

A FACTORIZATION THEORY FOR SOME FREE FIELDS

Konrad Schrempf

Received: 10 April 2019; Revised: 23 November 2019; Accepted: 19 December 2019

Communicated by Abdullah Harmancı

ABSTRACT. Although in general there is no meaningful concept of factorization in fields, that in free associative algebras (over a *commutative* field) can be extended to their respective free field (universal field of fractions) on the level of *minimal linear representations*. We establish a factorization theory by providing an alternative definition of left (and right) divisibility based on the *rank* of an element and show that it coincides with the “classical” left (and right) divisibility for non-commutative polynomials. Additionally we present an approach to factorize elements, in particular *rational formal power series*, into their (generalized) atoms. The problem is reduced to solving a system of polynomial equations with *commuting* unknowns.

Mathematics Subject Classification (2020): 16K40, 16Z05, 16G99, 16S10

Keywords: Free associative algebra, factorization of non-commutative polynomials, minimal linear representation, universal field of fractions, admissible linear system, non-commutative formal power series

1. Introduction

From an algebraic point of view fields are usually not very interesting (with respect to factorization) due to the lack of “structure”, for example, they do not have *non-zero non-units*. However here, the field—the *universal field of fractions* (“free field”) of the *free associative algebra* (over a *commutative* ground field)—is *non-commutative* and *infinite dimensional* over its center (at least if we exclude the one-variable case). A brief introduction can be found in [7, Section 9.3], for details we refer to [8, Chapter 7], where also historical information is provided: “Until 1970 the only purely algebraic methods of embedding rings in fields were based on Ore’s method [16].”

The main idea is to view all elements in terms of their *normal form* (minimal linear representation) [9]. Given an element, the dimension of a *minimal* linear representation defines its *rank* [10], for example, the rank of a word/monomial of length n is $n + 1$. Since multiplication (of two elements) can be formulated in terms of linear representations, we establish a concept to “reverse” this step, that

is, given an element (by a *minimal* linear representation) to find left (and right) divisors subject to conditions on the ranks of the involved elements.

In [22] we showed that in the *free associative algebra* there is a rather natural correspondence between a factorization of an element and (upper right) blocks of zeros in (a special form of) its minimal linear representations. One does not have to take care about the ranks. In general a *minimal* multiplication, that is, a multiplication on the level of *minimal* linear representations is much more subtle. Now, *how* do we have to define divisibility in terms of the rank such that it is equivalent to that in the free associative algebra?

Joining factorization theory in the non-commutative setting —for an overview see [23]— and the theory of embedding “non-commutative” rings into a (skew) field —to be more precise: embedding *free ideal rings* (firs) into their respective universal field of fractions, see [8, Chapter 2]— even for the “simplest” case of the *free associative algebra* results in a very rich structure, maybe not only for a “free factorization theory”. Somewhat paradoxical is the fact that the *inverse* plays a crucial role. Since *each* non-zero element (in the free field) is invertible, we can use both, its rank and that of its inverse, for example, the inverse of a polynomial of rank $n \geq 2$ has rank $n - 1$. A corollary to the *minimal* inverse (Theorem 3.20) is used to identify *trivial* units, that is, units from the (commutative) ground field. We do not even have to exclude the (commutative) one-variable case.

Factorization (of rational functions) in the latter (on the level of *realizations*) is well established in control theory [2]. Factorization in the non-commutative setting is discussed in [15] and [13].

After fixing the basic notation and stating the basic definitions in Section 2, we develop the main (technical) tools in Section 3. In a first reading only Proposition 3.1 (rational operations) and Theorem 3.20 (minimal inverse) are important. The main part is Section 4 where the factorization theory is developed, starting with Definition 4.1 and culminating (but not ending) in Theorem 4.11. Finally, in Section 5, minimal multiplication (Theorem 5.2) and factorization (Theorem 5.9) is discussed.

Remark 1.1. This exposition is not meant to serve as an introduction, neither to free fields nor to non-commutative factorization (in free associative algebras). Instead, depending on the background, the example in [22, Section 4], the connection to formal power series [21, Section 3] or the polynomial factorization [22, Section 2] might be helpful. One way to get acquainted with free fields is to use them (“almost” like the rational numbers) and explore the rich theory in parallel. The step

from inverting a non-zero number, say in $s = \frac{v}{a}$ or $as = v$ with *unique* solution s , to inverting “full” matrices (Definition 2.3) is non-trivial but similar: $As = v$ with *unique* solution *vector* s (we are usually interested in its first component s_1).

2. Preliminaries

We represent elements (in free fields) by *admissible linear systems* (Definition 2.11), which are just a special form of *linear representations* (Definition 2.5) and “general” *admissible systems* [8, Section 7.1]. Rational operations (scalar multiplication, addition, multiplication, inverse) can be easily formulated in terms of linear representations (Proposition 3.1).

Notation 2.1. The set of the natural numbers is denoted by $\mathbb{N} = \{1, 2, \dots\}$, that including zero by \mathbb{N}_0 . Zero entries in matrices are usually replaced by (lower) dots to emphasize the structure of the non-zero entries unless they result from transformations where there were possibly non-zero entries before. We denote by I_n the identity matrix and Σ_n the permutation matrix that reverses the order of rows/columns (of size n) respectively I and Σ if the size is clear from the context. The transpose of a vector v is denoted by v^\top , the unit (column) vector with a one at position n (and size depending on the context) by $e_n = \underbrace{[0, \dots, 0, 1, 0, \dots, 0]^\top}_{n-1}$.

Let \mathbb{K} be a *commutative* field, $\overline{\mathbb{K}}$ its algebraic closure and $X = \{x_1, x_2, \dots, x_d\}$ be a *finite* (non-empty) alphabet. $\mathbb{K}\langle X \rangle$ denotes the *free associative algebra* (or *free \mathbb{K} -algebra*) and $\mathbb{F} = \mathbb{K}\langle\langle X \rangle\rangle$ its *universal field of fractions* (or “free field”) [5], [10]. An element in $\mathbb{K}\langle X \rangle$ is called (non-commutative or nc) *polynomial*. In our examples the alphabet is usually $X = \{x, y, z\}$. Including the algebra of *nc rational series* we have the following chain of inclusions:

$$\mathbb{K} \subsetneq \mathbb{K}\langle X \rangle \subsetneq \mathbb{K}^{\text{rat}}\langle\langle X \rangle\rangle \subsetneq \mathbb{K}\langle\langle X \rangle\rangle =: \mathbb{F}.$$

The *free monoid* X^* generated by X is the set of all *finite words* $x_{i_1}x_{i_2}\cdots x_{i_n}$ with $i_k \in \{1, 2, \dots, d\}$. An element of the alphabet is called *letter*, one of the free monoid *word*. The multiplication on X^* is the *concatenation* of words, that is, $(x_{i_1}\cdots x_{i_m}) \cdot (x_{j_1}\cdots x_{j_n}) = x_{i_1}\cdots x_{i_m}x_{j_1}\cdots x_{j_n}$, with neutral element 1, the *empty word*. The *length* of a word $w = x_{i_1}x_{i_2}\cdots x_{i_m}$ is m , denoted by $|w| = m$ or $\ell(w) = m$. For detailed introductions see [3, Chapter 1] or [19, Section I.1].

Remark 2.2. For an overview about the many connections to formal language theory, automata, nc rational series and recognizability we recommend [17]. *Recognizable* series are defined via “regular” *linear representations* [3], a special case of those introduced later in Definition 2.5. A summary is available in [21, Section 3].

Definition 2.3 (Inner Rank, Full Matrix [8, Section 0.1], [10]). Given a matrix $A \in \mathbb{K}\langle X \rangle^{n \times n}$, the *inner rank* of A is the smallest number $m \in \mathbb{N}$ such that there exists a factorization $A = TU$ with $T \in \mathbb{K}\langle X \rangle^{n \times m}$ and $U \in \mathbb{K}\langle X \rangle^{m \times n}$. The matrix A is called *full* if $m = n$, *non-full* otherwise.

Remark 2.4. Every full matrix (over the free associative algebra) is invertible over the free field [8, Corollary 7.5.14].

Definition 2.5 (Linear Representations, Dimension, Rank [9,10]). Let $f \in \mathbb{F}$. A *linear representation* of f is a triple $\pi_f = (u, A, v)$ with $u \in \mathbb{K}^{1 \times n}$, full $A = A_0 \otimes 1 + A_1 \otimes x_1 + \dots + A_d \otimes x_d$, that is, A is invertible over \mathbb{F} , $A_\ell \in \mathbb{K}^{n \times n}$, $v \in \mathbb{K}^{n \times 1}$ and $f = uA^{-1}v$. The *dimension* of π_f is $\dim(u, A, v) = n$. It is called *minimal* if A has the smallest possible dimension among all linear representations of f . The “empty” representation $\pi = (., .)$ is the minimal one of $0 \in \mathbb{F}$ with $\dim \pi = 0$. Let $f \in \mathbb{F}$ and π be a *minimal* linear representation of f . Then the *rank* of f is defined as $\text{rank } f = \dim \pi$.

Remark 2.6. Cohn and Reutenauer define linear representations slightly more general, namely $f = c + uA^{-1}v$ with possibly non-zero $c \in \mathbb{K}$ and call it *pure* when $c = 0$. Two linear representations are called *equivalent* if they represent the same element [10]. Two (pure) linear representations (u, A, v) and $(\tilde{u}, \tilde{A}, \tilde{v})$ of dimension n are called *isomorphic* if there exist invertible matrices $P, Q \in \mathbb{K}^{n \times n}$ such that $u = \tilde{u}Q$, $A = P\tilde{A}Q$ and $v = P\tilde{v}$ [10].

Theorem 2.7 ([10, Theorem 1.4]). *If $\pi' = (u', A', v')$ and $\pi'' = (u'', A'', v'')$ are equivalent (pure) linear representations, of which the first is minimal, then the second is isomorphic to a representation $\pi = (u, A, v)$ which has the block decomposition*

$$u = \begin{bmatrix} . & u' & * \end{bmatrix}, \quad A = \begin{bmatrix} * & * & * \\ . & A' & * \\ . & . & * \end{bmatrix} \quad \text{and} \quad v = \begin{bmatrix} * \\ v' \\ . \end{bmatrix}.$$

Definition 2.8 (Left and Right Families [9]). Let $\pi = (u, A, v)$ be a linear representation of $f \in \mathbb{F}$ of dimension n . The families $(s_1, s_2, \dots, s_n) \subseteq \mathbb{F}$ with $s_i = (A^{-1}v)_i$ and $(t_1, t_2, \dots, t_n) \subseteq \mathbb{F}$ with $t_j = (uA^{-1})_j$ are called *left family* and *right family*

respectively. $L(\pi) = \text{span}\{s_1, s_2, \dots, s_n\}$ and $R(\pi) = \text{span}\{t_1, t_2, \dots, t_n\}$ denote their linear spans (over \mathbb{K}).

Proposition 2.9 ([9, Proposition 4.7]). *A representation $\pi = (u, A, v)$ of an element $f \in \mathbb{F}$ is minimal if and only if both, the left family and the right family are \mathbb{K} -linearly independent. In this case, $L(\pi)$ and $R(\pi)$ depend only on f .*

Definition 2.10 (Element Types). An element $f \in \mathbb{F}$ is called of *type* $(1, *)$ (respectively $(0, *)$) if $1 \in R(f)$, that is, $1 \in R(\pi)$ for some *minimal* linear representation π of f , (respectively $1 \notin R(f)$). It is called of *type* $(*, 1)$ (respectively $(*, 0)$) if $1 \in L(f)$ (respectively $1 \notin L(f)$). Both subtypes can be combined.

Definition 2.11 (Admissible Linear Systems, Admissible Transformations [21]). A linear representation $\mathcal{A} = (u, A, v)$ of $f \in \mathbb{F}$ is called *admissible linear system* (ALS) for f , written also as $As = v$, if $u = e_1 = [1, 0, \dots, 0]$. The element f is then the first component of the (unique) solution vector s . Given a linear representation $\mathcal{A} = (u, A, v)$ of dimension n of $f \in \mathbb{F}$ and invertible matrices $P, Q \in \mathbb{K}^{n \times n}$, the transformed $PAQ = (uQ, PAQ, Pv)$ is again a linear representation (of f). If \mathcal{A} is an ALS, the transformation (P, Q) is called *admissible* if the first row of Q is $e_1 = [1, 0, \dots, 0]$.

Remark 2.12. The left family $(A^{-1}v)_i$ (respectively the right family $(uA^{-1})_j$) and the solution vector s of $As = v$ (respectively t of $u = tA$) are used synonymously.

Transformations can be done by elementary row- and column operations, explained in detail in [21, Remark 1.12]. For further remarks and connections to the related concepts of linearization and realization see [21, Section 1].

For elements in the free associative algebra $\mathbb{K}\langle X \rangle$ a special form (with an upper unitriangular system matrix) can be used. It plays a crucial role in the factorization of polynomials because it allows to formulate a minimal polynomial multiplication (Proposition 3.19) and *upper unitriangular* transformation matrices (invertible by definition) suffice to find all possible factors (up to trivial units). For details we refer to [22, Section 2].

Remark 2.13. The following definition is slightly adapted to avoid confusion with other transformation matrices for the factorization, formulated *independent* of a given admissible linear system.

Definition 2.14 (Polynomial ALS and Transformation [22, Definition 24]). An ALS $\mathcal{A} = (u, A, v)$ of dimension n with system matrix $A = (a_{ij})$ for a non-zero polynomial $0 \neq p \in \mathbb{K}\langle X \rangle$ is called *polynomial*, if

- (1) $v = [0, \dots, 0, \lambda]^\top$ for some $\lambda \in \mathbb{K}$ and
- (2) $a_{ii} = 1$ for $i = 1, 2, \dots, n$ and $a_{ij} = 0$ for $i > j$, that is, A is upper triangular.

A polynomial ALS is also written as $\mathcal{A} = (1, A, \lambda)$ with $1, \lambda \in \mathbb{K}$. An admissible transformation (P, Q) for an ALS \mathcal{A} is called *polynomial* if it has the form

$$(P, Q) = \left(\begin{bmatrix} 1 & \alpha_{1,2} & \dots & \alpha_{1,n-1} & \alpha_{1,n} \\ & \ddots & \ddots & \vdots & \vdots \\ & & 1 & \alpha_{n-2,n-1} & \alpha_{n-2,n} \\ & & & 1 & \alpha_{n-1,n} \\ & & & & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ & 1 & \beta_{2,3} & \dots & \beta_{2,n} \\ & & 1 & \ddots & \vdots \\ & & & \ddots & \beta_{n-1,n} \\ & & & & 1 \end{bmatrix} \right).$$

If additionally $\alpha_{1,n} = \alpha_{2,n} = \dots = \alpha_{n-1,n} = 0$ then (P, Q) is called *polynomial factorization transformation*.

Definition 2.15 (Similar Right Ideals, Similar Elements [8, Section 3.1]). Let R be a ring. Two right ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$ are called *similar*, written as $\mathfrak{a} \sim \mathfrak{b}$, if $R/\mathfrak{a} \cong R/\mathfrak{b}$ as right R -modules. Two elements $p, q \in R$ are called *similar* if their right ideals pR and qR are similar, that is, $pR \sim qR$. See also [23, Section 4.1].

Definition 2.16 (Left and Right Coprime Elements [1, Section 2]). Let R be a domain and $H = R^\bullet = R \setminus \{0\}$. An element p *left divides* q , written as $p \mid_l q$, if $q \in pH = \{ph \mid h \in H\}$. Two elements p, q are called *left coprime* if for all h such that $h \mid_l p$ and $h \mid_l q$ implies $h \in H^\times = \{f \in H \mid f \text{ is invertible}\}$, that is, h is an element of the *group of units*. Right division $p \mid_r q$ and the notion of *right coprime* is defined in a similar way. Two elements are called *coprime* if they are left and right coprime.

Definition 2.17 (Atomic Domains [1, Section 2]). Let R be a domain and $H = R^\bullet$. An element $p \in H \setminus H^\times$, that is, a non-zero non-unit (in R), is called an *atom* (or *irreducible*) if $p = q_1 q_2$ with $q_1, q_2 \in H$ implies that either $q_1 \in H^\times$ or $q_2 \in H^\times$. The set of atoms in R is denoted by $\mathbf{A}(R)$. The (cancellative) monoid H is called *atomic* if every non-unit can be written as a finite product of atoms of H . The domain R is called *atomic* if the monoid R^\bullet is atomic.

Definition 2.18 (Similarity Unique Factorization Domains [23]). A domain R is called *similarity factorial* (or a *similarity-UFD*) if R is atomic and it satisfies the property that if $p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$ for atoms (irreducible elements) $p_i, q_j \in R$, then $m = n$ and there exists a permutation $\sigma \in \mathfrak{S}_m$ such that p_i is similar to $q_{\sigma(i)}$ for all $i \in 1, 2, \dots, m$.

Proposition 2.19 ([4, Theorem 6.3]). *The free associative algebra $R = \mathbb{K}\langle X \rangle$ is a similarity (unique) factorization domain.*

3. Rational operations

Usually we want to construct *minimal* admissible linear systems (out of minimal ones), that is, perform “minimal” rational operations. Minimal scalar multiplication is trivial. In some special cases *minimal addition* can be formulated (Proposition 3.5). For *minimal multiplication* we refer to Section 5. For the *minimal inverse* we have to distinguish four cases, which are summarized in Theorem 3.20. In general however, it is necessary to *minimize* a given system. For a *polynomial* ALS this is discussed in [22, Section 2.2], for the general case we refer to [20].

Proposition 3.1 (Rational Operations [10]). *Let $0 \neq f, g \in \mathbb{F}$ be given by the admissible linear systems $\mathcal{A}_f = (u_f, A_f, v_f)$ and $\mathcal{A}_g = (u_g, A_g, v_g)$ respectively and let $0 \neq \mu \in \mathbb{K}$. Then admissible linear systems for the rational operations can be obtained as follows:*

The scalar multiplication μf is given by

$$\mu \mathcal{A}_f = (u_f, A_f, \mu v_f).$$

The sum $f + g$ is given by

$$\mathcal{A}_f + \mathcal{A}_g = \left(\begin{bmatrix} u_f & \cdot \end{bmatrix}, \begin{bmatrix} A_f & -A_f u_f^\top u_g \\ \cdot & A_g \end{bmatrix}, \begin{bmatrix} v_f \\ v_g \end{bmatrix} \right).$$

The product fg is given by

$$\mathcal{A}_f \cdot \mathcal{A}_g = \left(\begin{bmatrix} u_f & \cdot \end{bmatrix}, \begin{bmatrix} A_f & -v_f u_g \\ \cdot & A_g \end{bmatrix}, \begin{bmatrix} \cdot \\ v_g \end{bmatrix} \right).$$

And the inverse f^{-1} is given by

$$\mathcal{A}_f^{-1} = \left(\begin{bmatrix} 1 & \cdot \end{bmatrix}, \begin{bmatrix} -v_f & A_f \\ \cdot & u_f \end{bmatrix}, \begin{bmatrix} \cdot \\ 1 \end{bmatrix} \right).$$

Definition 3.2 (Disjoint Elements [10]). Two elements $f, g \in \mathbb{F}$ are called *disjoint* if $\text{rank}(f + g) = \text{rank}(f) + \text{rank}(g)$.

Remark 3.3. Two polynomials are never disjoint. This can be easily seen in the construction (of an ALS) for the sum (of the polynomials). See also [10, Theorem 2.3].

For disjoint elements the formulation of a minimal addition (Proposition 3.5) is immediate. Testing if two elements are disjoint in \mathbb{F} is difficult because it relies on techniques for minimizing linear representations [20]. However, since minimality of a linear representation is equivalent to \mathbb{K} -linear independence of its left and right family respectively (Proposition 2.9), two elements f, g are disjoint if $L(f) \cap L(g) = \{0\}$ and $R(f) \cap R(g) = \{0\}$.

Example 3.4. For $f = x + ((1-x)^{-1} + x^{-1})$ a *minimal* ALS —constructed by Proposition 3.5— is

$$\begin{bmatrix} 1 & -x & -1 & \cdot \\ \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & 1-x & x+1 \\ \cdot & \cdot & \cdot & x \end{bmatrix} s = \begin{bmatrix} \cdot \\ 1 \\ 1 \\ 1 \end{bmatrix}, \quad s = \begin{bmatrix} f \\ 1 \\ (1+x)^{-1} + x^{-1} \\ x^{-1} \end{bmatrix}.$$

Proposition 3.5 (Minimal Disjoint Addition). *Let $f, g \in \mathbb{F}$ be disjoint and given by the minimal admissible linear systems $\mathcal{A}_f = (u_f, A_f, v_f)$ and $\mathcal{A}_g = (u_g, A_g, v_g)$ of dimension n_f and n_g respectively. Then the system*

$$\mathcal{A}_f + \mathcal{A}_g = \left(\begin{bmatrix} u_f & \cdot \end{bmatrix}, \begin{bmatrix} A_f & -A_f u_f^T u_g \\ \cdot & A_g \end{bmatrix}, \begin{bmatrix} v_f \\ v_g \end{bmatrix} \right)$$

of dimension $n_f + n_g$ (from Proposition 3.1) for $f + g$ is minimal.

Like in the polynomial case, factorization and *minimal* multiplication are tight together as opposite points of view. Further assumptions that guarantee minimality are developed in Section 4. They eventually enter in Theorem 5.2. We will need alternative constructions (to that in Proposition 3.1) for the product several times, so we state them already here in Propositions 3.11 and 3.12. These constructions are used in particular in Theorem 5.2. Before, we need some technical results from [21] and [22]. However these are rearranged such that similarities become more obvious and the flexibility in applications is increased. In particular we prove Lemma 3.8 by applying Lemma 3.6.

Lemma 3.6 ([22, Lemma 25]). *Let $\mathcal{A} = (u, A, v)$ be an ALS of dimension $n \geq 1$ with \mathbb{K} -linearly independent left family $s = A^{-1}v$ and $B = B_0 \otimes 1 + B_1 \otimes x_1 + \dots + B_d \otimes x_d$ with $B_\ell \in \mathbb{K}^{m \times n}$, such that $Bs = 0$. Then there exists a (unique) $T \in \mathbb{K}^{m \times n}$ such that $B = TA$.*

Lemma 3.7. *Let $\mathcal{A} = (u, A, v)$ be an ALS of dimension $n \geq 1$ with \mathbb{K} -linearly independent right family $t = uA^{-1}$ and $B = B_0 \otimes 1 + B_1 \otimes x_1 + \dots + B_d \otimes x_d$ with*

$B_\ell \in \mathbb{K}^{n \times m}$, such that $tB = 0$. Then there exists a (unique) $U \in \mathbb{K}^{n \times m}$ such that $B = AU$.

Lemma 3.8 (for Type $(0, 1)$ [21, Lemma 4.11]). *Let $\mathcal{A} = (u, A, v)$ be a minimal ALS with $\dim \mathcal{A} = n \geq 2$ and $1 \in L(\mathcal{A})$. Then there exists an admissible transformation (P, Q) such that the last row of PAQ is $[0, \dots, 0, 1]$ and $Pv = [0, \dots, 0, \lambda]^\top$ for some $\lambda \in \mathbb{K}$.*

Proof. Without loss of generality, assume that $v = [0, \dots, 0, 1]^\top$ and the left family $s = A^{-1}v$ is $(s_1, s_2, \dots, s_{n-1}, 1)$. Otherwise it can be brought to this form by some admissible transformation (P°, Q°) . Now let \bar{A} denote the upper left $(n-1) \times (n-1)$ block of A , let $\bar{s} = (s_1, \dots, s_{n-1})$ and write $As = v$ as

$$\begin{bmatrix} \bar{A} & b \\ c & d \end{bmatrix} \begin{bmatrix} \bar{s} \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Now let $B = [c, d - 1]$ and apply Lemma 3.6 to get the matrix $T = [\bar{T}, \tau] \in \mathbb{K}^{1 \times n}$ such that $B = TA$. Thus we get the transformation

$$(P, Q) = \left(\begin{bmatrix} I_{n-1} & \cdot \\ -\bar{T} & -\tau \end{bmatrix} P^\circ, Q^\circ \right). \quad \square$$

Lemma 3.9 (for Type $(1, 0)$ [21, Lemma 4.12]). *Let $\mathcal{A} = (u, A, v)$ be a minimal ALS with $\dim \mathcal{A} = n \geq 2$ and $1 \in R(\mathcal{A})$. Then there exists an admissible transformation (P, Q) such that the first column of PAQ is $[1, 0, \dots, 0]^\top$ and $Pv = [0, \dots, 0, \lambda]^\top$ for some $\lambda \in \mathbb{K}$.*

Remark 3.10. If g is of type $(*, 1)$ then, by Lemma 3.8, each minimal ALS for g can be transformed into one with a last row of the form $[0, \dots, 0, 1]$. If g is of type $(1, *)$ then, by Lemma 3.9, each minimal ALS for g can be transformed into one with a first column of the form $[1, 0, \dots, 0]^\top$. This can be done by *linear* techniques, see the remark before [21, Theorem 4.13].

Since $p \in \mathbb{K}\langle X \rangle$ is of type $(1, 1)$, both constructions can be used for the minimal polynomial multiplication (Proposition 3.19). One could call the multiplication from Proposition 3.1 type $(*, *)$. A *necessary* condition for minimality however is, that the left factor is of type $(*, 0)$ and the right factor is of type $(0, *)$, thus we will use this construction later as type $(0, 0)$. Section 4 is dedicated to a *sufficient* condition. See also Figure 2, page 33.

Proposition 3.11 (Multiplication Type $(1, *)$). *Let $f, g \in \mathbb{F} \setminus \mathbb{K}$ be given by the admissible linear systems $\mathcal{A}_f = (u_f, A_f, v_f) = (1, A_f, \lambda_f)$ of dimension n_f of the*

form

$$\mathcal{A}_f = \left(\left[\begin{array}{ccc} 1 & . & . \end{array} \right], \left[\begin{array}{ccc} a & b' & b \\ a' & B & b'' \\ . & . & 1 \end{array} \right], \left[\begin{array}{c} . \\ . \\ \lambda_f \end{array} \right] \right) \quad (1)$$

and $\mathcal{A}_g = (u_g, A_g, v_g) = (1, A_g, \lambda_g)$ of dimension n_g respectively. Then an ALS for fg of dimension $n = n_f + n_g - 1$ is given by

$$\mathcal{A} = \left(\left[\begin{array}{ccc} 1 & . & . \end{array} \right], \left[\begin{array}{ccc} a & b' & \lambda_f b u_g \\ a' & B & \lambda_f b'' u_g \\ . & . & A_g \end{array} \right], \left[\begin{array}{c} . \\ . \\ v_g \end{array} \right] \right). \quad (2)$$

Proof. Construct the ALS $\mathcal{A}' = (u', A', v')$ of dimension $n_f + n_g$ for the product fg using Proposition 3.1. Add λ_f -times column n_f to column $(n_f + 1)$ (in the system matrix A'). Remove column n_f from A' and v' and row n_f from A' and u' to get the ALS (2) of dimension $n_f + n_g - 1$. \square

Proposition 3.12 (Multiplication Type $(*, 1)$). *Let $f, g \in \mathbb{F} \setminus \mathbb{K}$ be given by the admissible linear systems $\mathcal{A}_f = (u_f, A_f, v_f) = (1, A_f, \lambda_f)$ of dimension n_f and $\mathcal{A}_g = (u_g, A_g, v_g) = (1, A_g, \lambda_g)$ of dimension n_g of the form*

$$\mathcal{A}_g = \left(\left[\begin{array}{ccc} 1 & . & . \end{array} \right], \left[\begin{array}{ccc} 1 & b' & b \\ . & B & b'' \\ . & c' & c \end{array} \right], \left[\begin{array}{c} . \\ . \\ \lambda_g \end{array} \right] \right) \quad (3)$$

respectively. Then an ALS for fg of dimension $n = n_f + n_g - 1$ is given by

$$\mathcal{A} = \left(\left[\begin{array}{ccc} u_f & . & . \end{array} \right], \left[\begin{array}{ccc} A_f & e_{n_f} \lambda_f b' & e_{n_f} \lambda_f b \\ . & B & b'' \\ . & c' & c \end{array} \right], \left[\begin{array}{c} . \\ . \\ \lambda_g \end{array} \right] \right). \quad (4)$$

Proof. Construct the ALS $\mathcal{A}' = (u', A', v')$ of dimension $n_f + n_g$ for the product fg using Proposition 3.1. Add λ_f -times row $(n_f + 1)$ to row n_f (in the system matrix A'). Remove row $(n_f + 1)$ from A' and v' and column $(n_f + 1)$ from A' and u' to get the ALS (4) of dimension $n_f + n_g - 1$. \square

Remark 3.13. Recall that, if f (respectively g) is given by a *minimal* ALS, it can be transformed appropriately by Lemma 3.8 (respectively Lemma 3.9) into the form (1) (respectively (3)).

Lemma 3.15 is a slightly more general version of [22, Lemma 27]. The proof of (the following) Proposition 3.19 becomes simple by the help of the two lemmas 3.16 and 3.18 which are extracted of the original proof (of the minimal polynomial multiplication). They are useful later, especially in Lemma 4.9.

Remark 3.14. Note that the transformation in the following lemma is *not* necessarily admissible. However, except for $n = 2$ (which can be treated by permuting the last two elements in the left family), it can be chosen such that it is *admissible*.

Lemma 3.15. *Let $\mathcal{A} = (u, A, v)$ be an ALS of dimension $n \geq 2$ with $v = [0, \dots, 0, \lambda]^\top$ and \mathbb{K} -linearly dependent left family $s = A^{-1}v$. Let $m \in \{2, 3, \dots, n\}$ be the minimal index such that the left subfamily $\underline{s} = (A^{-1}v)_{i=m}^n$ is \mathbb{K} -linearly independent. Let $A = (a_{ij})$ and assume that $a_{ii} = 1$ for $1 \leq i \leq m$ and $a_{ij} = 0$ for $j < i \leq m$ (upper triangular $m \times m$ block) and $a_{ij} = 0$ for $j \leq m < i$ (lower left zero block of size $(n - m) \times m$). Then there exists matrices $T, U \in \mathbb{K}^{1 \times (n+1-m)}$ such that*

$$U + (a_{m-1,j})_{j=m}^n - T(a_{ij})_{i,j=m}^n = \begin{bmatrix} 0 & \dots & 0 \end{bmatrix} \quad \text{and} \quad T(v_i)_{i=m}^n = 0.$$

Proof. By assumption, the left subfamily $(s_{m-1}, s_m, \dots, s_n)$ is \mathbb{K} -linearly dependent. Thus there are $\kappa_m, \dots, \kappa_n \in \mathbb{K}$ such that $s_{m-1} = \kappa_m s_m + \kappa_{m+1} s_{m+1} + \dots + \kappa_n s_n$. Let $U = [\kappa_m, \kappa_{m+1}, \dots, \kappa_n]$. Then $s_{m-1} - U \underline{s} = 0$. By assumption $v_{m-1} = 0$. Now we can apply Lemma 3.6 with $B = U + [a_{m-1,m}, a_{m-1,m+1}, \dots, a_{m-1,n}]$ (and \underline{s}). Hence, there exists a matrix $T \in \mathbb{K}^{1 \times (n+1-m)}$ such that

$$U + \begin{bmatrix} a_{m-1,m} & \dots & a_{m-1,n} \end{bmatrix} - T \begin{bmatrix} a_{m,m} & \dots & a_{m,n} \\ \vdots & \ddots & \vdots \\ a_{n,m} & \dots & a_{n,n} \end{bmatrix} = \begin{bmatrix} 0 & \dots & 0 \end{bmatrix}$$

holds. Recall that the last column of T is zero, whence $T(v_i)_{i=m}^n = 0$. \square

Lemma 3.16. *Let $p \in \mathbb{K}\langle X \rangle \setminus \mathbb{K}$ and $g \in \mathbb{F} \setminus \mathbb{K}$ be given by the minimal admissible linear systems $A_p = (u_p, A_p, v_p)$ and $A_g = (u_g, A_g, v_g)$ of dimension n_p and n_g respectively with $1 \in R(g)$. Then the left family of the ALS $\mathcal{A} = (u, A, v)$ for pg of dimension $n = n_p + n_g - 1$ from Proposition 3.12 is \mathbb{K} -linearly independent.*

Proof. Without loss of generality assume $v = [0, \dots, 0, 1]^\top$, A_p in polynomial form (by [10, Proposition 2.1 (ii)] every polynomial admits a linear representation with upper unitriangular system matrix) and A_g with first column $[1, 0, \dots, 0]^\top$. Let $s_p = (s_1^p, \dots, s_{n_p}^p)$ and $s_g = (s_1^g, \dots, s_{n_g}^g)$ be the respective left family of A_p and A_g . We have to show that the left family

$$s = (s_1, s_2, \dots, s_n) = (s_1^p g, \dots, s_{n_p-1}^p g, g, s_2^g, \dots, s_{n_g}^g).$$

of \mathcal{A} is \mathbb{K} -linearly independent. Assume to the contrary that there is an index $1 < m \leq n_p$ such that $(s_{m-1}, s_m, \dots, s_n)$ is \mathbb{K} -linearly dependent while (s_m, \dots, s_n)

is \mathbb{K} -linearly independent. Then, by Lemma 3.15, there exist matrices $T, U \in \mathbb{K}^{1 \times (n-m+1)}$ as blocks in (invertible) matrices $P, Q \in \mathbb{K}^{n \times n}$,

$$P = \begin{bmatrix} I_{m-2} & \cdot & \cdot \\ \cdot & 1 & T \\ \cdot & \cdot & I_{n-m+1} \end{bmatrix} \quad \text{and} \quad Q = \begin{bmatrix} I_{m-2} & \cdot & \cdot \\ \cdot & 1 & U \\ \cdot & \cdot & I_{n-m+1} \end{bmatrix},$$

that yield equation $s_{m-1} = 0$ (in row $m-1$) in PAQ . (This ‘‘potential’’ transformation (P, Q) is not necessarily admissible. But this is not an issue here, since we are only checking linear independence of the left family.) Let \tilde{P} (respectively \tilde{Q}) be the upper left part of P (respectively Q) of size $n_g \times n_g$. Then the equation in row $m-1$ in $\tilde{P}\mathcal{A}_p\tilde{Q}$ is $s_{m-1}^p = \alpha \in \mathbb{K}$, contradicting \mathbb{K} -linear independence of the left family of \mathcal{A}_p since $s_{n_p}^p = \lambda \in \mathbb{K}$. \square

Remark 3.17. Nothing can be said about minimality of \mathcal{A} since the right family $t = uA^{-1}$ could be \mathbb{K} -linearly dependent. As an example take $p = xy$ and $g = y^{-1} + z$. An ALS for $pg = x + xyz$ constructed by Proposition 3.12 is

$$\begin{bmatrix} 1 & -x & \cdot & \cdot & \cdot \\ \cdot & 1 & -y & \cdot & \cdot \\ \cdot & \cdot & 1 & 1 & -z \\ \cdot & \cdot & \cdot & y & 1 \\ \cdot & \cdot & \cdot & \cdot & 1 \end{bmatrix} s = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ \cdot \\ 1 \end{bmatrix}.$$

The right family is $t = [1, x, xy, x, x + xyz]$.

Lemma 3.18. *Let $f \in \mathbb{F} \setminus \mathbb{K}$ and $q \in \mathbb{K}\langle X \rangle \setminus \mathbb{K}$ be given by the minimal admissible linear systems $A_f = (u_f, A_f, v_f)$ and $A_q = (u_q, A_q, v_q)$ of dimension n_f and n_q respectively with $1 \in L(f)$. Then the right family of the ALS $\mathcal{A} = (u, A, v)$ for fq of dimension $n = n_f + n_q - 1$ from Proposition 3.11 is \mathbb{K} -linearly independent.*

Proposition 3.19 (Minimal Polynomial Multiplication [22, Proposition 28]). *Let $p, q \in \mathbb{K}\langle X \rangle$ be given by the minimal polynomial admissible linear systems $A_p = (1, A_p, \lambda_p)$ and $A_q = (1, A_q, \lambda_q)$ of dimension $n_p, n_q \geq 2$ respectively. Then the ALS \mathcal{A} from Proposition 3.11 for pq is minimal of dimension $n = n_p + n_q - 1$.*

Proof. The left family of \mathcal{A} is \mathbb{K} -linearly independent by Lemma 3.16 and its right family is \mathbb{K} -linearly independent by Lemma 3.18. Whence \mathcal{A} is minimal (by Proposition 2.9) and by construction in polynomial form. \square

Theorem 3.20 (Minimal Inverse [21, Theorem 4.13]). *Let $f \in \mathbb{F} \setminus \mathbb{K}$ be given by the minimal admissible linear system $\mathcal{A} = (u, A, v)$ of dimension n . Then a minimal ALS for f^{-1} is given in the following way:*

f of type $(1, 1)$ yields f^{-1} of type $(0, 0)$ with $\dim(\mathcal{A}') = n - 1$:

$$\mathcal{A}' = \left(1, \begin{bmatrix} -\lambda\Sigma b'' & -\Sigma B\Sigma \\ -\lambda b & -b'\Sigma \end{bmatrix}, 1 \right) \quad \text{for} \quad \mathcal{A} = \left(1, \begin{bmatrix} 1 & b' & b \\ . & B & b'' \\ . & . & 1 \end{bmatrix}, \lambda \right). \quad (5)$$

f of type $(1, 0)$ yields f^{-1} of type $(1, 0)$ with $\dim(\mathcal{A}') = n$:

$$\mathcal{A}' = \left(1, \begin{bmatrix} 1 & -\frac{1}{\lambda}c & -\frac{1}{\lambda}c'\Sigma \\ . & -\Sigma b'' & -\Sigma B\Sigma \\ . & -b & -b'\Sigma \end{bmatrix}, 1 \right) \quad \text{for} \quad \mathcal{A} = \left(1, \begin{bmatrix} 1 & b' & b \\ . & B & b'' \\ . & c' & c \end{bmatrix}, \lambda \right). \quad (6)$$

f of type $(0, 1)$ yields f^{-1} of type $(0, 1)$ with $\dim(\mathcal{A}') = n$:

$$\mathcal{A}' = \left(1, \begin{bmatrix} -\lambda\Sigma b'' & -\Sigma B\Sigma & -\Sigma a' \\ -\lambda b & -b'\Sigma & -a \\ . & . & 1 \end{bmatrix}, 1 \right) \quad \text{for} \quad \mathcal{A} = \left(1, \begin{bmatrix} a & b' & b \\ a' & B & b'' \\ . & . & 1 \end{bmatrix}, \lambda \right). \quad (7)$$

f of type $(0, 0)$ yields f^{-1} of type $(1, 1)$ with $\dim(\mathcal{A}') = n + 1$:

$$\mathcal{A}' = \left(1, \begin{bmatrix} \Sigma v & -\Sigma A\Sigma \\ . & u\Sigma \end{bmatrix}, 1 \right). \quad (8)$$

(Recall that the permutation matrix Σ reverses the order of rows/columns.)

Corollary 3.21. *Let $0 \neq f \in \mathbb{F}$. Then $f \in \mathbb{K}$ if and only if $\text{rank}(f) = \text{rank}(f^{-1}) = 1$.*

Remark 3.22. This simple consequence of Theorem 3.20 makes it possible to distinguish between *trivial* units (non-zero scalar elements) and *non-trivial* units, that is, elements in $\mathbb{F} \setminus \mathbb{K}$. The main idea in the factorization theory in Section 4 is to allow only (the insertion of) *trivial* units (in factorizations). It is used explicitly in Lemma 4.9 and implicitly in Theorem 4.11.

Remark 3.23. Note that $n \geq 2$ for type $(1, 1)$, $(1, 0)$ and $(0, 1)$. The block B is always square of size $n - 2$. For $n = 2$ the system matrix of \mathcal{A} is

- $\begin{bmatrix} 1 & b \\ . & 1 \end{bmatrix}$ for type $(1, 1)$,
- $\begin{bmatrix} 1 & b \\ . & c \end{bmatrix}$ for type $(1, 0)$ and
- $\begin{bmatrix} a & b \\ . & 1 \end{bmatrix}$ for type $(0, 1)$.

4. Factorization theory

To compensate the lack of non-zero non-units in $\mathbb{F} = \mathbb{K}\langle\langle X \rangle\rangle$, that is, $\mathbb{F} \setminus \{0\} = \mathbb{F}^\bullet = \mathbb{F}^\times = \{f \in \mathbb{F} \mid f \text{ is invertible}\}$, we will view the elements in terms of their *minimal* linear representations. Recall that the dimension of a minimal one of $f \in \mathbb{F}$ defines the rank of f .

Firstly, in Definition 4.1, we define *factors* based on the rank. Although this definition would suffice to define divisibility for polynomials, it is too rigid in general. Since this is far from obvious it is explained in detail in an example before Definition 4.6 (left and right divisibility). Secondly, some preparation is necessary to be able to exclude the insertion of non-trivial units. This is the essence of Lemma 4.9. Finally, Theorem 4.11 yields, as the main result, the equivalence of the “classical” divisibility (in free associative algebras) and the new one (for the free field) for polynomials.

For a factorization of a (non-zero) polynomial $p = q_1 q_2 \cdots q_m$ into atoms q_i we would like to have a factorization of its inverse $p^{-1} = (q_1 q_2 \cdots q_m)^{-1} = q_m^{-1} \cdots q_2^{-1} q_1^{-1}$ into atoms q_i^{-1} . For two polynomials p, q we have —due to the minimal polynomial multiplication— $\text{rank}(p) + \text{rank}(q) = \text{rank}(pq) + 1$. Recalling Definition 2.16 we have $p \mid_1 h$ if $h = pq$ for some $q \in \mathbb{K}\langle X \rangle$. The minimal inverse type $(1, 1)$ yields

$$\text{rank}(q^{-1}) + \text{rank}(p^{-1}) = \text{rank}(q) - 1 + \text{rank}(p) - 1 = \text{rank}(q^{-1}p^{-1}),$$

or q^{-1} “left divides” h^{-1} for $h = pq$. See Proposition 3.19, Theorem 3.20 and Lemma 4.7. To avoid inserting non-trivial units from $\mathbb{F} \setminus \mathbb{K}$, we have to bound the sum of the ranks of the two factors: $\text{rank}(px) + \text{rank}(x^{-1}q) = \text{rank}(pq) + 2$.

Definition 4.1 (Left and Right Factors). Let $h \in \mathbb{H} = \mathbb{F}^\bullet$ be given. An element $f \in \mathbb{H}$ is called *left factor* of h if

$$\begin{aligned} \text{rank}(f) + \text{rank}(f^{-1}h) &\leq \text{rank}(h) + 1 \quad \text{and} \\ \text{rank}(h^{-1}f) + \text{rank}(f^{-1}) &\leq \text{rank}(h^{-1}) + 1. \end{aligned}$$

An element $g \in \mathbb{H}$ is called *right factor* of h if

$$\begin{aligned} \text{rank}(hg^{-1}) + \text{rank}(g) &\leq \text{rank}(h) + 1 \quad \text{and} \\ \text{rank}(g^{-1}) + \text{rank}(gh^{-1}) &\leq \text{rank}(h^{-1}) + 1. \end{aligned}$$

Scalars and scalar multiples of h are called *trivial* factors. Non-trivial left/right factors are called *proper*. Left and right factors are also called *outer* to distinguish them from (general) factors of a factorization.

Remark 4.2. Straight away we have that f is a *left factor* of h if and only if $g = f^{-1}h$ is a *right factor* of h . And f is a *left factor* of h if and only if f^{-1} is a *right factor* of h^{-1} .

For two polynomials p and q the previous definition tells us that p (respectively q) is a left (respectively right) factor of pq . However, in general f is *not* a left factor of $h = fg$. As an example take $f = (xyz)^{-1}$ and $g = x$. Then

$$\begin{aligned} \text{rank}(f) + \text{rank}(g) &= \text{rank}(z^{-1}y^{-1}x^{-1}) + \text{rank}(x) \\ &= 3 + 2 \\ &> \text{rank}(z^{-1}y^{-1}) + 1. \end{aligned}$$

While here it is easy to see that f^{-1} and g have a non-trivial left divisor in $\mathbb{K}\langle X \rangle$ (in the sense of Definition 2.16), this can be much more delicate in general, illustrated in Example 4.3. This example will also show that the definition of outer factors is rather restrictive and not applicable directly. Later *left* and *right divisors* will be defined more generally in such a way that outer factors can be “split off” in at least one possible sequence (see Definition 4.6). Although we will see later that this is a generalization of the factorization in the free associative algebra, it is much more difficult to apply for two reasons: One has to test *all* possible “sequences” of factorizations to get the atoms (up to “similarity”). And the invertibility of the transformation matrices—to admissibly transform the ALS in such a way that the factors can be “extracted”—has to be ensured by including a condition for non-vanishing determinant. The latter might restrict practical applications to rank ≤ 6 , similar to the test if a matrix is full [14]. Section 5 provides further details. Experiments show that testing (ir)reducibility of polynomials (using polynomial admissible linear systems) works practically for rank ≤ 12 , in some cases up to rank ≤ 17 [14].

Example 4.3. Let $f = f_1f_2f_3$, with $f_1 = (xy)^{-1}$, $f_2 = 1 - xz$ and $f_3 = (yz)^{-1}$, be given by the *minimal* ALS

$$\begin{bmatrix} y & -1 & z & 0 \\ . & x & -1 & 0 \\ 0 & 0 & z & -1 \\ 0 & 0 & . & y \end{bmatrix} s = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \quad (9)$$

Then it is immediate (after recalling the construction of an ALS for the product from Proposition 3.1) that f_3 is a right factor of f by duplicating s_3 , that is,

inserting a “dummy” row (between row 2 and 3):

$$\begin{bmatrix} y & -1 & z & 0 & \cdot \\ \cdot & x & -1 & 0 & \cdot \\ 0 & 0 & 1 & -1 & 0 \\ \cdot & \cdot & 0 & z & -1 \\ \cdot & \cdot & 0 & \cdot & y \end{bmatrix} s' = \begin{bmatrix} \cdot \\ \cdot \\ 0 \\ \cdot \\ 1 \end{bmatrix}, \quad s' = \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_3 \\ s_4 \end{bmatrix}.$$

Thus, if a minimal ALS $\mathcal{A} = (u, A, v)$ for f is not of the form (9), we need to find an admissible transformation (P, Q) such that the (transformed) system matrix PAQ has a lower left zero block of size 2×2 and an upper right zero block of size 2×1 and only the last component of the right hand side Pv is non-zero, to detect the right factor f_3 . Similarly, subtracting row 3 from 1 and adding column 2 to 4 in (9) yields

$$\begin{bmatrix} y & -1 & 0 & 0 \\ \cdot & x & -1 & x \\ 0 & 0 & z & -1 \\ 0 & 0 & \cdot & y \end{bmatrix} s = \begin{bmatrix} 0 \\ 0 \\ \cdot \\ 1 \end{bmatrix}.$$

Compare with Figure 2, page 33, $k = 2$ in type $(*, 1)$. By duplicating t_2 , that is, inserting a “dummy” column (between column 2 and 3) one can see that $f_1 = (xy)^{-1}$ is a left factor of $f = (xy)^{-1}(1 - xz)(yz)^{-1}$:

$$\begin{bmatrix} 1 & \cdot & 0 & \cdot & \cdot \end{bmatrix} = \begin{bmatrix} t_1 & t_2 & t_2 & t_3 & t_4 \end{bmatrix} \begin{bmatrix} y & -1 & 0 & \cdot & \cdot \\ \cdot & x & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & x \\ \cdot & \cdot & 0 & z & -1 \\ \cdot & \cdot & 0 & \cdot & y \end{bmatrix}.$$

However, f_1 (respectively f_2) is *not* a left (respectively right) factor of $f_1 f_2$ while y^{-1} is a left factor of $f_1 f_2$ and x^{-1} is a left factor of $x^{-1} f_2$. We now take a closer look on that phenomenon. A *minimal* ALS for $f' = f_1 f_2$ is given by

$$\begin{bmatrix} y & -1 & z \\ \cdot & x & -1 \\ \cdot & \cdot & 1 \end{bmatrix} s = \begin{bmatrix} \cdot \\ \cdot \\ 1 \end{bmatrix}, \quad s = \begin{bmatrix} y^{-1}(x^{-1} - z) \\ x^{-1} \\ 1 \end{bmatrix}.$$

The reason is that the rank does not increase (when f_2 is multiplied by x^{-1} and y^{-1} from the left), because $1 \in R(x^{-1} f_2)$:

$$\begin{bmatrix} 1 & \cdot & \cdot \end{bmatrix} = t \begin{bmatrix} x & -x & -1 \\ \cdot & 1 & z \\ \cdot & \cdot & 1 \end{bmatrix}, \quad t = \begin{bmatrix} x^{-1} & 1 & x^{-1} - z \end{bmatrix}.$$

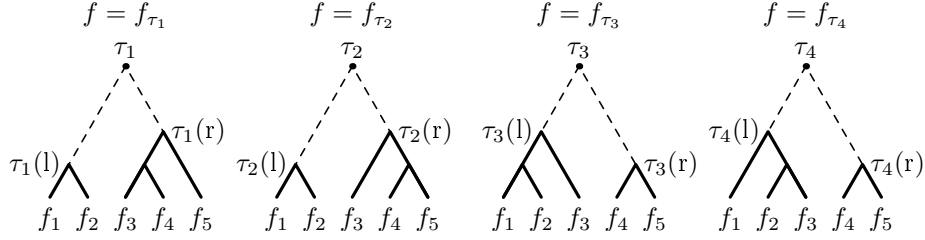


FIGURE 1. Four different derivation trees $\tau_k \in \mathcal{T}(f; f_1, f_2, \dots, f_5)$ with their respective (non-trivial) subtrees $\tau_k(l)$ and $\tau_k(r)$. The factorizations are $f_{\tau_1} = (f_1 f_2)((f_3 f_4) f_5)$, $f_{\tau_2} = (f_1 f_2)(f_3(f_4 f_5))$, $f_{\tau_3} = ((f_1 f_2) f_3)(f_4 f_5)$ resp. $f_{\tau_4} = (f_1(f_2 f_3))(f_4 f_5)$.

By adding column 2 to column 1 and switching the first two rows (this results in switching the first two columns in t) we get $[1, 0, 0]^T$ as the first column in the system matrix (for the existence of these transformations see Lemma 3.9):

$$\begin{bmatrix} 1 & \cdot & \cdot \end{bmatrix} = t \begin{bmatrix} 1 & 1 & z \\ 0 & -x & -1 \\ \cdot & \cdot & 1 \end{bmatrix}, \quad t = \begin{bmatrix} 1 & x^{-1} & x^{-1} - z \end{bmatrix}.$$

After multiplying $x^{-1}f_2$ from the left by y^{-1} , we have $1 \notin R(f')$. Hence a further multiplication by (for example) z^{-1} from the left *increases* the rank:

$$\begin{bmatrix} z & -1 & \cdot & \cdot \\ \cdot & y & -1 & z \\ \cdot & \cdot & x & -1 \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} s = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ 1 \end{bmatrix}, \quad s = \begin{bmatrix} z^{-1} f' \\ f' \\ x^{-1} \\ 1 \end{bmatrix}.$$

To summarize, there are essentially two different factorizations (on the level of outer factors in Definition 4.1) of $f = (xy)^{-1}(1 - xz)(yz)^{-1}$, namely

$$f = \left(y^{-1}(x^{-1}(1 - xz)) \right) (yz)^{-1} = (xy)^{-1} \left(((1 - xz)z^{-1})y^{-1} \right).$$

Now we come to the main definition which will generalize that of left and right divisors in the free associative algebra (Definition 2.16). To be able to show in Theorem 4.11 that these definitions are indeed equivalent on $\mathbb{K}\langle X \rangle$, some preparation is necessary.

Notation 4.4. Let $m \geq 2$ and $f = f_1 f_2 \cdots f_m$ be a product of m elements $f_i \in \mathbb{F}$. By $\mathcal{T} = \mathcal{T}(f; f_1, f_2, \dots, f_m)$ we denote the set of “multiplicative” *derivation trees* [18, Section 4.1] (or *parse trees*), that is, *complete plane binary trees* rooted at f with m leaves f_1, f_2, \dots, f_m [24] (or *ordered binary trees*). Now we fix some $\tau_0 \in \mathcal{T}$

and call a subtree τ of τ_0 *non-trivial* if it has at least two leaves. In this case we denote by $\tau(l)$ (respectively $\tau(r)$) the left (respectively right) subtree of τ and write f_τ for the product constructed by τ , that is, $f_\tau = f_{\tau(l)}f_{\tau(r)}$ (illustrated in Figure 1). The *height* (or *length*) of a subtree τ is defined as $\text{ht } \tau = 0$ in the trivial case and recursively as $\text{ht } \tau = 1 + \max\{\text{ht } \tau(l), \text{ht } \tau(r)\}$.

Remark 4.5. In a *complete plane binary tree*, no leaf is left out (that is, even “trivial” leaves or subtrees appear) and subtrees do not “cross”: Say $m = 5$ (as in Figure 1), $f_2 = 1$ and $f_4 = f_3^{-1}$. Then $f = (f_1 f_2) f_5$ is *not* “complete”, $f = (f_1 f_3)((f_2 f_4) f_5)$ is *not* “plane” (or “ordered”) and $f = (f_1 f_2)(f_3 f_4 f_5)$ is *not* “binary”.

Definition 4.6 (Left and Right Divisors and Coprime Elements). Let $\mathbb{H} = \mathbb{F}^\bullet$. An element $g \in \mathbb{H}$ *left divides* $f \in \mathbb{H}$, written as $g \mid_l^{\mathbb{F}} f$, if, for some $m' < m \in \mathbb{N}$, there exist $f_1, f_2, \dots, f_m \in \mathbb{H}$ and $\tau_0 \in \mathcal{T}(f; f_1, f_2, \dots, f_m)$ such that $g = f_1 f_2 \cdots f_{m'}$ and $f = g f_{m'+1} \cdots f_m$ and $f_{\tau(l)}$ is a *left factor* of $f_\tau = f_{\tau(l)} f_{\tau(r)}$ for all non-trivial subtrees τ of τ_0 .

Two elements $f, g \in \mathbb{H}$ are called *left coprime* (in \mathbb{H}) if for all $h \in \mathbb{H}$ such that $h \mid_l^{\mathbb{F}} f$ and $h \mid_l^{\mathbb{F}} g$ implies $h \in \mathbb{K}^\times$, that is, h is an element of the *trivial group of units*. Right division $f \mid_r^{\mathbb{F}} g$ and the notion of *right coprime* (in \mathbb{H}) is defined in a similar way. Two elements (in \mathbb{H}) are called *coprime* if they are left and right coprime.

Lemma 4.7 (Rank Lemma). *Let $0 \neq p, q \in \mathbb{F}$. Then*

- (i) $\text{rank}(pq) = \text{rank } p + \text{rank } q - 1$ if $p, q \in \mathbb{K}\langle X \rangle$,
- (ii) $\text{rank } p = \text{rank}(p^{-1}) + 1$ if $p \in \mathbb{K}\langle X \rangle$,
- (iii) $\text{rank}(p^{-1}q) \leq \text{rank}(p^{-1}) + \text{rank } q - 1$ if $1 \in R(q)$,
- (iv) $\text{rank}(p^{-1}q) \geq \text{rank}(p^{-1}) + \text{rank } q - 1$ if p^{-1} is a left factor of $p^{-1}q$,
- (v) $\text{rank}(pq^{-1}) \leq \text{rank } p + \text{rank}(q^{-1}) - 1$ if $1 \in L(p)$ and
- (vi) $\text{rank}(pq^{-1}) \geq \text{rank } p + \text{rank}(q^{-1}) - 1$ if q^{-1} is a right factor of pq^{-1} .

Proof. The rank identities (i) and (ii) are immediate consequences of the minimal polynomial multiplication (Proposition 3.19) and the minimal inverse (Theorem 3.20) respectively. The inequalities (iv) and (vi) follow directly from the Definition 4.1. To prove (iii), let p^{-1} and q be given by the *minimal* admissible linear systems $\mathcal{A}'_p = (u'_p, A'_p, v'_p)$ and $\mathcal{A}_q = (u_q, A_q, v_q)$ of dimension n'_p and n_q respectively. The construction of Proposition 3.12 yields an ALS of dimension n' (for $p^{-1}q$), hence $\text{rank}(p^{-1}q) \leq n' = \text{rank}(p^{-1}) + \text{rank } q - 1$. The proofs of (v) and (iii) are similar. \square

Remark 4.8. Note that (iii) and (v) hold in particular for polynomials. Further, recall from Example 4.3 that for (iv) to hold in the case of $p, q \in \mathbb{K}\langle X \rangle$ it is necessary but *not* sufficient that p and q are *left coprime*.

To illustrate the idea of the following lemma we take $p = xyz$ and an arbitrary f with $\text{rank}(f) = 2$. It is easy to see that $\text{rank}(pf^{-1}) \geq \text{rank}(p) - \text{rank}(f) = 2$ (with equality for $f = yz$) because otherwise we could construct an ALS of dimension $\text{rank}(pf^{-1}) + \text{rank}(f^{-1}) - 1 < \text{rank}(p)$. Now say that $f = xz$. Then $\text{rank}(pf^{-1}) = \text{rank}(xyx^{-1}) = 3$. However, for another polynomial q we get $\text{rank}(fq) = 2 + \text{rank}(q)$ thus $\text{rank}(pf^{-1}) + \text{rank}(fq) = 3 + 2 + \text{rank}(q) > 3 + \text{rank}(q) = \text{rank}(pq) + 1$.

What is rather simple in a concrete example, namely to verify that we cannot “insert” non-trivial units turns out to be very technical since we have to investigate the left and right families in detail.

Lemma 4.9. *Let $p \in \mathbb{K}\langle X \rangle \setminus \mathbb{K}$ and $f \in \mathbb{F} \setminus \mathbb{K}$ such that $p_{i_0}p_{i_0+1} \cdots p_m f^{-1} \notin \mathbb{K}^\times$ for all factorizations $p = p_1 p_2 \cdots p_m$ into atoms and all $i_0 \in \{1, 2, \dots, m\}$. Then $\text{rank}(pf^{-1}) + \text{rank}(f) > \text{rank}(p) + 1$.*

Proof. For a fixed non-scalar polynomial p we consider factorizations $p = p_1 p_2 \cdots p_m$ into m atoms p_j . For notational simplicity let $p_0 = p_{m+1} = 1$. Here p_1, p_2, \dots, p_m always denote atoms. Let

$$r = \min\{\text{rank}(p_{i_0}p_{i_0+1} \cdots p_m f^{-1}) \mid p = p_1 p_2 \cdots p_m \text{ and } i_0 \in \{1, 2, \dots, m\}\}$$

and i_0 and $p_1 p_2 \cdots p_m$ such that this minimum is attained. By assumption $h = p_{i_0} p_{i_0+1} \cdots p_m f^{-1} \in \mathbb{F} \setminus \mathbb{K}$ with $\text{rank}(h) = r$. Thus $f = h^{-1} p_{i_0} p_{i_0+1} \cdots p_m$ with *non-scalar* h . According to Theorem 3.20 there are four cases:

- $r \geq 2$ and $\text{rank}(h^{-1}) = r - 1$ for type (1, 1),
- $r \geq 2$ and $\text{rank}(h^{-1}) = r$ for type (1, 0),
- $r \geq 2$ and $\text{rank}(h^{-1}) = r$ for type (0, 1) and
- $r \geq 1$ and $\text{rank}(h^{-1}) = r + 1$ for type (0, 0).

Now fix an arbitrary factorization of p (into atoms q_i) and any $1 < \ell \leq m$ and let $p' = q_1 q_2 \cdots q_{\ell-1}$ and $p'' = q_\ell q_{\ell+1} \cdots q_m$ with ranks n' and n'' respectively. It is enough to show that

$$\text{rank}(p'h) + \text{rank}(h^{-1}p'') > \text{rank}(p'p'') + 1 = \text{rank}(p') + \text{rank}(p'').$$

We proceed as follows: Depending on the four cases we construct —using Proposition 3.11 and Proposition 3.12— admissible linear systems for $p'h$ and $h^{-1}p''$ respectively and find an upper bound for the number of rows/columns that can be removed (due to \mathbb{K} -linear dependent entries in their left and right families).

We start by assuming type $(1, 1)$. For $p'h$ we construct an ALS \mathcal{A}' of dimension $n_1 = n' + r - 1$ with the block decomposition (as linear representation according to Theorem 2.7)

$$\pi' = \left(\begin{bmatrix} 0 & u' & \cdot \end{bmatrix}, \begin{bmatrix} A'_{1,1} & A'_{1,2} & A'_{1,3} \\ \cdot & A'_{2,2} & A'_{2,3} \\ \cdot & \cdot & A'_{3,3} \end{bmatrix}, \begin{bmatrix} \cdot \\ v' \\ 0 \end{bmatrix} \right).$$

For $h^{-1}p''$ we construct \mathcal{A}'' of dimension $n_2 = n'' + r - 2$ with the block decomposition

$$\pi'' = \left(\begin{bmatrix} 0 & u'' & \cdot \end{bmatrix}, \begin{bmatrix} A''_{1,1} & A''_{1,2} & A''_{1,3} \\ \cdot & A''_{2,2} & A''_{2,3} \\ \cdot & \cdot & A''_{3,3} \end{bmatrix}, \begin{bmatrix} \cdot \\ v'' \\ 0 \end{bmatrix} \right).$$

Let k'_t (respectively k'_s) be the size of block $A'_{1,1}$ (respectively $A'_{3,3}$) in π' and k''_t (respectively k''_s) be the size of block $A''_{1,1}$ (respectively $A''_{3,3}$) in π'' . Firstly, we write the left and the right family of h^{-1} in terms of their respective family of h : Let $(s_1^h, s_2^h, \dots, s_r^h)$ and $(t_1^h, t_2^h, \dots, t_r^h)$ be the left and right family respectively of some minimal ALS for h . Then $s_{h^{-1}} = (1, s_{r-1}^h, \dots, s_2^h)h^{-1}$ and $t_{h^{-1}} = h^{-1}(t_{r-1}^h, \dots, t_2^h, 1)$ are the families of a minimal ALS for h^{-1} constructed by Theorem 3.20. Recall that row/column n' was eliminated in a system of dimension $n' + r$ to get \mathcal{A}' and row/column r was eliminated in a system of dimension $r - 1 + n''$ to get \mathcal{A}'' . Secondly, we take a closer look at the left families of \mathcal{A}' and \mathcal{A}'' . They are (without loss of generality)

$$s' = (s_1^{p'}h, s_2^{p'}h, \dots, s_{n'-1}^{p'}h, s_1^h, s_2^h, \dots, s_r^h) \quad \text{and} \\ s'' = \underbrace{(h^{-1}p'', s_{r-1}^h h^{-1}p'', \dots, s_2^h h^{-1}p'')}_{r-1}, \underbrace{s_2^{p''}, \dots, s_{n''}^{p''}}_{n''-1}$$

respectively. The first observation is that $k'_s = 0$, that is, the left family of \mathcal{A}' is \mathbb{K} -linearly independent because $1 \in R(h)$ and Lemma 3.16. The first $r - 1$ and the last $n'' - 1$ components of s'' are \mathbb{K} -linearly independent. At most $r - 1$ (linear combinations of) components in s'' can be eliminated. Hence we have $k''_s \leq r - 1$. However, we claim that

$$k''_s \leq r - 2.$$

Assume to the contrary that (the rank of p'' is large enough and) $k''_s = r - 1$, that is, the block $A''_{3,3}$ has dimension k''_s . Then *all* to h^{-1} corresponding (linear combinations of) components in s'' can be eliminated by the last $n'' - 1$ *polynomial* entries. If $r = 2$ then h is a polynomial, so we assume $r \geq 3$. Since the left family

$(1, s_{r-1}^h, \dots, s_2^h)h^{-1}$ of h^{-1} is \mathbb{K} -linear independent and

$$\text{rank}(h^{-1}p'') < \text{rank}(s_k^h h^{-1}p'') < \text{rank}(p'') = n''$$

for all $k \in \{2, 3, \dots, r-1\}$ it follows that these s_k^h 's are polynomials and therefore h is a polynomial because it is of type $(1, 1)$. Hence h and p'' have a non-trivial (left) greatest common divisor which contradicts the minimality of $r = \text{rank}(h)$. Thus $k_s'' \leq r-2$. Thirdly, we take a closer look at the right families

$$\begin{aligned} t' &= (\underbrace{t_1^{p'}, t_2^{p'}, \dots, t_{n'-1}^{p'}}_{n'}, p' t_1^h, p' t_2^h, \dots, p' t_r^h) \quad \text{and} \\ t'' &= (h^{-1} t_{r-1}^h, \dots, h^{-1} t_2^h, h^{-1}, h^{-1} t_2^{p''}, \dots, h^{-1} t_{n''}^{p''}) \\ &= h^{-1} (\underbrace{t_{r-1}^h, \dots, t_2^h}_{r-1}, 1, t_2^{p''}, \dots, t_{n''}^{p''}). \end{aligned}$$

By assumption, the first $r-1$ and the last n'' components in t'' are \mathbb{K} -linearly independent. Since the $t_i^{p''}$'s are polynomials, we can eliminate at most $k \leq r-2$ *polynomial* (linear combinations of) components in t'' . But then the corresponding k (linear combinations of) components in t' are \mathbb{K} -linearly independent of $(t_1^{p'}, \dots, t_{n'-1}^{p'})$ because they are of the form $p' t_i^h$ (see Lemma 3.18 or minimal polynomial multiplication). By assumption, the first n' and the last r components in t' are \mathbb{K} -linearly independent. Thus at most $r-1-k$ components can be eliminated. Hence we have $k_t' + k_t'' \leq r-1$. However, we claim that

$$k_t' + k_t'' \leq r-2.$$

Assume to the contrary that $k_t' + k_t'' = r-1$. Then $p' t_r^h$ would also “vanish”, that is,

$$p'g = p'h + \sum_{j=2}^{r-1} \beta_j p' t_j^h = \sum_{i=1}^{n'-1} \alpha_i t_i^{p'} = q$$

with $\text{rank}(q) < \text{rank}(p')$. Hence $g = \kappa q_{\ell-1}^{-1} \cdots q_{\ell'}^{-1}$ for some ℓ' such that $1 \leq \ell' < \ell-1$ and $\kappa \in \mathbb{K}$. By assumption h is of type $(1, 1)$, but g is of type $(0, 0)$ by Theorem 3.20. Therefore $g = h - h_0$ for some (non-zero) h_0 of type $(1, 1)$. But that would contradict \mathbb{K} -linear independence of the right family $(t_1^h, t_2^h, \dots, t_r^h)$. Finally, for h of type $(1, 1)$, we have

$$\begin{aligned} \text{rank}(p'h) + \text{rank}(h^{-1}p'') &= n' + r - 1 - (k_s' + k_t') + n'' + r - 2 - (k_s'' + k_t'') \\ &\geq n' + n'' + 2r - 3 - (r-2) - (r-2) \\ &= n' + n'' + 1 > \text{rank}(p'p'') + 1. \end{aligned}$$

If h is of type $(0, 0)$, then h^{-1} is of type $(1, 1)$ and t'' is \mathbb{K} -linearly independent, so we can use similar arguments. If h is of type $(1, 0)$ then the systems \mathcal{A}' and \mathcal{A}'' are of dimensions $n' + r - 1$ and $n'' + r - 1$ respectively. Their left families are

$$\begin{aligned} s' &= (s_1^{p'} h, s_2^{p'} h, \dots, s_{n'-1}^{p'} h, s_1^h, s_2^h, \dots, s_r^h) \quad \text{and} \\ s'' &= (\underbrace{h^{-1} p'', s_r^h h^{-1} p'', \dots, s_2^h h^{-1} p''}_r, \underbrace{s_2^{p''}, \dots, s_{n''}^{p''}}_{n''-1}). \end{aligned}$$

By similar arguments to the case $(1, 1)$ — s' is \mathbb{K} -linearly independent— we get $k_s'' \leq r - 1$. The right families are

$$\begin{aligned} t' &= (\underbrace{t_1^{p'}, t_2^{p'}, \dots, t_{n'-1}^{p'}, p' t_1^h, p' t_2^h, \dots, p' t_r^h}_{n'}, \underbrace{p' t_1^h, \dots, p' t_r^h}_{r-1}) \quad \text{and} \\ t'' &= h^{-1} (\underbrace{t_r^h, \dots, t_2^h}_r, 1, t_2^{p''}, \dots, t_{n''}^{p''}). \end{aligned}$$

Since neither h nor h^{-1} is a polynomial, at most $r - 2$ components in t' or t'' can be eliminated, that is, $k_t' + k_t'' \leq r - 2$. Therefore, for h of type $(1, 0)$, we have

$$\begin{aligned} \text{rank}(p'h) + \text{rank}(h^{-1}p'') &= n' + r - 1 - (k_s' + k_t') + n'' + r - 1 - (k_s'' + k_t'') \\ &\geq n' + n'' + 2r - 2 - (r - 1) - (r - 2) \\ &= n' + n'' + 1 > \text{rank}(p'p'') + 1. \end{aligned}$$

If h is of type $(0, 1)$, then we have, by Lemma 3.18, \mathbb{K} -linearly independent right family t'' . By similar arguments we have $k_t' \leq r - 1$ and $k_s' + k_s'' \leq 2$. Thus, at the end, we have shown that $\text{rank}(pf^{-1}) + \text{rank}(f) > \text{rank}(p) + 1$. \square

Lemma 4.10. *Let $q \in H = \mathbb{K}\langle X \rangle^\bullet$ and $p \in \mathbb{H} = \mathbb{F}^\bullet$. Then $p \stackrel{\mathbb{F}}{|} q$ implies $q = ph$ with $p, h \in H$.*

Proof. For some $m' < m$, let $p = f_1 f_2 \cdots f_{m'}$ and $q = p f_{m'+1} \cdots f_m$ and $\tau_0 \in \mathcal{T}(q; f_1, f_2, \dots, f_m)$ such that $q_{\tau(1)}$ is a left factor of $q_\tau = q_{\tau(1)} q_{\tau(r)}$ for all non-trivial subtrees τ of τ_0 . We have to show that $q_{\tau_k} \in H$ for all non-trivial subtrees τ_k of τ_0 with root in height k by induction on k from 0 to $\text{ht}(\tau_0) - 1$. For $k = 0$ we have $q_{\tau_0} = q \in H$. Without loss of generality assume that $q_{\tau_k(r)}$ is a *proper right* factor of $q_{\tau_k} = q_{\tau_k(1)} q_{\tau_k(r)}$ (in this case $q_{\tau_k(1)}$ is a *proper left* factor of q_{τ_k} ; nothing has to be shown for trivial factors), that is

$$\begin{aligned} \text{rank}(q_{\tau_k} q_{\tau_k(r)}^{-1}) + \text{rank}(q_{\tau_k(r)}) &\leq 1 + \text{rank}(q_{\tau_k}) \quad \text{and} \\ \text{rank}(q_{\tau_k(1)}^{-1}) + \text{rank}(q_{\tau_k(r)} q_{\tau_k}^{-1}) &\leq 1 + \text{rank}(q_{\tau_k}^{-1}). \end{aligned}$$

By assumption q_{τ_k} is a polynomial and thus all factorizations into atoms have the same length, say ℓ_k (which depends on τ_k). We claim that $q_{\tau_k(r)} = \kappa g_{\ell_0} \cdots g_{\ell_k}$ for some factorization $q_{\tau_k} = g_1 g_2 \cdots g_{\ell_k}$, some $\ell_0 \in \{1, 2, \dots, \ell_k\}$ and $\kappa \in \mathbb{K}$. Assume the contrary and apply Lemma 4.9 with $p = q_{\tau_k}$ and $f = q_{\tau_k(r)}$ to get the contradiction

$$\text{rank}(q_{\tau_k} q_{\tau_k(r)}^{-1}) + \text{rank}(q_{\tau_k(r)}) > 1 + \text{rank}(q_{\tau_k}).$$

Thus $q_{\tau_k(r)} \in H$ and $q_{\tau_k(l)} = q_{\tau_k} q_{\tau_k(r)}^{-1} \in H$. In particular $p = f_1 f_2 \cdots f'_m \in H$ and $h = f_{m'+1} f_{m'+2} \cdots f_m \in H$. \square

Theorem 4.11. *Let $p, q \in H = \mathbb{K}\langle X \rangle^\bullet$. Then $p \mid_l q$ (respectively $p \mid_r q$) if and only if $p \mid_l^{\mathbb{F}} q$ (respectively $p \mid_r^{\mathbb{F}} q$) in \mathbb{F} .*

Proof. Let $p \mid_l q$, that is $q \in pH = \{ph \mid h \in H\}$. We show that p is a left factor of $q = ph$. By Lemma 4.7 (i) we get $\text{rank}(q) = \text{rank}(p) + \text{rank}(p^{-1}q) - 1$ and by (ii) we get $\text{rank}(q^{-1}) + 1 = \text{rank}(p^{-1}) + 1 + \text{rank}(q^{-1}p)$, thus p is a left factor of $ph = q$ and therefore ($m' = 1$, $m = 2$ and a derivation tree τ_0 of height 1 in Definition 4.6) $p \mid_l^{\mathbb{F}} q$ (in \mathbb{F}). Conversely, we have to show that $q \in pH$. But this follows directly from the assumption $p \mid_l^{\mathbb{F}} q$ and Lemma 4.10. \square

Notation 4.12. Since the left (respectively right) division in $\mathbb{K}\langle X \rangle$ is the same as in \mathbb{F} we can simplify notation and use $f \mid_l g$ instead of $f \mid_l^{\mathbb{F}} g$ (respectively $f \mid_r g$ instead of $f \mid_r^{\mathbb{F}} g$) in the following.

Definition 4.13 (Atoms, Irreducible Elements). Let $\mathbb{H} = \mathbb{F}^\bullet$. An element $f \in \mathbb{H} \setminus \mathbb{K}$, that is, a non-trivial unit (in \mathbb{F}), is called (generalized) *atom* (or *irreducible*) if $f = g_1 g_2$ with $g_1, g_2 \in \mathbb{H}$ and $g_1 \mid_l f$ implies that either $g_1 \in \mathbb{K}^\times$ or $g_2 \in \mathbb{K}^\times$. Like in Definition 2.17, the set of atoms in \mathbb{F} is denoted by $\mathbf{A}(\mathbb{F})$.

Remark 4.14. Even in “simple” cases it is difficult to decide whether an element is irreducible (in the general sense of Definition 4.13) based on rational expressions. As an example take $f = 1 - xy$ and $g = (1 - zy)^{-1}$. Then fg is *irreducible* while gf is *reducible*. One has to look on their *minimal* linear representations. Minimal admissible linear systems for fg and gf are

$$\begin{bmatrix} 1 & -1 & -x \\ \cdot & y & 1 \\ \cdot & 1 & z \end{bmatrix} s = \begin{bmatrix} \cdot \\ \cdot \\ 1 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} y & 1 & \cdot & \cdot \\ 1 & z & -x & -1 \\ \cdot & \cdot & 1 & y \\ \cdot & \cdot & \cdot & 1 \end{bmatrix} s = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ 1 \end{bmatrix}$$

respectively.

Remark 4.15. In other words, a generalized atom can be created *multiplicatively* out of two atoms. This phenomenon is somewhat curious. As an example we consider $f = f_1 f_2^{-1}$ for $f_1 = 1 - xyz$ and $f_2 = 1 - zyz$. A *minimal* admissible linear system for f is given by

$$\begin{bmatrix} 1 & -1 & \cdot & -x \\ \cdot & z & 1 & \cdot \\ \cdot & \cdot & y & -1 \\ \cdot & 1 & \cdot & z \end{bmatrix} s = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ 1 \end{bmatrix}.$$

Since $\text{rank}(f_1) + \text{rank}(f_2^{-1}) = 7 > 5 = \text{rank}(f) + 1$, neither f_1 nor f_2 is an outer factor (of f). Indeed, f does not have any (non-trivial) outer factors.

Remark 4.16. Note the additional condition $g_1 \mid_1 f$ compared to Definition 2.17. It is *crucial*. Without $f = 1 - x = x \cdot (x^{-1} - 1)$ would not be an atom. (Actually there would not be any atoms at all.) However, $x \nmid_1 (1 - x)$ because $\text{rank}(x) + \text{rank}(x^{-1}(1 - x)) = 4 > 3 = 1 + \text{rank}(1 - x)$.

Remark 4.17. A reducible polynomial has only “polynomial” divisors. The result of Lemma 4.10 is stronger than the assumptions for the equivalence of divisibility in Theorem 4.11, in which one divisor is a polynomial.

Proposition 4.18. *A polynomial is an atom if and only if it is a generalized atom.*

Proof. We have to show that $\mathbf{A}(\mathbb{K}\langle X \rangle) = \mathbf{A}(\mathbb{F}) \cap \mathbb{K}\langle X \rangle$. Recall from Lemma 4.10 that for a polynomial p we have $g_1 \mid_1 p$ implies $p = g_1 g_2$ with polynomials g_1 and g_2 . Now both implications are immediate. \square

Notation 4.19. In the following we use “atom” as the general term and “polynomial atom” if we want to emphasize that the atom is an element in the free associative algebra.

5. Minimal multiplication and factorization

Before we describe the correspondence of zero (lower left and upper right) blocks in the system matrix of a minimal ALS and a non-trivial factorization, we describe a construction of a minimal ALS $\mathcal{A} = (u, A, v) = (1, A, \lambda)$, $A = (a_{ij})$, for the product of two non-zero elements f, g given by *minimal* admissible linear systems, say of dimension n_f and n_g respectively, if f is a *left factor* of fg . According to Theorem 5.2 there are three cases (see also Figure 2, page 33):

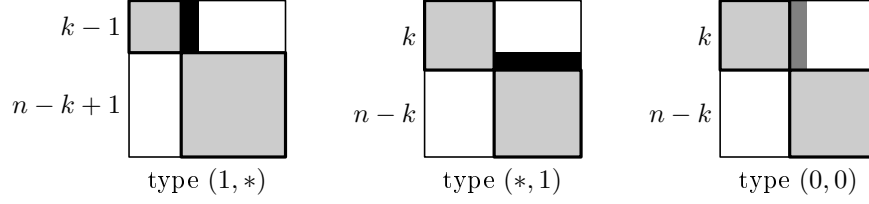


FIGURE 2. There are three types of factorization of an element $h = fg$ with $\text{rank}(h) = n$, $\text{rank}(f) = k$ and $\text{rank}(g) = n - k$ for type $(0, 0)$ or $\text{rank}(g) = n - k + 1$ otherwise. These types correspond to that of the minimal multiplication. For type $(1, *)$ and $(*, 1)$ the coupling has to be *non-scalar* for *all* transformations yielding appropriate zero blocks. The upper left (grey) block corresponds (modulo “overlapping”) to the system matrix A_f of the ALS $\mathcal{A}_f = (u_f, A_f, v_f)$ of f , the lower right to A_g of the ALS $\mathcal{A}_g = (u_g, A_g, v_g)$ of g . White blocks denote zeros, black blocks contain at least one non-scalar entry.

type	lower left zeros	“coupling”	upper right zeros
$(1, *)$	$n_g \times (n_f - 1)$	$\exists 1 \leq i < n_f : a_{i, n_f} \notin \mathbb{K}$	$(n_f - 1) \times (n_g - 1)$
$(*, 1)$	$(n_g - 1) \times n_f$	$\exists 1 \leq j < n_g : a_{n_f, n_f + j} \notin \mathbb{K}$	$(n_f - 1) \times (n_g - 1)$
$(0, 0)$	$n_g \times n_f$	$\forall i = 1, \dots, n_f : a_{i, n_f + 1} \in \mathbb{K}$	$n_f \times (n_g - 1)$

Note that for type $(1, *)$ and $(*, 1)$ the “coupling condition” must hold for *each* (admissibly) transformed system because otherwise both types could be “derived” easily from type $(0, 0)$. To “reverse” the multiplication we need to transform an ALS accordingly using transformations of the form

$$(P, Q) = \left(\begin{bmatrix} \alpha_{1,1} & \dots & \alpha_{1,n-1} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ \alpha_{n-1,1} & \dots & \alpha_{n-1,n-1} & 0 \\ \alpha_{n,1} & \dots & \alpha_{n,n-1} & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & \dots & 0 \\ \beta_{2,1} & \beta_{2,2} & \dots & \beta_{n,2} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n,1} & \beta_{n,2} & \dots & \beta_{n,n} \end{bmatrix} \right). \quad (10)$$

with entries $\alpha_{ij}, \beta_{ij} \in \mathbb{K}$. To ensure invertibility we need $\det P \neq 0$ and $\det Q \neq 0$.

Remark 5.1. The *minimal polynomial multiplication* (Proposition 3.19) can be formulated as a corollary to the following theorem. The difficulty of the proof of the former is hidden in the definition of *outer* factors, Definition 4.1. To test if f is a left factor of fg in general relies on techniques for minimization of linear representations which is discussed in [20].

Theorem 5.2 (Minimal Multiplication). *Let $f, g \in \mathbb{F} \setminus \mathbb{K}$ be given by the minimal admissible linear systems $\mathcal{A}_f = (u_f, A_f, v_f)$ and $\mathcal{A}_g = (u_g, A_g, v_g)$ of dimension n_f and n_g respectively. Let $n = n_f + n_g$. If f is a left factor of fg , then a minimal ALS for fg is given by*

$$\mathcal{A} = \begin{cases} \text{Proposition 3.11 with } \dim \mathcal{A} = n - 1 & \text{if } 1 \in L(f), \\ \text{Proposition 3.12 with } \dim \mathcal{A} = n - 1 & \text{if } 1 \in R(g), \\ \text{Proposition 3.1 with } \dim \mathcal{A} = n & \text{if } 1 \notin R(g) \text{ and } 1 \notin L(f). \end{cases}$$

Proof. Since f is a left factor of fg , we have $\text{rank}(f) + \text{rank}(g) \leq \text{rank}(fg) + 1$, thus

$$\text{rank}(fg) \geq \text{rank}(f) + \text{rank}(g) - 1 = \dim \mathcal{A} \geq \text{rank}(fg)$$

and hence minimality of \mathcal{A} if $1 \in R(g)$ or $1 \in L(f)$, that is, the first two cases/types $(*, 1)$ and $(1, *)$. For the last case/type $(0, 0)$ we distinguish four subcases. Recall from Theorem 3.20 that

$$\text{rank}(h^{-1}) = \begin{cases} \text{rank}(h) - 1 & \text{if } h \text{ is of type } (1, 1), \\ \text{rank}(h) & \text{if } h \text{ is of type } (1, 0) \text{ or } (0, 1) \text{ and} \\ \text{rank}(h) + 1 & \text{if } h \text{ is of type } (0, 0). \end{cases}$$

Since f is a left factor of fg , we have also

$$\text{rank}(g^{-1}f^{-1}) + 1 \geq \text{rank}(g^{-1}) + \text{rank}(f^{-1}).$$

Hence —by the minimal inverse on the right hand side—

$$\text{rank}(g^{-1}f^{-1}) + 1 \geq \begin{cases} \text{rank}(g) + \text{rank}(f) & \text{if } 1 \in R(f) \text{ and } 1 \in L(g), \\ \text{rank}(g) + 1 + \text{rank}(f) & \text{if } 1 \in R(f) \text{ and } 1 \notin L(g), \\ \text{rank}(g) + \text{rank}(f) + 1 & \text{if } 1 \notin R(f) \text{ and } 1 \in L(g) \text{ and} \\ \text{rank}(g) + 1 + \text{rank}(f) + 1 & \text{if } 1 \notin R(f) \text{ and } 1 \notin L(g). \end{cases}$$

Note that a priori we cannot assume minimality of \mathcal{A} for fg , since this is what we have to prove. Therefore we cannot use the minimal inverse on the left hand side because we only know that, for example, $1 \in L(g)$ implies $1 \in L(\mathcal{A})$ by construction. However, by the minimal inverse, we know —since g is of type $(0, *)$ — that g^{-1} is of type $(1, 1)$ or $(0, 1)$ and f^{-1} is of type $(1, 1)$ or $(1, 0)$. Hence we can use one of the first two cases and get $\text{rank}(fg) \geq \text{rank}(f) + \text{rank}(g)$. \square

Remark 5.3. Let $A = (a_{ij})$ be the system matrix of the ALS from Theorem 5.2. For type $(1, *)$ there exists an $i \in \{1, 2, \dots, n_f - 1\}$ such that a_{i, n_f} is *non-scalar*. For type $(*, 1)$ there exists an $j \in \{n_f + 1, n_f + 2, \dots, n\}$ such that $a_{n_f, j}$ is *non-scalar*.

And for type $(0, 0)$ the entries a_{i, n_f+1} are *scalar* for $i \in \{1, 2, \dots, n_f\}$. We refer to that as *coupling conditions*. Note that there is no transformation of the form (10) respecting the zero blocks yielding a “scalar coupling” in type $(1, *)$ (respectively type $(*, 1)$) because that would contradict minimality of \mathcal{A}_f (respectively \mathcal{A}_g) which one can see after recalling the construction of the product in Proposition 3.1.

Lemma 5.4. *Let $h, f, g \in \mathbb{F} \setminus \mathbb{K}$ be given by the minimal admissible linear systems $\mathcal{A} = (1, A, \lambda)$, $\mathcal{A}_f = (u_f, A_f, v_f) = (1, A_f, \lambda_f)$ and $\mathcal{A}_g = (u_g, A_g, v_g) = (1, A_g, \lambda_g)$ of dimension n , n_f and n_g respectively such that f is a left factor of $h = fg$.*

*Type $(1, *)$: If f is of type $(*, 1)$ then there exists an admissible transformation (P, Q) of the form (10) such that $PAQ = (a_{i,j})$ has*

- a lower left block of zeros of size $n_g \times (n_f - 1)$,
- an upper right block of zeros of size $(n_f - 1) \times (n_g - 1)$ and
- there exists an $i \in \{1, 2, \dots, n_f - 1\}$ such that a_{i, n_f} is non-scalar.

Type $(, 1)$: If g is of type $(1, *)$ then there exists an admissible transformation (P, Q) of the form (10) such that $PAQ = (a_{i,j})$ has*

- a lower left block of zeros of size $(n_g - 1) \times n_f$,
- an upper right block of zeros of size $(n_f - 1) \times (n_g - 1)$ and
- there exists an $j \in \{n_f + 1, n_f + 2, \dots, n\}$ such that $a_{n_f, j}$ is non-scalar.

Type $(0, 0)$: If f is of type $(, 0)$ and g is of type $(0, *)$ then there exists an admissible transformation (P, Q) of the form (10) such that $PAQ = (a_{i,j})$ has*

- a lower left block of zeros of size $n_g \times n_f$,
- an upper right block of zeros of size $n_f \times (n_g - 1)$ and
- $a_{i, n_f+1} \in \mathbb{K}$ for $i \in \{1, 2, \dots, n_f\}$.

Proof. Let $\mathcal{A}' = (u', A', v') = (1, A', \lambda')$ be the minimal ALS for $h = fg$ constructed by Theorem 5.2 from $\frac{\lambda_g}{\lambda} \mathcal{A}_f$ and $\frac{\lambda}{\lambda_g} \mathcal{A}_g$. The system matrix $A' = (a'_{i,j})$ has —by construction— appropriate (lower left and upper right) blocks of zeros and —for type $(0, 0)$ — scalar entries a'_{i, n_f+1} for $i \in \{1, 2, \dots, n_f\}$. Since both systems \mathcal{A} and \mathcal{A}' for h are minimal, there exists, by Theorem 2.7, an admissible transformation (P, Q) such that $PAQ = \mathcal{A}'$. The right hand side $Pv = v'$ does not change, hence (P, Q) is of the form (10). The coupling conditions are fulfilled due to the construction of the minimal multiplication. \square

Example 5.5. To illustrate the importance of the coupling conditions we consider $h = x^{-1}zy^{-1}x^{-1}$ given by the minimal ALS

$$\begin{bmatrix} x & -z & \cdot \\ \cdot & y & -1 \\ \cdot & \cdot & x \end{bmatrix} s = \begin{bmatrix} \cdot \\ \cdot \\ 1 \end{bmatrix}.$$

Multiplication of type $(0, 1)$ for $n_f = n_g = 2$ would violate the coupling condition, “creating” a *non-minimal* ALS for g in $h = fg$.

Lemma 5.6 (Factorization Type $(1, *)$). *Let $h = fg \in \mathbb{F} \setminus \mathbb{K}$ be given by the minimal admissible linear system $\mathcal{A} = (u, A, v) = (1, A, \lambda)$ of dimension $n \geq 2$ and fix $1 < k \leq n$. Assume that A has a lower left block of zeros of size $(n-k+1) \times (k-1)$ and an upper right block of zeros of size $(k-1) \times (n-k)$. For a transformation (P, Q) let a'_{ij} denote the entries of PAQ . If for each transformation (P, Q) of the form (10) respecting these zero blocks there exists an $i \in \{1, 2, \dots, k-1\}$ such that $a'_{i,k}$ is non-scalar then f is a left factor of type $(*, 1)$ of h with $\text{rank}(f) = k$ and $\text{rank}(g) = n - k + 1$.*

Proof. By assumption, \mathcal{A} is of the (block) form

$$\begin{bmatrix} A_{1,1} & A_{1,2} & \cdot \\ \cdot & A_{2,2} & A_{2,3} \\ \cdot & A_{3,2} & A_{3,3} \end{bmatrix} \begin{bmatrix} s_{\underline{1}} \\ s_k \\ s_{\underline{3}} \end{bmatrix} = \begin{bmatrix} \cdot \\ \cdot \\ v_{\underline{3}} \end{bmatrix}$$

with square diagonal blocks $A_{1,1}$, $A_{2,2}$ and $A_{3,3}$ of size $k-1$, 1 and $n-k-1$ respectively. We duplicate the entry s_k in the left family by inserting a “dummy” row (and column) to get the following ALS of dimension $n+1$:

$$\begin{bmatrix} A_{1,1} & A_{1,2} & 0 & \cdot \\ 0 & 1 & -1 & 0 \\ \cdot & 0 & A_{2,2} & A_{2,3} \\ \cdot & 0 & A_{3,2} & A_{3,3} \end{bmatrix} \begin{bmatrix} s_{\underline{1}} \\ s_k \\ s_k \\ s_{\underline{3}} \end{bmatrix} = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ v_{\underline{3}} \end{bmatrix},$$

that is, “reversing” the construction from Proposition 3.11. The subsystems of dimension k and $n-k+1$ are *minimal* for f (due to the coupling condition) and $g = \mu s_k$ respectively, otherwise we could construct an ALS for h of dimension $n' < n$, contradicting minimality of \mathcal{A} . Clearly, $1 \in L(f)$. By construction we have $\text{rank}(f) + \text{rank}(g) = \text{rank}(h) + 1$, thus we only have to show that $\text{rank}(g^{-1}) + \text{rank}(f^{-1}) \leq \text{rank}(h^{-1}) + 1$ for f to be a left factor of h by distinguishing four cases (like in the minimal multiplication) and apply the minimal inverse. If h is of type $(1, 1)$, then f is of type $(1, 1)$ and g is of type $(*, 1)$. Thus $\text{rank}(g^{-1}) \leq \text{rank}(g)$ and

we get $\text{rank}(g^{-1}) + \text{rank}(f^{-1}) \leq \text{rank}(g) + \text{rank}(f) - 1 = \text{rank}(h^{-1}) + 1$. The other cases are as easy. \square

Lemma 5.7 (Factorization Type $(*, 1)$). *Let $h = fg \in \mathbb{F} \setminus \mathbb{K}$ be given by the minimal admissible linear system $\mathcal{A} = (u, A, v) = (1, A, \lambda)$ of dimension $n \geq 2$ and fix $1 \leq k < n$. Assume that A has a lower left block of zeros of size $(n - k) \times k$ and an upper right block of zeros of size $(k - 1) \times (n - k)$. For a transformation (P, Q) let a'_{ij} denote the entries of PAQ . If for each transformation (P, Q) of the form (10) respecting these zero blocks there exists an $j \in \{k + 1, k + 2, \dots, n\}$ such that $a'_{k,j}$ is non-scalar then f is a left factor of type $(*, 1)$ of h with $\text{rank}(f) = k$ and $\text{rank}(g) = n - k + 1$.*

Proof. By assumption, \mathcal{A} is of the (block) form

$$\begin{bmatrix} u_{\underline{1}} & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix} = \begin{bmatrix} t_{\underline{1}} & t_k & t_{\underline{3}} \end{bmatrix} \begin{bmatrix} A_{1,1} & A_{1,2} & \cdot \\ A_{2,1} & A_{2,2} & A_{2,3} \\ \cdot & \cdot & A_{3,3} \end{bmatrix}$$

with square diagonal blocks $A_{1,1}$, $A_{2,2}$ and $A_{3,3}$ of size $k - 1$, 1 and $n - k$ respectively. We duplicate the entry t_k in the right family by inserting a “dummy” column (and row) to get the following ALS of dimension $n + 1$:

$$\begin{bmatrix} u_{\underline{1}} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix} = \begin{bmatrix} t_{\underline{1}} & t_k & t_k & t_{\underline{3}} \end{bmatrix} \begin{bmatrix} A_{1,1} & A_{1,2} & 0 & \cdot \\ A_{2,1} & A_{2,2} & -1 & 0 \\ 0 & 0 & 1 & A_{2,3} \\ \cdot & \cdot & 0 & A_{3,3} \end{bmatrix},$$

that is, “reversing” the construction from Proposition 3.12. The subsystems of dimension k and $n - k + 1$ are *minimal* for $f = \mu t_k$ and g (due to the coupling condition) respectively, otherwise we could construct an ALS for h of dimension $n' < n$, contradicting minimality of \mathcal{A} . Clearly, $1 \in R(g)$. Showing that f is a left factor of $h = fg$ is like in Lemma 5.6. \square

Lemma 5.8 (Factorization Type $(0, 0)$). *Let $h = fg \in \mathbb{F} \setminus \mathbb{K}$ be given by the minimal admissible linear system $\mathcal{A} = (u, A, v) = (1, A, \lambda)$ of dimension $n \geq 2$ and fix $1 \leq k < n$. If $A = (a_{ij})$ has a lower left block of zeros of size $(n - k) \times k$, an upper right block of zeros of size $k \times (n - k - 1)$ and $a_{i,k+1} \in \mathbb{K}$ for $i \in \{1, 2, \dots, k\}$ then f is a left factor of type $(*, 0)$ of h with $\text{rank}(f) = k$ and g is of type $(0, *)$ with $\text{rank}(g) = n - k$.*

Proof. We get the subsystems \mathcal{A}_f (for f) and \mathcal{A}_g (for g) directly from the construction of the multiplication in Proposition 3.1. Non-minimality of one of them

would contradict minimality of \mathcal{A} . As would $1 \in L(f)$ or $1 \in R(g)$ using multiplication type $(*, 1)$ and $(1, *)$ respectively. The arguments for showing that f is left factor of $h = fg$ are similar to that in (the proof of) Lemma 5.6. \square

Theorem 5.9 (Free Factorization). *Let $h \in \mathbb{F}$ with $n = \text{rank}(h) \geq 2$ be given by the minimal admissible linear system $\mathcal{A} = (u, A, v)$. Then h has a proper left factor f with $\text{rank}(f) = k$ if and only if there exists an admissible transformation (P, Q) of the form (10) such that PAQ is of “type” $(1, *)$, $(*, 1)$ or $(0, 0)$ as in Figure 2, page 33.*

Proof. Assuming a proper left factor of rank k , Lemma 5.4 applies. Conversely, assuming such a transformation, we get a proper left factor of rank k by Lemma 5.6 for type $(1, *)$, by Lemma 5.7 for type $(*, 1)$ and by Lemma 5.8 for type $(0, 0)$. \square

Fixing a rank of a possible left factor in $\overline{\mathbb{K}}\langle\langle X \rangle\rangle$, a variant of [10, Theorem 4.1] can be used to detect the lower left and upper right block of zeros (of appropriate sizes depending on the type of factorization). Notice that there is a misprint, the coefficients corresponding to $1 \in X^*$ are missing. Here we have

$$\mathbb{K}[\alpha, \beta] = \mathbb{K}[\alpha_{1,1}, \dots, \alpha_{1,n-1}, \alpha_{2,1}, \dots, \alpha_{2,n-1}, \dots, \alpha_{n,1}, \dots, \alpha_{n,n-1}, \\ \beta_{2,1}, \dots, \beta_{2,n}, \beta_{3,1}, \dots, \beta_{3,n}, \dots, \beta_{n,1}, \dots, \beta_{n,n}].$$

The coupling conditions for type $(0, 0)$ have to be implemented directly by adding the coefficients corresponding to $x \in X$ for the “coupling vector”. For type $(1, *)$ and $(*, 1)$ one can test for a “scalar” coupling first. If there is no solution one can try to find an appropriate transformation for the zero blocks only.

Example 5.10. Let the element $f \in \mathbb{Q}\langle\langle X \rangle\rangle$ be given by the *minimal* ALS $\mathcal{A} = (u, A, v)$,

$$\begin{bmatrix} -1 & . & x & -1 \\ 1+x & x & -1 & . \\ y & 1 & x & -1 \\ x & . & -2 & x \end{bmatrix} s = \begin{bmatrix} . \\ . \\ . \\ 1 \end{bmatrix}.$$

Before we start a “brute force” attack and try to find (admissible) transformations (P, Q) , say for multiplication type $(0, 0)$ and two systems of dimension 2, we can easily find out that f is *regular*. If it cannot be transformed into a polynomial form, that is, f is no polynomial, we could check if $f^{-1} \in \mathbb{Q}\langle X \rangle$.

Now we try to find a *left factor* f_1 of type $(*, 0)$ with rank $n_1 = 2$ and a *right factor* f_2 of type $(0, *)$ with rank $n_2 = 2$, that is, minimal multiplication type $(0, 0)$. We need an *invertible* transformation (P, Q) of the form (10) such

that $PAQ = (a'_{i,j})$ has a 2×2 lower left and a 2×1 upper right block of zeros and $a'_{1,3}, a'_{2,3} \in \mathbb{Q}$. Additional to $\det P = 1$ and $\det Q = 1$ we have $12+6+4$ equations. A Gröbner basis for the ideal generated by these 24 equations (computed by FRICAS [12], using *lexicographic order*) is

$$\begin{aligned} &(\alpha_{1,1} + \alpha_{1,2}\beta_{2,2}\beta_{3,3}\beta_{3,4} + \alpha_{1,3}, \quad \alpha_{1,2}\alpha_{2,3}\alpha_{3,1} - \alpha_{1,3}\alpha_{2,2}\alpha_{3,1} - 1, \\ &\alpha_{2,1} + \alpha_{2,2}\beta_{2,2}\beta_{3,3}\beta_{3,4} + \alpha_{2,3}, \quad \alpha_{3,2}, \quad \alpha_{3,3}, \quad \alpha_{4,2}, \quad \alpha_{4,3}, \\ &\beta_{2,2}\beta_{3,3}^2\beta_{3,4} - \beta_{2,3}, \quad \beta_{2,2}\beta_{3,3}\beta_{4,4} - \beta_{2,2}\beta_{3,4}\beta_{4,3} - 1, \quad \beta_{2,3}^2, \quad \beta_{2,3}\beta_{3,4}, \\ &\beta_{2,3}\beta_{4,4} - \beta_{3,3}\beta_{3,4}, \quad \beta_{2,4}, \quad \beta_{3,1}, \quad \beta_{3,2}, \quad \beta_{3,4}^2, \quad \beta_{4,1} + 1, \quad \beta_{4,2}). \end{aligned}$$

Since $\beta_{3,4} = 0$, the transformation (P, Q) is of the form

$$(P, Q) = \left(\begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & -\alpha_{1,1} & \cdot \\ \alpha_{2,1} & \alpha_{2,2} & -\alpha_{2,1} & \cdot \\ \alpha_{3,1} & 0 & 0 & \cdot \\ \alpha_{4,1} & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ \beta_{2,1} & \beta_{2,2} & 0 & 0 \\ 0 & 0 & \beta_{3,3} & 0 \\ -1 & 0 & \beta_{4,3} & \beta_{4,4} \end{bmatrix} \right)$$

with a solution over \mathbb{Q} :

$$(P, Q) = \left(\begin{bmatrix} 2 & 0 & -2 & \cdot \\ 0 & 1 & 0 & \cdot \\ \frac{1}{2} & 0 & 0 & \cdot \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & \cdot & \cdot & \cdot \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix} \right).$$

The transformed system PAQ is

$$\begin{bmatrix} -2 - 2y & -2 & \cdot & 0 \\ 1 + x & x & -1 & 0 \\ 0 & 0 & \frac{1}{2}x & -\frac{1}{2} \\ 0 & 0 & -2 & x \end{bmatrix} s = \begin{bmatrix} \cdot \\ \cdot \\ \cdot \\ 1 \end{bmatrix},$$

that is, $f = f_1 f_2$, with $f_1 = (1 - xy)^{-1}$ and $f_2 = (x^2 - 2)^{-1}$, which can be seen easily after applying the minimal inverse on the two subsystems of dimension $n_1 = n_2 = 2$. Both factors f_1, f_2 are atoms. Over $\mathbb{C}\langle\langle X \rangle\rangle$ the second factor f_2 is *reducible*, we have $f_2 = (x - \sqrt{2})^{-1}(x + \sqrt{2})^{-1}$.

Remark 5.11. To find a solution in general (more systematically), the primary decomposition of ideals can be used, see for example [11, Section 4.8] and [6, Section 10.8].

Epilogue

The presented “free factorization theory” is concrete enough to be implemented in computer algebra software to be able to apply it. But some more theoretical questions remain open: Is the extension of the “classical” factorization theory (in free associative algebras) to the free field—assuming that polynomial atoms (and their inverse) remain irreducible—unique? Is the free field (in this setting) a “similarity UFD”? If so, given an element, is the sequence of the ranks of the atoms of a factorization an invariant (modulo permutations)?

Acknowledgement. I thank Daniel Smertnig for the fruitful discussions about non-commutative factorization and Michael Moßhammer for some hints on graphs and trees and use this opportunity to thank Sergey Berezin and Vladimir Vasilchuk for their support in St. Petersburg in May 2017. I am very grateful for the constructive feedback of the anonymous referees to increase readability, in particular for the suggested simplification of the definition of left/right divisibility.

References

- [1] N. R. Baeth and D. Smertnig, *Factorization theory: from commutative to non-commutative settings*, J. Algebra, 441 (2015), 475-551.
- [2] H. Bart, I. Gohberg, M. A. Kaashoek and A. C. M. Ran, *Factorization of Matrix and Operator Functions: the State Space Method*, Operator Theory: Advances and Applications, 178, Linear Operators and Linear Systems, Birkhäuser Verlag, Basel, 2008.
- [3] J. Berstel and C. Reutenauer, *Noncommutative Rational Series with Applications*, Encyclopedia of Mathematics and its Applications, 137, Cambridge University Press, Cambridge, 2011.
- [4] P. M. Cohn, *Noncommutative unique factorization domains*, Trans. Amer. Math. Soc., 109 (1963), 313-331.
- [5] P. M. Cohn, *Skew Fields, Theory of General Division Rings*, Encyclopedia of Mathematics and its Applications, 57, Cambridge University Press, Cambridge, 1995.
- [6] P. M. Cohn, *Basic Algebra, Groups, Rings and Fields*, Springer-Verlag London, Ltd., London, 2003.
- [7] P. M. Cohn, *Further Algebra and Applications*, Springer-Verlag London, Ltd., London, 2003.
- [8] P. M. Cohn, *Free Ideal Rings and Localization in General Rings*, New Mathematical Monographs, 3, Cambridge University Press, Cambridge, 2006.

- [9] P. M. Cohn and C. Reutenauer, *A normal form in free fields*, *Canad. J. Math.*, 46(3) (1994), 517-531.
- [10] P. M. Cohn and C. Reutenauer, *On the construction of the free field*, Dedicated to the memory of Marcel-Paul Schützenberger, *Internat. J. Algebra Comput.*, 9(3-4) (1999), 307-323.
- [11] D. A. Cox, J. Little and D. O’Shea, *Ideals, Varieties, and Algorithms, An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Fourth edition, Undergraduate Texts in Mathematics, Springer, Cham, 2015.
- [12] FRICAS *Computer Algebra System*, W. Hebisch, 2018.
<http://axiom-wiki.newsynthesis.org/FrontPage>.
- [13] J. W. Helton, I. Klep and J. Volčič, *Geometry of free loci and factorization of noncommutative polynomials*, *Adv. Math.*, 331 (2018), 589-626.
- [14] B. Janko, *Factorization of Non-commutative Polynomials and Testing Fullness of Matrices*, Diplomarbeit, TU Graz, 2018.
- [15] D. S. Kaliuzhnyi-Verbovetskyi and V. Vinnikov, *Singularities of rational functions and minimal factorizations: the noncommutative and the commutative setting*, *Linear Algebra Appl.*, 430(4) (2009), 869-889.
- [16] O. Ore, *Linear equations in non-commutative fields*, *Ann. of Math.*, 32(3) (1931), 463-477.
- [17] C. Reutenauer, *Michel Fliess and non-commutative formal power series*, *Internat. J. Control*, 81(3) (2008), 336-341.
- [18] M. Rigo, *Advanced Graph Theory and Combinatorics*, with a foreword by Vincent Blondel, Computer Engineering Series, ISTE, London; John Wiley & Sons, Inc., Hoboken, NJ, 2016.
- [19] A. Salomaa and M. Soittola, *Automata-Theoretic Aspects of Formal Power Series*, Texts and Monographs in Computer Science, Springer-Verlag, New York-Heidelberg, 1978.
- [20] K. Schrempf, *A standard form in (some) free fields: How to construct minimal linear representations*, ArXiv e-prints, March 2018.
- [21] K. Schrempf, *Linearizing the word problem in (some) free fields*, *Internat. J. Algebra Comput.*, 28(7) (2018), 1209-1230.
- [22] K. Schrempf, *On the factorization of non-commutative polynomials (in free associative algebras)*, *J. Symbolic Comput.*, 94 (2019), 126-148.
- [23] D. Smertnig, *Factorizations of elements in noncommutative rings: a survey*, in *Multiplicative ideal theory and factorization theory*, Springer Proc. Math. Stat., Springer, Cham, 170 (2016), 353-402.

- [24] R. P. Stanley, Enumerative Combinatorics, Volume 1, Second edition, Cambridge Studies in Advanced Mathematics, 49, Cambridge University Press, Cambridge, 2012.

Konrad Schrempf

Faculty of Mathematics
University of Vienna
Oskar-Morgenstern-Platz 1
1090 Wien, Austria
e-mail: math@versibilitas.at