

MINIMAL REPRESENTATIONS AND ALGEBRAIC RELATIONS FOR SINGLE NESTED PRODUCTS

CARSTEN SCHNEIDER

ABSTRACT. Recently, it has been shown constructively how a finite set of hypergeometric products, multibasic hypergeometric products or their mixed versions can be modeled properly in the setting of formal difference rings. Here special emphasis is put on robust constructions: whenever further products have to be considered, one can reuse –up to some mild modifications– the already existing difference ring. In this article we relax this robustness criteria and seek for another form of optimality. We will elaborate a general framework to represent a finite set of products in a formal difference ring where the number of transcendental product generators is minimal. As a bonus we are able to describe explicitly all relations among the given input products.

1. INTRODUCTION

An important milestone of symbolic summation has been carried out by S.A. Abramov [3, 4] to simplify indefinite sums defined over rational functions. In particular, Gosper’s algorithm [16] for the simplification of indefinite hypergeometric sums and Zeilberger’s extension to definite sums via his creative telescoping paradigm [49, 27, 28] made symbolic summation highly popular in many areas of sciences. This successful story has been pushed forward for single nested sums and related problems, see, e.g., [25, 26, 10]. Further generalizations opened up substantially the class of applications, like the holonomic approach [48, 11, 21] dealing with objects that can be described by recurrence systems or the multi-summation approach of (q -)hypergeometric products [47, 46, 7].

In this regard, also the difference field/ring approach initiated by M. Karr [18, 19] and extended further in [41, 39, 42] has been applied to non-trivial problems arising, e.g., in particle physics; for recent calculations see [1, 2]. In the latter case one can represent indefinite nested sums defined over (q -)hypergeometric products in the setting of $R\Pi\Sigma$ -difference ring extensions. As a side product, one can simplify the sum expressions w.r.t. certain optimality criteria, like finding sum representations with optimal nesting depth [35, 38, 40], with a minimal number of summation objects in the summands [37], or with minimal degrees arising in the numerators and denominators [33]. In particular, the occurring sums and products in the reduced expression are algebraically independent among each other [36, 17, 42].

Various improvements have been derived for optimal representations of sums, but much less has been gained for products so far. Concerning the simplification of one product in the setting of difference fields we refer to [32, 6, 29]. For the simplification of several products, only few algorithms have been developed. All of them can be related to the following problem.

This work was supported by the Austrian Science Fund (FWF) grant SFB F50 (F5009-N15).

Problem RPTB (Representation of Products in a Transcendental Basis): *Given*

$$F_1(n) = \prod_{k=l_1}^n f_1(k), \dots, F_r(n) = \prod_{k=l_r}^n f_r(k), \quad (1)$$

where the multiplicands $f_i(k)$ are represented in an appropriate difference field \mathbb{F} and¹ $l_i \in \mathbb{N}$; *find* an alternative set of such products

$$\Phi_1(n) = \prod_{k=l_1}^n \phi_1(k), \dots, \Phi_s(n) = \prod_{k=l_s}^n \phi_s(k) \quad (2)$$

and

$$\Phi_0(n) = \rho^n = \prod_{k=1}^n \rho \quad \text{with a primitive root of unity } \rho \text{ of order } \lambda \quad (3)$$

where $\Phi_0(n)^\lambda = 1$ such that

- (i) any product in (1) can be rewritten in a Laurent polynomial expression in terms of the products given in (2) and (3);
- (ii) the sequences produced by the products in (2) are algebraically independent over their ground field of sequences² adjoined with the sequence $(\phi_0(n))_{n \geq 0}$.

Internally, the available algorithms [32, 23] represent a finite set of such products automatically in a difference ring built by $R\Pi$ -extensions [18, 41] and exploit results from the Galois theory of difference rings elaborated in [36, 17, 42]. We note that the algorithms presented in [32, 39] and implemented in `Sigma` [34] can handle only hypergeometric products. In particular, the products must evaluate to elements in a field \mathbb{K} that can be built by a multivariate rational function field defined over \mathbb{Q} or $\mathbb{Q}[\iota]$ where ι denotes the imaginary unit with $\iota^2 = -1$. Recently, these ideas have been generalized in [23] for mixed-multibasic hypergeometric products [8] defined over a more general field \mathbb{K} .

Definition 1. *Let $\mathbb{K} = \mathbb{K}'(q_1, \dots, q_v)$ be a rational function field where \mathbb{K}' is a field of characteristic 0. Whenever we focus on algorithmic aspects, we restrict \mathbb{K}' further to a rational function field defined over an algebraic number field. A product $\prod_{j=l}^k f(j, q_1^j, \dots, q_v^j)$, $l \in \mathbb{N}$, is called mixed-multibasic hypergeometric [8] (in short mixed-hypergeometric) in k over \mathbb{K} if $f(x, y_1, \dots, y_v)$ is an element from the rational function field $\mathbb{K}(x, y_1, \dots, y_v)$ where the numerator and denominator of $f(j, q_1^j, \dots, q_v^j)$ are nonzero for all $j \in \mathbb{Z}$ with $j \geq l$. Such a product is called multibasic hypergeometric if f is free of x and q -hypergeometric if f is free of x , $v = 1$ and $q_1 = q$. It is called hypergeometric if $v = 0$, i.e., $f \in \mathbb{K}(x)$ with $\mathbb{K} = \mathbb{K}'$.*

Example 2. *Consider the hypergeometric products*

$$\begin{aligned} F_1(n) &= \prod_{k=1}^n \underbrace{\frac{-13122k(1+k)}{(3+k)^3}}_{=f_1(k)}, & F_2(n) &= \prod_{k=1}^n \underbrace{\frac{26244k^2(2+k)^2}{(3+k)^2}}_{=f_2(k)}, \\ F_3(n) &= \prod_{k=1}^n \underbrace{\frac{\iota k(2+k)^3}{729(5+k)}}_{=f_3(k)}, & F_4(n) &= \prod_{k=1}^n \underbrace{-\frac{162k(2+k)}{5+k}}_{=f_4(k)}. \end{aligned} \quad (4)$$

¹For $1 \leq i \leq r$ we assume that $f_i(k) \neq 0$ for all $k \in \mathbb{N} = \{0, 1, 2, \dots\}$ with $k \geq l_i$.

²We assume that \mathbb{F} can be embedded into the ring of sequences.

Then the algorithms from [32, 39, 23] find $\Phi_1(n) = n!$, $\Phi_2(n) = 2^n$, $\Phi_3(n) = 3^n$ (whose sequences are algebraically independent among each other) and the algebraic product $\Phi_0(n) = \iota^n$ satisfying the relation $\phi_0(n)^4 = 1$ with the following property: the input products can be rephrased in terms of the output products with

$$\begin{aligned} F_1(n) &= \frac{216 (\iota^n)^2 2^n (3^n)^8}{(n+1)^2 (n+2)^3 (n+3)^3 n!}, & F_2(n) &= \frac{9 (2^n)^2 (3^n)^8 (n!)^2}{(n+3)^2}, \\ F_3(n) &= \frac{15(n+1)^2 (n+2)^2 \iota^n (n!)^3}{(n+3)(n+4)(n+5) (3^n)^6}, & F_4(n) &= \frac{60 (\iota^n)^2 2^n (3^n)^4 n!}{(n+3)(n+4)(n+5)}. \end{aligned} \quad (5)$$

In [32, 39] and more generally in [23] the algorithms are designed to treat products with highest possible flexibility. They split the input products as much as possible into irreducible elements. As a consequence, when further products arise in a later construction phase, the already obtained products can –up to some mild modifications– be reused. Note that such robust constructions are crucial for large-scale calculations that arise, e.g., in particle physics [1, 2]. The algorithms for single-nested products described in [23], and even more general algorithms for multiple nested products [24], are available in Ocansey’s package `NestedProducts`.

In this article we will supplement this more practical oriented toolbox with theoretical aspects. We will provide a general framework that solves Problem *RPTB* not only for mixed-hypergeometric products, but for general difference rings that satisfy certain (algorithmic) properties; for further details we refer to Subsection 2.4 and Section 3. In particular, the output of Problem *RPTB* is in the following sense optimal: among all possible products in (2) and (3) that provide a solution of Problem *RPTB*, the number $s \geq 0$ of products and the order $\lambda \geq 1$ of the root of unity ρ in (3) are minimal (if $\lambda = 1$, the product in (3) simplifies to $\gamma^n = 1^n = 1$.)

Example 3. *With our new algorithmic framework we will calculate the minimal number of products*

$$\Phi_1(n) = \prod_{k=1}^n \frac{-162k(2+k)}{5+k}, \quad \Phi_2(n) = \prod_{k=1}^n \frac{-\iota(3+k)^6}{9k(1+k)^2(2+k)(5+k)}$$

(again the produced sequences are algebraically independent) and the alternating sign $\Phi_0(n) = (-1)^n$ such that the input products can be rephrased in the form

$$\begin{aligned} F_1(n) &= \frac{5(1+n)^2(2+n)^5(3+n)^8}{52488(4+n)(5+n)} (-1)^n \left(\prod_{k=1}^n \frac{-162k(2+k)}{5+k} \right) \left(\prod_{k=1}^n \frac{-\iota(3+k)^6}{9k(1+k)^2(2+k)(5+k)} \right)^{-2}, \\ F_2(n) &= \frac{(4+n)^2(5+n)^2}{400} \left(\prod_{k=1}^n \frac{-162k(2+k)}{5+k} \right)^2, \\ F_3(n) &= \frac{2754990144(4+n)^2(5+n)^2}{25(1+n)^4(2+n)^{10}(3+n)^{16}} \left(\prod_{k=1}^n \frac{-\iota(3+k)^6}{9k(1+k)^2(2+k)(5+k)} \right)^3, \\ F_4(n) &= \prod_{k=1}^n \frac{-162k(2+k)}{5+k}. \end{aligned} \quad (6)$$

In particular, we can conclude that Problem *RPTB* can be solved only by using an algebraic product of the form (3) where the order $\lambda = 2$ is minimal.

In contrast to [32, 39, 23, 24] this representation with a minimal number of products has one essential disadvantage: When a new product has to be treated

in addition, a complete redesign of the already produced products might be necessary. However, our new approach will provide further insight: given the special representation proposed in this article, one can read off straightforwardly a finite set of generators that describe all relations of the input products.

Example 4. *Given the hypergeometric products $F_1(n), F_2(n), F_3(n), F_4(n)$ from Example 2, we can compute all algebraic relations among them. More precisely, take the ring $\mathbb{E} = \mathbb{Q}(\iota)(x)[y, y_1^{-1}][y_2, y_2^{-1}][y_3, y_3^{-1}][y_4, y_4^{-1}]$ of Laurent polynomials in the variables y_1, y_2, y_3, y_4 with coefficients from the rational function field $\mathbb{Q}(\iota)(x)$ and consider the ideal³*

$$Z = \{p(x, y_1, y_2, y_3, y_4) \in \mathbb{E} \mid \exists \delta \in \mathbb{N} \forall n \in \mathbb{N} \\ n \geq \delta \Rightarrow p(n, F_1(n), F_2(n), F_3(n), F_4(n)) = 0\}$$

in \mathbb{E} that encodes all algebraic relations among the products $F_i(n)$ with $i = 1, 2, 3, 4$. Then with our new algorithms we can compute the two generators

$$\begin{aligned} e_1 &= \frac{y_2}{y_4^2} - \frac{1}{400}(4+x)^2(5+x)^2, \\ e_2 &= \frac{y_2^2 y_4^2}{y_1^6 y_3^4} - \frac{1}{4199040^2}(1+x)^4(2+x)^{10}(3+x)^{16}(4+x)^2(5+x)^2 \end{aligned} \quad (7)$$

that span the ideal Z . This means⁴

$$Z = \langle e_1, e_2 \rangle_{\mathbb{E}} = \{f_1 e_1 + f_2 e_2 \mid f_1, f_2 \in \mathbb{E}\}. \quad (8)$$

This result is connected to [20, 43] where all relations of a finite set of sequences can be computed that satisfy homogeneous linear recurrences with constant coefficients. In particular in [20] their algorithm is reduced to find all relations of a finite set of geometric sequences, i.e., sequences produced by the products in (1) with $f_1(k), \dots, f_r(k) \in \mathbb{K}^*$, which are a subclass of hypergeometric sequences. Further strategies for mixed-multibasic hypergeometric products are also mentioned in [29].

The outline of the article is as follows. In Section 2 we will formalize the sketched construction from above in details: we will represent the products (1) in a formal difference ring equipped with an evaluation function. In particular, we will rephrase the problem specification *RPTB* to the problem specification *DR* in this formal setting. In Section 3 we will list the basic properties of our difference ring theory [41, 42] and will enhance it for the constructions required in this article. In Section 4 we will restrict to a special case of products from which an optimal product representation can be read off straightforwardly. Finally, using the Smith normal form of integer matrices we will show in Section 5 how the general problem can be reduced to the special case treated in Section 4. A conclusion is given in Section 6.

³In this example the evaluation of an element from $\mathbb{Q}(\iota)(x)$ is carried out by replacing x with concrete values $n \in \mathbb{N}$. Later we will generalize this simplest case to formal difference rings equipped with an evaluation function acting on the ring elements.

⁴More generally, if R is a commutative ring with 1, we define the ideal I generated by $a_1, \dots, a_r \in R$ with $I = \langle a_1, \dots, a_r \rangle_R = \{f_1 a_1 + \dots + f_r a_r \mid f_1, \dots, f_r \in R\}$.

2. THE PROBLEM DESCRIPTION IN THE SETTING OF DIFFERENCE RINGS

In the following it will be convenient to represent the products under consideration in a formal ring⁵, often denoted by \mathbb{A} or \mathbb{E} . In this regard, it is essential to define in addition

- an evaluation function that describes how the elements in the formal ring are interpreted as sequences (see Subsection 2.1);
- a ring automorphism that describes how the elements in the formal ring are shifted (see Subsection 2.2).

In particular, we will take care that the evaluation function and the ring automorphism are compatible: applying the automorphism to an element in the formal ring and evaluating it afterwards at the n th sequence entry must equal to the evaluation at the $(n + 1)$ th sequence entry (see Subsection 2.3). In Subsection 2.4 we will finally rephrase Problem *RPTB* and the examples from the introduction in this algebraic setting.

2.1. The evaluation function – sequence domains. Inspired by [22] we will provide a so-called evaluation function which maps the elements from a formal ring \mathbb{A} to sequences with entries from a field $\mathbb{K} \subseteq \mathbb{A}$. More precisely, we will take care that the following functions will be available within our constructions [36, 42].

Definition 5. *Let \mathbb{A} be a ring and let \mathbb{K} be a subfield of \mathbb{A} .*

- (1) *A function $\text{ev}: \mathbb{A} \times \mathbb{N} \rightarrow \mathbb{K}$ is called evaluation function for \mathbb{A} if for all $f, g \in \mathbb{A}$ and $c \in \mathbb{K}$ there exists a $\lambda \in \mathbb{N}$ with the following properties:*

$$\forall n \geq \lambda : \text{ev}(c, n) = c, \quad (9)$$

$$\forall n \geq \lambda : \text{ev}(f + g, n) = \text{ev}(f, n) + \text{ev}(g, n), \quad (10)$$

$$\forall n \geq \lambda : \text{ev}(f g, n) = \text{ev}(f, n) \text{ev}(g, n). \quad (11)$$

- (2) *A function $L: \mathbb{A} \rightarrow \mathbb{N}$ is called operation-function (in short o-function) for \mathbb{A} and ev if for any $f, g \in \mathbb{A}$ with $\lambda = \max(L(f), L(g))$ the properties (10) and (11) hold. If such a function exist, ev is also called operation-bounded (in short o-bounded). In particular, ev is called o-computable if the function ev is computable and there is a computable o-function L for ev .*
- (3) *$z: \mathbb{A} \rightarrow \mathbb{N}$ is called z-function for ev if for any $f \in \mathbb{A} \setminus \{0\}$ and for any integer $n \geq Z(f)$ we have $\text{ev}(f, n) \neq 0$.*

Later we will rely on the following simple observation.

Lemma 6. *Let $\text{ev}: \mathbb{A} \times \mathbb{N} \rightarrow \mathbb{K}$ be an evaluation function for a ring \mathbb{A} .*

- (1) *If $a \in \mathbb{A}^*$, then there is a $\delta \in \mathbb{N}$ such that $\text{ev}(a, n) \neq 0$ for all $n \geq \delta$.*
- (2) *If \mathbb{A} is a field, there is a z-function for \mathbb{A} .*

Proof. (1) For $a \in \mathbb{A}^*$ there is a $\delta \in \mathbb{N}$ with $\text{ev}(a, n) \text{ev}(\frac{1}{a}, n) = \text{ev}(a \frac{1}{a}, n) = 1$ for all $n \geq \delta$. Consequently, $\text{ev}(a, n) \neq 0$ for all $n \geq \delta$. (2) follows by (1). \square

In short, a ring/field \mathbb{A} equipped with such an evaluation function ev will be called a *sequence domain* and will be denoted by (\mathbb{A}, ev) ; see also [38]. In all our examples we will always start with the following ground field.

⁵Throughout this article, all rings and fields have characteristic 0 and with \mathbb{A}^* we denote the group of units. Furthermore, all rings are commutative. The order of $a \in \mathbb{A}^*$, denoted by $\text{ord}(a)$, is the smallest positive integer k with $a^k = 1$. If such a k does not exist, we set $\text{ord}(a) = 0$.

Example 7. Take the rational function field $\mathbb{F} = \mathbb{K}(x)$ over a field \mathbb{K} with characteristic 0 and consider the evaluation function $\text{ev}: \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{K}$ defined by

$$\text{ev}\left(\frac{p}{q}, n\right) = \begin{cases} 0 & \text{if } q(n) = 0 \\ \frac{p(n)}{q(n)} & \text{if } q(n) \neq 0 \end{cases} \quad (12)$$

where $p, q \in \mathbb{K}[x]$, $q \neq 0$ and p, q are co-prime; here $p(n), q(n)$ is the usual evaluation of polynomials at $n \in \mathbb{N}$. We define the o-function $L(\frac{p}{q})$ by taking the minimal $l \in \mathbb{N}$ with $q(n+l) \neq 0$ for all $n \in \mathbb{N}$, and we define the z-function by $Z(\frac{p}{q}) = L(pq)$.

Our product expressions will be rephrased in terms of Laurent polynomials with coefficients from a ring \mathbb{A} . More precisely, we will denote by $\mathbb{A}\langle \hat{x} \rangle$ the ring of Laurent polynomials $\mathbb{A}[\hat{x}, \hat{x}^{-1}]$ and by $\mathbb{A}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle$ a tower of such ring extensions. In order to represent products of the form (3), we will work also with ring extensions of the form $\mathbb{A}[z]$ over a ring \mathbb{A} subject to a relation $z^\lambda = 1$. Note that such a ring contains zero-divisors that originate from

$$(1-z)(1+z+z^2+\dots+z^{\lambda-1}) = 1-z^\lambda = 0.$$

More precisely, by [42, Lemma 5.4 (parts 1,3)] one can straightforwardly construct an evaluation function for single nested products.

Lemma 8. Let \mathbb{F} be a field with subfield \mathbb{K} and let $\text{ev}: \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{K}$ be an evaluation function of \mathbb{F} . Let $\mathbb{E} = \mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle [z]$ be a ring where the \hat{x}_i are Laurent polynomial variables and z is a ring generator subject to the relation $z^\lambda = 1$. Let $a_1, \dots, a_r \in \mathbb{F}^*$ and let $l_1, \dots, l_r \in \mathbb{N}$ where for all $1 \leq i \leq r$ we have $\text{ev}(a_i, n) \neq 0$ with $n \geq l_i$. Furthermore, let $\rho \in \mathbb{K}^*$ with $\rho^\lambda = 1$. Then $\hat{\text{ev}}: \mathbb{E} \times \mathbb{N} \rightarrow \mathbb{K}$ defined by

$$\hat{\text{ev}}(f, n) = \sum_{(m_1, \dots, m_r, \mu) \in \mathbb{Z}^r \times \mathbb{N}} \text{ev}(f_{(m_1, \dots, m_r, \mu)}, n) \left(\prod_{k=l_1}^n \text{ev}(a_1, k) \right)^{m_1} \dots \left(\prod_{k=l_r}^n \text{ev}(a_r, k) \right)^{m_r} (\rho^n)^\mu \quad (13)$$

with

$$f = \sum_{(m_1, \dots, m_r, \mu) \in \mathbb{Z}^r \times \mathbb{N}} f_{(m_1, \dots, m_r, \mu)} \hat{x}_1^{m_1} \dots \hat{x}_r^{m_r} z^\mu \in \mathbb{E} \quad (14)$$

is an evaluation function. In particular if $L: \mathbb{F} \rightarrow \mathbb{N}$ is an o-function for \mathbb{F} , then $\hat{L}: \mathbb{E} \rightarrow \mathbb{N}$ defined by

$$\hat{L}(f) = \max \{ L(f_{(m_1, \dots, m_r, \mu)}) \mid (m_1, \dots, m_r, \mu) \in \mathbb{Z}^r \times \mathbb{N} \} \cup \{ l_i \mid 1 \leq i \leq r \text{ where } \hat{x}_i \text{ occurs in } f \} \cup \{ 1 \mid f \text{ depends on } z \} \quad (15)$$

for (14) is an o-function. If L is computable, then \hat{L} is computable.

Remark. If there is a computable z-function Z for ev and \mathbb{F} , the lower bounds l_i can be computed with $l_i = Z(a_i)$.

Example 9 (Cont. Ex. 7). We specialize the ground field $\mathbb{F} = \mathbb{K}(x)$ with the evaluation function (12) and the corresponding o-function from Example 7 by choosing the algebraic number field $\mathbb{K} = \mathbb{Q}(\iota)$. Now take the Laurent polynomial ring $\mathbb{E} = \mathbb{F}\langle \hat{x}_1 \rangle \langle \hat{x}_2 \rangle \langle \hat{x}_3 \rangle \langle \hat{x}_4 \rangle$. Following Lemma 8 we can construct the evaluation function $\hat{\text{ev}}: \mathbb{E} \times \mathbb{N} \rightarrow \mathbb{K}$ for \mathbb{E} with $\hat{\text{ev}}|_{\mathbb{K}(x) \times \mathbb{N}} = \text{ev}$ and $\hat{\text{ev}}(\hat{x}_i, n) = F_i(n)$ for $1 \leq i \leq 4$ where the $F_i(n)$ are given in (4). In particular, we obtain the o-function defined by (15). In the following examples we will work with the evaluation domain $(\mathbb{E}, \hat{\text{ev}})$ in which the product expressions under consideration can be represented formally.

Let \mathbb{K} be a subfield of a ring \mathbb{A} . An evaluation function $\text{ev}: \mathbb{A} \times \mathbb{N} \rightarrow \mathbb{K}$ for \mathbb{A} naturally produces sequences in the commutative ring $\mathbb{K}^{\mathbb{N}}$ with the identity element $\mathbf{1} = (1, 1, 1, \dots)$ with component-wise addition and multiplication. More precisely, we can define the function $\tau: \mathbb{A} \rightarrow \mathbb{K}^{\mathbb{N}}$ with

$$\tau(f) = (\text{ev}(f, 0), \text{ev}(f, 1), \text{ev}(f, 2), \dots). \quad (16)$$

Due to (10) and (11) the map τ can be turned to a ring homomorphism by defining the equivalence relation $(f_n)_{n \geq 0} \equiv (g_n)_{n \geq 0}$ with $f_j = g_j$ for all $j \geq \lambda$ for some $\lambda \in \mathbb{N}$; compare [28]. It is easily seen that the set of equivalence classes $[f]$ with $f \in \mathbb{K}^{\mathbb{N}}$ forms with $[f] + [g] := [f + g]$ and $[f][g] := [fg]$ again a commutative ring with $[1]$ which we will denote by $\mathbf{S}(\mathbb{K})$. In the following we will simply write f instead of $[f]$. In this setting, $\tau: \mathbb{A} \rightarrow \mathbf{S}(\mathbb{K})$ forms a ring homomorphism.

2.2. The ring automorphism – difference rings. So far, we elaborated how sequences can be formulated in a formal ring \mathbb{A} equipped with an evaluation function. Finally, we will introduce in addition a ring automorphism $\sigma: \mathbb{A} \rightarrow \mathbb{A}$ in order to model the shift operator acting on sequences. Such a ring \mathbb{A} equipped with a ring automorphism σ is also called a *difference ring* denoted by (\mathbb{A}, σ) .

In order to construct difference rings iteratively, we will use the notion of difference ring/field extensions. (\mathbb{E}, σ') is called a *difference ring extension* of (\mathbb{A}, σ) if \mathbb{A} is a subring of \mathbb{E} and $\sigma'|_{\mathbb{A}} = \sigma$. If \mathbb{E} and \mathbb{A} are fields, we call such an extension a *difference field extension*. In the following we will need the following type of difference ring extensions (\mathbb{E}, σ) of (\mathbb{A}, σ) ; for more details see [41, 42].

- A *P-extension (product-extension)* if $\mathbb{E} = \mathbb{A}\langle \hat{x} \rangle$ is a ring of Laurent polynomials with $\sigma(\hat{x}) = \hat{\alpha}\hat{x}$ for some unit $\hat{\alpha} \in \mathbb{A}^*$. More precisely, for $f = \sum_{k=l}^r f_k \hat{x}^k$ with $l, r \in \mathbb{Z}$ we have $\sigma'(f) = \sum_{k=l}^r \sigma(f_k) \hat{\alpha}^k \hat{x}^k$. \hat{x} is also called a *P-monomial*.
- An *S-extension (sum-extension)* if $\mathbb{E} = \mathbb{A}[\hat{x}]$ is a polynomial ring with $\sigma(\hat{x}) = \hat{x} + \hat{\beta}$ for some $\hat{\beta} \in \mathbb{A}$. More precisely, for $f = \sum_{k=0}^r f_k \hat{x}^k$ with $r \in \mathbb{N}$ we have $\sigma'(f) = \sum_{k=0}^r \sigma(f_k) (\hat{x} + \hat{\beta})^k$. \hat{x} is also called an *S-monomial*.
- An *A-extension (algebraic extension)* of order $\lambda > 1$ if $\mathbb{E} = \mathbb{A}[z]$ is a ring subject to the relation $z^\lambda = 1$ (i.e., $\text{ord}(z) = \lambda$) with $\sigma(z) = \rho z$ where $\rho \in \mathbb{A}^*$ is a λ th root of unity (i.e., $\rho^\lambda = 1$). z is also called an *A-monomial*.

Since σ' and σ agree on \mathbb{A} , we will not distinguish them anymore. In particular, a *PS-extension* (resp. *AP-extension/APS-extension*) is a *P* or *S*-extension (resp. an *A*-extension or *P*-extension/an *A*-extension, *P*-extension or *S*-extension). More generally we call (\mathbb{E}, σ) a (nested) *P-extension/S-extension/A-extension/PS-extension/AP-extension/APS-extension* of (\mathbb{A}, σ) if it is built by a tower of such extensions over a difference ring (\mathbb{A}, σ) .

Let (\mathbb{E}, σ) be a difference field extension of a difference field (\mathbb{F}, σ) . It is a *P-field extension* (resp. *S-field extension*) if $\mathbb{E} = \mathbb{F}\langle \hat{x} \rangle$ is a rational function and $\sigma(\hat{x}) = \hat{\alpha}\hat{x}$ with $\hat{\alpha} \in \mathbb{F}^*$ (resp. $\sigma(\hat{x}) = \hat{x} + \hat{\beta}$ with $\hat{\beta} \in \mathbb{F}$). More generally, a (nested) *S-field extension/P-field extension/PS-field extension* is a tower of such extensions.

Remark. The quotient field of a (nested) *P-extension/S-extension/PS-extension* of a difference field is a special class of *P-field/S-field/PS-field* extensions (the multiplicands/summands can be chosen only from a subring of the ground field).

Example 10 (Cont. Ex. 9). Consider the difference field (\mathbb{F}, σ) with $\mathbb{F} = \mathbb{K}(x)$ where $\mathbb{K} = \mathbb{Q}(\iota)$ and with the field automorphism $\sigma: \mathbb{F} \rightarrow \mathbb{F}$ defined by $\sigma|_{\mathbb{K}} = \text{id}$

and $\sigma(x) = x + 1$. In the following we call this difference field also the rational difference field. Note that (\mathbb{F}, σ) is an S -field extension of (\mathbb{K}, σ) . In Example 9 we have introduced already the Laurent polynomial ring $\mathbb{E} = \mathbb{F}\langle \hat{x}_1 \rangle \langle \hat{x}_2 \rangle \langle \hat{x}_3 \rangle \langle \hat{x}_4 \rangle$ where the products (4) are represented by \hat{x}_i for $i = 1, 2, 3, 4$ and the evaluation function (20). We can now extend the automorphism σ from \mathbb{F} to \mathbb{E} by a tower of P -extensions with $\sigma(\hat{x}_i) = \hat{\alpha}_i \hat{x}_i$ for $1 \leq i \leq 4$ where

$$\begin{aligned} \hat{\alpha}_1 &= \frac{-13122(x+1)(x+2)}{(x+4)^3}, & \hat{\alpha}_2 &= \frac{26244(x+1)^2(x+3)^2}{(x+4)^2}, \\ \hat{\alpha}_3 &= \frac{\iota(x+1)(x+3)^3}{729(x+6)}, & \hat{\alpha}_4 &= \frac{-162(x+1)(x+3)}{x+6}. \end{aligned} \quad (17)$$

Note that $F_i(n+1) = \hat{\alpha}_i(n) F_i(n)$ for $1 \leq i \leq 4$, i.e., σ acting on \hat{x}_i models the shift operator applied to $F_i(n)$.

Similarly, S -extensions are used to model indefinite nested sums. Since we focus mainly on products, we skip these aspects and refer the reader to [35, 37, 41, 42].

In order to solve the Problem *RPTB* introduced in Section 1, the difference ring/field extensions from above have to be refined. In this regard, we introduce the *set of constants*

$$\text{const}_\sigma \mathbb{A} = \{c \in \mathbb{A} \mid \sigma(c) = c\}$$

of a difference ring (\mathbb{A}, σ) . In general, $\mathbb{K} = \text{const}_\sigma \mathbb{A}$ is a subring of \mathbb{A} that contains \mathbb{Q} as subfield. In particular, if \mathbb{F} is a field, \mathbb{K} is automatically a subfield of \mathbb{F} . In this article we will take care that \mathbb{K} is always a subfield of \mathbb{A} which we will also call the *constant field of* (\mathbb{A}, σ) .

Definition 11. A (nested) Π -extension (resp. Σ -/ R -/ $R\Pi$ -/ $R\Sigma$ -/ $\Sigma\Pi$ -/ $R\Pi\Sigma$ - extension) (\mathbb{E}, σ) of (\mathbb{A}, σ) is a P -extension (resp. S -/ A -/ AP -/ AS -/ SP -/ APS -extension) with $\text{const}_\sigma \mathbb{E} = \text{const}_\sigma \mathbb{A}$. In this case, an A -/ P -/ S -monomial is also called an R -/ Π -/ Σ -monomial. Similarly, a (nested) Π -field extension (resp. (nested) Σ -/ $\Pi\Sigma$ -field extension) is a P -field extension (resp. S -/ PS -field extension) where the constants remain unchanged. Finally, a $\Pi\Sigma$ -field (\mathbb{F}, σ) over \mathbb{K} is a (nested) $\Pi\Sigma$ -field extension of (\mathbb{K}, σ) with $\text{const}_\sigma \mathbb{F} = \text{const}_\sigma \mathbb{K}$.

Example 12. Consider the rational difference field (\mathbb{F}, σ) from Example 10. It is not difficult to see that $\text{const}_\sigma \mathbb{F} = \mathbb{K}$. Consequently, (\mathbb{F}, σ) is a $\Pi\Sigma$ -field over \mathbb{K} .

We remark that these extensions are motivated by Karr's work [18, 19]. More precisely, the Π -field and Σ -field extensions and in particular $\Pi\Sigma$ -fields have been introduced in [18, 19] and explored further, e.g., in [9, 31, 35, 37].

Remark 13. In the following we will restrict to AP -extensions (\mathbb{A}, σ) of a difference field (\mathbb{F}, σ) with $\mathbb{A} = \mathbb{F}\langle x_1 \rangle \dots \langle x_s \rangle [z_1] \dots [z_l]$ where the $\frac{\sigma(x_i)}{x_i} \in \mathbb{F}^*$ for $1 \leq i \leq s$ are P -monomials and the $\frac{\sigma(z_i)}{z_i} \in \text{const}_\sigma \mathbb{F}^*$ for $1 \leq i \leq l$ are A -monomials. One can rearrange the generators in any order and obtains again an AP -extension. For instance, (\mathbb{A}', σ) is an AP -extension of (\mathbb{F}, σ) with $\mathbb{A}' = \mathbb{F}[z_1] \dots [z_l] \langle x_1 \rangle \dots \langle x_s \rangle$. In particular, if $\text{const}_\sigma \mathbb{A} = \text{const}_\sigma \mathbb{F}$ holds then also $\text{const}_\sigma \mathbb{A}' = \text{const}_\sigma \mathbb{F}$ holds. I.e., if (\mathbb{A}, σ) is an $R\Pi$ -extension of (\mathbb{F}, σ) , (\mathbb{A}', σ) is an $R\Pi$ -extension of (\mathbb{F}, σ) .

2.3. The compatibility of ev and σ . Let (\mathbb{A}, σ) be a difference ring with constant field \mathbb{K} . $\text{ev}: \mathbb{A} \times \mathbb{N} \rightarrow \mathbb{K}$ is called an *evaluation function* for (\mathbb{A}, σ) if ev is an

evaluation function for the ring \mathbb{A} and ev and σ satisfy the following compatibility property: for all $f \in \mathbb{A}$ and $l \in \mathbb{Z}$ we have

$$\forall n \geq \lambda : \text{ev}(\sigma^l(f), n) = \text{ev}(f, n + l) \quad (18)$$

for some $\lambda \in \mathbb{N}$. L is called an o^σ -function for ev if L is and o -function for ev and for all $f \in \mathbb{A}$ and $l \in \mathbb{Z}$ with $\lambda = L(f) + \max(0, -l)$ property (18) holds. ev is called *operation bounded* for (\mathbb{A}, σ) if there is such a function L : In particular, ev is called o^σ -computable if ev is a computable function and there is a computable o^σ -function $L: \mathbb{A} \rightarrow \mathbb{N}$ for ev .

Example 14. Consider the rational difference field (\mathbb{F}, σ) with $\mathbb{F} = \mathbb{K}(x)$, $\mathbb{K} = \text{const}_\sigma \mathbb{K}$ and $\sigma(x) = x + 1$. Then (12) is an evaluation function for (\mathbb{F}, σ) and the function L from Example 7 is an o^σ -function.

Using [42, Lemma 5.4 (parts 1,3)] Lemma 8 can be extended to difference rings.

Lemma 15. Let (\mathbb{F}, σ) be a difference field with $\mathbb{K} = \text{const}_\sigma \mathbb{F}$ equipped with an evaluation function $\text{ev}: \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{K}$. Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle [z]$ be an AP-extension of (\mathbb{F}, σ) where the \hat{x}_i with $1 \leq i \leq r$ are P-monomials with $a_i = \frac{\sigma(\hat{x}_i)}{\hat{x}_i}$ and z is an A-monomial with $\rho = \frac{\sigma(z)}{z} \in \mathbb{K}^*$. For $1 \leq i \leq r$, let $l_i \in \mathbb{N}$ such that $\text{ev}(a_i, n) \neq 0$ holds for all $n \geq l_i$. Then $\hat{\text{ev}}: \mathbb{E} \times \mathbb{N} \rightarrow \mathbb{K}$ defined by (13) is an evaluation function for (\mathbb{E}, σ) . If L is an o^σ -function for ev , \hat{L} defined in (15) is an o^σ -function for \hat{L} . If L is computable, then \hat{L} is computable.

Example 16 (Cont. Example 10). Consider the P-extension (\mathbb{E}, σ) of (\mathbb{F}, σ) from Example 10 with $\mathbb{E} = \mathbb{F}\langle \hat{x}_1 \rangle \langle \hat{x}_2 \rangle \langle \hat{x}_3 \rangle \langle \hat{x}_4 \rangle$ and $\sigma(\hat{x}_i) = \hat{\alpha}_i \hat{x}_i$ for $1 \leq i \leq 4$ where the $\hat{\alpha}_i$ are given in (17), and take the evaluation function $\hat{\text{ev}}$ defined in Example 9. Then by Lemma 15 it follows that $\hat{\text{ev}}$ is an evaluation function for (\mathbb{E}, σ) .

It will be convenient to use the following convention. Let (\mathbb{A}, σ) be a difference ring with constant field \mathbb{K} and let ev be an evaluation function for (\mathbb{A}, σ) . We say that a sequence $(F(n))_{n \geq 0}$ is modeled by $a \in \mathbb{A}$ if there exists a $\lambda \in \mathbb{N}$ with $\text{ev}(a, n) = F(n)$ for all $n \geq \lambda$.

Example 17 (Cont. Example 16). For $i = 1, 2, 3, 4$ the sequences $(F_i(n))_{n \geq 0}$ are modeled by x_i , respectively.

Let ev be an evaluation function for (\mathbb{A}, σ) with constant field \mathbb{K} . Then the ring homomorphism $\tau: \mathbb{A} \rightarrow \mathbf{S}(\mathbb{K})$ defined by (16) turns to a difference ring homomorphism.

More precisely, let (\mathbb{B}, σ') be another difference ring. Then a ring homomorphism (resp. injective ring homomorphism) $\lambda: \mathbb{A} \rightarrow \mathbb{B}$ is called a *difference ring homomorphism* (resp. *difference ring embedding*) if for all $f \in \mathbb{A}$ we have $\lambda(\sigma(f)) = \sigma'(\lambda(f))$.

To turn $\tau: \mathbb{A} \rightarrow \mathbf{S}(\mathbb{K})$ to such a difference ring homomorphism, we consider the shift operation $S: \mathbf{S}(\mathbb{K}) \rightarrow \mathbf{S}(\mathbb{K})$ defined by

$$S((a_0, a_1, a_2, \dots)) = (a_1, a_2, \dots).$$

Then it can be easily verified that S forms a ring automorphism and thus $(\mathbf{S}(\mathbb{K}), S)$ forms a difference ring; compare [28]. In particular, due to (18) it follows that the ring homomorphism τ defined by (16) is a difference ring homomorphism, i.e., we have

$$\forall f \in \mathbb{A} : \tau(\sigma(f)) = S(\tau(f)).$$

Furthermore, by (9) it follows that $\tau(c) = \mathbf{c}$ with $\mathbf{c} := (c, c, c, \dots)$ for all $c \in \mathbb{K}$. Such a map will be also called \mathbb{K} -homomorphism.

Definition 18. Let (\mathbb{A}, σ) be a difference ring with constant-field \mathbb{K} . A function $\tau: \mathbb{A} \rightarrow \mathcal{S}(\mathbb{K})$ is called \mathbb{K} -homomorphism (resp. \mathbb{K} -embedding) if it is a difference ring homomorphism (resp. difference ring embedding) where $\tau(c) = \mathbf{c}$ for all $c \in \mathbb{K}$. A \mathbb{K} -homomorphism (resp. \mathbb{K} -embedding) is called o^σ -computable if there is a computable evaluation function $\text{ev}: \mathbb{A} \times \mathbb{N} \rightarrow \mathbb{K}$ with a computable o^σ -function $L: \mathbb{A} \rightarrow \mathbb{N}$ where (8) holds for all $f \in \mathbb{A}$.

Example 19. Consider the rational difference field (\mathbb{F}, σ) with $\mathbb{F} = \mathbb{K}(x)$ and $\sigma(x) = x + 1$ from Example 14 equipped with the evaluation function (12). Then $\tau: \mathbb{F} \rightarrow \mathcal{S}(\mathbb{K})$ given by (16) is a \mathbb{K} -homomorphism. In particular, since any non-zero polynomial in $\mathbb{K}[x]$ has only finitely many roots, $\tau(\frac{p}{q}) = \mathbf{0}$ with $p \in \mathbb{K}[x]$ and $q \in \mathbb{K}[x] \setminus \{0\}$ iff $p = 0$. Thus τ is injective, i.e., it is a \mathbb{K} -embedding.

More generally, we will consider the class of mixed-rational difference fields [8].

Example 20. Take the rational function field $\mathbb{K} = \mathbb{K}'(q_1, \dots, q_v)$ and consider the rational function field $\mathbb{F} = \mathbb{K}(x, y_1, \dots, y_v)$ on top together with the field automorphism $\sigma: \mathbb{F} \rightarrow \mathbb{F}$ defined by $\sigma_{\mathbb{K}} = \text{id}$, $\sigma(x) = x + 1$ and $\sigma(y_i) = q_i y_i$ for $1 \leq i \leq v$. We noted already that $\text{const}_\sigma \mathbb{K}(x) = \mathbb{K}$; see Example 12. It is not too difficult to see that there does not exist a $g \in \mathbb{K}(x)^*$ and $(0, \dots, 0) \neq (m_1, \dots, m_v) \in \mathbb{Z}^v$ with $\sigma(g) = q_1^{m_1} \dots q_v^{m_v} g$. Hence by Proposition 40 below it follows that $\text{const}_\sigma \mathbb{F} = \text{const}_\sigma \mathbb{K}(x) = \mathbb{K}$. In short, (\mathbb{F}, σ) is a $\Pi\Sigma$ -field over \mathbb{K} . (\mathbb{F}, σ) is also called the mixed-rational difference field. Furthermore, for $f = \frac{p}{q}$ with $p, q \in \mathbb{K}[x, y_1, \dots, y_v]$, $q \neq 0$ and p, q being co-prime we define

$$\text{ev}(f, n) = \begin{cases} 0 & \text{if } q(n, q_1^n, \dots, q_v^n) = 0 \\ \frac{p(n, q_1^n, \dots, q_v^n)}{q(n, q_1^n, \dots, q_v^n)} & \text{if } q(n, q_1^n, \dots, q_v^n) \neq 0. \end{cases} \quad (19)$$

By [8, Sec. 3.7] there is a minimal $\delta \in \mathbb{N}$ with $q(n, q_1^n, \dots, q_v^n) \neq 0$ for all $n \geq \delta$. Hence we can define the o^σ -function $L: \mathbb{F} \rightarrow \mathbb{N}$ by $L(f) = \delta$; a z -function $Z: \mathbb{F} \rightarrow \mathbb{N}$ can be defined by $Z(f) = L(pq)$. Finally, consider the difference ring homomorphism $\tau: \mathbb{F} \rightarrow \mathcal{S}(\mathbb{K})$ defined by (16). Suppose that $\tau(f) = \mathbf{0}$ with $f = \frac{p}{q}$. Since $q(n, q_1^n, \dots, q_v^n)$ is non-zero for all $n \geq Z(f)$ and $p(n, q_1^n, \dots, q_v^n)$ is non-zero for all $n \geq Z(f)$ provided that $p \neq 0$, it follows that $p = 0$. Hence τ is injective.

We will restrict for algorithmic reasons to the case that \mathbb{K}' is a rational function field over an algebraic number field. In this case, L and Z are computable by [8, Sec. 3.7]. Summarizing, we obtain a o^σ -computable \mathbb{K} -embedding $\tau: \mathbb{F} \rightarrow \mathcal{S}(\mathbb{K})$.

Example 21 (Cont. Ex. 16). Consider the difference ring (\mathbb{E}, σ) from Example 16 equipped with the evaluation function defined in Example 9 and the corresponding computable o^σ -function L and the computable z -function Z . Thus $\hat{\tau}: \mathbb{E} \rightarrow \mathcal{S}(\mathbb{K})$ defined by $\hat{\tau}(f) = (\hat{\text{ev}}(f, n))_{n \geq 0}$ for $f \in \mathbb{E}$ is a o^σ -computable \mathbb{K} -homomorphism.

So far, we exploited the fact that an evaluation function produces a \mathbb{K} -homomorphism. Later we will use the reverse construction: for a \mathbb{K} -homomorphism of a P -extension there exists an evaluation function that is based on product evaluations. More precisely, [42, Lemma 5.4 (parts 2,3)] provides the following result.

Lemma 22. Let (\mathbb{F}, σ) be a difference field with constant field \mathbb{K} equipped with a z -function $Z: \mathbb{F} \rightarrow \mathbb{N}$. Let (\mathbb{E}, σ) be an AP -extension of (\mathbb{F}, σ) with $\mathbb{E} =$

$\mathbb{F}\langle\hat{x}_1\rangle\dots\langle\hat{x}_r\rangle[z]$ where for $1 \leq i \leq r$ the \hat{x}_i with $\hat{\alpha}_i = \frac{\sigma(\hat{x}_i)}{\hat{x}_i} \in \mathbb{F}^*$ are P -monomials and z with $\rho = \frac{\sigma(z)}{z} \in \mathbb{K}^*$ is an A -monomial of order λ . Suppose that there is a \mathbb{K} -homomorphism $\hat{\tau}: \mathbb{E} \rightarrow \mathbf{S}(\mathbb{K})$ and let $\text{ev}: \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{K}$ be an evaluation function with $\hat{\tau}(f) = (\text{ev}(f, n))_{n \geq 0}$ for $f \in \mathbb{F}$. Then there is an evaluation function $\hat{\text{ev}}: \mathbb{E} \times \mathbb{N} \rightarrow \mathbb{K}$ defined by $\hat{\text{ev}}|_{\mathbb{F} \times \mathbb{N}} = \text{ev}$,

$$\hat{\text{ev}}(\hat{x}_i, n) = \kappa_i \prod_{k=l_i}^n \text{ev}(\hat{\alpha}_i, k-1), \quad 1 \leq i \leq r$$

for some $\kappa_i \in \mathbb{K}^*$ and⁶ $l_i \in \mathbb{N}$, and $\hat{\text{ev}}(z, n) = \langle c \rho^n \rangle_{n \geq 0}$ for some $c \in \mathbb{K}^*$ with $c^\lambda = 1$ such that $\hat{\tau}(f) = \langle \hat{\text{ev}}(f, n) \rangle_{n \geq 0}$ holds for all $f \in \mathbb{E}$. Furthermore, if there is a computable o^σ -function $L: \mathbb{F} \rightarrow \mathbb{N}$ for ev and Z is computable, there is a computable o^σ -function $\bar{L}: \mathbb{E} \rightarrow \mathbb{N}$ for $\hat{\text{ev}}$. In particular, $c \in \mathbb{K}^*$, and by choosing $l_i = \max(Z(\hat{\alpha}_i) - 1, L(\hat{\alpha}_i))$ for $1 \leq i \leq r$ the $\kappa_i \in \mathbb{K}^*$ can be computed.

2.4. The problem description in the setting of $R\Pi$ -extensions. Consider the products given in (1) where the multiplicands $f_1(k), \dots, f_r(k)$ can be modeled in a difference field (\mathbb{F}, σ) with constant field \mathbb{K} . This means that there is an evaluation function $\bar{\text{ev}}: \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{K}$ with an o^σ -function $\bar{L}: \mathbb{F} \rightarrow \mathbb{N}$ such that we can find $\hat{f}_1, \dots, \hat{f}_r \in \mathbb{F}^*$ with the following property: for all $1 \leq i \leq r$ we have $\bar{\text{ev}}(\hat{f}_i, n) = f_i(n)$ for all $n \geq l_i$ with $l_i \geq \bar{L}(\hat{f}_i)$. Then we can model also the products of (1) in a P -extension (\mathbb{E}, σ) of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle\hat{x}_1\rangle\dots\langle\hat{x}_r\rangle$ and $\sigma(\hat{x}_i) = \hat{\alpha}_i \hat{x}_i$ where $\hat{\alpha}_i = \sigma(\hat{f}_i)$: By Lemma 8 we can define the evaluation function $\text{ev}: \mathbb{E} \times \mathbb{N} \rightarrow \mathbb{K}$ with $\text{ev}|_{\mathbb{F} \times \mathbb{N}} = \bar{\text{ev}}$ and

$$\text{ev}(\hat{x}_i, n) = F_i(n) = \prod_{k=l_i}^n f_i(k). \quad (20)$$

In addition, we obtain an o^σ -function L for ev . Finally, we take the \mathbb{K} -homomorphism $\tau: \mathbb{E} \rightarrow \mathbf{S}(\mathbb{K})$ defined by (16). For further considerations we require in addition that $\tau|_{\mathbb{F}}$ is a \mathbb{K} -embedding. If we focus on algorithmic aspects, we assume that the \mathbb{K} -embedding τ is o^σ -computable.

As elaborated in the next remark, a finite set of mixed-hypergeometric products (see Definition 1) can be modeled in such a P -extension.

Remark 23 (Representation of mixed-hypergeometric products). *Take the rational function field $\mathbb{K} = \mathbb{K}'(q_1, \dots, q_v)$ and consider the mixed-rational difference field (\mathbb{F}, σ) with $\mathbb{F} = \mathbb{K}(x, y_1, \dots, y_v)$ where $\sigma: \mathbb{F} \rightarrow \mathbb{F}$ is defined by $\sigma|_{\mathbb{K}} = \text{id}$, $\sigma(x) = x + 1$ and $\sigma(y_i) = q_i y_i$ for $1 \leq i \leq v$. Note that (\mathbb{F}, σ) is a $\Pi\Sigma$ -field over \mathbb{K} . Furthermore take its evaluation function $\bar{\text{ev}}: \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{K}$ with an o^σ -function $\bar{L}: \mathbb{F} \rightarrow \mathbb{N}$; see Example 20. Suppose that we are given the mixed-hypergeometric products $F_1(n), \dots, F_r(n)$ with*

$$F_i(n) = \prod_{k=l_i}^n f_i(k, q_1^k, \dots, q_v^k)$$

for $1 \leq i \leq r$ where⁷ $f_i(x, y_1, \dots, y_v) \in \mathbb{F}^*$ and the numerator and denominator of $f_i(k, q_1^k, \dots, q_v^k)$ do not evaluate to zero for all $k \geq l_r \in \mathbb{N}$. By construction we

⁶Note that $\hat{\text{ev}}(\hat{x}_i, n) \neq 0$ for all $n \geq l_i$ by part (1) of Lemma 6.

⁷To fulfill the property $f_i \in \mathbb{F}^*$, the variables q_1, \dots, q_v and y_1, \dots, y_v and the field below \mathbb{K}' have to be set up accordingly.

can take $\hat{f}_r := f_r$ and get $\bar{\text{ev}}(\hat{f}_r, k) = f_r(k, q_1^k, \dots, q_v^k)$. Now take the P -extension (\mathbb{E}, σ) of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle$ and $\sigma(\hat{x}_i) = \hat{\alpha}_i \hat{x}_i$ where $\hat{\alpha}_i = \sigma(\hat{f}_i) = \hat{f}_i(x+1, q_1 y_1, \dots, q_r y_r)$; note that $\text{ev}(\hat{\alpha}_i, n) = \text{ev}(\sigma(\hat{f}_i), n) = \text{ev}(\hat{f}_i, n+1) = \hat{f}_i(n+1, q_1^{n+1}, \dots, q_v^{n+1})$. By Lemma 15 we can extend the evaluation function $\bar{\text{ev}}$ from (\mathbb{F}, σ) to (\mathbb{E}, σ) with $\text{ev}(\hat{x}_i, n) = \prod_{k=l_i}^n f_i(k, q_1^k, \dots, q_v^k)$; similarly one can extend \bar{L} to the σ^σ -function $L: \mathbb{E} \rightarrow \mathbb{N}$. As elaborated in Example 20, $\tau: \mathbb{E} \rightarrow \mathbf{S}(\mathbb{K})$ defined by (16) is a \mathbb{K} -embedding. If we restrict to the case that the subfield \mathbb{K}' of \mathbb{K} is a rational function field over an algebraic number field, all ingredients are computable. In particular, τ turns to a σ^σ -computable \mathbb{K} -embedding.

Given the above construction, we will consider the following problem.

Problem DR (Difference ring Representation): *Given a computable difference field (\mathbb{F}, σ) equipped with a computable evaluation function $\bar{\text{ev}}$ and computable σ^σ -function \bar{L} and given a P -extension (\mathbb{E}, σ) of (\mathbb{F}, σ) with a computable evaluation function ev with $\text{ev}|_{\mathbb{F} \times \mathbb{N}} = \bar{\text{ev}}$ and a computable σ^σ -function L as described above⁸. Find*

- an AP -extension (\mathbb{H}, σ) of (\mathbb{E}, σ) with

$$\mathbb{H} = \mathbb{F}\langle t_1 \rangle \dots \langle t_s \rangle [z_1] \dots [z_l] \quad (21)$$

where the t_i for $1 \leq i \leq s$ are P -monomials with $\alpha_i = \frac{\sigma(t_i)}{t_i} \in \mathbb{F}^*$ and the z_i for $1 \leq i \leq l$ are A -monomials with $\rho_i = \frac{\sigma(z_i)}{z_i} \in \mathbb{K}^*$ of order $d_i > 1$;

- a computable evaluation function $\text{ev}': \mathbb{H} \times \mathbb{N} \rightarrow \mathbb{K}$ for (\mathbb{H}, σ) with a computable σ^σ -function L' where ev' is defined by $\text{ev}'|_{\mathbb{F} \times \mathbb{N}} = \text{ev}|_{\mathbb{F} \times \mathbb{N}} (= \bar{\text{ev}})$, $\text{ev}'(t_i, n) = \prod_{k=l'_i}^n \text{ev}(\alpha_i, k-1)$ with $l'_i \in \mathbb{N}$ for $1 \leq i \leq s$, and $\text{ev}'(z_i, n) = \rho_i^n$ for $1 \leq i \leq l$;
- a computable **surjective** difference ring homomorphism $\lambda: \mathbb{E} \rightarrow \mathbb{H}$

such that

- (1) $\tau': \mathbb{E} \rightarrow \mathbf{S}(\mathbb{K})$ defined by $\tau'(f) = (\text{ev}'(f, n))_{n \geq 0}$ is a \mathbb{K} -embedding;
- (2) for all $f \in \mathbb{E}$ we have $\tau(f) = \tau'(\lambda(f))$, i.e., the following diagram commutes:

$$\begin{array}{ccc} \mathbb{E} & \xrightarrow{\lambda} & \mathbb{H} \\ & \searrow \tau & \downarrow \tau' \\ & & \mathbf{S}(\mathbb{K}). \end{array} \quad (22)$$

We emphasize that a solution of Problem *DR* solves also Problem *RPTB*. More precisely, for $1 \leq i \leq r$ we can take $g_i := \lambda(\hat{x}_i) \in \mathbb{H}$ and get

$$\text{ev}'(g_i, n) = \text{ev}'(\lambda(\hat{x}_i), n) = \text{ev}(\hat{x}_i, n) = F_i(n)$$

for all $n \geq \max(L(f_i), L'(g_i))$. Thus $F_i(n)$ is modeled by g_i in (\mathbb{E}, σ) . In particular, the evaluation function provides the full information to obtain an alternative production expression that evaluates to $F_i(n)$ (essentially, one replaces in g_i the t_j for $1 \leq j \leq s$ by the products $\prod_{k=l'_j}^n \text{ev}(\alpha_j, k-1)$ and the z_j for $1 \leq j \leq l$ by ρ_j^n respectively). This establishes part (i) of Problem *RPTB*. Furthermore, by Remark 13 we can reorder the generators in \mathbb{E} and get the AP -extension (\mathbb{E}', σ)

⁸Note that generators \hat{x}_i in \mathbb{E} represent products with no extra properties: in particular, all algebraic relations induced by their sequence evaluations are ignored.

of (\mathbb{F}, σ) with $\mathbb{E}' = \mathbb{F}[z_1] \dots [z_l] \langle t_1 \rangle \dots \langle t_s \rangle$. Furthermore, we observe that the difference ring $(\tau(\mathbb{E}), S)$ is contained in $(\mathbf{S}(\mathbb{K}), S)$ (as a subdifference ring) and is isomorphic to (\mathbb{E}, σ) . Thus $\tau(\mathbb{E}') = \tau(\mathbb{F}[z_1] \dots [z_l] \langle \tau'(t_1) \rangle \dots \langle \tau'(t_s) \rangle)$ forms a ring of Laurent polynomials, i.e., the sequences $\tau'(t_i) = (\prod_{k=l'_i}^n \text{ev}(\alpha_i, k-1))_{n \geq 0}$ are algebraically independent over the ring $\tau(\mathbb{F}[z_1] \dots [z_l])$ (which is a subring of the ring of sequences $\mathbf{S}(\mathbb{K})$). Hence also part (ii) of Problem *RPTB* is tackled.

The solution of Problem *DR* is strongly related with the following result which is a special case of [42, Thm. 5.14]; this result is also connected to [44, 36, 17].

Theorem 24. *Let (\mathbb{H}, σ) with (21) be an AP-extension of a difference field (\mathbb{F}, σ) with $\mathbb{K} = \text{const}_\sigma \mathbb{F}$ as supposed in Problem *DR*. Furthermore, let $\tau: \mathbb{H} \rightarrow \mathbf{S}(\mathbb{K})$ be a \mathbb{K} -homomorphism where $\tau|_{\mathbb{F}}$ is injective. Then $\text{const}_\sigma \mathbb{E} = \mathbb{K}$ iff τ is injective.*

Consequently property (1) in Problem *DR* can be dropped by imposing that $\text{const}_\sigma \mathbb{H} = \text{const}_\sigma \mathbb{F}$, i.e., by taking care that (\mathbb{H}, σ) is an *RPII*-extension of (\mathbb{F}, σ) . Precisely this construction for a solution of Problem *DR* has been carried out in [32, 39] for hypergeometric products, has been extended to a complete algorithm for mixed-hypergeometric products in [23], and has been generalized further for nested products in [24]. However, these approaches usually find a difference ring homomorphism λ that is not surjective.

In this article we will follow the same tactic to solve Problem *DR* for single nested products such that λ is always surjective. Note that in concrete examples the cases $s = 0$ or $l = 0$ might arise, i.e., no Π -monomials or no *R*-monomials are needed. E.g., if (\mathbb{E}, σ) itself is a Π -extension of (\mathbb{F}, σ) , one can solve Problem *DR* by taking $\mathbb{H} = \mathbb{E}$, $\lambda = \text{id}$ and $\tau' = \tau$; note that in this special case λ is even bijective. Otherwise, we will show in Theorem 69 below that we can solve Problem *DR* with a surjective λ and an *RPII*-extension (\mathbb{H}, σ) of (\mathbb{F}, σ) with (21) where $s \geq 0$ and $l \in \{0, 1\}$ (i.e., at most one *A*-monomial is needed) such that

- the number s of Π -monomials is minimal,
- the *R*-monomial $z := z_1$ is introduced only if it is necessary,
- and if it is necessary, the order $d := d_1$ of z is minimal⁹.

Example 25. *Recall the following naive constructions from Examples 7, 9, 10, 16 and 21 to represent the products (4) in a difference ring. We take the rational difference field $(\mathbb{K}(x), \sigma)$ with $\sigma(x) = x+1$ and $\text{const}_\sigma \mathbb{K}(x) = \mathbb{K} = \mathbb{Q}(\iota)$, which is a $\Pi\Sigma$ -field over \mathbb{K} . Furthermore we construct the *P*-extension (\mathbb{E}, σ) of $(\mathbb{K}(x), \sigma)$ with $\mathbb{E} = \mathbb{K}(x) \langle \hat{x}_1 \rangle \langle \hat{x}_2 \rangle \langle \hat{x}_3 \rangle \langle \hat{x}_4 \rangle$ where $\sigma(\hat{x}_i) = \hat{\alpha}_i \hat{x}_i$ for $1 \leq i \leq 4$ and (17) as introduced in Example 65. Further, we take the evaluation function $\hat{\text{ev}}: \mathbb{E} \times \mathbb{N} \rightarrow \mathbb{K}$ introduced in Example 9 (ev replaced by $\hat{\text{ev}}$) and define the \mathbb{K} -homomorphism $\hat{\tau}: \mathbb{E} \rightarrow \mathbf{S}(\mathbb{K})$ by $\hat{\tau}(f) = (\hat{\text{ev}}(f, n))_{n \geq 0}$. Then based on our main results in Theorem 69 below we can solve Problem *DR*. Namely, as will be carried out in Example 70 below we can construct¹⁰ the *RPII*-extension (\mathbb{H}, σ) of $(\mathbb{K}(x), \sigma)$ with $\mathbb{H} = \mathbb{K}(x) \langle x_3 \rangle \langle x_4 \rangle [z]$ and*

$$\sigma(x_3) = -\frac{\iota(x+4)^6}{9(x+1)(x+2)^2(x+3)(x+6)} x_3, \quad \sigma(x_4) = -\frac{162(x+1)(x+3)}{x+6} x_4, \quad \sigma(z) = -z.$$

⁹ Note that by Proposition 43 given below a difference ring generated by a finite set of *R*-monomials z'_1, \dots, z'_l is isomorphic to a difference ring generated by only one *R*-monomial z with $\text{ord}(z) = \text{lcm}(\text{ord}(z'_1), \dots, \text{ord}(z'_l)) = \text{ord}(z'_1) \dots \text{ord}(z'_l)$. Hence claiming that the order $d = \text{ord}(z)$ is optimal means that among all solutions of Problem *DR* (λ need not to be surjective) in a difference ring with the *A*-monomials z'_1, \dots, z'_l the order d of z is smaller or equal to $\text{ord}(z'_1) \dots \text{ord}(z'_l)$.

¹⁰In order to fit the specification in Problem *DR*, we set $t_1 := x_3$ and $t_2 := x_4$ and $z_1 := z$.

Further, we can construct the evaluation function $\text{ev}' : \mathbb{H} \times \mathbb{N} \rightarrow \mathbb{K}$ for (\mathbb{H}, σ) with

$$\text{ev}'(x_3, n) = \prod_{k=1}^n \frac{-\iota(3+k)^6}{9k(1+k)^2(2+k)(5+k)}, \quad \text{ev}'(x_4, n) = \prod_{k=1}^n \frac{-162k(2+k)}{5+k}, \quad \text{ev}'(z, n) = (-1)^n. \quad (23)$$

Note that the \mathbb{K} -homomorphism $\tau' : \mathbb{H} \rightarrow \mathbf{S}(\mathbb{K})$ defined by $\tau'(f) = (\text{ev}'(f, n))_{n \geq 0}$ is injective by Theorem 24. In addition we obtain in Example 70 below the surjective difference ring homomorphism $\hat{\lambda} : \mathbb{E} \rightarrow \mathbb{H}$ defined by $\hat{\lambda}|_{\mathbb{K}(x)} = \text{id}$ and

$$\begin{aligned} \hat{\lambda}(\hat{x}_1) &= \frac{5(x+1)^2(x+2)^5(x+3)^8x_4z}{52488(x+4)(x+5)x_3^2} & \hat{\lambda}(\hat{x}_2) &= \frac{1}{400}(x+4)^2(x+5)^2x_4^2 \\ \hat{\lambda}(\hat{x}_3) &= \frac{2754990144(x+4)^2(x+5)^2x_3^3}{25(x+1)^4(x+2)^{10}(x+3)^{16}} & \hat{\lambda}(\hat{x}_4) &= x_4 \end{aligned} \quad (24)$$

such that $\hat{\tau} = \tau' \circ \hat{\lambda}$ holds. Due to our main result stated in Theorem 69 below it will follow that the number $s = 2$ of the Π -monomials and the order $\lambda = 2$ of the R -monomial z are optimal among all possible solutions of Problem DR (where λ is not necessarily surjective). The construction implies that $\hat{\text{ev}}$ can be given in the following alternative form:

$$\begin{aligned} \hat{\text{ev}}(\hat{x}_1, n) &= \frac{5(1+n)^2(2+n)^5(3+n)^8}{52488(4+n)(5+n)} (-1)^n \prod_{k=1}^n -\frac{162k(2+k)}{5+k} \left(\prod_{k=1}^n -\frac{i(3+k)^6}{9k(1+k)^2(2+k)(5+k)} \right)^{-2}, \\ \hat{\text{ev}}(\hat{x}_2, n) &= \frac{(4+n)^2(5+n)^2}{400} \left(\prod_{k=1}^n -\frac{162k(2+k)}{5+k} \right)^2, \\ \hat{\text{ev}}(\hat{x}_3, n) &= \frac{2754990144(4+n)^2(5+n)^2}{25(1+n)^4(2+n)^{10}(3+n)^{16}} \left(\prod_{k=1}^n -\frac{\iota(3+k)^6}{9k(1+k)^2(2+k)(5+k)} \right)^3, \\ \hat{\text{ev}}(\hat{x}_4, n) &= \prod_{k=1}^n -\frac{162k(2+k)}{5+k} \end{aligned} \quad (25)$$

which is precisely (6). Furthermore, τ' is a difference ring embedding which implies that $\tau'(\mathbb{K}[z]) \langle (\text{ev}'(x_3, n))_{n \geq 0} \rangle \langle (\text{ev}'(x_4, n))_{n \geq 0} \rangle$ with ev' defined in (23) forms a Laurent polynomial ring with coefficients from the subring $\tau'(\mathbb{F}[z])$ of $\mathbf{S}(\mathbb{K})$.

But even more will be derived. By the first isomorphism theorem we get the ring isomorphism $\mu : \mathbb{E}/\ker(\lambda) \rightarrow \mathbb{H}$ defined by $\mu(f + I) = \lambda(f)$. Since $\ker(\lambda)$ is a reflexive difference ideal (i.e., $\sigma^k(f) \in \ker(\lambda)$ for all $k \in \mathbb{Z}$ and $f \in \ker(\lambda)$) it follows that $\sigma' : \mathbb{E}/\ker(\lambda) \rightarrow \mathbb{E}/\ker(\lambda)$ with $\sigma'(f + I) := \sigma(f) + I$ forms a ring automorphism; compare [13]. In particular, μ turns into a difference ring isomorphism between $(\mathbb{E}/\ker(\lambda), \sigma')$ and (\mathbb{H}, σ) . As a bonus we have

$$I := \ker(\lambda) = \ker(\tau) \quad (26)$$

which follows by the following lemma (by setting $\mathbb{S} = \mathbf{S}(\mathbb{K})$).

Lemma 26. *Let \mathbb{E} , \mathbb{H} and \mathbb{S} be rings with a ring homomorphism $\tau : \mathbb{E} \rightarrow \mathbb{S}$ and a ring embedding $\tau' : \mathbb{H} \rightarrow \mathbb{S}$. If $\lambda : \mathbb{E} \rightarrow \mathbb{H}$ is a ring homomorphism with $\tau'(\lambda(a)) = \tau(a)$ for all $a \in \mathbb{E}$, then $\ker(\lambda) = \ker(\tau)$.*

Proof. Suppose that λ is a ring homomorphism as claimed in the lemma and let $a \in \mathbb{E}$. If $\lambda(a) = 0_{\mathbb{H}}$, then $0_{\mathbb{S}} = \tau'(0_{\mathbb{H}}) = \tau'(\lambda(a)) = \tau(a)$. Conversely, if $\tau(a) = 0_{\mathbb{S}}$, then $\tau'(\lambda(a)) = 0_{\mathbb{S}}$. Since τ' is injective and $\tau'(0_{\mathbb{H}}) = 0_{\mathbb{S}}$, $\lambda(a) = 0_{\mathbb{H}}$. \square

Since τ' is injective by construction, we finally obtain the following difference ring isomorphisms:

$$(\mathbb{E}/\ker(\tau), \sigma') = (\mathbb{E}/\ker(\lambda), \sigma') \simeq (\mathbb{H}, \sigma) \simeq (\tau'(\mathbb{H}), S). \quad (27)$$

In addition, we will elaborate in Theorem 69 that one can compute explicitly a finite set of generators that span the difference ideal (26). This means that we obtain the full information of all the algebraic relations of the sequences $\tau(\hat{x}_1), \dots, \tau(\hat{x}_r)$. In particular, the corresponding mappings in (27) can be carried out explicitly.

Example 27 (Cont. Ex. 25). *In Example 70 (based on Theorem 69) we will get*

$$\begin{aligned} \ker(\hat{\tau}) = \ker(\hat{\lambda}) = \left\langle \frac{\hat{x}_2}{\hat{x}_4^2} - \frac{1}{400}(4+x)^2(5+x)^2, \right. \\ \left. \frac{\hat{x}_2^2 \hat{x}_4^2}{\hat{x}_1^6 \hat{x}_3^4} - \frac{1}{4199040x}(1+x)^4(2+x)^{10}(3+x)^{16}(4+x)^2(5+x)^2 \right\rangle_{\mathbb{E}}. \end{aligned} \quad (28)$$

Note that this yields (8) with (7).

As already indicated in Remark 23, this algorithmic toolbox is applicable for the mixed-rational difference field (\mathbb{F}, σ) given in Example 20. More generally, we will show in Theorem 69 below that we obtain a complete algorithm for Problem DR if the ground field (\mathbb{F}, σ) with $\mathbb{K} = \text{const}_{\sigma}\mathbb{F}$ satisfies various (algorithmic) properties. These properties (see Assumption 28) will be explored further in the next section.

3. REQUIRED PROPERTIES OF THE UNDERLYING DIFFERENCE FIELD

For our proposed strategy to solve Problem DR (see Subsection 2.4) we will rely on the following properties of the ground field (\mathbb{F}, σ) .

Assumption 28. *(Required properties of the ground field (\mathbb{F}, σ) for Problem DR):*

- (1) (\mathbb{F}, σ) is computable: the addition, multiplication, the inversion of elements in \mathbb{F} , and the automorphism σ are computable.
- (2) There is an σ -computable difference ring embedding $\tau: \mathbb{F} \rightarrow \mathcal{S}(\mathbb{K})$ together with a computable z -function; see Definitions 5 and 18 from above.
- (3) (\mathbb{F}, σ) is radical-stable; see Definition 45 below.
- (4) One can solve homogeneous first-order difference equations in (\mathbb{F}, σ) : given $w \in \mathbb{F}^*$, one can compute, if it exists, a $g \in \mathbb{F}^*$ with $\sigma(g) - wg = 0$.
- (5) For $\alpha_1, \dots, \alpha_r \in \mathbb{F}^*$ one can compute a \mathbb{Z} basis of $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$; see Definition 37 below.

In the following we will elaborate further details concerning these properties. In particular, we will show the following result in Subsection 3.5.

Theorem 29. *Let (\mathbb{F}, σ) be a mixed rational difference field where the constant field is built by a rational function field over an algebraic number field. Then (\mathbb{F}, σ) satisfies the properties listed in Assumption 28.*

3.1. Constant stability. Note that for any $k \in \mathbb{N}$ we have $\text{const}_\sigma \mathbb{F} \subseteq \text{const}_{\sigma^k} \mathbb{F}$. In the following we will often assume that the two sets are equal; compare [39, 42].

Definition 30. A difference ring (resp. field) (\mathbb{A}, σ) is called constant-stable if $\text{const}_{\sigma^k} \mathbb{A} = \text{const}_\sigma \mathbb{A}$ for all $k \in \mathbb{N}$.

We will show in Proposition 31 below that a nested $\Pi\Sigma$ -extension is constant-stable if the ground field is constant-stable. Here we will utilize

Lemma 31. Let $(\mathbb{F}(t), \sigma)$ be a $\Pi\Sigma$ -field extension of (\mathbb{F}, σ) with $\sigma(t) = \alpha t + \beta$ ($\alpha = 1$, or $\alpha \in \mathbb{F}^*$ and $\beta = 0$). Then the following holds.

- (1) If $a \in \mathbb{F}[t]$ is monic and irreducible, then: $\gcd(\sigma^m(a), a) = 1$ for all $m \geq 1$ if and only if $\beta \neq 0$ or $a \neq t$.
- (2) Suppose that $a \in \mathbb{F}[t]$ is monic and irreducible with $\beta \neq 0$ or $a \neq t$. Then for any irreducible $b \in \mathbb{F}[t]$ there is no $m \in \mathbb{Z}$ with $\gcd(\sigma^m(a), b) \neq 1$ or there is precisely one $m \in \mathbb{Z}$ with $\gcd(\sigma^m(a), b) = 1$.
- (3) If $a \in \mathbb{F}(t) \setminus \mathbb{F}$ and $m \geq 1$, then $a \sigma(a) \dots \sigma^m(a) \notin \mathbb{F}$.
- (4) If (\mathbb{F}, σ) is constant-stable, then $(\mathbb{F}(t), \sigma)$ is constant-stable.

Proof. (1) This follows by [18, 9]; see also [31, Theorem 2.2.4].

(2) Let a be monic and irreducible as stated above and suppose that there is an irreducible $b \in \mathbb{F}[t]$ with $\gcd(\sigma^m(a), b) \neq 1$ and $\gcd(\sigma^n(a), b) \neq 1$ for some $0 \leq m < n$. Then $b = u \sigma^m(a)$ and $b = v \sigma^n(a)$ for some $u, v \in \mathbb{F}^*$. Thus $\sigma^m(a) = \frac{v}{u} \sigma^n(a)$ and hence $a = \sigma^{-m}(\frac{v}{u}) \sigma^{n-m}(a)$. By part (1), it follows that $n = m$.

(3) Define $h = a \sigma(a) \dots \sigma^m(a)$. If t is a Π -monomial (i.e., $\beta = 0$) and $a = bt^r$ for some $b \in \mathbb{F}$ and $r \in \mathbb{Z}$, we get $h = qt^{mr}$ for some $q \in \mathbb{F}^*$ and thus $h \notin \mathbb{F}$. Otherwise, by part (2) of our lemma we can take a monic irreducible $f \in \mathbb{F}[t]$ (which is not t if $\beta = 0$) that arise in a such that for any irreducible polynomial g in a there is no $m \geq 1$ with $\gcd(\sigma^m(f), g) \neq 1$ (If there are several irreducible factors $f_1, f_2 \in \mathbb{F}[t]$ in a with $\sigma^m(f_1) = u f_2$ where $u \in \mathbb{F}^*$ and $m \in \mathbb{Z} \setminus \{0\}$, we take that one which is related to the others only by positive shifts m). Thus f occurs in a , but not in the elements $\sigma(a), \sigma^2(a), \dots, \sigma^m(a)$. Therefore f cannot cancel in h and it follows that $h \notin \mathbb{F}$.

(4) Let $a \in \mathbb{F}(t)$ and suppose that $\sigma^m(a) = a$ for some $m \geq 2$. If $a \in \mathbb{F}$, then $a \in \text{const}_\sigma \mathbb{F}$ by assumption. Otherwise if $a \notin \mathbb{F}$, define $h := a \sigma(a) \dots \sigma^{m-1}(a)$. By part (3) it follows that $h \notin \mathbb{F}$. However, $\frac{\sigma(h)}{h} = \frac{\sigma^m(a)}{a} = 1$ and hence $h \in \text{const}_\sigma \mathbb{F}(t) = \text{const}_\sigma \mathbb{F} \subseteq \mathbb{F}$, a contradiction. Summarizing, $\text{const}_{\sigma^m} \mathbb{F}(t) \subseteq \text{const}_\sigma \mathbb{F}(t)$ and thus equality holds. \square

Applying part (4) of Lemma 31 iteratively we obtain

Proposition 32. Let (\mathbb{E}, σ) be a (nested) $\Pi\Sigma$ -field extension of (\mathbb{F}, σ) . If (\mathbb{F}, σ) is constant-stable, then (\mathbb{E}, σ) is constant-stable.

We note that a difference field (\mathbb{K}, σ) with $\sigma = \text{id}$ is trivially constant-stable. Thus we rediscover the following result of [18].

Corollary 33. A $\Pi\Sigma$ -field is constant-stable.

In particular, one can enhance Proposition 32 to the following ring-version.

Corollary 34. Let (\mathbb{E}, σ) be a $\Pi\Sigma$ -extension of a difference field (\mathbb{F}, σ) . If (\mathbb{F}, σ) is constant-stable, (\mathbb{E}, σ) is constant-stable.

Proof. Let $\mathbb{E} = \mathbb{F}\langle t_1 \rangle \dots \langle t_e \rangle [s_1] \dots [s_l]$ where the t_i are Π -monomials and the s_i are Σ -monomials. Consider the PS -field extension (\mathbb{H}, σ) of (\mathbb{F}, σ) with $\mathbb{H} = \mathbb{F}(t_1) \dots (t_e)(s_1) \dots (s_l)$ in which (\mathbb{E}, σ) is contained as sub-difference ring of (\mathbb{H}, σ) . By Prop. 40 $\text{const}_\sigma \mathbb{H} = \text{const}_\sigma \mathbb{F}$ and by Prop. 32 (\mathbb{H}, σ) is constant-stable. Thus for any integer $m > 0$, $\text{const}_\sigma \mathbb{F} = \text{const}_\sigma \mathbb{H} = \text{const}_{\sigma^m} \mathbb{H} \supseteq \text{const}_{\sigma^m} \mathbb{E} \supseteq \text{const}_\sigma \mathbb{E} = \text{const}_\sigma \mathbb{F}$ and hence $\text{const}_{\sigma^m} \mathbb{E} = \text{const}_\sigma \mathbb{E} (= \text{const}_\sigma \mathbb{F})$. \square

Later we assume that there is a \mathbb{K} -embedding $\tau: \mathbb{F} \rightarrow \mathbf{S}(\mathbb{K})$ of a difference field (\mathbb{F}, σ) with constant field \mathbb{K} . In this case we can specialize [42, Lemma 5.12] to

Lemma 35. *Let (\mathbb{F}, σ) be a difference field with $\mathbb{K} = \text{const}_\sigma \mathbb{F}$. If there is a \mathbb{K} -embedding $\tau: \mathbb{F} \rightarrow \mathbf{S}(\mathbb{K})$, then (\mathbb{F}, σ) is constant-stable.*

3.2. The shape of solutions of first-order homogeneous equations. Suppose we are given a difference field (\mathbb{F}, σ) with $w \in \mathbb{F}^*$. Then at various places in the article we will use the fact that one can predict the shape of the solution g of a difference equation $\sigma(g) - wg = 0$ if g is from a certain class of $R\Pi$ -extensions. More precisely, applying [41, Thm. 2.22] with [41, Cor. 4.15] yields

Proposition 36. *Let (\mathbb{F}, σ) be a difference field with constant field \mathbb{K} , and let (\mathbb{E}, σ) be an $R\Pi$ -extension of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle [z_1] \dots [z_l]$ where for $1 \leq i \leq r$ the x_i with $\frac{\sigma(x_i)}{x_i} \in \mathbb{F}\langle x_1 \rangle \dots \langle x_{i-1} \rangle^*$ are Π -monomials and for $1 \leq i \leq l$ the z_i with $\frac{\sigma(z_i)}{z_i} \in \mathbb{K}^*$ are R -monomials. If there are $g \in \mathbb{E} \setminus \{0\}$ and $w \in \mathbb{F}^*$ with $\sigma(g) = wg$, then*

$$g = h x_1^{m_1} \dots x_r^{m_r} z_1^{n_1} \dots z_l^{n_l}$$

with $m_1, \dots, m_r \in \mathbb{Z}$ and $n_1, \dots, n_l \in \mathbb{N}$ with $0 \leq n_i < \text{ord}(z_i)$ for $1 \leq i \leq l$.

3.3. Characterizations of $R\Pi$ -extensions. We start with the following

Definition 37 ([18]). *Let (\mathbb{F}, σ) be a difference field. For $\alpha_1, \dots, \alpha_r \in \mathbb{F}^*$,*

$$M((\alpha_1, \dots, \alpha_r), \mathbb{F}) = \{(n_1, \dots, n_r) \in \mathbb{Z}^r \mid \exists g \in \mathbb{F}^* : \alpha_1^{n_1} \dots \alpha_r^{n_r} = \frac{\sigma(g)}{g}\}.$$

Note that $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$ is a submodule of \mathbb{Z}^r over \mathbb{Z} . As a consequence, it is finitely generated and has a basis of rank $\leq r$. Due to [32, Thm. 3.2 and 3.5] (based on [18, 15]) such a basis can be calculated for $\Pi\Sigma$ -fields.

Proposition 38. *Let (\mathbb{F}, σ) be a $\Pi\Sigma$ -field over \mathbb{K} where \mathbb{K} is built by a rational function field over an algebraic number field. Then a basis of $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$ for $\alpha_1, \dots, \alpha_r \in \mathbb{F}^*$ can be computed.*

In the following we will elaborate a characterization of single-nested $R\Pi$ -extensions using the notion given in Definition 37. For one Π -monomial we start with

Proposition 39. ([41, Thm. 2.12.(2)]) *Let $(\mathbb{A}\langle t \rangle, \sigma)$ be a P -extension of a difference ring (\mathbb{A}, σ) with $\sigma(t) = at$. Then this is a Π -extension (i.e., $\text{const}_\sigma \mathbb{A}\langle t \rangle = \text{const}_\sigma \mathbb{A}$) iff there are no $n \in \mathbb{Z} \setminus \{0\}$ and $g \in \mathbb{A} \setminus \{0\}$ with $\sigma(g) = a^n t$.*

For nested Π -extensions defined over a difference field we will need in addition

Proposition 40. ([23, Lemma 5.1]) *Let (\mathbb{F}, σ) be a difference field with $\alpha_1, \dots, \alpha_r \in \mathbb{F}^*$. Let (\mathbb{E}, σ) be the P -extension of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}(x_1) \dots (x_r)$ and $\sigma(x_i) = \alpha_i x_i$ for $1 \leq i \leq r$ and let¹¹ (\mathbb{H}, σ) be the P -ring extension of (\mathbb{F}, σ) with $\mathbb{H} =$*

¹¹Note that the quotient field of \mathbb{E} is \mathbb{H} . In particular, (\mathbb{H}, σ) is a sub-difference ring of (\mathbb{E}, σ) .

$\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$ and $\sigma(x_i) = \alpha_i x_i$ for $1 \leq i \leq r$. Then the following statements are equivalent.

- (1) $M((\alpha_1, \dots, \alpha_r), \mathbb{F}) = \{\mathbf{0}\}$.
- (2) $\text{const}_\sigma \mathbb{E} = (\mathbb{F}, \sigma)$, i.e., (\mathbb{E}, σ) is a Π -field extension of (\mathbb{F}, σ) .
- (3) $\text{const}_\sigma \mathbb{H} = (\mathbb{F}, \sigma)$, i.e., (\mathbb{H}, σ) is a Π -extension of (\mathbb{F}, σ) .

Next, we will consider the case for several R -monomials. We start with the following simple observations.

Lemma 41. *Let (\mathbb{A}, σ) be a constant-stable difference ring with constant field $\mathbb{K} = \text{const}_\sigma \mathbb{A}$. Then there are no $\gamma \in \mathbb{A} \setminus \{0\}$ and no root of unity $w \in \mathbb{K}^*$ with $\text{ord}(w) > 1$ and $\sigma(\gamma) = w\gamma$.*

Proof. Assume that there are such γ and w with $k = \text{ord}(w) > 1$. Then $\sigma^k(\gamma) = \sigma^{k-1}(w\gamma) = w\sigma^{k-1}(\gamma) = \dots = w^k\gamma = \gamma$ and thus $\gamma \in \text{const}_{\sigma^k} \mathbb{A}$. Since (\mathbb{A}, σ) is constant-stable, $\gamma \in \mathbb{K}^*$. Hence $\gamma = w\gamma$ and thus $w = 1$, a contradiction. \square

Proposition 42. *Let $(\mathbb{A}[z], \sigma)$ be an A -extension of (\mathbb{A}, σ) of order n with $\sigma(z) = az$ where $a \in \mathbb{A}^*$. Then the following holds.*

- (1) z is an R -monomial (i.e., $\text{const}_\sigma \mathbb{A}[z] = \text{const}_\sigma \mathbb{A}$) iff there is no $g \in \mathbb{A}^*$ and $\lambda \in \mathbb{N}$ with $1 \leq \lambda < n$ such that $\sigma(g) = a^\lambda g$ holds
- (2) If z is an R -monomial, a is a λ th primitive root of unity and $\text{ord}(z^k) = \text{ord}(a^k)$ for all $0 \leq k \leq \lambda$.
- (3) If (\mathbb{A}, σ) is constant-stable, $\mathbb{K} = \text{const}_\sigma \mathbb{A}$ is a field and $a \in \mathbb{K}^*$ is a λ th primitive root of unity, then z is an R -monomial.

Proof. (1) This equivalence follows from [41, Thm. 2.12].

(2) In addition, if z is an R -monomial, a is a λ th primitive root of unity by [41, Thm. 2.12]. In particular, since $z^\lambda = 1$ is the defining relation, we get $\text{ord}(z) = \text{ord}(a) = \lambda$. Trivially, we have $1 = \text{ord}(a^0) = \text{ord}(z^0)$. Now suppose that $\text{ord}(z^k) \neq \text{ord}(a^k)$ for some $1 < k < \lambda$. If $\text{ord}(z^k) > \text{ord}(a^k) =: l$, then $\sigma(z^{kl}) = a^{kl} z^{kl} = z^{kl}$ with $z^{kl} = (z^k)^l \neq 1$ and thus $z^{kl} \in \text{const}_\sigma \mathbb{A}[z] \setminus \mathbb{A}$, a contradiction to the assumption that z is an R -monomial. Otherwise, if $l := \text{ord}(z^k) < \text{ord}(a^k)$, then $a^{kl} = a^{kl} z^{kl} = \sigma(z^{kl}) = \sigma(1) = 1$, i.e., $\text{ord}(a^k) \leq l$, a contradiction.

(4) Suppose that (\mathbb{A}, σ) is constant-stable and $a \in \mathbb{K}^*$ with $\text{ord}(a) = \lambda$. Since $\text{ord}(a^k) \neq 1$ for $1 \leq k < \lambda$, there are no $\gamma \in \mathbb{A} \setminus \{0\}$ and $k \in \mathbb{N}$ with $1 \leq k < \lambda$ and $\sigma(\gamma) = a^k \gamma$ by Lemma 41. Thus z is an R -monomial by statement (1). \square

In particular, we will require the following result [42, Prop. 2.23].

Proposition 43. *Let (\mathbb{F}, σ) be a constant-stable difference field with constant field \mathbb{K} . Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{F}[z_1] \dots [z_l]$ be an A -extension of (\mathbb{F}, σ) with $a_i = \frac{\sigma(z_i)}{z_i} \in \mathbb{K}^*$ for $1 \leq i \leq l$ of orders $\lambda_1, \dots, \lambda_l$, respectively. Then this is an R -extension iff for $1 \leq i \leq l$, the a_i are primitive λ_i -th roots of unity and $\text{gcd}(\lambda_i, \lambda_j) = 1$ for pairwise distinct i, j .*

Finally, we are in the position to present a characterization that combines single-nested R -extensions and Π -extensions.

Proposition 44. *Let (\mathbb{F}, σ) be a constant-stable difference field with constant field \mathbb{K} . Furthermore let (\mathbb{E}, σ) be AP -extension of (\mathbb{F}, σ) with $\mathbb{F}(x_1) \dots (x_r)[z_1] \dots [z_l]$ where the x_i are P -monomials with $\alpha_i = \frac{\sigma(x_i)}{x_i} \in \mathbb{F}^*$ for $1 \leq i \leq r$ and the z_i*

are A -monomials with $a_i = \frac{\sigma(z_i)}{z_i} \in \mathbb{K}^*$ of order λ_i for $1 \leq i \leq l$. Consider the sub-difference ring (\mathbb{H}, σ) of (\mathbb{E}, σ) with $\mathbb{H} = \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle [z_1] \dots [z_l]$ which forms an AP-extension of (\mathbb{F}, σ) . Then the following statements are equivalent.

- (1) $M((\alpha_1, \dots, \alpha_r), \mathbb{F}) = \{\mathbf{0}\}$, the a_i primitive roots of unity and $\gcd(\lambda_i, \lambda_j) = 1$ for pairwise distinct i, j .
- (2) $\text{const}_\sigma \mathbb{E} = \mathbb{K}$, i.e., (\mathbb{E}, σ) is an RII-extension of (\mathbb{F}, σ) .
- (3) $\text{const}_\sigma \mathbb{H} = \mathbb{K}$, i.e., (\mathbb{H}, σ) is an RII-extension of (\mathbb{F}, σ) .

Proof. (1) \Rightarrow (2): By Proposition 40 $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle, \sigma)$ is a Π -extension of (\mathbb{F}, σ) . In particular, by Proposition 32 it is constant-stable. Thus Prop. 43 is applicable which shows that $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle [z_1] \dots [z_l], \sigma)$ is an R -extension of $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle, \sigma)$.

(2) \Rightarrow (1): This follows immediately by Propositions 40 and 43.

(2) \Rightarrow (3): This follows by $\mathbb{K} \subseteq \text{const}_\sigma \mathbb{H} \subseteq \text{const}_\sigma \mathbb{E}$.

(3) \Rightarrow (2): Suppose that statement (3) holds, but (2) does not hold. With Proposition 40 it follows that (\mathbb{G}, σ) with $\mathbb{G} = \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$ is a Π -field extension of (\mathbb{F}, σ) . Consequently, there is a j with $1 \leq j < l$ such that $(\mathbb{G}[z_1] \dots [z_j], \sigma)$ is an R -extension of (\mathbb{G}, σ) and z_{j+1} is not an R -monomial. By Proposition 42 there are a $\nu_{j+1} \in \mathbb{N}$ with $1 \leq \nu_{j+1} < \lambda_{j+1}$ and $g \in \mathbb{G}[z_1] \dots [z_j] \setminus \{0\}$ with $\sigma(g) = a_{j+1}^{\nu_{j+1}} g$. Furthermore, by Proposition 36 (with $\mathbb{F} = \mathbb{G}$ and $r = 0$) it follows that $g = h z_1^{\nu_1} \dots z_j^{\nu_j}$ for some $h \in \mathbb{G}^*$. Thus $\sigma(h) = \gamma h$ where $\gamma = a_1^{-\nu_1} \dots a_j^{-\nu_j} a_{j+1}^{\nu_{j+1}} \in \mathbb{K}^*$ is a root of unity, and hence $\gamma^\lambda = 1$ for some $\lambda \in \mathbb{N} \setminus \{0\}$. This implies that $\sigma^\lambda(h) = \gamma^\lambda h = 1$. Since (\mathbb{G}, σ) is constant-stable by Proposition 32, $h \in \text{const}_\sigma \mathbb{G} = \mathbb{K}$. Consequently $g \in \mathbb{F}[z_1] \dots [z_j] \setminus \{0\}$ with $\sigma(g) = a_{j+1}^{\nu_{j+1}} g$. However, $\mathbb{K} \subseteq \text{const}_\sigma \mathbb{F}[z_1] \dots [z_l] \subseteq \text{const}_\sigma \mathbb{H} = \mathbb{K}$. Hence $(\mathbb{F}[z_1] \dots [z_j][z_{j+1}], \sigma)$ is an R -extension of $(\mathbb{F}[z_1] \dots [z_j], \sigma)$, a contradiction to part (1) of Proposition 42. \square

3.4. Radical stability. In order to solve Problem *DR* as described in Section 2.4, the following properties are crucial.

Definition 45. Let (\mathbb{F}, σ) be a difference field with $\mathbb{K} = \text{const}_\sigma \mathbb{F}$. Following [18] we define the homogeneous group by

$$H_{(\mathbb{F}, \sigma)} := \left\{ \frac{\sigma(g)}{g} \mid g \in \mathbb{F}^* \right\}.$$

We call (\mathbb{F}, σ) radical-stable if for any $a \in \mathbb{F}^*$ and $m \in \mathbb{N} \setminus \{0\}$ with $a^m \in H_{(\mathbb{F}, \sigma)}$ there is a $\rho \in \mathbb{K}^*$ with $\rho^m = 1$ such that

$$a \rho \in H_{(\mathbb{F}, \sigma)}$$

holds. (\mathbb{F}, σ) is called radical-solvable if it is radical-stable and for given $a \in \mathbb{F}^*$ and $m \in \mathbb{N} \setminus \{0\}$ with $a^m \in H_{(\mathbb{F}, \sigma)}$ one can compute $\rho \in \mathbb{K}^*$ with $\rho^m = 1$ and $g' \in \mathbb{F}^*$ such that $\sigma(g') = \gamma a g'$ holds.

First we show that one can reduce the property of being radical-solvable to the property of being radical-stable and solving first-order homogeneous equations.

Lemma 46. If a difference field (\mathbb{F}, σ) is radical stable and one can solve first-order homogeneous linear difference equations in (\mathbb{F}, σ) , then it is radical-solvable.

Proof. Let (\mathbb{F}, σ) be radical-stable and take $a \in \mathbb{F}^*$ and $m \in \mathbb{N} \setminus \{0\}$ with $a^m \in H_{(\mathbb{F}, \sigma)}$. Then we can conclude that there are a $\rho \in \mathbb{K}^*$ with $\rho^m = 1$ and a $\hat{g} \in \mathbb{F}^*$ with $\frac{\sigma(\hat{g})}{\hat{g}} = \rho a$. Take a primitive m th root of unity $\lambda \in \mathbb{K}^*$ and loop through

$i = 0, 1, 2, \dots, m-1$ until one finds a $\hat{g} \in \mathbb{F}^*$ with $\frac{\sigma(\hat{g})}{\hat{g}} = \lambda^i a$. In this way one considers all¹² m th roots of unity, in particular $\rho = \lambda^i$ will arise for some i . \square

In Subsection 3.1 we succeeded in lifting the property of being constant-stable from a smaller field to a larger field. The main goal of this subsection is to obtain a similar result for the property of being radical-stable. For Σ -monomials this lifting process will work in full generality (see Prop. 51). To obtain such a result for Π -monomials, we have to require further properties on (\mathbb{F}, σ) (see Prop. 52). This finally enables us to show in Corollary 53 that the mixed-rational difference field is radical-stable. We expect that this lifting-machinery can be applied also for other types of $\Pi\Sigma$ -field extensions to show that they are radical-stable.

In this subsection we will use the following convention. Let a multivariate rational function $\gamma = \frac{p}{q} \in \mathbb{F}(t_1, \dots, t_e) \setminus \{0\}$ be in reduced representation, i.e., $p, q \in \mathbb{F}[t_1, \dots, t_e] \setminus \{0\}$ are polynomials that are co-prime. Then for an irreducible polynomial $h \in \mathbb{F}[t_1, \dots, t_e]$ we write $h \nmid \gamma$ if $h \nmid p$ and $h \nmid q$ holds.

The following lemma elaborates the main complication of our desired lifting process.

Lemma 47. *Let $(\mathbb{F}(t), \sigma)$ be a $\Pi\Sigma$ -field extension of (\mathbb{F}, σ) and let $a, g \in \mathbb{F}(t)^*$ and $m \in \mathbb{N} \setminus \{0\}$ with $\frac{\sigma(g)}{g} = a^m$. Then there is a $\gamma \in \mathbb{F}(t)^*$ and $u \in \mathbb{F}^*$ with*

$$g = \gamma^m u t^n \quad (29)$$

for some $n \in \mathbb{Z}$. If t is a Σ -monomial, $n = 0$; if t is a Π -monomial, $t \nmid \gamma$.

Proof. If $g \in \mathbb{F}^*$, we can set $\gamma = 1$, $n = 0$ and $u = g$. Otherwise suppose that $g \notin \mathbb{F}$. By [18, Thm. 7] (see also [32, Sec. 2.3]) we can write g in the following form¹³: $g = u t^n g_1 \cdots g_k$ where $n \in \mathbb{Z}$, $u \in \mathbb{F}^*$, $\gcd(g_i, \sigma^l(g_j)) = 1$ for all $i \neq j$ and $l \in \mathbb{Z}$, and for $1 \leq i \leq k$,

$$g_i = \prod_{j=0}^{r_i} \sigma^j(h_i)^{m_{ij}} \neq 1 \quad (30)$$

where $h_i \in \mathbb{F}[t] \setminus \mathbb{F}$ are irreducible, $m_{ij} \in \mathbb{Z}$ and $r_i \geq 0$. In particular, $n = 0$ if t is a Σ -monomial, and $t \nmid g_i$ for all i if t is a Π -monomial. Then by $\frac{\sigma(g)}{g} = \alpha^m$ it follows that for all $1 \leq i \leq k$ and all $0 \leq j \leq r_i - 1$ we have $m \mid (m_{i,j+1} - m_{i,j})$ and $m \mid m_{i,r_i}$. Because of $m \mid m_{i,r_i}$ and $m \mid (m_{i,r_i} - m_{i,r_i-1})$, it follows that $m \mid m_{i,r_i-1}$. Applying this argument r_i times proves that $m \mid m_{ij}$ for all $1 \leq i \leq k$ and all $1 \leq j \leq r_i$. Hence $g_i = g_i'^m$ for $g_i' := \prod_{j=0}^{r_i} \sigma^j(h_i)^{m_{ij}/m} \in \mathbb{F}(t)$ for all $1 \leq i \leq k$. With $\gamma = g_1' \cdots g_k'$ we get $g = u \gamma^m t^n$ which completes the proof. \square

More precisely, in (29) one obtains a solution which is close to derive radical-stability for $(\mathbb{F}(t), \sigma)$: the only troublemaker is the possible factor t^n with $n \in \mathbb{Z}$ if t is a Π -monomial. This property can be carried over for several Π -extensions.

Corollary 48. *Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{F}(t_1) \cdots (t_e)$ be a Π -field extension of (\mathbb{F}, σ) with $\alpha_i = \frac{\sigma(t_i)}{t_i} \in \mathbb{F}^*$ for $1 \leq i \leq e$. Let $a, g \in \mathbb{E}^*$ and $m \in \mathbb{N} \setminus \{0\}$ with $\frac{\sigma(g)}{g} = a^m$. Then there are $m_1, \dots, m_e \in \mathbb{Z}$, $\gamma \in \mathbb{E}^*$ with $t_i \nmid \gamma$ for $1 \leq i \leq e$ and $u \in \mathbb{F}^*$ such that $g = u \gamma^m t_1^{m_1} \cdots t_e^{m_e}$ holds.*

¹²If m is minimal such that $a^m \in H_{(\mathbb{F}, \sigma)}$ holds, we only have to consider all i with $\gcd(i, m) = 1$, i.e., all cases where λ^i is again a primitive m th root of unity.

¹³In [18] this representation is also called σ -representation. Its existence can be derived from the statements (1) and (2) of Lemma 31.

Proof. For all $1 \leq j \leq e$ we get the following construction: Moving t_j for $1 \leq j \leq e$ on top and applying Lemma 47 we get $u_j \in \mathbb{E}_j = \mathbb{F}(t_1) \dots (t_{j-1})(t_{j+1}) \dots (t_e)^*$, $\gamma_j \in \mathbb{E}_j(t_j)^*$, $t_j \nmid \gamma_j$ and $m_j \in \mathbb{Z}$ with

$$g = u_j \gamma_j^{m_j} t_j^{m_j}. \quad (31)$$

Write $\gamma_j = \frac{p_j}{q_j}$ with $p_j, q_j \in \mathbb{F}[t_1, \dots, t_e]$ being coprime; we can assume that the polynomials p_j and q_j contain no polynomial factors in $\mathbb{F}[t_1, \dots, t_e]$ that are free of t_j by moving them into u_j . Define $\gamma := \frac{\text{lcm}(p_1, \dots, p_e)}{\text{lcm}(q_1, \dots, q_e)} \in \mathbb{E}^*$ and

$$u := \frac{g}{\gamma^m t_1^{m_1} \dots t_e^{m_e}} \in \mathbb{E}^*. \quad (32)$$

By construction, $g = u \gamma^m t_1^{m_1} \dots t_e^{m_e}$. The corollary follows if $u \in \mathbb{F}$. Suppose that $u \notin \mathbb{F}$. Then we can take an irreducible factor f from u such that for some $1 \leq j \leq e$ the variable t_j depends on f .

Case 1: $f = t_j$. By construction γ_j is free of the factor t_j and by (31) also $g/t_j^{m_j}$ is free of the factor t_j . Furthermore γ_i for all i with $i \neq j$ is free of the factor t_j (it is collected in the content $u_i \in \mathbb{E}_i$). Thus also $t_j \nmid \gamma$. With (32), t_j cannot occur as a factor in u , a contradiction.

Case 2: $f \neq t_j$. Since f occurs in u , it must occur in g or in γ . Suppose that it does not occur in g . Then for $1 \leq k \leq e$ it does not occur in γ_k as a factor by (31) and thus it cannot occur in γ , a contradiction. Thus f must occur in g . Let n be maximal such that f^n is a factor in g . Then n is maximal such that f^n occurs in γ_j by (31). In particular, n is maximal such that f^n occurs in p_j^m or q_j^m , thus in $\text{lcm}(p_1, \dots, p_e)^m$ or in $\text{lcm}(q_1, \dots, q_e)^m$ and therefore in γ^m . In conclusion, f cannot occur in $\frac{g}{\gamma^m}$ and thus not in (32), again a contradiction. \square

The following lemma is basic, but for completeness we state it here.

Lemma 49. *Let (\mathbb{E}, σ) be a PS-field extension of (\mathbb{F}, σ) , $a \in \mathbb{E}^*$ and $m \in \mathbb{N} \setminus \{0\}$. If $a^m \in \mathbb{F}$ then $a \in \mathbb{F}$.*

Proof. Let $\mathbb{E} = \mathbb{F}(t_1) \dots (t_e)$. Suppose that $a^m \in \mathbb{F}$ and let i be maximal such that $a \in \mathbb{F}(t_1) \dots (t_i) \setminus \mathbb{F}(t_1) \dots (t_{i-1})$. Write $a = \frac{p}{q}$ with $p, q \in \mathbb{F}(t_1) \dots (t_{i-1})[t_i]$ where $\gcd(p, q) = 1$ and either p or q depend on t_i . We get $p^m = a^m q^m$ with $a^m \in \mathbb{F}^*$ and thus $\gcd(p^m, q^m) = p^m$ and $\gcd(p^m, q^m) = q^m$. However, $\gcd(p, q) = 1$ implies that $\gcd(p^m, q^m) = 1$ and thus $p^m \in \mathbb{F}^*$ and $q^m \in \mathbb{F}^*$, a contradiction that one of the polynomials p or q depend on t_i . \square

Finally, we can give a recipe how one can lift the property of being radical-stable within a PS-extension. Here the crucial assumption is that the factor t^n in (29) (and more generally, several such Π -monomials) does not appear.

Lemma 50. *Let (\mathbb{E}, σ) be a $\Pi\Sigma$ -field extension of (\mathbb{F}, σ) and let $m \in \mathbb{N} \setminus \{0\}$. Take $g = u \gamma^m$ with $u \in \mathbb{F}^*$ and $\gamma \in \mathbb{E}^*$ such that $\frac{\sigma(g)}{g} = a^m$. If (\mathbb{F}, σ) is radical-stable, there are a $\tilde{\gamma} \in \mathbb{E}^*$ and a $\rho \in (\text{const}_\sigma \mathbb{F})^*$ with $\rho^m = 1$ such that $\frac{\sigma(\tilde{\gamma})}{\tilde{\gamma}} = a \rho$ holds.*

Proof. Suppose that (\mathbb{F}, σ) is radical-stable and let $g = u \gamma^m$ as claimed above. Thus $a^m = \frac{\sigma(g)}{g} = \frac{\sigma(\gamma^m)}{\gamma^m} \frac{\sigma(u)}{u}$ and consequently

$$\frac{\sigma(u)}{u} = \left(a \frac{\gamma}{\sigma(\gamma)} \right)^m.$$

Since the left-hand side is in \mathbb{F}^* , also the right-hand side is in \mathbb{F}^* and therefore also $a' := a \frac{\gamma}{\sigma(\gamma)} \in \mathbb{F}^*$ by Lemma 49. Since (\mathbb{F}, σ) is radical-stable, it follows that there are a $u' \in \mathbb{F}$ and a root of unity $\rho \in \text{const}_\sigma \mathbb{F}$ with $\rho^m = 1$ with $\frac{\sigma(u')}{u'} = \rho a'$. Therefore $\frac{\sigma(u')}{u'} = \rho a \frac{\gamma}{\sigma(\gamma)}$ and thus $\frac{\sigma(\tilde{\gamma})}{\tilde{\gamma}} = a \rho$ with $\tilde{\gamma} = u' \gamma \in \mathbb{F}^*$. \square

Using this lemma, we can derive our two main statements to lift the property of being radical-stable for Σ -monomials and certain types of Π -monomials.

Proposition 51. *Let $(\mathbb{F}(t), \sigma)$ be a Σ -field extension of (\mathbb{F}, σ) . If (\mathbb{F}, σ) is radical-stable, then $(\mathbb{F}(t), \sigma)$ is radical-stable.*

Proof. Suppose that (\mathbb{F}, σ) is radical-stable. Let $a, g \in \mathbb{F}(t)^*$ and $m \in \mathbb{N} \setminus \{0\}$ with $\frac{\sigma(g)}{g} = a^m$. By Lemma 47 there are a $\gamma \in \mathbb{F}(t)^*$ and $u \in \mathbb{F}^*$ with $g = \gamma^m u$. Thus we can activate Lemma 50 with $\mathbb{E} = \mathbb{F}(t)$ and it follows that there is a $\tilde{\gamma} \in \mathbb{F}(t)^*$ and a root of unity $\rho \in (\text{const}_\sigma \mathbb{F})^*$ with $\rho^m = 1$ such that $\frac{\sigma(\tilde{\gamma})}{\tilde{\gamma}} = a \rho$ holds. Consequently, $(\mathbb{F}(t), \sigma)$ is radical-stable. \square

Proposition 52. *Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{F}(t_1) \dots (t_e)$ be a Π -field extension of (\mathbb{F}, σ) with $\alpha_i = \frac{\sigma(t_i)}{t_i} \in \mathbb{F}^*$ for $1 \leq i \leq e$. Suppose that (\mathbb{F}, σ) is radical-stable and the following property holds:*

$$\begin{aligned} \forall m \in \mathbb{N} \setminus \{0\} \forall (m_1, \dots, m_e) \in \mathbb{Z}^e \forall a, w \in \mathbb{F}^* : \frac{\sigma(w)}{w} = a^m \alpha_1^{m_1} \dots \alpha_e^{m_e} \\ \Rightarrow m \mid m_1 \wedge \dots \wedge m \mid m_e. \end{aligned} \quad (33)$$

Then (\mathbb{E}, σ) is radical-stable.

Proof. Suppose that (\mathbb{F}, σ) is radical-stable and that (33) holds. Let $a, g \in \mathbb{E}^*$ and $m \in \mathbb{N} \setminus \{0\}$ with $\frac{\sigma(g)}{g} = a^m$. By Corollary 48 there are $m_1, \dots, m_e \in \mathbb{Z}$, $\gamma \in \mathbb{E}^*$ with $t_i \nmid \gamma$ for $1 \leq i \leq e$ and $u \in \mathbb{F}^*$ such that $g = u \gamma^m t_1^{m_1} \dots t_e^{m_e}$ holds. Hence $\frac{\sigma(w)}{w} = a^m \alpha_1^{m_1} \dots \alpha_e^{m_e}$ with $a = \frac{\sigma(\gamma)}{\gamma} \in \mathbb{E}^*$ and $w = u^{-1} \in \mathbb{F}^*$. Since $\frac{\sigma(w)}{w} \in \mathbb{F}^*$ and $\alpha_1^{m_1} \dots \alpha_e^{m_e} \in \mathbb{F}^*$, $a^m \in \mathbb{F}^*$. Thus by Lemma 49 it follows $a \in \mathbb{F}^*$. By property (33) we conclude that there are $n_i \in \mathbb{Z}$ with $m n_i = m_i$ for $1 \leq i \leq e$. Thus $g = u \gamma'^m$ with $\gamma' = \gamma t_1^{n_1} \dots t_e^{n_e} \in \mathbb{E}$. As in the proof of Proposition 51 we can apply Lemma 50 with $\mathbb{E} = \mathbb{F}(t_1) \dots (t_e)$ and it follows that there are a $\tilde{\gamma} \in \mathbb{E}^*$ and a root of unity $\rho \in (\text{const}_\sigma \mathbb{F})^*$ with $\rho^m = 1$ such that $\frac{\sigma(\tilde{\gamma})}{\tilde{\gamma}} = a \rho$ holds. Consequently, (\mathbb{E}, σ) is radical-stable. \square

Finally, we show that the mixed-rational difference field is radical-stable and radical-solvable.

Corollary 53. *Let $\mathbb{K} = \mathbb{K}'(q_1, \dots, q_v)$ be a rational function field with coefficients from a field \mathbb{K}' . The mixed-rational difference field (\mathbb{F}, σ) with $\mathbb{F} = \mathbb{K}(x)(y_1) \dots (y_v)$ where $\text{const}_\sigma \mathbb{K} = \mathbb{K}$, $\sigma(x) = x+1$ and $\sigma(y_i) = q_i y_i$ for $1 \leq i \leq v$ is radical-stable. If \mathbb{K}' is a rational function field over an algebraic number field, one can solve homogeneous first-order linear difference equations in (\mathbb{F}, σ) and (\mathbb{F}, σ) is radical-solvable.*

Proof. Note that the constant field (\mathbb{K}, σ) is trivially radical-stable: If there are a $g \in \mathbb{K}^*$ and $a \in \mathbb{K}^*$ with $a^m = \frac{\sigma(g)}{g} = 1$ for some $m \in \mathbb{N} \setminus \{0\}$ then a is a root of unity. Thus we can set $\rho = a^{-1} \in \mathbb{K}^*$ with $\rho^m = 1$ and $\gamma = 1 \in \mathbb{K}^*$ and get $\frac{\sigma(\tilde{\gamma})}{\tilde{\gamma}} = a \rho$. Furthermore, property (33) (with $\mathbb{E} = \mathbb{K}(y_1) \dots (y_v)$ and $\alpha_i = q_i$ for

$1 \leq i \leq v = e$) holds: Let $a, g \in \mathbb{K}^*$, $m \in \mathbb{N} \setminus \{0\}$ and $(m_1, \dots, m_v) \in \mathbb{Z}^v$ such that $1 = \frac{\sigma(g)}{g} = a^m q_1^{m_1} \dots q_v^{m_v}$ holds. Suppose that $m_i \neq 0$ for some $1 \leq i \leq v$. Then q_i must occur as factor in a , say with multiplicity $l_i \in \mathbb{Z} \setminus \{0\}$. More precisely, we must have $m_i = l_i m$, i.e., $m \mid m_i$. Since property (33) holds, we can apply Proposition 52 and it follows that $(\mathbb{K}(y_1) \dots (y_v), \sigma)$ is radical-stable. By Proposition 51 we conclude that also $(\mathbb{K}(y_1) \dots (y_v)(x), \sigma)$ and thus by reordering of the generators also $(\mathbb{K}(x)(y_1) \dots (y_v), \sigma)$ is radical-stable. In particular, if \mathbb{K}' is a rational function field over an algebraic number field, one can solve linear first-order homogeneous difference equations in (\mathbb{F}, σ) by¹⁴ [32, Thm. 3.2 and 3.5]. As a consequence, (\mathbb{F}, σ) is also radical-solvable by Lemma 46. \square

As a consequence also the rational difference ring (i.e., $v = 0$), the q -rational difference ring (i.e., $v = 1$ and $\mathbb{F} = \mathbb{K}(y_1)$), and the multi-basic difference ring (i.e., $\mathbb{F} = \mathbb{K}(y_1) \dots (y_v)$) are radical-stable. We remark that the property of being radical-stable has been shown already earlier for the rational case in [32, Lemma 5.3] and for the q -rational case in [32, Lemma 5.5 and Lemma 5.6].

Example 54. Consider the rational difference field (\mathbb{F}, σ) with $\mathbb{F} = \mathbb{K}(x)$, $\sigma(x) = x + 1$ and α_2 given in (36). It will turn out that $m = 2$ is minimal such that $\alpha_2^m \in H_{(\mathbb{F}, \sigma)}$ holds. Since (\mathbb{F}, σ) is radical-stable by Corollary 53, there is a $\rho \in \mathbb{K}^*$ with $\rho^2 = 1$ and a $\bar{g}_2 \in \mathbb{F}$ such that $\sigma(\bar{g}_2) = \rho \alpha_2 \bar{g}_2$ holds. We can calculate \bar{g}_2 and ρ following the proof of Lemma 46. Take the primitive 2nd root of unity $\rho = -1$. Then we check for $i = 0, 1$ if there is a $\bar{g}_2 \in \mathbb{F}^*$ with $\sigma(\bar{g}_2) = (-1)^i \alpha_2 \bar{g}_2$. Since $m = 2$ is minimal with $\alpha_2^m \in H_{(\mathbb{F}, \sigma)}$, it suffices to look at $i = 1$; see the footnote in the proof of Corollary 53). Solving this first-order homogeneous difference equation we obtain

$$\bar{g}_2 = (1+x)^2(2+x)^5(3+x)^8(4+x)(5+x). \quad (34)$$

3.5. Properties of the mixed-rational difference field (Theorem 29). Collecting results of the previous subsections yields a

Proof of Theorem 29. Let (\mathbb{F}, σ) be a mixed-rational difference field with constant field \mathbb{K} where \mathbb{K} is a rational function field over an algebraic number field. Note that (\mathbb{F}, σ) is a $\Pi\Sigma$ -field over \mathbb{K} .

- (1) Since the standard operations in a rational function field defined over \mathbb{K} are computable, (\mathbb{F}, σ) is computable.
- (2) As elaborated in Example 20 there is a σ -computable \mathbb{K} -embedding into the ring of sequences.
- (3) By Corollary 53 the difference field (\mathbb{F}, σ) is radical-stable.
- (4) By Corollary 53 one can solve linear first-order homogeneous difference equations in (\mathbb{F}, σ) .
- (5) Finally, by Proposition 38 one can compute a basis of $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$ with $\alpha_1, \dots, \alpha_r \in \mathbb{F}^*$. \square

We remark that the mixed-rational difference field (\mathbb{F}, σ) introduced in Example 20 is also constant-stable. This follows either by Corollary 33 ((\mathbb{F}, σ) is a $\Pi\Sigma$ -field) or by Lemma 35 ((\mathbb{F}, σ) can be embedded into the ring of sequences).

¹⁴The proof is based on Karr's summation algorithm [18] and Ge's algorithm [15]. For the rational and q -rational case we refer also to [5].

4. THE SOLUTION OF PROBLEM *DR* FOR A SPECIAL CASE

In the following we will consider a P -extension $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle, \sigma)$ of a difference field (\mathbb{F}, σ) with $\alpha_i = \frac{\sigma(x_i)}{x_i} \in \mathbb{F}^*$ for $1 \leq i \leq r$ with the following special property: the \mathbb{Z} -submodule $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$ of \mathbb{Z}^r has rank $u \geq 1$ and there is a basis of the form

$$\{(d_1, 0, \dots, 0), (0, d_2, 0, \dots, 0), \dots, (0, \dots, 0, d_u, 0, \dots, 0)\} \quad (35)$$

with $d_1 \mid \dots \mid d_u$.

Example 55. *As running example we will start with the difference field (\mathbb{F}, σ) with $\mathbb{F} = \mathbb{K}(x)$ where $\mathbb{K} = \mathbb{Q}(t)$ and $\sigma(x) = x + 1$ equipped with $\bar{\text{ev}}: \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{K}$ defined in Example 7 (ev replaced by $\bar{\text{ev}}$). Furthermore, we consider the P -extension (\mathbb{H}, σ) of (\mathbb{F}, σ) with $\mathbb{H} = \mathbb{F}\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle$ where $\sigma(x_i) = \alpha_i x_i$ for $1 \leq i \leq 4$ with*

$$\begin{aligned} \alpha_1 &= \frac{(x+6)^2}{(x+4)^2}, & \alpha_2 &= -\frac{(x+4)^7(x+6)}{(x+1)^2(x+2)^3(x+3)^3}, \\ \alpha_3 &= -\frac{t(x+4)^6}{9(x+1)(x+2)^2(x+3)(x+6)}, & \alpha_4 &= -\frac{162(x+1)(x+3)}{x+6}. \end{aligned} \quad (36)$$

Further, we extend the evaluation function $\bar{\text{ev}}: \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{K}$ to $\text{ev}: \mathbb{H} \times \mathbb{N} \rightarrow \mathbb{K}$ by

$$\begin{aligned} \text{ev}(x_1, n) &= \prod_{k=1}^n \frac{(5+k)^2}{(3+k)^2}, & \text{ev}(x_2, n) &= \prod_{k=1}^n \frac{-(3+k)^7(5+k)}{k^2(1+k)^3(2+k)^3}, \\ \text{ev}(x_3, n) &= \prod_{k=1}^n \frac{-t(3+k)^6}{9k(1+k)^2(2+k)(5+k)}, & \text{ev}(x_4, n) &= \prod_{k=1}^n \frac{-162k(2+k)}{5+k}. \end{aligned} \quad (37)$$

Using, e.g., the algorithm from [18] we obtain the basis

$$\{(1, 0, 0, 0), (0, 2, 0, 0)\} \quad (38)$$

of $M((\alpha_1, \alpha_2, \alpha_3, \alpha_4), \mathbb{F})$, i.e., $u = 2$ with $d_1 = 1$ and $d_2 = 2$.

For such an extension, we will solve Problem *DR* as described in Subsection 2.4. In order to derive this result, we will first treat a more general situation in Lemma 58 that does not require that there is a \mathbb{K} -embedding $\tau: \mathbb{F} \rightarrow \mathbf{S}(\mathbb{K})$. Afterwards we will specialize this result to Theorem 60 for a given \mathbb{K} -embedding.

Before we can proceed with this construction, we will elaborate several lemmas. In their proofs we will use the following definition. For a Laurent polynomial $f \in \mathbb{A}[t, t^{-1}] \setminus \{0\}$ we define

$$\overline{\text{deg}}(f) = \text{deg}(f) - \text{ord}(f).$$

This means that for $f = \sum_{k=l}^r f_k t^k$ with $l \leq r$ where $f_l \neq 0 \neq f_r$ (i.e., $\text{ord}(f) := l$ and $\text{deg}(f) := r$) we have $\overline{\text{deg}}(f) = r - l$.

Lemma 56. *Let (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{A}\langle x_1 \rangle \dots \langle x_r \rangle$ be a P -extension of a difference ring (\mathbb{A}, σ) with $\alpha_i = \frac{\sigma(x_i)}{x_i} \in \mathbb{A}^*$ for $1 \leq i \leq r$. Let (\mathbb{H}, σ) be a difference ring extension of (\mathbb{A}, σ) and take the ring homomorphism $\lambda: \mathbb{E} \rightarrow \mathbb{H}$ with $\lambda|_{\mathbb{A}} = \text{id}$ and $\lambda(x_i) = g_i$ for some $g_i \in \mathbb{H}^*$ with $1 \leq i \leq r$. Then λ is a difference ring homomorphism iff $\alpha_i = \frac{\sigma(g_i)}{g_i}$ for $1 \leq i \leq r$.*

Proof. Suppose that λ is a difference ring homomorphism. Then for $1 \leq i \leq r$ we have $\frac{\sigma(g_i)}{g_i} = \frac{\sigma(\lambda(x_i))}{\lambda(x_i)} = \lambda\left(\frac{\sigma(x_i)}{x_i}\right) = \lambda(\alpha_i) = \alpha_i$. Conversely, if $\alpha_i = \frac{\sigma(g_i)}{g_i}$ for $1 \leq i \leq r$, then $\lambda(\sigma(x_i)) = \lambda(\alpha_i x_i) = \alpha_i g_i = \sigma(g_i) = \sigma(\lambda(x_i))$ which implies that $\sigma(\lambda(f)) = \lambda(\sigma(f))$ for all $f \in \mathbb{E}$. \square

Lemma 57. *Let $(\mathbb{F}\langle x \rangle, \sigma)$ be a P -extension of a difference field (\mathbb{F}, σ) with $\sigma(x) = \alpha x$ and $\mathbb{K} = \text{const}_\sigma \mathbb{F}$. Let (\mathbb{H}, σ) be a difference ring extension of (\mathbb{F}, σ) with $\text{const}_\sigma \mathbb{H} = \mathbb{K}$ equipped with a difference ring homomorphism $\lambda: \mathbb{F}\langle x \rangle \rightarrow \mathbb{H}$ with $\lambda|_{\mathbb{K}} = \text{id}$. Then the following holds.*

- (1) $M((\alpha), \mathbb{F}) \neq \{0\}$ if and only if $\ker(\lambda) \neq \{0\}$.
- (2) If $M((\alpha), \mathbb{F}) = \langle m \rangle_{\mathbb{Z}}$ with $m > 0$, then $\ker(\lambda) = \langle \mu \rangle_{\mathbb{F}\langle x \rangle}$ with $\mu = x^m + g$ for some $g \in \mathbb{F}^*$ with $\sigma(g) = \alpha^m g$.

Proof. (1) Suppose that $M((\alpha), \mathbb{F}) \neq \{0\}$. Then there is a $\gamma \in \mathbb{F}^*$ with $\sigma(\gamma) = \alpha^m \gamma$ for some $m > 0$ (if $m < 0$, we can take $\gamma' = 1/\gamma \in \mathbb{F}^*$ with $\sigma(\gamma') = \alpha^{-m} \gamma'$). Hence $\sigma(\frac{x^m}{\gamma}) = \frac{x^m}{\gamma}$, therefore $\sigma(\lambda(\frac{x^m}{\gamma})) = \lambda(\frac{x^m}{\gamma})$, and thus $\lambda(\frac{x^m}{\gamma}) \in \text{const}_\sigma \mathbb{H} = \text{const}_\sigma \mathbb{F} = \mathbb{K}$. Since $\frac{x^m}{\gamma}$ is a unit, $\lambda(\frac{x^m}{\gamma}) \neq 0$. Hence $\lambda(\frac{x^m}{\gamma}) = c$ for some $c \in \mathbb{K}^*$ and consequently $\lambda(\frac{x^m}{\gamma} - c) = 0$ or equivalently $\lambda(x^m - g) = 0$ with $g = c\gamma \in \mathbb{F}^*$; obviously we have that $\sigma(g)/g = \alpha^m$. Conversely, suppose that there is a $\mu \in \mathbb{F}\langle x \rangle \setminus \{0\}$ with $\lambda(\mu) = 0$. Take such a μ such that $n = \overline{\text{deg}}(\mu)$ is minimal. W.l.o.g. we may assume that $\mu = x^n + b$ with $b \in \mathbb{F}[x]$ and $\text{deg}(b) < n$ (otherwise we may take $\mu' = \text{lc}(\mu)^{-1} x^{-\text{ord}(n)} \mu \in \mathbb{F}[x]$ with $\lambda(\mu') = \lambda(\text{lc}(\mu)^{-1} x^{-\text{ord}(n)}) \lambda(\mu) = 0$ and $\overline{\text{deg}}(\mu') = \text{deg}(\mu') = m$). Define $h := \sigma(\mu) - \alpha^n \mu$. By construction, $\overline{\text{deg}}(h) = \text{deg}(h) < n$. Furthermore, since $\lambda(\sigma(\mu)) = \sigma(\lambda(\mu)) = \sigma(0) = 0$, we get $\lambda(h) = \lambda(\sigma(\mu) - \alpha^n \mu) = \lambda(\sigma(\mu)) - \lambda(\alpha^n) \lambda(\mu) = 0$. Because of the minimality of μ , it follows that $h = 0$ and thus

$$\sigma(\mu) = \alpha^n \mu. \quad (39)$$

Suppose that $b = 0$. Then $0 = \lambda(\mu) = \lambda(x)^n$. But $\lambda(x) \lambda(x^{-1}) = 1$ and therefore $\lambda(x) \neq 0$, a contradiction. Thus $b = g_l x^l + d$ with $g_l \in \mathbb{F}^*$, $0 \leq l < n$ and $d \in \mathbb{F}[x]$ with $\text{deg}(d) < l$. By coefficient comparison w.r.t. x^l in (39) we conclude that $\sigma(g_l) = \alpha^{n-l} g_l$. Therefore $M((\alpha), \mathbb{F}) \neq \{0\}$.

(2) Suppose that $M((\alpha), \mathbb{F}) = \langle m \rangle_{\mathbb{Z}}$ with $m > 0$. By part (1) there is a polynomial $h = x^m - g \in \mathbb{F}[x] \setminus \mathbb{F}$ with $\lambda(\mu) = 0$ where $g \in \mathbb{F}^*$ with $\sigma(g) = \alpha^m g$. Moreover, looking at the proof of part (1), among the $\mu \in \mathbb{F}\langle x \rangle^*$ with $\lambda(\mu) = 0$ where $n = \overline{\text{deg}}(\mu)$ is minimal, we can take $\mu = x^n + g_l x^l + d$ with $g_l \in \mathbb{F}^*$ and $d \in \mathbb{F}[t]$ with $\text{deg}(d) < l$ where $\sigma(g_l) = \alpha^{n-l} g_l$. Because of $n \leq m$ and $M((\alpha), \mathbb{F}) = \langle m \rangle_{\mathbb{Z}}$, it follows that $m = n$ and $l = 0$. Consequently, $\mu = x^m + g_l$. Finally, we show that¹⁵ $\ker(\lambda) = \langle \mu \rangle_{\mathbb{F}\langle x \rangle}$. $\ker(\lambda) \supseteq \langle \mu \rangle_{\mathbb{F}\langle x \rangle}$ holds trivially. Let $f \in \ker(\lambda)$. By polynomial reductions (polynomial divisions) in $\mathbb{F}\langle x \rangle$ we remove all terms whose degrees are larger than x^m or smaller than 0. Thus we get $f = r + \mu g$ with $g \in \mathbb{F}\langle x \rangle$ and $r \in \mathbb{F}[x]$ where $\text{deg}(r) < m$. Since $f, \mu \in \ker(\lambda)$, $r \in \ker(\lambda)$, and by the minimality of μ it follows that $r = 0$. Thus $f = \mu g \in \langle \mu \rangle_{\mathbb{F}\langle x \rangle}$ which completes the proof. \square

Lemma 58. *Let (\mathbb{F}, σ) be a radical-stable difference field with $\mathbb{K} = \text{const}_\sigma \mathbb{F}$, and let $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle, \sigma)$ be a P -extension of (\mathbb{F}, σ) with $\alpha_i = \frac{\sigma(x_i)}{x_i} \in \mathbb{F}^*$. Suppose that (35) with $u \geq 1$ and $d_1 \mid \dots \mid d_u$ is a basis of $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$. If $d_u > 0$, suppose in addition that (\mathbb{F}, σ) is constant-stable. Then the following holds:*

- (1) (\mathbb{E}, σ) with $\mathbb{E} = \mathbb{F}\langle x_{u+1} \rangle \dots \langle x_r \rangle$ is a Π -extension of (\mathbb{F}, σ) (i.e., $\text{const}_\sigma \mathbb{E} = \text{const}_\sigma \mathbb{F} = \mathbb{K}$).

¹⁵Note that $\mathbb{F}\langle x \rangle$ is a p.i.d. which implies this statement. For completeness we carry out the proof explicitly.

- 2a) If $d_u = 1$, there are $\bar{g}_i \in \mathbb{F}^*$ with $\sigma(\bar{g}_i) = \alpha_i \bar{g}_i$ for $1 \leq i \leq u$ and for any $c_1, \dots, c_u \in \mathbb{K}^*$ the surjective ring homomorphism $\lambda: \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbb{E}$ defined by $\lambda|_{\mathbb{E}} = \text{id}$ and

$$\lambda(x_i) = c_i \bar{g}_i \quad 1 \leq i \leq u \quad (40)$$

is a difference ring homomorphism.

- 2b) Otherwise, if $d_u > 1$, there is an R -extension $(\mathbb{E}[z], \sigma)$ of (\mathbb{E}, σ) of order d_u with $\frac{\sigma(z)}{z} = \rho$. In addition, one can take $\bar{g}_i \in \mathbb{F}^*$ and $\nu_i \in \mathbb{N}$ for $1 \leq i \leq u$ with $\sigma(\bar{g}_i) = \rho^{\nu_i} \alpha_i \bar{g}_i$ such that for any choice $c_1, \dots, c_u \in \mathbb{K}^*$ the surjective ring homomorphism $\lambda: \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbb{E}[z]$ defined by $\lambda|_{\mathbb{E}} = \text{id}$ and

$$\lambda(x_i) = c_i z^{d_u - \nu_i} \bar{g}_i \quad 1 \leq i \leq u \quad (41)$$

is a difference ring homomorphism; further¹⁶, $\text{ord}(z^{\nu_i}) = \text{ord}(z^{d_u - \nu_i}) = \text{ord}(\rho^{\nu_i}) = \text{ord}(\rho^{d_u - \nu_i}) = d_i$.

- (3) $\ker(\lambda) = \langle x_1^{d_1} - (c_1 \bar{g}_1)^{d_1}, \dots, x_u^{d_u} - (c_u \bar{g}_u)^{d_u} \rangle_{\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle}$ where the \bar{g}_i are given by (2a) or (2b), respectively.

If (\mathbb{F}, σ) is in addition computable and one can solve first-order homogeneous difference equations in (\mathbb{F}, σ) , then one can compute (\mathbb{E}, σ) , λ is computable and the generators of $\ker(\lambda)$ can be given explicitly.

Proof. (1) Since $M((\alpha_{u+1}, \dots, \alpha_r), \mathbb{F}) = \{\mathbf{0}\}$, we can activate Proposition 40 and it follows that (\mathbb{E}, σ) is a Π -extension of (\mathbb{F}, σ) .

(2a) Suppose that $d_1 = \dots = d_u = 1$. Then for $1 \leq i \leq u$ there are $\bar{g}_i \in \mathbb{F}^*$ with $\sigma(\bar{g}_i) = \alpha_i \bar{g}_i$. Therefore we can define for any $c_i \in \mathbb{K}^*$ with $u < i \leq r$ the ring homomorphism $\lambda: \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbb{E}$ with $\lambda|_{\mathbb{E}} = \text{id}$ and $\lambda(x_i) = c_i \bar{g}_i$ for $1 \leq i \leq u$. Furthermore, λ is a difference ring homomorphism by Lemma 56.

(2b) Suppose that $d_u > 1$. For $1 \leq i \leq u$ take $g_i \in \mathbb{F}^*$ with $\sigma(g_i) = \alpha_i^{d_i} g_i$. Since (\mathbb{F}, σ) is radical-stable, there are a d_i th root of unity $\rho_i \in \mathbb{K}^*$ and $\bar{g}_i \in \mathbb{F}^*$ with $\sigma(\bar{g}_i) = \rho_i \alpha_i \bar{g}_i$ for $1 \leq i \leq u$. Note that

$$\text{ord}(\rho_i) = d_i. \quad (42)$$

Otherwise we would get $\rho_i^s = 1$ for some s with $1 < s < d_i$. Therefore $\sigma(\bar{g}_i^s) = \rho_i^s \alpha_i^s \bar{g}_i^s = \alpha_i^s \bar{g}_i^s$. Since $s < d_i$, $(0, \dots, 0, d_i, 0, \dots, 0)$ cannot be a basis element of $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$, a contradiction. Thus the ρ_i are primitive d_i th roots of unity for $1 \leq i \leq u$. Let $\rho = \rho_u$ and take the A -extension $(\mathbb{E}[z], \sigma)$ of (\mathbb{E}, σ) of order d_u with $\sigma(z) = \rho z$. Since (\mathbb{F}, σ) is constant-stable, (\mathbb{E}, σ) is constant-stable by Proposition 32. Thus by part (3) of Proposition 42 we conclude that z is an R -monomial. In particular, since $d_i \mid d_u$ for all $1 \leq i \leq u$, there are $\nu_i \in \{0, \dots, d_u - 1\}$ with $\rho_i = \rho^{\nu_i}$. Consequently, $\sigma(\bar{g}_i) = \rho^{\nu_i} \alpha_i \bar{g}_i$ for all $1 \leq i \leq u$. Define $g'_i = z^{d_u - \nu_i} \bar{g}_i$. Then

$$\sigma(g'_i) = \sigma(z^{d_u - \nu_i} \bar{g}_i) = \rho^{d_u - \nu_i} \rho^{\nu_i} \alpha_i z^{d_u - \nu_i} \bar{g}_i = \alpha_i g'_i.$$

Finally, define the ring homomorphism $\lambda: \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbb{E}$ with $\lambda|_{\mathbb{E}} = \text{id}$ and $\lambda(x_i) = c_i g'_i$ for $1 \leq i \leq u$. Then by Lemma 56 it follows that λ is a difference ring homomorphism. By (42) we have $d_i = \text{ord}(\rho^{\nu_i}) = \text{ord}(\rho^{d_u - \nu_i})$ and by part 2 of Proposition 42 we get $d_i = \text{ord}(z^{\nu_i}) = \text{ord}(z^{d_u - \nu_i})$.

- (3) Let $\mathbb{E}_k = \mathbb{F}\langle x_1 \rangle \dots \langle x_k \rangle$ and denote by I_k the difference ideal $I_k := \ker(\lambda|_{\mathbb{E}_k})$.

¹⁶Since $\text{ord}(z^{d_u - \nu_i}) = d_i$, it follows that $z^{d_u - \nu_i} = z^{n_i \frac{d_u}{d_i}}$ for some $n_i \in \mathbb{N}$ with $1 \leq n_i < d_i$ and $\text{gcd}(n_i, d_i) = 1$.

Let (\mathbb{H}, σ) be the $R\Pi$ -extension of (\mathbb{F}, σ) from case (2a) with $\mathbb{H} = \mathbb{E}$ or case (2b) with $\mathbb{H} = \mathbb{E}[z]$. In any case,

$$\text{const}_\sigma \mathbb{H} = \mathbb{K}. \quad (43)$$

We show part (3) by induction on the number of P -monomials in $\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$. Since $\lambda|_{\mathbb{E}_0} = \lambda|_{\mathbb{F}} = \text{id}$, $I_0 = \{0\} = \langle \rangle$ and the statement holds. Now suppose that

$$I_{k-1} = \ker(\lambda|_{\mathbb{E}_{k-1}}) = \langle x_1^{d_1} - (c_1 \bar{g}_1)^{d_1}, \dots, x_{k-1}^{d_{k-1}} - (c_{k-1} \bar{g}_{k-1})^{d_{k-1}} \rangle_{\mathbb{E}_{k-1}} \quad (44)$$

where $\lambda(x_i^{d_i}) = (c_i \bar{g}_i)^{d_i}$ for $1 \leq i < k$.

Case 1: $k \leq u$. If $d_u = 1$, we have $\lambda(x_k) = c_k \bar{g}_k$. Since $d_k \mid d_u$, $d_k = 1$ and we get trivially $\lambda(x_k^{d_k}) = (c_k \bar{g}_k)^{d_k}$. Otherwise, if $d_u > 1$, we have $\lambda(x_k) = c_k z^{d_u - \nu_k} \bar{g}_k$ where $(z^{d_u - \nu_k})^{d_k} = 1$. Thus again $\lambda(x_k^{d_k}) = (c_k \bar{g}_k)^{d_k}$. Since $\lambda(c_k \bar{g}_k) = c_k \bar{g}_k$, we conclude for both cases that $\lambda(x_k^{d_k} - (c_k \bar{g}_k)^{d_k}) = 0$. Consequently

$$h := x_k^{d_k} - (c_k \bar{g}_k)^{d_k} \in I_k. \quad (45)$$

We will show that

$$I_k = \ker(\lambda|_{\mathbb{E}_k}) = \langle x_1^{d_1} - (c_1 \bar{g}_1)^{d_1}, \dots, x_k^{d_k} - (c_k \bar{g}_k)^{d_k}, h \rangle_{\mathbb{E}_k}. \quad (46)$$

The inclusion \supseteq holds trivially by (45). For the inclusion \subseteq two cases are considered. In what follows, $\overline{\text{deg}}$ is considered w.r.t. x_k .

Case 1.1: Suppose that there is no $\mu \in I_k \setminus \langle I_{k-1} \rangle_{\mathbb{E}_k}$ with $\overline{\text{deg}}(\mu) < d_k = \overline{\text{deg}}(h)$. Now let $f \in I_k$ be arbitrary but fixed. Then by polynomial division we can write $f = ah + b$ where $a, b \in \mathbb{E}_k$ with $\overline{\text{deg}}(b) < d_k$. Since $f, h \in I_k$, also $b \in I_k$. Thus $b \in \langle I_{k-1} \rangle_{\mathbb{E}_k}$ by the assumption of Case 1.1. Thus (46) holds with (44).

Case 1.2: Suppose that there is a $\mu \in I_k \setminus \langle I_{k-1} \rangle_{\mathbb{E}_k}$ with $\overline{\text{deg}}(\mu) < d_k$. Note that $\overline{\text{deg}}(\mu) \neq 0$, since otherwise $\mu = x^l c$ for some $l \in \mathbb{Z}$ and $c \in \mathbb{F}^*$. Thus $0 = \lambda(\mu) = \lambda(c) \lambda(x^l)$ with $\lambda(x^l) \neq 0$ which would imply $\lambda(c) = 0$. But then $\mu \in \langle I_{k-1} \rangle_{\mathbb{E}_k}$ which we have excluded. Among all $\mu \in I_k \setminus \langle I_{k-1} \rangle_{\mathbb{E}_k}$ with $0 < \overline{\text{deg}}(\mu) < d_k$, we take one such that $\overline{\text{deg}}(\mu)$ is minimal. Write $\mu = \sum_i f_i x_k^i$ with $f_i \in \mathbb{E}_{k-1}$. Now consider the Laurent polynomial $\mu' = \mu|_{x_1 \mapsto \lambda(x_1), \dots, x_{k-1} \mapsto \lambda(x_{k-1})}$ in x_k . Note that $\mu' \neq 0$ since otherwise $\lambda(f_i) = 0$ for all i and thus $\mu \in \langle I_{k-1} \rangle_{\mathbb{E}_k}$. In particular, μ' must depend on x_k , since $0 = \lambda(\mu) = \lambda(\mu') = \mu'|_{x_k \mapsto \lambda(x_k)}$.

If $d_{k-1} = 1$, $\lambda(x_1), \dots, \lambda(x_{k-1}) \in \mathbb{F}^*$ and thus $\mu' \in \mathbb{F}\langle x_k \rangle$ with $0 < \overline{\text{deg}}(\mu') < d_k$. Otherwise, if $d_{k-1} > 1$, $\mu' \in \mathbb{F}[z]\langle x_k \rangle$ with $0 < \overline{\text{deg}}(\mu') < d_k$. Write $\mu' = \sum_i \mu'_i x_k^i$ with $\mu'_i \in \mathbb{F}[z]$ where we can take $r \neq 0$ with $\mu'_r \neq 0$. Now consider $\tilde{\mu} = \mu'|_{x_k \mapsto z^{d_u - \nu_k} x_k}$. Then $\tilde{\mu} = \sum_i \mu'_i x_k^i (z^{d_u - \nu_k})^i$. Since $(z^{d_u - \nu_k})^r \neq 0$, $\mu'_r (z^{d_u - \nu_k})^r \neq 0$ and consequently $\tilde{\mu} \neq 0$. Now write $\tilde{\mu} = \sum_{i=0}^{d_u-1} \gamma_i z^i$ with $\gamma_i \in \mathbb{F}\langle x_k \rangle$. Note that $0 = \lambda(\mu') = \tilde{\mu}|_{x_k \mapsto \bar{g}_k}$ and thus $\tilde{\mu}$ depends on x_k . In particular, $0 < \overline{\text{deg}}(\tilde{\mu}) < d_k$. Furthermore, we can take an l with $\gamma_l \in \mathbb{F}\langle x_k \rangle$ and $0 < \overline{\text{deg}}(\gamma_l) < d_k$. Since $\mathbb{F}\langle x_k \rangle[z]$ is a $\mathbb{F}\langle x_k \rangle$ -module with basis $z^0, z^1, \dots, z^{d_u-1}$ and $0 = \tilde{\mu}|_{x_k \mapsto \bar{g}_k} = \sum_i (\gamma_i|_{x_k \mapsto \bar{g}_k}) z^i$, it follows that $\lambda(\gamma_i) = \gamma_i|_{x_k \mapsto \bar{g}_k} = 0$ for all i . In particular, this holds for γ_l . Hence, we get $\gamma_l \in \mathbb{F}\langle x_k \rangle \setminus \mathbb{F}$ with $0 < \overline{\text{deg}}(\gamma_l) < d_k$ and $\lambda(\gamma_l) = 0$. Summarizing there is a $\nu \in \mathbb{F}\langle x_k \rangle$ (for the case $d_{k-1} = 1$ we take $\nu = \mu'$ and for the case $d_{k-1} > 1$, we take $\nu = \gamma_l$) such that $\lambda(\nu) = 0$ and $0 < \overline{\text{deg}}(\nu) < d_{k-1}$. Note that $(\mathbb{F}\langle x_k \rangle, \sigma)$ is a P -extension of (\mathbb{F}, σ) and $\lambda|_{\mathbb{F}\langle x_k \rangle}$ is a difference ring homomorphism with $\lambda|_{\mathbb{F}} = \text{id}$. Furthermore, since (35) is a basis of $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$, it follows that $M((\alpha_k), \mathbb{F}) = \langle d_k \rangle_{\mathbb{Z}}$. Consequently, we may apply Lemma 57 and conclude that $\ker(\lambda|_{\mathbb{F}\langle x_k \rangle}) = \langle m \rangle_{\mathbb{F}\langle x_k \rangle}$ for some $m \in \mathbb{F}\langle x_k \rangle$.

with $\overline{\deg}(m) = \deg(m) = d_k$; a contradiction to the existence of ν .

Case 2: $k > u$. Suppose that $f = \sum_i f_i x_k^i \in I_k$. As in the previous case define $f' = f|_{x_1 \mapsto \lambda(x_1), \dots, x_{k-1} \mapsto \lambda(x_{k-1})}$. Note that $0 = \lambda(f) = f'|_{x_k \mapsto x_k} = f'$. Thus $\lambda(f_i) = 0$ for all i and therefore $f \in \langle I_{k-1} \rangle_{\mathbb{E}_k}$. This proves that $I_k = \langle I_{k-1} \rangle_{\mathbb{E}_k}$ and thus $I_k = \langle x_1^{d_1} - (c_1 \bar{g}_1)^{d_1}, \dots, x_u^{d_u} - (c_u \bar{g}_u)^{d_u} \rangle_{\mathbb{E}_k}$ by the induction assumption. Finally suppose that (\mathbb{F}, σ) is computable and one can solve homogeneous first-order difference equations in (\mathbb{F}, σ) . Since (\mathbb{F}, σ) is radical-stable, it is also radical-solvable by Lemma 46. Thus for $1 \leq i \leq u$ one can compute the d_i th roots of unity $\rho_i \in \mathbb{K}^*$ and $g'_i \in \mathbb{F}^*$ for $1 \leq i \leq u$ with $\sigma(g'_i) = \rho_i \alpha_i g'_i$ which enables one to define λ explicitly. In particular, the generators of $\ker(\lambda)$ can be calculated. \square

Example 59 (Cont. Ex. 55). Recall that (38) is a basis of $M((\alpha_1, \alpha_2, \alpha_3, \alpha_4), \mathbb{F})$ with (36). Thus by part (1) of Lemma 58 we can construct the Π -extension (\mathbb{E}, σ) of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle x_3 \rangle \langle x_4 \rangle$ and $\sigma(x_3) = \alpha_3 x_3$, $\sigma(x_4) = \alpha_4 x_4$. In particular, by part (2b) of Lemma 58, we can take the R -extension $(\mathbb{E}[z], \sigma)$ of (\mathbb{E}, σ) with $\sigma(z) = -z$. Furthermore, we can compute the solution $\bar{g}_1 = (4+x)^2(5+x)^2 \in \mathbb{K}(x)$ for $\sigma(g_1) = \alpha_1 g_1$. In addition, in Example 54 we obtained \bar{g}_2 with (34) such that $\sigma(\bar{g}_2) = -\alpha_2 \bar{g}_2$ holds. With these \bar{g}_i we can now define the ring homomorphism $\lambda: \mathbb{H} \rightarrow \mathbb{K}(x)\langle x_3 \rangle \langle x_4 \rangle [z]$ with $\mathbb{H} = \mathbb{K}(x)\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle$ given by $\lambda|_{\mathbb{K}(x)} = \text{id}$ and

$$\begin{aligned} \lambda(x_1) &= c_1 \bar{g}_1 = c_1(4+x)^2(5+x)^2 \\ \lambda(x_2) &= c_2 \bar{g}_2 z = c_2(1+x)^2(2+x)^5(3+x)^8(4+x)(5+x)z \\ \lambda(x_3) &= x_3 \\ \lambda(x_4) &= x_4 \end{aligned} \tag{47}$$

for any $c_1, c_2 \in \mathbb{K}^*$. By part (2b) of Lemma 58 this forms a difference ring homomorphism. Finally, by part (3) of Lemma 58 we obtain

$$\begin{aligned} \ker(\lambda) &= \langle x_1 - (c_1 \bar{g}_1)^{1/d_1}, x_2^2 - (c_2 \bar{g}_2)^{2/d_2} \rangle_{\mathbb{H}} = \langle x_1 - c_1(4+x)^2(5+x)^2, \\ &\quad x_2^2 - c_2^2(1+x)^4(2+x)^{10}(3+x)^{16}(4+x)^2(5+x)^2 \rangle_{\mathbb{H}}. \end{aligned}$$

Specialize Lemma 58 to Theorem 60 yields the following solution of Problem DR.

Theorem 60. Let (\mathbb{F}, σ) be a radical-stable difference field with $\mathbb{K} = \text{const}_\sigma \mathbb{F}$ equipped with a \mathbb{K} -embedding $\bar{\tau}: \mathbb{F} \rightarrow \mathbf{S}(\mathbb{K})$. Let $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle, \sigma)$ be a P -extension of (\mathbb{F}, σ) with $\alpha_i = \frac{\sigma(x_i)}{x_i} \in \mathbb{F}^*$ and let $\tau: \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbf{S}(\mathbb{K})$ be a \mathbb{K} -homomorphism with $\tau|_{\mathbb{F}} = \bar{\tau}$. Suppose that (35) with $u \geq 1$ and $d_1 \mid \dots \mid d_u$ is a basis of $M((\alpha_1, \dots, \alpha_r), \mathbb{F}) \neq \{\mathbf{0}\}$. Then the following holds.

- (1) $\tau|_{\mathbb{E}}$ with $\mathbb{E} = \mathbb{F}\langle x_{u+1} \rangle \dots \langle x_r \rangle$ is a \mathbb{K} -embedding where (\mathbb{E}, σ) is a Π -extension of (\mathbb{F}, σ) .
- (2a) If $d_r = 1$, there are $\bar{g}_i \in \mathbb{F}^*$ with $\sigma(\bar{g}_i) = \alpha_i \bar{g}_i$ for $1 \leq i \leq u$. Furthermore, one can refine λ from (2a) of Lemma 58 by appropriate $c_1, \dots, c_u \in \mathbb{K}^*$ such that $\tau|_{\mathbb{E}}(\lambda(f)) = \tau(f)$ for all $f \in \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$ holds, i.e., the following diagram commutes:

$$\begin{array}{ccc} \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle & \xrightarrow{\lambda} & \mathbb{E} \\ & \searrow \tau & \downarrow \tau|_{\mathbb{E}} \\ & & \mathbf{S}(\mathbb{K}). \end{array} \tag{48}$$

- (2b) Otherwise, if $d_u > 1$, one can take the R -extension $(\mathbb{E}[z], \sigma)$ of (\mathbb{E}, σ) with order d_u from part (2b) of Lemma 58 and the \mathbb{K} -homomorphism $\tau': \mathbb{E}[z] \rightarrow \mathcal{S}(\mathbb{K})$ with $\tau'|_{\mathbb{E}} = \tau|_{\mathbb{E}}$ and $\tau'(z) = \langle \rho^i \rangle_{i \geq 0}$ which forms a \mathbb{K} -embedding. Furthermore, one can take $\bar{g}_i \in \mathbb{F}^*$ and $\nu_i \in \mathbb{N}$ for $1 \leq i \leq u$ with $\sigma(\bar{g}_i) = \rho^{\nu_i} \alpha_i \bar{g}_i$, and one can refine λ from (2b) of Lemma 58 by appropriate $c_1, \dots, c_u \in \mathbb{K}^*$ such that $\tau'(\lambda(f)) = \tau(f)$ for all $f \in \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$ holds, i.e., the following diagram commutes:

$$\begin{array}{ccc}
 \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle & \xrightarrow{\lambda} & \mathbb{E}[z] \\
 & \searrow \tau & \downarrow \tau' \\
 & & \mathcal{S}(\mathbb{K}).
 \end{array} \tag{49}$$

- (3) $\ker(\tau) = \ker(\lambda) = \langle x_1^{d_1} - (c_1 \bar{g}_1)^{d_1}, \dots, x_u^{d_u} - (c_u \bar{g}_u)^{d_u} \rangle_{\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle}$ where the c_i and \bar{g}_i are given by (2a) or (2b), respectively.

If^{d7} (\mathbb{F}, σ) is in addition computable and one can solve first-order homogeneous difference equations in (\mathbb{F}, σ) , then one can compute (\mathbb{E}, σ) , λ is computable and the generators of $\ker(\lambda) = \ker(\tau)$ can be given explicitly.

Proof. (1) Since (\mathbb{E}, σ) is a Π -extension of (\mathbb{F}, σ) , $\tau|_{\mathbb{E}}$ is injective by Theorem 24.

(2a) Suppose that $d_1 = \dots = d_u = 1$. For $1 \leq i \leq u$ we have $\bar{g}_i \in \mathbb{F}^*$ with $\sigma(\bar{g}_i) = \alpha_i \bar{g}_i$. Thus $\sigma(\frac{x_i}{\bar{g}_i}) = \frac{x_i}{\bar{g}_i}$ and consequently $S(\tau(\frac{x_i}{\bar{g}_i})) = \tau(\sigma(\frac{x_i}{\bar{g}_i})) = \tau(\frac{x_i}{\bar{g}_i})$. This implies that $\tau(\frac{x_i}{\bar{g}_i})$ is a constant sequence, i.e., $\tau(\frac{x_i}{\bar{g}_i}) = \tau(c_i)$ for some $c_i \in \mathbb{K}$. In particular, $\tau(x_i) = \tau(c_i \bar{g}_i)$. By part (1) of Lemma 6, $\tau(x_i) \neq \mathbf{0}$ and thus $c_i \neq 0$. Therefore we can refine the difference ring homomorphism $\lambda: \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbb{E}$ with $\lambda|_{\mathbb{E}} = \text{id}$ and (40) with the particular choice of c_i given above and get $\tau(\lambda(f)) = \tau(f)$ for all $f \in \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$.

(2b) Suppose that $d_u > 1$ and consider the $R\Pi$ -extension $(\mathbb{E}[z], \sigma)$ of (\mathbb{F}, σ) . By Theorem 24 it follows that the \mathbb{K} -homomorphism $\tau': \mathbb{E}[z] \rightarrow \mathcal{S}(\mathbb{K})$ with $\tau'|_{\mathbb{E}} = \tau|_{\mathbb{E}}$ and $\tau'(z) = \langle \rho^i \rangle_{i \geq 0}$ is injective. As in (2a) we can conclude that there are $c_i \in \mathbb{K}^*$ for $1 \leq i \leq u$ such that $\tau(x_i) = \tau'(c_i z^{d_u - \nu_i} \bar{g}_i)$. Therefore we can refine as in case (2a) the difference ring homomorphism $\lambda: \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbb{E}$ with $\lambda|_{\mathbb{E}} = \text{id}$ and $\lambda(x_i) = c_i \bar{g}_i z^{d_u - \nu_i}$ for $1 \leq i \leq u$ and get $\tau'(\lambda(f)) = \tau(f)$ for all $f \in \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$.

(3) By Lemma 26 we conclude that $\ker(\lambda) = \ker(\tau)$. Thus with part (3) of Lemma 58 the statement is proven.

Suppose that one can solve first-order homogeneous linear difference equations in (\mathbb{F}, σ) . Then by Lemma 58 λ can be given with generic $c_i \in \mathbb{K}^*$ and the generators of $\ker(\lambda)$ can be computed. Since τ is σ^σ -computable, one can determine the c_i for $1 \leq i \leq u$ with $\tau(x_i) = \tau(c_i \bar{g}_i)$ in case 2a or $\tau(x_i) = \tau'(c_i \bar{g}_i z^{d_u - \nu_i})$ in case 2b. \square

Example 61 (Cont. Ex. 59). As elaborated in Example 59 we can take the $R\Pi$ -extension $(\mathbb{E}[z], \sigma)$ of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle x_3 \rangle \langle x_4 \rangle$ and $\sigma(x_3) = \alpha_3 x_3$, $\sigma(x_4) = \alpha_3 x_4$ where the α_3, α_4 are given in (36) and $\sigma(z) = -z$. Now take the evaluation function $\text{ev}': \mathbb{E}[z] \times \mathbb{N} \rightarrow \mathbb{K}$ for $(\mathbb{E}[z], \sigma)$ with $\text{ev}'_{\mathbb{E} \times \mathbb{N}} = \text{ev}|_{\mathbb{E} \times \mathbb{N}}$ and $\text{ev}'(z, n) = (-1)^n$ where $\text{ev}: \mathbb{F}\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle \times \mathbb{N} \rightarrow \mathbb{K}$ is given in Example 55. This gives the \mathbb{K} -embedding $\tau': \mathbb{E}[z] \rightarrow \mathcal{S}(\mathbb{K})$ with $\tau'(f) = (\text{ev}'(f, n))_{n \geq 0}$. By the ansatz $\tau(x_i) = \tau(c_i \bar{g}_i)$ with $i = 1, 2$ for the given \bar{g}_i in Example 59, i.e., by $\text{ev}(x_i, n) =$

¹⁷Note that all the requirements of Assumption 28 except item (5) are needed.

$c_i \operatorname{ev}(\bar{g}_i, n)$, we conclude that $c_1 = \frac{1}{400}$ and $c_2 = \frac{1}{4199040}$. Thus with these particular values we obtain the surjective difference ring homomorphism $\lambda: \mathbb{H} \rightarrow \mathbb{E}$ with $\mathbb{H} = \mathbb{F}\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle$, $\lambda|_{\mathbb{F}} = \operatorname{id}$ and (47) such that the diagram (49) commutes. In particular, we get

$$\begin{aligned} \ker(\tau) = \ker(\lambda) &= \langle x_1 - (c_1 \bar{g}_1)^1, x_2^2 - (c_2 \bar{g}_2)^2 \rangle_{\mathbb{H}} = \langle x_1 - \frac{1}{400}(4+x)^2(5+x)^2, \\ & x_2^2 - \frac{1}{4199040^2}(1+x)^4(2+x)^{10}(3+x)^{16}(4+x)^2(5+x)^2 \rangle_{\mathbb{H}}. \end{aligned} \quad (50)$$

Note that $\tau = \tau' \circ \lambda$ implies that

$$\operatorname{ev}(x_1, n) = \frac{(4+n)^2(5+n)^2}{400}, \quad \operatorname{ev}(x_2, n) = \frac{(1+n)^2(2+n)^5(3+n)^8(4+n)(5+n)(-1)^n}{4199040}$$

holds. In short, we derived a simplification of the products given on the right-hand sides of $\operatorname{ev}(x_1, n)$ and $\operatorname{ev}(x_2, n)$ in (37).

Finally, we will show in Theorem 63 that the difference ring construction in Theorem 60 is optimal. For this task we will use

Lemma 62. *Let (\mathbb{E}, σ) be a Π -extension of a difference field (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$ and $f_i = \frac{\sigma(x_i)}{x_i} \in \mathbb{F}^*$ for $1 \leq i \leq r$, and let (\mathbb{H}, σ) be an $R\Pi$ -extension of $\mathbb{H} = \mathbb{F}\langle y_1 \rangle \dots \langle y_s \rangle [z_1] \dots [z_l]$ where the y_i with $1 \leq i \leq s$ are Π -monomials with $\alpha_i = \frac{\sigma(y_i)}{y_i} \in \mathbb{F}\langle y_1 \rangle \dots \langle y_{i-1} \rangle^*$ and the z_i with $1 \leq i \leq l$ are R -monomials with $a_i = \frac{\sigma(z_i)}{z_i} \in (\operatorname{const}_{\sigma} \mathbb{F})^*$. If there is a difference ring embedding $\lambda: \mathbb{E} \rightarrow \mathbb{H}$ with $\lambda|_{\mathbb{F}} = \operatorname{id}$, then $r \leq s$.*

Proof. Let $\mathbb{K} = \operatorname{const}_{\sigma} \mathbb{F}$ and suppose that $r > s$. For any $i \in \mathbb{N}$ with $1 \leq i \leq r$ we have $\frac{\sigma(\lambda(x_i))}{\lambda(x_i)} = \lambda\left(\frac{\sigma(x_i)}{x_i}\right) = \lambda(f_i) = f_i$. With Proposition 36 we get $\lambda(x_i) = g_i y_1^{n_{i,1}} \dots y_s^{n_{i,s}} z_1^{m_{i,1}} \dots z_l^{m_{i,l}}$ for some $n_{i,j} \in \mathbb{Z}$ with $1 \leq j \leq s$, $m_{i,j} \in \mathbb{N}$ with $1 \leq j \leq l$ and $g_i \in \mathbb{F}^*$. In particular, we get

$$f_i = \frac{\sigma(g_i)}{g_i} \alpha_1^{n_{i,1}} \dots \alpha_s^{n_{i,s}} a_1^{m_{i,1}} \dots a_l^{m_{i,l}}. \quad (51)$$

Since $r > s$, there is a nonzero vector $(\xi_1, \dots, \xi_r) \in \mathbb{Z}^r$ with

$$\begin{pmatrix} n_{1,1} & n_{2,1} & \dots & n_{r,1} \\ n_{1,2} & n_{2,2} & \dots & n_{r,2} \\ \vdots & \vdots & \dots & \vdots \\ n_{1,s} & n_{2,s} & \dots & n_{r,s} \end{pmatrix} \begin{pmatrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_r \end{pmatrix} = \mathbf{0}. \quad (52)$$

Exponentiation of (51) with ξ_i and multiplying these equations for $1 \leq i \leq r$ yield

$$f_1^{\xi_1} \dots f_r^{\xi_r} = \frac{\sigma(g_1^{\xi_1} \dots g_r^{\xi_r})}{g_1^{\xi_1} \dots g_r^{\xi_r}} \alpha_1^{\tilde{n}_1} \dots \alpha_s^{\tilde{n}_s} a_1^{\tilde{m}_1} \dots a_l^{\tilde{m}_l}$$

with $\tilde{n}_i = n_{1,i}\xi_1 + \dots + n_{r,i}\xi_r = 0$ for $1 \leq i \leq s$ and $\tilde{m}_i = m_{1,i}\xi_1 + \dots + m_{r,i}\xi_r \in \mathbb{N}$ for $1 \leq i \leq l$. With (52) we obtain

$$f_1^{\xi_1} \dots f_r^{\xi_r} = \frac{\sigma(\gamma)}{\gamma} \tilde{a}$$

where $\gamma = g_1^{\xi_1} \dots g_r^{\xi_r} \in \mathbb{F}^*$ and $\tilde{a} = a_1^{\tilde{m}_1} \dots a_l^{\tilde{m}_l} \in \mathbb{K}^*$. Since a_1, \dots, a_l are roots of unity, also \tilde{a} is a root of unity. Hence we can take a $\nu \in \mathbb{N}$ with $\tilde{a}^{\nu} = 1$. Thus

$$f_1^{\nu \xi_1} \dots f_r^{\nu \xi_r} = \frac{\sigma(\gamma^{\nu})}{\gamma^{\nu}}$$

and consequently $(\mathbb{F}\langle y_1 \rangle \dots \langle y_r \rangle, \sigma)$ is not a Π -extension of (\mathbb{F}, σ) by Proposition 40, a contradiction. \square

Theorem 63. *Suppose that the properties of (\mathbb{F}, σ) and $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle, \sigma)$ as stated in Theorem 60 hold. Then the constructions in (2a) and (2b) of Theorem 60 are optimal: For any RII-extension (\mathbb{H}, σ) of (\mathbb{F}, σ) where $\mathbb{H} = \mathbb{F}\langle y_1 \rangle \dots \langle y_e \rangle [z_1] \dots [z_l]$ with Π -monomials y_i ($\frac{\sigma(y_i)}{y_i} \in \mathbb{F}\langle y_1 \rangle \dots \langle y_{i-1} \rangle^*$) and R -monomials z_i ($\frac{\sigma(z_i)}{z_i} \in \mathbb{K}^*$) equipped with a difference ring homomorphism $\lambda': \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbb{H}$ with $\lambda'|_{\mathbb{F}} = \text{id}$ and \mathbb{K} -embedding $\tau'': \mathbb{H} \rightarrow \mathbf{S}(\mathbb{K})$ with $\tau''|_{\mathbb{F}} = \bar{\tau}$ such that*

$$\begin{array}{ccc} \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle & \xrightarrow{\lambda'} & \mathbb{H} \\ & \searrow \tau & \downarrow \tau'' \\ & & \mathbf{S}(\mathbb{K}) \end{array} \quad (53)$$

commutes, the following holds.

- (1) $r - u \leq e$.
- (2) In addition, if $d_u > 1$, then $l \geq 1$ and

$$\text{ord}(z) \leq \text{lcm}(\text{ord}(z_1), \dots, \text{ord}(z_l)) = \text{ord}(z_1) \dots \text{ord}(z_l). \quad (54)$$

Proof. (1) Within both constructions of (2a) and (2b) in Theorem 60 we have $\lambda(\mathbb{F}\langle x_{u+1} \rangle \dots \langle x_r \rangle) = \mathbb{F}\langle x_{u+1} \rangle \dots \langle x_r \rangle =: \mathbb{E}$. Thus

$$\tau(\mathbb{F}\langle x_{u+1} \rangle \dots \langle x_r \rangle) = \mathbb{H}_1$$

with $\mathbb{H}_1 = \tau(\lambda(\mathbb{F}\langle x_{u+1} \rangle \dots \langle x_r \rangle)) = \tau(\mathbb{F})\langle \tau(x_{u+1}) \rangle \dots \langle \tau(x_r) \rangle$ with $\frac{S(\tau(x_i))}{\tau(x_i)} = \tau(\frac{\sigma(x_i)}{x_i}) \in \tau(\mathbb{F})$ for $u+1 \leq i \leq r$. Since $\tau|_{\mathbb{E}}$ is a difference ring embedding, (\mathbb{H}_1, S) is a Π -extension of $(\tau(\mathbb{F}), \sigma)$ with the Π -monomials $\tau(x_i)$ for $u+1 \leq i \leq r$. Furthermore,

$$\tau''(\mathbb{F}\langle y_1 \rangle \dots \langle y_e \rangle [z_1] \dots [z_l]) = \mathbb{H}_2$$

with $\mathbb{H}_2 = \tau''(\mathbb{F})\langle \tau''(y_1) \rangle \dots \langle \tau''(y_e) \rangle [\tau''(z_1)] \dots [\tau''(z_l)]$. As τ'' is a difference ring embedding, (\mathbb{H}_2, S) is an RII-extension of $(\tau''(\mathbb{F}), S)$. Since $\tau(f) = \tau''(\lambda'(f))$ for all $f \in \mathbb{E}$, (\mathbb{H}_1, S) is a subdifference ring of (\mathbb{H}_2, S) . In particular, there is the trivial difference ring embedding $\tilde{\lambda}: \mathbb{H}_1 \rightarrow \mathbb{H}_2$ with $\tilde{\lambda} = \text{id}$. Hence we can apply Lemma 62 and we conclude that $r - u \leq e$.

(2) If $d_u > 1$, it remains to show that the order of the R -monomial z in our construction (2b) is optimal. By (41) and $\alpha_u := \frac{\sigma(x_u)}{x_u} \in \mathbb{F}^*$ we get

$$\alpha_u = \lambda(\alpha_u) = \lambda\left(\frac{\sigma(x_u)}{x_u}\right) = \frac{\sigma(\lambda(x_u))}{\lambda(x_u)} = \rho^{d_u - \nu_u} \frac{\sigma(\bar{g}_u)}{\bar{g}_u} \quad (55)$$

for some $\bar{g}_u \in \mathbb{F}^*$ and $0 \leq \nu_u \leq d_u - 1$ with

$$\text{ord}(\rho^{d_u - \nu_u}) = d_u. \quad (56)$$

By assumption we have

$$\alpha_u = \lambda'(\alpha_u) = \lambda'\left(\frac{\sigma(x_u)}{x_u}\right) = \frac{\sigma(\lambda'(x_u))}{\lambda'(x_u)}, \quad (57)$$

and by Proposition 36 we get

$$\lambda'(x_u) = h y_1^{n_1} \dots y_e^{n_e} z_1^{m_1} \dots z_l^{m_l} \quad (58)$$

with $n_i \in \mathbb{Z}$ for $1 \leq i \leq e$, $m_i \in \mathbb{N}$ where¹⁸ $1 \leq m_i \leq \text{ord}(z_i)$ for $1 \leq i \leq l$ and $h \in \mathbb{F}^*$. Let $a_i = \frac{\sigma(y_i)}{y_i} \in \mathbb{F}\langle y_1 \rangle \dots \langle y_{i-1} \rangle^*$ for $1 \leq i \leq e$ and let $\gamma_i = \frac{\sigma(z_i)}{z_i} \in \mathbb{K}^*$ for $1 \leq i \leq l$ where the γ_i are roots of unity. Then plugging (58) into (57) yields

$$\alpha_u = \frac{\sigma(h)}{h} a_1^{n_1} \dots a_{n_e}^{n_e} b \quad (59)$$

with

$$b = \gamma_1^{m_1} \dots \gamma_l^{m_l} \in \mathbb{K}^* \quad (60)$$

being a root of unity. Note that we also cover the case $l = 0$ (i.e., no R -monomials arise); then we simply get $b = 1$. Combining (55) with (59) gives

$$\frac{\sigma(\gamma)}{\gamma} a_1^{n_1} \dots a_{n_e}^{n_e} = \frac{\rho^{d_u - \nu_u}}{b} =: w \in \mathbb{K}^* \quad (61)$$

with $\gamma = \frac{h}{g_u} \in \mathbb{F}^*$. Since the right-hand side $w \in \mathbb{K}^*$ of the last equation is also a root of unity, we can choose a $k > 0$ such that $w^k = 1$. Thus $\frac{\sigma(\gamma^k)}{\gamma^k} a_1^{k n_1} \dots a_e^{k n_e} = 1$. Suppose that $(n_1, \dots, n_e) \neq \mathbf{0}$ and let ν be maximal such that $n_\nu \neq 0$. Then $\sigma(v) = a_\nu^{-k n_\nu} v$ with $v := \gamma^k y_1^{k n_1} \dots y_{\nu-1}^{k n_{\nu-1}} \in \mathbb{F}\langle y_1 \rangle \dots \langle y_{\nu-1} \rangle \setminus \{0\}$. This contradicts to Proposition 39 and the assumption that y_ν is a Π -monomial. Thus $n_1 = \dots = n_e = 0$ and hence with (61) we get

$$\frac{\sigma(\gamma)}{\gamma} = w (= \frac{\rho^{d_u - \nu_u}}{b}). \quad (62)$$

Therefore $\sigma^k(\gamma) = \sigma^{k-1}(w\gamma) = w\sigma^{k-1}(\gamma) = \dots = w^k \gamma = \gamma$ and thus $\gamma \in \text{const}_{\sigma^k} \mathbb{F}$. Since there is a \mathbb{K} -embedding $\bar{\tau}: \mathbb{F} \rightarrow \mathbf{S}(\mathbb{K})$, (\mathbb{F}, σ) is constant-stable by Lemma 35. Thus $\gamma \in \mathbb{K}^*$. With (62) it follows that $\rho^{\nu_u} = b$. Further, with (56) we get $\text{ord}(b) = d_u > 1$. In particular, by (60) we obtain $l \geq 1$. Furthermore,

$$d_u = \text{ord}(\rho^{\nu_u}) = \text{ord}(b) = \frac{\text{ord}(\gamma_1) \dots \text{ord}(\gamma_l)}{m_1 \dots m_l}. \quad (63)$$

The last equality follows from Proposition 44: the γ_i are roots of unity where $\text{gcd}(\text{ord}(\gamma_i), \text{ord}(\gamma_j)) = 1$ for pairwise different i, j . Together with (56) we get $d_u \mid \text{ord}(z_1) \dots \text{ord}(z_e) = \text{lcm}(\text{ord}(\alpha_1), \dots, \text{ord}(\alpha_e)) = \text{lcm}(\text{ord}(z_1), \dots, \text{ord}(z_e))$. \square

Example 64 (Cont. Example 61). *In order to rephrase $(\mathbb{K}(x)\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle, \sigma)$ from Example 61 in an RII-extension, one needs at least 2 Π -monomials and one R -monomial of order 2. Such an optimal choice is given by the RII-extension $(\mathbb{K}(x)\langle x_3 \rangle \langle x_4 \rangle [z], \sigma)$ of (\mathbb{K}, σ) in Example 61.*

5. THE SOLUTION OF PROBLEM DR FOR THE GENERAL CASE

Finally, suppose that we are given a difference field (\mathbb{F}, σ) with constant field \mathbb{K} equipped with an evaluation function $\text{ev}: \mathbb{F} \times \mathbb{N} \rightarrow \mathbb{K}$ that satisfies the properties enumerated in Assumption 28. In particular, suppose that the \mathbb{K} -homomorphism $\bar{\tau}: \mathbb{F} \rightarrow \mathbf{S}(\mathbb{K})$ defined by $\bar{\tau}(f) = (\text{ev}(f, n))_{n \geq 0}$ for $f \in \mathbb{F}$ is injective.

We will solve Problem DR for a general P -extension (\mathbb{E}, σ) of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle$ and $\hat{\alpha}_i = \frac{\sigma(\hat{x}_i)}{\hat{x}_i} \in \mathbb{F}^*$ for $1 \leq i \leq r$ equipped with an evaluation function $\text{ev}: \mathbb{E} \times \mathbb{N} \rightarrow \mathbb{K}$ where $\text{ev}|_{\mathbb{F} \times \mathbb{N}} = \bar{\text{ev}}$. Note that for the \mathbb{K} -homomorphism $\tau: \mathbb{E} \rightarrow \mathbf{S}(\mathbb{K})$ defined by $\tau(f) = (\text{ev}(f, n))_{n \geq 0}$ for $f \in \mathbb{E}$ we have $\tau|_{\mathbb{F}} = \bar{\tau}$.

¹⁸For (63) we will require that $m_i \neq 0$. Thus we allow $m_i = \text{ord}(z_i)$ instead of $m_i = 0$.

We start to compute a basis $\mathcal{B} = \{z_{i1}, \dots, z_{ir}\}_{1 \leq i \leq u}$ of the \mathbb{Z} -module $\hat{V} = M((\hat{\alpha}_1, \dots, \hat{\alpha}_r), \mathbb{F})$ of \mathbb{Z}^r ; this is possible by the requirement (5) in Assumption 28.

Then we distinguish two cases. If the rank of \hat{V} is $u = 0$, i.e., $\hat{V} = \{0\}$, we can conclude that (\mathbb{E}, σ) is a Π -extension of (\mathbb{F}, σ) by Proposition 40 and that $\tau: \mathbb{E} \rightarrow \mathbf{S}(\mathbb{K})$ is injective by Theorem 24. Thus we can take $\mathbb{H} := \mathbb{E}$, $\lambda := \text{id}$ and $\tau' := \tau$ and obtain a solution of Problem *DR* where λ is even bijective. Since $\ker(\tau) = \{0\}$, there is no non-zero Laurent polynomial in \mathbb{E} whose sequence evaluation turns to the zero-sequence. Finally note that there is no solution of Problem *DR* with a Π -extension with less than r Π -monomials by Lemma 62.

In order to treat the remaining case where \hat{V} has rank $u \geq 1$, we compute the Smith normal form¹⁹

$$\begin{pmatrix} d_1 & 0 & \dots & \dots & \dots & 0 \\ & \ddots & & & & \\ & & d_u & 0 & \dots & 0 \end{pmatrix} \in \mathbb{Z}^{u \times r} \quad (64)$$

with $d_1, \dots, d_u \in \mathbb{N} \setminus \{0\}$ and $d_1 \mid d_2 \mid \dots \mid d_u$ of the integer matrix $Z = (z_{ij})_{ij} \in \mathbb{Z}^{u \times r}$ whose entries are given from \mathcal{B} . In particular, we can compute matrices $A \in \mathbb{Z}^{u \times u}$ and $B \in \mathbb{Z}^{r \times r}$ being invertible over \mathbb{Z} with

$$AZB = D. \quad (65)$$

Note that for any invertible matrix $C \in \mathbb{Z}^{u \times u}$ over \mathbb{Z} , D is again the Smith normal form of $CZ = (\tilde{b}_{ij})_{ij}$. Moreover observe that $\tilde{\mathcal{B}} = \{\tilde{b}_{i1}, \dots, \tilde{b}_{ir}\}_{1 \leq i \leq u}$ is again a basis of \hat{V} . In particular C can be considered as a basis transform between the two bases \mathcal{B} and $\tilde{\mathcal{B}}$. In other words, for any choice of basis of \hat{V} , we obtain the same Smith normal form D . We call u the *rank* and d_r the *largest divisor* of \hat{V} .

Example 65. Take the P -extension $(\mathbb{F}\langle \hat{x}_1 \rangle \langle \hat{x}_2 \rangle \langle \hat{x}_3 \rangle \langle \hat{x}_4 \rangle, \sigma)$ of (\mathbb{F}, σ) with $\sigma(\hat{x}_i) = \hat{\alpha}_i \hat{x}_i$ for $1 \leq i \leq 4$ where the $\hat{\alpha}_i$ are given in (17) Using Karr's algorithm [18] we can compute the basis $\{(-6, 0, -4, 6), (0, 1, 0, -2)\}$ of $\hat{V} = M((\hat{\alpha}_1, \hat{\alpha}_2, \hat{\alpha}_3, \hat{\alpha}_4), \mathbb{F})$. We calculate the Smith normal form of $Z = \begin{pmatrix} -6 & 0 & -4 & 6 \\ 0 & 1 & 0 & -2 \end{pmatrix}$ and get

$$\underbrace{\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}}_{=A} Z \underbrace{\begin{pmatrix} -1 & 1 & -2 & 1 \\ 1 & 0 & 0 & 2 \\ 2 & -2 & 3 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}_{=B} = \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}}_{=D}. \quad (66)$$

Thus $u = 2$ and $d_1 = 1$, $d_2 = 2$; in particular the largest divisor of \hat{V} is 2.

In the following we will show how one can solve Problem *DR* under the assumption that a basis of $\hat{V} = M((\hat{\alpha}_1, \dots, \hat{\alpha}_r), \mathbb{F})$ is given. For this task, the following two observations are central.

- (1) Let $\tilde{b}_{i,j} \in \mathbb{Z}$ be the coefficients of the inverse matrix B , i.e., $B^{-1} = (\tilde{b}_{ij})_{ij}$ and define the P -extension $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle, \sigma)$ of (\mathbb{F}, σ) with

$$\frac{\sigma(x_i)}{x_i} = \alpha_1^{\tilde{b}_{i1}} \dots \alpha_r^{\tilde{b}_{ir}} =: \alpha_i \in \mathbb{F} \quad 1 \leq i \leq r. \quad (67)$$

¹⁹So far it was sufficient in our applications to use the standard algorithm (see, e.g. [12]) based on column and row reductions to calculate the Smith Normal form for integer matrices. For faster algorithms we refer to [30, 45]. For an excellent survey on the available strategies see also [14].

Then by Lemma 67 below the difference ring $(\mathbb{F}\langle\hat{x}_1\rangle\dots\langle\hat{x}_r\rangle, \sigma)$ is isomorphic to the difference ring $(\mathbb{F}\langle x_1\rangle\dots\langle x_r\rangle, \sigma)$, i.e., they cannot be distinguished up to renaming of the arising objects by an explicitly given bijective map $\mu: \mathbb{F}\langle\hat{x}_1\rangle\dots\langle\hat{x}_r\rangle \rightarrow \mathbb{F}\langle x_1\rangle\dots\langle x_r\rangle$.

- (2) Furthermore, using Lemma 66 below one can read off a basis of $V = M(\alpha_1, \dots, \alpha_r, \mathbb{F})$ by looking at the matrix D from (64): it is simplify (35).

Thus using the difference ring isomorphism μ^{-1} one can carry over all the results of Section 4, in particular Theorem 63 can be extended from the special case $(\mathbb{F}\langle x_1\rangle\dots\langle x_r\rangle, \sigma)$ to the general version $(\mathbb{F}\langle\hat{x}_1\rangle\dots\langle\hat{x}_r\rangle, \sigma)$.

Lemma 66. *Let (\mathbb{F}, σ) be a difference field with $(\hat{\alpha}_1, \dots, \hat{\alpha}_r) \in (\mathbb{F}^*)^r$. Take a basis $\{(z_{i1}, \dots, z_{ir})\}_{1 \leq i \leq u}$ of $M((\hat{\alpha}_1, \dots, \hat{\alpha}_r), \mathbb{F})$, in particular, take $w_i \in \mathbb{F}^*$ for $1 \leq i \leq u$ with*

$$\frac{\sigma(w_i)}{w_i} = \hat{\alpha}_1^{z_{i1}} \dots \hat{\alpha}_r^{z_{ir}}.$$

Consider the Smith normal form of $Z = (z_{ij})_{ij} \in \mathbb{Z}^{u \times r}$, i.e., the equation (65) holds for some $A = (a_{ij})_{ij} \in \mathbb{Z}^{u \times u}$ and $B \in \mathbb{Z}^{r \times r}$ being invertible matrices over \mathbb{Z} , in particular, $B^{-1} = (b_{ij}) \in \mathbb{Z}^{r \times r}$ and (64) being a diagonal matrix. Define

$$\alpha_i = \hat{\alpha}_1^{b_{i1}} \dots \hat{\alpha}_r^{b_{ir}} \in \mathbb{F}^* \quad 1 \leq i \leq r, \quad (68)$$

$$\tilde{w}_i = w_1^{a_{i1}} \dots w_u^{a_{iu}} \in \mathbb{F}^* \quad 1 \leq i \leq u. \quad (69)$$

Then a basis of $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$ is

$$\{(d_1, 0, \dots, 0), (0, d_2, 0, \dots, 0), \dots, (0, \dots, 0, d_u, 0, \dots, 0)\} \quad (70)$$

and for $1 \leq i \leq u$ we get

$$\frac{\sigma(\tilde{w}_i)}{\tilde{w}_i} = \alpha_i^{d_i}. \quad (71)$$

Proof. Let $(\tilde{z}_{ij})_{ij} = AZ \in \mathbb{Z}^{u \times r}$. Since A is invertible over \mathbb{Z} , A can be considered as a basis transformation. Consequently, also $\{(\tilde{z}_{i1}, \dots, \tilde{z}_{ir})\}_{1 \leq i \leq u}$ is a basis of $M((\hat{\alpha}_1, \dots, \hat{\alpha}_r), \mathbb{F})$. In particular, for $1 \leq i \leq u$ we get

$$\frac{\sigma(\tilde{w}_i)}{\tilde{w}_i} = \left(\frac{\sigma(w_1)}{w_1}\right)^{a_{i1}} \dots \left(\frac{\sigma(w_u)}{w_u}\right)^{a_{iu}} = \hat{\alpha}_1^{p_{i1}} \dots \hat{\alpha}_r^{p_{ir}} \quad (72)$$

with

$$p_{ik} = a_{i1}z_{1k} + a_{i2}z_{2k} + \dots + a_{iu}z_{uk} = \tilde{z}_{ik}, \quad 1 \leq k \leq r;$$

the last equality follows from $(p_{ik})_{ik} = AZ = (z_{ik})_{ik} \in \mathbb{Z}^{u \times r}$. Let $D = (d_{ij})_{ij} \in \mathbb{Z}^{u \times r}$, i.e., $d_{ii} = d_i$ for $1 \leq i \leq u$ and all other entries are zero. For $1 \leq i \leq r$ we have

$$\alpha_i^{d_i} = \alpha_1^{d_{i1}} \dots \alpha_u^{d_{iu}} = \hat{\alpha}_1^{q_{i1}} \dots \hat{\alpha}_r^{q_{ir}}$$

with

$$q_{ik} = d_{i1}\tilde{b}_{1k} + d_{i2}\tilde{b}_{2k} + \dots + d_{ir}\tilde{b}_{rk} = \tilde{z}_{ik};$$

the last equality follows from $(\tilde{q}_{ik})_{ik} = DB^{-1} = AZ = \tilde{Z} = (\tilde{z}_{ik})_{ik} \in \mathbb{Z}^{r \times r}$. With (72) we conclude that (71) holds. Thus the elements in (70) are contained in $V = M((\alpha_1, \dots, \alpha_r), \mathbb{F})$. Finally, we will show that the linearly independent

vectors in (70) generate V . Let $(n_1, \dots, n_r) \in \mathbb{Z}^r$ such that there is a $w \in \mathbb{F}^*$ with $\frac{\sigma(w)}{w} = \alpha_1^{n_1} \dots \alpha_r^{n_r}$. Then using (68) we obtain

$$\begin{aligned} \frac{\sigma(w)}{w} &= (\hat{\alpha}_1^{\tilde{b}_{11}} \dots \hat{\alpha}_r^{\tilde{b}_{1r}})^{n_1} (\hat{\alpha}_1^{\tilde{b}_{21}} \dots \hat{\alpha}_r^{\tilde{b}_{2r}})^{n_2} \dots (\hat{\alpha}_1^{\tilde{b}_{r1}} \dots \hat{\alpha}_r^{\tilde{b}_{rr}})^{n_r} \\ &= \hat{\alpha}_1^{\tilde{b}_{11} n_1 + \dots + \tilde{b}_{r1} n_r} \dots \hat{\alpha}_r^{\tilde{b}_{1r} n_1 + \dots + \tilde{b}_{rr} n_r} = \hat{\alpha}_1^{m_1} \dots \hat{\alpha}_r^{m_r} \end{aligned}$$

with

$$(m_1, \dots, m_r) = (n_1, \dots, n_r) (\tilde{b}_{ij})_{ij} = (n_1, \dots, n_r) B^{-1}.$$

Conversely, B maps (m_1, \dots, m_r) to (n_1, \dots, n_r) . In particular, the given basis elements $(z_{i,1}, \dots, z_{i,r})$ for $1 \leq i \leq u$ of $M((\hat{\alpha}_1, \dots, \hat{\alpha}_r), \mathbb{F})$ are mapped in bijection to

$$(z_{i,1}, \dots, z_{i,r}) B = (\mu_{i,1}, \dots, \mu_{i,r})$$

with $(\mu_{i,j})_{i,j} = ZB$. As a consequence, the vectors $(\mu_{i,1}, \dots, \mu_{i,r})$ for $1 \leq i \leq u$ form a basis of V . Since A is invertible over \mathbb{Z} , these latter basis elements are mapped via a basis transformation with

$$A \begin{pmatrix} \mu_{i,1} \\ \vdots \\ \mu_{i,r} \end{pmatrix} = \begin{pmatrix} \nu_{i,1} \\ \vdots \\ \nu_{i,r} \end{pmatrix}$$

to the another basis $\{(\nu_{i,1}, \dots, \nu_{i,r})\}_{1 \leq i \leq u}$ of V . With $A Z B = D$ we conclude that $(\nu_{i,1}, \dots, \nu_{i,r}) = (0, \dots, 0, d_i, 0, \dots, 0)$ for $1 \leq i \leq u$. Thus (70) is a basis of V . \square

Lemma 67. *Let $(\mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle, \sigma)$ be a P -extension of a difference field (\mathbb{F}, σ) with $\alpha_i = \frac{\sigma(\hat{x}_i)}{\hat{x}_i} \in \mathbb{F}^*$ with $1 \leq i \leq r$. Let $B = (b_{ij})_{ij} \in \mathbb{Z}^{r \times r}$ be an invertible matrix over \mathbb{Z} , i.e., $B^{-1} = (\tilde{b}_{ij})_{ij} \in \mathbb{Z}^{r \times r}$, and let $c_1, \dots, c_r \in \mathbb{K}^*$. Take the P -extension $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle, \sigma)$ of (\mathbb{F}, σ) with (67). Then the ring homomorphism $\mu: \mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle \rightarrow \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$ given by $\mu|_{\mathbb{F}} = \text{id}$ and*

$$\mu(\hat{x}_i) = c_i x_1^{b_{i1}} \dots x_r^{b_{ir}}. \quad 1 \leq i \leq r \quad (73)$$

is a difference ring isomorphism. Moreover, its inverse is given by $\mu^{-1}|_{\mathbb{F}} = \text{id}$ and

$$\mu^{-1}(x_i) = \left(\frac{\hat{x}_1}{c_1}\right)^{\tilde{b}_{i1}} \dots \left(\frac{\hat{x}_r}{c_r}\right)^{\tilde{b}_{ir}}, \quad 1 \leq i \leq r. \quad (74)$$

Proof. Similarly to the proof in Lemma 66 one can verify that μ is invertible with (74). In particular, for $1 \leq i \leq r$ we have

$$\begin{aligned} \sigma(\mu(\hat{x}_i)) &= \sigma(c_i x_1^{b_{i1}} \dots x_r^{b_{ir}}) \\ &= (\alpha_1^{\tilde{b}_{i1}} \dots \alpha_r^{\tilde{b}_{ir}})^{c_i} (\alpha_1^{\tilde{b}_{21}} \dots \alpha_r^{\tilde{b}_{2r}})^{b_{i2}} \dots (\alpha_1^{\tilde{b}_{r1}} \dots \alpha_r^{\tilde{b}_{rr}})^{b_{ir}} c_i x_1^{b_{i1}} \dots x_r^{b_{ir}} \\ &= \alpha_1^{b_{i1} \tilde{b}_{i1} + b_{i2} \tilde{b}_{i2} + \dots + b_{ir} \tilde{b}_{ir}} \dots \alpha_r^{b_{i1} \tilde{b}_{i1} + b_{i2} \tilde{b}_{i2} + \dots + b_{ir} \tilde{b}_{ir}} \mu(\hat{x}_i) \\ &= \alpha_1^{p_{i1}} \dots \alpha_r^{p_{ir}} \mu(\hat{x}_i) \end{aligned}$$

with $(p_{ij})_{ij} = B B^{-1} = I_r$ where I_r is the identity matrix. Consequently $\sigma(\mu(\hat{x}_i)) = \alpha_i \mu(\hat{x}_i) = \mu(\alpha_i \hat{x}_i) = \mu(\sigma(\hat{x}_i))$. Thus μ is a difference ring isomorphism. \square

Example 68. *Take B from (66) and compute the $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ using (67). This yields (36). Now compute*

$$B^{-1} = \begin{pmatrix} 0 & 1 & 0 & -2 \\ -3 & 1 & -2 & 1 \\ -2 & 0 & -1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then using Lemma 65 it follows that the difference ring $(\mathbb{F}\langle\hat{x}_1\rangle\langle\hat{x}_2\rangle\langle\hat{x}_3\rangle\langle\hat{x}_4\rangle, \sigma)$ is isomorphic to $(\mathbb{F}\langle x_1\rangle\langle x_2\rangle\langle x_3\rangle\langle x_4\rangle, \sigma)$. More precisely, there is the difference ring isomorphism $\mu: \mathbb{F}\langle\hat{x}_1\rangle\langle\hat{x}_2\rangle\langle\hat{x}_3\rangle\langle\hat{x}_4\rangle \rightarrow \mathbb{F}\langle x_1\rangle\langle x_2\rangle\langle x_3\rangle\langle x_4\rangle$ defined by $\mu|_{\mathbb{F}} = \text{id}$ and

$$\begin{aligned} \mu(\hat{x}_1) &= \frac{x_2x_4}{x_1x_3^2}, & \mu(\hat{x}_2) &= x_1x_4^2, \\ \mu(\hat{x}_3) &= \frac{x_1^2x_3^3}{x_2^2}, & \mu(\hat{x}_4) &= x_4; \end{aligned} \quad (75)$$

its inverse difference ring isomorphism μ^{-1} is given by $\mu^{-1}|_{\mathbb{F}} = \text{id}$ and

$$\begin{aligned} \mu^{-1}(x_1) &= \frac{\hat{x}_2}{\hat{x}_4^2}, & \mu^{-1}(x_2) &= \frac{\hat{x}_2\hat{x}_4}{\hat{x}_1^3\hat{x}_3^2}, \\ \mu^{-1}(x_3) &= \frac{\hat{x}_4^2}{\hat{x}_1^2\hat{x}_3}, & \mu^{-1}(x_4) &= \hat{x}_4. \end{aligned} \quad (76)$$

Moreover, by Lemma 66 one can read off the basis of $V = M((\alpha_1, \alpha_2, \alpha_3, \alpha_4), \mathbb{F})$ from D in (66). Namely, we get (38).

We are now in the position to apply the results from the previous Section 4 and obtain the following main result. The constructed difference ring homomorphisms that arise in the proof of Theorem 69 can be visualized by the following diagram.

$$\begin{array}{ccc} \mathbb{F}\langle\hat{x}_1\rangle \dots \langle\hat{x}_r\rangle & \xrightarrow{\mu} & \mathbb{F}\langle x_1\rangle \dots \langle x_r\rangle & \xrightarrow{\lambda} & \mathbb{H} & (77) \\ & \searrow \hat{\tau} & & \searrow \tau = \hat{\tau} \circ \mu^{-1} & \downarrow \tau' & \\ & & & & \mathbf{S}(\mathbb{K}). & \end{array}$$

$\hat{\lambda} = \lambda \circ \mu$ (dotted arrow from $\mathbb{F}\langle\hat{x}_1\rangle \dots \langle\hat{x}_r\rangle$ to \mathbb{H})

Theorem 69. Let (\mathbb{F}, σ) be a radical-stable difference field with $\mathbb{K} = \text{const}_{\sigma}\mathbb{F}$ equipped with a \mathbb{K} -embedding $\bar{\tau}: \mathbb{F} \rightarrow \mathbf{S}(\mathbb{K})$. Let $(\mathbb{F}\langle\hat{x}_1\rangle \dots \langle\hat{x}_r\rangle, \sigma)$ be a P -extension of (\mathbb{F}, σ) with $\hat{\alpha}_i = \frac{\sigma(\hat{x}_i)}{\hat{x}_i} \in \mathbb{F}^*$ for $1 \leq i \leq r$ together with a \mathbb{K} -homomorphism $\hat{\tau}: \mathbb{F}\langle\hat{x}_1\rangle \dots \langle\hat{x}_r\rangle \rightarrow \mathbf{S}(\mathbb{K})$ with $\hat{\tau}|_{\mathbb{F}} = \bar{\tau}$. Assume that $M((\hat{\alpha}_1, \dots, \hat{\alpha}_r), \mathbb{F}) \neq \{\mathbf{0}\}$, and let $u \geq 1$ be its rank and $d \geq 1$ be its largest divisor.

Then there is an RPI-extension (\mathbb{H}, σ) of the difference field (\mathbb{F}, σ) together with a \mathbb{K} -embedding $\tau': \mathbb{H} \rightarrow \mathbf{S}(\mathbb{K})$ with $\tau'|_{\mathbb{F}} = \bar{\tau}$ and a surjective difference ring homomorphism $\hat{\lambda}: \mathbb{F}\langle\hat{x}_1\rangle \dots \langle\hat{x}_r\rangle \rightarrow \mathbb{H}$ such that the following properties hold.

- (1) We have $\tau'(\hat{\lambda}(f)) = \hat{\tau}(f)$ for all $f \in \mathbb{F}\langle\hat{x}_1\rangle \dots \langle\hat{x}_r\rangle$, i.e., the diagram

$$\begin{array}{ccc} \mathbb{F}\langle\hat{x}_1\rangle \dots \langle\hat{x}_r\rangle & \xrightarrow{\hat{\lambda}} & \mathbb{H} & (78) \\ & \searrow \hat{\tau} & \downarrow \tau' & \\ & & \mathbf{S}(\mathbb{K}) & \end{array}$$

commutes.

- (2) If $d = 1$, \mathbb{H} is built by $r - u$ Π -monomials, say $\mathbb{H} = \mathbb{F}\langle x_{u+1}\rangle \dots \langle x_r\rangle$ with $\alpha_i = \frac{\sigma(x_i)}{x_i} \in \mathbb{F}^*$ for $u + 1 \leq i \leq r$. Otherwise, $\mathbb{H} = \mathbb{F}\langle x_{u+1}\rangle \dots \langle x_r\rangle[z]$ where the x_i are Π -monomials with $\alpha_i = \frac{\sigma(x_i)}{x_i} \in \mathbb{F}^*$ for $u + 1 \leq i \leq r$ and z is an R -monomial of order d with $\rho = \frac{\sigma(z)}{z} \in \mathbb{K}^*$.

(3) $\hat{\lambda}$ is defined by $\hat{\lambda}|_{\mathbb{F}} = \text{id}$ and

$$\hat{\lambda}(\hat{x}_i) = \gamma_i z^{o_i} x_{u+1}^{m_{i,u+1}} \dots x_r^{m_{i,r}} \quad (79)$$

for all $1 \leq i \leq r$ for some $\gamma_i \in \mathbb{F}^*$, $o_i \in \mathbb{N}$ with $0 \leq o_i < d$ and $m_{i,j} \in \mathbb{Z}$.

(4) If $\bar{\text{ev}}$ is an evaluation function for $\bar{\tau} (= \hat{\tau}|_{\mathbb{F}} = \tau'|_{\mathbb{F}})$, then there is an evaluation function ev' for τ' defined by $\text{ev}'|_{\mathbb{F} \times \mathbb{N}} = \bar{\text{ev}}$ and

$$\text{ev}'(x_i, n) = \kappa_i \prod_{k=l_i}^n \text{ev}(\alpha_i, k-1) \quad (80)$$

for all $u+1 \leq i \leq r$ for some $l_i \in \mathbb{N}$ and $\kappa_i \in \mathbb{K}^*$; if $d > 1$, we define in addition $\text{ev}'(z, n) = \rho^n$.

(5) Among all possible RII-extensions²⁰ with this property, $r-u$ is the minimal number of Π -monomials; furthermore, if $d > 1$, only one R -monomial is necessary and its order d is minimal.

(6) There are $n_{i,j} \in \mathbb{Z}$ where the rows in $(n_{i,j})_{i,j} \in \mathbb{Z}^{u \times r}$ are linearly independent such that for $g_i := \hat{\lambda}(\hat{x}_1^{n_{i,1}} \dots \hat{x}_r^{n_{i,r}}) \in \mathbb{F}^*$ with $1 \leq i \leq u$ we have

$$\ker(\hat{\tau}) = \ker(\hat{\lambda}) = \langle \hat{x}_1^{n_{1,1}} \dots \hat{x}_r^{n_{1,r}} - g_1, \dots, \hat{x}_1^{n_{u,1}} \dots \hat{x}_r^{n_{u,r}} - g_u \rangle_{\mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle}. \quad (81)$$

If the properties in Assumption 28 hold, then one can compute (\mathbb{H}, σ) , $\hat{\lambda}$ and the generators of $\ker(\hat{\lambda})$ explicitly. In particular, the evaluation function ev' for (\mathbb{H}, σ) defined in (80) can be given explicitly.

Proof. (1,2,3) Let $\mathcal{B} = \{z_{i1}, \dots, z_{ir}\}_{1 \leq i \leq u}$ be a basis of $M((\hat{\alpha}_1, \dots, \hat{\alpha}_r), \mathbb{F}) \neq \{\mathbf{0}\}$. Consider the Smith normal form of $Z = (z_{ij})_{i,j} \in \mathbb{Z}^{u \times r}$, i.e., the decomposition (65) with $A = (a_{ij})_{i,j} \in \mathbb{Z}^{u \times u}$ and $B \in \mathbb{Z}^{r \times r}$ being invertible matrices over \mathbb{Z} , in particular, $B^{-1} = (\tilde{b}_{ij}) \in \mathbb{Z}^{r \times r}$ with the diagonal matrix (64) with $d_1 \mid d_2 \mid \dots \mid d_u = d$. Take the P -extension $(\mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle, \sigma)$ of (\mathbb{F}, σ) defined by (67). By Lemma 67 there is the difference ring isomorphism $\mu: \mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle \rightarrow \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$ given by $\mu|_{\mathbb{F}} = \text{id}$ and (73) ($c_1 = \dots = c_r = 1$). Define the map $\tau: \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbf{S}(\mathbb{K})$ with $\tau = \hat{\tau} \circ \mu^{-1}$ which forms a \mathbb{K} -homomorphism. In particular, by Lemma 66 a basis of $M((\alpha_1, \dots, \alpha_r), \mathbb{F})$ is given in (70). Hence we can apply Theorem 60 and obtain a surjective difference ring homomorphism $\lambda: \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbb{H}$ with $\lambda|_{\mathbb{F}} = \text{id}$ and $\tau'(\lambda(f)) = \tau(f)$ for all $f \in \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle$. Thus with the surjective difference ring homomorphism

$$\hat{\lambda} = \lambda \circ \mu \quad (82)$$

we get $\tau'(\hat{\lambda}(f)) = \tau'(\lambda(\mu(f))) = \tau(\mu(f)) = \hat{\tau}(f)$ which proves the first part. Part (2) follows by (2a) and (2b) of Theorem 60. In particular, part (3) follows by (82), the definition of μ given in (73) and the definition of λ given in (40) or (41). (4) Since \mathbb{F} is a field, there is a z -function by part (2) of Lemma 6 for $\bar{\text{ev}}$. Thus we can activate Lemma 22 and statement (4) follows.

(5) Suppose that there is an RII-extension (\mathbb{H}', σ) of (\mathbb{F}, σ) with the shape given in Footnote 20 equipped with a difference ring homomorphism $\lambda': \mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle \rightarrow \mathbb{H}'$ as claimed in statement (1). Suppose further that (\mathbb{H}', σ) is built by less than $r-u$ Π -monomials or, if $d > 1$, it can be built without R -monomial or is built with R -monomials but the product of their orders is smaller than d . Then (\mathbb{H}', σ) together with $\lambda'': \mathbb{F}\langle x_1 \rangle \dots \langle x_r \rangle \rightarrow \mathbb{H}'$ where $\lambda'' = \lambda' \circ \mu^{-1}$ yields a better construction than

²⁰This means that the RII-extension (\mathbb{H}', σ) of the difference field (\mathbb{F}, σ) has the form $\mathbb{H}' = \mathbb{F}\langle y_1 \rangle \dots \langle y_e \rangle [z_1] \dots [z_l]$ with $\frac{\sigma(y_i)}{y_i} \in \mathbb{F}\langle y_i \rangle \dots \langle y_{i-1} \rangle^*$ for $1 \leq i \leq e$ and $\frac{\sigma(z_i)}{z_i} \in \mathbb{K}^*$ for $1 \leq i \leq l$.

(\mathbb{H}, σ) with λ , a contradiction to Theorem 63.

(6) By part (3) of Theorem 60 we have $\ker(\lambda) = \ker(\tau) = \langle x_1^{d_1} - g_1, \dots, x_u^{d_u} - g_u \rangle$ with $g_i := \lambda(x_i^{d_i})$. With $\hat{\lambda} = \lambda \circ \mu$ and $\hat{\tau} = \tau \circ \mu$ we get

$$\ker(\hat{\lambda}) = \ker(\hat{\tau}) = \langle \mu^{-1}(x_1)^{d_1} - \mu^{-1}(g_1), \dots, \mu^{-1}(x_u)^{d_u} - \mu^{-1}(g_u) \rangle.$$

With $\mu^{-1}(g_i) = g_i$ for $1 \leq i \leq u$ and (74) it follows that

$$\mu^{-1}(x_i)^{d_i} - \mu^{-1}(g_i) = (\hat{x}_1^{\tilde{b}_{i1}} \dots \hat{x}_r^{\tilde{b}_{ir}})^{d_i} - g_i$$

for $1 \leq i \leq u$. In particular, for $n_{i,j} := d_i \tilde{b}_{ir}$ we get (81). Since $B^{-1} = (\tilde{b}_{i,j})_{i,j}$, the first u rows in B^{-1} are linearly independent and thus the rows in $(n_{i,j})_{i,j} \in \mathbb{Z}^{u \times r}$ are linearly independent. Finally, with (82) it follows that $\hat{\lambda}((\hat{x}_1^{\tilde{b}_{i1}} \dots \hat{x}_r^{\tilde{b}_{ir}})^{d_i}) = \lambda(\mu(\mu^{-1}(x_i)^{d_i})) = \lambda(x_i^{d_i}) = g_i$ which completes the proof of part (6).

Suppose that the properties in Assumption 28 hold. Then a basis \mathcal{B} can be computed. Further, one can compute the Smith normal form of Z , and obtains μ and its inverse μ^{-1} explicitly. The remaining constructions in (1),(2) and (6) follow by the constructive statements of Theorem 63. By Lemma 22 we conclude that the claimed κ_i and l_i in (80) can be calculated. \square

Example 70 (Details for Ex. 25). *We will illustrate the construction given in the proof of Theorem 69 in order to obtain the calculations given in Example 25 above. We take the rational difference field (\mathbb{F}, σ) with $\mathbb{F} = \mathbb{K}(x)$, $\sigma(x) = x + 1$ and $\text{const}_\sigma \mathbb{F} = \mathbb{K} = \mathbb{Q}(t)$, which is a $\Pi\Sigma$ -field over \mathbb{K} . Furthermore we construct the P -extension (\mathbb{E}, σ) of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle \hat{x}_1 \rangle \langle \hat{x}_2 \rangle \langle \hat{x}_3 \rangle \langle \hat{x}_4 \rangle$ where $\sigma(\hat{x}_i) = \hat{\alpha}_i \hat{x}_i$ for $1 \leq i \leq 4$ and (17) as introduced in Example 65. Further, we take the \mathbb{K} -homomorphism $\hat{\tau}: \mathbb{F}\langle \hat{x}_1 \rangle \langle \hat{x}_2 \rangle \langle \hat{x}_3 \rangle \langle \hat{x}_4 \rangle \rightarrow \mathcal{S}(\mathbb{K})$ with the evaluation function $\hat{\text{ev}}$ defined by (12) for $p, q \in \mathbb{K}[x]$ and (20) for $1 \leq i \leq 4$ with (4). In a nutshell, we model the products (4) with $\hat{x}_1, \hat{x}_2, \hat{x}_3, \hat{x}_4$, respectively. Utilizing the calculations in Example 65 we proceed with the constructions given in the proof of Theorem 69 as follows. As elaborated in Example 68 we take the difference ring $(\mathbb{F}\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle, \sigma)$ with $\sigma(x_i) = \alpha_i x_i$ for $1 \leq i \leq 4$ where the α_i are given in (36). By construction $\mu: \mathbb{F}\langle \hat{x}_1 \rangle \langle \hat{x}_2 \rangle \langle \hat{x}_3 \rangle \langle \hat{x}_4 \rangle \rightarrow \mathbb{F}\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle$ forms a difference ring isomorphism and a basis of $V = M((\alpha_1, \alpha_2, \alpha_3, \alpha_4), \mathbb{F})$ is (38). Now we can utilize the construction of Section 4. As preprocessing step, we define the \mathbb{K} -homomorphism $\tau: \mathbb{F}\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle \rightarrow \mathcal{S}(\mathbb{K})$ with $\tau = \hat{\tau} \circ \mu^{-1}$. Here one obtains the evaluation function $\text{ev}: \mathbb{F}\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle \times \mathbb{N} \rightarrow \mathbb{K}$ with*

$$\begin{aligned} \text{ev}(x_1, n) &= \left(\prod_{k=1}^n \frac{26244k^2(2+k)^2}{(3+k)^2} \right) \left(\prod_{k=1}^n \frac{-(5+k)}{162k(2+k)} \right)^2, \\ \text{ev}(x_2, n) &= \left(\prod_{k=1}^n \frac{26244k^2(2+k)^2}{(3+k)^2} \right) \left(\prod_{k=1}^n \frac{-(3+k)^3}{13122k(1+k)} \right)^3 \left(\prod_{k=1}^n \frac{-162k(2+k)}{5+k} \right) \left(\prod_{k=1}^n \frac{-729t(5+k)}{k(2+k)^3} \right)^2 \\ \text{ev}(x_3, n) &= \left(\prod_{k=1}^n \frac{-(3+k)^3}{13122k(1+k)} \right)^2 \left(\prod_{k=1}^n \frac{-162k(2+k)}{5+k} \right)^2 \left(\prod_{k=1}^n \frac{-729t(5+k)}{k(2+k)^3} \right), \\ \text{ev}(x_4, n) &= \prod_{k=1}^n \frac{-162k(2+k)}{5+k}. \end{aligned}$$

Now we activate Theorem 60. Repeating the construction from Example 61 one obtains the $R\Pi$ -extension $(\mathbb{E}[z], \sigma)$ of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle x_3 \rangle \langle x_4 \rangle$ and $\sigma(x_3) = \alpha_3 x_3$, $\sigma(x_4) = \alpha_4 x_4$, $\sigma(z) = -z$ where the α_3, α_4 are given in (36). Moreover, we can define the evaluation function $\text{ev}' : \mathbb{E}[z] \times \mathbb{N} \rightarrow \mathbb{K}$ with $\text{ev}'(f, n) = \text{ev}(f, n)$ for all $f \in \mathbb{F}$, $\text{ev}'(x_3, n) = \text{ev}(x_3, n)$, $\text{ev}'(x_4, n) = \text{ev}(x_4, n)$ and $\text{ev}'(z, n) = (-1)^n$ yielding

the \mathbb{K} -embedding $\tau': \mathbb{E}[z] \rightarrow \mathbf{S}(\mathbb{K})$. By coincidence these evaluations equal the evaluations given in (37); this comes from the fact the lower bounds are all the same. Thus we can use the construction from Example 59 and obtain λ with (47) such that the diagram (49) commutes. Finally, we take $\hat{\lambda}: \mathbb{F}\langle x_1 \rangle \langle x_2 \rangle \langle x_3 \rangle \langle x_4 \rangle \rightarrow \mathbb{F}\langle x_3 \rangle \langle x_4 \rangle [z]$ with $\hat{\lambda} = \lambda \circ \mu$. In other words, $\hat{\lambda}$ is determined by $\lambda|_{\mathbb{F}} = \text{id}$ and (24). It follows that $\hat{\tau} = \tau' \circ \hat{\lambda}$. Summarizing, we have carried out the construction visualized in (77) with $r = 4$ and $\mathbb{H} = \mathbb{E}[z]$. In particular, we have (50). Thus applying the inverse of μ defined in (76) to the entries given in (50) we obtain (28) (compare also (8) with (7)).

Suppose that we are given a P -extension $(\mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle, \sigma)$ of a difference field (\mathbb{F}, σ) with $\mathbb{K} = \text{const}_\sigma \mathbb{F}$, $\sigma(\hat{x}_i) = \hat{\alpha}_i \hat{x}_i$ for $1 \leq i \leq r$ and an evaluation function $\hat{\text{ev}}: \mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle \times \mathbb{N} \rightarrow \mathbb{K}$ of the form

$$\hat{\text{ev}}(\hat{x}_i, n) = F_i(n) = \prod_{k=l_i}^n \text{ev}(\hat{\alpha}_i, k-1). \quad (83)$$

This yields the \mathbb{K} -homomorphism $\tau: \mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle \rightarrow \mathbf{S}(\mathbb{K})$ defined by $\hat{\tau}(f) = (\hat{\text{ev}}(f, n))_{n \geq 0}$. In addition, suppose that the (algorithmic) properties in Assumption 28 hold. By Theorem 69 any expression in terms of products modeled in $(\mathbb{F}\langle \hat{x}_1 \rangle \dots \langle \hat{x}_r \rangle, \sigma)$ together with $\hat{\text{ev}}$ can be also modeled in an $R\Pi$ -extension (\mathbb{H}, σ) of (\mathbb{F}, σ) together with an evaluation function $\text{ev}': \mathbb{H} \times \mathbb{N} \rightarrow \mathbb{K}$. This yields the following consequences.

(1) Using the symbolic summation toolbox described in [33, 35, 37, 38, 40] any expression of indefinite nested sums defined over these products can be modeled in a Σ -extension defined over $R\Pi$ -extensions. In particular, the efficient simplification machinery of the summation package `Sigma` for indefinite nested sums can be applied in this general setting.

(2) Restricting to single nested products given in (1), we obtain an improved calculation formula for the evaluation function $\hat{\text{ev}}$. Namely, using the composition $\hat{\tau} = \tau' \circ \hat{\lambda}$ together with the definition of $\hat{\lambda}$ given in (79) and the definition of the evaluation ev' of τ' given in (80) one gets:

$$\hat{\text{ev}}(\hat{x}_i, n) = (\rho^n)^{\alpha_i} \text{ev}(\gamma_i, n) \text{ev}'(x_{u+1}, n)^{m_{i,u+1}} \dots \text{ev}'(x_r, n)^{m_{i,r}} \quad (84)$$

for some $l_i \in \mathbb{N}$ and $\kappa_i \in \mathbb{K}^*$ for $1 \leq i \leq r$. By setting $\phi_{i-u}(k) := \text{ev}(\alpha_{i-u}, k-1)$ equation (80) turns to

$$\text{ev}'(x_i) = \kappa_i \Phi_{i-u}(n) = \kappa_i \prod_{k=l_{i-u}}^n \phi_{i-u}(k), \quad u+1 \leq i \leq r.$$

In short, the products given in (1) can be simplified to expressions in terms of the products given in (2). In particular, the sequences $\tau'(x_i) = (\text{ev}'(x_i, n))_{n \geq 0} = \kappa_i (\Phi_{i-u}(n))_{n \geq 0}$ are algebraically independent over the sequences $\tau(\mathbb{F}[z])$ while the sequences of the products in (83) are usually algebraically dependent (except for the special case $r = s$).

Example 71 (Cont. Ex. 70). Consider the difference ring $(\mathbb{F}\langle \hat{x}_1 \rangle \langle \hat{x}_2 \rangle \langle \hat{x}_3 \rangle \langle \hat{x}_4 \rangle, \sigma)$ with the evaluation function $\hat{\text{ev}}$ defined by $\hat{\text{ev}}(\hat{x}_i, n) = F_i(n)$ for $i = 1, 2, 3, 4$ with (4). The construction from Example 70 yields an improved way to define $\text{ev}(\hat{x}_i, n)$. Namely, we constructed the $R\Pi$ -extension $(\mathbb{E}[z], \sigma)$ of (\mathbb{F}, σ) with $\mathbb{E} = \mathbb{F}\langle x_3 \rangle \langle x_4 \rangle$ and $\sigma(x_3) = \alpha_3 x_3$, $\sigma(x_4) = \alpha_4 x_4$ and $\sigma(z) = -z$ where the α_3, α_4 are

given in (36). Moreover, we obtained the induced evaluation function $ev': \mathbb{E}[z] \times \mathbb{N} \rightarrow \mathbb{K}$ defined by (23). Since $\hat{\tau} = \tau' \circ \hat{\lambda}$ by construction, it follows with (24) that the evaluation ev can be given also in the following form (25) which is precisely (6).

6. CONCLUSION

Given a finite set of products (1) whose multiplicands can be modeled in a difference field (\mathbb{F}, σ) , we presented a general framework in Theorem 69 to find a minimal RII-extension defined over (\mathbb{F}, σ) in which the products can be modeled. In particular, the class of mixed-multibasic hypergeometric products are covered in this machinery. As a consequence, the input products can be rephrased by alternative products (2) which are algebraically independent among each other and by one product of the form γ^n with a root of unity γ . In particular, the number s of output products and the order of the root of unity γ are minimal among the possible choices of product representations. Moreover, we are able to compute a finite set of generators that produce all relations among the input products.

We remark that the analogous result for indefinite nested sums has been elaborated in [42, Thm. 3.13]. A natural task is to merge the product and sum representations accordingly to find the difference ideal of all relations of indefinite nested sums defined over mixed-multibasic hypergeometric products.

The underlying algorithms for Theorem 69 require that the ground difference field (\mathbb{F}, σ) satisfies certain (algorithmic) properties enumerated in Assumption 28. An interesting question is whether these requirements can be relaxed to weaker properties in order to calculate such representations or to find all relations among the given input products.

Furthermore, we showed explicitly that this machinery can be applied to the rational difference field (see Examples 14 and 19) and more generally to the mixed-rational difference field (see Example 20). An novel task will be the application of this machinery to more general classes of difference fields that satisfy these requirements.

REFERENCES

- [1] J. Ablinger, A. Behring, J. Blümlein, A. D. Freitas, A. von Manteuffel, and C. Schneider. Calculating Three Loop Ladder and V-Topologies for Massive Operator Matrix Elements by Computer Algebra. *Comput. Phys. Comm.*, 202:33–112, 2016. arXiv:1509.08324 [hep-ph].
- [2] J. Ablinger, J. Blümlein, A. D. Freitas, A. Goedicke, C. Schneider, and K. Schönwald. The Two-mass Contribution to the Three-Loop Gluonic Operator Matrix Element $A_{99,Q}^{(3)}$. *Nucl. Phys. B*, 932:129–240, 2018. arXiv:1804.02226 [hep-ph].
- [3] S. A. Abramov. On the summation of rational functions. *Zh. vychisl. mat. Fiz.*, 11:1071–1074, 1971.
- [4] S. A. Abramov. The rational component of the solution of a first-order linear recurrence relation with a rational right-hand side. *U.S.S.R. Comput. Maths. Math. Phys.*, 15:216–221, 1975. Transl. from *Zh. vychisl. mat. mat. fiz.* 15, pp. 1035–1039, 1975.
- [5] S. A. Abramov. Rational solutions of linear differential and difference equations with polynomial coefficients. *U.S.S.R. Comput. Math. Math. Phys.*, 29(6):7–12, 1989.
- [6] S. A. Abramov and M. Petkovšek. Polynomial ring automorphisms, rational (w, σ) -canonical forms, and the assignment problem. *J. Symbolic Comput.*, 45(6):684–708, 2010.
- [7] M. Apagodu and D. Zeilberger. Multi-variable Zeilberger and Almkvist-Zeilberger algorithms and the sharpening of Wilf-Zeilberger theory. *Adv. Appl. Math.*, 37:139–152, 2006.
- [8] A. Bauer and M. Petkovšek. Multibasic and mixed hypergeometric Gosper-type algorithms. *J. Symbolic Comput.*, 28(4–5):711–736, 1999.

- [9] M. Bronstein. On solutions of linear ordinary difference equations in their coefficient field. *J. Symbolic Comput.*, 29(6):841–877, 2000.
- [10] S. Chen and M. Kauers. Order-Degree Curves for Hypergeometric Creative Telescoping. In J. van der Hoeven and M. van Hoeij, editors, *Proceedings of ISSAC 2012*, pages 122–129, 2012.
- [11] F. Chyzak. An extension of Zeilberger’s fast algorithm to general holonomic functions. *Discrete Math.*, 217:115–134, 2000.
- [12] P. M. Cohn. *Algebra*, volume 2. John Wiley & Sons, 2nd edition, 1989.
- [13] R. M. Cohn. *Difference Algebra*. John Wiley & Sons, 1965.
- [14] M. Elsheikh, M. Giesbrecht, A. Novocin, and B. D. Saunders. Fast computation of Smith forms of sparse matrices over local rings. In *Proc. ISSAC 2012*, pages 146–153. ACM, New York, 2012.
- [15] G. Ge. *Algorithms Related to the Multiplicative Representation of Algebraic Numbers*. PhD thesis, University of California at Berkeley, 1993.
- [16] R. W. Gosper. Decision procedures for indefinite hypergeometric summation. *Proc. Nat. Acad. Sci. U.S.A.*, 75:40–42, 1978.
- [17] C. Hardouin and M. Singer. Differential Galois theory of linear difference equations. *Math. Ann.*, 342(2):333–377, 2008.
- [18] M. Karr. Summation in finite terms. *J. ACM*, 28:305–350, 1981.
- [19] M. Karr. Theory of summation in finite terms. *J. Symbolic Comput.*, 1:303–315, 1985.
- [20] M. Kauers and B. Zimmermann. Computing the algebraic relations of c-finite sequences and multisequences. *Journal of Symbolic Computation*, 43(11):787–803, 2008.
- [21] C. Koutschan. Creative telescoping for holonomic functions. In C. Schneider and J. Blümlein, editors, *Computer Algebra in Quantum Field Theory: Integration, Summation and Special Functions*, Texts and Monographs in Symbolic Computation, pages 171–194. Springer, 2013. arXiv:1307.4554 [cs.SC].
- [22] I. Nemes and P. Paule. A canonical form guide to symbolic summation. In A. Miola and M. Temperini, editors, *Advances in the Design of Symbolic Computation Systems*, Texts Monogr. Symbol. Comput., pages 84–110. Springer, Wien-New York, 1997.
- [23] E. D. Ocansey. Representing (q -)hypergeometric products and mixed versions in difference rings. pages 175–213.
- [24] E. D. Ocansey. *Difference ring algorithms for nested products*. PhD thesis, RISC, J. Kepler University, 2019.
- [25] P. Paule. Greatest factorial factorization and symbolic summation. *J. Symbolic Comput.*, 20(3):235–268, 1995.
- [26] P. Paule and A. Riese. A Mathematica q -analogue of Zeilberger’s algorithm based on an algebraically motivated approach to q -hypergeometric telescoping. In M. Ismail and M. Rahman, editors, *Special Functions, q -Series and Related Topics*, volume 14, pages 179–210. AMS, 1997.
- [27] P. Paule and M. Schorn. A Mathematica version of Zeilberger’s algorithm for proving binomial coefficient identities. *J. Symbolic Comput.*, 20(5-6):673–698, 1995.
- [28] M. Petkovšek, H. S. Wilf, and D. Zeilberger. *$A = B$* . A. K. Peters, Wellesley, MA, 1996.
- [29] G. F. S. Chen, R. Feng and Z. Li. On the structure of compatible rational functions. In *Proceedings of ISSAC 2011*, pages 91–98, 2011.
- [30] B. D. Saunders and Z. Wan. Smith normal form of dense integer matrices fastalgorithms into practice. In J. Gutierrez, editor, *Proc. ISSAC’04*, pages 274–281. ACM Press, 2004.
- [31] C. Schneider. Symbolic summation in difference fields. Technical Report 01-17, RISC-Linz, J. Kepler University, November 2001. PhD Thesis.
- [32] C. Schneider. Product representations in $\Pi\Sigma$ -fields. *Ann. Comb.*, 9(1):75–99, 2005.
- [33] C. Schneider. Simplifying sums in $\Pi\Sigma$ -extensions. *J. Algebra Appl.*, 6(3):415–441, 2007.
- [34] C. Schneider. Symbolic summation assists combinatorics. *Sém. Lothar. Combin.*, 56:1–36, 2007. Article B56b.
- [35] C. Schneider. A refined difference field theory for symbolic summation. *J. Symbolic Comput.*, 43(9):611–644, 2008. [arXiv:0808.2543v1].
- [36] C. Schneider. Parameterized telescoping proves algebraic independence of sums. *Ann. Comb.*, 14:533–552, 2010. [arXiv:0808.2596]; for a preliminary version see FPSAC 2007.
- [37] C. Schneider. Structural theorems for symbolic summation. *Appl. Algebra Engrg. Comm. Comput.*, 21(1):1–32, 2010.

- [38] C. Schneider. A symbolic summation approach to find optimal nested sum representations. In A. Carey, D. Ellwood, S. Paycha, and S. Rosenberg, editors, *Motives, Quantum Field Theory, and Pseudodifferential Operators*, volume 12 of *Clay Mathematics Proceedings*, pages 285–308. Amer. Math. Soc, 2010. arXiv:0808.2543.
- [39] C. Schneider. A streamlined difference ring theory: Indefinite nested sums, the alternating sign and the parameterized telescoping problem. In F. Winkler, V. Negru, T. Ida, T. Jebelean, D. Petcu, S. Watt, and D. Zaharie, editors, *Symbolic and Numeric Algorithms for Scientific Computing (SYNASC), 2014 15th International Symposium*, pages 26–33. IEEE Computer Society, 2014. arXiv:1412.2782v1 [cs.SC].
- [40] C. Schneider. Fast algorithms for refined parameterized telescoping in difference fields. In M. W. J. Guitierrez, J. Schicho, editor, *Computer Algebra and Polynomials*, number 8942 in *Lecture Notes in Computer Science (LNCS)*, pages 157–191. Springer, 2015. arXiv:1307.7887 [cs.SC].
- [41] C. Schneider. A difference ring theory for symbolic summation. *J. Symb. Comput.*, 72:82–127, 2016. arXiv:1408.2776 [cs.SC].
- [42] C. Schneider. Summation Theory II: Characterizations of $R[[\Sigma]]$ -extensions and algorithmic aspects. *J. Symb. Comput.*, 80(3):616–664, 2017. arXiv:1603.04285 [cs.SC].
- [43] M. Singer. Algebraic and algorithmic aspects of linear difference equations. In M. S. C. Hardouin, J. Sauloy, editor, *Galois theories of linear difference equations: An Introduction*, volume 211 of *Mathematical Surveys and Monographs*. AMS, 2016.
- [44] M. van der Put and M. Singer. *Galois theory of difference equations*, volume 1666 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1997.
- [45] P. G. A. S. W. Eberly, M. Giesbrecht and G. Villard. Faster inversion and other black box matrix computations using efficient block projections. In C. Brown, editor, *Proc. ISSAC'07*, pages 143–150. ACM Press, 2007.
- [46] K. Wegschaider. Computer generated proofs of binomial multi-sum identities. Master’s thesis, RISC, J. Kepler University, May 1997.
- [47] H. Wilf and D. Zeilberger. An algorithmic proof theory for hypergeometric (ordinary and “q”) multisum/integral identities. *Invent. Math.*, 108:575–633, 1992.
- [48] D. Zeilberger. A holonomic systems approach to special functions identities. *J. Comput. Appl. Math.*, 32:321–368, 1990.
- [49] D. Zeilberger. The method of creative telescoping. *J. Symbolic Comput.*, 11:195–204, 1991.

RESEARCH INSTITUTE FOR SYMBOLIC COMPUTATION, J. KEPLER UNIVERSITY LINZ, A-4040
LINZ, AUSTRIA

E-mail address: Carsten.Schneider@risc.jku.at