimes_K L \to A \times \cdots \times A$ related to a given splitting. This map generalizes evaluation map on polynomials with coefficients in a commutative extension A of K modulo the ideal generated by a given polynomial split in A evaluated on the corresponding set of roots. Since in the definition of the canonical map we use right substitution which is not an algebra homomorphism it is a bit surprising that its structure is related to the very fundamental mathematical structure, a distributive law between monads. Such a distributive law defines (and is equivalent to) some multiplication on the tensor product $A \otimes_K L$. In the commutative case this multiplication coincides with the standard multiplication on $A \otimes_K L$ regarded as a push-out in the category of commutative rings. We show noncommutative examples where this multiplication is different from the standard one. However, we show that any formal deformation of the standard multiplication, induced by a formal (possibly noncommutative) deformation of a splitting of any separable polynomial in the center of the algebra A, is trivial.

In the examples one can observe some intimate relations between automorphisms of the extension and the above splitting twist (equivalently, the above distributive law for monads). Regretfully, at this stage it is not clear whether one could expect any precise connection between splittings of polynomials in noncommutative extensions and their automorphisms, resembling Galois theory.

2. Results. We start from a lemma which is the essence of the original argument of Wedderburn [6]. However, the original context of division rings is inessential for properties we are interested in.

Lemma 1. *Let g, h be elements of a monoid G, where h is right cancelable and the product gh commutes with h. Then g and h commute.*

Proof. Since gh commutes with h, we have

$$ghh = hgh. \tag{5}$$

But h is right cancelable, hence consequently

$$gh = hg. \ \square \tag{6}$$

Lemma 2. *Let A be a ring and A^a be its subring of elements commuting with a fixed $a \in A$. If $f(X) \in A^a[X]$ decomposes in $A[X]$ as follows*

$$f(X) = g(X)(X - a) \tag{7}$$

then $g(X) \in A^a[X]$ and $f(a) = 0$.

Proof. To prove that $g(X) \in A^a[X] = A[X]^{X-a}$ take $G = A[X]$ with multiplication of polynomials, $g = g(X)$, $h = h(X) = X - a$ and apply Lemma 1.

Using the already proven fact that $g(X) \in A^a[X]$ we can apply the substitution homomorphism

$$\begin{aligned} A^a[X] &\to A^a, \\ X &\mapsto a \end{aligned} \tag{8}$$

well defined by the definition of A^a, to the decomposition (7), which proves the root property. $\square$

Theorem 1. *Let A be a unital ring and $A^{a_1,\dots,a_n}$ be its subring of elements commuting with $a_1, \dots, a_n \in A$. If $f(X) \in A^{a_1,\dots,a_n}[X]$ splits in $A[X]$ as follows*

$$f(X) = f_n(X - a_1)(X - a_2) \cdots (X - a_n) \tag{9}$$

then

$$f(X) = f_n(X - a_n)(X - a_1) \cdots (X - a_{n-1}) \tag{10}$$

and

$$f(a_1) = \cdots = f(a_n) = 0. \tag{11}$$

Proof. To prove the cyclic property of the splitting take $a = a_n$, $g(X) = f_n(X - a_1)(X - a_2) \cdots (X - a_{n-1})$ and apply Lemma 2. Then Lemma 2 also implies the root property for a_n. By the cyclic property the same holds for all other a_k's. $\square$

The canonical map. The most important consequence of cyclic and root properties of the above splitting is the existence of a canonical map extending a well known canonical ring homomorphism related to a splitting of a polynomial with commutative coefficients by a commutative base change.

First, with every polynomial $f(X) \in K[X]$ with coefficients in a unital ring K we can associate the following cyclic left $K[X]$-module

$$L := K[X]/K[X]f(X). \tag{12}$$

After tensoring it by a K-ring A we get a cyclic $A[X]$-module

$$A \otimes_K L = A[X]/A[X]f(X). \tag{13}$$

Assume now that $f(X)$ splits in $A[X]$ as follows

$$f(X) = f_n(X - a_1)(X - a_2)\cdots(X - a_n) \tag{14}$$

with $a_1, ..., a_n \in A$ commuting with the image of K in A.

Fix one a_i. By the cyclic property we have

$$f(X) = f_n(X - a_{i+1})\cdots(X - a_n)(X - a_1)\cdots(X - a_i), \tag{15}$$

where $a_{n+1} := a_1$. Substituting (15) into (13) we obtain a canonical homomorphism of left A-modules

$$A \otimes_K L \to A[X]/A[X](X - a_i). \tag{16}$$

Next, by the following identity

$$X^k = (X^{k-1} + aX^{k-2} + \cdots + a^{k-1})(X - a) + a^k \tag{17}$$

in $A[X]$, valid for every $a \in A$, we obtain a well defined canonical homomorphism of left A-modules

$$\begin{aligned} \pi_i : A[X]/A[X](X - a_i) &\to A, \\ X^k + A[X](X - a_i) &\mapsto a_i^k. \end{aligned} \tag{18}$$

Although A can be noncommutative the following fact is still true, as in the commutative case.

Lemma 3. *The morphism of left A-modules (18) is an isomorphism.*

Proof. Composing π_i with a map

$$\begin{aligned} \sigma_i : A &\to A[X]/A[X](X - a_i), \\ a &\mapsto a \cdot 1 + A[X](X - a_i), \end{aligned} \tag{19}$$

we obtain $(\pi_i \circ \sigma_i)(a) = a$ and

$$(\sigma_i \circ \pi_i)(X^k + A[X](X - a_i)) \tag{20}$$

$$= a_i^k \cdot 1 + A[X](X - a_i) \tag{21}$$

$$= X^k - (X^{k-1} + a_i X^{k-2} + \cdots + a_i^{k-1})(X - a_i) + A[X](X - a_i) \tag{22}$$

$$= X^k + A[X](X - a_i), \tag{23}$$

hence $\sigma_i = \pi_i^{-1}$. □

The following proposition says that also moding out $A \otimes_K L = A[X]/A[X]f(X)$ by the (left) ideal $A[X](X - a_i)$ still can be identified with the (right) substitution morphism (well defined by the root property)

$$\begin{aligned} A[X]/A[X]f(X) &\to A, \\ X^k + A[X]f(X) &\mapsto a_i^k, \end{aligned} \tag{24}$$

as in the commutative case. It can be proved immediately, by simple checking.

Proposition 1. *The following diagram of left A-modules, with arrows defined as in (18), (16) and (24),*

$$\begin{array}{ccc} & A \otimes_K L & \\ \swarrow & & \searrow \\ A[X]/A[X](X - a_i) & \xrightarrow{\cong} & A, \end{array}$$

commutes.

Collecting together compositions of (16) and (18) for all i's we get the following *canonical map* (A-module homomorphism)

$$A \otimes_K L \to A \times \cdots \times A \tag{25}$$

well defined by the formula

$$a \otimes (X^k + K[X]f(X)) \mapsto (aa_1^k, \ldots, aa_n^k). \tag{26}$$

Let us note now that the right hand side of the canonical map has a canonical product A-ring structure, in particular we have a canonical diagonal ring homomorphisms $A \to A \times \cdots \times A$.

If K and A are commutative then the canonical map is a ring homomorphism, where on the left (resp. right) hand side the ring structure comes from the push-out (resp. the product) in the category of commutative rings.

If only K is commutative and A is a K-algebra, the cyclic $K[X]$-module L still has a canonical structure of a commutative K-algebra and the tensor product $A \otimes_K L$ has a canonical structure of an L-algebra. The product of evaluation maps of polynomials with coefficients in K at roots $(a_1, \ldots, a_n)$ defines a canonical ring homomorphism $L \to A \times \cdots \times A$, well defined thanks to the root property. Then using the formula (26) one can easily check commutativity of the diagram of K-modules

$$\begin{array}{ccc} & A & \\ \swarrow & & \searrow \\ A \otimes_K L & \longrightarrow & A \times \cdots \times A \\ \nwarrow & & \nearrow \\ & L & \end{array} \tag{27}$$

where the left skew arrows are ring homomorphisms defined by tensoring by the unit of the other tensor factor, the right skew arrows are ring homomorphisms descibed above and the horizontal arrow, the canonical map, is an (A, L)-bimodule homomorphism of cyclic (A, L)-bimodules preserving the generator, i.e. mapping $1 \otimes 1 \mapsto (1, \ldots, 1)$.

The $\star$ -product. If the canonical map is bijective it is an (A, L)-bimodule isomorphism. Then one can transport the product ring structure via this isomorphism to $A \otimes_K L$ to obtain another K-algebra structure on $A \otimes_K L = A[X]/A[X]f(X)$ with the same unit. Since the canonical map is an (A, L)-bimodule homomorphism the new multiplication

$$(-) \star (-) : (A \otimes_K L) \otimes_K (A \otimes_K L) \to A \otimes_K L \tag{28}$$

is uniquely determined by the K-linear map (we call it *the splitting twist*)

$$\tau : L \otimes_K A \to A \otimes_K L, \tag{29}$$

$$l \otimes a \mapsto (1 \otimes l) \star (a \otimes 1) \tag{30}$$

as follows

$$(a \otimes l) \star (a' \otimes l') = a\tau(l \otimes a')l'. \tag{31}$$

Theorem 2. *The splitting twist τ is a* distributive law *between monads $A\otimes_K(-)$ and $L\otimes_K(-)$ on the category of K-modules, or equivalently, the following diagrams (32)-(34) commute.*

$$\begin{array}{ccccc} L\otimes_K L\otimes_K A & \xrightarrow{L\otimes\tau} & L\otimes_K A\otimes_K L & \xrightarrow{\tau\otimes L} & A\otimes_K L\otimes_K L \\ \downarrow{\scriptstyle \mu_L\otimes A} & & & & \downarrow{\scriptstyle A\otimes\mu_L} \\ L\otimes_K A & & \xrightarrow{\qquad\qquad\tau\qquad\qquad} & & A\otimes_K L, \end{array} \tag{32}$$

$$\begin{array}{ccccc} L\otimes_K A\otimes_K A & \xrightarrow{\tau\otimes A} & A\otimes_K L\otimes_K A & \xrightarrow{A\otimes\tau} & A\otimes_K A\otimes_K L \\ \downarrow{\scriptstyle L\otimes\mu_A} & & & & \downarrow{\scriptstyle \mu_A\otimes L} \\ L\otimes_K A & & \xrightarrow{\qquad\qquad\tau\qquad\qquad} & & A\otimes_K L, \end{array} \tag{33}$$

$$\begin{array}{ccc} & A & \\ {\scriptstyle \eta_L\otimes A}\swarrow & & \searrow{\scriptstyle A\otimes\eta_L} \\ L\otimes_K A & \xrightarrow{\tau} & A\otimes_K L, \end{array} \qquad \begin{array}{ccc} & L & \\ {\scriptstyle L\otimes\eta_A}\swarrow & & \searrow{\scriptstyle \eta_A\otimes L} \\ L\otimes_K A & \xrightarrow{\tau} & A\otimes_K L, \end{array} \tag{34}$$

where η's and μ's denote the unit and the multiplication maps of K-algebras.

Proof. Below we use the property that maps from L and A in the commutative diagram (27) are ring homomorphisms, associativity of the $\star$ -product with the unit $1\otimes 1$ and the notation $a^{(\tau)}\otimes l^{(\tau)} := \tau(l\otimes a)$.

Proof of (32):

$$\begin{aligned} (\tau\circ(\mu_L\otimes A))(l'\otimes l\otimes a) &= \tau(l'l\otimes a) = (1\otimes l'l)\star(a\otimes 1) \\ &= (1\otimes l')\star(1\otimes l)\star(a\otimes 1) = (1\otimes l')\star\tau(l\otimes a) \\ &= (1\otimes l')\star(a^{(\tau)}\otimes l^{(\tau)}) = \tau(l'\otimes a^{(\tau)})l^{(\tau)} \\ &= ((A\otimes\mu_L)\circ(\tau\otimes L)\circ(L\otimes\tau))(l'\otimes l\otimes a). \end{aligned} \tag{35}$$

Proof of (33):

$$\begin{aligned} (\tau\circ(L\otimes\mu_A))(l\otimes a\otimes a') &= \tau(l\otimes aa') = (1\otimes l)\star(aa'\otimes 1) \\ &= (1\otimes l)\star(a\otimes l)\star(a'\otimes 1) = \tau(l\otimes a)\star(a'\otimes 1) \\ &= (a^{(\tau)}\otimes l^{(\tau)})\star(a'\otimes 1) = a^{(\tau)}\tau(l^{(\tau)}\otimes a'), \\ &= ((\mu_A\otimes L)\circ(A\otimes\tau)\circ(\tau\otimes A))(l\otimes a\otimes a'). \end{aligned} \tag{36}$$

Proof of (34):

$$(\tau\circ(\eta_L\otimes A))(a) = \tau(1\otimes a) = (1\otimes 1)\star(a\otimes 1) = a\otimes 1 = (A\otimes\eta_L)(a), \tag{37}$$

$$(\tau\circ(L\otimes\eta_A))(l) = \tau(l\otimes 1) = (1\otimes l)\star(1\otimes 1) = 1\otimes l = (\eta_A\otimes L)(l). \tag{38}$$

□

Corollary 1. *The splitting twist is uniquely determined by its values on the set of simple tensors $l\otimes a$, where l's and a's run through the sets of generators of K-algebras L and A, respectively.*

Deforming multiplication by deforming a splitting. Assume now that $f(X)$ is monic separable and splits in the center of a finite K-algebra A. Since the square of the Vandermonde determinant of commuting roots $a_1, \dots, a_n$ equals the discriminant of $f(X)$ the Vandermonde matrix is invertible. Since for commuting roots $a_1, \dots, a_n$ the canonical map is a ring homomorphism the $\star$ -product coincides with the standard multiplication on $A \otimes_K L$. If we start to deform this central splitting inside a noncommutative K-algebra $A[X]$ the Vandermonde matrix stays invertible for sufficiently small Zariski open subset in the scheme parameterizing the deformation. The corresponding $\star$ -product provides then a deformation of the standard multiplication on $A \otimes_K L$, under which the unit $1 \otimes 1$ stays not deformed.

Now we are interested in deformations parameterized by the formal scheme Spec$K[[T]]$. The corresponding formal deformation of the canonical map is uniquely determined by a $K[[T]]$-linear map (we call it *a formal deformation of the splitting twist*)

$$\tau[[T]] : L[[T]] \otimes_{K[[T]]} A[[T]] \to A[[T]] \otimes_{K[[T]]} L[[T]], \tag{39}$$

defining a distributive law between the monads $A[[T]] \otimes_{K[[T]]} (-)$ and $L[[T]] \otimes_{K[[T]]} (-)$ on the category of $K[[T]]$-modules.

The following theorem describes a remarkable rigidity property of the commutative canonical map.

Theorem 3. *Any formal deformation of the splitting of a separable polynomial $f(X) \in K[X]$ with roots in the center of a finite K-algebra A to a splitting with (possibly noncommutative) roots in A induces a trivial deformation of the standard multiplication on $A \otimes_K K[X]/(f(X))$.*

Equivalently, under such a deformation the splitting twist is constant

$$\tau[[T]] = \tau \otimes K[[T]]. \tag{40}$$

Equivalently, under such a deformation the canonical map is a ring homomorphism.

Proof. Any formal deformation of the splitting twist can be written as the formal series

$$\tau[[T]] = \sum_{k=0}^{\infty} \tau_k \otimes T^k, \tag{41}$$

where $\tau_0 = \tau$ is the initial splitting twist corresponding to the splitting with roots in the center of A, which is nothing else but the flip

$$\tau(l \otimes a) = a \otimes l. \tag{42}$$

We will prove by induction that all higher coefficients must vanish. The commutativity of the diagram (32) applied to the expansion (41) gives the following relations between its coefficients

$$\tau_k \circ (\mu_L \otimes A) = (A \otimes \mu_L) \circ \sum_{i+j=k} (\tau_i \otimes L) \circ (L \otimes \tau_j). \tag{43}$$

Assuming that $\tau_0(l \otimes a) = a \otimes l$, $\tau_1 = \dots = \tau_k = 0$ we prove that $\tau_{k+1} = 0$.

By (43)

(44)
$$\tau_{k+1} \circ (\mu_L \otimes A) = (A \otimes \mu_L) \circ ((\tau_0 \otimes L) \circ (L \otimes \tau_{k+1}) + (\tau_{k+1} \otimes L) \circ (L \otimes \tau_0))$$

Evaluating on $l' \otimes l \otimes a$, using the notation $a^{(\tau_k)} \otimes l^{(\tau_k)} := \tau_k(l \otimes a)$ and the fact that L is commutative (this moment will be indicated by ©), we obtain

$$(\tau_{k+1} \circ (\mu_L \otimes A))(l' \otimes l \otimes a) = \tau_{k+1}(l'l \otimes a), \tag{45}$$

$$\begin{aligned}
& ((A \otimes \mu_L) \circ (\tau_0 \otimes L) \circ (L \otimes \tau_{k+1}))(l' \otimes l \otimes a) && (46)\\
= \; & ((A \otimes \mu_L) \circ (\tau_0 \otimes L))(l' \otimes \tau_{k+1}(l \otimes a)) && (47)\\
= \; & ((A \otimes \mu_L) \circ (\tau_0 \otimes L))(l' \otimes a^{(\tau_{k+1})} \otimes l^{(\tau_{k+1})}) && (48)\\
= \; & (A \otimes \mu_L)(a^{(\tau_{k+1})} \otimes l' \otimes l^{(\tau_{k+1})}) && (49)\\
= \; & a^{(\tau_{k+1})} \otimes l' l^{(\tau_{k+1})} && (50)\\
\overset{©}{=} \; & a^{(\tau_{k+1})} \otimes l^{(\tau_{k+1})} l' && (51)\\
= \; & \tau_{k+1}(l \otimes a) l', && (52)
\end{aligned}$$

$$\begin{aligned}
& ((A \otimes \mu_L) \circ (\tau_{k+1} \otimes L) \circ (L \otimes \tau_0))(l' \otimes l \otimes a) && (53)\\
= \; & ((A \otimes \mu_L) \circ (\tau_{k+1} \otimes L))(l' \otimes a \otimes l)) && (54)\\
= \; & (A \otimes \mu_L)(a^{(\tau_{k+1})} \otimes l'^{(\tau_{k+1})} \otimes l) && (55)\\
= \; & a^{(\tau_{k+1})} \otimes l'^{(\tau_{k+1})} l && (56)\\
= \; & \tau_{k+1}(l' \otimes a) l, && (57)
\end{aligned}$$

hence by (44)

$$\tau_{k+1}(l'l \otimes a) = \tau_{k+1}(l \otimes a) l' + \tau_{k+1}(l' \otimes a) l. \tag{58}$$

This means that for every $a \in A$ the map $\tau_{k+1}(- \otimes a)$ is a K-linear derivation

$$\tau_{k+1}(- \otimes a) \in \mathrm{Der}_K(L, A \otimes_K L) = \mathrm{Hom}_L(\Omega^1_{L/K}, A \otimes_K L). \tag{59}$$

Since $f(X)$ is a separable polynomial, i.e. its discriminant is invertible, L is an étale commutative algebra, hence $\Omega^1_{L/K} = 0$. This implies that $\tau_{k+1} = 0$. □

The case of a monic polynomial. If $f(X)$ is monic both sides of the canonical map are free A-modules of rank n, where on the left hand side the basis consists of the congruence equivalence classes of representatives $(1, X, \ldots, X^{n-1})$. Then the canonical map is described by means of the Vandermonde matrix

$$\alpha_0 + \alpha_1 X + \ldots + \alpha_{n-1} X^{n-1} \mapsto (\alpha_0, \ldots, \alpha_{n-1}) \begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ \vdots & & \vdots \\ a_1^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}. \tag{60}$$

In this case the canonical map is invertible whenever the corresponding Vandermonde matrix is invertible, hence the $\star$ -product is given by the explicit formula

(61)

$$g(X)\star h(X) = (g(a_1)h(a_1),\ldots,g(a_n)h(a_n)) \begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ \vdots & & \vdots \\ a_1^{n-1} & \cdots & a_n^{n-1} \end{pmatrix}^{-1} \begin{pmatrix} 1 \\ X \\ \vdots \\ X^{n-1} \end{pmatrix},$$

where for $g(X) = g_0+g_1X+\cdots+g_{n-1}X^{n-1}$ we define $g(a)$ by the right substitution

$$g(a) := g_0 + g_1a + \cdots + g_{n-1}a^{n-1}. \tag{62}$$

Note that, in spite of the fact that in general the right substitution of a non-central element $a \in A$ is not a ring homomorphism, i.e. for $(gh)(X) := g(X)h(X)$ we can have $(gh)(a) \neq g(a)h(a)$, the $\star$ -product is associative and unital with the unit $1(X) := 1 \in A[X]/A[X]f(X) = A \otimes_K L$.

The splitting twist can be regarded also as a rewriting of a left polynomial $\alpha_0 + X\alpha_1 + \cdots + X^{n-1}\alpha_{n-1}$ as a right polynomial $\alpha_0^\tau + \alpha_1^\tau X + \cdots + \alpha_{n-1}^\tau X^{n-1}$, where the row vector $\alpha^\tau := (\alpha_0^\tau,\ldots,\alpha_{n-1}^\tau)$ is computed from the column vector $\alpha := (\alpha_0,\ldots,\alpha_{n-1})^\intercal$ by matrix multiplication

$$\alpha^\tau = (V^\intercal\alpha)^\intercal V^{-1}, \tag{63}$$

in which V stands for the Vandermonde matrix as in (60) and $(-)^\intercal$ denotes matrix transposition. This rewriting is invertible whenever the transposed Vandermonde matrix is also invertible. The latter condition is fulfilled automatically, provided the roots $a_1,\ldots,a_n$ commute one with each other.

Note also, that if the roots $a_1,\ldots,a_n$ are central in A, the right substitution is a ring homomorphism, and the Vandermonde matrix in the above formula (63) cancels, hence consequently $g(X)\star h(X) = g(X)h(X)$ in $A[X]/A[X]f(X)$, as follows from the general argument that then the canonical map is a ring homomorphism.

3. Examples.

In this paragraph we give examples of noncommutative splittings which resemble, to some extent, splittings of separable polynomials in their splitting fields. However, new phenomena appear as a consequence of noncommutativity and/or non-separability, related to the action of the algebra endomorphisms on the roots.

Example 1. Let $A = \mathbb{H}$ be the algebra of quaternions over the field $K = \mathbb{R}$ of real numbers and take $f(X) = X^2+1 \in K[X] \subset A[X]$. It can be split as follows

$$f(X) = (X-a_1)(X-a_2), \tag{64}$$

with commuting roots $(a_1,a_2) = (i,-i)$ in A, where i is a quaternionic imaginary unit. The Vandermonde matrix

$$\begin{pmatrix} 1 & 1 \\ a_1 & a_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix} \tag{65}$$

is invertible, as well as its inverse, since the roots commute.

Since the left hand side of the canonical map is isomorphic to the simple algebra $\mathbb{H}\otimes_{\mathbb{R}}\mathbb{C} \cong \mathrm{M}_2(\mathbb{C})$ of 2×2 matrices over complex numbers, while the right hand side is equal to $\mathbb{H}\times\mathbb{H}$, the splitting twist is nontrivial (different from the flip)

$$\tau(X\otimes q) = iqi^{-1}\otimes X. \tag{66}$$

Note the appearance of a nontrivial automorphism of the extension in the formula for the splitting twist.

Example 2. Let A be the ring of 3×3 matrices over a nonzero commutative ring K and take $f(X) = X^3 - 4 \in K[X] \subset A[X]$. It can be split as follows

$$f(X) = (X - a_1)(X - a_2)(X - a_3), \tag{67}$$

with roots in A

$$a_1 = \begin{pmatrix} 0 & 2 & 0 \\ 0 & 0 & 2 \\ 1 & 0 & 0 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & 2 \\ -2 & 0 & 0 \end{pmatrix}, \quad a_3 = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -4 \\ 1 & 0 & 0 \end{pmatrix}. \tag{68}$$

whose Vandermonde matrix

$$\begin{pmatrix} 1 & 1 & 1 \\ a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 2 & 0 & 0 & -1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 2 & 0 & 0 & -4 \\ 1 & 0 & 0 & -2 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & -2 & 0 & 0 & 4 \\ 2 & 0 & 0 & -4 & 0 & 0 & -4 & 0 & 0 \\ 0 & 2 & 0 & 0 & 2 & 0 & 0 & -1 & 0 \end{pmatrix} \tag{69}$$

and its $\intercal$-transpose

$$\begin{pmatrix} 1 & a_1 & a_1^2 \\ 1 & a_2 & a_2^2 \\ 1 & a_3 & a_3^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & 0 & 2 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 & 2 & -4 & 0 & 0 \\ 0 & 0 & 1 & -2 & 0 & 0 & 0 & 2 & 0 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 & 0 & -4 & -4 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & -1 & 0 \end{pmatrix} \tag{70}$$

are both invertible, provided 6 is invertible in K, and then the splitting twist is invertible. Although the linear factors can be cyclically permuted, none two of them can be transposed if $3 \neq 0$ in K, because

$$[a_1, a_2] = [a_2, a_3] = [a_3, a_1] = \begin{pmatrix} 0 & 0 & 6 \\ -6 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}. \tag{71}$$

Moreover, if 6 is not a zero divisor in K the subalgebra $A^{a_1,a_2,a_3} \subset A$ of elements commuting with a_1, a_2, a_3 coincides with K. Indeed, A^{a_1,a_2,a_3} consists of elements

$$a = \begin{pmatrix} \alpha & \beta & 2\gamma \\ -2\gamma & \alpha & \beta \\ -\beta & \gamma & \alpha \end{pmatrix}, \tag{72}$$

where $3\beta = 0$, $6\gamma = 0$.

If 210 is invertible in K, A is generated by a_1, a_2, a_3 as an algebra over K. Indeed, then we have

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = -\frac{1}{9}a_1^2a_2 - \frac{1}{18}a_2^2a_3, \tag{73}$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \frac{13}{45}a_1 - \frac{13}{90}a_2 + \frac{1}{60}a_1^2a_3^2 + \frac{1}{60}a_2^2a_3^2 + \frac{7}{180}a_1^2a_2^2, \tag{74}$$

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \frac{1}{9}a_1^2 - \frac{1}{18}a_2^2 + \frac{1}{9}a_3^2, \tag{75}$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \frac{1}{18}a_1^2 - \frac{1}{9}a_2^2 - \frac{1}{9}a_3^2, \tag{76}$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \frac{1}{12}a_1a_2^2 - \frac{1}{12}a_3a_2^2 - \frac{1}{9}a_1^2a_2 - \frac{1}{18}a_2^2a_3, \tag{77}$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} = \frac{2}{9}a_1 + \frac{2}{9}a_2 - \frac{1}{36}a_1^2a_2^2, \tag{78}$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix} = -\frac{5}{18}a_2 - \frac{1}{36}a_1^2a_2^2 - \frac{1}{36}a_2^2a_3^2, \tag{79}$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = \frac{2}{9}a_1^2 + \frac{2}{9}a_2^2 - \frac{1}{9}a_3^2, \tag{80}$$

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \frac{1}{4}a_1a_2a_3 - \frac{1}{12}a_1a_2^2 + \frac{1}{12}a_3a_2^2 + \frac{2}{9}a_1^2a_2 + \frac{1}{9}a_2^2a_3. \tag{81}$$

Note that a_1, a_2, a_3 are conjugate one to each other by some K-algebra automorphisms of the algebra A:

$$a_1 = u_{12}a_2u_{12}^{-1}, \quad a_2 = u_{23}a_3u_{23}^{-1}, \quad a_3 = u_{31}a_1u_{31}^{-1}, \tag{82}$$

where

$$u_{12} = \begin{pmatrix} -2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad u_{23} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -2 \end{pmatrix}, \quad u_{31} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \tag{83}$$

provided 2 is invertible in K. The matrices (83), which define automorphisms of the extension A/K permuting roots of the splitting, appear also in the following formula for the splitting twist

$$\tau(X \otimes a_1) = a_1^2u_{23}^{-1} \otimes 1 - a_2 \otimes X + u_{23} \otimes X^2, \tag{84}$$

$$\tau(X \otimes a_2) = a_2^2u_{31}^{-1} \otimes 1 - a_3 \otimes X + u_{31} \otimes X^2, \tag{85}$$

$$\tau(X \otimes a_3) = a_3^2u_{12}^{-1} \otimes 1 - a_1 \otimes X + u_{12} \otimes X^2, \tag{86}$$

reflecting the cyclic symmetry of the splitting and determining the splitting twist uniquely, provided 210 is invertible in K. It would be desirable to find a conceptual explanation of this relationship in terms of some Galois type theory connecting splittings of polynomials in noncommutative extensions and their automorphisms.

Example 3. Let A be the ring of upper triangular 2×2 matrices over a nonzero commutative ring K and take $f(X)=X^2(X-1)\in K[X]\subset A[X]$. This polynomial is completely split in K and non-separable. Although it has a double root in K it can be split in A as follows

$$f(X)=(X-a_1)(X-a_2)(X-a_3), \tag{87}$$

where

$$a_1=\begin{pmatrix}0&0\\0&1\end{pmatrix},\quad a_2=\begin{pmatrix}0&-1\\0&0\end{pmatrix},\quad a_3=\begin{pmatrix}1&1\\0&0\end{pmatrix} \tag{88}$$

are pairwise distinct roots in A. However, the Vandermonde matrix

$$\begin{pmatrix}1&1&1\\a_1&a_2&a_3\\a_1^2&a_2^2&a_3^2\end{pmatrix}=\begin{pmatrix}1&0&1&0&1&0\\0&1&0&1&0&1\\0&0&0&-1&1&1\\0&1&0&0&0&0\\0&0&0&0&1&1\\0&1&0&0&0&0\end{pmatrix} \tag{89}$$

is not invertible (look at fourth and sixth rows or first and third columns on the right hand side). In fact, for every splitting of $f(X)$ in $A[X]$ (they all will be described below) the Vandermonde matrix is not invertible.

The linear factors can be cyclically permuted, but none two of them can be transposed, because

$$[a_1,a_2]=[a_2,a_3]=[a_3,a_1]=-a_2\neq 0. \tag{90}$$

First of all, it is obvious that $A^{a_1,a_2,a_3}=K$. Moreover, A is freely generated by a_1,a_2,a_3 as a module over K with a multiplication table

	a_1	a_2	a_3
a_1	a_1	0	0
a_2	a_2	0	0
a_3	$-a_2$	a_2	a_3

If K doesn't contain nontrivial idempotents all endomorphisms of the extension $K\subset A$ come in families $\varepsilon,\varepsilon',\varepsilon_s^\sigma,\varepsilon_s$ parameterized by elements σ and s, where σ's are elements of the multiplicative monoid of K acting (from the right) on elements s of the (right) K-module K by right multiplication. The logic of this notation will be clear later, when the rules of matrix multiplication

$$\begin{pmatrix}\sigma&s\\0&1\end{pmatrix}\begin{pmatrix}\tau&t\\0&1\end{pmatrix}=\begin{pmatrix}\sigma\tau&\sigma t+s\\0&1\end{pmatrix},\quad \begin{pmatrix}\sigma&s\\0&1\end{pmatrix}\begin{pmatrix}t\\1\end{pmatrix}=\begin{pmatrix}\sigma t+s\\1\end{pmatrix} \tag{91}$$

will appear in the structure of the endomorphism monoid and its various actions.

The K-algebra endomorphism monoid M of A is determined by its values on basic elements a_1,a_2,a_3 as follows

	a_1	a_2	a_3
ε	$a_1+a_2+a_3$	0	0
ε'	0	0	$a_1+a_2+a_3$
ε_s^σ	a_1-sa_2	σa_2	$(1-\sigma+s)a_2+a_3$
ε_s	$(1+s)a_2+a_3$	0	a_1-sa_2

hence the monoid structure is

	ε	ε'	ε_t^τ	ε_t
ε	ε	ε'	ε	ε'
ε'	ε	ε'	ε'	ε
ε_s^σ	ε	ε'	$\varepsilon_{\sigma t+s}^{\sigma\tau}$	$\varepsilon_{\sigma t+s}$
ε_s	ε	ε'	ε_s	ε_s^0

with the neutral element ε_0^1. Note that the only invertible elements are ε_t^τ's with τ invertible in K. All such automorphisms are inner

$$\varepsilon_t^\tau(a)=u_{\tau,t}au_{\tau,t}^{-1},\quad u_{\tau,t}=\begin{pmatrix}\tau & t\\ 0 & 1\end{pmatrix}.$$

It is easy to check that if there is an element τ invertible in K such that $(\tau-1)$ is not a zero divisor in K the subring $A^G\subset A$ fixed by the group G of K-algebra automorphisms of A equals K.

If K is a domain all roots and all cycles of $f(X)$ also come in families parameterized by elements τ and t.

The families of roots are

$$\begin{aligned} r^\tau &= \tau a_2,\\ r_t^0 &= (1+t)a_2+a_3,\\ r_t &= a_1-ta_2,\\ r &= a_1+a_2+a_3. \end{aligned}$$

The families of cycles are

$$\begin{aligned} c^\tau &= (r^\tau, r^{-\tau}, r),\\ c_t^\tau &= (r^\tau, r_{-\tau+t}^0, r_t),\\ c_t &= (r^0, r_t, r_t^0). \end{aligned}$$

We see that

(a) The set of all roots is the union of supports of all cycles.
(b) Different cycles can have the same support: $|c^\tau|=|c^{-\tau}|$, $|c_t^0|=|c_t|$.
(c) Different cycles can define the same splitting: c^τ and $c^{-\tau}$, c_t^0 and c_t.

The action of the endomorphism monoid on roots is

	r^τ	r_t^0	r_t	r
ε	r^0	r^0	r	r
ε'	r^0	r	r^0	r
ε_s^σ	$r^{\sigma\tau}$	$r_{\sigma t+s}^0$	$r_{\sigma t+s}$	r
ε_s	r^0	r_s	r_s^0	r

which implies that

(d) (Orbits) There are five G-orbits:
r^0 and r as fixpoints,
an orbit of r^1 with the additive stabilizer $\{\varepsilon_s^1\} = K \subset G$,
an orbit of r_0 with the multiplicative stabilizer $\{\varepsilon_0^\sigma\} = K^\times \subset G$,
and a free orbit of r_0^1.
(e) (Sources) Every root is an M-translate of r^1 or r_0^1.
(f) (Sinks) r^0 and r are fixed by M and every root can be translated by M either to r^0 or to r.

The action of the endomorphism monoid on cycles is

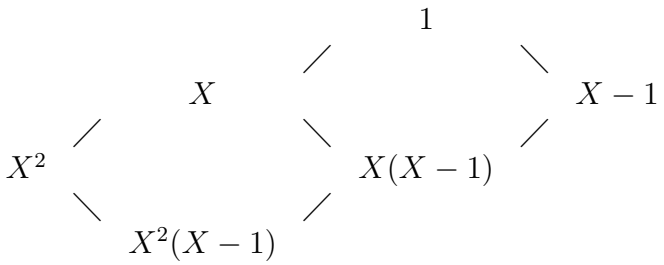
	c^τ	c_t^τ	c_t
$\varepsilon, \varepsilon'$	c^0	c^0	c^0
ε_s^σ	$c^{\sigma\tau}$	$c_{\sigma t+s}^{\sigma\tau}$	$c_{\sigma t+s}$
ε_s	c^0	c_s	c_s^0

which implies that

(g) (Orbits) There are five G-orbits:
c^0 as a fixpoint,
an orbit of c^1 with the additive stabilizer $\{\varepsilon_s^1\} = K \subset G$,
two orbits, of c_0 and c_0^0, with the multiplicative stabilizer $\{\varepsilon_0^\sigma\} = K^\times \subset G$,
and a free orbit of c_0^1.
(h) (Sources) Every cycle is an M-translate of c^1 or c_0^1.
(i) (Sinks) c^0 is fixed by M and every cycle can be translated by M to c^0.

As we see, in our example there are many cycles and endomorphisms can move roots from one cycle to another. It turns out that roots are no more equivalent. Instead of strict equivalence of roots of a separable polynomial induced by the transitive Galois action we have the action of endomorphisms on some lattice of roots. This can be described as follows.

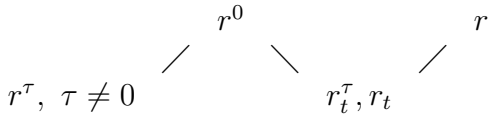
The lattice of ideals in $K[X]$



defines a partial order on roots by taking the minimal polynomial

r^0	r^τ, $\tau \neq 0$	r_t^τ	r_t	r
X	X^2	$X(X-1)$	$X(X-1)$	$X-1$

which looks as follows



One can check that all endomorphisms act along the above poset of roots moving them at most upwards (it is obvious that no endomorphism can diminish a root with respect to the partial order induced by the minimal polynomial).

Among all endomorphisms only ε and ε' do not preserve this partial order (there are essentially four exceptions: $r^0 \succ r_t^\tau$, $r^0 \succ r_t$, $r \succ r_t^\tau$, $r \succ r_t$ but $\varepsilon'(r^0) \not\succ \varepsilon'(r_t^\tau)$, $\varepsilon(r^0) \not\succ \varepsilon(r_t)$, $\varepsilon(r) \not\succ \varepsilon(r_t^\tau)$, $\varepsilon'(r) \not\succ \varepsilon'(r_t)$). In particular, all automorphisms do preserve the above partial order on roots. All endomorphisms preserve the weaker partial order opposite to that one which is induced by the degree (levels in the above poset of roots). Again, it would be desirable to explain this accordance of automorphisms of the extension with the structure of the lattice (or poset) of roots in frames of some Galois type theory of (non-separable) polynomials split in noncommutative and non-separable extensions.

References

[1] Gelfand, I.; Retakh, V.: *Noncommutative Vieta theorem and symmetric functions.* In *The Gelfand Mathematical Seminars, 1993-1995*, Gelfand Math. Sem., pp. 93-100, Birkhauser Boston, Boston, MA, 1996.

[2] Gelfand, I.; Gelfand, S.; Retakh, V.; Wilson, R. L.: *Factorization over noncommutative algebras and sufficient sets of edges in directed graphs.* Lett. Math. Physics, **74** (2005), pp. 153–167.

[3] Gelfand, I.; Retakh, V.; Wilson, R. L.: *Quadratic linear algebras associated with factorizations of noncommutative polynomials and noncommutative differential polynomials, Selecta Math. (N. S.)*, **7**(4) (2001), pp. 493–523.

[4] Lam, T. Y.; Leroy, A.: *Wedderburn polynomials over division rings, I.* J. Pure Appl. Algebra **186** (2004), no. 1, 43–76.

[5] Retakh, V.; Serconek, S.; Wilson, R. L: *Constructions of some algebras associated to directed graphs and related to factorizations of noncommutative polynomials,* Proc. of the Conference "Lie algebras, vertex operator algebras and their applications" (to appear), preprint math.RA/0603327.

[6] Wedderburn, J.H.M.: *On division algebras*, Trans. Amer. Math. Soc. **22** (1921), 129-135.

Institute of Mathematics, Polish Academy of Sciences, Sniadeckich 8
00–956 Warszawa, Poland,
Institute of Mathematics, University of Warsaw, Banacha 2
02–097 Warszawa, Poland

E-mail address: t.maszczyk@uw.edu.pl