Glasgow Math. J. **50** (2008) 191–201. © 2008 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089508004138. Printed in the United Kingdom

FACTORIZATION OF MONOMORPHISMS OF A POLYNOMIAL ALGEBRA IN ONE VARIABLE

V. V. BAVULA

Department of Pure Mathematics, University of Sheffield, Hicks Building, Sheffield S3 7RH, UK
e-mail: v.bavula@sheffield.ac.uk

(Received 11 January, 2007; revised 14 September, 2007; accepted 14 October, 2007)

Abstract. Let $K[x]$ be a polynomial algebra in a variable x over a commutative $\mathbb{Q}$-algebra K, and Γ' the monoid of K-algebra monomorphisms of $K[x]$ of the type $\sigma : x \mapsto x + \lambda_2 x^2 + \cdots + \lambda_n x^n$, $\lambda_i \in K$, λ_n is a unit of K. It is proved that for each $\sigma \in \Gamma'$ there are only finitely many distinct decompositions $\sigma = \sigma_1 \cdots \sigma_s$ in Γ'. Moreover, each such decomposition is uniquely determined by the degrees of components: if $\sigma = \sigma_1 \cdots \sigma_s = \tau_1 \cdots \tau_s$ then $\sigma_1 = \tau_1, \ldots, \sigma_s = \tau_s$ if and only if $\deg(\sigma_1) = \deg(\tau_1), \ldots, \deg(\sigma_s) = \deg(\tau_s)$. Explicit formulae are given for the components σ_i via the coefficients λ_j and the degrees $\deg(\sigma_k)$ (as an application of the inversion formula for polynomial automorphisms in *several* variables from [**1**]). In general, for a polynomial there are no formulae (in radicals) for its divisors (elementary Galois theory). Surprisingly, one can write such formulae where instead of the product of polynomials one considers their composition (as polynomial functions).

2000 *Mathematics Subject Classification.* 16W20, 16W22.

Contents

1. Introduction. Throughout, K is a commutative $\mathbb{Q}$-algebra (if it is not stated otherwise) with the group of units K^*, $K[x]$ is a polynomial algebra over K in a single variable x, $\mathrm{Aut}_K(K[x])$ and $\mathrm{Mon}_K(K[x])$ are the group of automorphisms and the monoid of monomorphisms of the polynomial algebra $K[x]$ respectively.

$$\Gamma' := \Gamma'(K) := \{\sigma \in \mathrm{Mon}_K(K[x]) \,|\, \sigma : x \mapsto x + \lambda_2 x^2 + \cdots + \lambda_n x^n, \lambda_i \in K, \lambda_n \in K^*\}$$

is the submonoid of $\mathrm{Mon}_K(K[x])$, and $\deg(\sigma) := \deg(\sigma(x))$ is called the *degree* of σ. For $\sigma_1, \ldots, \sigma_s \in \Gamma'$,

$$\deg(\sigma_1 \cdots \sigma_s) = \deg(\sigma_1) \cdots \deg(\sigma_s). \tag{1}$$

The group $\mathrm{Aut}_K(K[x])$ contains the *affine* group $\mathrm{Aff} := \{\sigma : x \mapsto ax + b \,|\, a \in K^*, b \in K\}$. If K is a reduced $\mathbb{Q}$-algebra then $\mathrm{Aut}_K(K[x]) = \mathrm{Aff}$. If, in addition, K is an algebraically closed field then $\mathrm{Mon}_K(K[x]) = \mathrm{Aff} \times_{ex} \Gamma'$ is the exact product of

monoids, i.e. each monomorphism $\sigma \in \mathrm{Mon}_K(K[x])$ is a unique product $\sigma = \tau\gamma$ for some $\tau \in \mathrm{Aff}$ and $\gamma \in \Gamma'$.

The monoid Γ' is large, it is an infinite dimensional algebraic monoid. The submonoid M of Γ' generated by the monomorphisms $\{\sigma_{\lambda x^n} : x \mapsto x + \lambda x^n \mid \lambda \in K^*, n \geq 2\}$ is a *free* monoid (Theorem 3.3) with the free generators $\{\sigma_{\lambda x^n}\}$.

For an element $\sigma \in \Gamma' \backslash \{e\}$ (where e is the identity of Γ'), the set

$$\mathrm{Dec}(\sigma) := \{(\sigma_1, \ldots, \sigma_s) \mid \sigma_1 \cdots \sigma_s = \sigma, s \geq 1, \sigma_i \in \Gamma' \backslash \{e\}\}$$

is called the *decomposition set* for σ, the set

$$\mathrm{Sign}(\sigma) := \{(\deg(\sigma_1), \ldots, \deg(\sigma_s)) \mid (\sigma_1, \ldots, \sigma_s) \in \mathrm{Dec}(\sigma)\}$$

is called the *signature* of σ, and the map

$$\mathrm{sign} := \mathrm{sign}_\sigma : \mathrm{Dec}(\sigma) \mapsto \mathrm{Sign}(\sigma), \quad (\sigma_1, \ldots, \sigma_s) \mapsto (\deg(\sigma_1), \ldots, \deg(\sigma_s)),$$

is called the *signature map*. It is obvious that the signature map is a surjection and the signature $\mathrm{Sign}(\sigma)$ is a *finite* set since, for each $(\sigma_1, \ldots, \sigma_s) \in \mathrm{Dec}(\sigma)$, $\deg(\sigma) = \deg(\sigma_1) \cdots \deg(\sigma_s)$. The next theorem shows that the signature map is a bijection, i.e. each decomposition $\sigma = \sigma_1 \cdots \sigma_s$ is completely determined by the degrees of the components.

THEOREM 1.1. *Let K be a commutative $\mathbb{Q}$-algebra. For each $\sigma \in \Gamma'$, the signature map $\mathrm{sign}_\sigma : \mathrm{Dec}(\sigma) \mapsto \mathrm{Sign}(\sigma)$ is a bijection. In particular, there are only finitely many, namely $|\mathrm{Sign}(\sigma)|$, distinct decompositions $\sigma = \sigma_1 \cdots \sigma_s$.*

For each natural number $n \geq 1$, the set

$$\Gamma'_n := \left\{\sigma \in \Gamma' \mid \sigma(x) - x \in \sum_{i \geq 1} Kx^{1+ni}\right\}$$

is a submonoid of Γ', $\Gamma' = \Gamma'_1$, and $m|n$ (m divides n) implies $\Gamma'_n \subseteq \Gamma'_m$.

THEOREM 1.2. *Let K be a commutative $\mathbb{Q}$-algebra. If $\sigma \in \Gamma'_n$ and $\sigma = \sigma_1 \cdots \sigma_s$ in Γ' then all $\sigma_i \in \Gamma'_n$.*

Suppose that a monomorphism $\Gamma' \ni \delta : x \mapsto x + c_2x^2 + \cdots + c_dx^d$, $c_i \in K$, $c_d \in K^*$, is a product $\delta = \sigma\tau$ of two monomorphisms $\sigma, \tau \in \Gamma' \backslash \{e\}$, we say that δ is *decomposable*. Theorem 3.2 gives the *formulae* for σ and τ via the constants $c_2, \ldots, c_d$ of the polynomial $\delta(x)$ and the degree $\deg(\sigma)$ of σ.

A decomposability criterion for elements of Γ' is given (Corollary 2.4). Using it and the chain rule, a necessary condition for irreducibility of a polynomial is found (Corollary 4.2).

Using different language the monoid $\mathrm{Mon}_{\mathbb{C}}(\mathbb{C}[x])$ was studied by J. F. Ritt [**4**]. He proved two fundamental theorems on decompositions of elements in this monoid. Later, H. T. Engstrom [**2**] and H. Levi [**3**] proved, respectively, the first and the second theorem for $\mathrm{Mon}_K(K[x])$ where K is a field of characteristic zero.

2. Proof of Theorem 1.1. In this section, Theorems 1.1 and 1.2 are proved based on Theorem 2.2. A criterion of decomposability (Corollary 2.4) for a monomorphism of Γ' is given.

https://doi.org/10.1017/S0017089508004138 Published online by Cambridge University Press

A polynomial $p \in K[x]$ of the type $x + \lambda_2 x^2 + \cdots + \lambda_n x^n, \lambda_i \in K, \lambda_n \in K^*$, is called a *unitary* polynomial. Note that the map $p \mapsto (\delta_p : x \mapsto p)$ is a bijection between the set of unitary polynomials and Γ'.

If K is a *field* of characteristic zero then the fact that for each monomorphism $e \neq \sigma \in \Gamma'$ there are only *finitely many* distinct decompositions $\sigma = \sigma_1 \cdots \sigma_s$ follows directly from the chain rule and the fact that the polynomial algebra $K[x]$ is a unique factorization domain:

LEMMA 2.1. *Let K be a field of characteristic zero and $e \neq \sigma \in \Gamma'$. There are only finitely many distinct decompositions $\sigma = \sigma_1 \cdots \sigma_s$ in Γ' with all $\sigma_i \neq e$.*

Proof. Using induction on the degree $\deg(\sigma)$ and (1), it suffices to show that there are finitely many distinct decompositions for $s = 2$, i.e. $\sigma = \sigma_1\sigma_2$. Let $F := \sigma(x)$, $g := \sigma_1(x)$, and $f := \sigma_2(x)$. Then $F = f(g)$, the composition of polynomials. By the chain rule, $F' = f'(g)g'$, the product of polynomials with scalar term 1, g' is a divisor of the polynomial F' where $a' := \frac{da}{dx}$. Since there are only finitely many divisors of the polynomial F' with scalar term 1 the result follows. □

The ratio form of $\sigma \in \Gamma'$. Let K be a commutative $\mathbb{Q}$-algebra. Each element $\sigma \in \Gamma'$ is uniquely determined by the polynomial $\sigma(x) = x(1 + \lambda_1 x + \cdots + \lambda_n x^n)$ where $\lambda_i \in K$, $\lambda_n \in K^*$, and $\deg(\sigma) = n + 1$. For computational reasons it is convenient to write the polynomial $\sigma(x)$ in the *ratio* form

$$\sigma(x) = x(1 + (a_{n-1}x^{-(n-1)} + \cdots + a_1 x^{-1} + 1)\lambda x^n) = x(1 + (A + 1)\lambda x^n) \tag{2}$$

where $\lambda := \lambda_n$; $a_i := \frac{\lambda_{n-i}}{\lambda_n}$, $i = 1, \ldots, n-1$; and $A := \sum_{i=1}^{n-1} a_i x^{-i}$. Let $\mathbb{R}^{n-1}$ be the standard $(n-1)$-dimensional vector space over the reals $\mathbb{R}$ with the standard inner product $yz := y_1 z_1 + \cdots + y_{n-1} z_{n-1}$. Let $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}^{n-1}$, $|\alpha| := \alpha_1 + \cdots + \alpha_{n-1}$, $a^\alpha := a_1^{\alpha_1} \cdots a_{n-1}^{\alpha_{n-1}}$, $\overrightarrow{n-1} := (1, 2, \ldots, n-1)$, $\overrightarrow{n-1}\alpha = \alpha_1 + 2\alpha_2 + \cdots + (n-1)\alpha_{n-1}$ (the inner product of vectors). For $\alpha \in \mathbb{N}^{n-1}$ with $|\alpha| \leq i$, $\binom{i}{\alpha} := \frac{i!}{(i-|\alpha|)!\alpha_1! \cdots \alpha_{n-1}!}$ is the multi-binomial coefficient. We set $0^0 := 1$.

For each $m \geq 1$, we have the equality

$$\sigma(x^m) = x^m\left(1 + \sum_{i=1}^{m} \binom{m}{i} \lambda^i x^{in} + \sum_{i=1}^{m} \sum_{1 \leq |\alpha| \leq i} \binom{m}{i}\binom{i}{\alpha} a^\alpha \lambda^i x^{-\overrightarrow{n-1}\alpha + in}\right). \tag{3}$$

In more detail,

$$\begin{aligned}\sigma(x^m) = x^m(1 + (A+1)\lambda x^n)^m &= x^m\left(1 + \sum_{i=1}^{m} \binom{m}{i} (A+1)^i \lambda^i x^{in}\right) \\ &= x^m\left(1 + \sum_{i=1}^{m} \binom{m}{i}\left(1 + \sum_{1 \leq |\alpha| \leq i} \binom{i}{\alpha} a^\alpha x^{-\overrightarrow{n-1}\alpha}\right)\lambda^i x^{in}\right),\end{aligned}$$

multiplying out we obtain (3).

THEOREM 2.2. *Let K be a commutative $\mathbb{Q}$-algebra, $\Gamma' \ni \delta : x \mapsto \delta(x) = x + c_2 x^2 + \cdots + c_d x^d$, $c_i \in K$, $c_d \in K^*$. If $\delta = \sigma\tau$ for some elements $\sigma, \tau \in \Gamma'$ then the elements σ and τ are uniquely determined by the degree of σ. In more detail, if $\sigma(x) = x(1 + (a_{n-1}x^{-(n-1)} + \cdots + a_1 x^{-1} + 1)\lambda x^n)$ where $n + 1 = \deg(\sigma)$, and $\tau(x) = x + \mu_2 x^2 + \cdots + \mu_m x^m$ where $\deg(\tau) = m = \frac{d}{n+1}$ then*

https://doi.org/10.1017/S0017089508004138 Published online by Cambridge University Press

1. *the coefficients* $a_1, \dots, a_{n-1}, \lambda$ *are the unique solution to the following triangular system of non-linear equations:*

$$ma_j + \sum_{C_j} \binom{m}{\alpha_1, \dots, \alpha_{j-1}} a_1^{\alpha_1} \cdots a_{j-1}^{\alpha_{j-1}} = \frac{c_{d-j}}{c_d}, \quad j = 1, \dots, n-1,$$

$$m\lambda^{-1} + \sum_{\alpha \in \mathbb{N}^{n-1},\, |\alpha| \le m,\, \overrightarrow{n-1}\alpha = n} \binom{m}{\alpha} a^\alpha = \frac{c_{d-n}}{c_d},$$

where $C_1 := \emptyset$ *and* $C_j := \{\alpha = (\alpha_1, \dots, \alpha_{j-1}) \in \mathbb{N}^{j-1} \mid \alpha_1 + 2\alpha_2 + \cdots + (j-1)\alpha_{j-1} = j,\ |\alpha| \le m\}$, $j \ge 2$, *and*

2. *the coefficients* $\mu_j, j = 2, \dots, m$, *are the unique solution to the following triangular system of linear equations in* μ_j*:*

$$\mu_j + \sum_{D_j} \mu_{m'} \binom{m'}{i} \lambda^i + \sum_{E_j} \mu_{m'} \binom{m'}{i} \binom{i}{\alpha} a^\alpha \lambda^i = c_j, \quad j = 2, \dots, m,$$

where $\mu_1 := 1$,

$$D_j := \{(m', i) \in \mathbb{N}^2 \mid 1 \le i \le m' < j,\ m' + in = j\},$$
$$E_j := \{(m', i, \alpha) \in \mathbb{N}^2 \times \mathbb{N}^{n-1} \mid 1 \le |\alpha| \le i \le m' < j,\ m' - \overrightarrow{n-1}\alpha + in = j\}.$$

Proof. Note that $\tau(x) = b + \mu_m x^m$ where $b := x + \sum_{i=2}^{m-1} \mu_i x^i$, $\deg \sigma(b) = \deg \sigma(x^{m-1}) = (m-1)(n+1)$ and

$$\deg \sigma(\mu_m x^m) - \deg \sigma(b) = m(n+1) - (m-1)(n+1) = n+1. \tag{4}$$

By (3) and (4), $c_d = \mu_m \lambda^m$, and for each $j = 1, \dots, n-1$,

$$c_{d-j} = \mu_m \lambda^m \left(ma_j + \sum_{C_j} \binom{m}{\alpha_1, \dots, \alpha_{j-1}} a_1^{\alpha_1} \cdots a_{j-1}^{\alpha_{j-1}} \right),$$

$$c_{d-n} = \mu_m \lambda^m \left(m\lambda^{-1} + \sum_{\alpha \in \mathbb{N}^{n-1},\, |\alpha| \le m,\, \overrightarrow{n-1}\alpha = n} \binom{m}{\alpha} a^\alpha \right).$$

Taking the ratios $\frac{c_{d-j}}{c_d}$, $j = 1, \dots, n$, we have the system of equations as in the first statement. The triangular structure of the system gives the unique solution for the coefficients $a_1, \dots, a_{n-1}, \lambda$. Since σ is an algebra monomorphism of $K[x]$, the element τ in the equality $\delta = \sigma\tau$ is unique.

2. There is the equality

$$\delta(x) = \sum_{m'=1}^{m} \mu_{m'} x^{m'} + \sum_{m'=1}^{m} \sum_{i=1}^{m'} \mu_{m'} \binom{m'}{i} \lambda^i x^{m'+in}$$
$$+ \sum_{m'=1}^{m} \sum_{i=1}^{m'} \sum_{1 \le |\alpha| \le i} \mu_{m'} \binom{m'}{i} \binom{i}{\alpha} a^\alpha \lambda^i x^{m' - \overrightarrow{n-1}\alpha + in}.$$

https://doi.org/10.1017/S0017089508004138 Published online by Cambridge University Press

In more detail,

$$\delta(x) = \sum_{m'=1}^{m} \mu_{m'}\sigma(x^{m'}) = \sum_{m'=1}^{m} \mu_{m'}x^{m'}\left(1 + \sum_{i=1}^{m'}\binom{m'}{i}\left(1 + \sum_{1\le|\alpha|\le i}\binom{i}{\alpha}a^{\alpha}x^{-\overrightarrow{n-1}\alpha}\right)\lambda^{i}x^{in}\right).$$

By opening up the brackets we obtain the result. The formula for $\delta(x)$ above can be written shortly as the sum $S_1 + S_2 + S_3$ where S_1, S_2 and S_3 are the single, double, and triple sum respectively. For each $j = 2, \dots, m$, the coefficient of x^j in the sum S_1 is equal to μ_j; the coefficient of x^j in the sum S_2 is equal to $\sum_{D_j}\mu_{m'}\binom{m'}{i}\lambda^i$ since the conditions $1 \le i \le m'$ and $m' + in = j$ imply $m' < j$; and the coefficient of x^j in the sum S_3 is equal to $\sum_{E_j}\mu_{m'}\binom{m'}{i}\binom{i}{\alpha}a^{\alpha}\lambda^i$ since the two conditions $in - \overrightarrow{n-1}\alpha \ge 1$ (as follows easily from the equality $\alpha_1 + \cdots + \alpha_{n-1} \le i$) and $m' - \overrightarrow{n-1}\alpha + in = j$ imply the strict inequality $m' < j$. In more detail,

$$\begin{aligned} in - \overrightarrow{n-1}\alpha &= in - \alpha_1 - 2\alpha_2 - \cdots - (n-1)\alpha_{n-1} \\ &\ge n(\alpha_1 + \cdots + \alpha_{n-1}) - \alpha_1 - 2\alpha_2 - \cdots - (n-1)\alpha_{n-1} \\ &= \sum_{i=1}^{n-1}(n-i)\alpha_i \ge 1 \end{aligned}$$

since $|\alpha| \ge 1$ and all $n - i \ge 1$. For each $j = 2, \dots, m$, equating the coefficients of x^j of both sides of the equality $\sigma\tau(x) = \delta(x)$ we obtain the triangular system of linear equations with the unknowns μ_j as in statement 2. It has the unique solution that can be easily written explicitly using the Cramer's formula via the elements $a_1, \dots, a_{n-1}, \lambda$. This proves the theorem. □

Equating the coefficients of x^j, $m < j < d - n$, of both sides of the equality $\delta(x) = \sigma\tau(x)$, we get the system of equations

$$c_j = \sum_{F_j}\mu_{m'}\binom{m'}{i}\lambda^i + \sum_{G_j}\mu_{m'}\binom{m'}{i}\binom{i}{\alpha}a^{\alpha}\lambda^i, \quad m < j < d - n, \tag{5}$$

where

$$\begin{aligned} F_j &:= \{(m', i) \in \mathbb{N}^2 \mid 1 \le i \le m' \le m,\ m' + in = j\}, \\ G_j &:= \{(m', i, \alpha) \in \mathbb{N}^2 \times \mathbb{N}^{n-1} \mid 1 \le |\alpha| \le i \le m' \le m,\ m' - \overrightarrow{n-1}\alpha + in = j\}. \end{aligned}$$

Note that in (5),

$$a^{\alpha}\lambda^i = \lambda_{n-1}^{\alpha_1}\lambda_{n-2}^{\alpha_2}\cdots\lambda_1^{\alpha_{n-1}}\lambda^{i-\alpha_1-\cdots-\alpha_{n-1}}, \quad i - \alpha_1 - \cdots - \alpha_{n-1} \ge 0.$$

So, the RHS of (5) is a polynomial in μ_i and λ_k with integer coefficients.

Proof of Theorem 1.1. By the very definition, the signature map is surjective. If $\sigma = \sigma_1\cdots\sigma_s = \tau_1\cdots\tau_s$ in Γ' and $\deg(\sigma_1) = \deg(\tau_1), \dots, \deg(\sigma_s) = \deg(\tau_s)$ then, by Theorem 2.2, $\sigma_1 = \tau_1, \dots, \sigma_s = \tau_s$, i.e. the signature map is injective. □

COROLLARY 2.3. *We keep the notation of Theorem 2.2. Then*

1. *for each* $j = 1, \dots, n-1$, $a_j \in \mathbb{Z}[\frac{1}{m}][\frac{c_{d-j}}{c_d}, \frac{c_{d-j+1}}{c_d}, \dots, \frac{c_{d-1}}{c_d}]$, *i.e.* a_j *is a polynomial in* $\frac{c_{d-j}}{c_d}, \frac{c_{d-j+1}}{c_d}, \dots, \frac{c_{d-1}}{c_d}$ *with coefficients from* $\mathbb{Z}[\frac{1}{m}]$.

https://doi.org/10.1017/S0017089508004138 Published online by Cambridge University Press

2. $\lambda \in \mathbb{Q}(\frac{c_{d-n}}{c_d}, \frac{c_{d-n+1}}{c_d}, \dots, \frac{c_{d-1}}{c_d})$, *i.e.* λ *is a rational function in* $\frac{c_{d-n}}{c_d}, \frac{c_{d-n+1}}{c_d}, \dots, \frac{c_{d-1}}{c_d}$ *with rational coefficients,*
3. $\mu_j \in \sum_{k=2}^{j} c_k \mathbb{Q}(\frac{c_{d-n}}{c_d}, \frac{c_{d-n+1}}{c_d}, \dots, \frac{c_{d-1}}{c_d})$ *and* $\mu_j \in \sum_{k=2}^{j} c_k \mathbb{Q}(\lambda_1, \dots, \lambda_n)$, *for each* $j = 2, \dots, m$.

Proof. It is obvious. □

Recall that a monomorphism $\delta \in \Gamma' \backslash \{e\}$ is *decomposable* if $\delta = \sigma\tau$ for some monomorphisms $\sigma, \tau \in \Gamma' \backslash \{e\}$. The next corollary is a decomposability criterion.

COROLLARY 2.4. *We keep the notation of Theorem 2.2. The monomorphism* δ *of* Γ' *of degree* $d = (n+1)m$, $\delta(x) = x + c_2x^2 + \cdots + c_dx^d$ *is equal to the product* $\delta = \sigma\tau$ *of some monomorphisms* σ *and* τ *(as in Theorem 2.2) with* $\deg(\sigma) = n+1$ *and* $\deg(\tau) = m$ *iff* $c_d = \mu_m\lambda^m$ *and the coefficients* c_j, $m < j < d-n$, *satisfy the equations* (5) (*i.e. the coefficients* c_d *and* c_j *are uniquely determined by the elements* $c_2, \dots, c_m, \frac{c_{d-n}}{c_d}, \frac{c_{d-n+1}}{c_d}, \dots, \frac{c_{d-1}}{c_d}$).

Proof. In the proof of Theorem 2.2 we used only the equalities of the coefficients of x^j in $\delta(x) = \sigma\tau(x)$ for $j = 2, \dots, m, d-n, d-n+1, \dots, d-1$. The remaining equalities are $c_d = \mu_m\lambda^m$ for $j = d$ and (5) for j such that $m < j < d-n$. Now, the corollary is obvious. □

Proof of Theorem 1.2. We prove the theorem in two steps: first, when the algebra K contains a primitive nth root of unity, and then the general case can be reduced to the first one using Corollary 2.3.

Suppose that the algebra K contains a primitive nth root of unity, say λ. $\mathrm{Aut}_K(K[x]) \ni \gamma : x \mapsto \lambda x$, and $\omega = \omega_\gamma : \tau \mapsto \gamma\tau\gamma^{-1}$ is the inner automorphism of the group $\mathrm{Aut}_{K,c}(K[[x]])$ of *continuous* automorphisms of the series algebra $K[[x]]$. It is obvious that $\Gamma'_n = \Gamma'^{\omega} := \{\delta \in \Gamma' \mid \omega(\delta) = \delta\}$. Since

$$\sigma_1 \cdots \sigma_s = \sigma = \omega(\sigma) = \omega(\sigma_1) \cdots \omega(\sigma_s)$$

and $\deg(\sigma_1) = \deg(\omega(\sigma_1)), \dots, \deg(\sigma_s) = \deg(\omega(\sigma_s))$ we must have $\sigma_1 = \omega(\sigma_1), \dots, \sigma_s = \omega(\sigma_s)$, by Theorem 1.1, i.e. $\sigma_1, \dots, \sigma_s \in \Gamma'^{\omega} = \Gamma'_n$, as required.

In the general case, fix a commutative $\mathbb{Q}$-algebra, say L, that contains both K and a primitive nth root of unity. Then $\Gamma' \subseteq \Gamma'(L)$ and $\Gamma'_n \subseteq \Gamma'_n(L)$. By the previous case, $\sigma_1, \dots, \sigma_s \in \Gamma'_n(L)$, and, by Corollary 2.3, $\sigma_1, \dots, \sigma_s \in \Gamma'$. Therefore, $\sigma_1, \dots, \sigma_s \in \Gamma' \cap \Gamma'_n(L) = \Gamma'_n$, as required. □

Let $\mathrm{Aut}_{\mathbb{Q}}(K)$ be the group of $\mathbb{Q}$-algebra automorphisms of K. Each element $\theta \in \mathrm{Aut}_{\mathbb{Q}}(K)$ acts naturally on the polynomial algebra $K[x]$, $\theta(\sum_{i\geq 0} \lambda_i x_i) = \sum_{i\geq 0} \theta(\lambda_i)x^i$. Let $\mathrm{Aut}(\Gamma')$ be the group of automorphisms of the monoid Γ'. The map

$$\omega_{\cdot} : \mathrm{Aut}_{\mathbb{Q}}(K) \to \mathrm{Aut}(\Gamma'), \quad \theta \mapsto \omega_\theta : \sigma \mapsto \theta\sigma\theta^{-1},$$

is a group monomorphism as follows from the equality $(\theta\sigma\theta^{-1})(x) = \theta(\sigma(x))$.

COROLLARY 2.5. *Let* K *be a commutative* $\mathbb{Q}$*-algebra,* $\sigma \in \Gamma'$ *and* $\theta \in \mathrm{Aut}_{\mathbb{Q}}(K)$. *If* $\sigma = \sigma_1 \cdots \sigma_s$ *in* Γ' *and* $\omega_\theta(\sigma) = \sigma$ *then* $\omega_\theta(\sigma_1) = \sigma_1, \dots, \omega_\theta(\sigma_s) = \sigma_s$.

Proof. Since $\deg \omega_\theta(\tau) = \deg \tau$ for all $\tau \in \Gamma'$ and

$$\sigma_1 \cdots \sigma_s = \sigma = \omega_\theta(\sigma) = \omega_\theta(\sigma_1) \cdots \omega_\theta(\sigma_s)$$

we must have $\omega_\theta(\sigma_1) = \sigma_1, \dots, \omega_\theta(\sigma_s) = \sigma_s$, by Theorem 2.2. □

https://doi.org/10.1017/S0017089508004138 Published online by Cambridge University Press

3. Formulae for the components σ and τ in $\delta = \sigma\tau$. In this section, K is a commutative $\mathbb{Q}$-algebra. If a monomorphism $\delta \in \Gamma'$ is decomposable, $\delta = \sigma\tau$, then one can write formulae for the monomorphisms σ and τ via the coefficients of the polynomial $\delta(x)$ and the degree $\deg(\sigma)$ of σ (Theorem 3.2). In order to do so, we use the inversion formula [**1**] for an automorphism of a polynomial algebra $P_n := K[x_1, \dots, x_n]$.

The inversion formula. Let us recall the inversion formula (for details the reader is referred to [**1**]). For purpose of application (because we have $n-1$ elements $a_1, \dots, a_{n-1}$ in Theorem 2.2), it is convenient to state it for a polynomial algebra $P_{n-1} := K[x_1, \dots, x_{n-1}]$ in $n-1$ variables rather than n as in [**1**].

An automorphism $s \in \mathrm{Aut}_K(P_{n-1})$ is uniquely determined by the elements $x_1' := s(x_1), \dots, x_{n-1}' := s(x_{n-1})$. Let $\partial_1 := \frac{\partial}{\partial x_1}, \dots, \partial_{n-1} := \frac{\partial}{\partial x_{n-1}}$ be the partial derivatives that corresponds to the canonical generators $x_1, \dots, x_{n-1}$ of the polynomial algebra P_{n-1}. The corresponding elements, $x_1', \dots, x_{n-1}'$, partial derivatives, $\partial_1' := \frac{\partial}{\partial x_1'}, \dots, \partial_{n-1}' := \frac{\partial}{\partial x_{n-1}'}$, are given by the rule

$$\partial_i'(\cdot) := \Delta^{-1}\det\begin{pmatrix} \frac{\partial s(x_1)}{\partial x_1} & \cdots & \frac{\partial s(x_1)}{\partial x_{n-1}} \\ \vdots & \vdots & \vdots \\ \frac{\partial}{\partial x_1}(\cdot) & \cdots & \frac{\partial}{\partial x_m}(\cdot) \\ \vdots & \vdots & \vdots \\ \frac{\partial s(x_{n-1})}{\partial x_1} & \cdots & \frac{\partial s(x_{n-1})}{\partial x_{n-1}} \end{pmatrix}, \quad i = 1, \dots, n-1, \tag{6}$$

where we 'drop' $s(x_i)$ in the *Jacobian* $\Delta := \det(\frac{\partial s(x_i)}{\partial x_j}) \in P_{n-1}^*$.

For each $i = 1, \dots, n-1$, and $j \geq 0$, let

$$\phi_i' := \sum_{k\geq 0}(-1)^k \frac{x_i'^k}{k!}\partial_i'^k, \quad \phi_{i,j}' := \sum_{k=0}^{j}(-1)^k \frac{x_i'^k}{k!}\partial_i'^k : P_{n-1} \to P_{n-1}, \tag{7}$$

and

$$\phi_s := \phi_1' \cdots \phi_{n-1}' : P_{n-1} \to P_{n-1}, \quad \phi_s(P_{n-1}) = K. \tag{8}$$

THEOREM 3.1. (The Inversion Formula, [**1**]) *For each $s \in \mathrm{Aut}_K(P_{n-1})$ and $a \in P_{n-1}$,*

$$s^{-1}(a) = \sum_{\alpha\in\mathbb{N}^{n-1}} \phi_s\left(\frac{\partial'^\alpha}{\alpha!}(a)\right)x^\alpha$$

where $\phi_s(\frac{\partial'^\alpha}{\alpha!}(a)) \in K$, $x^\alpha := x_1^{\alpha_1}\cdots x_{n-1}^{\alpha_{n-1}}$ and $\partial'^\alpha := \partial_1'^{\alpha_1}\cdots\partial_{n-1}'^{\alpha_{n-1}}$.

REMARK. In [**1**], the theorem is proved for a field K of characteristic zero but the proof goes without a change for an arbitrary commutative $\mathbb{Q}$-algebra K.

The formulae for σ and τ in $\delta = \sigma\tau$. Let $\delta = \sigma\tau$ be as in Theorem 2.2. Using the inversion formula (Theorem 3.1) we obtain the formulae for the monomorphisms σ and τ (Theorem 3.2).

https://doi.org/10.1017/S0017089508004138 Published online by Cambridge University Press

Consider the automorphism $s : P_{n-1} \to P_{n-1}$ given by the expressions for the elements a_j in Theorem 2.2:

$$x'_j := s(x_j) := mx_j + \sum_{C_j} \binom{m}{\alpha_1, \ldots, \alpha_{n-1}} x_1^{\alpha_1} \cdots x_{j-1}^{\alpha_{j-1}}, \quad j = 1, \ldots, n-1.$$

Its triangular structure guarantees that s is an automorphism of P_{n-1} with the Jacobian $\Delta := \det(\frac{\partial s(x_i)}{\partial x_j}) = m^{n-1}$. Putting $a = x_j$ in Theorem 3.1 and then applying s yields

$$x_j = \sum_{\alpha \in \mathbb{N}^j} \phi_s\left(\frac{\partial'^{\alpha}}{\alpha!}(x_j)\right) x'^{\alpha} \tag{9}$$

where $x'^{\alpha} := s(x^{\alpha}) = x_1'^{\alpha_1} \cdots x_j'^{\alpha_j}$ (we used also the triangular structure of s). Each x_j is a polynomial in variables $x'_1, \ldots, x'_j$ with coefficients $\phi_s(\frac{\partial'^{\alpha}}{\alpha!}(x_j)) \in K$. Therefore, instead of the map ϕ_s in (9) one can write the map $\phi'_1 \cdots \phi'_j$, i.e.

$$x_j = \sum_{\alpha \in \mathbb{N}^j} \phi'_1 \cdots \phi'_j\left(\frac{\partial'^{\alpha}}{\alpha!}(x_j)\right) x'^{\alpha}. \tag{10}$$

The *total* degree $\deg_{x'}(x_j)$ of the polynomial x_j with respect to the variables $x'_1, \ldots, x'_{n-1}$ (or to $x'_1, \ldots, x'_j$) satisfies the inequality

$$\deg_{x'}(x_j) \leq j. \tag{11}$$

To prove this inequality we use induction on j. The case $j = 1$ is obvious since $x'_1 = mx_1$. Suppose that $j \geq 2$ and the inequality is true for all $j' < j$. Since $mx_j = x'_j - \sum_{C_j} \binom{m}{\alpha_1, \ldots, \alpha_{j-1}} x_1^{\alpha_1} \cdots x_{j-1}^{\alpha_{j-1}}$ we have

$$\deg_{x'}(x_j) \leq \sum_{k=1}^{j-1} \alpha_k \deg_{x'}(x_k) \leq \sum_{k=1}^{j-1} \alpha_k k = j,$$

see the definition of the set C_j in Theorem 2.2. By induction on j, (11) holds.

Note that by (10),

$$\deg_{x'}\left(\frac{\partial'^{\alpha}}{\alpha!}(x_j)\right) \leq \deg_{x'}(x_j) - |\alpha| \leq j - |\alpha|.$$

In a view of (11) and the triangular structure of the automorphism s, the formula for x_j, (10), can be written as follows

$$x_j = x_j(x'_1, \ldots, x'_j) = \sum_{\alpha \in \mathbb{N}^j, |\alpha| \leq j} \phi'_{1,j-|\alpha|} \cdots \phi'_{j,j-|\alpha|}\left(\frac{\partial'^{\alpha}}{\alpha!}(x_j)\right) x'^{\alpha}, \tag{12}$$

it contains only finitely many terms where $x'^{\alpha} := x_1'^{\alpha_1} \cdots x_j'^{\alpha_j}$.

THEOREM 3.2. *We keep the notation of Theorem 2.2. Then*

https://doi.org/10.1017/S0017089508004138 Published online by Cambridge University Press

1. *the coefficients* λ *and* a_j, $j = 1, \dots, n-1$, *are given by the rule*

$$a_j = x_j\left(\frac{c_{d-1}}{c_d}, \dots, \frac{c_{d-j)}}{c_d}\right) = \sum_{\alpha \in \mathbb{N}^j, |\alpha| \le j} \phi'_{1,j-|\alpha|} \cdots \phi'_{j,j-|\alpha|}\left(\frac{\partial'^{\alpha}}{\alpha!}(x_j)\right)\left(\frac{c_{d-1}}{c_d}\right)^{\alpha_1} \cdots \left(\frac{c_{d-j}}{c_d}\right)^{\alpha_j},$$

$$\lambda = m\left(\frac{c_{d-n}}{c_d} - \sum_{\alpha \in \mathbb{N}^{n-1},\ |\alpha| \le m,\ \overrightarrow{n-1}\alpha = n} \binom{m}{\alpha}\left(\frac{c_{d-1}}{c_d}\right)^{\alpha_1} \cdots \left(\frac{c_{d-(n-1)}}{c_d}\right)^{\alpha_{n-1}}\right)^{-1}.$$

2. *Then the coefficients* μ_j, $j = 2, \dots, m$, *can be written explicitly via the elements* $a_1, \dots, a_{n-1}, \lambda$ *using Cramer's formula for the unique solution of a system of linear equations.*

Proof. 1. The formula for a_j follows at once from (12) and the system of equations for the elements a_j in Theorem 2.2.(1). The formula for λ is obvious due to the last equality in Theorem 2.2.(1).

2. It is obvious. □

THEOREM 3.3. *Let* K *be a commutative* $\mathbb{Q}$*-algebra. Then the submonoid of* Γ', *say* M, *generated by the set* $\{\sigma_{\lambda x^n} : x \mapsto x + \lambda x^n \mid \lambda \in K^*, n \ge 2\}$ *is a free monoid, i.e.* $\sigma_{a_1} \cdots \sigma_{a_s} = \sigma_{b_1} \cdots \sigma_{b_t}$ *iff* $s = t$, $a_1 = b_1, \dots, a_s = b_s$.

Proof. Let $a = \lambda x^{n+1}, \lambda \in K^*, n \ge 1$. Then $\sigma_a(x) = x(1 + \lambda x^n)$ and, for each $m \ge 1$,

$$\sigma_a(x^m) = x^m(1 + \lambda x^n)^m = x^m \sum_{i=0}^{m} \binom{m}{i} \lambda^i x^{in}.$$

The polynomial $\sigma_a(x^m)$ has degree $m + mn$. It is the sum of monomials $\binom{m}{i}\lambda^i x^{m+in}$ with coefficients from K^*, the *leading* and the *pre-leading* terms are $l := \lambda^m x^{m+mn}$ and $p := m\lambda^{m-1}x^{m+(m-1)n}$ respectively. Note that $\deg \sigma_a(x) < \deg \sigma_a(x^2) < \cdots < \deg \sigma_a(x^i) < \cdots$ and

$$\deg \sigma_a(x^{m-1}) = m - 1 + (m-1)n < m + (m-1)n = \deg p.$$

Therefore, for any polynomial, say $f = \mu x^m + \cdots$, of degree m with the leading coefficient $\mu \in K^*$, $\sigma_a(f) = L + P + \cdots$ where $L := \mu l$ and $P := \mu p$ are the leading and the pre-leading terms of the polynomial $\sigma_a(f)$ and the three dots mean smaller terms. Note that $\frac{L}{P} = \frac{\lambda}{m}x^n$, hence

$$n = \deg\left(\frac{L}{P}\right), \quad m = \frac{\deg \sigma_a(f)}{n+1}, \quad \lambda = mx^{-n}\frac{L}{P}. \tag{13}$$

Let $\sigma = \sigma_{a_1} \cdots \sigma_{a_s}$. By induction on s, it is easy to prove that the coefficients of the leading and the pre-leading term of the element $\sigma(x)$ are units of K. By (13), the element a_1 is uniquely determined by the leading and the pre-leading terms of the polynomial $\sigma(x)$. Since $\sigma = \sigma_{b_1} \cdots \sigma_{b_t}$, we must have $a_1 = b_1$. Then $\sigma_{a_1} = \sigma_{b_1}$ and then $\sigma_{a_2} \cdots \sigma_{a_s} = \sigma_{b_2} \cdots \sigma_{b_t}$. Repeating the same argument we see that the equality $\sigma_{a_1} \cdots \sigma_{a_s} = \sigma_{b_1} \cdots \sigma_{b_t}$ holds iff $s = t$, $a_1 = b_1, \dots, a_s = b_s$. □

https://doi.org/10.1017/S0017089508004138 Published online by Cambridge University Press

4. Necessary conditions for irreducibility of a polynomial. In this section, necessary conditions for irreducibility of a polynomial are given (Corollary 4.2). These conditions are far from being sufficient. Their advantage is that they are explicit and if they do not hold then one can find explicitly (using Theorem 3.2) a nontrivial divisor of the polynomial (i.e. a formula for certain divisors is given explicitly).

Let K be a commutative $\mathbb{Q}$-algebra. Let $\mathcal{P}$ be the set of all the polynomials of the type $p = 1 + \lambda_1 x + \cdots + \lambda_t x^t$ where $\lambda_i \in K$, $\lambda_t \in K^*$, and $\mathcal{Q}$ be the set of all the unitary polynomials, i.e. of the type $q = x + \mu_2 x^2 + \cdots + \mu_s x^s$ where $\mu_i \in K$ and $\mu_s \in K^*$. The derivation $(\cdot)' := \frac{d}{dx} : \mathcal{Q} \to \mathcal{P}$, $q \mapsto q'$, is a *bijection* with the inverse

$$\int : \mathcal{P} \to \mathcal{Q}, \quad 1 + \sum_{i \geq 1} \lambda_i x_i \mapsto x + \sum_{i \geq 1} \frac{\lambda_i}{i+1} x^{i+1}.$$

A polynomial $p \in \mathcal{P}$ is called *reducible* if $p = qr$ for some polynomial $q, r \in \mathcal{P}$ each of degree ≥ 1. A polynomial $p \in \mathcal{P}$ of degree $d - 1 \geq 1$ can be written uniquely in the form $p = 1 + \sum_{i=2}^{d} c_i i x^{i-1}$. Then its integral $\int p := x + c_2 x^2 + \cdots + c_d x^d$ determines the monomorphism $\Gamma' \ni \delta_p : x \mapsto \delta_p(x) = \int p$. We say that a polynomial $p \in \mathcal{P}$ is *decomposable* if the monomorphism δ_p is *decomposable*, i.e. $\delta_p = \sigma\tau$ for some monomorphisms $\sigma, \tau \in \Gamma' \backslash \{e\}$. It is obvious that each polynomial of degree $d - 1$ where d is a prime number is indecomposable (i.e. not decomposable) since $\deg \delta_p(x) = d$ (see (1)).

Let $f(x) := \sigma(x)$ and $g(x) := \tau(x)$ where $\sigma, \tau \in \Gamma' \backslash \{e\}$. The polynomials f and g are *unitary* and have degree ≥ 2. Therefore, their derivatives f' and g' belong to $\mathcal{P}$ and have degree ≥ 1. By the chain rule,

$$p := \delta(x)' = (f(g(x)))' = f'(g(x)) \cdot g'. \tag{14}$$

LEMMA 4.1.

1. *A polynomial $p \in \mathcal{P}$ is decomposable iff $p = f'(g)g'$ for some polynomials $f, g \in \mathcal{Q}$ of degree ≥ 2.*
2. *Each decomposable polynomial is reducible.*

Proof. Both statements follow at once from (14). □

REMARK. If the polynomial $p \in \mathcal{P}$ is decomposable then using Theorem 3.2 one can find explicitly all the pairs $(f'(g), g')$ of the divisors of p as in Lemma 4.1, i.e. $p = f'(g)g'$.

The next corollary gives necessary conditions for a polynomial being irreducible.

COROLLARY 4.2. *Let K be a commutative $\mathbb{Q}$-algebra. If a polynomial $p = 1 + \sum_{i=2}^{d} c_i i x^{i-1}$, $c_i \in K$, $c_d \in K^*$, is irreducible then for the polynomial $\delta(x) := \int p = x + c_2 x^2 + \cdots + c_d x^d$ the conditions of Corollary 2.4 do not hold for each pair (m, n) such that $m \geq 2$, $n \geq 1$, $d = m(n+1)$.*

Proof. This follows directly from Lemma 4.1 and Corollary 2.4. □

ACKNOWLEDGEMENTS. The author would like to thank the referee of this paper for the comments and for pointing out the papers [**2**]–[**4**].

REFERENCES

1. V. V. Bavula, The inversion formula for automorphisms of the Weyl algebras and polynomial algebras, *J. Pure Appl. Algebra* **210** (2007), 147–159. arXiv:math.RA/0512215.

2. H. T. Engstrom, Polynomial substitutions, *Amer. J. Math.* **63** (1941), 249–255.

3. H. Levi, Composite polynomials with coefficients in an arbitary field of characteristic zero, *Amer. J. Math.* **64** (1942), 389–400.

4. J. F. Ritt, Prime and composite polynomials, *Trans. Amer. Math. Soc.* **23** (1922), 51–66.