A Difference Ring Theory for Symbolic Summation

Carsten Schneider

Research Institute for Symbolic Computation (RISC)
Johannes Kepler University
Altenbergerstraße 69, 4040 Linz, Austria

Abstract

A summation framework is developed that enhances Karr’s difference field approach. It covers not only indefinite nested sums and products in terms of transcendental extensions, but it can treat, e.g., nested products defined over roots of unity. The theory of the so-called $R\Pi\Sigma^*$-extensions is supplemented by algorithms that support the construction of such difference rings automatically and that assist in the task to tackle symbolic summation problems. Algorithms are presented that solve parameterized telescoping equations, and more generally parameterized first-order difference equations, in the given difference ring. As a consequence, one obtains algorithms for the summation paradigms of telescoping and Zeilberger’s creative telescoping. With this difference ring theory one obtains a rigorous summation machinery that has been applied to numerous challenging problems coming, e.g., from combinatorics and particle physics.

Key words: difference ring extensions, roots of unity, indefinite nested sums and products, parameterized telescoping (telescoping, creative telescoping), semi-constants, semi-invariants

1. Introduction

In his pioneering work [24,25] M. Karr introduced a very general class of difference fields, the so-called $\Pi\Sigma$-fields, in which expressions in terms of indefinite nested sums and products can be represented. In particular, he developed an algorithm that decides constructively if for a given expression $f(k)$ represented in a $\Pi\Sigma$-field $F$ there is an expression $g(k)$ represented in the field $F$ such that the telescoping equation (anti-difference)

$$f(k) = g(k + 1) - g(k)$$

is satisfied.

* Supported by the Austrian Science Fund (FWF) grant SFB F50 (F5009-N15) and the European Commission through contract PITN-GA-2010-264564 (LHCPhenoNet).

Email address: Carsten.Schneider@risc.jku.at (Carsten Schneider).
holds. If such a solution exists, one obtains for an appropriately chosen \( a \in \mathbb{N} \) the identity
\[
\sum_{k=a}^{b} f(k) = g(k + 1) - g(1).
\] (2)

His algorithms can be viewed as the discrete version of Risch’s integration algorithm; see [40,13]. In the last years the \( \Pi\Sigma \)-field theory has been pushed forward. It is now possible to obtain sum representations, i.e., right hand sides in (2) with certain optimality criteria such as minimal nesting depth [53,56], minimal number of generators in the summands [45] or minimal degrees in the denominators [51]. For the simplification of products see [48,8]. We emphasize that exactly such refined representations give rise to more efficient telescoping algorithms worked out in [55,58].

A striking application is that Karr’s algorithm and all the enhanced versions can be used to solve the parameterized telescoping problem [41,54]: for given indefinite nested product-sum expressions \( f_1(k), \ldots, f_n(k) \) represented in \( \mathbb{F} \), find constants \( c_1, \ldots, c_n \), free of \( k \) and not all zero, and find \( g(k) \) represented in \( \mathbb{F} \) such that
\[
g(k + 1) - g(k + 1) = c_1 f_1(k) + \cdots + c_n f_n(k) \tag{3}
\]
holds. In particular, this problem covers Zeilberger’s creative telescoping paradigm [62] by setting \( f_i(k) = F(m + i - 1, k) \) and representing these \( f_i(k) \) in \( \mathbb{F} \). Namely, if one finds such a solution, one ends up at the recurrence
\[
g(m, b + 1) - g(m, a) = c_1 \sum_{k=a}^{b} f(m, k) + \cdots + c_n \sum_{k=a}^{b} f(m + n - 1, k).
\]

In a nutshell one cannot only treat indefinite summation but also definite summation problems. In this regard, also recurrence solvers have been developed where the coefficients of the recurrence and the inhomogeneous part can be elements from a \( \Pi\Sigma \)-field [14,49,6]. All these algorithms generalize and enhance substantially the \( (q-) \)hypergeometric and holonomic toolbox [5,18,61,62,34,37,35,9,15,26,30] in order to rewrite definite sums to indefinite nested sums. For details on these aspects we refer to [59].

Besides all these sophisticated developments, e.g., within the summation package \texttt{Sigma} [52], there is one critical gap which concerns all the developed tools in the setting of difference fields: Algebraic products, like
\[
(-1)^k = \prod_{i=1}^{k} (-1), \quad (-1)^{\frac{k+1}{2}} = \prod_{i=1}^{k} \prod_{j=1}^{i} (-1), \quad (-1)^{\frac{k+2}{3}} = \prod_{i=1}^{k} \prod_{j=1}^{i} \prod_{k=1}^{j} (-1), \ldots \tag{4}
\]
cannot be expressed in \( \Pi\Sigma \)-fields, which are built by a tower of transcendental field extensions. Even worse, the objects given in (4) introduce zero-divisors, like
\[
(1 - (-1)^k)(1 + (-1)^k) = 0 \tag{5}
\]
which cannot be treated in a field or in an integral domain. In applications these objects occur rather frequently as standalone objects or in nested sums [3,4]. It is thus a fundamental challenge to include such objects in an enhanced summation theory.

With the elegant theory of [60,19] one can handle such objects by several copies of the underlying difference field, i.e., by implementing the concept of interlacing in an algebraic way. First steps to combine these techniques with \( \Pi\Sigma \)-fields have been made in [17].
Within the package **Sigma** a different approach [42] has been implemented. Summation objects like \((-1)^k\) and sums over such objects are introduced by a tower of generators subject to the relations such as (5). In this way one obtains a direct translation between the summation objects and the generators of the corresponding difference rings. This enhancement has been applied non-trivially, e.g., to combinatorial problems [44,39], number theory [50,33] or to problems from particle physics [12]: for the most recent evaluations of Feynman integrals [11,2,1] up to 300 generators were used to model the summation objects in difference rings. But so far, this successful and very efficient machinery of Sigma was built, at least partially, on heuristic considerations.

In this article we shall develop the underlying difference ring theory and supplement it with the missing algorithmic building blocks in order to obtain a rigorous summation machinery. More precisely, we will enhance the difference field theory of [24,25] to a difference ring theory by introducing besides \(\Pi\)-extensions (for transcendental product extensions) and \(\Sigma^*\)-extensions (for transcendental sum extensions) also \(R\)-extensions which enables one to represent objects such as (4). An important ingredient of this theory is the exploration of the so-called semi-constants (resp. semi-invariants) and the formulation of the symbolic summation problems within these notions. In particular, we obtain algorithms that can solve parameterized first-order linear difference equations. As special instance we obtain algorithms for the parameterized telescoping problem, in particular for the summation paradigms of telescoping and creative telescoping. In addition, we provide an algorithmic toolbox that supports the construction of the so-called simple \(R\Pi\Sigma^*\)-extensions automatically. As special case we demonstrate, how d’Alembertian solutions [7] of a recurrence, a subclass of Liouvillian solutions [20,38], can be represented in such \(R\Pi\Sigma^*\)-extensions. In particular, we will illustrate the underlying problems and their solutions by discovering the following identities

\[
\sum_{k=1}^{b} (-1)^{\frac{k+1}{2}} k^2 \sum_{j=1}^{k} \frac{(-1)^j}{j} = \frac{1}{2} \sum_{j=1}^{b} \frac{(-1)^{\frac{j+1}{2}}}{j} - \frac{1}{4} (-1)^{\frac{b+1}{2}} \left( - 1 + (-1)^b + 2b \right) + (-1)^{\frac{b+1}{2}} \frac{1}{2} (b(b+2) + (-1)^b (b^2 - 1)) \sum_{j=1}^{b} \frac{(-1)^j}{j},
\]

\[
\prod_{k=1}^{b} \frac{-(i^k)}{1 + k} = \left( - \frac{b}{2} - \frac{1}{2} \right) \frac{(-1)^b + b}{b(b+1)} \left( \prod_{j=1}^{b-1} j \right)^l;
\]

here the imaginary part is denoted with \(i\), i.e., \(i^2 = -1\).

The outline is as follows. In Section 2 we will introduce the basic notations of difference rings (resp. fields) and define \(R\Pi\Sigma^*\)-ring extensions. Furthermore, we will work out the underlying problems in the setting of difference rings and motivate the different challenges that will be treated in this article. In addition, we give an overview of the main results and show how they can be applied for symbolic summation. In the remaining sections these results will be worked out in details. In Section 3 we present the crucial properties of single nested \(R\Pi\Sigma^*\)-extension. Special emphasis will be put on the properties of the underlying ring. In Section 4 we will consider a tower of such extensions and explore the set of semi-constants. In Section 5 we present algorithms that calculate the order, period and factorial order of the generators of \(R\)-extensions. Finally, in Section 6 and Section 7 we elaborate algorithms that are needed to construct \(R\Pi\Sigma^*\)-extensions and that solve as special case the (parameterized) telescoping problem. A conclusion is given in Section 8.
2. Basic definitions, the outline of the problems, and the main results

In this article all rings are commutative with 1 and all rings (resp. fields) have characteristic 0; in particular, they contain the rational numbers \( \mathbb{Q} \) as a subring (resp. subfield). A ring (resp. field) is called computable if there are algorithms available that can perform the standard operations (including zero recognition and deciding constructively if an element is invertible). The multiplicative group of units (invertible elements) of \( \mathbb{A} \) is denoted by \( \mathbb{A}^* \). If \( \mathbb{A} \) is a subring (resp. subfield/multiplicative subgroup) of \( \mathbb{A} \) we also write \( \mathbb{A} \leq \mathbb{A} \). The non-negative integers are denoted by \( \mathbb{N} = \{0, 1, 2, \ldots\} \).

In this section we will present a general framework in which the symbolic summation problems can be formulated and tackled in the setting of difference rings. Here indefinite nested product-sum expression \( f(k) \) such as in (1) and (3) are described in a ring (resp. field) \( \mathbb{A} \) and the shift behaviour of such an expression is reflected by a ring automorphism (resp. field automorphism) \( \sigma : \mathbb{A} \rightarrow \mathbb{A} \), i.e., \( \sigma^i(f) \) with \( i \in \mathbb{Z} \) represents the expression \( F(k + i) \). In the following we call such a ring \( \mathbb{A} \) (resp. field) equipped with a ring automorphism (resp. field automorphism) \( \sigma \) a difference ring (resp. difference field) [16,31] and denote it by \( (\mathbb{A}, \sigma) \). We remark that any difference field is also a difference ring. Conversely, any difference ring \( (\mathbb{A}, \sigma) \) with \( \mathbb{A} \) being a field is automatically a difference field. A difference ring (resp. field) \( (\mathbb{A}, \sigma) \) is called computable if both, \( \mathbb{A} \) and the function \( \sigma \) are computable; note that in such rings one can decide if an element is a constant, i.e., if \( \sigma(c) = c \). The set of constants is also denoted by \( \text{const}(\mathbb{A}, \sigma) = \{ c \in \mathbb{A} \mid \sigma(c) = c \} \), and if it is clear from the context we also write \( \text{const}\mathbb{A} = \text{const}(\mathbb{A}, \sigma) \). It is easy to check that \( \text{const}\mathbb{A} \) is a subring (resp. a subfield) of \( \mathbb{A} \) which contains as subring (resp. subfield) the rational numbers \( \mathbb{Q} \). Throughout this article we will take care that \( \text{const}\mathbb{A} \) is always a field (and not just a ring), called the constant field and denoted by \( \mathbb{K} \).

In the first subsection we introduce the class of difference rings in which we will model indefinite nested sums and products. They will be introduced by a tower of ring extensions, the so-called \( R\Pi\Sigma^* \)-difference extensions.

In Subsection 2.2 we will focus on two tasks:

1. Introduce techniques that enable one to test if the given tower of extensions is an \( R\Pi\Sigma^* \)-extension; even more, derive tactics that enable one to represent sums and products automatically in \( R\Pi\Sigma^* \)-extensions.

2. Work out the underlying subproblems in order to solve two central problems of symbolic summation: telescoping (compare (1)) and parameterized telescoping (compare (3)). In their simplest form they can be specified as follows.

**Problem T for** \( (\mathbb{A}, \sigma) \). Given a difference ring \( (\mathbb{A}, \sigma) \) and given \( f \in \mathbb{A} \). Find, if possible, a \( g \in \mathbb{A} \) such that the telescoping (T) equation holds:

\[
\sigma(g) - g = f. \tag{8}
\]

**Problem PT for** \( (\mathbb{A}, \sigma) \). Given a difference ring \( (\mathbb{A}, \sigma) \) with constant field \( \mathbb{K} \) and given \( f_1, \ldots, f_n \in \mathbb{A} \). Find, if possible, \( c_1, \ldots, c_n \in \mathbb{K} \) (not all \( c_i \) being zero) and a \( g \in \mathbb{A} \) such that the parameterized telescoping (PT) holds:

\[
\sigma(g) - g = c_1 f_1 + \cdots + c_n f_n. \tag{9}
\]

In Subsection 2.3 we will present the main results of theoretical and algorithmic nature to handle these problems, and in Subsection 2.4 we demonstrate how the new summation theory can be used to represent d’Alembertian solutions in \( R\Pi\Sigma^* \)-extensions.
2.1. The definition of $\Pi\Sigma^*$-extensions

A difference ring $(\mathcal{A}, \sigma)$ is a difference ring extension of a difference ring $(\mathcal{A}, \sigma)$ if $\mathcal{A} \subseteq \mathcal{A}'$ and $\sigma|_{\mathcal{A}} = \sigma$, i.e., $\mathcal{A}$ is a subring of $\mathcal{A}'$ and $\sigma(a) = \sigma(a)$ for all $a \in \mathcal{A}$. The definition of difference field extensions is the same by replacing the word ring with field. In short (for the ring and field version) we also write $(\mathcal{A}, \sigma) \leq (\mathcal{A}', \sigma')$. If it is clear from the context, we do not distinguish anymore between $\sigma$ and $\sigma'$.

For the construction of $\Pi\Pi\Sigma^*$-extensions, we start with the following basic properties.

**Lemma 1.** Let $\mathcal{A}$ be a ring with $\alpha \in \mathcal{A}^*$ and $\beta \in \mathcal{A}$ together with a ring automorphism $\sigma : \mathcal{A} \to \mathcal{A}$. Let $\mathcal{A}[t]$ be a polynomial ring and $\mathcal{A}[t, \frac{1}{t}]$ be the ring of Laurent polynomials.

1. There is a unique automorphism $\sigma' : \mathcal{A}[t] \to \mathcal{A}[t]$ with $\sigma'|_{\mathcal{A}} = \sigma$ and $\sigma'(t) = \alpha t + \beta$.
2. There is a unique automorphism $\sigma'' : \mathcal{A}[t, \frac{1}{t}] \to \mathcal{A}[t, \frac{1}{t}]$ with $\sigma''|_{\mathcal{A}} = \sigma$ and $\sigma''(t) = \alpha t$ (where $\alpha' = \alpha^{1-\frac{1}{\beta}}$). In particular, if $\beta = 0$, $\sigma''|_{\mathcal{A}[t]} = \sigma'$.

3. If $\mathcal{A}$ is a field and $\mathcal{A}(t)$ is a rational function field, there is a unique field automorphism $\sigma''' : \mathcal{A}(t) \to \mathcal{A}(t)$ with $\sigma'''|_{\mathcal{A}} = \sigma$ and $\sigma'''(t) = \alpha t + \beta$. In particular, $\mathcal{A}(t)$ is called $\Pi$-field extension.

In summary, we obtain the uniquely determined difference ring extension $(\mathcal{A}[t], \sigma)$ of $(\mathcal{A}, \sigma)$ with $\sigma(t) = \alpha t + \beta$ where $\alpha \in \mathcal{A}^*$ and $\beta \in \mathcal{A}$. In particular, we get the uniquely determined difference ring extension $(\mathcal{A}[t, \frac{1}{t}], \sigma)$ of $(\mathcal{A}, \sigma)$ with $\sigma(t) = \alpha t$. Thus for $\beta = 0$, we have the chain of extensions $(\mathcal{A}, \sigma) \leq (\mathcal{A}[t], \sigma) \leq (\mathcal{A}[t, \frac{1}{t}], \sigma)$. Moreover, if $\mathcal{A}$ is a field, we obtain the uniquely determined difference field extension $(\mathcal{A}(t), \sigma)$ of $(\mathcal{A}, \sigma)$ with $\sigma(t) = \alpha t + \beta$. Following the notions of [14] each of the extensions, i.e., $(\mathcal{A}, \sigma) \leq (\mathcal{A}[t], \sigma), (\mathcal{A}, \sigma) \leq (\mathcal{A}[t, \frac{1}{t}], \sigma)$ or $(\mathcal{A}, \sigma) \leq (\mathcal{A}(t), \sigma)$ are called unimonomial extensions (of polynomial, Laurent polynomial or of rational function type, respectively).

**Example 1.** (0) Take the difference field $(\mathbb{Q}, \sigma)$ with $\sigma(c) = c$ for all $c \in \mathbb{Q}$.

1. Take the unimonomial field extension $Q(k, \sigma)$ of $(\mathbb{Q}, \sigma)$ with $\sigma(k) = k + 1$: $\mathbb{Q}(k)$ is a rational function field and $\sigma$ is extended from $\mathbb{Q}$ to $\mathbb{Q}(k)$ with $\sigma(k) = k + 1$. $\mathbb{Q}(k)$ is a field, a unimonomial field extension $(\mathbb{Q}(k), \sigma)$ of $(\mathbb{Q}, \sigma)$ with $\sigma(t) = \alpha t$.

2. Take the unimonomial field extension $Q(k)[t, \frac{1}{t}], \sigma)$ of $(\mathbb{Q}(k), \sigma)$ with $\sigma(t) = (k + 1)t$: $Q(k)[t, \frac{1}{t}]$ is a ring of Laurent polynomials with coefficients from $\mathbb{Q}(k)$ and the automorphism is extended from $\mathbb{Q}(k)$ to $\mathbb{Q}(k)[t, \frac{1}{t}]$ with $\sigma(t) = (k + 1)t$.

Finally, we consider those extensions where the constants remain unchanged.

**Definition 1.** Let $(\mathcal{A}, \sigma)$ be a difference ring.

- A unimonomial ring extension $(\mathcal{A}[t], \sigma)$ of $(\mathcal{A}, \sigma)$ with $\sigma(t) - t \in \mathcal{A}$ and $\text{const}\mathcal{A}[t] = \text{const}\mathcal{A}$ is called $\Sigma^*$-ring extension (in short $\Sigma^*$-extension).
- If $\mathcal{A}$ is a field, a unimonomial field extension $(\mathcal{A}(t), \sigma)$ of $(\mathcal{A}, \sigma)$ with $\sigma(t) - t \in \mathcal{A}$ and $\text{const}\mathcal{A}(t) = \text{const}\mathcal{A}$ is called $\Sigma^*$-field extension.
- A unimonomial ring extension $(\mathcal{A}[t, \frac{1}{t}], \sigma)$ of $(\mathcal{A}, \sigma)$ with $\sigma(t) \in \mathcal{A}^*$ and $\text{const}\mathcal{A}[t, \frac{1}{t}] = \text{const}\mathcal{A}$ is called $\Pi$-ring extension (in short $\Pi$-extension).
- If $\mathcal{A}$ is a field, a unimonomial field extension $(\mathcal{A}(t), \sigma)$ of $(\mathcal{A}, \sigma)$ with $\sigma(t) \in \mathcal{A}^*$ = $\mathcal{A}(t) \setminus \{0\}$ and $\text{const}\mathcal{A}(t) = \text{const}\mathcal{A}$ is called $\Pi$-field extension.

---

1. We restrict Karr’s $\Sigma$-field extensions to $\Sigma^*$-field extensions being slightly less general but covering all sums treated explicitly in Karr’s work [24].
The generators of a $\Sigma^*$-extension (in the ring or field version) and a $\Pi$-extension (in the ring or field version) are called $\Sigma^*$-monomials and $\Pi$-monomials, respectively.

**Remark 1.** Keeping the constants unchanged is a central property to tackle the parameterized telescoping problem. E.g., if the constants are extended, there do not exist bounds on the degrees as utilized in Subsection 7.1.1. Moreover, introducing no extra constants is the essential property to embed the derived difference rings into the ring of sequences; this fact has been worked out, e.g., in [54] which is related to [19].

**Example 2** (Cont. Ex. 1). For $(\mathbb{Q}, \sigma) \leq (\mathbb{Q}(k), \sigma) \leq (\mathbb{Q}(k)[t, \frac{1}{t}], \sigma)$ from Example 1 we have that $\text{const} \mathbb{Q}(k)[t, \frac{1}{t}] = \text{const} \mathbb{Q}(k) = \text{const} \mathbb{Q} = \mathbb{Q}$, which can be checked algorithmically; either by our algorithms given below or given in [24]. Thus $(\mathbb{Q}(k), \sigma)$ is a $\Sigma^*$-field extension of $(\mathbb{Q}, \sigma)$ and $(\mathbb{Q}(k)[t, \frac{1}{t}], \sigma)$ is a $\Pi$-extension of $(\mathbb{Q}(k), \sigma)$. The generator $k$ is a $\Sigma^*$-monomial and the generator $t$ is a $\Pi$-monomial.

For further considerations we introduce the order function $\text{ord}: A \to \mathbb{N}$ with

$$\text{ord}(h) = \begin{cases} 0 & \text{if } \exists n > 0 \text{ s.t. } h^n = 1 \\ \min\{n > 0 | h^n = 1\} & \text{otherwise.} \end{cases}$$

The third type of extensions is concerned with algebraic objects like (4). Let $\lambda \in \mathbb{N}$ with $\lambda > 1$, take a root of unity $\alpha \in A^*$ with $\alpha^\lambda = 1$ and construct the unimonomial extension $(A[y], \sigma)$ of $(A, \sigma)$ with $\sigma(y) = \alpha y$. Now take the ideal $I := (y^\lambda - 1)$ and consider the quotient ring $E = A[y]/I$. Since $I$ is closed under $\sigma$, i.e., $I$ is a difference ideal, one can verify that $\sigma: E \to E$ with $\sigma(f + I) = \sigma(f) + I$ forms a ring automorphism. In other words, $(E, \sigma)$ is a difference ring. Moreover, there is the natural embedding of $A$ into $E$ with $a \to a + I$. By identifying $a$ with $a + I$, $(E, \sigma)$ is a difference ring extension of $(A, \sigma)$.

**Lemma 2.** Let $(A, \sigma)$ be a difference ring and $\alpha \in A^*$ with $\alpha^\lambda = 1$ for some $\lambda > 1$. Then there is (up to a difference ring isomorphism) a unique difference ring extension $(A[x], \sigma)$ of $(A, \sigma)$ subject to the relations $x^\lambda = 1$ and $\sigma(x) = \alpha x$.

**Proof.** Consider the difference ring extension $(E, \sigma)$ of $(A, \sigma)$ constructed above. Define $x := y + I$. Then $\sigma(x) = \alpha x$ and $x^\lambda = y^\lambda + I = 1 + I = 1$. Moreover $E = \{\sum_{i=0}^{\lambda-1} a_i x^i | a_i \in A\}$. Thus we obtain a difference ring extension as claimed in the lemma. Now suppose that there is another difference ring extension $(A[x'], \sigma')$ of $(A, \sigma)$ subject to the relations $\sigma'(x') = \alpha x'$ and $x'^\lambda = 1$. Then by the first isomorphism theorem, there is the ring isomorphism $\tau: E \to A[x']$ with $\tau(\sum_{i=0}^{\lambda-1} f_i x_i) = \sum_{i=0}^{\lambda-1} f_i x'_i$. Since $\tau(\sigma(x)) = \tau(\alpha x) = \tau(\alpha) \tau(x) = \alpha x' = \sigma'(x')$, it follows that $\tau(\sigma(f)) = \sigma'(\tau(f))$ for all $f \in A[x]$. Summarizing, $\tau$ is a difference ring isomorphism. □

The extension $(A[x], \sigma)$ of $(A, \sigma)$ in Lemma 2 is called algebraic extension of order $\lambda$.

**Example 3.** (0) Take the $\Sigma^*$-extension $(\mathbb{Q}(k), \sigma)$ of $(\mathbb{Q}, \sigma)$ with $\sigma(k) = k + 1$ from Ex. 2.

1. Take the algebraic extension $(\mathbb{Q}(k)[x], \sigma)$ of $(\mathbb{Q}(k), \sigma)$ with $\sigma(x) = -x$ of order 2: $\mathbb{Q}(k)[x]$ is an algebraic ring extension of $\mathbb{Q}(k)$ subject to the relation $x^2 = 1$ and $\sigma$ is extended form $\mathbb{Q}(k)$ to $\mathbb{Q}(k)[x]$ with $\sigma(x) = -x$. Note that $x$ represents $(-1)^k$.

2. Take the algebraic extension $(\mathbb{Q}(k)[y], \sigma)$ of $(\mathbb{Q}(k)[x], \sigma)$ with $\sigma(y) = -xy$ of order 2: $\mathbb{Q}(k)[x][y]$ is a ring extension of $\mathbb{Q}(k)[x]$ with $y^2 = 1$ and $\sigma$ is extended from $\mathbb{Q}(k)[x]$ to $\mathbb{Q}(k)[x][y]$ with $\sigma(y) = -xy$. Note that $y$ represents $(-1)^{(k+1)} = \prod_{j=1}^{k}(-1)^j$. 

6
As for unimonomial extensions, we restrict now to those algebraic extensions where the constants remain unchanged. For the underlying motivation we refer to Remark 1.

**Definition 2.** Let \( \lambda \in \mathbb{N} \setminus \{0, 1\} \). An algebraic extension \((\mathbb{A}[x], \sigma)\) of \((\mathbb{A}, \sigma)\) order \( \lambda \) with \( \text{const}\mathbb{A}[x] = \text{const}\mathbb{A} \) is called root of unity extension (in short \( R \)-extension) of order \( \lambda \).

The generator \( x \) is called \( R \)-monomial.

**Example 4 (Cont. Ex. 3).** For \((\mathbb{Q}(k), \sigma) \leq (\mathbb{Q}(k)[x], \sigma) \leq (\mathbb{Q}(k)[x][y], \sigma)\) from Example 3 we have that \( \text{const}\mathbb{Q}(k)[x][y] = \text{const}\mathbb{Q}(k) = \mathbb{Q} \), which can be checked algorithmically; see Example 6 below. Thus \((\mathbb{Q}(k)[x], \sigma)\) is an \( R \)-extension of \((\mathbb{Q}(k), \sigma)\) and \((\mathbb{Q}(k)[x][y], \sigma)\) is an \( R \)-extension of \((\mathbb{Q}(k)[x], \sigma)\).

To this end, we define a tower of such extensions. First, we introduce the following notion. Let \((\mathbb{A}, \sigma) \leq (\mathbb{E}, \sigma)\) with \( t \in \mathbb{E} \). In the following \( \mathbb{A}(t) \) denotes the polynomial ring \( \mathbb{A}[t] \) if \((\mathbb{A}(t), \sigma)\) is a \( \Sigma^* \)-extension of \((\mathbb{A}, \sigma)\). \( \mathbb{A}(t) \) denotes the ring of Laurent polynomials \( \mathbb{A}[t, \frac{1}{t}] \) if \((\mathbb{A}(t, \frac{1}{t}), \sigma)\) is a \( \Pi \)-extension of \((\mathbb{A}, \sigma)\). Finally, \( \mathbb{A}(t) \) denotes the algebraic ring \( \mathbb{A}[t] \) subject to the relation \( t^\lambda = 1 \) if \((\mathbb{A}(t), \sigma)\) is an \( R \)-extension of \((\mathbb{A}, \sigma)\) of order \( \lambda \).

**Definition 3.** A difference ring extension \((\mathbb{A}(t), \sigma)\) of \((\mathbb{A}, \sigma)\) is called \( R\Pi\Sigma^* \)-extension if it is an \( R \)-extension, \( \Pi \)-extension or \( \Sigma^* \)-extension. Analogously, it is called \( R\Sigma^* \)-extension, \( R\Pi \)-extension or \( \Pi\Sigma^* \)-extension if it is one of the corresponding extensions. More generally, \((\mathbb{G}(t_1)\langle t_2 \rangle \ldots \langle t_e \rangle, \sigma)\) is an \( R\Pi\Sigma^* \)-extension (resp. \( R\Pi, R\Sigma^*, \Pi\Sigma^*, \Pi\Sigma^*-\)field extension) of \((\mathbb{G}, \sigma)\) if it is a tower of such extensions.

Similarly, if \( \mathbb{A} \) is a field, \((\mathbb{A}(t), \sigma)\) is called a \( \Pi\Sigma^* \)-field extension if it is either a \( \Pi \)-field extension or a \( \Sigma^* \)-field extension. \((\mathbb{G}(t_1) \ldots \langle t_e \rangle, \sigma)\) is called a \( \Pi\Sigma^* \)-field extension (resp. \( \Pi \)-field extension, \( \Sigma^* \)-field extension) of \((\mathbb{G}, \sigma)\) if it is a tower of such extensions. In particular, if \( \text{const}\mathbb{G} = \mathbb{G} \), \((\mathbb{G}(t_1)\langle t_2 \rangle \ldots \langle t_e \rangle, \sigma)\) is called a \( \Pi\Sigma^* \)-field over \( \mathbb{G} \).

In both, the ring and field version, \( t_i \) is called \( \Pi\Sigma^* \)-monomial (resp. \( \Pi\Pi\Pi \), \( R\Sigma^* \), \( \Pi\Sigma^* \)-monomial) if it is a generator of a \( R\Pi\Sigma^* \)-extension (resp. \( R\Pi\Pi \), \( R\Sigma^* \), \( \Pi\Sigma^* \)-extension).

**Example 5 (Cont. Ex. 4).** (1) \((\mathbb{Q}(k), \sigma)\) is a \( \Pi\Sigma^* \)-field over \( \mathbb{Q} \).

(2) \((\mathbb{Q}(k)[x]/(y), \sigma)\) is an \( R \)-extension of \((\mathbb{Q}(k), \sigma)\).

The generators with their sequential arrangement, incorporating the recursive definition of the automorphism, are always given explicitly. In particular, any reordering of the generators must respect the recursive nature induced by the automorphism.

### 2.2. A characterization of \( R\Pi\Sigma^* \)-extensions and their algorithmic construction

For the construction of \( R\Pi\Sigma^* \)-extensions we rely on the following result; for the proofs we refer to page 18 for part 1, page 19 for part 2, and page 21 for part 3.

**Theorem 1.** Let \((\mathbb{A}, \sigma)\) be a difference ring. Then the following holds

1. Let \((\mathbb{A}[t], \sigma)\) be a unimonomial ring extension of \((\mathbb{A}, \sigma)\) with \( \sigma(t) = t + \beta \) where \( \beta \in \mathbb{A} \) such that \( \text{const}\mathbb{A} \) is a field. Then this is a \( \Sigma^* \)-extension (i.e., \( \text{const}\mathbb{A}[t] = \text{const}\mathbb{A} \)) if there does not exist a \( g \in \mathbb{A} \) with \( \sigma(g) = g + \beta \).

2. Let \((\mathbb{A}[t, \frac{1}{t}], \sigma)\) be a unimonomial ring extension of \((\mathbb{A}, \sigma)\) with \( \sigma(t) = \alpha \) where \( \alpha \in \mathbb{A}^* \). Then this is a \( \Pi \)-extension (i.e., \( \text{const}\mathbb{A}[t, \frac{1}{t}] = \text{const}\mathbb{A} \)) if there are no \( g \in \mathbb{A} \setminus \{0\} \) and \( m \in \mathbb{Z} \setminus \{0\} \) with \( \sigma(g) = \alpha^m g \). If it is a \( \Pi \)-extension, \( \text{ord}(\alpha) = 0 \).
(3) Let be \((\mathbb{A}[t], \sigma)\) an algebraic ring extension of \((\mathbb{A}, \sigma)\) of order \(\lambda > 1\) with \(\sigma(t) = \alpha t\) where \(\alpha \in \mathbb{A}^*\). Then this is an \(R\)-extension (i.e. \(\text{const}\mathbb{A}[t] = \text{const}\mathbb{A}\)) if there are no \(g \in \mathbb{A} \setminus \{0\}\) and \(m \in \{1, \ldots, \lambda - 1\}\) with \(\sigma(g) = \alpha^m g\). If it is an \(R\)-extension, then \(\alpha\) is primitive, i.e., \(\text{ord}(\alpha) = \lambda\).

For Karr’s celebrated field version \([24,25]\) of this result we refer to Theorems 6 and 10, that can be nicely embedded in the general difference ring framework. As in Karr’s work, Theorem 1 facilitates algorithmic tactics to verify if a given extension is an \(R\Pi\Sigma^*\)-extension. Here we consider two cases.

### 2.2.1. Testing and constructing \(R\Pi\Sigma^*\)-extensions

For a unimonomial extension as given in Theorem 1.2 or an algebraic extension as given Theorem 1.3 with \(\alpha = \sigma(t)/t\) one should first check if \(\alpha \in \mathbb{A}^*\). For the class of difference rings \((\mathbb{A}, \sigma)\), built by simple \(R\Pi\Sigma^*\)-extensions introduced in Definition 4 below, this task will be straightforward. Next, we need the order of \(\alpha\), i.e., we have to solve the following Problem O with \(G := \mathbb{A}^*\).

#### Problem O in \(G\). Given a group \(G\) and \(\alpha \in G\). Find \(\text{ord}(\alpha)\).

Given \(\lambda = \text{ord}(\alpha)\), we can decide which case has to be treated: if \(\lambda = 0\), we have to test if the generator \(t\) is a \(\Pi\)-monomial, and if \(\lambda > 0\), we have to check if the generator \(t\) is an \(R\)-monomial. Using Theorem 1 this test can be accomplished by solving

#### Problem MT in \((\mathbb{A}, \sigma)\). Given a difference ring \((\mathbb{A}, \sigma)\) and \(\alpha \in \mathbb{A}^*\) with \(\lambda = \text{ord}(\alpha)\). Decide if there are a \(g \in \mathbb{A} \setminus \{0\}\) and an \(m \in \mathbb{Z} \setminus \{0\}\) for the case \(\lambda = 0\) (resp. \(m \in \{1, \ldots, \lambda - 1\}\) for the case \(\lambda > 0\)) such that the multiplicative version of the telescoping equation holds:

\[
\sigma(g) = \alpha^m g. \tag{11}
\]

**Example 6** (Cont. Ex. 4). We verify that \((\mathbb{Q}(k)[x][y], \sigma)\) is an \(R\)-extension of \((\mathbb{Q}(k), \sigma)\).

(1) Take \(\alpha = -1\). We can solve Problem O and get \(\lambda = \text{ord}(\alpha) = 2\). Moreover, we solve Problem MP by the algorithms presented below: there are no \(g \in \mathbb{Q}(k)^*\) and \(m \in \{1\}\) with \(\sigma(g) = (-1)^m g\). Hence by Theorem 1.3 \((\mathbb{Q}(k)(x), \sigma)\) is an \(R\)-extension of \((\mathbb{Q}(x), \sigma)\).

(2) Now we solve Problem O for \(\alpha = -x\) and get \(\lambda = \text{ord}(-x) = 2\); see Example 12.2. Moreover, solving Problem MP for \(\alpha\) shows that there is no \(g \in \mathbb{Q}(k)[x] \setminus \{0\}\) with \(\sigma(g) = -x g\). Thus by Theorem 1.3 \((\mathbb{Q}(k)[x][y], \sigma)\) forms an \(R\)-extension of \((\mathbb{Q}(k)[x], \sigma)\).

**Example 7.** We construct a difference ring in which the objects in (7) can be represented.

(0) Take the \(\Pi\Sigma^*\)-field \((K(k), \sigma)\) over \(K = \mathbb{Q}(\iota)\) with \(\sigma(k) = k + 1\).

(1) Take \(\alpha = \iota\). Then solving Problem O provides \(\lambda = \text{ord}(\alpha) = 4\). In particular solving Problem MP proves that there are no \(g \in K(k)^*\) and \(m \in \{1, 2, 3\}\) with (11). Hence by Theorem 1.3 we can construct the \(R\)-extension \((K(k)[x], \sigma)\) of \((K(k), \sigma)\) with \(\sigma(x) = \iota x\). Note that the \(R\)-monomial \(x\) represents \(t^k\).

(2) Take \(\alpha = x k\). Solving Problem O yields \(\lambda = \text{ord}(\alpha) = 0\) and solving Problem MP shows that there are no \(g \in K(k)[x] \setminus \{0\}\) and \(m \in \mathbb{Z} \setminus \{0\}\) with (11). With Theorem 1.2 we get the \(\Pi\)-extension \((K(k)[x], \sigma) \leq (K(k)[x](t), \sigma)\) with \(\sigma(t) = x k t\); here the \(\Pi\)-monomial \(t\) represents \(\prod_{j=1}^{k-1} j^k\).
2.2.2. Testing and constructing $\Sigma^*$-extensions

In order to verify if a unimonomial extension as given in Theorem 1.1 is a $\Sigma^*$-extension, it suffices to solve Problem T with $f = \beta$ and to check if there is a telescoping solution. We illustrate this feature by actually constructing a difference ring in which the summand

$$f(k) = (-1)^k \sum_{j=1}^{k} \frac{(-1)^j}{j}$$

(12)
given on the left hand side of (6) and the additional sum

$$\sum_{j=1}^{k} \frac{(-1)^j}{j}$$

(13)

occurring on the right hand side of (6) can be represented. In particular, we demonstrate how identity (6) can be discovered in this difference ring.

Example 8 (Cont. Ex. 4). (0) Take the difference ring $(\mathbb{A}, \sigma)$ with $\mathbb{A} = \mathbb{Q}(k)[x][y]$. (1) Take $f = \frac{y}{x}$. Then solving Problem T shows that there is no $g \in \mathbb{A}$ with $\sigma(g) - g = \frac{y}{x}$. Hence we can construct the $\Sigma^*$-extension $(\mathbb{A}[s], \sigma)$ of $(\mathbb{A}, \sigma)$ with $\sigma(s) = s + \frac{x}{y}$; note that the $\Sigma^*$-monomial $s$ represents $\sum_{j=1}^{k} \frac{(-1)^j}{j}$ in our difference ring.

(2) Take $f = \frac{y}{x}$. Then solving Problem T shows that there is no $g \in \mathbb{A}[s]$ such that $\sigma(g) - g = \frac{y}{x}$. Hence we can construct the $\Sigma^*$-extension $(\mathbb{A}[s][S], \sigma)$ of $(\mathbb{A}[s], \sigma)$ with $\sigma(S) = S + \frac{x}{y}$; note that the $\Sigma^*$-monomial $S$ represents the sum (13).

(3) Take $f = \frac{y}{x}k^2s$ which represents (12). Solving Problem T produces the solution

$$g = sy\left(\frac{1}{2}(k-1)(k+1)x - \frac{1}{2}(k-2)k\right) + y\left(\frac{1}{4}(1-2k) - \frac{1}{4}x\right) + \frac{1}{2}S.$$  

(14)

Hence this yields the solution of the telescoping equation (1) for our summand (12) by replacing the $R \Sigma^*$-monomials $x, y, s, S$ with the corresponding summation objects. Taking $a = 1$ in (2) and performing the evaluation $c := g(1) = 0 \in \mathbb{Q}$ gives the identity (6).

(4) Note that we succeeded in representing the sum $F(k) = \sum_{i=1}^{k} f(i)$ with $f$ from (12) in the difference ring in $\mathbb{A}[s][S]$ with $\sigma(g) - c = \sigma(g)$. Namely, replacing the variables in $\sigma(g)$ with the corresponding summation objects yields the right hand side of (6). This is of particular interest if there are further sums defined over $F(k)$ which one wants to represent in a $\Sigma^*$-extension over $(\mathbb{A}[s][S], \sigma)$.

We remark that for the derivation of the identity (6) it is crucial to introduce the extra sum (13). Here this was accomplished manually. But, using algorithms from [53,58] in combination with the results of this article, this sum can be determined automatically.

2.2.3. The underlying problems for $R \Pi \Sigma^*$-extensions

As in the difference field approach [24,49,53,58], Problem T (and more generally Problem PT) and Problem MT will be solved by reducing these problems from $(\mathbb{A}, \sigma)$ to smaller difference rings (i.e., rings built by less $R \Pi \Sigma^*$-monomials). However, in order to succeed in this reduction, parameterized versions of these problems have to be solved.

For Problem MT the following generalization is needed. Let $(\mathbb{A}, \sigma)$ be a difference ring, let $W \subseteq \mathbb{A}$ and let $\mathbf{f} = (f_1, \ldots, f_n) \in (\mathbb{A}^*)^n$. Then we define the set

$$M(\mathbf{f}, W) := \{(m_1, \ldots, m_n) \in \mathbb{Z}^n | \sigma(g) = f_1^{m_1} \cdots f_n^{m_n} g \text{ for some } g \in W \setminus \{0\}\}.$$
In the following, we want to calculate a finite representation of \( M(\mathcal{A}) \). If \( \mathcal{A} \) is a field, i.e., \( \mathcal{A}^* = \mathcal{A} \setminus \{0\} \), it is immediate that \( M(\mathcal{A}) \) is a submodule of \( \mathbb{Z}^n \) over \( \mathbb{Z} \) and there is a basis of \( M(\mathcal{A}) \) with rank \( \leq n \). In the setting of rings, this result carries over if the set of semi-constants (also called semi-invariants \([14]\)) of \( (\mathcal{A}, \sigma) \) defined by

\[
\text{sconst}(\mathcal{A}, \sigma) = \{ c \in \mathcal{A} | \sigma(c) = u c \text{ for some } u \in \mathcal{A}^* \}
\]

forms a multiplicative group (excluding the 0 element). Note: if \( \mathcal{A} \) is a field, we have that \( \text{sconst}(\mathcal{A}, \sigma) = \mathcal{A} \). Unfortunately, for a general difference ring the set \( \text{sconst}(\mathcal{A}, \sigma) \setminus \{0\} \) is only a multiplicative monoid \([14]\). In order to gain more flexibility, we introduce the following refinement. For a given multiplicative subgroup \( G \) of \( \mathcal{A}^* \) (in short \( G \leq \mathcal{A}^* \)), we define the set of semi-constants (semi-invariants) of \( (\mathcal{A}, \sigma) \) over \( G \) by

\[
\text{sconst}_G(\mathcal{A}, \sigma) = \{ c \in \mathcal{A} | \sigma(c) = u c \text{ for some } u \in G \}.
\]

Note that \( \text{sconst}_{(\mathcal{A}^*)}(\mathcal{A}, \sigma) = \text{sconst}(\mathcal{A}, \sigma) \) and \( \text{sconst}_{\{1\}}(\mathcal{A}, \sigma) = \text{const}(\mathcal{A}, \sigma) \). If it is clear from the context, we drop \( \sigma \) and just write \( \text{sconst}_G \mathcal{A} \) and \( \text{sconst} \mathcal{A} \), respectively.

Here is one of the main challenges: For all our considerations we will choose \( G \) such that \( \text{sconst}_G(\mathcal{A}) \setminus \{0\} \) is a subgroup of \( \mathcal{A}^* \) (in short, \( \text{sconst} \mathcal{A} \setminus \{0\} \leq \mathcal{A}^* \)). Then with this careful choice of \( G \) we can summarize the above considerations with the following lemma.

**Lemma 3.** Let \( (\mathcal{A}, \sigma) \) be a difference ring and \( G \leq \mathcal{A}^* \) such that \( \text{sconst}_G(\mathcal{A}) \setminus \{0\} \leq \mathcal{A}^* \); let \( f \in \mathbb{G}^{\mathcal{A}} \). Then \( M(\mathcal{A}, \mathcal{A}) = M(f, \text{sconst}_G \mathcal{A}) \). In particular, \( M(\mathcal{A}, \mathcal{A}) \) is a submodule of \( \mathbb{Z}^n \) over \( \mathbb{Z} \), and it has a finite \( \mathbb{Z} \)-basis with rank \( n \).

In the light of this property, we can state Problem PMT.

**Problem PMT in \((\mathcal{A}, \sigma)\) for \( G \).** Given a difference ring \((\mathcal{A}, \sigma)\) with \( G \leq \mathcal{A}^* \) such that \( \text{sconst}_G(\mathcal{A}) \setminus \{0\} \leq \mathcal{A}^* \); given \( f \in \mathbb{G}^{\mathcal{A}} \). Find a \( \mathbb{Z} \)-basis of \( M(f, \mathcal{A}) \).

Observe that Problem MT can be reduced to Problem PMT. Suppose that we are given a group \( G \) with \( \text{sconst}_G(\mathcal{A}) \setminus \{0\} \leq \mathcal{A}^* \) and \( \alpha \in G \). Moreover, assume that we have calculates \( \lambda = \text{ord}(\alpha) \) and succeeded in solving Problem PMT, i.e., we are given a basis of \( M = M((\alpha), \mathcal{A}) \subseteq \mathbb{N}^1 \). If the basis is empty, there cannot be an \( m \in \mathbb{N} \setminus \{0\} \) and a \( g \in \mathcal{A} \setminus \{0\} \) with (11). Otherwise, if the basis is not empty, the rank is 1. More precisely, we obtain \( m > 0 \) with \( M = m \mathbb{Z} \). Hence \( m \) is the smallest positive choice such that there is a \( g \in \mathcal{A} \setminus \{0\} \) with (11). Therefore we can again decide Problem MT.

For the generalization of Problems T and PT we introduce the following set. Let \( (\mathcal{A}, \sigma) \) be a difference ring with constant field \( \mathbb{K} \), let \( W \subseteq \mathcal{A} \), and let \( a \in \mathcal{A} \setminus \{0\} \) and \( f = (f_1, \ldots, f_n) \in \mathcal{A}^n \). Then we define

\[
V(a, f, (W, \sigma)) = \{ (c_1, \ldots, c_n, g) \in \mathbb{K}^n \times W | \sigma(g) = c_1 f_1 + \cdots + c_n f_n \};
\]

if it is clear from the context, we write \( V(a, f, W) \) and suppress the automorphism \( \sigma \). As Lemma 3 the following result will be crucial for further considerations.

---

2 If \( \lambda > 0 \) we have that \( \lambda \in M \), i.e., the rank of \( M \) is 1. In particular, we can construct an \( R \)-extension \((\mathcal{A}, \sigma) \leq (\mathcal{A}[t], \sigma) \) with \( \sigma(t) = \alpha t \) if \( \lambda = m > 0 \). Note that this observation also shows that Problem O can be reduced to Problem PMT. However, since we will need Problem O as a subproblem to solve Problem PMT below, it is natural to consider it as a problem of its own.
Lemma 4. Let \((A, \sigma)\) be a difference ring with constant field \(K\) and let \(G \leq A^*\) such that \(\text{sconst}_G A \setminus \{0\} \leq A^*\). Let \(V\) be a \(K\)-subspace of \(A\). Then for \(f \in A^n\) and \(a \in G\) we have that \(V(a, f, V)\) is a \(K\)-subspace of \(K^n \times V\) with \(\dim V(a, f, V) \leq n + 1\).

Proof. Suppose that there are \(m\) linearly independent solutions with \(m > n + 1\), say \((c_1, \ldots, c_{m}, g_i)\) with \(1 \leq i \leq m\). Then by row operations over the field \(K\) we can derive at least two linearly independent vectors, say \(v_1 = (0, \ldots, 0, g)\) and \(v_2 = (0, \ldots, 0, h)\). Hence we have that \(\sigma(g) = a g\) and \(\sigma(h) = a h\) where \(g, h \in \text{sconst}_G A \setminus \{0\} \leq A^*\).

Consequently, \(\sigma\left(\frac{g}{h}\right) = \frac{a g}{a h}\), thus \(c = g/h \in K^*\) and therefore \(v_1 = c v_2\); a contradiction that the vectors are linearly independent. \(\square\)

This result gives rise to the following problem specification.

**Problem PFLDE in \((A, \sigma)\) for \(G\) (with constant field \(K\)).** Given a difference ring \((A, \sigma)\) with constant field \(K\) and \(G \leq A^*\) such that \(\text{sconst}_G A \setminus \{0\} \leq A^*\); given \(a \in G\) and \(f \in A^n\). Find a \(K\)-basis of \(V(a, f, A)\).

In particular, if we can solve Problem PFLDE in \((A, \sigma)\) for \(G = \{1\}\), we can solve Problem T and PT in \((A, \sigma)\). Furthermore, we can solve the multiplicative version of telescoping: if \(a \in G\), we can determine \(g \in A \setminus \{0\}\), in case of existence, such that \(\sigma(g) = a g\) holds. This feature is illustrated by the following example.

Example 9 (Cont. Ex. 7). Given \(Q(b) = \prod_{k=1}^{b} \frac{-(k^2)}{k+1}\) on the left hand side of (7), we want to rewrite it in terms of the product \(P(b) = \prod_{j=1}^{b-1} \frac{(-j)}{j+1}\). In a preparation step we constructed already the RIIΣ*-extension \((\mathbb{K}(k)[x]\langle t \rangle, \sigma)\) of \((\mathbb{K}(k), \sigma)\) with \(\mathbb{K} = \mathbb{Q}(i)\), \(\sigma(x) = i x\) and \(\sigma(t) = k x t\) in Example 7. There we can represent \(\frac{-(k^2)}{k+1}\) with \(u = \frac{-x}{k+1}\) and \(P(k)\) with \(t\). Now we search for a \(g \in \mathbb{K}(k)[x]\langle t \rangle \setminus \{0\}\) such that \(\sigma(g) = u g\) holds. More precisely, we are interested in a basis of \(V = V(u, (0), \mathbb{K}(k)[x]\langle t \rangle)\). Observe that \(u \in G\) with \(G = (\mathbb{K}(k)^*)^{\mathbb{K}(k)[x]\langle t \rangle}\). Thus we are in the position to consider the corresponding Problem PFLDE in \((\mathbb{K}(k)[x]\langle t \rangle, \sigma)\) for \(G\). Activating our algorithms in Example 16 below, we get the basis \(\{(0, g), (1, 0)\}\) of \(V\) with \(g = \frac{z^{(i+1)} t^{-1}}{k+1}\). Since \(g\) is a solution of \(\sigma(g) = u g\), \(g(k) = \left(i + (-1)^k\right) \frac{z^k}{k+1} P(k)^{-1}\) is a solution of \(\frac{-(k^2)}{k+1} = g(k+1)\). Hence by the telescoping trick we get \(\prod_{k=1}^{b} \frac{-(k^2)}{k+1} = g(b+1)\) which produces (7).

2.3. The main results

Suppose that we are given a difference ring \((G, \sigma)\) which is computable and we are given a group \(G \leq G^*\) with \(\text{sconst}_G G \setminus \{0\} \leq G^*\). In this article we will restrict to certain classes of RIIΣ*-extensions \((\mathbb{E}, \sigma)\) of \((G, \sigma)\) equipped with a group \(G\) with \(G \leq \mathbb{E}^*\) and \(\text{sconst}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*\) such that we can derive the following algorithmic machinery:

1. Problem O in \(\hat{G}\) can be reduced to Problem O in \(G\);
2. Problems PMT and PFLDE in \((\mathbb{E}, \sigma)\) for \(\hat{G}\) can be reduced to Problem PMT in \((G, \sigma)\) for \(G\) and to the Problems PFLDE in \((G, \sigma^k)\) for \(G\) for all \(k \geq 1\).

In a nutshell, if we choose as base case a difference ring \((\mathbb{G}, \sigma)\) and a group \(G \leq G^*\) in which we can solve Problem O in \(G\) and Problems PMT and FFLDE in \((\mathbb{G}, \sigma)\) for \(G\), we obtain recursive algorithms that solve the corresponding problems in the larger difference ring \((\mathbb{E}, \sigma)\) and larger group \(\hat{G}\).
As it turns out, we will succeed in this task for a subclass of $R\Pi\Sigma^*$-extensions $(\mathbb{G}, \sigma) \leq (\mathbb{E}, \sigma)$ and a properly chosen group $\tilde{G} \leq \mathbb{E}^*$ that can treat all objects (among the general class of $R\Pi\Sigma^*$-extensions) that the author has encountered in practical problem solving so far. More precisely, we will restrict to simple $R\Pi\Sigma^*$-extensions.

Let $(\mathbb{G}(t_1) \ldots t_e), \sigma)$ be a $R\Pi\Sigma^*$-extension of $(\mathbb{G}, \sigma)$ and let $G \leq \mathbb{G}^*$. Then we define

$$G^e_G = \{ g t_{i_1}^{m_1} \ldots t_{i_s}^{m_s} | h \in \mathbb{G} \text{ and } m_i \in \mathbb{Z} \text{ where } m_i = 0 \text{ if } t_i \text{ is a } \Sigma^*-\text{monomial} \}.$$  \hfill (15)

It is easy to see that $\tilde{G} = G^e_G$ forms a group. More precisely, we obtain the following chain of subgroups: $G \leq G^e_G \leq \mathbb{E}^*$. We call $G^e_G$ also the product-group over $G$ for the $R\Pi\Sigma^*$-extension $(\mathbb{E}, \sigma)$ of $(\mathbb{G}, \sigma)$. We are now ready to define $(G)$-simple $R\Pi\Sigma^*$-extensions.

**Definition 4.** Let $(\mathbb{G}, \sigma)$ be a difference ring and let $G \leq \mathbb{G}^*$ be a group. An $R\Pi\Sigma^*$-extension $(\mathbb{E}, \sigma)$ of $(\mathbb{G}, \sigma)$ with $\mathbb{E} = \mathbb{G}(t_1)/t_2) \ldots (t_e)$ is called $G$-simple if for any $R\Pi\Sigma^*$-monomial $t_i$ we have that $\sigma(t_i)/t_i \in G_{\mathbb{E}}^e$. Moreover, an $R\Pi, R\Sigma^*, \Pi\Sigma^*, R-, \Pi-$, and $\Sigma^*$-extension of $(\mathbb{G}, \sigma)$ is $G$-simple if it is a simple $R\Pi\Sigma^*$-extension. We call any such extension simple if it is $\mathbb{G}^*$-simple. Analogously, we call an $R\Pi, R\Sigma^*, \Pi\Sigma^*, R-, \Pi-$, and $\Sigma^*$-monomial $G$-simple if the extension is $G$-simple.

So far, in all our examples the difference rings have been built by simple $R\Pi\Sigma^*$-extensions. Before we finally turn to the class of simple $R\Pi\Sigma^*$-extensions, we present one example which cannot be treated properly with our toolbox under consideration.

**Example 10.** Take $(\mathbb{Q}(k)(t), \sigma)$ from Example 2 with $\sigma(k) = k + 1$ and $\sigma(t) = (k + 1)t$. Then we can construct the $R$-extension $(\mathbb{Q}(k)(t)[x], \sigma)$ of $(\mathbb{Q}(k)(t), \sigma)$ with $\sigma(x) = -x$ of order 2. In this ring we are given the idempotent elements $e_1 = (x - 1)/2$ and $e_2 = (x + 1)/2$ with $e_1^2 = 1$ and $e_2^2 = 1$. Finally take $\alpha = e_1 + e_2 t$. Then observe that $\alpha \cdot (e_1 + e_2/t) = 1$, i.e., $\alpha \in \mathbb{Q}(k)(t)[x]^*$. Note that $\mathrm{ord}(\alpha) = 0$. Otherwise it would follow that $e_2^2 = 0$; a contradiction that $e_2$ is idempotent. Consequently $T$ cannot be an $R$-extension, and we construct the unimonomial extension $(\mathbb{Q}(k)(t)[x][T, \frac{1}{T}], \sigma)$ of $(\mathbb{Q}(k)(t)[x], \sigma)$ with $\sigma(T) = \alpha T$. We let it open if $T$ is a $\Pi$-monomial.

Summarizing, we aim at solving Problems PMT and PFLDE in a $G$-simple $R\Pi\Sigma^*$-extension $(\mathbb{G}, \sigma)$, and we want to solve Problem O in $\tilde{G}$. In order to accomplish this task, we will restrict ourselves further to the following two situations.

2.3.1. A solution for single-rooted $R\Pi\Sigma^*$-extensions

In most applications $R$-extensions are not nested, e.g., only objects like $(-1)^k$ arise. Moreover, such objects do not occur in transcendental products, but only in sums, like cyclotomic sums [3] or generalized harmonic sums [4]. A formal definition of this special, but very practical oriented class of $R\Pi\Sigma^*$-extensions is as follows.

**Definition 5.** An $R\Pi\Sigma^*$-extension $(\mathbb{E}, \sigma)$ of $(\mathbb{G}, \sigma)$ is called single-rooted if the generators of the extension can be reordered to

$$\mathbb{E} = \mathbb{G}(t_1) \ldots t_e(x_1) \ldots \langle x_u \rangle \langle s_1 \rangle \ldots \langle s_v \rangle,$$  \hfill (16)

respecting the recursive nature of the automorphism, such that the $t_i$ are $\Pi$-monomials, the $x_i$ are $R$-monomials with $\sigma(x_i)/x_i \in \mathbb{G}^*$ and the $s_i$ are $\Sigma^*$-monomials.

Given this class of single-rooted and simple $R\Pi\Sigma^*$-extension, we will show the following

\footnote{Note: If $\mathbb{G}$ is a field, any single-nested $R\Pi\Sigma^*$-extension is simple by Corollary 4.}
Theorem 2. Let \((G, \sigma)\) be a difference ring and \(G \leq G^*\) such that \(sconst_G G \setminus \{0\} \leq G^*\). Let \((E, \sigma)\) be a simple and single-rooted \(RI\Sigma^*\)-extension of \((G, \sigma)\) with (16) as specified in Definition 5, and let \(\tilde{G} = G^{\bigstar(\{t_i\})...\bigstar(\{t_i\})}\). Then \(sconst_E G \setminus \{0\} \leq E^*\) with 
\[
sconst_G E = \{ h t_1^{m_1} \cdots t_r^{m_r} x_1^{n_1} \cdots x_u^{n_u} \mid h \in sconst_G G, m_i \in \mathbb{Z} \text{ and } n_i \in \mathbb{N} \}.
\]

For its proof see page 24. In particular, we obtain the following reduction algorithm summarized in Theorem 3; for a proof of part 1 see page 32 and of part 2 see page 41.

Theorem 3. Let \((G, \sigma)\) be a computable difference ring and \(G \leq G^*\) with \(sconst_G G \setminus \{0\} \leq G^*\). Let \((E, \sigma)\) be a simple-rooted and \(G\)-simple \(RI\Sigma^*\)-extension of \((G, \sigma)\) with (16) as given in Definition 5, and let \(\tilde{G} = G^{\bigstar(\{t_i\})...\bigstar(\{t_i\})}\). Then the following holds.

1. Problem PMT is solvable in \((E, \sigma)\) for \(\tilde{G}\) if it is solvable in \((G, \sigma)\) for \(G\).
2. Problem PFLDE is solvable in \((E, \sigma)\) for \(\tilde{G}\) if Problem PFLDE and PMT are solvable in \((G, \sigma)\) for \(G\) and \((F, \sigma)\) for \(F\).

All the calculations in [44,39,50,33,11,2] rely precisely on this machinery.

2.3.2. A solution for \(RI\Sigma^*\)-extensions of a strong constant-stable difference field

In the following we restrict to \(RI\Sigma^*\)-extensions where the ground domain \(G = F\) is a field. In this setting, we will show that the semi-constants form a multiplicative group.

Theorem 4. Let \((E, \sigma)\) be a simple \(RI\Sigma^*\)-extension of a difference field \((F, \sigma)\) and consider its product-group \(\tilde{G} = (F^*)^{\bigstar}_F\). Then \(sconst_G E \setminus \{0\} \leq E^*\).

For a proof of this theorem we refer to page 26. In order to solve Problems PMT and PFLDE we require in addition that \((F, \sigma)\) is strong constant-stable.

Definition 6. A difference ring \((A, \sigma)\) with constant field \(K\) is called constant-stable if for all \(k > 0\) we have that \(const(A, \sigma^k) = K\). It is called strong constant-stable if it is constant-stable and any root of unity of \(A\) is in \(K\).

This means that we can treat products over roots of unity from \(K\) and, more generally, products that are built recursively over such products; for examples see (4) and for further (algorithmic) properties see Corollary 5 below. Given such a tower of \(RI\Sigma^*\)-extensions, we can solve Problems PMT and PFLDE as follows; for the proofs, resp. the underlying algorithms, of part 1 see page 29, of part 2 see page 35 and of part 3 see page 44.

Theorem 5. Let \((F, \sigma)\) be a computable difference field where Problem O is solvable in \((const F)^*\). Let \((E, \sigma)\) be a simple \(RI\Sigma^*\)-extension of \((F, \sigma)\). Then

1. Problem O is solvable in \((F^*)^{\bigstar}_F\).

   If \((F, \sigma)\) is in addition strong constant-stable, then

2. Problem PMT is solvable in \((E, \sigma)\) for \((F^*)^{\bigstar}_F\) if it is solvable in \((F, \sigma)\) for \(F^*\); 

3. Problem PFLDE is solvable in \((E, \sigma)\) for \((F^*)^{\bigstar}_F\) if Problem PMT is solvable in \((F, \sigma)\) for \(F^*\) and Problem PFLDE is solvable in \((F, \sigma^k)\) for \(F^*\) for all \(k > 0\).

We remark that the underlying machinery of this theorem has been utilized in Examples 8 and 9 to obtain the identities (6) and (7), respectively. Further details will be given below.
2.3.3. A complete machinery: algorithms for the ground difference rings

Both, Theorem 3 and Theorem 5 provide algorithms to reduce Problem PMT and PFLDE (and thus Problems MT, PT and T) from an \( R_{\Pi\Sigma^*} \)-extension \((E, \sigma)\) of \((G, \sigma)\) to the ground difference ring \((G, \sigma)\). Theorem 3 requires less conditions on \((G, \sigma)\), but considers only single–rooted \( R_{\Pi\Sigma^*} \)-extensions, whereas Theorem 5 requires more properties on \((G, \sigma)\) but allows nested \( R \)-extensions which are of the type as given in Corollary 5. Note that the algorithms for the latter case are more demanding, in particular, one has to solve Problem PFLDE in \((G, \sigma^k)\) with \( k > 0 \) instead of \( k = 1 \) only.

We emphasize that both theorems are applicable for a rather general class of difference fields \((G, \sigma)\). Namely, \((G, \sigma)\) itself can be a \( \Pi\Sigma^* \)-field extension of \((H, \sigma)\) where certain properties in the difference field \((H, \sigma)\) hold. Here the following remarks are in place.

(a) By [24] a \( \Pi\Sigma^* \)-field extension \((G, \sigma)\) of \((H, \sigma)\) is constant-stable if \((H, \sigma)\) is constant-stable. In particular, if we are given a root of unity from \( G \), it cannot depend on transcendental elements and is therefore from \( H \). Thus \((G, \sigma)\) is strong constant-stable if \((H, \sigma)\) is constant-stable.

(b) It has been shown in [28] that one can solve Problem PMT in \((G, \sigma)\) for \( G^* \) and Problem PFLDE in \((G, \sigma^k)\) for \( G^* \) for \( k > 0 \) if certain properties hold for the difference field \((H, \sigma)\). Among others (see Def. 1 and 2 in [28]) Problem PMT must be solvable in \((H, \sigma)\) for \( H^* \) and Problem PFLDE must be solvable in \((H, \sigma^k)\) for \( H^* \).

Summarizing, if we are given the tower of extensions
\[
(H, \sigma) \xrightarrow{\Pi\Sigma^*\text{-field ext.}} (G, \sigma) \xrightarrow{R_{\Pi\Sigma^*}\text{-ring ext.}} (E, \sigma)
\]
where \((H, \sigma)\) is strong constant-stable and the properties given in Def. 1 and 2 of [28] hold in \((H, \sigma)\), then we can solve Problems PMT and PFLDE in \((E, \sigma)\) for \((G^*)_E^G\).

So far, the required properties have been verified and the necessary algorithms have been worked out for the following difference fields \((H, \sigma)\) with constant field \( K \).

(1) \( K = \mathbb{H} \), i.e., \((G, \sigma)\) is a \( \Pi\Sigma^* \)-field over \( K \); here \( K \) can be a rational function field over an algebraic number field; see [48].

(2) \((H, \sigma)\) is a free difference field, i.e., \( H = \mathbb{K}(\ldots, x_{-1}, x_0, x_1, \ldots) \) with \( \sigma(x_i) = x_{i+1} \);

here \( K \) is of the type as given in item 1. Note that in this field one can model unspecified sequences; see [28,27].

(3) \((H, \sigma)\) can be a radical difference field representing objects like \( \sqrt[k]{K} \); see [29].

For simplicity, all our examples are chosen from case (1). More precisely, we always take the \( \Pi\Sigma^* \)-field \((H, \sigma) = (\mathbb{K}(k), \sigma)\) over \( K \in \{\mathbb{Q}, \mathbb{Q}(i)\} \) with \( \sigma(k) = k + 1 \).

2.4. Application: representation of d’Alembertian solutions in \( R_{\Pi\Sigma^*} \)-extensions

We illustrate how an important class of d’Alembertian solutions [7], a subclass of Liouvillian solutions [20,38], of a given linear difference operator, can be represented completely automatically in \( R_{\Pi\Sigma^*} \)-extensions. In order to obtain d’Alembertian solutions one starts as follows: first the linear difference operator is factored as much as possible into linear right hand factors. This can be accomplished, e.g., with the algorithms [36,21,22] or, within the setting of \( \Pi\Sigma^* \)-fields with the algorithms given in [6] which are based on [14,42,49]. The latter machinery is available within the summation package Sigma. Then given this factored form of the operator, the d’Alembertian solutions can be read
off. They can be given by a finite number of hypergeometric expressions and indefinite nested sums defined over such expressions. More precisely, each solution is of the form

$$\sum_{i_1=\lambda_1}^{k} h_1(i_1) \sum_{i_2=\lambda_2}^{i_1} h_2(i_2) \cdots \sum_{i_{r-1}=\lambda_{r-1}}^{i_r} h_r(i_r)$$

(17)

where $\lambda_i \in \mathbb{N}$ and the hypergeometric expression $h_i(k)$ can be written in the form $\prod_{j=\lambda_i}^{k} \alpha_i(j)$ with $\alpha_i(z)$ being a rational function from $\mathbb{K}(z)$.

Subsequently, we restrict ourselves to a field $\mathbb{K}$ which is a rational function field $\mathbb{K} = \mathbb{Q}(n_1, \ldots, n_r)$ over the rational numbers. Now take the $\Pi\Sigma^*$-field $(\mathbb{K}(k), \sigma)$ over $\mathbb{K}$ with $\sigma(k) = k + 1$. Then the solutions, all being of the form (17), can be represented in a single-rooted simple $\Pi\Sigma^*$-extension as follows.

1. In [48] an algorithm has been presented that calculates a single-rooted simple $\Pi\Sigma^*$-extension $(\mathbb{G}, \sigma)$ of $(\mathbb{K}(k), \sigma)$ in which all hypergeometric expressions occurring in the d’Alembertian solutions are explicitly represented.

2. Then the challenging task is to construct a $\Sigma^*$-extension of $(\mathbb{G}, \sigma)$ and to represent there the arising sums of the d’Alembertian solutions. Given $(\mathbb{G}, \sigma)$ from step 1, this can be accomplished by applying iteratively Theorem 1.1. Suppose we represented already an inner summand in a $\Sigma^*$-extension $(\mathbb{A}, \sigma)$ of $(\mathbb{G}, \sigma)$ with $\beta \in \mathbb{A}$. Since $(\mathbb{A}, \sigma)$ is a simple $\Pi\Sigma^*$-extension of $(\mathbb{K}(k), \sigma)$ and $(\mathbb{K}(k), \sigma)$ is a $\Pi\Sigma$-field over $\mathbb{K}$, we can solve Problem $T$ with $f = \beta$ by using the underlying algorithm of Theorem 3 in combination with the base case algorithms; see Subsection 2.3.3. If we find a $g \in \mathbb{A}$ with $\sigma(g) = g + \beta$, we can represent the sum under consideration with $g + c$ where $c \in \mathbb{K}$ is determined by the boundary condition (lower summation bound) of the given sum; for further details we refer to Example 8.4. Otherwise, we construct the $\Sigma^*$-extension $(\mathbb{A}[t], \sigma)$ of $(\mathbb{A}, \sigma)$ with $\sigma(t) = t + \beta$ by Theorem 1.1. In total we are given again a single-rooted simple $\Pi\Sigma^*$-extension of $(\mathbb{K}(k), \sigma)$. Proceeding iteratively, all nested sums over the hypergeometric terms can be expressed in such an $\Pi\Sigma^*$-extension over $(\mathbb{K}(k), \sigma)$.

Exactly this difference ring machinery is implemented in $\text{Sigma}$ and has been used to tackle challenging applications, like [44,39,50,33,11,2,1] mentioned already in the introduction. In particular, this toolbox has been combined with the algorithms worked out in [45,48,51,53,8,58] in order to find representations of d’Alembertian solutions with certain optimality properties, like minimal nesting depth. For a recent summary of all these features (unfortunately, in the setting of difference fields) we refer to [57,59].

3. Single nested $\Pi\Sigma^*$-extensions

This section delivers relevant properties of single $\Pi\Sigma^*$-extensions. First, Theorem 1 will be proved. In addition, properties of the set of semi-constants of $\Pi\Sigma^*$-extensions are derived to gain further insight in the nature of $\Pi\Sigma^*$-extensions and to prove Theorems 2 and 4 in Section 4.

We start with some general properties in ring theory. A ring $\mathbb{A}$ is called reduced if there are no non-zero nilpotent elements, i.e., for any $f \in \mathbb{A} \setminus \{0\}$ and any $n > 0$ we have that $f^n \neq 0$. Moreover, a ring is called connected if $0$ and $1$ are the only idempotent elements, i.e., for any $f \in \mathbb{A} \setminus \{0, 1\}$ we have that $f^2 \neq f$. Then we rely on the following properties in rings. A polynomial $\sum_{i=0}^{n} a_i x^i \in \mathbb{A}[t]$ with coefficients from a ring $\mathbb{A}$ is invertible if and only if $a_0 \in \mathbb{A}^*$ and $a_i$ with $i \geq 1$ are nilpotent elements. Thus in a reduced ring, i.e., a
ring which has no nilpotent non-zero elements, we have that \( A[t]^* = A^* \). Moreover, there is a complete characterization of invertible elements in the ring of Laurent polynomials \( A[t, \frac{1}{t}] \) presented in [23, Theorem 1] (see also [32]). Based on this work we extract

**Lemma 5.** Let \( A \) be a commutative ring with 1. If \( A \) is reduced, then \( A[t]^* = A^* \). If \( A \) is reduced and connected, then \( A[t, \frac{1}{t}]^* = \{u t^r | u \in A^* \text{ and } r \in \mathbb{Z} \} \).

Since the rings are usually not connected, Lemma 5 can be applied only partially.

**Example 11.** The generators in the ring given in Example 10 can be reordered to \( \mathbb{Q}(k)[x](t) \). Since \( \mathbb{Q}(k)[x] \) has the idempotent elements \( e_1, e_2 \), it is not connected. Therefore, we get relations such as \( (e_1 + e_2) t(e_1 + e_2) \) which are predicted in [23,32].

Subsequently, we enumerate further definitions and properties in difference rings and fields that will be used throughout the article. Let \((A, \sigma)\) be a difference ring. The rising factorial (or \( \sigma \)-factorial) of \( f \in A^* \) to \( k \in \mathbb{Z} \) is defined by

\[
f_{(k, \sigma)}(f) = \begin{cases} f \sigma(f) \ldots \sigma^{k-1}(f) & \text{if } k > 0 \\ 1 & \text{if } k = 0 \\ \sigma^{-1}(f^{-1}) \sigma^{-2}(f^{-1}) \ldots \sigma^{k}(f^{-1}) & \text{if } k < 0. \end{cases}
\]

If the automorphism is clear from the context, we also will write \( f_{(k)} \) instead of \( f_{(k, \sigma)} \). We will rely on the following simple identities (compare also [25, page 307]). The proofs are omitted to the reader.

**Lemma 6.** Let \((A, \sigma)\) be a difference ring, \( f, h \in A^* \) and \( n, m \in \mathbb{Z} \). Then:

1. \((f h)_{(n)} = f_{(n)} h_{(n)}\).
2. \(f_{(n+m)} = \sigma^n(f_{(m)}) f_{(n)}\).
3. \(f_{(n m)} = (f_{(n, \sigma)})_{(m, \sigma^n)}\).
4. If \( \sigma(h) = f h \), then \( \sigma^n(h) = f_{(n)} h \).
5. \( \sigma^k(f) \in A^* \) and \( f_{(n)} \in A^* \).

Let \( A[t] \) be a ring of (Laurent) polynomials. For \( f = \sum_i f_i t^i \in A[t] \) we define

\[
\deg(f) = \begin{cases} \max \{i | f_i \neq 0\} & \text{if } f \neq 0 \\ -\infty & \text{if } f = 0 \end{cases}
\]

and \( \deg(f) = \begin{cases} \min \{i | f_i \neq 0\} & \text{if } f \neq 0 \\ \infty & \text{if } f = 0. \end{cases} \)

In addition, for \( a, b \in \mathbb{Z} \) we introduce the set of truncated (Laurent) polynomials by

\[
A[t]_{a,b} = \left\{ \sum_{i=a}^{b} f_i t^i | f_i \in A \right\}.
\]

We conclude this section with the following two lemmas.

**Lemma 7.** Let \((A[t], \sigma)\) be a unimonomial ring extension of \((A, \sigma)\) of (Laurent) polynomial type. Then for any \( k \in \mathbb{Z} \) and \( f \in A[t] \) we have that \( \deg(\sigma^k(f)) = \deg(f) \).

**Proof.** Let \( f = \sum_i f_i t^i \). If \( f = 0 \), \( \sigma^k(f) = 0 \) and thus with \( \deg(0) = -\infty \) the statement holds. Otherwise, let \( m := \deg(f) \in \mathbb{Z} \). Then note that \( \sigma^k(f) = \sum_i \sigma^k(f_i)(\alpha^i t^i + \beta) \), i.e., \( t^m \) is the largest possible monomial in \( \sigma^k(f) \) with the coefficient \( \alpha_{(k)} \sigma(f_m) \). Since \( \alpha_{(k)} \in A^* \) by Lemma 6.5, the coefficient is non-zero. \( \square \)
Lemma 8. Let \((F(t, \sigma)\) be a unimonomial field extension of \((F, \sigma)\), and let \(p, q \in F[t]^*\) with \(\gcd(p, q) = 1\) and \(k \in \mathbb{Z}\). Then the following holds.

1. If \(p \mid q\) then \(\sigma^k(p) \mid \sigma^k(q)\).
2. \(\gcd(\sigma^k(p), \sigma^k(q)) = 1\).
3. \(\frac{\sigma(p/q)}{p/q} \in F\) if and only if \(\sigma(p)/p \in F\) and \(\sigma(q)/q \in F\).

Proof. (1) If \(p \mid q\), i.e., \(p \cdot w = q\) for some \(w \in F[t] \setminus \{0\}\), then \(\sigma^k(p) = \sigma^k(w) \sigma^k(q)\), and thus \(\sigma^k(p) \mid \sigma^k(q)\).

(2) Suppose that \(1 \neq \gcd(\sigma^k(p), \sigma^k(q)) =: u \in F[t] \setminus F\). Then \(\sigma^{-k}(u) \in F[t] \setminus F\). Since \(\sigma^{-k}(u) \mid p\) and \(\sigma^{-k}(u) \mid q\) by part (1) of the lemma, \(\gcd(p, q) \neq 1\), a contradiction to the assumption.

(3) The implication \(\Leftarrow\) is immediate. Suppose that \(u := \sigma(p/q)/(p/q) \in F\), i.e., \(\sigma(p)q = up \sigma(q)\). By part 2 of the lemma, \(\sigma(p) \mid p\) and \(p \mid \sigma(p)\) which implies that \(\sigma(p)/p \in F\). Analogously, it follows that \(\sigma(q)/q \in F\). □

3.1. \(\Sigma^*\)-extensions

The essence of all the properties of \(\Sigma^*\)-extensions is contained in the following lemma.

Lemma 9. Let \((\mathbb{A}, \sigma)\) be a difference ring and \(G \leq \mathbb{A}^*\) such that \(\text{const}_{G}\mathbb{A} \setminus \{0\} \leq \mathbb{A}^*\).

Let \((\mathbb{A}[t], \sigma)\) be a unimonomial ring extension of \((\mathbb{A}, \sigma)\) with \(\sigma(t) = t + \beta\) for some \(\beta \in \mathbb{A}\). If there are \(u \in G\) and \(g \in \mathbb{A}[t]\) with \(\deg(g) \geq 1\) such that

\[
\deg(\sigma(g) - ug) < \deg(g) - 1,
\]

then there is a \(\gamma \in \mathbb{A}\) with \(\sigma(\gamma) - \gamma = \beta\).

Proof. Let \(g = \sum_{i=0}^{n} g_it^i \in \mathbb{A}[t]\) with \(\deg(g) = n \geq 1\) and \(u \in G\) as stated in the lemma, and define \(f = \sigma(g) - ug \in \mathbb{A}[t]\). With (19) it follows that \(f = \sum_{i=0}^{n-2} f_it^i\).

Thus comparing the \(n\)th and \((n - 1)\)th coefficient in \(\sum_{i=0}^{n-2} f_it^i = f = \sigma(g) - ug = \sum_{i=0}^{n} \sigma(g_i)(t + \beta)^i - u \sum_{i=0}^{n} g_it^i\) and using \((t + \beta)^i = \sum_{j=0}^{i} \binom{i}{j} t^{i-j} \beta^j\) for \(0 \leq i \leq n\) yield

\[
\sigma(g_n) - ug_n = 0,
\]

\[
\sigma(g_{n-1}) + \sigma(g_n)(\binom{n}{1})\beta - ug_{n-1} = 0.
\]

The first equation shows that \(g_n \in \text{const}_{G}\mathbb{A} \setminus \{0\} \leq \mathbb{A}^*\). Hence we get \(u = \sigma(g_n)/g_n\).

Replacing \(u\) by this relation into the second equation gives

\[
\sigma(g_{n-1}) - \frac{\sigma(g_n)}{g_n} g_{n-1} = -n\beta^n\sigma(g_n).
\]

Dividing this equation by \(-n\sigma(g_n)\) in \(\mathbb{A}^*\) yields \(\sigma(\gamma) - \gamma = \beta\) with \(\gamma := \frac{-g_{n-1}}{ng_n} \in \mathbb{A}\). □

Lemma 9 leads to the following equivalent properties of \(\Sigma^*\)-extensions.

Lemma 10. Let \((\mathbb{A}, \sigma)\) be a difference ring and \(G \leq \mathbb{A}^*\) such that \(\text{const}_{G}\mathbb{A} \setminus \{0\} \leq \mathbb{A}^*\).

Let \((\mathbb{A}[t], \sigma)\) be a unimonomial ring extension of \((\mathbb{A}, \sigma)\) with \(\sigma(t) = t + \beta\) for some \(\beta \in \mathbb{A}\). Then the following statements are equivalent.

1. There is a \(g \in \mathbb{A}[t] \setminus \mathbb{A}\) and \(u \in G\) with \(\sigma(g) = ug\).
2. There is a \(g \in \mathbb{A}\) with \(\sigma(g) = g + \beta\).
3. \(\text{const}\mathbb{A}[t] \geq \text{const}\mathbb{A}\).

Proof. (1) \(\Rightarrow\) (2): Let \(g \in \mathbb{A}[t] \setminus \mathbb{A}\), \(u \in G\) with \(\sigma(g) = ug\). Since \(\deg(g) \geq 1\) and \(\deg(\sigma(g) - g) = \deg(0) = -\infty \leq \deg(\sigma(g) - g) - 1\), there is a \(\gamma \in \mathbb{A}\) with \(\sigma(\gamma) = \gamma + \beta\) by Lemma 9.

(2) \(\Rightarrow\) (3): Let \(g \in \mathbb{A}\) with \(\sigma(g) = g + \beta\). Since \(\sigma(t) = t + \beta\), it follows that \(\sigma(t - g) = (t - g)\),
i.e., \( t - g \in \text{const}\, A[t] \). Since \( t - g \notin A \), \( t - g \notin \text{const}\, A \).

3 \implies 1: Suppose that \( \text{const}\, A \subseteq \text{const}\, A[t] \) and take \( g \in \text{const}\, A[t]\setminus\text{const}\, A \). Then \( \sigma(g) = u g \) with \( u = 1 \in G \). Thus the lemma is proven. \( \square \)

As a consequence we can now establish the first part of our characterisation theorem.

**Proof of Theorem 1.1** (see page 7). For \( G = \{1\} \) we have that \( \text{sconst}_G A = \text{const}\, A = K \). By assumption \( K \) is a field and thus \( \text{sconst}_G A \setminus \{0\} \leq A^* \). Therefore we can apply Lemma 10 and with its equivalence (2) \( \iff \) (3) the theorem follows. \( \square \)

In order to rediscover the difference field version from [24,25], we specialize Lemma 10 to difference fields by exploiting Lemma 8.3.

**Lemma 11.** [24,25] Let \((F, \sigma)\) be a unimonomial field extension of \((F, \sigma)\) with \( \sigma(t) = t + \beta \) for some \( \beta \in F \). Then the following statements are equivalent.

1. There is a \( g \in F(t) \setminus F \) with \( \frac{\sigma(g)}{g} \in F \).
2. There is a \( g \in F \) with \( \sigma(g) = g + \beta \).
3. \( \text{const}\, F(t) \geq \text{const}\, F \).

**Proof.** 1 \( \implies \) 2: Let \( g \in F(t) \setminus F \) with \( \sigma(g)/g \in F \). Write \( g = \frac{\sigma(a)}{a} \) with \( p, q \in F[t]^* \) and \( \gcd(p, q) = 1 \). By Lemma 8, \( \sigma(p)/p \in F \) and \( \sigma(q)/q \in F \). Since \( g \notin F \), we have that \( p \notin F \) or \( q \notin F \). Thus there is a \( g' \in F[t] \) with \( \deg(g') \geq 1 \) and \( \deg(\sigma(g') - g') = \deg(0) = -\infty < 0 \leq \deg(g') - 1 \). Hence by Lemma 9 there is a \( \gamma \in F \) with \( \sigma(\gamma) = \gamma + \beta \).

2 \( \implies \) 3 follows by Lemma 10. 3 \( \implies \) 1 is analogous to the proof of Lemma 10. \( \square \)

**Theorem 6** ([24,25]). Let \((F(t), \sigma)\) be a unimonomial field extension of \((F, \sigma)\) with \( \sigma(t) = t + \beta \) for some \( \beta \in F \). Then this is a \( \Sigma^* \)-extension (i.e., \( \text{const}\, F(t) = \text{const}\, F \)) iff there is no \( g \in F \) with \( \sigma(g) = g + \beta \).

Finally, by the equivalence (3) \( \iff \) (1) of Lemma 10 we obtain the following result concerning the semi-constants.

**Theorem 7.** Let \((A, \sigma)\) be a difference ring and \( G \leq A^* \) such that \( \text{sconst}_G A \setminus \{0\} \leq A^* \). If \((A[t], \sigma)\) is a \( \Sigma^* \)-extension of \((A, \sigma)\), then \( \text{sconst}_G A[t] = \text{sconst}_G A \).

If we specialize to \( G = A[t]^* \) and assume that \( A \) is reduced, we get Theorem 8. For the proof we use in addition the following lemma.

**Lemma 12.** Let \((A, \sigma)\) be a difference ring. \( \text{const}\, A \setminus \{0\} \leq A^* \) iff \( \text{const}\, A \setminus \{0\} = A^* \).

**Proof.** Suppose that \( \text{const}\, A \setminus \{0\} \leq A^* \). If \( a \in A^* \), then \( \sigma(a) \in A^* \) by Lemma 7. Thus \( u := \frac{\sigma(a)}{a} \in A^* \). With \( \sigma(a) = u a \) it follows that \( a \in \text{const}\, A \). This proves that \( \text{const}\, A \setminus \{0\} = A^* \). The other direction is immediate. \( \square \)

**Theorem 8.** Let \((A[t], \sigma)\) be a \( \Sigma^* \)-extension of \((A, \sigma)\) where \( A \) is reduced and \( \text{sconst}\, A \setminus \{0\} \leq A^* \). Then \( \text{sconst}\, A[t] \setminus \{0\} = \text{sconst}\, A \setminus \{0\} = A^* \).

**Proof.** By Lemma 12 it follows that \( \text{sconst}\, A \setminus \{0\} = A^* \). Since \( A \) is reduced, \( A[t]^* = A^* \) by Lemma 5 and thus \( \text{sconst}\, A[t] = \text{sconst}\, A[t][t] = \text{sconst}\, A \cdot A[t] \). Now take \( G = A^* \) and apply Theorem 7. Hence \( \text{sconst}_{A^*} A[t] = \text{sconst}_{A^*} A = \text{sconst}\, A \). \( \square \)
3.2. Π-extensions

Analogously to Lemma 9 we obtain by coefficient comparison

Lemma 13. Let \((\mathbb{A}[t, \frac{1}{t}], \sigma)\) be a unimonomial ring extension of \((\mathbb{A}, \sigma)\) with \(\alpha = \frac{\sigma(t)}{t} \in \mathbb{A}^*\); let \(u \in \mathbb{A}\) and \(g = \sum_{i=0}^n g_i t^i \in \mathbb{A}[t, \frac{1}{t}]\). If \(\sigma(g) = u g\), then \(\sigma(g_i) = u \alpha^{-i} g_i\) for all \(i\).

Proof of Theorem 1.2 (see page 7). “⇐” Let \(m \in \mathbb{Z} \setminus \{0\}\) and \(g \in \mathbb{A} \setminus \{0\}\) such that \(\sigma(g) = \alpha^m g\). Since \(\sigma(t^m) = \alpha^m t^m\), it follows that \(\sigma(g/t^m) = g/t^m\), i.e., \(g/t^m \in \text{const} \mathbb{A}[t, \frac{1}{t}]\). Clearly \(g/t^m \notin \mathbb{A}\) which implies that \(g/t^m \notin \text{const} \mathbb{A}\).

“⇒” Let \(g = \sum_i g_i t^i \in \mathbb{A}[t, \frac{1}{t}] \setminus \mathbb{A}\) such that \(\sigma(g) = g\). Thus \(g_m \neq 0\) for some \(m \neq 0\). By Lemma 13 we have that \(\sigma(g_m) = \alpha^{-m} g_m\). Suppose that \(t\) is a Π-ring, but \(\text{ord}(\alpha) = n > 0\). Then \(\sigma(t^n) = \alpha^n t^n = t^n\), which is a contradiction to the first part of the statement. \(\square\)

Requiring in addition that the semi-constants form a group, this result can be sharpened.

Theorem 9. Let \((\mathbb{A}, \sigma)\) be a difference ring and \(G \leq \mathbb{A}^*\) such that \(\text{scost}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*\). Let \((\mathbb{A}[t, \frac{1}{t}], \sigma)\) be a unimonomial ring extension of \((\mathbb{A}, \sigma)\) with \(\sigma(t) = \alpha t\) for some \(\alpha \in G\). Then this is a Π-extension iff there are no \(g \in \text{scost}_G \mathbb{A} \setminus \{0\}\) and \(m > 0\) with \(\sigma(g) = \alpha^m g\).

Proof. \(\Rightarrow\): Suppose that \(t\) is not a Π-monomial. Then we can take \(g \in \mathbb{A} \setminus \{0\}\) and \(m \in \mathbb{Z} \setminus \{0\}\) with \(\sigma(g) = \alpha^m g\). Hence \(g \in \text{scost}_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*\). Thus if \(m < 0\), we get \(\sigma(g) = \alpha^{-m} \tilde{g}\) with \(\tilde{g} = \frac{1}{\tilde{\alpha}} \in \mathbb{A}^*\). The other direction is immediate by Theorem 1.2. \(\square\)

Together with Lemma 8 we rediscover Karr’s characterization of Π-field extensions.

Theorem 10 ([24, 25]). Let \((\mathcal{F}(t), \sigma)\) be a unimonomial difference extension of \((\mathbb{F}, \sigma)\) with \(\sigma(t) = \alpha t\) for some \(\alpha \in \mathbb{F}^*\). Then this is a Π-extension iff there are no \(g \in \mathbb{F}^*\) and \(m > 0\) with \(\sigma(g) = \alpha^m g\).

Proof. The direction from right to left follows by Theorem 1.2 and the fact that any Π-field extension is a Π-ring extension. Now let \(g \in \mathcal{F}(t) \setminus \mathbb{F}\) with \(\sigma(g) = g\). Write \(g = p/q\) with \(p, q \in \mathcal{F}(t)\) where \(\gcd(p, q) = 1\) and \(q\) is monic. W.l.o.g. suppose that \(\deg(q) \geq \deg(p)\) (otherwise take \(1/g\) instead of \(g\)). By Lemma 8,

\[
\sigma(p)/p \in \mathbb{F} \quad \text{and} \quad \sigma(q)/q \in \mathbb{F}.
\]

We consider two cases. First suppose that \(p \in \mathbb{F}^*\) and \(q = t^m\) with \(m > 0\). Then \(\frac{p}{t^m} = g = \sigma(g) = \frac{\alpha^m p}{\alpha^m t^m}\) which implies that \(\sigma(p) = \alpha^m p\). What remains to consider is the case that \(p \notin \mathbb{F}\) or \(q \neq t^m\) for some \(m > 0\). Define

\[
a := \begin{cases} 
  p & \text{if } q = t^m \text{ for some } m > 0, \\
  q & \text{otherwise.}
\end{cases}
\]

The following holds.

1. \(a \in \mathbb{F}[t] \setminus \mathbb{F}\): If \(a = q\), note that \(q \notin \mathbb{F}\) by \(\deg(p) \leq \deg(q)\) and \(p/q \notin \mathbb{F}\); if \(a = p\), \(q = t^m\) and hence \(p \notin \mathbb{F}\) by the assumption of our second case.

2. \(u := \sigma(a)/a \in \mathbb{F}^*\) by (20).

3. \(a \neq u t^m\) for all \(u \in \mathbb{F}^*\) and \(m > 0\); \(a\) could be only of this form, if \(q = t^m\) for some \(m > 0\), but since \(\gcd(p, q) = 1\), \(t \nmid p\).
By properties (1) and (3), it follows that $a = \sum_{i=k}^n a_i t^i$ with $a_k \neq 0 \neq a_n$ where $n > k \geq 0$. With property (2) and Lemma 13 it follows that $\sigma(a_k) = \frac{1}{\alpha^k} a_k$ and $\sigma(a_n) = \frac{1}{\alpha^n} a_n$ which implies $\sigma\left(\frac{a_k}{a_n}\right) = \alpha^{n-k} \frac{a_k}{a_n}$. Since $\frac{a_k}{a_n} \in \mathbb{F}^*$ and $n-k > 0$, the theorem is proven. \hfill $\Box$

Finally, we characterize the set of semi-constants for II-extensions.

**Theorem 11.** Let $(A, \sigma)$ be a difference ring and $G \subseteq A^*$ such that $\text{sconst}_G A \setminus \{0\} \subseteq A^*$. Let $(A[t, \frac{1}{t}], \sigma)$ be II-extension of $(A, \sigma)$ with $\sigma(t) = \alpha t$ for some $\alpha \in G$. Then we have that $\text{sconst}_G A[t, \frac{1}{t}] = \{h t^m | h \in \text{sconst}_G A \text{ and } m \in \mathbb{Z}\}$ and $\text{sconst}_G A[t, \frac{1}{t}] \setminus \{0\} \subseteq A[t, \frac{1}{t}]^*$.

**Proof.** “$\subseteq$”: Let $g \in \text{sconst}_G A[t, \frac{1}{t}]$, i.e., $g = \sum_i g_i t^i \in A[t, \frac{1}{t}]$ with $\sigma(g) = u g$ for some $u \in G$. By Lemma 13 we get $\sigma(g_i) = u g_i$ and thus $\sigma(g) = \frac{u}{\alpha^i} g_i$. Now suppose that there are $r, s \in \mathbb{Z}$ with $s > r$ and $g_r \neq 0 \neq g_s$. As $\frac{u}{\alpha^i} \in G$, it follows that $g_s \in \text{sconst}_G A \setminus \{0\} \subseteq A^*$. Thus we conclude that $\sigma\left(\frac{u}{\alpha^i} \right) = \alpha^{s-r} \frac{u}{\alpha^i} g_i$ with $s-r > 0$; a contradiction to Theorem 1.2. Hence $g = h t^m$ for some $h \in \text{sconst}_G A \text{ and } m \in \mathbb{Z}$.

“$\supseteq$”: Let $g = h t^m$ with $h \in \text{sconst}_G A$, $m \in \mathbb{Z}$. Then there is a $u \in G$ with $\sigma(h) = u h$. Hence $\sigma(g) = (uh) \alpha^m t^m = u \alpha^m h t^m = u \alpha^m g$ with $u \alpha^m \in G$. Thus $g \in \text{sconst}_G A[t, \frac{1}{t}]$. Summarizing, we proved equality which implies that $\text{sconst}_G A[t, \frac{1}{t}] \setminus \{0\} \subseteq A[t, \frac{1}{t}]^*$. \hfill $\Box$

So far we obtained a description of the semi-constants for a subgroup $G$ of $A^*$. Now we will lift this result to the group $\tilde{G} = G_{\tilde{A}} = \{h t^m | h \in G \text{ and } m \in \mathbb{Z}\} \subseteq A\{t\}^*$.

**Theorem 12.** Let $(A, \sigma)$ be a difference ring and $G \subseteq A^*$ such that $\text{sconst}_G A \setminus \{0\} \subseteq A^*$. Let $(A[t, \frac{1}{t}], \sigma)$ be II-extension of $(A, \sigma)$ with $\sigma(t) = \alpha t$ for some $\alpha \in G$ and let $\tilde{G} = G_{\tilde{A}}$. Then $\text{sconst}_G A[t, \frac{1}{t}] = \text{sconst}_G A[t, \frac{1}{t}] = \{h t^m | h \in \text{sconst}_G A \text{ and } m \in \mathbb{Z}\}$.

**Proof.** We show that $\text{sconst}_G A[t, \frac{1}{t}] = \text{sconst}_G A[t, \frac{1}{t}]$. Then by Theorem 11 the theorem is proven. Since $G \subseteq \tilde{G}$ the inclusion $\text{sconst}_G A[t, \frac{1}{t}] \supseteq \text{sconst}_G A[t, \frac{1}{t}]$ is immediate. Now suppose that $g = \sum_i g_i t^i \in \text{sconst}_G A[t, \frac{1}{t}]$. Hence there are $m \in \mathbb{Z}$ and an $h \in G$ such that $\sigma(g) = h t^m g$. By coefficient comparison it follows that $\sigma(g_i) = h g_i$. If $m \geq 1$, take $s$ minimal such that $g_s \neq 0$. Then $\sigma(g_s) \neq 0$. But by the choice of $s$, we get $g_s = 0$ and thus $h g_s = 0$, a contradiction. Otherwise, if $m < 0$, take $s$ maximal such that $g_s \neq 0$. Then $h g_s \neq 0$. But by the choice of $s$, we get $\sigma(g_s) = 0$, again a contradiction. Thus $m = 0$ and consequently, $g \in \text{sconst}_G A[t, \frac{1}{t}]$. \hfill $\Box$

We conclude this subsection by specializing to the group $\tilde{G} = A\{t\}^*$ under the assumption that $A$ is reduced and connected. We remark that this result is not applicable if general $R$-extensions pop up; see Example 11. However, with this result we obtain further insights summarized in Corollary 2.2, Proposition 2 and Corollary 4 below.

**Theorem 13.** Let $(A, \sigma)$ be a difference ring being reduced and connected s.t. $\text{sconst}_K \setminus \{0\} = A^*$. Let $(A[t, \frac{1}{t}], \sigma)$ be II-extension of $(A, \sigma)$ with $\sigma(t) = \alpha t$ for some $\alpha \in A^*$. Then $\text{sconst}_A[t, \frac{1}{t}] = \{h t^m | h \in \text{sconst}_A \text{ and } m \in \mathbb{Z}\}$.

**Proof.** Take $\tilde{G} = (A^*)_{\tilde{A}}$. Then by Lemma 5 we have $\tilde{G} = A[t, \frac{1}{t}]^*$. Thus $\text{sconst}_A[t, \frac{1}{t}] = \text{sconst}_A[t, \frac{1}{t}] = \text{sconst}_A[t, \frac{1}{t}]$. \hfill $\Box$
3.3. $R$-extensions

We start to derive a characterization of $R$-extensions.

Proof of Theorem 1.3 (see page 7). “$\Rightarrow$”: Let $m \in \{1, \ldots, \lambda - 1\}$ and $g \in \mathbb{A} \setminus \{0\}$ such that $\sigma(g) = \alpha^m g$. Since $\sigma(t^m) = \alpha^m t^m$, it follows that $\sigma(g t^{\lambda-m}) = g t^{\lambda-m}$, i.e., $gt^{\lambda-m} \in \text{const}_{A}[t]$. Clearly $g t^{\lambda-m} \notin \mathbb{A}$ which implies that $g t^{\lambda-m} \notin \text{const}_{A}$.

“$\Leftarrow$”: Let $g = \sum_{i=0}^{\lambda-1} g_i t^i \in \mathbb{A}[t] \setminus \mathbb{A}$ with $\sigma(g) = g$. Thus $g_r \neq 0$ for some $r \in \{1, \ldots, \lambda-1\}$.

By coefficient comparison we get $\sigma(g_r) = \alpha^{\lambda-r} g_r$ with $\lambda - r \in \{1, \ldots, \lambda-1\}$.

Let $t$ be an $R$-monomial and let $m := \text{ord}(\alpha) < \lambda$. Then with $g = 1 \in \mathbb{A} \setminus \{0\}$ we have that $\sigma(g) = 1 = \alpha^m 1 = \alpha^m g$. A contradiction to the first statement.

Finally, we deviate properties for the set of semi-constants. Since the proof of the following theorem is completely analogous to the proof of Theorem 11, it is skipped.

Theorem 14. Let $(\mathbb{A}, \sigma)$ be a difference ring and $G \leq \mathbb{A}^*$ with $\text{scost}_{G}\mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. Let $(\mathbb{A}[x], \sigma)$ be an $R$-extension of $(\mathbb{A}, \sigma)$ with $\alpha = \frac{\sigma(x)}{x} \in G$ and $\lambda := \text{ord}(x) = \text{ord}(\alpha) > 1$.

Then $\text{scost}_{G}\mathbb{A}[x] = \{h x^m | h \in \text{scost}_{G}\mathbb{A}, 0 \leq m < \lambda\}$ and $\text{scost}_{G}\mathbb{A}[x] \setminus \{0\} \leq \mathbb{A}[x]^*$.

As in Theorem 12 we will lift this result from the group $G \leq \mathbb{A}^*$ to

$$G = G_{\mathbb{A}}^G = \{h x^m | h \in G \text{ and } m \in \{0, \ldots, \lambda - 1\}\} \leq \mathbb{A}[x]^*.$$

We remark that there is the following subtlety. We have to assume that $\mathbb{A}[x]$ is reduced in order to prove the result below. In order to take care of this extra property, further investigations will be necessary in Subsection 4.1.

Theorem 15. Let $(\mathbb{A}[x], \sigma)$ be an $R$-extension of $(\mathbb{A}, \sigma)$ and $G \leq \mathbb{A}^*$ with $\text{scost}_{G}\mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$. If $\mathbb{A}[x]$ is reduced, then $\text{scost}_{G}\mathbb{A}[x] \setminus \{0\} \leq \mathbb{A}[x]^*$ for $G = G_{\mathbb{A}}^G$.

Proof. Let $\alpha := \frac{\sigma(x)}{x} \in \mathbb{A}^*$ and $n = \text{ord}(\alpha) = \text{ord}(x)$. Let $g \in \text{scost}_{G}\mathbb{A}[x] \setminus \{0\}$, i.e., $\sigma(g) = ux^m g$ with $u \in G$ and $0 \leq m < n$. Since $x^m n = 1$, $\sigma(u^n) = u^n \in G$ with $u^n \in G$.

First suppose that $\sigma(v) = g^n \in \mathbb{A}$. Since $\mathbb{A}[x]$ is reduced, $v \neq 0$ and thus $v \in \text{scost}_{G}\mathbb{A}[x] \setminus \{0\} \leq \mathbb{A}^*$, i.e., $\sigma(u^n/v) = 1$. Hence $g$ is invertible, i.e., $g \in \mathbb{A}[x]^*$.

Otherwise, suppose that $\sigma(v) = g^n \notin \mathbb{A}$. Define $a := u^n \in G$. We consider two subcases. Suppose that there are a $k > 0$ and a $w \in \mathbb{A} \setminus \{0\}$ with $\sigma(w) = aw^k$. Then $w \in \text{scost}_{G}\mathbb{A}[x] \setminus \{0\} \leq \mathbb{A}^*$. Hence $\sigma((g^n)^k/w) = (g^n)^k/w$, i.e., $c := (g^n)^k/w \in \mathbb{K}$, and since $\mathbb{A}[x]$ is reduced, $c \neq 0$. Thus (as above) $g((g^n)_{k-1}/w/c) = 1$ and therefore $g \in \mathbb{K}[x]^*$.

Finally, suppose that there are no $k > 0$ and $w \in \mathbb{A} \setminus \{0\}$ with $\sigma(w) = aw^k$. Hence by Theorem 1.2 there is the $\Pi$-extension $(\mathbb{A}[t], \frac{1}{t})$ of $(\mathbb{A}, \sigma)$ with $\sigma(t) = at$ (a $\in G \leq \mathbb{A}^*$).

Let $v = g^n = \sum_{i=0}^{n-1} v_i x^i \in \mathbb{A}[x] \setminus \mathbb{A}$. Then $\sigma(v) = av$ and thus by coefficient comparison it follows that $\sigma(v_i) = a \alpha^{n-i} v_i$ for some $v_i \in \mathbb{A} \setminus \{0\}$ with $1 \leq i < n$. Hence $\alpha^n = \alpha^{n-1} v_i t$ and thus $\sigma(\frac{v_i}{t^n}) = \frac{u^n}{t^n}$. Since $\mathbb{A}$ is reduced, we have $v_i^n \neq 0$, and consequently $\frac{v_i^n}{t^n} \in \text{const}_{\mathbb{A}[t], \frac{1}{t}} \setminus \mathbb{A}$, a contradiction that $t$ is a $\Pi$-monomial. Thus this case can be excluded. Summarizing any element in $\text{scost}_{G}\mathbb{A}[x] \setminus \{0\}$ is from $\mathbb{A}[x]^*$.

4. Nested $R\Pi\Sigma^*$-extensions and simple $R\Pi\Sigma^*$-extensions

So far we studied single-nested $R\Pi\Sigma^*$-extension. After some further investigations into $R$-extensions, we will glue all the results together and will obtain Theorems 2 and 4.
4.1. Nested $R$-extensions

A special case is obtained immediately by applying iteratively Theorem 14.

**Proposition 1.** Let $(\mathbb{A}, \sigma)$ be a difference ring and $G \leq \mathbb{A}^*$ with sconst$_G \mathbb{A} \setminus \{0\} \leq \mathbb{A}^*$.

Let $(\mathbb{E}, \sigma)$ with $\mathbb{E} = \mathbb{A} \langle x_1 \ldots x_e \rangle$ be an $R$-extension of $(\mathbb{A}, \sigma)$ with $\frac{\sigma(x_i)}{x_i} \in G$ and $n_i = \text{ord}(x_i)$. Then sconst$_G \mathbb{E} = \{h \ x_1^{n_1} \cdots x_e^{n_e} | h \in \text{sconst}_G \mathbb{A} \text{ and } 0 \leq m_i < n_i \text{ for } 1 \leq i \leq e\}$ and sconst$_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$.

In order to treat nested $R$-extensions, we proceed as follows. Let $(\mathbb{A}(x_1) \ldots (x_e), \sigma)$ be an $R$-extension of $(\mathbb{A}, \sigma)$ with $\lambda_i = \text{ord}(x_i)$ and $\sigma(x_i) = \alpha_i x_i$. Moreover, take the polynomial ring $R = \mathbb{A}[y_1, \ldots, y_e]$ and define $\alpha'_i = \alpha |_{x_1 \rightarrow y_1, \ldots, x_{i-1} \rightarrow y_{i-1}}$. Then we obtain the automorphism $\sigma': R \to R$ by $\sigma'(y_i) = \sigma(y_i) = \alpha_i y_i$, i.e., $(\mathbb{R}, \sigma')$ is a difference ring extension of $(\mathbb{A}, \sigma)$. Thus by iterative application of the construction used for Lemma 2 it follows that $\mathbb{A}(x_1) \ldots (x_e)$ is isomorphic to $R/I$ where $I$ is the ideal

$$I = \langle y_1^{\lambda_1} - 1, \ldots, y_e^{\lambda_e} - 1 \rangle$$

(21)

in $\mathbb{R}$. In particular, we obtain the automorphism $\sigma'': R/I \to R/I$ defined by $\sigma''(f + I) = \sigma(f) + I$ and it follows that the difference ring $(\mathbb{A}(x_1) \ldots (x_e), \sigma)$ is isomorphic to $(R/I, \sigma'')$; here $f \in \mathbb{A}(x_1) \ldots (x_e)$ is mapped to $f' + I$ with $f' = f|_{x_1 \rightarrow y_1, \ldots, x_e \rightarrow y_e}$.

Take $G = (\mathbb{F}^*)_E \leq \mathbb{E}^*$. In order to show that sconst$_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$ holds as claimed in Corollary 1 below, we use Gröbner bases theory.

**Lemma 14.** Let $\lambda_i \in \mathbb{N} \setminus \{0\}$. The zero-dimensional ideal $I$ given in (21) in the polynomial ring $R = \mathbb{F}[y_1, \ldots, y_e]$ is radical.

**Proof.** The ideal $I$ is zero-dimensional. Since $\mathbb{F}$ has characteristic 0, it is perfect. We therefore apply the criterion (algorithm) given in [10, Thm. 8.22]. Define $f_i = y_i^{\lambda_i} - 1$. Then for each $i$ ($1 \leq i \leq e$) we have that $f_i \in R \cap \mathbb{F}[y_i]$ and $\gcd(f_i, \frac{\partial f_i}{\partial y_i}) = \gcd(y_i^{\lambda_i} - 1, \lambda_i y_i^{\lambda_i - 1}) = 1$. Thus [10, Thm. 8.22] implies that $\langle f_1, \ldots, f_e \rangle$ is radical. □

**Corollary 1.** Let $(\mathbb{E}, \sigma)$ be an $R$-extension of a difference field $(\mathbb{F}, \sigma)$ and let $G = (\mathbb{F}^*)_E$. Then $\mathbb{E}$ is reduced and sconst$_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$.

**Proof.** The difference ring $(\mathbb{E}, \sigma)$ with $\mathbb{E} = \mathbb{F} \langle x_1 \ldots x_r \rangle$ is isomorphic to $(R/I, \sigma'')$ as defined above with (21) where $\mathbb{K} = \mathbb{F}$. Suppose that $\mathbb{E}$ is not reduced. Then there are $f \in \mathbb{E} \setminus \{0\}$ and $n > 0$ such that $f^n = 0$. Hence there are a $h \in R$ with $h + I \neq I$ and $(h + I)^n = h^n + I = I$. This implies that $h \notin I$ and $h^n \in I$. Therefore $I$ is not radical, a contradiction to Lemma 14. Hence $\mathbb{E}$ is reduced. Thus we can apply Theorem 15 iteratively and it follows that sconst$_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*$. □

4.2. Nested $\Pi \Sigma^*$-extensions

In Corollary 2 we will characterize the set of semi-constants for $\Pi \Sigma^*$-extensions. Part 1 will deal with the general case. Part 2 assumes in addition that the ground ring is reduced and connected. In order to obtain these results, we rely on the following lemmas.

**Lemma 15.** Let $(\mathbb{A}(t), \sigma)$ be a $\Pi \Sigma^*$-extension of $(\mathbb{A}, \sigma)$. If $\mathbb{A}$ is reduced, $\mathbb{A}(t)$ is reduced. If $\mathbb{A}$ is reduced and connected, $\mathbb{A}(t)$ is reduced and connected.
Proof. Let \( t \) be a \( \Pi \)-monomial. Moreover let \( \mathcal{A} \) be reduced. Now take \( f = \sum_i f_i t^i \in \mathcal{A}(t) = \mathcal{A}[t, \frac{1}{t}] \) with \( f \neq 0 \) and \( f^n = 0 \) for some \( n > 0 \). Since \( \mathcal{A} \) is reduced, \( f \notin \mathcal{A} \). Let \( m \in \mathbb{Z} \) be maximal such that \( f_m \neq 0 \). Then the coefficient of \( t^m \) in \( f^n \) is \( f^*_m \). Hence \( f^*_m = 0 \) and thus \( f_m \) is a nilpotent element in \( \mathcal{A} \), a contradiction.

Now let \( \mathcal{A} \) be reduced and connected and take \( f = \sum_i f_i t^i \in \mathcal{A}(t) = \mathcal{A}[t, \frac{1}{t}] \) with \( f^2 = f \) and \( f \notin \{0, 1\} \). Since \( \mathcal{A} \) is connected, \( f \notin \mathcal{A} \). Let \( m \) be maximal such that \( f_m \neq 0 \). If \( m > 0 \), then the coefficient of \( t^m \) in \( f^2 \) is \( f^*_m \) and thus with \( f^2 = f \) we have that \( f^*_m = 0 \); a contradiction that \( \mathcal{A} \) is reduced. Otherwise, if \( m = 0 \), we take \( \bar{m} \) minimal such that \( f_{\bar{m}} \neq 0 \). Note that \( \bar{m} < 0 \) since \( f \notin \mathcal{A} \). As above, it follows that \( f^2_{\bar{m}} = 0 \), a contradiction that \( \mathcal{A} \) is reduced. Summarizing, if \( \mathcal{A} \) is reduced (resp. reduced and connected), \( \mathcal{A}[t, \frac{1}{t}] \) is reduced (resp. reduced and connected). If \( t \) is a \( \Sigma^* \)-monomial, we conclude the same implications since \( \mathcal{A}(t) = \mathcal{A}[t] \leq \mathcal{A}[t, \frac{1}{t}] \). \( \Box \)

In particular, if \( \mathcal{A} \) is reduced, a \( \Pi \Sigma^* \)-extension has the following particular nature: the shift behaviour of \( \Pi \)-monomials does not depend on \( \Sigma^* \)-monomials.

**Lemma 16.** Let \( (\mathcal{E}, \sigma) \) be a \( \Pi \Sigma^* \)-ring extension of \( (\mathcal{A}, \sigma) \) where \( \mathcal{A} \) is reduced. Then the generators can be reordered such that we get the form \( \mathcal{E} = \mathcal{A}(t_1) \ldots (t_p)(s_1) \ldots (s_e) \) where the \( t_i \) are \( \Pi \)-monomials and the \( s_i \) are \( \Sigma^* \)-monomials.

**Proof.** Let \( \mathcal{E} = \langle t_1 \ldots t_e \rangle \). By iterative application of Lemma 15 it follows that \( \mathcal{E} \) is reduced. Let \( t_i \) be a \( \Pi \)-monomial where \( \alpha = \sigma(t_i)/t_i \in \mathcal{A}(t_1) \ldots (t_{i-1}) \) depends on a \( \Sigma^* \)-monomial \( t_j \) with \( j < i \). Then we can reorder the generators such that we get \( \mathcal{H} = \mathcal{A}(t_1) \ldots (t_{j-1})(t_{j+1}) \ldots (t_{i-1}) \); here we forget \( \sigma \) and argue purely in the given ring. In particular, \( \alpha \in \mathcal{H}(t_j) = \mathcal{H}[t_j] \setminus \mathcal{H} \). Since \( \alpha \) is invertible, \( \alpha \in \mathcal{H} \) by Lemma 5; a contradiction. Summarizing, for all \( \Pi \)-monomials \( t_j \) we have that \( \sigma(t_j)/t_j \) is free of \( \Sigma^* \)-monomials. Thus we can shuffle all \( \Pi \)-monomials to the left and all \( \Sigma^* \)-monomials to the right and obtain again a \( \Pi \Sigma^* \)-extension. \( \Box \)

With this preparation we obtain the following result.

**Corollary 2.** Let \( (\mathcal{E}, \sigma) \) be a \( \Pi \Sigma^* \)-extension of \( (\mathcal{A}, \sigma) \) with \( \mathcal{E} = \mathcal{A}(t_1) \ldots (t_e) \).

1. Let \( G \leq \mathcal{A}^* \) with \( \text{sconst}_G \mathcal{A} \setminus \{0\} \leq \mathcal{A}^* \) and let \( \bar{G} = G^{\mathcal{E}}_\mathcal{A} \). If \( (\mathcal{E}, \sigma) \) is a \( \Pi \)-simple \( \Pi \Sigma^* \)-extension of \( (\mathcal{A}, \sigma) \), then \( \text{sconst}_G \mathcal{E} \setminus \{0\} \leq \mathcal{E}^* \) where

\[
\text{sconst}_G \mathcal{E} = \{ h t_1^{m_1} \ldots t_e^{m_e} \mid h \in \text{sconst}_G \mathcal{A} \text{ and } m_i \in \mathbb{Z} \text{ where } m_i = 0 \text{ if } t_i \text{ is a } \Sigma^* \text{-monomial} \}.
\]

2. If \( \mathcal{A} \) is reduced and connected and \( \text{sconst} \mathcal{A} \setminus \{0\} = \mathcal{A}^* \), then

\[
\text{sconst} \mathcal{E} \setminus \{0\} = \{ h t_1^{m_1} \ldots t_e^{m_e} \mid h \in \mathcal{A}^* \text{ and } m_i \in \mathbb{Z} \text{ where } m_i = 0 \text{ if } t_i \text{ is a } \Sigma^* \text{-monomial} \} = \mathcal{E}^*.
\] \( (22) \)

3. If \( \mathcal{A} \) is a field then we have that \( (22) \).

**Proof.** The first part is proven by induction on the number \( e \) of extensions. If \( e = 0 \), nothing has to be shown. Now suppose that the first part holds and consider one extra \( \bar{G} \)-simple \( \Pi \Sigma^* \)-monomial \( t_{e+1} \) on top. Define \( \bar{G} = G^{\mathcal{E}(t_{e+1})} = G^{\mathcal{E}(t_{e+1})}_\mathcal{A} \). If \( t_i \) is a \( \Sigma^* \)-monomial, \( \bar{G} = \bar{G} \). Together with Theorem 7 it follows that \( \text{sconst}_G \mathcal{E}[t_{e+1}] = \]

23
\[\text{sconst}_G E[t_{e+1}] = \text{sconst}_G E \text{ and } \text{sconst}_G E[t_{e+1}] \setminus \{0\} \leq E^* \leq E[t_{e+1}]^*.\] If \(t_i\) is a \(\Pi\)-monomial, we have \(\sigma(t_{e+1})/t_{e+1} \in \mathcal{G}\). Hence Theorem 12 yields \[\text{sconst}_G E[t_{e+1}, \frac{1}{t_{e+1}}] = \{h t_{e+1}^m | m \in \mathbb{Z} \text{ and } h \in \text{sconst}_G E\}\] and thus by the induction assumption we have that
\[\text{sconst}_G E[t_{e+1}, \frac{1}{t_{e+1}}] = \{h t_1^{m_1} \ldots t_i^{m_i} | h \in \text{sconst}_G A \text{ and } m_i \in \mathbb{Z}\}\]
where \(m_i = 0\) if \(t_i\) is a \(\Sigma^*\)-monomial
and thus \[\text{sconst}_G E[t_{e+1}, \frac{1}{t_{e+1}}] \setminus \{0\} \leq E[t_{e+1}, \frac{1}{t_{e+1}}]^*.\] This completes the induction step.
Similarly, the first equality of part (2) follows by Theorems 8 and 13. The second equality follows by iterative application of Lemmas 5 and 15. Since any field is connected and reduced and \(\text{sconst}_A \setminus \{0\} = \mathcal{A}^*\) by Lemma 12, part (3) follows by part (2).

Restricting to \(\Sigma^*\)-extensions, the above result simplifies as follows.

**Corollary 3.** Let \((\mathcal{E}, \sigma)\) be a \(\Sigma^*\)-extension of \((\mathcal{A}, \sigma)\). Then the following holds.
(1) If \(G \leq \mathcal{A}^*\) such that \(\text{sconst}_G A \setminus \{0\} \leq \mathcal{A}^*\), then \(\text{sconst}_G \mathcal{E} = \text{sconst}_G \mathcal{A}\).
(2) If \(\mathcal{A}\) is reduced and \(\text{sconst}_A \setminus \{0\} = \mathcal{A}^*\), then \(\mathcal{E}\) is reduced and \(\text{sconst}_E = \text{sconst}_A\).
(3) If \(\mathcal{A}\) is a field, then \(\text{sconst}_E \setminus \{0\} = \mathcal{A}^* = \mathcal{A} \setminus \{0\}\).

### 4.3. \(\mathcal{R}\Pi\Sigma^*\)-extensions and their simple and single-rooted restrictions

For simple and single-rooted \(\mathcal{R}\Pi\Sigma^*\)-extensions we obtain immediately the

**Proof of Theorem 2 (see page 13).** Combine Corollary 2.1 and Proposition 1.

In order to get Theorem 4 for general simple \(\mathcal{R}\Pi\Sigma^*\)-extensions, further properties are needed. The first lemma states that a tower of simple \(\mathcal{R}\Pi\Sigma^*\)-extensions is again a simple \(\mathcal{R}\Pi\Sigma^*\)-extension; the proof is immediate.

**Lemma 17.** Let \((\mathcal{A}, \sigma)\) be a difference ring with a group \(G \leq \mathcal{A}^*\) and let \((\mathcal{H}, \sigma) \leq (\mathcal{E}, \sigma)\) be \(\mathcal{R}\Pi\Sigma^*\)-extensions. Then \((G^\mathcal{A}_{\mathcal{H}})_{\mathcal{H}} = G^\mathcal{A}_{\mathcal{E}}\). Moreover, if \((\mathcal{A}, \sigma) \leq (\mathcal{H}, \sigma)\) is \(G\)-simple and \((\mathcal{H}, \sigma) \leq (\mathcal{E}, \sigma)\) is \(G^\mathcal{A}\)-simple, then \((\mathcal{A}, \sigma) \leq (\mathcal{E}, \sigma)\) is \(G\)-simple.

In particular, any simple \(\mathcal{R}\Pi\Sigma^*\)-extension can be reordered such that the \(R\)-monomials are at the first place and the \(\Sigma^*\)-monomials are on top.

**Lemma 18.** Let \((\mathcal{A}, \sigma)\) be a difference ring with \(G \leq \mathcal{A}^*\) a group. Any \(G\)-simple \(\mathcal{R}\Pi\Sigma^*\)-extension \((\mathcal{E}, \sigma)\) of \((\mathcal{A}, \sigma)\) can be reordered to the form \(\mathcal{E} = \mathcal{A}(t_1) \langle t_2 \rangle \ldots \langle t_e \rangle\) with \(r, p \in \mathbb{N}\) \((0 \leq r \leq p \leq e)\) such that the following properties hold:
(1) For all \(i\) \((1 \leq i \leq r)\), \(t_i\) is an \(R\)-monomial with \(\sigma(t_i)/t_i = u_i t_i^{z_1} \ldots t_i^{z_{i-1}}\) for some root of unity \(u_i \in \mathcal{G}\) and \(z_i \in \mathbb{N}\).
(2) For all \(i\) \((r < i \leq p)\), \(t_i\) is a \(\Pi\)-monomial with \(\sigma(t_i)/t_i = u_i t_i^{z_1} \ldots t_i^{z_{i-1}}\) for some \(u_i \in \mathcal{G}\) and \(z_i \in \mathbb{Z}\).
(3) For all \(i\) \((p < i \leq e)\), \(t_i\) is a \(\Sigma^*\)-monomial with \(\sigma(t_i) - t_i \in \mathcal{A}(t_1) \langle t_2 \rangle \ldots \langle t_{i-1} \rangle\).

In particular, for any \(f \in G^\mathcal{A}_{\mathcal{A}}\) which depends on a \(\Pi\)-monomial \(t_i\) we have that \(\text{ord}(f) = 0\).

**Proof.** We show the lemma by induction on the number of \(\mathcal{R}\Pi\Sigma^*\)-monomials. Suppose that the lemma holds for \(e\) extensions. Now let \(\mathcal{E} = \mathcal{A}(t_1) \ldots \langle t_e \rangle\) and consider the \(\mathcal{R}\Pi\Sigma^*\)-monomial \(t_{e+1}\) on top of \(\mathcal{E}\). By the induction assumption we can reorder \(\mathcal{E}\) such that it has the desired form (all \(R\)-monomials are on the left, all \(\Pi\)-monomials are in the middle
and all $\Sigma^*$-monomials are on the right). If $t_{e+1}$ is a $\Sigma^*$-monomial, the required shape is fulfilled. If $t_{e+1}$ is an $R$-monomial, observe that $\alpha := \sigma(t_{e+1})/t_{e+1} \in G_{\sigma}^e$. Since $\text{ord}(\alpha) = \text{ord}(t_{e+1}) > 1$ by Theorem 1.3, $\alpha$ is free of $\Pi$-monomials by the induction assumption and (by definition) free of $\Sigma^*$-monomials. Thus we can shuffle $t_{e+1}$ to the left (such that all $\Pi\Sigma^*$-monomials are to the right), and the required shape is satisfied. Similarly, if $t_{e+1}$ is a $\Pi$-monomial, $\sigma(t_{e+1})/t_{e+1} \in G_{\sigma}^e$ is free of $\Sigma^*$-monomials by definition and we can shuffle $t_{e+1}$ to the left such that all $\Sigma^*$-monomials are to the right. This completes the first part of the lemma. Now let $E = K(x_1) \ldots (x_{e+1})$ be in the desired ordered form. If $x_{e+1}$ is a $\Sigma^*$-monomial, we have that $G_{\sigma}^{E(x_{e+1})} = G_{\sigma}^e$. Thus the second part holds by the induction assumption. If $x_{e+1}$ is an $R$-extension, also all $x_i$ with $1 \leq i \leq e$ are $R$-monomials, and the second statement holds trivially. Finally, let $x_{e+1}$ be a $\Pi$-monomial and take $f \in G_{\sigma}^{E(x_{e+1})}$. If $f \in E$ and $f$ depends on $\Pi$-monomials, we have again that $\text{ord}(f) = 0$ by the induction assumption. To this end, suppose that $f$ depends on $x_{e+1}$ and we have that $\text{ord}(f) = n > 0$. Then $f = u x_{e+1}^m$ where $m \neq 0$ and $u \in E^*$. Since $f^n = 1$, $u^n x_{e+1}^m = 1$ where $u^n \neq 0$. Hence $x_{e+1}$ is not transcendental over $E$, a contradiction to the definition of a $\Pi$-monomial. Consequently, $\text{ord}(f) = n = 0$. This completes the proof.

For completeness we observe that this reordering is also possible if one relaxes the condition that the $\Pi\Sigma^*$-extension is simple but requires that the ground ring is a field.

**Lemma 19.** Let $(E, \sigma)$ be a $\Pi\Sigma^*$-ring extension of a difference field $(F, \sigma)$. Then $(E, \sigma)$ can be reordered to the form $E = F(x_1) \ldots (x_e)\langle t_1 \ldots \langle p \rangle s_1 \ldots s_e \rangle$ where the $x_i$ are $R$-monomials, the $t_i$ are $\Pi$-monomials and the $s_i$ are $\Sigma^*$-monomials.

**Proof.** First we try to shuffle all $R$-extensions to the front. Suppose that this fails at the first time. Then there are an $R$-extension $(H, \sigma)$ of $(F, \sigma)$, a $\Pi\Sigma^*$-extension $(G, \sigma)$ of $(H, \sigma)$ with $G = \mathcal{H}(y_1) \ldots (y_l)$ and an $R$-extension $(G(x), \sigma)$ of $(G, \sigma)$ with $\alpha = \sigma(x)/x$ in which $y_l$ occurs. Note that $H$ is reduced by Corollary 1 and $G$ is reduced by iterative application of Lemma 15. Write $\alpha = \sum_i f_i y_i^l$. Let $m \neq 0$ such that $f_m \neq 0$ and such that $|m| \geq 1$ is maximal (we remark that $m < 0$ can only happen if $y_l$ is a $\Pi$-monomial). By the choice of $m$ we have that the coefficient of $y_i^m$ in $\alpha^n$ is $f_m^n$. Hence with $\alpha^n = 1$ it follows that $f_m^n = 0$, a contradiction to the assumption that $G$ is reduced. Therefore we can shuffle all $R$-monomials to the left and all $\Pi\Sigma^*$-monomials to the right. Since the nested $R$-extension is reduced by Corollary 1, we can apply Lemma 16 to reorder the $\Pi\Sigma^*$-monomials further as claimed in the statement.

By definition any (nested) $\Sigma^*$-extension is also a simple $\Sigma^*$-extension. If the ground ring is reduced and connected, we obtain the following stronger result.

**Proposition 2.** Let $(G, \sigma)$ be a difference ring where $G$ is reduced and connected and where $\text{const}G \setminus \{0\} = G^*$. Then a $\Pi\Sigma^*$-extension $(E, \sigma)$ of $(G, \sigma)$ is simple.

**Proof.** Let $E = G\langle t_1 \ldots (t_e) \rangle$. By Lemma 16 we may suppose that the generators are ordered such that $t_1 \ldots t_p$ are $\Pi$-monomials and $t_{p+1} \ldots t_e$ are $\Sigma^*$-monomials. By Corollary 2.2 we have that $\alpha(t_{i-1})^* \in G(t_1) \ldots (t_{i-1})^* = (G^*)G(t_1)^* \ldots (t_{i-1})^*$ with $1 \leq i \leq p$. Thus the $\Pi$-monomials $t_i$ are $G^*$-simple. Moreover, the $\Sigma^*$-monomials $t_i$ on top are all $G^*$-simple by definition. Summarizing $(F, \sigma) \preceq (E, \sigma)$ is simple.

25
In other words, for a reduced and connected difference ring \((\mathbb{A}, \sigma)\) (e.g., if \(\mathbb{A}\) is a field) the notions \(\Pi\Sigma^*\)-ring extension and simple \(\Pi\Sigma^*\)-ring extension are equivalent. The situation becomes rather different if the ring is, e.g., not connected; see Example 10. However, for single-rooted \(R\Pi\Sigma^*\)-extensions over a difference field, the situation is again tame.

**Corollary 4.** A single-rooted \(R\Pi\Sigma^*\)-extension \((\mathbb{E}, \sigma)\) of a difference field \((\mathbb{G}, \sigma)\) is simple.

**Proof.** By definition, the \(R\Pi\Sigma^*\)-extension can be reordered to the form (5). Since \(\mathbb{G}\) is a field, we have that \(\text{sconst}_\mathbb{G} \setminus \{0\} = \mathbb{G}^*\). Hence we can apply Proposition 2 and it follows that the \(\Pi\)-extension \((\mathbb{G}(t_1) \ldots (t_r), \sigma)\) of \((\mathbb{G}, \sigma)\) is simple. Since \(\frac{\sigma(t_i)}{x_i} \in \mathbb{G}^*\) for \(1 \leq i \leq u\), the \(R\)-monomials \(x_i\) are \(\mathbb{G}^*\)-simple. Since also the \(\Sigma^*\)-monomials \(s_i\) are \(\mathbb{G}^*\)-simple, we conclude that \((\mathbb{G}, \sigma) \leq (\mathbb{E}, \sigma)\) is simple. \(\square\)

To this end, we obtain the following main result.

**Theorem 16.** Let \((\mathbb{H}, \sigma)\) be an \(R\)-extension of a difference field \((\mathbb{F}, \sigma)\) and let \((\mathbb{E}, \sigma)\) with \(\mathbb{E} = \mathbb{H}(t_1)(t_2) \ldots (t_e)\) be a simple \(\Pi\Sigma^*\)-extension of \((\mathbb{H}, \sigma)\). Let \(\mathbb{G} = (\mathbb{F}^*)^\mathbb{H}\) and define \(\tilde{\mathbb{G}} = \tilde{\mathbb{G}}_{\mathbb{H}}\). Then we have \(\text{sconst}_{\tilde{\mathbb{G}}_\mathbb{F}} \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*\) where

\[
\text{sconst}_{\tilde{\mathbb{G}}_\mathbb{F}} \mathbb{E} = \{ h t_1^{m_1} \ldots t_e^{m_e} \mid h \in \text{sconst}_{\tilde{\mathbb{G}}} \mathbb{H}, m_i \in \mathbb{Z} \text{ where } m_i = 0 \text{ if } t_i \text{ is a } \Sigma^*\text{-monomial} \}.
\]

**Proof.** By Corollary 1 we have that \(\text{sconst}_{\tilde{\mathbb{G}}} \mathbb{H} \setminus \{0\} \leq \mathbb{H}^*\). Hence we can apply Corollary 2.1 and the result follows. \(\square\)

**Proof of Theorem 4 (see page 13).** This is a special case of Theorem 16. \(\square\)

5. **The algorithmic machinery I: order, period, factorial order**

An important ingredient for the development of our summation algorithms is the knowledge of the order (see its definition in (10) and the corresponding Problem O), the period and the factorial order. In \((\mathbb{A}, \sigma)\) we define the period of \(h \in \mathbb{A}^*\) by

\[
\text{per}(h) = \begin{cases} 
0 & \text{if } \exists n > 0 \text{ s.t. } \sigma^n(h) = h \\
\min \{ n > 0 \mid \sigma^n(h) = h \} & \text{otherwise};
\end{cases}
\]

and the factorial order of \(h\) by

\[
\text{ford}(h) = \begin{cases} 
0 & \text{if } \exists n > 0 \text{ s.t. } h(n) = 1 \\
\min \{ n > 0 \mid h(n) = 1 \} & \text{otherwise}.
\end{cases}
\]

Using the properties of the automorphism \(\sigma\) and Lemma 6 it is easy to see that the \(\mathbb{Z}\)-modules generated by \(\text{ord}(h)\), \(\text{per}(h)\) and \(\text{ford}(h)\) are \(\langle \text{ord}(h) \rangle = \text{ord}(h) \mathbb{Z} = \{ k \in \mathbb{Z} \mid h^k = 1 \}, \langle \text{per}(h) \rangle = \text{per}(h) \mathbb{Z} = \{ k \in \mathbb{Z} \mid \sigma^k(h) = h \}, \langle \text{ford}(h) \rangle = \text{ford}(h) \mathbb{Z} = \{ k \in \mathbb{Z} \mid h^{(k)} = 1 \} \rangle = \text{ford}(h) \mathbb{Z} = \{ k \in \mathbb{Z} \mid h^{(k)} = 1 \}\rangle, \text{respectively. In addition, the following basic properties hold.}

**Lemma 20.** Let \((\mathbb{A}, \sigma)\) be a difference ring with \(\alpha, h \in \mathbb{A}^*\).

(1) If \(\alpha \in (\text{const}_\mathbb{A})^*\), then \(\text{per}(\alpha) = 1\) and \(\text{ford}(\alpha) = \text{ord}(\alpha)\).

(2) If \(\sigma(h) = \alpha h\), then \(\text{per}(h) = \text{ford}(\alpha)\).
(3) If \( \text{ord}(\alpha) > 0 \) and \( \text{per}(\alpha) > 0 \), then \( \text{per}(\alpha) | \text{ford}(\alpha) | \text{per}(\alpha) \text{ ord}(\alpha) \) and
\[
\text{ford}(\alpha) = \min(i \mid \text{per}(\alpha) | 1 \leq i \leq \text{ord}(\alpha) \text{ and } \alpha(i \mid \text{per}(\alpha)) = 1) > 0. \tag{23}
\]

**Proof.** (1) Since \( \sigma(\alpha) = \alpha, \text{per}(\alpha) = 1. \) Since \( \alpha(n) = \alpha^n \) for \( n \geq 0 \), \( \text{ford}(\alpha) = \text{ord}(\alpha) \).

(2) By Lemma 6.4 we have that \( \sigma^n(h) = h \iff \alpha(n) = 1 \). Hence \( \text{per}(h) = \text{ford}(\alpha) \).

(3) Take \( p = \text{per}(\alpha) > 0 \) and \( v = \text{ord}(\alpha) > 0 \). Then we have that
\[
\alpha(p) = \alpha \sigma(\alpha) \ldots \sigma^{p-1}(\alpha) = (\alpha \sigma(\alpha) \ldots \sigma^{p-1}(\alpha))^v = \alpha^v \sigma(\alpha^v) \ldots \sigma^{p-1}(\alpha^v) = 1.
\]
Consequently, we can choose \( n = \text{ord}(\alpha) \text{ per}(\alpha) \) to obtain \( \alpha(n) = 1 \). In particular, for any \( i \geq 0 \) with \( \alpha(i) = 1 \) we have that \( 1 = \frac{\sigma(1)}{1} = \frac{\sigma(\alpha(i))}{\alpha(i)} = \frac{\sigma(i)}{\alpha} \). Hence \( \text{per}(\alpha)|i \). Therefore the smallest \( \lambda \) with \( \alpha(\lambda) = 1 \) is given by (23). In particular, \( \text{per}(\alpha) | \text{ford}(\alpha) | \text{ord}(\alpha) \text{ per}(\alpha) \).

We will present methods to calculate the order, period and factorial order for the elements of \( (\mathbb{A}^\times)^R_{\mathbb{G}} \) of a simple \( R \)-extension \( (\mathbb{E}, \sigma) \geq (\mathbb{G}, \sigma) \) by recursion. First, we assume that the orders of the \( R \)-monomials in \( (\mathbb{E}, \sigma) \geq (\mathbb{G}, \sigma) \) are already computed and show how the orders of the elements of \( (\mathbb{A}^\times)^R_{\mathbb{G}} \) can be determined.

**Lemma 21.** Let \( (\mathbb{E}, \sigma) \) with \( \mathbb{E} = \mathbb{A}(x_1) \ldots (x_e) \) be an \( R \)-extension of \( (\mathbb{A}, \sigma) \) and define
\[
\alpha := u x_1^{z_1} \ldots x_e^{z_e} \in (\mathbb{A}^\times)^R_{\mathbb{A}} \tag{24}
\]
with \( u \in \mathbb{A}^\times \) and \( z_i \in \mathbb{N} \). Then \( \text{ord}(\alpha) > 0 \) iff \( \text{ord}(u) > 0 \). If \( \text{ord}(u) > 0 \), then
\[
\text{ord}(\alpha) = \text{lcm}(\text{ord}(u), \frac{\text{ord}(x_1)}{\text{gcd}(\text{ord}(x_1), z_1)}, \ldots, \frac{\text{ord}(x_e)}{\text{gcd}(\text{ord}(x_e), z_e)}). \tag{25}
\]

**Proof.** If \( e = 0 \), the lemma holds. Now let \( n := \text{ord}(\alpha) > 0 \). Suppose that \( 1 \neq (x_1^{z_1} \ldots x_e^{z_e})^n = x_1^{n z_1} \ldots x_e^{n z_e} \). Let \( i \) be maximal such that \( \text{ord}(x_i) \mid z_i n \). Then there is an \( s \) with \( 0 < s < \text{ord}(x_i) \) with \( x_i^{\text{ord}(x_i) - s} = u^n x_1^{s z_1} \ldots x_{i-1}^{s z_{i-1}} \in \mathbb{A}(x_1) \ldots (x_{i-1}) \) which contradicts to the construction that \( x_i^{\text{ord}(x_i)} = 1 \) is the defining relation of the \( R \)-monomial. Thus \( (x_1^{z_1} \ldots x_e^{z_e})^n = 1 \) and \( u^n = 1 \), i.e., \( \text{ord}(u) > 0 \) and \( \text{ord}(x_1^{z_1} \ldots x_e^{z_e}) > 0 \). In particular, \( \text{ord}(\alpha) = \text{lcm}(\text{ord}(u), \text{ord}(x_1^{z_1} \ldots x_e^{z_e})) \). By similar arguments we show that \( (x_1^{z_1})^n = \cdots = (x_e^{z_e})^n \) and consequently \( \text{ord}(x_1^{z_1} \ldots x_e^{z_e}) = \text{lcm}(\text{ord}(x_1^{z_1}), \ldots, \text{ord}(x_e^{z_e})) \). Since also \( \text{ord}(x_i^{z_i}) = \frac{\text{ord}(x_i)}{\text{gcd}(\text{ord}(x_i), z_i)} \) holds, the identity (25) is proven.

Conversely, suppose that \( \text{ord}(u) > 0 \). Then the value of the right right hand side of (25) is positive. Denote it by \( n \). Then one can check that \( \alpha^n = 1 \). Therefore \( \text{ord}(\alpha) > 0 \).

In the next lemma we set up the stage to calculate the period and factorial order.

**Lemma 22.** Let \( (\mathbb{E}, \sigma) \) with \( \mathbb{E} = \mathbb{A}(x_1) \ldots (x_e) \) be an \( R \)-extension of \( (\mathbb{A}, \sigma) \) where we have \( \text{per}(x_i) > 0 \) for \( 1 \leq i \leq e \). Let \( \alpha \in (\mathbb{A}^\times)^R_{\mathbb{A}} \) as in (24) with \( z_1, \ldots, z_e \in \mathbb{N} \) and \( u \in \mathbb{A}^\times \).

(1) Then \( \text{per}(\alpha) > 0 \) iff \( \text{per}(u) > 0 \). If \( \text{per}(u) > 0 \), then
\[
\text{per}(\alpha) = \min(1 \leq j \leq \mu | \sigma^j(\alpha) = \alpha \text{ and } j \mid \mu) \tag{26}
\]
with \( \mu = \text{lcm}(\text{per}(u), \text{per}(x_{i_1}), \ldots, \text{per}(x_{i_k})) \) where \( \{i_1, \ldots, i_k\} = \{i : \text{ord}(x_i) \mid z_i\} \).

(2) We have that \( \text{ford}(\alpha) > 0 \) iff \( \text{ord}(u) > 0 \).

(3) If \( \text{per}(u), \text{ord}(u) > 0 \), then \( \text{ford}(\alpha) > 0 \) and \( 0 < \text{per}(\alpha)|\text{ford}(\alpha)|\text{per}(\alpha)\text{ ord}(\alpha) \).

(4) If the values \( \text{ord}(x_i) \) and \( \text{per}(x_i) \) for \( 1 \leq i \leq e \) and the values \( \text{per}(u) > 0 \) and \( \text{ord}(u) > 0 \) are given explicitly, then \( \text{per}(\alpha) \) and \( \text{ford}(\alpha) \) can be calculated.
Proof. (1) Suppose that \( \text{per}(u) > 0 \). Then \( \mu > 0 \). In particular, it follows that \( \sigma^\mu(\alpha) = \alpha \). Consequently, per(\(\alpha\)) > 0 with \( \text{per}(\alpha)\mu \). Hence we have (26). Conversely, suppose that \( \text{per}(\alpha) > 0 \). Then with \( \nu := \text{lcm}(\text{per}(\alpha), \text{per}(x_1), \ldots, \text{per}(x_e)) > 0 \) we get \( u x_1^{\nu_1} \cdots x_e^{\nu_e} = \alpha = \sigma^\nu(\alpha) x_1^{\nu_1} \cdots x_e^{\nu_e} \). Thus \( \sigma^\nu(u) = u \), and consequently \( \text{ord}(u) > 0 \). (2) By part 1, \( \text{per}(\alpha) > 0 \). And with \( \text{ord}(u) > 0 \) and Lemma 21 it follows that \( \text{ord}(\alpha) > 0 \). Hence by Lemma 20.3 we get \( \text{per}(\alpha)\text{ord}(\alpha)\text{per}(\alpha) \).

(3) Since \( \text{ord}(x_i) \) and \( \text{per}(x_i) > 0 \), it follows that \( \text{ford}(x_i) > 0 \) by Lemma 20.3 for all \( 1 \leq i \leq e \). If \( \text{ford}(u) > 0 \), take \( \nu = \text{lcm}(\text{ford}(u), \text{ord}(x_1), \ldots, \text{ord}(x_e)) \). By Lemma 6.1, \( \alpha(\nu) = 1 \). Conversely, if \( n = \text{ford}(\alpha) > 0 \), take \( \nu' = \text{lcm}(\text{ford}(\alpha), \text{ord}(x_1), \ldots, \text{ord}(x_e)) > 0 \). Then again by Lemma 6.1: \( 1 = \alpha(\nu') = (u x_1^{\nu_1} \cdots x_e^{\nu_e})_{(\nu')} = u(\nu') \). Thus \( \text{ford}(u) > 0 \).

(4) If \( \text{per}(u) \) and the values \( \text{per}(x_i) \) are given, \( \mu \) from item 1 can be computed. In particular, if \( \text{ord}(u) \) and \( \text{ord}(x_i) \) are given explicitly, \( \text{ord}(\alpha) \) can be calculated by Lemma 21. Thus \( \text{per}(\alpha) \) can be determined by (26) and then \( \text{ford}(\alpha) \) can be computed by (23). □

Example 12. (1) Take \( \alpha = u = -1 \in \mathbb{Q} \). We get \( \text{ord}(\alpha) = 2 \). In addition, \( \text{per}(\alpha) = 1 \). Moreover, \( 1 = \text{per}(-1) = 1 \) for \( \text{ord}(\alpha) = 2 \). Hence (26) yields \( \text{ford}(-1) = 2 \).

(2) Consider the \( R \)-extension \( (\mathbb{Q}[x], \sigma) \) of \( (\mathbb{Q}, \sigma) \) with \( \sigma(x) = -x \) and \( \text{ord}(x) = 2 \), and take \( \alpha = -x \). We get \( \text{ord}(\alpha) = \text{lcm}(\text{ord}(-1), \text{ord}(x)) = 2 \) by (25). With \( \mu = \text{lcm}(\text{per}(-1), \text{per}(x)) = 2 \) we get \( \text{per}(\alpha) = 2 \) by using (26). Moreover, we get \( 2 = \text{per}(\alpha)\text{ord}(\alpha)\text{per}(\alpha) \text{ord}(\alpha) = 4 \). Hence with (26) we get \( \text{ford}(\alpha) = 4 \).

(3) Consider the \( R \)-extension \( (\mathbb{K}[k][x], \sigma) \) of \( (\mathbb{K}[k], \sigma) \) with \( \sigma(x) = i \) and \( \text{ord}(x) = 4 \) from Example 7. We have \( \text{per}(x) = 4 \). Take \( \alpha = x \). We obtain the following bounds

\[ 4 = \text{per}(\alpha)\text{ord}(\alpha)\text{per}(\alpha) \text{ord}(\alpha) = 16. \]

Thus with (26) we determine \( \text{ford}(\alpha) = 8 \).

Combining the two lemmas from above we arrive at the following result.

Proposition 3. Let \( (\mathbb{A}(x_1), \ldots, x_e), \sigma) \) be a simple \( R \)-extension of \( (\mathbb{A}, \sigma) \) where for \( 1 \leq i < e \) we have \( \sigma(x_i)/x_i = u_i x_1^{m_1 i} \cdots x_{i-1}^{m_{i-1} i}-1 \) with \( u_i \in \mathbb{A}^* \) and \( m_{i-1} \in \mathbb{N} \).

(1) Then \( \text{ord}(u_i) > 0 \) for \( 1 \leq i \leq e \). In particular, if the values \( \text{ord}(u_i) \) are given explicitly (are computable), then the values \( \text{ord}(x_i) \) are computable.

(2) If \( \text{per}(u_i) > 0 \) for \( 1 \leq i \leq e \), then \( \text{per}(x_i) > 0 \) for \( 1 \leq i \leq e \). In particular, if the values \( \text{ord}(u_i) \) and \( \text{per}(u_i) \) for \( 1 \leq i \leq e \) are given explicitly (can be computed), the values \( \text{per}(x_i) \) for all \( 1 \leq i \leq e \) are computable.

Proof. (1) By iterative application of Lemma 22 it follows that \( \text{ord}(u_i) > 0 \) for all \( 1 \leq i \leq e \). Moreover, suppose that \( \text{ord}(u_i) \) is given for \( 1 \leq i \leq e \). Furthermore, assume that the values \( \text{ord}(x_i) \) for \( 1 \leq i \leq s \) with \( s < e \) are already determined. Then define \( \alpha = \sigma(x_s)/x_s \). By (25) we obtain \( \text{ord}(\alpha) \) and thus \( \text{ord}(x_s) = \text{ord}(\alpha) \) by Theorem 1.3. This completes the inductive step.

(2) Suppose that \( \text{per}(u_i) > 0 \) for \( 1 \leq i \leq e \). Moreover, suppose that we have shown already that \( d_i = \text{per}(x_i) > 0 \) for \( 1 \leq i < s \) with \( s < e \). Define \( \alpha = \sigma(x_s)/x_s \). By Lemma 22 we have \( \text{per}(\alpha) > 0 \) and \( \text{ford}(\alpha) > 0 \). By Lemma 20.2 it follows that \( \text{per}(x_s) = \text{ford}(\alpha) > 0 \).

If the values \( \text{ord}(u_i) \) are given explicitly, we can compute \( \text{ord}(\alpha) \) by part 1. If \( u_s \) is given explicitly and \( d_1, \ldots, d_{s-1} \) are given (are already computed), \( \text{ford}(\alpha) = \text{ord}(x_s) \) can be calculated with (23). This completes the induction step. □
Corollary 5. Let \((E, \sigma)\) with \(E = F(x_1) \cdots (x_e)\) be a simple \(R\)-extension of a difference field \((F, \sigma)\) with constant field \(K\) such that all roots of unity in \(F\) are constants (e.g., if \((F, \sigma)\) is strong constant-stable). Then the following holds:

1. For \(1 \leq i \leq e\) we have that
   \[
   \sigma(x_i)/x_i = u_i x_1^{m_{i,1}} \cdots x_{i-1}^{m_{i,i-1}}
   \]
   for some root of unity \(u_i \in \mathbb{K}^*\) with \(\text{ord}(u_i)\mid\text{ord}(x_i)\) and \(m_{i,j} \in \mathbb{N}\).

2. \((E(x_1) \cdots x_e), \sigma)\) is a simple \(R\)-extension of \((K, \sigma)\).

3. Let \(\alpha = u x_1^{z_1} \cdots x_e^{z_e} \in (\mathbb{K}^*)^E_{U}\) with \(z_1, \ldots, z_e \in \mathbb{N}\) and \(u \in \mathbb{K}^*\). Then
   \[
   \text{ord}(u) > 0 \iff \text{ord}(\alpha) > 0 \iff \text{per}(\alpha) > 0 \iff \text{ford}(\alpha) > 0.
   \]

4. If \((K, \sigma)\) is computable and Problem O solvable in \(\mathbb{K}^*\), the values of \(\text{ord}(\alpha), \text{per}(\alpha)\) and \(\text{ford}(\alpha)\) are computable for all \(\alpha \in (\mathbb{K}^*)^E_{U}\).

5. Problem O is solvable in \((E^*)^E_E\) if it is solvable in \(\mathbb{K}^*\) and \((F, \sigma)\) is computable.

Proof. (1) By definition we have that (27) with \(m_i \in \mathbb{N}\) and \(u_i \in F^*\). By Lemma 21 it follows that \(\text{ord}(u_i) > 0\) and \(\text{ord}(u_i)\mid\text{ord}(x_i)\). In particular, \(u_i \in \mathbb{K}^*\) since all roots of unity from \(F\) are constants by assumption.

(2) It is immediate that \((H, \sigma)\) with \(H = K(x_1) \cdots x_e\) forms a difference ring. Since \(\text{const}E = \text{const}F = K\), \((H, \sigma)\) is a simple \(R\)-extension of \((K, \sigma)\).

(3) By part 1 we get \(u_i \in \mathbb{K}^*\) and \(\text{ord}(u_i) > 0\) for \(1 \leq i \leq e\). In particular, \(\text{per}(u_i) = 1\). With Proposition 3 we get \(\text{per}(x_i) > 0\), and by Lemma 20.1 we obtain \(\text{per}(u) = 1\) and \(\text{ford}(u) = \text{ord}(u)\). Thus the equivalences follow by Lemmas 21 and 22 (part 1.2).

(4) Since \(u_i \in \mathbb{K}^*\), the values of \(\text{ord}(u_i) > 0\) can be determined by solving Problem O in \(\mathbb{K}^*\). Thus by Proposition 3 the orders and periods of the \(x_i\) can be computed. Let \(\alpha := u x_1^{z_1} \cdots x_e^{z_e}\) with \(u \in \mathbb{K}^*\) and \(z_i \in \mathbb{N}\). Then by Lemma 21 and the computation of \(\text{ord}(u)\) the order of \(\alpha\) can be computed. Moreover, since \(\text{per}(u) = 1\) and \(\text{ord}(u) = \text{ford}(u)\) are given, we can invoke Lemma 22 to calculate the period and factorial order of \(\alpha\).

(5) Let \(\alpha\) be given as in (24) with \(u \in F^*\) and \(m_i \in \mathbb{N}\). By Lemma 21 \(\text{ord}(\alpha) > 0\) iff \(\text{ord}(u) > 0\). By assumption, \(\text{ord}(u) > 0\) implies \(u \in \mathbb{K}^*\). Thus, if \(u \notin \mathbb{K}\), \(\text{ord}(\alpha) = 0\). Otherwise, if \(u \in \mathbb{K}^*\), we can apply part 4. \(\square\)

To this end, we are now in the position to prove Theorem 5.1.

Proof of Theorem 5.1 (see page 13). Let \((E, \sigma)\) be a simple \(R\PiSigma^*\)-extension of \((F, \sigma)\) where \((F, \sigma)\) is computable and where any root of unity of \(F\) is from \(K = \text{const}F\). Reorder it to the shape as given in Lemma 18. In particular, the \(R\)-extension \((E(t_1) \cdots (t_t), \sigma)\) of \((F, \sigma)\) has the shape as given in Corollary 5.1. Let \(f \in (F^*)^E_F\). Suppose first that \(f\) depends on a \(\Pi\)-monomial \(t_i\). Now assume that \(\text{ord}(f) = n > 0\), and let \(i\) be maximal such that a \(\Pi\)-monomial depends on \(f\). Then \(f = u t_i^n\) with \(u \in F(t_1) \cdots (t_{i-1})^*\) and \(m \in \mathbb{Z} \setminus \{0\}\). Hence \(1 = f^n = v^n t_i^{m n}\) and thus \(t_i\) is not algebraically independent over \(F(t_1) \cdots (t_{i-1})\); a contradiction. Consequently, if \(f\) depends on \(\Pi\)-monomials, \(\text{ord}(f) = 0\). Otherwise, \(f = u t_1^{m_1} \cdots t_r^{m_r}\) with \(m_i \in \mathbb{N}\) where the \(t_i\) are all \(R\)-monomials. Therefore the value \(\text{ord}(f)\) can be computed by Corollary 5.5. \(\square\)
6. The algorithmic machinery II: Problem PMT

We aim at proving Theorems 3.1 and 5.2, i.e., providing recursive algorithms that reduce Problem PMT from a given \( \Pi \Sigma^* \)-extension to its ground ring (resp. field). For this reduction we assume that for the given ground ring \((\mathcal{G}, \sigma)\) and given group \(G \leq \mathcal{G}^*\) we have that \(\text{const} \mathcal{G} \setminus \{0\} \leq \mathcal{G}^*\). This property guarantees that for any \(f \in \mathcal{G}^n\) a \(\mathbb{Z}\)-basis of \(M(f, \mathcal{G})\) with rank \(\leq n\) exists; see Lemma 3. In particular, we rely on the fact that there are algorithms available that solve Problem PMT in \((\mathcal{G}, \sigma)\) for \(G\).

6.1. A reduction strategy for \(\Pi \Sigma^*\)-extensions

First, we treat the reduction for \(\Pi \Sigma^*\)-extensions. More precisely, we will obtain

**Theorem 17.** Let \((\mathcal{G}, \sigma)\) be a computable difference ring and \(G \leq \mathcal{G}^*\) with \(\text{const} \mathcal{G} \setminus \{0\} \leq \mathcal{G}^*\). Let \((\mathcal{E}, \sigma)\) be a \(G\)-simple \(\Pi \Sigma^*\)-extension of \((\mathcal{G}, \sigma)\). Then \(\text{const} \mathcal{G} \setminus \{0\} \leq \mathcal{E}^*\) and Problem PMT is solvable in \((\mathcal{E}, \sigma)\) for \(G\).

For the underlying reduction method we use the following two lemmas.

**Lemma 23.** Let \((\mathcal{A}(t), \sigma)\) be a \(\Sigma^*\)-extension of \((\mathcal{A}, \sigma)\) and let \(H \leq \mathcal{A}^*\) be a group such that \(\text{const} \mathcal{H} \mathcal{A} \setminus \{0\} \leq \mathcal{A}^*\). Then for \(f \in H^n\) we have that \(M(f, \mathcal{A}(t)) = M(f, \mathcal{A})\).

**Proof.** The inclusion \(\subseteq\) is clear. Let \((m_1, \ldots, m_n) \in M(f, \mathcal{A}(t))\) with \(f = (f_1, \ldots, f_n) \in H^n\). Then for \(g \in \mathcal{A}(t) \setminus \{0\}\) with \(\sigma(g) = f_1^m \cdots f_n^m\) we have that \(g \in \text{const} \mathcal{H} \mathcal{A} \setminus \{0\}\) and thus by Theorem 7 we have that \(g \in \text{const} \mathcal{H} \mathcal{A}\). Consequently, \(g \in M(f, \mathcal{A})\).

**Lemma 24.** Let \((\mathcal{A}(t), \sigma)\) be a \(\Pi\)-extension of \((\mathcal{A}, \sigma)\) and let \(H \leq \mathcal{A}^*\) with \(\text{const} \mathcal{H} \mathcal{A} \setminus \{0\} \leq \mathcal{A}^*\) and \(\alpha := \sigma(t)/t \in H\). Let \(f = (f_1, \ldots, f_n) \in (H^\mathcal{A}(t))^n\) with \(f_i = h_i t^{e_i}, \quad h_i \in H, \quad e_i \in \mathbb{Z}\).

Then \(M(f, \mathcal{A}(t)) = M_1 \cap M_2\) where

\[
M_1 = \{(m_1, \ldots, m_n) | (m_1, \ldots, m_n, m_{n+1}) \in M((h_1, \ldots, h_n, \frac{1}{t}), \mathcal{A})\},
\]

\[
M_2 = \text{Ann}_\mathbb{Z}(e_1, \ldots, e_n) = \{(m_1, \ldots, m_n) \in \mathbb{Z}^n | m_1 e_1 + \cdots + m_n e_n = 0\}.
\]

**Proof.** Let \((m_1, \ldots, m_n) \in M(f, \mathcal{A}(t))\). Hence we can take \(g \in \mathcal{A}(t) \setminus \{0\}\) with \(\sigma(g) = f_1^m \cdots f_n^m\) and \(g \in \text{const} \mathcal{H} \mathcal{A} \setminus \{0\}\) with \(H = H^\mathcal{A}(t)\). Thus by Theorem 12 it follows that \(g = \hat{g} t^m\) with \(m \in \mathbb{Z}\) and \(\hat{g} \in \text{const} \mathcal{H} \mathcal{A} \setminus \{0\}\). Hence \(\sigma(\hat{g}) = f_1^{m_1} \cdots f_n^{m_n} \alpha^{-m} \hat{g} = h_1^{m_1} \cdots h_n^{m_n} \alpha^{-m} \hat{g} t^{m_1 e_1 + \cdots + m_n e_n}\).

Since \(\hat{g} \neq 0\), we conclude that \(\sigma(\hat{g}) \neq 0\). By coefficient comparison it follows then that \(m_1 e_1 + \cdots + m_n e_n = 0\), i.e., \((m_1, \ldots, m_n) \in M_2\). Thus \(\sigma(\hat{g}) = h_1^{m_1} \cdots h_n^{m_n} \alpha^{-m} \hat{g}\) and consequently \((m_1, \ldots, m_n) \in M((h_1, \ldots, h_n, \frac{1}{t}), \mathcal{A})\), i.e., \((m_1, \ldots, m_n) \in M_1\).

**Proof of Theorem 17.** Let \((\mathcal{G}, \sigma)\) be a difference ring and let \(G \leq \mathcal{G}^*\) such that \(\text{const} \mathcal{G} \setminus \{0\} \leq \mathcal{G}^*\) and suppose that Problem PMT is solvable in \((\mathcal{G}, \sigma)\) for \(G\). Now
let \((E, \sigma)\) be a \(G\)-simple \(\Pi\Sigma^*\)-extension of \((G, \sigma)\) as in the theorem with \(\tilde{G} = G^n_G\) and let \(f \in G^n\). By Corollary 2.1 it follows that \(\text{sconst}_G E \setminus \{0\} \leq E^*\) and together with Lemma 3 it follows that \(M(f, E) = M(f, \text{sconst}_G E)\) is a \(\mathbb{Z}\)-module. The calculation of a basis of \(M(f, E)\) will be accomplished by recursion/induction. If \(E = A\), nothing has to be shown. Otherwise, let \((A, \sigma)\) be a \(G\)-simple \(\Pi\Sigma^*\)-extension of \((G, \sigma)\) in which we know how one can solve Problem PMT for \(H = G^n_G\), and let \(E = A(t)\) where \(t\) is a \(H\)-simple \(\Pi\Sigma^*-\)monomial. We have to treat two cases. First, suppose that \(t\) is a \(\Sigma^*\)-monomial. Then it follows that \(\tilde{G} = G^n_G = G^n = H \leq A^*\) and thus \(f \in H^n\). Hence we can activate Lemma 23 and it follows that \(M(f, E) = M(f, A)\). Thus by assumption we can compute a basis. Second, suppose that \(t\) is a \(H\)-simple \(\Pi\)-monomial. Then we can utilize Lemma 24: We calculate a basis of \(M_2\) by linear algebra. Moreover, we compute a basis of \(M((h_1, \ldots, h_n, \frac{1}{t}), A)\) by the induction assumption (by recursion). Hence we can derive a basis of \(M_2\) and thus of \(M_1 \cap M_2 = M(f, A(t))\). This completes the proof. \(\Box\)

Note that the reduction presented in Lemma 24 is accomplished by increasing the dimension of \(M_1\) by one. In general, the more \(\Pi\)-monomials are involved, the higher the dimension will be in the arising Problems PMT.

Looking closer at the reduction algorithm, we can extract the following shortcut, resp. a refined version of Theorem 1.2.

**Corollary 6.** Let \((A, \sigma)\) be a difference ring and \(G \leq A^*\) be a group such that \(\text{sconst}_G A \setminus \{0\} \leq A^*\). Let \((H, \sigma)\) be a \(G\)-simple \(\Pi\)-extension of \((A, \sigma)\) and let \((E, \sigma)\) be a \(\Sigma^*\)-extension of \((H, \sigma)\). Then \(G^n_A = G^n_A\) and the following holds.

1. \(M(f, E) = M(f, H)\) for any \(f \in (G^n_A)^n\).
2. Let \(\alpha \in G^n_A\). There is a \(\Pi\)-extension \((E(t), \sigma)\) of \((E, \sigma)\) with \(\sigma(t) = \alpha \cdot t\) iff there is a \(\Pi\)-extension \((H(t), \sigma)\) of \((H, \sigma)\) with \(\sigma(t) = \alpha \cdot t\).

**Proof.** Note that \(G^n_A \leq H^*\). Hence by iterative application of Lemma 23 the first statement is proven. The second statement follows by statement 1 and Theorem 1.2. \(\Box\)

The following remark is in place. If one restricts to the special case that \((G, \sigma)\) is a \(\Pi\Sigma^*\)-field with \(G = G^*\), the presented reduction techniques boil down to the reduction presented in [24, Theorem 8]. The major contribution here is that Theorem 17 can be applied for any computable difference ring \((G, \sigma)\) with the properties given in Theorem 17. Subsequently, we utilize this additional flexibility to tackle (nested) \(R\)-extensions.

### 6.2. A reduction strategy for \(R\)-extensions and thus for \(R\Pi\Sigma^*\)-extensions

First, we treat the special case where the \(R\)-extensions are single-rooted.

**Lemma 25.** Let \((A, \sigma)\) be a difference ring and \(G \leq A^*\) with \(\text{sconst}_G A \setminus \{0\} \leq A^*\). Let \((A[x], \sigma)\) be an \(R\)-extension of \((A, \sigma)\) with \(\sigma(x) = \alpha x\) where \(\alpha \in G\); let \(f = (f_1, \ldots, f_n) \in G^n\). Then \(M(f, A[x]) = \{(m_1, \ldots, m_n) | (m_1, \ldots, m_{n+1}) \in M((f_1, \ldots, f_n, \frac{1}{\alpha}), A)\} \).

**Proof.** Let \((m_1, \ldots, m_n) \in M(f, A[x])\). Hence there is a \(g \in \text{sconst}_G A[x] \setminus \{0\}\) with \(\sigma(g) = f_1^{m_1} \cdots f_n^{m_n} g\). By Theorem 14 it follows that \(g = \tilde{g} x^m\) with \(\tilde{g} \in A \setminus \{0\}\) and \(m \in \mathbb{N}\). Thus

\[
\sigma(\tilde{g}) = f_1^{m_1} \cdots f_n^{m_n} \alpha^{-m} \tilde{g}
\]

and hence \((m_1, \ldots, m_n, -m) \in M((f_1, \ldots, f_n, \frac{1}{\alpha}), A)\). Conversely, if \((m_1, \ldots, m_n, -m) \in M((f_1, \ldots, f_n, 1/\alpha), A)\), there is a \(\tilde{g} \in A \setminus \{0\}\) with (28). Therefore we conclude that \(\sigma(\tilde{g} x^m) = f_1^{m_1} \cdots f_n^{m_n} \tilde{g} x^m\) which implies \((m_1, \ldots, m_n) \in M(f, A[x])\). \(\Box\)
As a consequence we obtain the

**Proof of Theorem 3.1 (see page 13).** Since Problem PMT is solvable in \((\mathbb{G}, \sigma)\) for \(G\), it follows by Theorem 17 that Problem PMT is solvable in \((\mathbb{H}, \sigma)\) for \(\tilde{G}\) with \(\mathbb{H} = \mathbb{G}\langle t_1 \rangle \ldots \langle t_r \rangle\) and that \(\text{sconst}_G \mathbb{H} \setminus \{0\} \leq \mathbb{H}^*\). Thus by iterative applications of Lemma 25 and Theorem 14 we conclude that Problem PMT is solvable in \((\mathbb{H}, \sigma)\) for \(\tilde{G}\) with \(\mathbb{H} = \mathbb{H}\langle x_1 \rangle \ldots \langle x_u \rangle\) and that \(\text{sconst}_G \mathbb{H} \setminus \{0\} \leq \mathbb{H}^*\). Finally, by applying again Theorem 17 it follows that Problem PMT is solvable in \((\mathbb{E}, \sigma)\) for \(\tilde{G}\). 

In order to tackle the more general case that the \(R\)-extensions are nested (and that they might occur also in \(\Pi\)-extensions), we require additional properties on the difference rings: they must be strong constant-stable; see Definition 6. In order to derive the underlying algorithms in Theorem 5.2 below, we utilize the following structural property of the semi-constants. They factor into two parts: a factor which depends only on the \(R\)-monomials with constant coefficients and a factor which is free of the \(R\)-monomials.

**Lemma 26.** Let \((\mathbb{A}, \sigma)\) be a difference ring which is constant-stable and let \(G \leq \mathbb{A}^\ast\) being closed under \(\sigma\) and where \(\text{sconst}_G (\mathbb{A}, \sigma^k) \setminus \{0\} \leq \mathbb{A}^\ast\) for any \(k > 0\). Let \((\mathbb{E}, \sigma)\) be a simple \(R\)-extension of \((\mathbb{A}, \sigma)\) with \(\mathbb{E} = \mathbb{A}[x_1, \ldots, x_e]\) where we have (27) with \(m_{i,j} \in \mathbb{N}\) and \(u_i \in G\) with \(\text{per}(u_i) > 0\). Define

\[
\begin{align*}
    r := \begin{cases} 
        \text{lcm}(\text{ford}(u_1), \ldots, \text{ford}(u_e), \text{ford}(x_1), \ldots, \text{ford}(x_e)) & \text{if } e > 0 \\
        1 & \text{if } e = 0.
    \end{cases}
\end{align*}
\]

(29)

Let \(\tilde{G} = G^\ast\) with \(\text{sconst}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*\). Then: (1) \(r > 0\). (2) For any \(g \in \text{sconst}_G \mathbb{E} \setminus \{0\}\),

\[
g = \tilde{g} h
\]

(30)

with \(\tilde{g} \in \text{sconst}_G (\mathbb{A}, \sigma^r) \setminus \{0\} \leq \mathbb{A}^\ast\) and \(h \in \text{const}(\mathbb{E}[x_1, \ldots, x_e], \sigma^r)^\ast\).

(3) If \(\sigma(g) = v x_1^{m_1} \ldots x_e^{m_e} g\) with \(v \in G\), \(m_i \in \mathbb{N}\), then \(\sigma(\tilde{g}) = \lambda v \tilde{g}\) with \(\lambda \in \mathbb{A}^\ast\), \(\lambda^r = 1\).

**Proof.** Let \(g \in \text{sconst}_G \mathbb{E} \setminus \{0\}\), i.e., \(\sigma(g) = v x_1^{m_1} \ldots x_e^{m_e} g\) with \(v \in G\) and \(m_i \in \mathbb{Z}\). Let \(r\) be given as in (29). If \(e = 0\), i.e., \(r = 1\), the lemma holds by taking \(\tilde{g} := g \in \mathbb{A}^\ast\) and \(h = 1\). Otherwise, we may suppose that \(e > 0\).

(1) Let \(1 \leq i \leq e\). By Proposition 3.1 it follows that \(\text{ord}(u_i) > 0\). Together with the assumption that \(\text{per}(u_i) > 0\) we have that \(\text{ford}(u_i) > 0\) by Lemma 20.3. Moreover, by Proposition 3.2 it follows that \(\text{per}(x_i) > 0\). Again with \(\text{ord}(x_i) > 0\) and \(\text{per}(x_i)\) it follows that \(\text{ford}(x_i) > 0\) by Lemma 20.3. Therefore \(r > 0\).

(2) By the choice of \(r\) it follows that for all \(1 \leq i \leq e\) we have

\[
(u_i)_{(r)} = 1, \quad (x_i)_{(r)} = 1 \quad \text{and} \quad \sigma^r(x_i) = x_i;
\]

(31)

the last equality follows by Lemma 22.3. Moreover, by Lemma 6 we conclude that

\[
\sigma^r(g) = (v x_1^{m_1} \ldots x_e^{m_e})_{(r)} g = v_{(r)} (x_1)_{(r)}^{m_1} \ldots (x_e)_{(r)}^{m_e} g = \tilde{u} g
\]

with \(\tilde{u} := v_{(r)}\). Since \(G\) is closed under \(\sigma\), we have that \(\tilde{u} \in G\). Write \(g = \sum_{s \in S} g_s x^s\) where \(S \subseteq \mathbb{N}^e\) is finite, \(g_s \in \mathbb{F}^\ast\) and for \((s_1, \ldots, s_e) \in S\) and \(x = (x_1, \ldots, x_e)\) we use the multi-index notation \(x^s = x_1^{s_1} \ldots x_e^{s_e}\). In particular, we suppose that if \(s, s' \in S\) with \(x^s = x^{s'}\) then \(s = s'\). Then by coefficient comparison w.r.t. \(x^t\) and using (31) we obtain

\[
\sigma^r(g_i) = \tilde{u} g_i \quad \text{for any } i \in S.
\]

Note that \(g_i \in \text{sconst}_G (\mathbb{A}, \sigma^r) \setminus \{0\} \leq \mathbb{A}^\ast\). Hence for any \(s, r \in \mathbb{Z}^e\)
We have that \( \sigma^r(\frac{g_s}{g_r}) = \frac{g_s}{g_r} \). Thus it follows that \( \frac{g_s}{g_r} \in \operatorname{cons}(\Lambda, \sigma^r) \) for all \( s \in S \) we have that \( g_s = c_s \tilde{g} \) for some \( c_s \in \mathbb{K}^* \) with \( \sigma^r(\tilde{g}) = \tilde{u} \tilde{g} \).

Consequently, \( g = \tilde{g} h \) with \( h = \sum_{s \in S} c_s x^s \). Since \( g \in \mathbb{K}^* \), \( h \in \mathbb{K}[x_1, \ldots, x_e]^* \). Finally, with \( (31) \) we conclude that \( h \in \operatorname{cons}(\mathbb{K}[x_1, \ldots, x_e], \sigma^r)^* \).

(3) Taking \( s = (s_1, \ldots, s_e) \in S \), it is easy to see that there is exactly one \( s' \in S \) such that

\[
\sigma(c_s x^s g) = v x_1^{m_1} \cdots x_e^{m_e} c_{s'} x^{s'}.
\]

This means that on both sides the same monomial \( x^{s''} \) in reduced form occurs. By coefficient comparison this gives \( \sigma(\tilde{g}) = v u_1^{s_1} \cdots u_e^{s_e} \tilde{g} \). Thus with \( (31) \) and Lemma 6 we get \( \sigma^r(\tilde{g}) = v (\frac{\tilde{u}}{u_1^{s_1} \cdots u_e^{s_e}})^r \tilde{g} \). Hence with \( (32) \) we obtain \( (\frac{\tilde{u}}{u_1^{s_1} \cdots u_e^{s_e}})^r = 1 \).

Finally, with \( \lambda := u_1^{s_1} \cdots u_e^{s_e} \tilde{g} \) we have that \( \sigma(\tilde{g}) = \lambda v \tilde{g} \) with \( \lambda^r = 1 \) and \( \lambda \in \Lambda^* \). \( \square \)

Specializing \( \Lambda \) to a strong constant-stable difference field \( \mathbb{F} \), the lemma reads as follows.

**Corollary 7.** Let \( (\mathbb{F}, \sigma) \) be a difference field with \( \mathbb{K} = \operatorname{const} \mathbb{F} \) which is strong constant-stable. Let \( (\mathbb{E}, \sigma) \) be a simple \( R \)-extension of \( (\mathbb{F}, \sigma) \) with \( \mathbb{E} = \mathbb{F}[x_1, \ldots, x_e] \) such that \( (27) \) with \( m_{i,j} \in \mathbb{N} \), \( u_i \in \mathbb{K}^* \), and define \( (29) \). Let \( G = (\mathbb{F}^*)^S \). Then: (1) \( r > 0 \).

(2) For any \( g \in \operatorname{const} \mathbb{E} \setminus \{0\} \) we have \( (30) \) with \( \tilde{g} \in \mathbb{K}^* \) and \( h \in \mathbb{K}[x_1, \ldots, x_e], \sigma^r)^* \).

(3) If \( \sigma(g) = v x_1^{m_1} \cdots x_e^{m_e} g \) with \( v \in \mathbb{F}^* \), \( m_i \in \mathbb{Z} \), then \( \sigma(g) = \lambda v \tilde{g} \) with \( \lambda \in \mathbb{K}^* \), \( \lambda^r = 1 \).

**Proof.** Since \( u_i \in \mathbb{K}^* \) by Corollary 5.1, \( \operatorname{per}(u_i) = 1 \). Define \( G = \mathbb{F}^* \) which is closed under \( \sigma \). In particular, \( \operatorname{const} \mathbb{F}(\mathbb{F}, \sigma^k) \setminus \{0\} = \mathbb{F}^* \) for any \( k > 0 \). Moreover, by Corollary 1 it follows that \( \operatorname{const} \mathbb{E}(\mathbb{E}, \sigma^r) \setminus \{0\} \leq \mathbb{E}^* \). Thus we may apply Lemma 26. The corollary follows by observing that \( \lambda \in \mathbb{K}^* \) with \( \lambda^r = 1 \). Then by our assumption it follows that \( \lambda \in \mathbb{K}^* \). \( \square \)

With this result we get the following reduction tactic for simple \( R \)-extensions.

**Lemma 27.** Let \( (\mathbb{F}, \sigma) \) be a difference field with \( \mathbb{K} = \operatorname{const} \mathbb{F} \) which is strong constant-stable. Let \( (\mathbb{E}, \sigma) \) be a simple \( R \)-extension of \( (\mathbb{F}, \sigma) \) with \( \mathbb{E} = \mathbb{F}[x_1, \ldots, x_e] \) where we have \( (27) \) with \( m_{i,j} \in \mathbb{N} \) and \( u_i \in \mathbb{K}^* \). Define \( r > 0 \) as given in \( (29) \) and choose a set \( \{\alpha_1, \ldots, \alpha_s\} \) of \( r \)-th roots of unity which generate multiplicatively all \( r \)-th roots of unity of \( \mathbb{K} \). Let \( G = (\mathbb{F}^*)^S \) and let \( f = (f_1, \ldots, f_n) \in G^n \) with \( f_i = \tilde{f}_i h_i \) where \( \tilde{f}_i \in \mathbb{F}^* \) and \( h_i = x_1^{z_{i,1}} \cdots x_e^{z_{i,e}} \) with \( z_{i,j} \in \mathbb{N} \). Then

\[
M(f, \mathbb{E}) = \{(m_1, \ldots, m_n) | (m_1, \ldots, m_{n+s}) \in M_1 \cap M_2\}
\]

where

\[
M_1 = M((f_1, \ldots, f_n, \alpha_1, \ldots, \alpha_s), \mathbb{F})
\]

\[
M_2 = M((h_1, \ldots, h_n, \frac{1}{\alpha_1}, \ldots, \frac{1}{\alpha_s}), \mathbb{K}[x_1] \cdots [x_e]).
\]

\footnote{In principal, we could also take one primitive \( r \)-th root of unity \( \alpha \). However, if \( \alpha \notin \mathbb{K} \), we have to extend the constant field. By efficiency reasons we prefer to stay in the original field. We remark that extending the constant field will not change the possibility to find more relations.}
Proof. Let \((m_1, \ldots, m_n) \in M(f, \mathbb{E})\), i.e., there is a \(g \in \text{scost}_G \mathbb{E} \setminus \{0\}\) with \(\sigma(g) = f_1^{m_1} \cdots f_n^{m_n} g\). Hence by Corollary 7 it follows that \(g = \tilde{g} h\) with \(\tilde{g} \in \mathbb{F}^*\) and \(h \in \mathbb{K}[x_1] \ldots [x_e]^*\). In particular, \(\sigma(\tilde{g}) = f_1^{m_1} \cdots f_n^{m_n} \lambda \tilde{g}\) for \(\lambda \in \mathbb{K}^*\) being an \(r\)th root of unity. Hence we can take \(m_{n+1}, \ldots, m_{n+s} \in \mathbb{N}\) such that \(\lambda = \alpha_1^{m_{n+1}} \cdots \alpha_s^{m_{n+s}}\). Consequently,

\[
\sigma(\tilde{g}) = f_1^{m_1} \cdots f_n^{m_n} \alpha_1^{m_{n+1}} \cdots \alpha_s^{m_{n+s}} \tilde{g},
\]

which yields

\[
\sigma(h) = f_1^{m_1} \cdots f_n^{m_n} \alpha_1^{-m_{n+1}} \cdots \alpha_s^{-m_{n+s}} h.
\]

Then (34) and (35) imply \((m_1, \ldots, m_{n+s}) \in M_1 \cap M_2\). Conversely, let \((m_1, \ldots, m_n) \in M_1 \cap M_2\). I.e., there are \(m_i \in \mathbb{N}\), \(\tilde{g} \in \mathbb{F}^*\) and \(h \in \mathbb{K}[x_1] \ldots [x_e]^*\) s.t. (34) and (35) hold. Therefore \(\sigma(\tilde{g} h) = f_1^{m_1} \cdots f_n^{m_n} \tilde{g} h\) which implies that \((m_1, \ldots, m_n) \in M(f, \mathbb{E})\). \(\square\)

**Example 13.** Take the \(\Pi \Sigma^*\)-field \((\mathbb{K}(k), \sigma)\) over \(\mathbb{K} = \mathbb{Q}(\iota)\) with \(\sigma(k) = k + 1\) and consider the \(R\)-extension \((\mathbb{K}(k)[x], \sigma)\) of \((\mathbb{K}(k), \sigma)\) with \(\sigma(x) = \iota x\) and \(\text{ord}(x) = 4\) from Example 4. In order to obtain a degree bound in Example 16 below, we need a basis of \(M = M(f, \mathbb{K}(k)[x])\) with \(f = (k x, -\frac{1}{3} k^2)\). Here we will apply Lemma 27. By Example 12.3 we get \(\text{ord}(x) = 8\). With \(u_1 = 1\) we determine \(r = 8\) by (29). We define \(f_1 = k\), \(f_2 = -1/(k + 1)\) and \(h_1 = h_2 = x\). All 8th roots of unity of \(\mathbb{K}\) are generated by \(\alpha_1 = \iota\). As worked out in the above lemma, we have to determine a basis of \(M_1 = M((f_1, f_2, \alpha_1), \mathbb{K}(k)) = M(k, -\frac{1}{3}, \iota, \mathbb{K}(k))\). Here we use, e.g., the algorithms worked out in [24] (this is the base case of our machinery) and obtain the basis \(\{(1, 1, 2), (0, 0, 4)\}\). Moreover, we compute the basis \(\{(1, 1, 0), (2, 0, 0), (0, 0, 1)\}\) of \(M_2 = M((h_1, h_2, \alpha_1), \mathbb{K}[x]) = M((x, x, \iota), \mathbb{K}[x])\), for details see Example 14 below. Thus a basis of \(M_1 \cap M_2\) is \(\{(1, 1, 2), (0, 0, 4)\}\) and we conclude that \(\{(1, 1)\}\) is a basis of \(M\).

Note that \(\text{scost}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^*\) by Corollary 1 and thus \(M(f, \mathbb{E})\) in Lemma 27 has a \(\mathbb{Z}\)-basis with rank \(\leq n\). In particular, we can compute such a basis as follows. First note that both \(M_1\) and \(M_2\) given in Lemma 27 have \(\mathbb{Z}\)-bases with rank \(\leq n + s\): for \(M_1\) this follows since \(\mathbb{F}\) is a field. Moreover, if one takes \(\mathbb{H} = \mathbb{K}[x_1] \ldots [x_e] \leq \mathbb{E}\) and \(H = (\mathbb{K}^*)_{\mathbb{H}}\), it follows by Corollary 1 that \(\text{scost}_H \mathbb{H} \setminus \{0\} \leq \mathbb{H}^*\) and thus a \(\mathbb{Z}\)-basis exists. Summarizing, we can determine a \(\mathbb{Z}\)-basis of \(M(f, \mathbb{E})\) by using (33) after we obtained bases of \(M_1\) and \(M_2\). By assumption (i.e., the base case in our recursion) a basis of \(M_1\) can be determined. The calculation of a \(\mathbb{Z}\)-basis of \(M_2\) can be accomplished by the following proposition.

**Proposition 4.** Let \((\mathbb{H}, \sigma)\) with \(\mathbb{H} = \mathbb{K}[x_1] \ldots [x_e]\) be a simple \(R\)-extension of \((\mathbb{K}, \sigma)\) with a computable constant field \(\mathbb{K}\) and given \(\alpha_i = \text{ord}(x_i)\) for \(1 \leq i \leq e\). Define \(G = (\mathbb{K}^*)^H\) and let \(f = (f_1, \ldots, f_n) \in G^n\) with given \(\lambda_i = \text{ord}(f_i) > 0\) for \(1 \leq i \leq n\). Then a basis of \(M(f, \mathbb{H})\) can be computed.

**Proof.** Define the finite sets

\[G := \{(m_1, \ldots, m_e) \in \mathbb{N}^e | 0 \leq m_i < \alpha_i\}\]

and \(\tilde{M} := \{(m_1, \ldots, m_n) \in \mathbb{N}^n | 0 \leq m_i < \lambda_i\}\).

Then loop through all vectors \(m = (m_1, \ldots, m_n) \in \tilde{M}\) and check if there is a \(g \in \mathbb{H}^*\) with \(\sigma(g) = f_1^{m_1} \cdots f_n^{m_n} g\). More precisely, we can make the Ansatz \(g = \sum_{i \in G} \gamma_i \mathbb{K}^\mathbb{I}\) which leads to a linear system of equations in the \(\gamma_i\) with coefficients from \(\mathbb{K}\). Solving this system gives the solution space of \(L\) and we can check if the considered \(m\) from \(\tilde{M}\) is contained in

\[\mathbb{L}\]
\[ M(f, \mathbb{H}) \]. In this way we can generate the subset \( M' = \tilde{M} \cap M(f, \mathbb{H}) \). Denote by \( b_i \in \mathbb{K}^n \) the \( i \)th unit vector. We show that
\[ \text{span}(M' \cup \{ \lambda_1 b_1, \ldots, \lambda_n b_n \}) = M(f, \mathbb{H}). \] (36)

Namely, since \( M(f, \mathbb{H}) \) is a \( \mathbb{Z} \)-module (see the remarks above the proposition) and since \( \lambda_i b_i \in M(f, \mathbb{H}) \), the left hand side is contained in the right hand side. Conversely, suppose that \( (m_1, \ldots, m_n) \in M(f, \mathbb{H}) \). Then let \( m'_i = m_i \mod \lambda_i \), i.e., \( 0 \leq m'_i < \lambda_i \) with \( m_i = m'_i + z_i \lambda_i \) for some \( z_i \in \mathbb{Z} \). Thus \( (m_1, \ldots, m_n) = (m'_1, \ldots, m'_n) + (\lambda_1 z_1, \ldots, \lambda_n z_n) \) where \( (m'_1, \ldots, m'_n) \in M \) and \( (\lambda_1 z_1, \ldots, \lambda_n z_n) = z_1 (\lambda_1 b_1) + \cdots + z_n (\lambda_n b_n) \). Consequently, \( (m_1, \ldots, m_n) \) is an element of the left hand side of (36). Since the number of vectors of the span on the left hand side is finite, we can derive a \( \mathbb{Z} \)-basis of (36). \( \square \)

**Remark 2.** A basis of \( M(f, \mathbb{H}) \) can be obtained more efficiently as follows. We start with a vector space which is given by the basis \( B = \{ \lambda_1 b_1, \ldots, \lambda_n b_n \} \) where \( b_i \notin \mathbb{K}^n \) is the \( i \)th unit vector. Now go through all elements from \( M \). Take the first element \( m \) from \( M \). If it is in \( \text{span}(B) \) (this can be easily checked), proceed to the next element. Otherwise, if it is an element from \( M(f, \mathbb{H}) \) (for the check see the proof of Proposition 4), put it in \( B \) and transform the set again to a \( \mathbb{Z} \)-basis. More precisely, the rows of the matrix should give a matrix which is in Hermite normal form. In this way, one can again check easily if an element is in \( \text{span}(B) \). We proceed until all elements of \( M \) are visited and update step by step \( B \) as described above. By construction we have that our \( \text{span}(B) \) equals the left hand side of (36) and thus equals \( M(f, \mathbb{H}) \). We remark that \( B \) consists always of \( e \) linearly independent vectors. However, the \( \mathbb{Z} \)-span is more and more refined.

**Example 14** (Cont. Ex. 13). Take the \( R \)-extension \( (\mathbb{K}[x], \sigma) \) of \( (\mathbb{K}, \sigma) \) with \( \mathbb{K} = \mathbb{Q}(\iota) \), \( \sigma(x) = \iota x \) and \( \text{ord}(x) = 4 \). We calculate a basis of \( M(f, \mathbb{K}[x]) \) with \( f = (x, x, \iota) \) as presented in Remark 2. We start with \( \{ (4, 0, 0), (0, 4, 0), (0, 0, 4) \} \) whose rows form a matrix in Hermite normal form. Now we go through all elements of \( M \), say in the order
\[ \tilde{M} = \{ (1, 0, 0), (2, 0, 0), (3, 0, 0), (0, 1, 0), (0, 2, 0), (0, 3, 0), (0, 0, 1), (0, 0, 2), (0, 0, 3), (1, 1, 0), \ldots \}. \]

Since \( (1, 0, 0) \notin \text{span}(B) \), we check if there is a \( g \in \mathbb{K}[x] \setminus \{ 0 \} \) with \( \sigma(g) = x^4 x^0 \iota^0 g \); this is not the case. We continue with \( (2, 0, 0) \). Here we have that \( (2, 0, 0) \notin \text{span}(M) \).

Now we check if there is a \( g \in \mathbb{K}[x] \setminus \{ 0 \} \) with \( \sigma(g) = x^2 x^0 \iota^0 g \). Plugging in \( g = g_0 + g_1 x + g_2 x^2 + g_3 x^3 \) into \( \sigma(g) = x^2 g \) gives the constraint \( (g_0 - g_2) x^0 + \iota x (g_1 + i g_3) + x^2 (g_0 - g_2) + x^3 (-g_1 - i g_3) = 0 \) which leads to the solution \( g = x + \iota x^3 \).

A basis of \( \text{span}(B \cup \{ (2, 0, 0) \}) \) is \( \{ (2, 0, 0), (0, 4, 0), (0, 0, 4) \} \). Thus we update \( B \), i.e., \( B = \{ (2, 0, 0), (0, 4, 0), (0, 0, 4) \} \). We have \( (3, 0, 0) \notin \text{span}(B) \), but there is no \( g \in \mathbb{K}[x] \setminus \{ 0 \} \) with \( \sigma(g) = x^3 g \). Similarly to \( (1, 0, 0) \), also \( (0, 1, 0) \) does not change \( B \), and similarly to \( (2, 0, 0) \), \( (0, 2, 0) \) leads to the updated basis \( B = \{ (2, 0, 0), (0, 2, 0), (0, 0, 4) \}, (0, 3, 0) \) does not change \( B \). However, for \( (0, 0, 1) \notin \text{span}(B) \) we find \( g = x \) with \( \sigma(g) = x^0 x^0 \iota^1 g \) which yields \( B = \{ (2, 0, 0), (0, 2, 0), (0, 0, 1) \} \). We have that \( (0, 0, 2), (0, 0, 3) \in \text{span}(B) \).

Now we consider \( (1, 1, 0) \notin \text{span}(B) \). We find \( g = x + \iota x^3 \) with \( \sigma(g) = x^2 g \) (as already above). Hence we update \( B \) to \( B = \{ (1, 1, 0), (0, 2, 0), (0, 1, 0) \} \) (where the rows form a matrix in Hermite normal form). As it turns out, no further elements form \( M \) leads to a modification of \( B \). Thus \( B \) is a basis of \( V(1, f, \mathbb{K}[x]) \).

**Proof of Theorem 5.2 (see page 13).** By Lemma 18 we can reorder the generators of the \( \mathbb{R} \mathbb{H} \Sigma^* \)-extension such that \( (\mathbb{E}, \sigma) \) is an \( \mathbb{F}^* \)-simple \( R \)-extension of \( (\mathbb{F}, \sigma) \) and \( (\mathbb{E}, \sigma) \)
is a $G$-simple $\Pi\Sigma^*$-extension of $(\bar{E}, \sigma)$ with $G = (\bar{F}^*)^0_F$. Let $\bar{E} = F[x_1, \ldots, x_e]$ with $u_0$, $\alpha$, and $f \in G^n$ with $f_i$ and $h_n$ as given in Lemma 27. By assumption we can compute a basis of $M_1$ as given in Lemma 27. Since Problem $O$ is solvable in $K^*$, we can compute $o_i = \text{ord}(x_i)$ and $\lambda_i = \text{ord}(u_i)$ by Corollary 5.4. Thus we can use Proposition 4 to compute a basis of $M_2$ as posed in Lemma 27. Hence we can compute a basis of $(33)$. Summarizing, we can solve Problem PMT in $(\bar{E}, \sigma)$ for $G$. In particular, we have that $\text{const}_G \bar{E} \setminus \{0\} \leq \bar{E}^*$ by Corollary 1. Hence by Theorem 17 we can solve Problem PMT for $(\bar{E}, \sigma)$ in $G^0_{\bar{E}}$. Since $G^0_{\bar{E}} = (\bar{F}^*)^0_F$ by Lemma 17, the theorem is proven. 

To this end, we work out the following shortcut, resp. refined version of Theorem 1.3.

**Corollary 8.** Let $(\bar{F}, \sigma)$ be a strong constant-stable difference field with constant field $K$, and let $G \leq \bar{F}^*$ be a group with $\text{const}_G \bar{F} \setminus \{0\} \leq \bar{F}^*$. Let $(\bar{H}, \sigma)$ with $H = F[x_1, \ldots, x_r]$ be a $G$-simple $R$-extension of $(\bar{A}, \sigma)$ and let $(\bar{E}, \sigma)$ be a $G^0_{\bar{E}}$-simple $\Pi\Sigma^*$-extension of $(\bar{H}, \sigma)$.

1. If $f \in G^0_{\bar{H}}$ with $\text{ord}(f) > 0$, then $f \in (K^* \cap G)^0_{\bar{F}}$.
2. $M(f, \bar{E}) = M(f, K[x_1, \ldots, x_r])$ for any $f = (f_1, \ldots, f_n) \in (G^0_{\bar{H}})^n$ with $\text{ord}(f_i) > 0$.
3. Let $\alpha \in G^0_{\bar{H}}$ with $\text{ord}(\alpha) > 0$. Then there is an $R$-extension $(\bar{E}(t), \sigma)$ of $(\bar{E}, \sigma)$ with $\frac{\tau(\alpha)}{\alpha} = \alpha$ iff there is an $R$-extension $(\bar{H}(x_1, \ldots, x_r), \sigma)$ of $(K[x_1, \ldots, x_r], \sigma)$ with $\frac{\tau(\alpha)}{\alpha}$.

**Proof.**

1. Let $f \in G^0_{\bar{H}}$. By Corollary 5.3, $f = \alpha x_1^{m_1} \cdots x_r^{m_r}$ where $\alpha \in K^*$ is a root of unity and $m_i \in \mathbb{N}$. Thus $u \in K^* \cap G$ and hence $f \in (K^* \cap G)^0_{\bar{F}}$.
2. Let $f \in (G^0_{\bar{H}})^n$ be as given above. By part 1, $f_i = \alpha_i x_1^{m_{i,1}} \cdots x_r^{m_{i,r}}$ where $\alpha_i \in K$ are roots of unity and $m_{i,j} \in \mathbb{N}$. Suppose that (after reordering of the $\Pi\Sigma^*$-monomials) we have that $\bar{E} = \bar{H}(t_1, \ldots, t_k)[s_1, \ldots, s_e]$ where the $t_i$ are $\Pi$-monomials and the $s_i$ are $\Sigma^*$-monomials. By Corollary 6 we have that $M(f, \bar{E}) = M(f, \bar{H}(t_1, \ldots, t_k))$. Now let $(m_1, \ldots, m_n) \in M(f, \bar{H}(t_1, \ldots, t_k))$. Then we can take $g \in \bar{H}(t_1, \ldots, t_k) \setminus \bar{H}$ with

$$\sigma(g) = u g$$

for some $u = a x_1^{\mu_1} \cdots x_r^{\mu_r}$ with $\mu_i \in \mathbb{N}$ and $a$ being a root of unity in $\bar{H}$ and thus by assumption being from $K$. By Corollary 5.3 we get $u = \text{ord}(u) > 0$; in addition we have that $\mu' = \text{ord}(u) > 0$. By Theorem 16 it follows that $g = q t_1^{\nu_1} \cdots t_k^{\nu_k}$ with $q \in \text{const}_G \bar{H} \setminus \{0\}$ and $\nu_i \in \mathbb{Z}$. Since $u^{\mu} = 1$, it follows with (37) that $\sigma(g^{\mu'}) = g^{\mu'}$. Now suppose that $g$ depends on $t_m$ with $1 \leq m \leq k$. Then $g^{\mu'}$ depends also on $t_m$ which contradicts to $\text{const}(\bar{H}(t_1, \ldots, t_k)) = \text{const} \bar{H}$. Consequently $g = q \in \text{const}_G \bar{H} \setminus \{0\}$. By Corollary 7 it follows that $g = \hat{g} h$ with $h \in K[x_1, \ldots, x_r]$ and $\hat{g} \in F^*$ with $\sigma(h) = \lambda u h$ where $\lambda \in K^*$ is a root of unity. Recall that $\mu' = \text{ord}(u) > 0$ and hence $\mu'' = \text{gcd}(\mu', \text{ord}(\lambda)) > 0$. Since $\mu''(h) = h$ and $(\bar{F}, \sigma)$ is constant-stable, it follows that $h \in K^*$. Therefore $g \in K[x_1, \ldots, x_r]$. Summarizing $(m_1, \ldots, m_n) \in M(f, K[x_1, \ldots, x_r])$ and we conclude that $M(f, \bar{E}) \subset M(f, K[x_1, \ldots, x_r])$. The other direction is immediate.

(3) The third part follows by parts 1 and 2 and Theorem 9. □

**7. The algorithmic machinery III: Problem PFLDE**

We aim at proving Theorems 3.2 and 5.3, i.e., providing recursive algorithms that reduce Problem PFLDE from a given $R\Pi\Sigma^*$-extension to its ground ring (resp. field). If we are considering single-rooted $R\Pi\Sigma^*$-extension (Theorem 3.2), we rely heavily on the fact that for a given difference ring $(\bar{G}, \sigma)$ with constant field $K$ and given group
$G \leq \mathcal{G}$ we have that $s_{\text{const}} G (\mathcal{G}, \sigma) \setminus \{0\} \leq \mathcal{G}^*$. This property allows us to assume that for any $f \in \mathcal{G}^*$ and any $u \in G$ the $\mathbb{K}$-space $V = V(u, f, (\mathcal{A}, \sigma))$ has a basis with dimension $\leq n + 1$; see Lemma 4. In particular, our reduction algorithm is based on the assumption that there are algorithms available that solve Problem PFLDE in $(\mathcal{G}, \sigma)$ for $G$, i.e., one can compute a basis of $V$. For general $\mathcal{R}\Pi\Sigma^*$-extensions over a strong constant-stable difference field $(\mathcal{G}, \sigma)$ (Theorem 5.3) we need stronger properties: all what we stated above must hold not only for $\sigma$ but for the automorphisms $\sigma^l$ with $l \geq 1$.

7.1. A reduction strategy for $\Pi\Sigma^*$-extensions

We show the following theorem.

**Theorem 18.** Let $(\mathcal{A}, \sigma)$ be a computable difference ring and $G \leq \mathcal{A}^*$ such that $s_{\text{const}} G (\mathcal{A}, \sigma) \setminus \{0\} \leq \mathcal{A}^*$. Let $(\mathcal{A}(t), \sigma)$ be a $G$-simple $\Pi\Sigma^*$-extension of $(\mathcal{A}, \sigma)$.

1. If $t$ is a $\Sigma^*$-monomial and Problem PFLDE is solvable in $(\mathcal{A}, \sigma)$ for $G$, then Problem PFLDE is solvable in $(\mathcal{A}(t), \sigma)$ for $G^{\mathcal{A}(t)} = G$.
2. If $t$ is a $\Pi$-monomial and Problems PFLDE and PMT are solvable in $(\mathcal{A}, \sigma)$ for $G$, then Problem PFLDE is solvable in $(\mathcal{A}(t), \sigma)$ for $G^{\mathcal{A}(t)}$.

Define $\tilde{G} = G^{\mathcal{A}(t)}$ and let $\sigma(t) = \alpha t + \beta$ with $\alpha \in G$ and $\beta \in \mathcal{A}$. Moreover let $u \in \tilde{G}$, i.e.,

$$u = vt^m, \quad \text{with } v \in G, m \in \mathbb{Z},$$

(38)

and let $f = (f_1, \ldots, f_n) \in \tilde{G}^n$. By Theorem 11 we have that $s_{\text{const}} G (\mathcal{A}(t) \setminus \{0\}) \leq \mathcal{A}(t)^*$ and hence by Lemma 4 a basis of $V(u, f, \mathcal{A}(t))$ with dimension $\leq n + 1$ exists. We show how such a basis can be computed with the assumptions given in the theorem.

7.1.1. Degree bounds

The essential step is to search for degree bounds: we will determine $a, b \in \mathbb{Z}$ such that

$$V(u, f, \mathcal{A}(t)_{a, b}) = V(u, f, \mathcal{A}(t))$$

holds: for the definition of the truncated set of (Laurent) polynomials see (18). For technical reasons we also require that the constraints

$$a \leq \tilde{a} + m \quad \text{and} \quad \tilde{b} + m \leq b$$

(40)

hold where the $m$ is given by (38) and where

$$\tilde{a} = \min(l \text{deg}(f_1), \ldots, l \text{deg}(f_n)) \quad \text{and} \quad \tilde{b} = \max(l \text{deg}(f_1), \ldots, \text{deg}(f_n)).$$

(41)

The recovery of these bounds (see Lemmas 28 and 30 below) is based on generalizations of ideas given in [24]; for further details and proofs in the setting of difference fields see also [43,46].

If $t$ is a $\Sigma^*$-monomial, we have that $\mathcal{A}(t) = \mathcal{A}[t]$, $\alpha = 1$ and $\tilde{G} = G$; in particular we have $m = 0$ in (38). In this case, we can utilize the following lemma.

**Lemma 28.** Let $(\mathcal{A}[t], \sigma)$ be a $\Sigma^*$-extension of $(\mathcal{A}, \sigma)$ and $G \leq \mathcal{A}^*$ such that $s_{\text{const}} G (\mathcal{A}) \setminus \{0\} \leq \mathcal{A}^*$. Let $f \in \mathcal{A}[t]$ and $u \in G$. Then any solution $g \in \mathcal{A}[t]$ of $\sigma(g) - ug = f$ is bounded by $\text{deg}(g) \leq \max(\text{deg}(f) + 1, 0)$.

**Proof.** Suppose there is a $g \in \mathcal{A}[t]$ with $\text{deg}(g) > \max(\text{deg}(f) + 1, 0)$. Thus by Lemma 10 there is a $\gamma \in \mathcal{A}$ with $\sigma(\gamma) - \gamma = \sigma(t) - t$ which contradicts to Theorem 1.1. \qed
Thus we can set \( a = 0 \) and \( b = \max(\tilde{a} + 1, 0) \) to guarantee that (39) and (40) hold.

**Example 15** (Cont. Ex. 8). Consider the \( \Sigma^* \)-extension \((A[S], \sigma)\) of \((A, \sigma)\) with \( A = Q(k)[x][y][s] \) and \( \sigma(S) = S + y/k \) from Example 8.2. As stated in Example 8.3, we want to determine a \( g \in A[S] \) with \( \sigma(g) - g = f \) where \( f = yk^2s \), i.e., to find a basis of \( V(1, f, A[S]) \) with \( f = (k^2sy) \in A[S]^1 \). Using Lemma 28 it follows that \( \deg(g) \leq 1 \), i.e., that \( V(1, f, A[S]) = V(1, f, A[S]) \). Using our methods below (see Example 18) we get the basis \( \{(1, g), (0, 1)\} \) with \( g \) as given in (14).

If \( t \) is a \( \Pi \)-monomial, we have that \( A(t) = A[t, \frac{1}{t}] \) and \( \beta = 0 \). First suppose that \( u \notin A \), i.e., \( m \in \mathbb{Z} \setminus \{0\} \) as given in (38). If \( f_i = 0 \) for all \( i \), it is easy to see that \( g = 0 \) is the only choice. Hence take \( a = \max(0, m) \) and \( b = \max(-1, -1 + m) \), and (39) and (40) hold. Otherwise, if not all \( f_i \) are 0, we can use the following fact; the proof is left to the reader.

**Lemma 29.** Let \((A, \sigma)\) be a \( \Pi \)-extension of \((A, \sigma)\). Let \( \nu \in A^* \), \( m \in \mathbb{Z} \setminus \{0\} \), \( f = \sum_{i=\lambda}^\mu f_i t^i \in A(t) \) with \( \lambda, \mu \in \mathbb{Z} \) and \( g = \sum_{i=\tilde{\lambda}}^\tilde{\mu} g_i t^i \in A(t) \) with \( \tilde{\lambda}, \tilde{\mu} \in \mathbb{Z} \) and \( g_\tilde{\lambda} \neq 0 \neq g_\tilde{\mu} \) such that \( \sigma(g) - v \in \mathbb{M} \). Then \( \max(\lambda, \lambda - m) \leq \tilde{\lambda} \) and \( \tilde{\mu} \leq \max(\mu, \mu - m) \).

Note that in this scenario we have that \( \tilde{a}, \tilde{b} \in \mathbb{Z} \) for (41). Hence by setting \( a = \tilde{a} \) and \( b = \tilde{b} \), we can conclude that (39) and (40) hold.

What remains to consider is the case \( u \in G \) with \( m = 0 \). Here we utilize

**Lemma 30.** Let \((A(t), \sigma)\) be a \( \Pi \)-extension of \((A, \sigma)\) with \( G \leq A^* \) such that \( \sconst_G A \setminus \{0\} \leq A^* \) and \( \alpha = \sigma(t)/t \in G \). Let \( u \in G \), \( f = \sum_{i=\lambda}^\mu f_i t^i \in A(t) \) and \( g = \sum_{i=\tilde{\lambda}}^\tilde{\mu} g_i t^i \in A(t) \) with \( g_\tilde{\lambda} \neq 0 \neq g_\tilde{\mu} \) such that

\[
\sigma(g) - u \in \mathbb{M}.
\]

If there is a \( \nu \in \mathbb{Z} \) such that

\[
\sigma(\gamma) = \alpha^{-\nu} u \gamma
\]

for some \( \gamma \in \sconst_G A \setminus \{0\} \), then \( \nu \) is uniquely determined and we have that \( \min(\lambda, \nu) \leq \tilde{\lambda} \) and \( \tilde{\mu} \leq \max(\mu, \nu) \). If there is not such a \( \nu \), we have that \( \lambda \leq \tilde{\lambda} \) and \( \tilde{\mu} \leq \mu \).

**Proof.** Suppose there is a \( \nu \in \mathbb{Z} \) such that (43) for some \( \gamma \in \sconst_G A \setminus \{0\} \). Take in addition, \( \tilde{\nu} \in \mathbb{Z} \) such that \( \sigma(\tilde{\gamma}) = \alpha^{-\tilde{\nu}} u \tilde{\gamma} \) for some \( \tilde{\gamma} \in \sconst_G A \setminus \{0\} \). Then \( \sigma(\gamma/\tilde{\gamma}) = \alpha^{\nu - \tilde{\nu}} \gamma/\tilde{\gamma} \). Since \( t \) is a \( \Pi \)-monomial it follows by Theorem 1.2 that \( \nu = \tilde{\nu} \), i.e., \( \nu \) is uniquely determined. Now suppose that there is an \( i \) such that \( g_i \neq 0 \) where we have \( i < \min(\lambda, \nu) \) or \( i > \max(\mu, \nu) \). Then by coefficient comparison in (42) we get \( \sigma(g_i) = u \alpha^{-i} g_i \) with \( g_i \in \sconst_G A \setminus \{0\} \). Consequently \( \nu = i \), a contradiction. Otherwise, suppose that there is not such a \( \nu \in \mathbb{Z} \). Then by the same arguments, it follows that \( \lambda < \lambda \) or \( \tilde{\mu} \mu \) is not possible, i.e., \( \lambda \geq \lambda \) and \( \tilde{\mu} \leq \mu \). This completes the proof. \( \square \)

Therefore we derive the desired bounds if we solve Problem PMT and compute a basis of \( M((\alpha, u), A) \). Then given a basis, we can decide constructively if there is a \( \nu \in \mathbb{Z} \) such that (43) holds. If yes, take the uniquely determined \( \nu \) and we can take \( a = \min(\tilde{a}, \nu) \) and \( b = \max(b, \nu) \) to obtain (39) and (40). Otherwise, if there is not such a \( \nu \), we can set \( a = \min(\tilde{a}, 0) \) and \( b = \max(b, -1) \).

**Example 16** (Cont. Ex. 9). Take \((\mathbb{K}(k)[x][t], \sigma)\) with \( \alpha = \sigma(t)/t = xk \) defined in Example 9. In order to find the identity (7), we need a basis of \( V = V(u, (0), \mathbb{K}(k)[x][t]) \)
with \( u = \frac{\alpha}{\beta} \in (\mathbb{K}(x)^*)^{\mathbb{K}(k)[x](t)} \). Here we apply Lemma 30. Therefore we compute a basis of \( M((\alpha, u), \mathbb{K}(k)[x]) = M((k x, x/(k+1)), \mathbb{K}(k)[x]). \) As worked out in Example 13, a basis is \( \{(1,1)\} \). Thus we find \( \nu = -1 \) such that there is a \( g \in \mathbb{K}(k)[x] \setminus \{0\} \) with (30). We conclude that \( V = V(u, (0), \mathbb{K}(k)[x](t)_{-1}^{-1}) \). Using our methods below (see Example 17) we get the basis \((0, x(t + x^2)/k/t), (1,0)\) of \( V \) used in Example 9.

Summarizing, we obtain bounds \( a, b \in \mathbb{Z} \) such that (39) and (40) hold for a \( \Sigma^* \)-monomial. For a \( \Pi \)-monomial we need in addition that Problem PMT is solvable in \((\mathbb{A}, \sigma)\) for \( G \).

### 7.1.2. Degree Reduction

The following reduction has been introduced in [24] in the setting of difference fields. Subsequently, we present the basic ideas in the setting of difference rings; further technical details can be found in [42, Thm. 3.2.2].

We want to determine all \( c_1, \ldots, c_n \in \mathbb{K} = \text{const} \mathbb{A} \) and \( g_i \in \mathbb{A} \) in \( g = \sum_{i=a}^b g_i t_i \) such that

\[
\sigma(g) - u g = c_1 f_1 + \cdots + c_n f_n \tag{44}
\]

holds. If \( b < a \), \( g = 0 \) and a basis of \( V(u, (f, \mathbb{A}(t))) = V(u, (f, \{0\}) \) can be determined by linear algebra. Otherwise, we continue as follows. Due to (40), it follows that \( \lambda = \max(b, b + m) \) is the highest possible exponent in (44). Let \( \tilde{f}_i \) be the coefficient of the term \( t^\lambda \) in \( f_i \). Then by coefficient comparison w.r.t. \( t^\lambda \) in (44) we get the following constraints:

If \( m > 0 \),

\[
-v g_b = c_1 \tilde{f}_1 + \cdots + c_n \tilde{f}_n; \tag{45}
\]

if \( m = 0 \),

\[
\alpha^b \sigma(g_b) - v g_b = c_1 \tilde{f}_1 + \cdots + c_n \tilde{f}_n; \tag{46}
\]

if \( m < 0 \),

\[
\alpha^b \sigma(g_b) = c_1 \tilde{f}_1 + \cdots + c_n \tilde{f}_n. \tag{47}
\]

For the cases \( m > 0 \) and \( m < 0 \) one can easily determine a basis of the \( \mathbb{K} \)-vector spaces \( \{(c_1, \ldots, c_n, g_m)\} \) (45) holds\} and \( \{(c_1, \ldots, c_n, g_m)\} \) (47) holds\} by linear algebra. Moreover, if \( m = 0 \), equation (46) can be written in the form \( \sigma(g_b) - v \alpha^{-b} g_b = c_1 \tilde{f}_1 \alpha^{-b} + \cdots + c_n \tilde{f}_n \alpha^{-b} \) where \( v \alpha^{-b} \in G \) and \( \tilde{f}_i \alpha^{-b} \in \mathbb{A} \). Thus a basis of

\[
V(v \alpha^{-b}, \tilde{f}_1 \alpha^{-b}, \ldots, \tilde{f}_n \alpha^{-b}), \mathbb{A} \tag{48}
\]

can be determined if one can solve Problem PFLDE for \((\mathbb{A}, \sigma)\) in \( G \). Now we plug in this partial solution (i.e., the possible leading coefficient \( g_b \) with the corresponding linear combinations of the \( f_i \)), and end up at a new first-order parameterized difference equation where the highest possible coefficient is \( \lambda - 1 \). In other words, we reduced the problem by degree reduction. We continue to search for the next highest coefficient \( g_{b-1} \). Hence we proceed recursively by updating \( \lambda \to \lambda - 1 \) and \( b \to b - 1 \) and determine a basis of the reduced problem (with highest degree \( \lambda - 1 \)). Finally, given a basis of this solution space and given the basis of (48), one can determine a basis of \( V(v, f, \mathbb{A}(t))_{a,b} \). Summarizing, solving various instances of Problem PFLDE with the degree reductions \( b \to b - 1 \to \cdots \to a - 1 \) enables one to determine a basis of \( V(u, f, \mathbb{A}(t)) \). This concludes the proof of Theorem 18.
Example 17 (Cont. Ex. 16). We know that \( g = g_1 t^{-1} \). Plugging in \( g \) into \( \sigma(g) + \frac{x^2 y}{x + 1} = 0 \) yields \( \sigma(g_1) + \frac{x^2 y}{x + 1} g_1 = 0 \). Therefore we look for a basis of \( V\left(\frac{x^2 y}{x + 1}, (0), K(k)[x]\right) \). By using the algorithms presented in Subsection 7.2 we get the basis \( \{(1, x(x + x^2)/k), (0, 1)\} \). This finally gives the basis \( (0, x(x + x^2)/k/t), (1, 0)\) of \( V\left(\frac{x^2 y}{x + 1}, (0), K(k)[x]\right) \).

Example 18 (Cont. Ex. 15). We want to find a basis of \( V = V(1, f, A[S]_{10}) \) with \( A = Q(k)[x][y][s] \) and \( f = (y k^2 s) \). Hence we make the Ansatz \( (c_1, g_0 + g_1 S) \in V \) with indeterminates \( c_1 \in Q \) and \( g_0, g_1 \in A \) such that \( \sigma(g_0 + g_1 S) = c_1 y k^2 s \) (49).

holds. Doing coefficient comparison w.r.t. \( S^1 \) yields the constraint \( \sigma(g_1) - g_1 = c_1 0; \) compare (46). Thus we get all solutions by determining a basis of \( V(1, \tilde{f}, Q(k)[x][s]) \) with \( \tilde{f} = (0) \in A^1 \). In this particular instance, the \( Q \)-basis \( \{(1, 0), (0, 1)\} \) is immediate utilizing the fact that the constants are precisely \( Q \). Summarizing, the solutions are \( (c_1, g_1) \in Q^2 \). Consequently, our Ansatz can be refined with \( (c_1, g_0 + c_2 S) \in V \) where \( c_1 \in Q \), \( c_2 (= g_1) \in A \) and \( g_0 \in A \) such that \( \sigma(g_0 + c_2 S) - (g_0 + c_2 S) = c_1 k^2 s y \) holds. Bringing the \( c_2 S \) part to the right hand side yields the new equation \( \sigma(g_0) - g_0 = c_1 y k^2 s + c_2 h \) (50) with \( h = \sigma(s) - s = \frac{x^2 y}{x + 1} \in A \). In other words, we need a basis of \( V(1, h, A) \) with \( h = (y k^2 s, \frac{x^2 y}{x + 1}) \in A^2 \). Now we apply again the reduction method, but this time in the smaller ring \( A \) without the \( \Sigma^* \)-monomial \( S \). We skip all the details, but refer to a particular subproblem that we will consider in Example 19. Finally, we get the basis

\[
\{(0, 0, 1), (1, \frac{1}{2}, (\frac{1}{2}(1 - 2k) - \frac{1}{2}x)y + s(\frac{1}{2}(k - 1)(k + 1)x - \frac{1}{2}(k - 2)k)y\}
\]

of \( V(1, h, A) \). Thus we can reconstruct the basis \( \{(1, g), (0, 1)\} \) of \( V \) with \( g \) given in (14).

Note that the reduction of Theorem 18 simplifies to Karr’s field version given in [24] if one specializes \( A \) to a field and sets \( G = A^* = A \setminus \{0\} \). However, our version works not only for a field, but for any computable difference ring \( (A, \sigma) \) as specified in Theorem 18. Subsequently, we will exploit this enhancement in order to treat (nested) \( R \)-extensions.

7.2. A reduction strategy for \( R \)-extensions and thus for \( R\Pi\Sigma^* \)-extensions

The proof and the underlying algorithm for Theorem 3.2 is based on

Proposition 5. Let \( (A, \sigma) \) be a computable difference ring and \( G \leq A^* \) with \( s \text{const}_G A \setminus \{0\} \leq A^* \). Let \( (A[t], \sigma) \) be an \( R \)-extension of \( (A, \sigma) \) of given order \( d \) with \( \frac{\sigma(t)}{t} \in G \). Then Problem PFLDE is solvable in \( (A[t], \sigma) \) for \( G \) if it is solvable in \( (A, \sigma) \) for \( G \).

Proof. The proof follows by a simplified version of the degree reduction presented for Theorem 18. Let \( u \in G \) and \( f = (f_1, \ldots, f_n) \in A[t]^n \). By definition, it follows that a solution \( g \in A[t] \) and \( c_1, \ldots, c_n \in K = \text{const}A \) of (44) is of the form \( g = \sum_{i=0}^{b} g_i t^i \)

Note that we reduced the problem to find a polynomial solution of (49) with maximal degree \( 1 \) to a polynomial solution of (49) with maximal degree \( 0 \). This degree reduction has been achieved by introducing an extra parameter \( c_2 \). In general, the more \( \Sigma^* \)-monomials are involved, the more parameters will be introduced within the reduction.
with \( a := 0 \) and \( b := d - 1 \). Thus the bounds are immediate (under the assumption that
\( d \) has been determined; see Section 5). Since \( \sum_{i=0}^{d-1} h_i t^i = \sum_{i=0}^{d-1} h_i t^i \) iff \( h_i = h_i \), we

\[ \text{can activate the degree reduction as outlined in Subsection 7.1.2.} \]

\( \text{Namely, by coefficient comparison of the highest term we always enter in the case (46) (note that } m = 0 \text{ in (38)).} \]

By assumption we can solve Problem PFLDE in \((A, \sigma)\) for \( G \) and thus can determine a

basis of (48). By recursion we finally obtain a basis of \( V(u, f, A[f]) \). \( \square \)

**Proof of Theorem 3.2 (see page 13).** Since Problem PFLDE is solvable in \((G, \sigma)\)

for \( G \), it follows by iterative applications of Theorem 18 and Corollary 2.1 that

Problem PFLDE is solvable in \((H, \sigma)\) for \( H \) with \( H = G(t_1) \ldots (t_r) \) and that \( \text{const}_G H \setminus \{0\} \leq H^* \). Thus by iterative applications of Proposition 5 and Theorem 14 we

conclude that Problem PFLDE is solvable in \((H, \sigma)\) for \( H \) with \( H = H(x_1) \ldots (x_u) \) and that \( \text{const}_G H \setminus \{0\} \leq H^* \). Finally, by applying iteratively Theorem 18 and Corollary 2.1 it

follows that Problem PFLDE is solvable in \((E, \sigma)\) for \( G \). Note that in Proposition 5 we

have to know the values \( \text{ord}(x_i) = \text{ord}(\alpha_i) \) with \( \alpha_i \in G \) (either as input or by computing

them first by solving instances of Problem O in \( G \)). \( \square \)

Finally, we present an algorithm for Theorem 5.3 which is based on the following lemma.

**Lemma 31.** Let \((A, \sigma)\) be a difference ring, \( f \in A \), \( u \in A^* \) and \( \lambda \in \mathbb{N} \setminus \{0\} \). Then

\[ \sigma^{\lambda}(g) - u g = f \]

implies

\[ \sigma^{\lambda}(g) - u g = \sum_{j=0}^{\lambda-1} \frac{u^{(j)}}{u^{(j+1)}} \sigma^j(f). \]

**Proof.** From \( \sigma(g) - u g = f \) we get

\[ \sigma^{j+1}(g) - \sigma^j(u) \sigma^j(g) = \sigma^j(f) \]

for all \( j \in \mathbb{N} \). Multiplying it with \( u^{(j)}/u^{(j+1)} \) yields

\[ \frac{u^{(j)}}{u^{(j+1)}} \sigma^{j+1}(g) - \frac{u^{(j)}}{u^{(j+1)}} \sigma^j(g) = \frac{u^{(j)}}{u^{(j+1)}} \sigma^j(f). \]

Summing this equation over \( j \) from 0 to \( \lambda - 1 \) produces (51). \( \square \)

**Proposition 6.** Let \((A, \sigma)\) be a constant-stable and computable difference ring with

constant field \( K \). Let \( G \subseteq A^* \) which is closed under \( \sigma \) and where \( \text{const}_G(A, \sigma)^{\setminus \{0\}} \leq A^* \)

for all \( l > 0 \). Let \((E, \sigma)\) with \( E = A\langle x_1 \rangle \ldots (x_r) \) be a \( G \)-simple \( R \)-extension of \((A, \sigma)\) where

\( \text{ord}(x_i) > 0 \) and \( \text{per}(x_i) > 0 \) for \( 1 \leq i \leq r \) are given and where \( \text{const}_G \mathbb{E} \setminus \{0\} \leq \mathbb{E}^* \).

If for all \( l > 0 \) Problem PFLDE is solvable in \((G, \sigma^l)\) for \( G \), it is solvable in \((E, \sigma)\) for \( G_{\mathbb{E}} \).

**Proof.** Let \( K = \text{const}A \), let \( E = A\langle x_1 \rangle \ldots (x_r) \), let \( f = (f_1, \ldots, f_n) \subseteq \mathbb{E}^n \) and let \( u = v x_{i_1} x_{i_2} \ldots x_{i_r} \in G_{\mathbb{E}} \) with \( v \in G \) and \( m_i \in \mathbb{N} \). We will present a reduction method to

obtain a basis of \( V(u, f, E) \). Let \( \alpha = x_{i_1} x_{i_2} \ldots x_{i_r} \). Then by Lemma 21 it follows that

\( \text{ord}(\alpha) > 0 \) can be computed by the given values of \( \text{ord}(x_i) \) with \( 1 \leq i \leq r \). Hence we can

activate Lemma 22.4 and can compute \( \text{ord}(\alpha) > 0 \). Now take

\[ \lambda = \text{lcm}(\text{ord}(\alpha), \text{per}(x_1), \ldots, \text{per}(x_r)). \]

Thus we have that \( \alpha^{(\lambda)} = 1 \) and \( \sigma^\lambda(x_i) = x_i \) for all \( 1 \leq i \leq r \). Finally, define

\[ w := \alpha^{(\lambda)} = (\alpha v)^{(\lambda)} = u^{(\lambda)} \in G. \]

\( ^8 \) By a mild modification of the proof it suffices to take a \( \lambda \) such that \( \alpha^{(\lambda)} \in \text{const}A \) holds.
Now let \((c_1, \ldots, c_n, g) \in V(u, f, E)\), i.e., we have that (44). Thus Lemma 31 yields
\[
\sigma^\Lambda(g) - w g = c_1 \hat{f}_1 + \cdots + c_n \hat{f}_n
\]  
(54)
with
\[
\hat{f}_i = \sum_{i=0}^{\lambda-1} \frac{u(\lambda-i)}{(\lambda+1)^i} \sigma^i(f_i).
\]  
(55)
Hence \(V(u, f, E)\) is a subset of
\[
\tilde{V} = \{(c_1, \ldots, c_n) \in \mathbb{K}^n \times A[x_1, \ldots, x_r] \mid (54) \text{ holds}\}. 
\]  
(56)
Note that \(\tilde{V}\) is a \(\mathbb{K}\) subspace of \(\mathbb{K}^n \times A[x_1, \ldots, x_r]\). Thus \(V(u, f, E)\) is a subspace of \(\tilde{V}\) over \(\mathbb{K}\). Hence we concentrate first on the task to find a finite description of this solution set. More precisely, we show that it has a finite basis and show how one can compute it.

For this task define \(M := \{(n_1, \ldots, n_r) \in \mathbb{N}^r \mid 0 \leq n_i < \text{ord}(x_i)\}\). Write \(g = \sum_{i \in M} g_i x^i\) and \(\tilde{f}_j = \sum_{i \in M} \tilde{f}_{j,i} x^i\) in multi-index notation. Since \(\sigma^\Lambda(x_i) = x_i\), it follows by coefficient comparison that for \(i \in M\) we have that
\[
\sigma^\Lambda(g_i) - w g_i = c_1 \tilde{f}_{1,i} + \cdots + c_n \tilde{f}_{n,i}.
\]
By assumption, \(\text{const}_G(A, \sigma^\Lambda) \setminus \{0\} \subseteq A^*\). In particular, since \((A, \sigma)\) is constant-stable, we have that \(\text{const}(A, \sigma^\Lambda) = \mathbb{K}\). Thus with our \(w \in G\) and \(\tilde{f}_i = (\tilde{f}_{1,i}, \ldots, \tilde{f}_{n,i}) \in A^n\) we can solve Problem PFLDE in \((A, \sigma^\Lambda)\) with constant field \(\mathbb{K}\). Hence we get for all \(i \in M\) the bases for
\[
V_i = V(w, \tilde{f}_i, (A, \sigma^\Lambda)).
\]  
(57)
Note that by construction it follows that \(\tilde{V}\) from (56) is given by
\[
\tilde{V} = \{(c_1, \ldots, c_n) \sum_{i \in M} g_i x_i \mid (c_1, \ldots, c_n, g_i) \in V_i\}. 
\]  
(58)
Thus by linear algebra we get a basis of (58), say \(b_1, \ldots, b_s \in \mathbb{K}^n \times A[x_1, \ldots, x_r]\). Recall that \(V(u, f, (E, \sigma))\) is a subspace of (58). To this end, we make the Ansatz \((c_1, \ldots, c_n, g) = d_1 b_1 + \cdots + d_s b_s\) for indeterminates \(d_1, \ldots, d_s \in \mathbb{K}\) and plug in the generic solution into (44). This yields another linear system with unknowns \((d_1, \ldots, d_s)\). Solving this system enables one to derive a basis of \(V(u, f, E)\). \(\square\)

Example 19 (Cont. Ex. 18). In order to get a basis of \(V(1, h, A)\) in Ex. 18, the recursive reduction enters in the following subproblem. We are given the \(R\)-extension \((\mathbb{Q}(k)[x], \sigma)\) of \((\mathbb{Q}(k), \sigma)\) with \(\sigma(x) = -x\) and need a basis of \(V(x, f, \mathbb{Q}(k)[x])\) with \(f = (f_1, f_2, f_3) = (\frac{1}{x} + \frac{1}{x^2} - \frac{2}{x}, 0)\). By Example 12.2 we get \(\text{per}(x) = 2\) and \(\text{ford}(x) = 4\). Hence using (52) we determine \(\lambda = \text{lcm}(\text{ford}(x), \text{per}(x)) = 4\). Using (55) with \(u = x\) yields \((\tilde{f}_1, \tilde{f}_2, \tilde{f}_3) = (\frac{1}{k+1}(k+3)^2 - \frac{2}{k+1}, \frac{1}{k+1}(k+3)^2 - \frac{2}{k+1}, 0)\). Next we write the entries in multi-index notation. Namely, with \(M = \{(0), (1)\} \subseteq \mathbb{N}^1\) we get
\[
\tilde{f}_0 = (\tilde{f}_{1,0}, \tilde{f}_{2,0}, \tilde{f}_{3,0}) = (\frac{2k^2+4k+1}{k(k+2)}, \frac{2}{k(k+2)}, 0)
\]
\[
\tilde{f}_1 = (\tilde{f}_{1,1}, \tilde{f}_{2,1}, \tilde{f}_{3,1}) = (\frac{1}{k+1}(k+3), \frac{1}{k+1}(k+3), 0)
\]
with \(f = \sum_{(m) \in M} \tilde{f}_{(m)} x^m = \tilde{f}_0 + \tilde{f}_1 x\). Following (53) we get \(w = 1\) and we have to compute bases of the (57) with \(i \in M\). We obtain the basis \{\((0, 0, 1, 0), (1, -\frac{1}{2}, 0, -k/2)\)\}. 

42
of $V_{(0)} = V(1, \tilde{f}(0), (Q(k), \sigma^4))$ and the basis \{(−1, 1, 2, 0, 0), (0, 0, 0, 1), (0, 0, 1, 0)\} of $V_{(1)} = V(1, \tilde{f}(0), (Q(k), \sigma^4))$. Therefore a basis of

$$
\tilde{V} = \{(c_1, c_2, c_3, g) \in \mathbb{Q}^3 \times Q(k)[x]\sigma^4(g) - g = c_1 \tilde{f}_1 + c_2 \tilde{f}_2 + c_3 \tilde{f}_3\}
$$

\[= \{(c_1, c_2, c_3, \sum_{i \in \{0, 1\}} g_i x^i) | (c_1, c_2, c_3, g_{(i)}) \in V_{(i)}\}
\]

can be read off: \{(−1, 1/2, 0, −k/2), (0, 0, 1, 0), (0, 0, 0, 1)\}. Since $V(x, f, Q(k)[x])$ is a subspace of $\tilde{V}$, we plug in \{(c_1, c_2, c_3, g) = d_4(1, −1/2, 0, −k/2) + d_2(0, 0, 1, 0) + d_3(0, 0, 0, x) + d_4(0, 0, 1, 0)\} into (44) with our given $\tilde{f}_i$ and $u$ and get the constraint $\frac{1}{2}(d_1 - 2d_3 + 2d_4) + x(-d_3 - d_4) = 0$ or equivalently the constraints $−d_3 − d_4 = 0$ and $\frac{1}{2}(d_1 - 2d_3 + 2d_4)$. This yields $d_3 = \frac{1}{4}$ and $d_4 = −\frac{1}{4}$. Thus we obtain the generic solution $d_1(1, −\frac{1}{2}, 0, −\frac{1}{2} + \frac{\sqrt{2}}{4} − \frac{1}{4}) + d_2(0, 0, 1, 0)$ of $V(x, f, Q(k)[x])$, i.e., the basis \{(1, −\frac{1}{2}, 0, −\frac{1}{2} + \frac{\sqrt{2}}{4} − \frac{1}{4}) (0, 0, 1, 0)\} of $V(x, f, Q(k)[x])$.

**Remark 3.** (1) In the underlying algorithm of Proposition 6 we construct for all $i \in M$ the solution spaces given in (57) and combine them in one stroke as proposed in (58). This approach is interesting if one wants to perform calculations in parallel. Another approach is to apply similar tactics as given in Subsection 7.1: compute a basis of one of the (57), plug in the found solutions and continue with a constraint of one of the remaining monomials. In this way, one usually shortens step by step the length of the vectors $\tilde{f}_i$ in (57) and ends up very soon to a trivial situation (shortcut). As a side effect, one can combine the solution spaces given in (58) step by step.

(2) A different approach is to consider an $R$-extension $(F[x], \sigma)$ of $(F, \sigma)$ of order $d$ as a holonomic expression \cite{61,15,30} over a difference field. Then as worked out in \cite{47,17}, a solution $g = \sum_{i=0}^{d-1} g_i x^i$ and $c_i \in \text{const} F$ of (9) leads to a coupled system of first-order difference equations in terms of the $g_i$ that can be uncoupled explicitly. More precisely, there is an explicitly given formula that constitutes a higher-order parameterized linear difference equation in $g_{d-1}$ and the parameters $c_i$. Solving this difference equation in terms of $g_{d-1}$ and the $c_i$ delivers automatically the remaining coefficients $g_i$, i.e., the solution $g$ of (9). Here one usually has to solve a general higher-order linear difference equation. For further details on the holonomic Ansatz in the context of algebraic ring extensions (also on handling such objects in the basis of idempotent elements \cite{60,19}) we refer to \cite{17}. The advantage of the reduction technique proposed in Proposition 6 is that it can be applied in one stroke for nested $R$-extensions. In particular, Problem PFLDE can be always reduced again to Problem PFLDE by possibly switching to $(F, \sigma^k)$ for some $k > 1$. In this way, general higher-order linear difference equations can be avoided.

Combining all algorithmic parts we obtain the following result.

**Theorem 19.** Let $(E, \sigma)$ with $E = F(t_1) \ldots (t_c)$ be a simple $R\Pi\Sigma^*$-extension of a constant-stable and computable difference field $(F, \sigma)$. Suppose that for all $R$-monomials the period is positive, and the order and period of the $R$-monomials are given explicitly. Then Problem PFLDE in $(E, \sigma)$ for $(F^*)^k \leq E^*$ is solvable if one of the following holds:

(1) All $t_i$ are $R\Sigma^*$-monomials and PFLDE is solvable in $(F, \sigma^k)$ for $F^*$ for all $k > 0$.

(2) Problem PMT is solvable in $(F, \sigma)$ for $F^*$ and Problem PFLDE is solvable in $(F, \sigma^k)$ for $F^*$ for all $k > 0$.
Proof. Let \( H = (\mathbb{F}^*)_{\overline{E}}^* \). Recall that by Theorem 4 we have that \( \text{sconst}_H \mathbb{E} \setminus \{0\} \leq \mathbb{E}^* \), i.e., Problem PFLDE is applicable in \((\mathbb{E}, \sigma)\) for \( H \). By Lemma 18 we can reorder the generators of the \( R\Pi\Sigma^*\)-extension such that \((\overline{\mathbb{E}}, \sigma)\) is an \( \mathbb{F}^*\)-simple \( R\)-extension of \((\mathbb{F}, \sigma)\) and \((\mathbb{E}, \sigma)\) is a \( G\)-simple \( \Pi\Sigma^*\)-extension of \((\overline{\mathbb{E}}, \sigma)\) with \( G = (\mathbb{F}^*)_{\overline{E}}^* \). Note that the multiplicative group \( \mathbb{F}^\ast \) is closed under \( \sigma \), \( \text{sconst}((\mathbb{F}^*)_{\overline{E}}^* \mathbb{F}^\ast) = \mathbb{F}^\ast \) for all \( I > 0 \) and \( \text{sconst}((\mathbb{F}^*)_{\overline{E}}^* \mathbb{E} \setminus \{0\}) \leq \mathbb{E}^* \) by Corollary 1. Thus we can apply Proposition 6 and PFLDE is solvable in \((\overline{H}, \sigma)\) for \( G \) with the requirements stated in the two cases (1) and (2), respectively. Applying Theorem 18 and Corollary 2.1 iteratively shows that Problem PFLDE is solvable in \((\mathbb{E}, \sigma)\) for \( G_{\overline{E}} = H \); again we need the requirements stated in the cases (1) and (2), respectively. \( \square \)

**Proof of Theorem 5.3 (see page 13).** Let \((\mathbb{E}, \sigma)\) be a simple \( R\Pi\Sigma^*\)-extension of \((\mathbb{F}, \sigma)\) where \((\mathbb{F}, \sigma)\) is computable and strong constant-stable. Then by Corollary 5 (part 3 and 4) the periods and orders of all \( R \)-monomials are positive and can be computed. Thus Theorem 19.2 is applicable which completes the proof. \( \square \)

We remark that in Theorem 5.3 one can drop the condition that Problem PMT is solvable in \((\mathbb{F}, \sigma)\) for \( \mathbb{F}^\ast \) if in the \( R\Pi\Sigma^*\)-extension no \( \Pi \)-monomials occur, i.e., one applies case 1 and not case 2 of Theorem 19.

8. Conclusion

We provided important building blocks that extend the well established difference field theory to a difference ring theory. In this setting one can handle in addition objects such as (4). We elaborated algorithms for the (multiplicative) telescop ing problem (Problems T and MT) and the (multiplicative) parameterized telescop ing problem (Problems PT and PMT). In particular, Problem PT enables one to apply Zeilberger’s creative telescoping paradigm in the rather general class of simple \( R\Pi\Sigma^*\)-extensions. In order to derive these algorithms we showed that certain semi-constants (resp. semi-invariants) of the difference rings under consideration form a multiplicative group.

A future task will be to push forward the difference ring theory and the underlying algorithms in order to relax the requirements in Theorem 3 and 5 (i.e., that the \( R\Pi\Sigma^*\)-extensions are simple and/or that the ground difference ring is strong constant-stable). In any case, the currently developed toolbox widens the class of indefinite nested sums and products in the setting of difference rings. We are looking forward to see new kind of applications that can be attacked with this machinery.

References

[1] J. Ablinger, A. Behring, J. Blümlein, A. De Freitas, A. Hasselhuhn, A. von Manteuffel, M. Round, C. Schneider, and F. Wissbrock. The 3-loop non-singlet heavy flavor contributions and anomalous dimensions for the structure function \( F_2(x, Q^2) \) and transversity. *Nucl. Phys. B*, 886:733–823, 2014. [arXiv:1406.4654 [hep-ph]].

[2] J. Ablinger, J. Blümlein, A. De Freitas A. Hasselhuhn, A. von Manteuffel, M. Round, C. Schneider, and F. Wissbrock. The transition matrix element \( A_{Q\bar{q}}(N) \) of the variable flavor number scheme at \( O(\alpha_s^3) \). *Nucl. Phys. B*, 882:263–298, 2014. [arXiv:1402.0359 [hep-ph]].
[3] J. Ablinger, J. Blümlein, and C. Schneider. Harmonic sums and polylogarithms generated by cyclotomic polynomials. J. Math. Phys., 52(10):1–52, 2011. [arXiv:1007.0375 [hep-ph]].

[4] J. Ablinger, J. Blümlein, and C. Schneider. Analytic and algorithmic aspects of generalized harmonic sums and polylogarithms. J. Math. Phys., 54(8):1–74, 2013. [arXiv:1302.0378 [math-ph]].

[5] S. A. Abramov. On the summation of rational functions. Zh. vychisl. mat. Fiz., 11:1071–1074, 1971.

[6] S. A. Abramov, M. Bronstein, M. Petkovšek, and C. Schneider. In preparation, 2014.

[7] S. A. Abramov and M. Petkovšek. D’Alembertian solutions of linear differential and difference equations. In J. von zur Gathen, editor, Proc. ISSAC’94, pages 169–174. ACM Press, 1994.

[8] S. A. Abramov and M. Petkovšek. Polynomial ring automorphisms, rational $(w, \sigma)$-canonical forms, and the assignment problem. J. Symbolic Comput., 45(6):684–708, 2010.

[9] A. Bauer and M. Petkovšek. Multibasic and mixed hypergeometric Gosper-type algorithms. J. Symbolic Comput., 28(4–5):711–736, 1999.

[10] Thomas Becker and Volker Weispfenning. Gröbner bases, volume 141 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1993. A computational approach to commutative algebra, In cooperation with Heinz Kredel.

[11] J. Blümlein, A. Hasselhuhn, S. Klein, and C. Schneider. The $O(\alpha_s^3 n_f T_{\text{C,A,F}})$ contributions to the gluonic massive operator matrix elements. Nucl. Phys. B, 866:196–211, 2013. [arXiv:1205.4184 [hep-ph]].

[12] J. Blümlein, S. Klein, C. Schneider, and F. Stan. A symbolic summation approach to Feynman integral calculus. J. Symbolic Comput., 47:1267–1289, 2012.

[13] M. Bronstein. Symbolic Integration I, Transcendental functions. Springer, Berlin-Heidelberg, 1997.

[14] M. Bronstein. On solutions of linear ordinary difference equations in their coefficient field. J. Symbolic Comput., 29(6):841–877, 2000.

[15] F. Chyzak. An extension of Zeilberger’s fast algorithm to general holonomic functions. Discrete Math., 217:115–134, 2000.

[16] R. M. Cohn. Difference Algebra. Interscience Publishers, John Wiley & Sons, 1965.

[17] B. Érocíal. Algebraic extensions for summation in finite terms. PhD thesis, RISC, Johannes Kepler University, Linz, February 2011.

[18] R. W. Gosper. Decision procedures for indefinite hypergeometric summation. Proc. Nat. Acad. Sci. U.S.A., 75:40–42, 1978.

[19] C. Hardouin and M.F. Singer. Differential Galois theory of linear difference equations. Math. Ann., 342(2):333–377, 2008.

[20] P. A. Hendriks and M. F. Singer. Solving difference equations in finite terms. J. Symbolic Comput., 27(3):239–259, 1999.

[21] M. van Hoeij. Finite singularities and hypergeometric solutions of linear recurrence equations. J. Pure Appl. Algebra, 139(1-3):109–131, 1999.

[22] P. Horn, W. Koepf, and T. Sprenger. $m$-fold hypergeometric solutions of linear recurrence equations revisited. Math. Comput. Sci., 6(1):61–77, 2012.

[23] G. Karpilovsky. On finite generation of unit groups of commutative group rings. Arch. Math. (Basel), 40(6):503–508, 1983.

[24] M. Karr. Summation in finite terms. J. ACM, 28:305–350, 1981.

[25] M. Karr. Theory of summation in finite terms. J. Symbolic Comput., 1:303–315, 1985.

[26] M. Kauers and P. Paule. The concrete tetrahedron. Texts and Monographs in Symbolic Computation. SpringerWienNewYork, Vienna, 2011. Symbolic sums, recurrence equations, generating functions, asymptotic estimates.

[27] M. Kauers and C. Schneider. Application of unspecified sequences in symbolic summation. In J.G. Dumas, editor, Proc. ISSAC’06., pages 177–183. ACM Press, 2006.
[52] C. Schneider. Symbolic summation assists combinatorics. Sém. Lothar. Combin., 56:1–36, 2007. Article B56b.

[53] C. Schneider. A refined difference field theory for symbolic summation. J. Symbolic Comput., 43(9):611–644, 2008. [arXiv:0808.2543v1].

[54] C. Schneider. Parameterized telescoping proves algebraic independence of sums. Ann. Comb., 14(4):533–552, 2010. [arXiv:0808.2590].

[55] C. Schneider. Structural theorems for symbolic summation. Appl. Algebra Engry. Comm. Comput., 21(1):1–32, 2010.

[56] 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:0808.2543v1].

[57] C. Schneider. Simplifying multiple sums in difference fields. 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 325–360. Springer, 2013. [arXiv:1304.4134 [cs.SC]].

[58] C. Schneider. Fast algorithms for refined parameterized telescoping in difference fields. In M. Weimann J. Guitierrez, J. Schicho, editor, Computer Algebra and Polynomials, Lecture Notes in Computer Science (LNCS), to appear. Springer, 2014. [arXiv:1307.7887 [cs.SC]].

[59] C. Schneider. Modern summation methods for loop integrals in quantum field theory: The packages Sigma, EvaluateMultiSums and SumProduction. In Proc. ACAT 2013, volume 523 of J. Phys.: Conf. Ser., pages 1–17, 2014. [arXiv:1310.0160 [cs.SC]].

[60] M. van der Put and M.F. Singer. Galois theory of difference equations, volume 1666 of Lecture Notes in Mathematics. Springer-Verlag, Berlin, 1997.

[61] D. Zeilberger. A holonomic systems approach to special functions identities. J. Comput. Appl. Math., 32:321–368, 1990.

[62] D. Zeilberger. The method of creative telescoping. J. Symbolic Comput., 11:195–204, 1991.