PRODUCT REPRESENTATIONS IN ΠΣ-FIELDS

CARSTEN SCHNEIDER

Abstract. ΠΣ-fields are a very general class of difference fields that enable to discover and prove multisum identities arising in combinatorics and special functions. In this article we focus on the problem how such multisums can be represented in terms of ΠΣ-fields. In particular we consider product representations and their simplifications in ΠΣ-fields.

1. Introduction

In [Kar81, Kar85] Karr developed an indefinite summation algorithm that enables to simplify a very general class of nested multisum expressions. More precisely, he designed so called ΠΣ-fields in which those multisum expressions can be formulated. Since in this difference field setting one can solve the telescoping problem, and more generally one can solve parameterized first order linear difference equations (see Problem *LDE*), this enables to eliminate summation quantifiers in a given multisum expression. Based on these results, the summation package *Sigma* [Sch00, Sch01] has been developed; in particular the user is completely freed from working in difference fields, but can describe all the summation problems in terms of sum and product expressions. We want to point out that the summation package *Sigma* is a streamlined version [Sch02c, Sch02b, Sch02a] of [Kar81] which is based on results from [Bro00]. Moreover the algorithms cannot only solve Problem *LDE*, but even enable to search for solutions of linear difference equations with arbitrary order. Moreover we want to emphasize that Problem *LDE* not only contains the telescoping problem for indefinite summation, but also Zeilberger's creative telescoping [Zei90] for a very general class of definite multisums [Sch00]. In other words, these extensions enable to deal with definite summation problems, as it is illustrated for instance in [PS03, DPSW03].

In [Kar81, Kar85] the main emphasize is put on the aspect to decide algorithmically, if a sum or product can be adjoined to a ΠΣ-field. But so far one has not considered in details that there are various alternatives to construct a ΠΣ-field in which a given multisum can be represented. An important question is how one should construct such a ΠΣ-field iteratively in order to obtain simplifications from the point of view of symbolic summation. Whereas in [Sch03b] we focus on the problem to eliminate the nested depth of a given sum expression, in this article we will give various strategies how one handle products in the ΠΣ-field setting.

In Section 2 we will introduce the basic notions of ΠΣ-fields and elaborate on two important aspects. First we will motivate that solving Problem *LDE* and the so called orbit problem (see Problem *GOH*) in a given ΠΣ-field plays an important role to construct ΠΣ-fields in an algorithmic fashion. Second we will emphasize that, in contrast to sums, there might occur problems to formulate certain products in an already constructed ΠΣ-field. These two problems are the starting point for further considerations.

As already shown in [Kar81], the central Problems *LDE* and *GOH* are algorithmically solvable in a ΠΣ-field, if certain problems in the ground field, i.e., constant field, can be computed (see Definition 3.1). In Section 3 we will show that for a very general class of constant fields (see Property 3.1) such algorithms exist, and hence the theory of ΠΣ-fields with those constant

Supported by the Austrian Academy of Science and the SFB-grant F1305 of the Austrian FWF.

fields becomes completely constructive. It is important to mention that the algorithmic considerations in Section 3 are only needed, if products occur in a $\Pi\Sigma$-field.
In the second part of this work we will focus on how products can be formulated in $\Pi\Sigma$-fields. In Section 5 we analyze which kind of (q-)hypergeometric terms $f(k)$ in k can be represented in $\Pi\Sigma$-fields. For instance for the hypergeometric case, this will be always possible, except for expressions like $\gamma^k r(k)$ where $r(k)$ is a rational function in k and $\gamma \neq 1$ is a root of unity. More generally, in Section 6 we ask the question how several hypergeometric terms can be formulated in $\Pi\Sigma$-fields. In general, this will be always possible in a $\Pi\Sigma$-field plus one additional (ring) extension of an object like γ^k from above. Moreover in Section 4 we will generalize ideas from [AP02] that enable to simplify algorithmically products in a given $\Pi\Sigma$-field. Hence products can be represented in a compact form which in particular plays an important role in solving Problems *LDE* and *GOH* from the point of view of efficiency.

2. Construction of $\Pi\Sigma$-fields

In this section we introduce $\Pi\Sigma$-fields, a very general class of difference fields. In general, a difference field (resp. ring) $(\mathbb{F}, \sigma)$ is a field (resp. ring) $\mathbb{F}$ together with a field (resp. ring) automorphism $\sigma : \mathbb{F} \to \mathbb{F}$. The constant field (resp. ring) of $(\mathbb{F}, \sigma)$ is defined as $\text{const}_\sigma\mathbb{F} = \{g \in \mathbb{F} \,|\, \sigma(g) = g\}$. It follows easily that this set is indeed a subfield (resp. subring) of $\mathbb{F}$. Throughout this article we will suppose that $\mathbb{K}$ has characteristic 0.
An important aspect is that one can formulate a huge class of multisum expressions in $\Pi\Sigma$-fields; see Section 2.2. Moreover, in a $\Pi\Sigma$-field $(\mathbb{F}, \sigma)$ with constant field $\mathbb{K}$ there exist algorithms [Kar81, Bro00, Sch01] that enable to deal with the

Problem *LDE*: Solving parameterized first order *l*inear *d*ifference *e*quations

- Given $a_0, a_1 \in \mathbb{F}^*$ and $f_1, \dots, f_n \in \mathbb{F}$;
- find all $g \in \mathbb{F}$ and all $c_1, \dots, c_n \in \mathbb{K}$ such that $a_1\,\sigma(g) + a_0\,g = c_1\,f_1 + \dots + c_n\,f_n$.

This enables to carry out two fundamental paradigms of symbolic summation [PWZ96], namely telescoping and Zeilberger's creative telescoping, for a very general class of multisums; see [Sch01, Sch02c]. We want to emphasize that this (summation) algorithm that solves Problem *LDE* in $\Pi\Sigma$-fields requires certain computational properties on the constant field $\mathbb{K}$ that will be explored further in Section 3.

2.1. **$\Pi\Sigma$ and first order linear extensions.** In order to introduce $\Pi\Sigma$-fields in an appropriate way, we need the concept of difference field extensions. More generally, $(\mathbb{E}, \sigma')$ is a difference field (resp. ring) extension of $(\mathbb{F}, \sigma)$ if $\mathbb{F}$ is a subfield (resp. subring) of $\mathbb{E}$ and $\sigma'(g) = \sigma(g)$ for all $g \in \mathbb{F}$. Note that in the sequel we do not distinguish anymore the automorphisms σ and σ' within such a difference field (resp. ring) extension $(\mathbb{E}, \sigma')$ of $(\mathbb{F}, \sigma)$.

In the following we motivate important results from [Kar81]. One should keep in mind that we are basically interested in the following type of difference field extensions.

Definition 2.1. A difference field extension $(\mathbb{F}(t), \sigma)$ of $(\mathbb{F}, \sigma)$ is called *first order linear*, if t is transcendental over $\mathbb{F}$, we have $\sigma(t) = \alpha\,t + \beta$ for some $\alpha \in \mathbb{F}^*$, $\beta \in \mathbb{F}$, and $\text{const}_\sigma\mathbb{F}(t) = \text{const}_\sigma\mathbb{F}$. In particular, $(\mathbb{F}(t), \sigma)$ is called a Π- (resp. Σ^*-) extension of $(\mathbb{F}, \sigma)$, if it is first order linear and $\sigma(t) = f\,t$ (resp. $\sigma(t) = t + f$) for some $f \in \mathbb{F}^*$.

As it will be explained further in Subsection 2.2, Π- and Σ^*-extensions are exactly those first order linear extensions that are needed to describe nested sums and products. But first we will describe how Π- and Σ^*-extensions can be described in an alternative way; we want to emphasize that these results will enable to build up a completely constructive theory for $\Pi\Sigma$-fields. According to [Kar81] we introduce

Definition 2.2. For a difference field $(\mathbb{F}, \sigma)$ we define $\mathrm{H}_{(\mathbb{F},\sigma)} := \{\sigma(g)/g \mid g \in \mathbb{F}^*\}$.

Note that $\mathrm{H}_{(\mathbb{F},\sigma)}$ forms a multiplicative group which in the sequel will be called *homogeneous group*. With this notion one obtains equivalent descriptions of Π-and Σ^*-extensions; see [Kar85, Theorem 2.2] or [Sch01, Theorem 2.2.2] for the case **(1)**, and [Kar85, Theorem 2.3] combined with the remarks below for the case **(2)**.

Theorem 2.1. *Let $(\mathbb{F}(t), \sigma)$ be a difference field extension of $(\mathbb{F}, \sigma)$.* **(1)** *Then this is a Π-extension iff $\sigma(t) = \alpha\, t$, $t \neq 0$, $\alpha \in \mathbb{F}^*$ and there is no $n > 0$ with $\alpha^n \in \mathrm{H}_{(\mathbb{F},\sigma)}$.* **(2)** *Then this is a Σ^*-extension iff $\sigma(t) = t + \beta$, $t \notin \mathbb{F}$, $\beta \in \mathbb{F}^*$, and there is no $g \in \mathbb{F}$ with $\sigma(g) - g = \beta$.*

Next we want to introduce Σ-extensions which is a generalization of Σ^*-extensions.

Definition 2.3. $(\mathbb{F}(t), \sigma)$ is a Σ-*extension* of $(\mathbb{F}, \sigma)$ if **(1)** $\sigma(t) = \alpha\, t + \beta$ with $\alpha, \beta \in \mathbb{F}^*$, $t \notin \mathbb{F}$, **(2)** $\nexists g \in \mathbb{F}$ with $\sigma(g) - \alpha g = \beta$, and **(3)** if $\alpha^n \in \mathrm{H}_{(\mathbb{F},\sigma)}$ for some $n \in \mathbb{Z}^*$ then $\alpha \in \mathrm{H}_{(\mathbb{F},\sigma)}$.

In general, all Σ-extensions are first order linear; this follows by [Sch01, Theorem 2.2.3] which is a corrected version of [Kar81, Theorem 3] or [Kar85, Theorem 2.3]. In particular for the case $\alpha = 1$ the class of Σ-extensions coincide with the class of Σ^*-extensions.
Next we want to motivate that the combination of Π- and Σ-extensions enables to cover almost all kind of first order linear extensions $(\mathbb{F}(t), \sigma)$ of $(\mathbb{F}, \sigma)$. First we want to point out that only conditions (2) or (3) of Σ-extensions might restrict the class of first order linear extensions. Now suppose that our extension is first order linear, but condition (2) does not hold. Hence we find a $g \in \mathbb{F}$ such that $\sigma(g) - \alpha\, g = \beta$. Then it follows that $\sigma(t - g) = \alpha\,(t - g)$. Since t is transcendental over $\mathbb{F}$, also $t - g$ is transcendental over $\mathbb{F}$. Moreover $\mathrm{const}_\sigma \mathbb{F}(t - g) = \mathrm{const}_\sigma \mathbb{F}$. Hence $(\mathbb{F}(t - g), \sigma)$ is a Π-extension of $(\mathbb{F}, \sigma)$. In other words, condition (2) guarantees that there does not exist an overlapping between the class of Π-extensions and Σ-extensions among the class of first order linear extensions. Hence only condition (3) might exclude a first order linear extension. More precisely, we cannot express first order linear extensions with ΠΣ-extensions if there exists an $n > 0$ such that $\alpha^n \in \mathrm{H}_{(\mathbb{F},\sigma)}$, but $\alpha \notin \mathrm{H}_{(\mathbb{F},\sigma)}$. Since the same problem can occur while trying to construct Π-extension, we refer for more details to Section 2.2.
In the end we define ΠΣ-extensions and ΠΣ-fields.

Definition 2.4. A (nested) Π-extension (resp. ΠΣ-extension) $(\mathbb{F}(t_1, \dots, t_e), \sigma)$ of $(\mathbb{F}, \sigma)$ is a difference field extension where $(\mathbb{F}(t_1, \dots, t_i), \sigma)$ is a Π-extension (resp. Π- or Σ-extension) of $(\mathbb{F}(t_1, \dots, t_{i-1}), \sigma)$ for all $1 \leq i \leq e$. (For $i = 0$ we define $\mathbb{F}(t_1, \dots, t_{i-1}) = \mathbb{F}$.) A ΠΣ-field $(\mathbb{F}, \sigma)$ over $\mathbb{K}$ is a ΠΣ-extension of $(\mathbb{K}, \sigma)$ with constant field $\mathbb{K}$.

Note that in this definition the order of the extensions in $\mathbb{F}(t_1, \dots, t_e)$ is essential. So we have to distinguish for instance between the fields $\mathbb{F}(t_1, \dots, t_e)$ and $\mathbb{F}(t_e, \dots, t_1)$. If there might be confusion, we will emphasize this fact by the more precise notation $\mathbb{F}(t_1)(t_2)\dots(t_e)$.

2.2. **Automatic constructions of ΠΣ-fields for symbolic summation.** In [Kar81] algorithms are developed that enable to solve Problems *LDE* and *GOH* in a given ΠΣ-field $(\mathbb{F}, \sigma)$, if the constant field $\mathbb{K}$ has certain properties; see Section 3.

Problem *GOH*: The *g*eneralized *o*rbit problem for the *h*omogeneous group of dimension r

- Given a difference field $(\mathbb{F}, \sigma)$ and $f_1, \dots, f_r \in \mathbb{F}^*$;
- find a basis of the submodule $\left\{(n_1, \dots, n_r) \in \mathbb{Z}^r \mid f_1^{n_1} \dots f_r^{n_r} \in \mathrm{H}_{(\mathbb{F},\sigma)}\right\}$ of $\mathbb{Z}^r$ over $\mathbb{Z}$.

Then applying Theorem 2.1 in combination with those algorithms gives a completely constructive theory to build up a $\Pi\Sigma$-field for a given nested multisum expression. More precisely, for a given sum $S(n) := \sum_{k=0}^{n} f(k)$ or product $P(n) := \prod_{k=0}^{n} f(k)$ one has to construct first a concrete $\Pi\Sigma$-field $(\mathbb{F}, \sigma)$ for $f(k)$ (which again can consist of nested sums and products). This means, one has to define a map which links the given summation objects, i.e., sequences $f(k)$, with elements f', say, in the constructed $\Pi\Sigma$-field; in other words, $f' \in \mathbb{F}$ represents $f(k)$. **(a)** First we turn to the sum case $S(n)$. Then given this translation machinery one tries to compute a $g' \in \mathbb{F}$ with $\sigma(g') - g' = \sigma(f') =: \beta$. If one finds such a g', one can reinterpret this result as a sequence $g(k+1)$ for which the telescoping problem $g(k+1) - g(k) = f(k)$ holds, i.e. we have that $S(n) = g(n+1) - g(0)$. Moreover the sum itself can be represented in $\mathbb{F}$ with g'. Otherwise, if one fails to compute such a g', Theorem 2.1 tells us that this sum $S(n)$ can be adjoined to the $\Pi\Sigma$-field in form of a Σ^*-extension $(\mathbb{F}(t), \sigma)$ of $(\mathbb{F}, \sigma)$ with $\sigma(t) = t + \beta$. **(b)** Similarly, for the product case $P(n)$ one first tries to compute a $g' \in \mathbb{F}$ with $\frac{\sigma(g')}{g'} = \sigma(f') =: \alpha$; this enables to express the product $P(n)$ by g' in the already given difference field $\mathbb{F}$. Otherwise, if this fails, one tries to adjoin it in form of a Π-extension $(\mathbb{F}(t), \sigma)$ of $(\mathbb{F}, \sigma)$ with $\sigma(t) = \alpha\, t$. This works by Theorem 2.1, if there does not exist an $n > 0$ and a $g \in \mathbb{F}^*$ with $\alpha^n = \frac{\sigma(g)}{g}$; recall that this can be checked, if one knows how to solve Problem *GOH* (see Section 3). Otherwise, if $\alpha \notin \mathrm{H}_{(\mathbb{F},\sigma)}$ and there exists an $n > 1$ with $\alpha^n \in \mathrm{H}_{(\mathbb{F},\sigma)}$, we fail to adjoin $P(n)$ in form of a Π-extension. In general, this problem can always occur for an arbitrary $\alpha \in \mathbb{F}$. In Section 6 we will analyze this problematic case in more details for certain classes of $\Pi\Sigma^*$-fields $(\mathbb{F}, \sigma)$. This will result in an algorithmic strategy that allows to construct $\Pi\Sigma$-fields in which this problem can be at least partially avoided.

2.3. **The σ-equivalence relation and σ-factorization.** Finally we need some important computational results of $\Pi\Sigma$-fields that are essentially all covered in [Kar81]. First note that if $(\mathbb{F}(t), \sigma)$ is a $\Pi\Sigma$-extension of $(\mathbb{F}, \sigma)$, $\mathbb{F}(t)$ is the quotient field of the polynomial ring $\mathbb{F}[t]$. Moreover, for all $f \in \mathbb{F}[t]$ and all $k \in \mathbb{Z}$ it follows that $\sigma^k(f) \in \mathbb{F}[t]$. This shows that $(\mathbb{F}(t), \sigma)$ is a difference ring extension of $(\mathbb{F}[t], \sigma)$. Moreover if $f \in \mathbb{F}[t]$ is irreducible, also $\sigma^k(f)$ is irreducible for any $k \in \mathbb{Z}$. Next we introduce

Definition 2.5. Let $(\mathbb{F}(t), \sigma)$ be a $\Pi\Sigma$-extension of $(\mathbb{F}, \sigma)$. $f, g \in \mathbb{F}(t)^*$ are called σ-equivalent, if there exists a $k \in \mathbb{Z}$ such that $\sigma^k(f)/g \in \mathbb{F}$.

Obviously this is an equivalence relation. Moreover one can easily see that such a k always exists and is not uniquely determined, if $f, g \in \mathbb{F}^*$, or if $f = c\, t^m$, $g = d\, t^n$ for some $c, d \in \mathbb{F}^*$, $m, n \in \mathbb{Z}$ and $\frac{\sigma(t)}{t} \in \mathbb{F}$. In all other cases, if such a k exists, it is uniquely determined. This is a consequence of the following remarkable theorem; for proofs we refer to [Kar81, Theorem 4] or [Bro00, Corollary 1,2] together with [Sch01, Theorem 2.2.4].

Theorem 2.2. *Let $(\mathbb{F}(t), \sigma)$ be a $\Pi\Sigma$-extension of $(\mathbb{F}, \sigma)$ and $g \in \mathbb{F}(t)^*$ with $\frac{\sigma^k(g)}{g} \in \mathbb{F}$ for some $k \neq 0$. If $\frac{\sigma(t)}{t} \in \mathbb{F}$, $g = w\, t^r$ where $w \in \mathbb{F}^*$ and $r \in \mathbb{Z}$. Otherwise, if $\frac{\sigma(t)}{t} \notin \mathbb{F}$, $g \in \mathbb{F}$.*

Corollary 2.1. *Let $(\mathbb{F}(t), \sigma)$ be a $\Pi\Sigma$-extension of $(\mathbb{F}, \sigma)$ and $f, g \in \mathbb{F}(t) \setminus \mathbb{F}$ be σ-equivalent. If $\frac{\sigma(t)}{t} \notin \mathbb{F}$ or $g \neq c\, f^m$ where $c \in \mathbb{F}^*$, $m \in \mathbb{Z}^*$, then there is a unique $k \in \mathbb{Z}$ with $\frac{\sigma^k(f)}{g} \in \mathbb{F}$.*

Proof: The existence of k follows by assumption. Suppose there are $k_1 < k_2$ with $\frac{\sigma^{k_i}(f)}{g} \in \mathbb{F}$. Then $\frac{\sigma^{k_2}(f)}{\sigma^{k_1}(f)} \in \mathbb{F}$, and hence $\frac{\sigma^{k_2-k_1}(f')}{f'} \in \mathbb{F}$ for $f' := \sigma^{k_1}(f)$, a contradiction to Theorem 2.2. $\square$

Now suppose that we have given a $\Pi\Sigma$-field $(\mathbb{F}, \sigma)$ over a constant field $\mathbb{K}$ which is semi-computable, i.e., fulfills the following properties:

Definition 2.6. A field $\mathbb{K}$ is called *semi-computable*, if **(1)** for any $k \in \mathbb{K}$ one is able to decide, if $k \in \mathbb{Z}$, **(2)** polynomials in the polynomial ring $\mathbb{K}[t_1, \dots, t_e]$ can be factored over $\mathbb{K}$, and **(3)** one knows how to solve Problem O for the multiplicative group $\mathbb{K}^*$:

Problem O: The *o*rbit problem

- Given a field $\mathbb{K}$ and $f, g \in \mathbb{K}^*$;
- decide if there exists a $k \in \mathbb{Z}$ such that $f^k = g$; in case of existence, compute such a k.

Then for any ΠΣ-extension $(\mathbb{F}(t), \sigma)$ of $(\mathbb{F}, \sigma)$ one can decide, if there exists a $k \in \mathbb{Z}$ with $\sigma^k(f)/g \in \mathbb{F}$, and can compute such a k, in case of existence. This important result given in [Kar81, Section 2.3] is summarized in Theorem 2.3.

Remark 2.1. In [AB00] combined with [KL86] the Problem O has been solved for an important class of fields $\mathbb{K}$ specified in Property 3.1; hence for any ΠΣ-field over such fields $\mathbb{K}$ one can check, if two elements are σ-equivalent. Note that in Section 3 we require additional properties on the constant field $\mathbb{K}$, see Definition 3.1, that also hold for this class of constant fields; we refer to Section 3 for further details. Moreover we want to point out that for the ΠΣ-field $(\mathbb{K}(x), \sigma)$ over $\mathbb{K}$ with $\sigma(x) = x + 1$ there are more efficient algorithms, like in [MW94], that can check if two elements are σ-equivalent.

Finally we will introduce the σ-factorization in [Kar81], or equivalently the orbit decomposition in [Bro00] which play a major role throughout this article. Given a ΠΣ-extension $(\mathbb{F}(t), \sigma)$ of $(\mathbb{F}, \sigma)$ and $g \in \mathbb{F}(t)$ write $g = f_1^{m_1} \dots f_l^{m_l}$ with irreducible and pairwise prime polynomials $f_i \in \mathbb{F}[t]$ with multiplicities $m_i \in \mathbb{Z}^*$; all factors with positive (resp. negative) multiplicity give the numerator (resp. denominator). The basic idea is that with the field automorphism σ, g can be represented in a more compact form $g = u\, g_1 \cdots g_k$, $k \geq 0$, where $u \in \mathbb{F}$ and the g_i contain all the irreducible polynomials f_i (with its multiplicity) in g that belong to the same σ-equivalence class. More precisely, one can write the g_i as

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

where $m_{ij} \in \mathbb{Z}$ and the $h_i \in \mathbb{F}[t]$ are irreducible polynomials, pairwise prime and pairwise not σ-equivalent. In other words, the h_i generate all elements in the same σ-equivalence class with positive powers of σ. In this context the h_i are representants of the different σ-equivalence classes (it might happen that $g_i = 1$, if $m_{ij} = 0$ for all j). Note that for simplicity our definition of the σ-factorization differs slightly from the original one in [Kar81]: in Karr's version the g_i can be generated also by negative shifts. Moreover note that if we insisted that $m_{i1} \neq 0$, this representation would be even uniquely determined.
In this article we denote a *σ-factorization* of $g \in \mathbb{F}(t)$ as $g = u\, g_1 \dots g_k$ with the above properties, i.e., its refined version given by (1). Recall that if $(\mathbb{F}(t), \sigma)$ is a Π-extension of $(\mathbb{F}, \sigma)$, all σ-equivalent irreducible elements to t are just $c\, t^i$ for some $c \in \mathbb{F}^*$ and $i \in \mathbb{Z}$; see Theorem 2.2. Hence, if t is a factor in g and $\frac{\sigma(t)}{t} \in \mathbb{F}$, we can write $g_i = t^z$ for some $z \in \mathbb{Z}^*$ and $t \nmid g_j$ for all $i \neq j$. Moreover by Corollary 2.1 any irreducible factor $p \in \mathbb{F}[t]$ ($p \neq t$, if $\frac{\sigma(t)}{t} \in \mathbb{F}$) that occurs in g has a uniquely determined $l \in \mathbb{Z}$ with $\frac{\sigma^l(h_i)}{p} \in \mathbb{F}$ for some $1 \leq i \leq k$. Now suppose that the constant field is semi-computable. Then, as already pointed out above, such an l (uniquely determined) can be computed. Therefore given all the irreducible factors in g with its multiplicities (by factoring the numerator and denominator of g), one can collect them according to their different σ-equivalence classes in the expression g_i; for further details see [Kar81, Bro00, Sch02b]. All these remarks are collected in

Theorem 2.3. *Let $(\mathbb{F}(t),\sigma)$ be a $\Pi\Sigma$-field over a semi-computable constant field $\mathbb{K}$. Then one can decide for $f,g\in\mathbb{F}(t)$ if there exists a $k\in\mathbb{Z}$ with $\frac{\sigma^k(f)}{g}\in\mathbb{F}$; in case of existence one can compute such a k. Moreover the σ-factorization can be computed in $\mathbb{F}(t)$.*

3. The Constant Field and the Generalized Orbit Problem

As already motivated above, Problem *GOH* plays a major role in building up a constructive theory of $\Pi\Sigma$-fields, i.e., in checking if a product can be adjoined in form of a Π-extension to a already given $\Pi\Sigma$-field $(\mathbb{F},\sigma)$ over $\mathbb{K}$. The central question is, if there exists an $n>0$ such that $\alpha^n\in\mathrm{H}_{(\mathbb{F},\sigma)}$. In the sequel we formulate this problem in a slightly more general way. Consider $\mathbb{V}:=\left\{(n)\in\mathbb{Z}^1\,|\,\alpha^n\in\mathrm{H}_{(\mathbb{F},\sigma)}\right\}$ as a submodule of $\mathbb{Z}^1$ over $\mathbb{Z}$. Then there is an element $b\in\mathbb{Z}$ such that $\mathbb{V}=\{(b)\,z\,|\,z\in\mathbb{Z}\}$. In other words $b=0$ if and only if there does not exist an $n>0$ with $\alpha^n\in\mathrm{H}_{(\mathbb{F},\sigma)}$. Hence if we can compute a basis of $\mathbb{V}$, i.e., solve Problem *GOH* of dimension 1, we can also answer the above question.
In [Kar81] the problem to solve Problem *GOH* has been reduced to solving the problem *GOH* in a sub-difference field of $(\mathbb{F},\sigma)$. More precisely, if $\mathbb{F}=\mathbb{K}(t_1,\dots,t_e)$ for some $e\geq 1$, the problem to solve Problem *GOH* with dimension r can be reduced to a problem *GOH* in $\mathbb{K}(t_1,\dots,t_{e-1})$ with dimension r' where $r\leq r'\leq r+1$. Again this problem can be reduced to a *GOH* in the subfield $\mathbb{K}(t_1,\dots,t_{e-2})$ with dimension r'' where $r'\leq r''\leq r'+1$, and so on. We want to emphasize that in [Kar81] this reduction strategy can be turned to an algorithm, if certain conditions (namely condition (1) and (2) in Definition 2.6) hold for the constant field $\mathbb{K}$. In the end, after at most e reductions steps one reaches the *GOH* Problem in the constant field $\mathbb{K}$ where the dimension ranges between r and $r+e$. In this case, with $\mathrm{H}_{(\mathbb{K},\sigma)}=\{1\}$, Problem *GOH* reads with $\mathbb{G}:=\mathbb{K}^*$ as follows.

Problem *GO*: The *g*eneralized *o*rbit problem

- Given a multiplicative group $\mathbb{G}$ and $\boldsymbol{c}=(c_1,\dots,c_r)\in\mathbb{G}^r$;
- find a basis of the submodule $\mathbb{V}:=\{(n_1,\dots,n_r)\in\mathbb{Z}^r\,|\,c_1^{n_1}\dots c_r^{n_r}=1\}$ of $\mathbb{Z}^r$ over $\mathbb{Z}$.

Summarizing, Problem *GOH* can be solved algorithmically, if the constant field is computable.

Definition 3.1. A field $\mathbb{K}$ is called *computable*, if it is semi-computable (Definition 2.6) and there exists an algorithm to solve Problem *GO* for the multiplicative group $\mathbb{K}^*$.

Theorem 3.1. *Let $(\mathbb{F},\sigma)$ be a $\Pi\Sigma$-field over a computable field $\mathbb{K}$. Then there exist algorithms that solve Problem GOH and LDE.*

All these results have been developed in [Kar81]. Note that not only the algorithm for Problem *GOH* but also for Problem *LDE* given in [Kar81] or [Sch01, Sch02c] requires all three properties of a computable constant field $\mathbb{K}$. More precisely, certain degree and denominator bounds [Kar81, Sch02b, Sch02a] have to be computed for a Π-extension, which so far can be only derived by solving Problem *GOH*, and therefore Problem *GO*.

Remark 3.1. Any Problem *GOH* with dimension r can be reduced to a Problem *GO* also with dimension r, if all extensions in the $\Pi\Sigma$-field $(\mathbb{K}(t_1,\dots,t_e),\sigma)$ over $\mathbb{K}$ are Σ-extensions. This comes from the fact that in each of these reductions from $\mathbb{K}(t_1,\dots,t_l)$ to $\mathbb{K}(t_1,\dots,t_{l-1})$ the dimension is only increased by one, if t_l is a Π-extension, otherwise the dimension remains the same. In this case the computation of a basis of $\mathbb{V}$ (dimension 1) reduces to a *GO* Problem of dimension 1 which is equivalent to Problem *O*. Hence we only need that $\mathbb{K}$ is semi-computable.

In this section we will show that a huge class of fields $\mathbb{K}$ are actually computable, and hence Problems *LDE* and *GOH* can by solved algorithmically. Note that the following class of constant fields coincides with the semi-computable fields given in [AB00].

Property 3.1. $\mathbb{A}$ is a finitely generated algebraic field extension of the rational numbers $\mathbb{Q}$, and $\mathbb{K} := \mathbb{A}(x_1, \dots, x_s)$ is a field of rational functions over $\mathbb{A}$. Moreover we suppose that the field $\mathbb{K}$ is represented in such a way that we are able to deal with Problem (1) in Definition 2.6.

Given such a representation of the field $\mathbb{K}$ there are algorithms that solve Problem (2) in Definition 2.6. More precisely, given a multivariate polynomial $f \in \mathbb{A}[x_1, \dots, x_s][t_1, \dots, t_e]$ over an algebraic number field $\mathbb{A}$, there exist algorithms to factorize f over $\mathbb{A}$. But then clearly we obtain also a factorization of f over $\mathbb{A}(x_1, \dots, x_s)$. For an exhaustive list of references for such factorization algorithms see for instance [Win96]. Note that in all major computer algebra system, like Mathematica or Maple, such algorithms are implemented.
Hence what remains to consider is that in any such field $\mathbb{K}$ the Problem *GO* for $\mathbb{K}^*$ can be solved. In the last years several algorithms and strategies have been introduced in order to solve the problem *GO* for the group $\mathbb{A}^*$. So for instance in [CLZ00] they use results from [Mas88] which enables to bound a basis $\{\boldsymbol{b_1}, \dots, \boldsymbol{b_l}\} \subset \mathbb{Z}^r$ for the submodule $\mathbb{V}$ of the Problem *GO* in the following way: the entries in $\boldsymbol{b_i} = (b_{i1}, \dots, b_{ir}) \in \mathbb{Z}^r$ are all bounded by a common maximum value m. Hence an extensive search enables to find a set $\mathbb{S} \subset \mathbb{Z}^r$ of solutions that spans $\mathbb{V}$. With linear algebra methods one can finally find a subset of $\mathbb{S}$ which forms a basis of $\mathbb{V}$. We want to emphasize that a more sophisticated and efficient algorithm for Problem *GO* is developed in [Ge93a, Ge93b].
Summarizing, Problem *GO* can be solved for the algebraic number field $\mathbb{A}$. Finally the following proposition shows how Problem *GO* can be solved for a field $\mathbb{K}^*$ with Property 3.1.

Proposition 3.1. *Suppose that for a unique factorization domain $\mathbb{U}$ one can compute its prime factorization and that for the group of units of $\mathbb{U}$ Problem GO can be solved. Then Problem GO can be solved for the group $Q(\mathbb{U})^*$ where $Q(\mathbb{U})$ is the quotient field of $\mathbb{U}$.*

Proof: Let $f_i \in Q(\mathbb{U})^*$ for $1 \leq i \leq r$. Then we can represent f_i as $f_i = u_i \prod_{j=1}^{s} h_j^{m_{ij}}$ for primes $h_{ij} \in \mathbb{U}$, all pairwise prime, units u_i, and $m_{ij} \in \mathbb{Z}$. This can be done completely constructively: first we compute the prime factorization of f_i; this can be done by assumption. Afterwards collect all its primes, all relatively prime, namely $\{h_1, \dots, h_s\}$. Together with the multiplicities m_{ij} of h_j in f_i and $u_i := f_i / \prod_{j=1}^{s} h_j^{m_{ij}} \neq 0$ we obtain this representation.
Next compute a basis of the Problem *GO* for $(u_1, \dots, u_r) \in (\mathbb{U}^*)^r$, i.e., a basis $\mathcal{U}$ of a submodule $\mathbb{U}$ of $\mathbb{Z}^r$ over $\mathbb{Z}$; this can be done by assumption. Afterwards we search for all solutions $\boldsymbol{y} = (y_1, \dots, y_r) \in \mathbb{Z}^r$ of the linear diophantine system

$$\begin{pmatrix} m_{11} & \dots & m_{1r} \\ \vdots & \vdots & \vdots \\ m_{s1} & \dots & m_{sr} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_r \end{pmatrix} = 0.$$

The solution set $\mathbb{Y}$ builds up a submodule of $\mathbb{Z}^r$ over $\mathbb{Z}$ which is finitely dimensional and free. A basis $\mathcal{Y}$ for this solution space can be computed by linear algebra; see for instance [Sim84]. Given these two bases $\mathcal{U}$ and $\mathcal{Y}$ one can compute by linear algebra a basis $\mathcal{P}$ of the finitely dimensional submodule $\mathbb{U} \cap \mathbb{Y}$ of $\mathbb{Z}^r$ over $\mathbb{K}$. We show that this set $\mathbb{U} \cap \mathbb{Y}$ gives exactly the solution of Problem *GO* of $(f_1, \dots, f_r)$. Let $\boldsymbol{v} := (v_1, \dots, v_r) \in \mathbb{U} \cap \mathbb{Y} \subseteq \mathbb{Z}^r$. Since $\boldsymbol{v} \in \mathbb{Y}$ and $\boldsymbol{v} \in \mathbb{U}$, it follows that $\prod_{i=1}^{r} u_i^{v_i} = 1$ and $\prod_{i=1}^{r} h_j^{m_{ij}\,v_i} = 1$ for all $1 \leq j \leq s$. Therefore with

$$\left(\prod_{i=1}^{r} u_i^{v_i} \right) \prod_{j=1}^{s} \prod_{i=1}^{r} h_j^{m_{ij}\,v_i} = \prod_{i=1}^{r} \left(u_i \prod_{j=1}^{s} h_j^{m_{ij}} \right)^{v_i} = \prod_{i=1}^{r} f_i^{v_i}, \tag{2}$$

we have $\prod_{i=1}^{r} f_i^{v_i} = 1$. Now suppose that there exists a $\boldsymbol{v} = (v_1, \dots, v_r) \in \mathbb{Z}^r \setminus \mathbb{U} \cap \mathbb{Y}$ with $\prod_{i=1}^{r} f_i^{v_i} = 1$. We will show that this leads to a contradiction. Set $w_j := \prod_{i=1}^{r} h_j^{m_{ij} v_i}$ for $1 \leq j \leq s$ and $c := \prod_{i=1}^{r} u_i^{v_i}$. We may assume that $w_a \neq 1$ for some $1 \leq a \leq s$ or $c \neq 1$, since otherwise $\boldsymbol{v} \in \mathbb{U} \cap \mathbb{Y}$. If $c \neq 1$, then there must be an a with $w_a \neq 1$. Hence we may suppose that there there exists an a with $w_a \neq 0$ in any case. Let $1 \leq j \leq s$ be arbitrary but fixed. If $w_j \neq 1$, we have that $w_j = h_j^z$ for some $z \neq 0$, and therefore, with h_j a prime, w_j cannot be a unit. Hence for any $1 \leq j \leq s$ it follows that w_j is 1 or not a unit. Moreover, since all h_j with $1 \leq j \leq s$ are pairwise prime, also all $w_j \neq 1$ are pairwise prime. Hence, since $w_a \neq 1$ for some a, $w := \prod_{j=1}^{s} w_j$ is not a unit. But since c is a unit by construction, it follows that $w\,c$ is not a unit. By (2) we conclude that $1 \neq w\,c = \prod_{i=1}^{r} f_i^{v_i}$, a contradiction. □

Theorem 3.2. *A field $\mathbb{K}$ with Property 3.1 is computable.*

Proof: By the above remarks one can solve Problems (1) and (2) in Definition 3.1 for $\mathbb{K}$. Moreover one can solve Problem *GO* for $\mathbb{A}^*$, with $\mathbb{A}$ an algebraic number field. Recall that $\mathbb{A}[x_1, \dots, x_e]$ is a unique factorization domain in which one can compute its prime factorization, i.e., solve Problem (2) in Definition 3.1. Hence by Proposition 3.1 one can also solve the Problem *GO* for $Q(\mathbb{A}[x_1, \dots, x_e])^* = \mathbb{A}(x_1, \dots, x_e)^*$. Consequently also Problem *GO* can be solved algorithmically which proves that $\mathbb{K}$ is computable. □

Remark 3.2. We want to emphasize that Proposition 3.1 itself gives an algorithm to solve Problem *GO* for $\mathbb{G} = \mathbb{A}^*$, if $\mathbb{A}$ is the quotient field of a unique factorization domain $\mathbb{U}$ in which one can compute its prime factorization and if the problem *GO* for the units in $\mathbb{U}$ is solvable. An example for this situation are the integers $\mathbb{Z}$ or the Gaussian integers $\mathbb{Z}[i]$: they are unique factorization domains, in which one can compute its prime factorization; see for instance [PZ89]. Moreover for the units $1, -1$ in $\mathbb{Z}$ and $1, -1, i, -i$ in $\mathbb{Z}[i]$ Problem *GO* can be easily solved. Hence, by applying Proposition 3.1 twice, we can solve Problem *GO* for a field $\mathbb{K}$ with Property 3.1 where the algebraic number field is restricted to $\mathbb{A} = \mathbb{Q}$ or $\mathbb{A} = \mathbb{Q}(i)$. I want to point out that this is exactly that class of computable fields that can be treated in *Sigma* [Sch00, Sch01] so far; certainly, implementations of the algorithms proposed in [Ge93a, Ge93b] would be an important contribution.

4. Simplification of Π-extensions

In this section we deal with the problem to simplify Π-extensions $(\mathbb{F}(t)(p), \sigma)$ of $(\mathbb{F}(t), \sigma)$ where $(\mathbb{F}(t), \sigma)$ is a ΠΣ-field. For instance with the proposed algorithms we are able to obtain the following simpler product representations:

$$\prod_{k=1}^{n} \frac{(-k-1)(k+7)}{(k+4)^2} = \frac{4}{35} \frac{(n+5)(n+6)(n+7)}{(n+2)(n+3)(n+4)} (-1)^n, \tag{3}$$

$$\prod_{k=1}^{n} \frac{(k+3)(H_k(k+1)+1)^2(H_k(k+2)(k+1)+2k+3)}{(k+1)^2 H_k(H_k(k+3)(k+2)(k+1)+3(k+4)k+11)} = \frac{11}{6} \frac{(n+3)(n+2)(H_n(n+1)+1)^2}{(n+1)(H_n(n+3)(n+2)(n+1)+3(n+4)n+11)} \prod_{k=1}^{n} H_k, \tag{4}$$

$$\prod_{k=1}^{n} \frac{k!(H_k(k+2)(k+1)+2k+3)(H_k(k+1)+1)}{H_k(k+3)(k+2)(k+1)+3(k+4)k+11} = \frac{11(H_n(n+1)+1)}{H_n(n+3)(n+2)(n+1)+3(n+4)n+11} \prod_{k=1}^{n} k!H_k, \tag{5}$$

$$\prod_{k=1}^{n} \frac{(q^{k+2}+(k+1)!)(q^{k+1}+k!)(k+2)(k+1)}{(q^{k+3}+(k+2)!)(k+3)} = \frac{3(q^3+2)}{q+1} \frac{(q^{n+1}(n+1)+(n+1)!)}{(q^{n+3}+(n+2)!)(n+3)} \prod_{k=1}^{n} (kq^k+k!). \tag{6}$$

Example 4.1. Consider the ΠΣ-field $(\mathbb{Q}(x)(t), \sigma)$ over $\mathbb{K}$ with $\sigma(x) = x+1$ and $\sigma(t) = t + \frac{1}{x+1}$. The left side in (4) can be rephrased with the Π-extension $(\mathbb{Q}(x)(t)(p), \sigma)$ of $(\mathbb{Q}(x)(t), \sigma)$ with $\sigma(p) = f\,p$ where $f := \sigma(\frac{(x+3)(t(x+1)+1)^2(t(x+2)(x+1)+2x+3)}{(x+1)^2 t(t(x+3)(x+2)(x+1)+3(x+4)x+11)})$. The product at the right side can be represented by the Π-extension $(\mathbb{Q}(x)(t)(q), \sigma)$ with $\sigma(q) = f'\,q$ where $f' = \sigma(t)$.

As it will turn out, these two ΠΣ-fields $(\mathbb{Q}(x)(t)(p), \sigma)$ and $(\mathbb{Q}(x)(t)(q), \sigma)$ are isomorph. In general we try to find among all the equivalent Π-extensions a specific one where the degrees of numerator and denominator in $\frac{\sigma(p)}{p} \in \mathbb{F}(t)$ are minimal.

Definition 4.1. Two difference field extensions $(\mathbb{F}(p),\sigma)$, $(\mathbb{F}(q),\sigma)$ are $\mathbb{F}$-isomorphic, if there exists a field isomorphism $\tau:\mathbb{F}(p)\to\mathbb{F}(q)$ with $\tau\,\sigma=\tilde{\sigma}\,\tau$ and $\tau(f)=f$ for all $f\in\mathbb{F}$. We also say that $(\mathbb{F}(p),\sigma)$ and $(\mathbb{F}(q),\sigma)$ are $\mathbb{F}$-isomorphic and τ is an $\mathbb{F}$-isomorphism.

Suppose we have given two Π-extensions $(\mathbb{F}(p),\sigma)$, $(\mathbb{F}(q),\sigma)$ of $(\mathbb{F},\sigma)$ with an $\mathbb{F}$-isomorphism $\tau:\mathbb{F}(p)\to\mathbb{F}(q)$ and $a_i\in\mathbb{F}(p)$, $f\in\mathbb{F}(p)$. Then for any $g\in\mathbb{F}(p)$ it follows that $a_m\,\sigma^m(g)+\dots+a_1\,\sigma(g)+a_0\,g=f$ if and only if $\tau(a_m)\,\sigma^m(\tau(g))+\dots+\tau(a_1)\,\sigma(\tau(g))+\tau(a_0)\,g=\tau(f)$. Hence p and q describe in the difference field setting the "same" object. Nevertheless, all these isomorphic extensions can be represented in different complicated ways as it is illustrated in(4)–(6). This motivates to consider

Problem SΠ: Simplification of Π-extensions

- Given a ΠΣ-extension $(\mathbb{F}(t),\sigma)$ of $(\mathbb{F},\sigma)$ and a Π-extension $(\mathbb{F}(t)(p),\sigma)$ of $(\mathbb{F}(t),\sigma)$ with $f:=\frac{\sigma(p)}{p}$;
- find among all the $\mathbb{F}(t)$-isomorphic Π-extensions $(\mathbb{F}(t)(q),\sigma)$ of $(\mathbb{F}(t),\sigma)$ with $f':=\frac{\sigma(q)}{q}$ that one where the degrees of the numerator and denominator of $f\in\mathbb{F}(t)$ are minimal; construct also the $\mathbb{F}(t)$-isomorphism.

As it will turn out there are such extensions in which the numerator **and** denominator of $\frac{\sigma(p)}{p}\in\mathbb{F}(t)$ have minimal degree. Moreover this problem can be solved algorithmically if $(\mathbb{F},\sigma)$ is a ΠΣ-field over a computable constant field.

First we try to specify the above problem in more concrete terms. The following lemma states how an $\mathbb{F}$-isomorphic Π-extension looks like.

Proposition 4.1. *Let $(\mathbb{F}(p),\sigma)$, $(\mathbb{F}(q),\sigma)$ with $f:=\frac{\sigma(p)}{p}$, $f':=\frac{\sigma(q)}{q}$ be Π-extensions of $(\mathbb{F},\sigma)$ with an $\mathbb{F}$-isomorphism $\tau:\mathbb{F}(p)\to\mathbb{F}(q)$. Then $\tau(p)=g\,q^i$ and $f=\frac{\sigma(g)}{g}\,f'^i$ for some $g\in\mathbb{F}^*$ and $i\in\{-1,1\}$.*

Proof: Consider any $\mathbb{F}$-isomorphism $\tau:\mathbb{F}(p)\to\mathbb{F}(q)$. Then $\frac{\sigma(\tau(p))}{\tau(p)}=\tau(\frac{\sigma(p)}{p})=\tau(f)=f=\frac{\sigma(p)}{p}\in\mathbb{F}$. By Theorem 2.2 it follows that $\tau(p)=g\,q^i$ for some $g\in\mathbb{F}^*$ and $i\in\mathbb{Z}$. Since the reversed map $\tau^{-1}:\mathbb{F}(q)\to\mathbb{F}(p)$ is also an $\mathbb{F}$-isomorphism, the same argument from above can be applied: there exists an $h\in\mathbb{F}$ and a $j\in\mathbb{Z}$ such that $\tau(q)=h\,p^j$. Therefore $p=\tau^{-1}(\tau(p))=\tau^{-1}(g\,q^i)=g\,\tau^{-1}(q)^i=g\,(h\,p^j)^i=g\,h^i\,p^{i\,j}$ which shows that $i\,j=1$ and hence that $i,j\in\{-1,1\}$. Moreover we have that $f=\frac{\sigma(p)}{p}=\frac{\sigma(\tau(p))}{\tau(p)}=\frac{\sigma(g)}{g}\left(\frac{\sigma(q)}{q}\right)^i=\frac{\sigma(g)}{g}\,f'^i$. □

The next lemma states that one basically can reduce the above problem to the case that $i=1$. The other case $i=-1$ does not yield to something really new.

Proposition 4.2. *Let $(\mathbb{F}(p),\sigma)$ and $(\mathbb{F}(q),\sigma)$ be Π-extensions of $(\mathbb{F},\sigma)$ which are $\mathbb{F}$-isomorphic by $\tau:\mathbb{F}(p)\to\mathbb{F}(q)$ with $\tau(p)=\frac{g}{q}$ for some $g\in\mathbb{F}^*$. Then there is a Π-extension $(\mathbb{F}(q'),\sigma)$ of $(\mathbb{F},\sigma)$ with $\frac{\sigma(q')}{q'}=\frac{q}{\sigma(q)}$ together with an $\mathbb{F}$-isomorphism $\tau':\mathbb{F}(p)\to\mathbb{F}(q')$ with $\tau'(p)=\frac{g}{q'}$.*

Proof: Write $\alpha:=\frac{\sigma(p)}{p}\in\mathbb{F}^*$. Consider the rational function field $\mathbb{F}(q')$ and define the difference field extension $(\mathbb{F}(q'),\sigma)$ of $(\mathbb{F},\sigma)$ with $\sigma(q')=\frac{1}{\alpha}\,q'$. Now suppose that there is an $n>0$ and a $g\in\mathbb{F}$ with $\left(\frac{1}{\alpha}\right)^n=\frac{\sigma(g)}{g}$. Then we have that $\alpha^n=\frac{\sigma(1/g)}{1/g}$ and therefore $(\mathbb{F}(p),\sigma)$ is not a Π-extension of $(\mathbb{F},\sigma)$ by Theorem 2.1, a contradiction. Hence by Theorem 2.1 $(\mathbb{F}(q'),\sigma)$ is a Π-extension of $(\mathbb{F},\sigma)$. Next construct the field isomorphism $\tau':\mathbb{F}(p)\to\mathbb{F}(q')$ with $\tau'(p)=\frac{g}{q'}$ and $\tau'(f)=f$ for all $f\in\mathbb{F}$. What remains to show is that this is indeed an $\mathbb{F}$-isomorphism. First note that $\frac{\sigma(g/q)}{g/q}=\frac{\sigma(g)}{g}\,\frac{q}{\sigma(q)}=\frac{\sigma(g)}{g}\,\frac{\sigma(q')}{q'}=\frac{\sigma(g\,q')}{g\,q'}$. Moreover note that $\alpha=\frac{\sigma(p)}{p}=\frac{\sigma(\tau^{-1}(g/q))}{\tau^{-1}(g/q)}=\tau^{-1}\left(\frac{\sigma(g/q)}{g/q}\right)$. Since τ cannot map any element from $\mathbb{F}(p)\setminus\mathbb{F}$ to $\mathbb{F}$, also

τ^{-1} cannot map any element from $\mathbb{F}(q)\backslash\mathbb{F}$ to $\mathbb{F}$. Therefore $\frac{\sigma(g/q)}{g/q} \in \mathbb{F}$, thus $\alpha = \frac{\sigma(g/q)}{g/q} = \frac{\sigma(g\,q')}{g\,q'}$, and hence $\sigma(\tau'(p)) = \sigma(g\,q') = \alpha g\,q' = \alpha\,\tau'(p) = \tau'(\alpha\,p) = \tau'(\sigma(p))$ which shows that τ is an $\mathbb{F}$-isomorphism. □

Hence Propositions 4.1 and 4.2 from above motivate us to reduce Problem $S\Pi$ to

Problem *MPE*: Find a *m*inimal *p*roduct-*e*quivalence

- Given a $\Pi\Sigma$-extension $(\mathbb{F}(t),\sigma)$ of $(\mathbb{F},\sigma)$ and $f \in \mathbb{F}(t)^*$;
- find $f', g \in \mathbb{F}(t)$ such that $f = \frac{\sigma(g)}{g}\,f'$ where the degrees of the numerator and denominator of f' are minimal.

Example 4.2. In Example 4.1 we have $f = \frac{\sigma(g)}{g}\,f'$ with $g = \frac{(x+3)(x+2)(t(x+1)+1)^2}{(x+1)(t(x+3)(x+2)(x+1)+3(x+4)x+11)}$.

The next goal is to show Proposition 4.3 which says that any solution of Problem *MPE* also solves Problem $S\Pi$. First we consider further the relation between f and f'.

Definition 4.2. Let $(\mathbb{F},\sigma)$ be a difference field. Then $f, f' \in \mathbb{F}^*$ are called product-equivalent, in symbols $f \equiv_\pi f'$, if there exists a $g \in \mathbb{F}^*$ such that $f = \frac{\sigma(g)}{g}\,f'$.

The observation that $\equiv_\pi$ forms an equivalence relation will be heavily used in the sequel. The following lemma is needed for Proposition 4.3 which connects the Problems $S\Pi$ and *MPE*.

Lemma 4.1. *Let $(\mathbb{F}(p),\sigma)$ be a Π-extension of $(\mathbb{F},\sigma)$ with $\alpha := \frac{\sigma(p)}{p} \in \mathbb{F}$. If $1 \equiv_\pi f$ for some $f \in \mathbb{F}$, there exists a Π-extension $(\mathbb{F}(q),\sigma)$ of $(\mathbb{F},\sigma)$ with $\frac{\sigma(q)}{q} = \alpha\,f$.*

Proof: Since $1 \equiv_\pi f$, there is a $g \in \mathbb{F}^*$ with $f = \frac{\sigma(g)}{g}$. Suppose that there is no Π-extension $(\mathbb{F}(q),\sigma)$ of $(\mathbb{F},\sigma)$ with $\frac{\sigma(q)}{q} = \alpha\,f$. Then by Theorem 2.1 there are $n > 0$ and $h \in \mathbb{F}$ with $\frac{\sigma(h)}{h} = (\alpha\,f)^n$. Thus $\frac{\sigma(h)}{h} = \alpha^n\,\frac{\sigma(f^n)}{f^n}$, and consequently $\frac{\sigma(h\,f^{-n})}{h\,f^{-n}} = \alpha^n$ with $h\,f^{-n} \in \mathbb{F}$, a contradiction by Theorem 2.1. □

Proposition 4.3. *Let $(\mathbb{F}(p),\sigma)$ be a Π-extension of $(\mathbb{F},\sigma)$ with $f := \frac{\sigma(p)}{p} \in \mathbb{F}$ and constant field $\mathbb{K}$ and let $f \equiv_\pi f'$ for some $f' \in \mathbb{F}$. Then one can construct an $\mathbb{F}$-isomorphic Π-extension $(\mathbb{F}(q),\sigma)$ of $(\mathbb{F},\sigma)$ with $\frac{\sigma(q)}{q} = f'$. In particular, if $f = \frac{\sigma(g)}{g}\,f'$ for $g \in \mathbb{F}^*$, an $\mathbb{F}$-isomorphism $\tau : \mathbb{F}(p) \to \mathbb{F}(q)$ can be defined by $\tau(p) = k\,g\,q$ for any $k \in \mathbb{K}^*$.*

Proof: Since $f \equiv_\pi f'$, there exists a $g \in \mathbb{F}^*$ with $f' = \frac{\sigma(g)}{g}\,f$, i.e., $f'/f \equiv_\pi 1$. Hence by Lemma 4.1 there is a Π-extension $(\mathbb{F}(q),\sigma)$ of $(\mathbb{F},\sigma)$ with $\frac{\sigma(q)}{q} = f'$. Now define the field isomorphism $\tau : \mathbb{F}(p) \to \mathbb{F}(q)$ with $\tau(p) = k\,g\,q$ for some $k \in \mathbb{K}^*$ and $\sigma(h) = h$ for all $h \in \mathbb{F}$. Since $\tau(\sigma(p)) = \tau(f\,p) = k\,\tau(f)\,\tau(p) = k\,f\,g\,q = k\,\sigma(g)\,f'\,q = k\,\sigma(g)\,\sigma(q) = \sigma(k\,g\,q) = \sigma(\tau(p))$, τ is an $\mathbb{F}$-isomorphism. □

In other words, given a Π-extension $(\mathbb{F}(t)(p),\sigma)$ of $(\mathbb{F}(t),\sigma)$ with $f := \frac{\sigma(p)}{p}$, and elements $f_1, \dots, f_k \in \mathbb{F}^*$ with $f \equiv_\pi f_1 \equiv_\pi \dots \equiv_\pi f_k$, one can construct Π-extensions $(\mathbb{F}(t)(p_i),\sigma)$ of $(\mathbb{F}(t),\sigma)$ with $\frac{\sigma(p_i)}{p_i} = f_i$ which are all isomorphic to each other.

Example 4.3. In Examples 4.1 and 4.2 the $\Pi\Sigma$-fields $(\mathbb{Q}(x)(t)(p),\sigma)$ and $(\mathbb{Q}(x)(t)(q),\sigma)$ are $\mathbb{Q}(x)(t)$-isomorph with $\tau(p) = k\,g\,q$ for any $k \in \mathbb{Q}^*$. This is exactly reflected in Identity (4) with the specific value $k = \frac{11}{6}$ which comes from checking initial values.

Suppose that one is able to solve Problem $S\Pi$, i.e., to find among all those f_i a specific one, say f_r, where the degrees of numerator **and** denominator are minimal. Then also for the Π-extension $(\mathbb{F}(t)(p_r),\sigma)$ of $(\mathbb{F}(t),\sigma)$ the numerator **and** denominator of $f'_r = \frac{\sigma(p_r)}{p_r}$ will have minimal degrees among all the possible Π-extensions $(\mathbb{F}(t)(p_i),\sigma)$. In addition, Propositions 4.1 and 4.2 ensure that there do not exist any further $\mathbb{F}(t)$-isomorphic Π-extensions that are of simpler type. *In other words Problem* $S\Pi$ *is solved, if one can solve Problem MPE.*

Finally we introduce algorithms that enable to solve Problem *MPE*. We want to point out that the following results are inspired by the work of [AP02]. In particular for the special case that $(\mathbb{F}(t),\sigma)$ is the ΠΣ-field over $\mathbb{F}$ with $\sigma(t)=t+1$ the following results can be embedded in [AP02]. On one side our algorithms are not as efficient as in [AP02] in order to solve the Problem *MPE*. On the other side our results are much more general. This in particular enables to solve the Problem *MPE* not only for the special case as in [AP02], but for any ΠΣ-field $(\mathbb{F}(t),\sigma)$ over $\mathbb{K}$. In particular we cover the q-hypergeometric case $t \leftrightarrow q^k$ or for instance the case $t \leftrightarrow H_k$.

Lemma 4.2. *Let $(\mathbb{F}(t),\sigma)$ be a ΠΣ-extension of $(\mathbb{F},\sigma)$ and write $f = u\,f_1\dots f_k \in \mathbb{F}(t)$ and $f' = u'\,f'_1\dots f'_k \in \mathbb{F}(t)$ in σ-factorizations where the factors in f_i, f'_i are σ-equivalent. If $f \equiv_\pi f'$ then for all $1 \le i \le k$ we have $f_i \equiv_\pi u_i\,f'_i$ for some $u_i \in \mathbb{F}^*$.*

Proof: The proof will be done by induction on k. For $k=1$ nothing has to be shown. Now suppose that the lemma holds for $k \ge 1$ and consider the σ-factorizations $g = v\,g_1\dots g_{k+1}$, $f = u\,f_1\dots f_{k+1}$ and $f = u'\,f'_1\dots f'_{k+1}$ where all factors in f_i, f'_i and g_i are σ-equivalent. Suppose that there does not exist a $u_{k+1} \in \mathbb{F}^*$ such that $f_{k+1} = u_{k+1}\frac{\sigma(g_{k+1})}{g_{k+1}}f'_{k+1}$. Write $p := v\,g_1\dots g_k$, $q := u\,f_1\dots f_k$ and $q' := u'\,f'_1\dots f'_k$. Since $q\,f_{k+1} = \frac{\sigma(p)}{p}\frac{\sigma(g_{k+1})}{g_{k+1}}q'\,f'_{k+1}$, it follows that $f_{k+1} = h\,\frac{\sigma(g_{k+1})}{g_{k+1}}f'_{k+1}$ where $h := \frac{\sigma(p)}{p}\frac{q'}{q} \notin \mathbb{F}$. Note that all nontrivial factors in p, q, and q' are not σ-equivalent with any nontrivial factor in f_{k+1}. Hence also all nontrivial factors in $\sigma(p)$ and therefore also in h (at least one factor, since $h \notin \mathbb{F}$) are not σ-equivalent to the nontrivial factors in f_{k+1}. Conversely, any nontrivial factor in $\frac{\sigma(g_{k+1})}{g_{k+1}}f'_{k+1}$ is σ-equivalent with any nontrivial factor in f_{k+1}. Altogether, $f_{k+1} = \frac{\sigma(g_{k+1})}{g_{k+1}}f'_{k+1}\,h$ contains at least one nontrivial factor that is not σ-equivalent in f_{k+1}, a contradiction. Therefore there exists such a $u_{k+1} \in \mathbb{F}$, more precisely, we can take $u_{k+1} := h \in \mathbb{F}$. Moreover this means that $q = \frac{1}{h}\frac{\sigma(p)}{p}q'$ and hence we may apply the induction assumption which proves the theorem. □

Given a field of rational functions $\mathbb{F}(t)$, $f \in \mathbb{F}(t)$ can be uniquely represented with $f = \frac{f_1}{f_2}$ where $f_1, f_2 \in \mathbb{F}[t]$, $\gcd(f_1,f_2)=1$ and f_2 is monic. In the sequel we denote $\mathrm{num}(f) = f_1$ and $\mathrm{den}(f) = f_2$ as the numerator and denominator of f.

Definition 4.3. Let $(\mathbb{F}(t),\sigma)$ be a ΠΣ-extension of $(\mathbb{F},\sigma)$. $f \in \mathbb{F}(t)$ is *σ-reduced*, if for all $k \in \mathbb{Z}$ we have that $\gcd(\sigma^k(\mathrm{num}(f)),\mathrm{den}(f)) = 1$.

With this definition that generalizes the notions in [AP02] Theorem 4.1 will give the key idea to solve Problem *MPE*. Note that Lemma 4.3 is immediate.

Lemma 4.3. *Let $(\mathbb{F}(t),\sigma)$ be a ΠΣ-extension of $(\mathbb{F},\sigma)$ and $f = u\,f_1\dots f_k \in \mathbb{F}(t)$ with $f_i = \prod_{j=1}^{n_i}\sigma^j(h_i^{m_{ij}})$ be its σ-factorization. Then f is σ-reduced if and only if for all i we have that either $m_{ij} \ge 0$ for all j, or $m_{ij} \le 0$ for all j.*

Lemma 4.4. *Let $(\mathbb{F}(t),\sigma)$ be a ΠΣ-extension of $(\mathbb{F},\sigma)$ and $p,q \in \mathbb{F}[t]$ with $\sigma^k(p) = q$ for some $k \in \mathbb{Z}$. Then one can construct a $g \in \mathbb{F}[t]$ with $\deg(g) = |k|\,\deg(p)$ and $q = p\,\frac{\sigma(g^{sign(k)})}{g^{sign(k)}}$.*

Proof: If $k \geq 0$, take $g := \prod_{i=0}^{k-1} \sigma^i(p) \in \mathbb{F}[t]$. Then $\frac{\sigma(g)}{g} = \frac{\prod_{i=0}^{k-1} \sigma^{i+1}(p)}{\prod_{i=0}^{k-1} \sigma^i(p)} = \frac{\sigma^k(p)}{p} = \frac{q}{p}$. If $k < 0$, take $g := \prod_{i=1}^{-k} \sigma^{-i}(\frac{1}{p})$. Then $\frac{\sigma(g)}{g} = \frac{\prod_{i=1}^{-k} \sigma^{-i+1}(1/p)}{\prod_{i=0}^{-k} \sigma^{-i}(1/p)} = \frac{1/p}{\sigma^k(1/p)} = \frac{q}{p}$. Since $\deg(\sigma^i(p)) = \deg(p)$ for $i \in \mathbb{Z}$, the lemma follows. □

Theorem 4.1. *Let $(\mathbb{F}(t), \sigma)$ be a $\Pi\Sigma$-extension of $(\mathbb{F}, \sigma)$ and $f \in \mathbb{F}(t)$. Then there exists an $f' \in \mathbb{F}(t)$ with $f \equiv_\pi f'$ such that* $\deg(\text{den}(f')) < \deg(\text{den}(f))$ *or* $\deg(\text{num}(f')) < \deg(\text{num}(f))$ *if and only if f is not σ-reduced.*

Proof: Write $f = u\, f_1 \dots f_k$ in a σ-factorization where $f_i = \prod_{j=1}^{n_i} \sigma^j(h_i^{m_{ij}})$. First suppose that f is not σ-reduced. Then by Lemma 4.3 there exist k and r, s such that $m_{kr} > 0$ and $m_{ks} < 0$. If $r > s$, set $w := \sigma^s(h_k)$. Otherwise, if $r < s$, set $w := \sigma^r(1/h_k)$. Then $\frac{\sigma^r(h_k)}{\sigma^s(h_k)} = \frac{\sigma^l(w)}{w}$ for $l = |r - s|$. Hence by Lemma 4.4 there is a $g \in \mathbb{F}(t)^*$ with $\frac{\sigma(g)}{g} = \frac{\sigma^l(w)}{w} = \frac{\sigma^r(h_k)}{\sigma^s(h_k)}$. Thus for $f' := \frac{f\, \sigma^s(h_k)}{\sigma^r(h_k)}$ we have $\deg(\text{num}(f')) < \deg(\text{num}(f))$ and $\deg(\text{den}(f')) < \deg(\text{den}(f))$ with $f = \frac{\sigma(g)}{g} f'$. Conversely, suppose that there are $f', g \in \mathbb{F}(t)$ with $f = \frac{\sigma(g)}{g} f'$ such that $\deg(\text{den}(f')) < \deg(\text{den}(f))$ or $\deg(\text{num}(f')) < \deg(\text{num}(f))$. By Lemma 4.2 there exist $g_i \in \mathbb{F}(t)$ and $u_i \in \mathbb{F}(t)$ for all $1 \leq i \leq k$ such that $f_i = u_i \frac{\sigma(g_i)}{g_i} f'_i$. Moreover we may suppose that there exists a j such that $0 \leq \deg(\text{num}(f'_j)) < \deg(\text{num}(f_j))$ or $0 \leq \deg(\text{den}(f'_j)) < \deg(\text{den}(f_j))$; otherwise for f' it would follow that $\deg(\text{den}(f')) \geq \deg(\text{den}(f))$ and $\deg(\text{num}(f')) \geq \deg(\text{num}(f))$, a contradiction. Take such a j. Write $\frac{\sigma(g_j)}{g_j} = \frac{a}{b}$ with $a := \text{num}(\sigma(g_j))\, \text{den}(g_j) \in \mathbb{F}[t]$ and $b := \text{den}(\sigma(g_j))\, \text{num}(g_j) \in \mathbb{F}[t]$. Since $\deg(\text{num}(g_j)) = \deg(\text{num}(\sigma(g_j)))$ and $\deg(\text{den}(g_j)) = \deg(\text{den}(\sigma(g_j)))$, it follows that $\deg(a) = \deg(b)$. Moreover with $d := \deg(\gcd(a, b))$, we have $\deg(\text{num}(\frac{\sigma(g_j)}{g_j})) = \deg(a) - d = \deg(b) - d = \deg(\text{den}(\frac{\sigma(g_j)}{g_j}))$. Furthermore with $d' := \deg(\gcd(\text{num}(\frac{\sigma(g_j)}{g_j} f'_j), \text{den}(\frac{\sigma(g_j)}{g_j} f'_j)))$ it follows $\deg(\text{num}(f_j)) = \deg(\text{num}(\frac{\sigma(g_j)}{g_j} f'_j)) = \deg(\text{num}(f'_j)) + \deg(\text{num}(\frac{\sigma(g_j)}{g_j})) - d'$ and $\deg(\text{den}(f_j)) = \deg(\text{den}(\frac{\sigma(g_j)}{g_j} f'_j)) = \deg(\text{den}(f'_j)) + \deg(\text{den}(\frac{\sigma(g_j)}{g_j})) - d'$. Subtracting both equations gives $\deg(\text{num}(f_j)) - \deg(\text{num}(f'_j)) = \deg(\text{den}(f_j)) - \deg(\text{den}(f'_j))$. In particular one of those differences must be positive by the choice of j. Hence $\deg(\text{num}(f_j)) > 0$ and $\deg(\text{den}(f_j)) > 0$. But this means that f is not σ-reduced which proofs the theorem. □

Corollary 4.1. *Let $(\mathbb{F}(t), \sigma)$ be a $\Pi\Sigma$-extension of $(\mathbb{F}, \sigma)$ and $f \in \mathbb{F}(t)$. Any $f', g \in \mathbb{F}(t)$ with $f = \frac{\sigma(g)}{g} f'$ where f' σ-reduced is a solution of the Problem MPE.*

Proof: Suppose that there is a solution $\phi, \gamma \in \mathbb{F}(t)$ with $f = \frac{\sigma(\gamma)}{\gamma} \phi$ where the degree of the numerator or denominator of ϕ is smaller than that one of f'. Since $f \equiv_\pi \phi$ and $f \equiv_\pi f'$, we have $f' \equiv_\pi \phi$. Hence f' is not σ-reduced by Theorem 4.1, a contradiction. □

Remark 4.1. For the rational case, i.e., $(\mathbb{F}(t), \sigma)$ is the $\Pi\Sigma$-field over $\mathbb{F}$ with $\sigma(t) = t + 1$, such a representation of $f \in \mathbb{F}(t)$ with $f = \frac{\sigma(g)}{g} f'$, $f', g \in \mathbb{F}(t)$ and f' σ-reduced is called *rational normal form* in [AP02].

Lemma 4.3 in combination with Lemma 4.4 immediately gives a recipe to solve Problem *MPE*.

Algorithm 4.1. An algorithm for Problem *MPE*

(f', g)=`FindMinimalProductEquivalence`$((\mathbb{F}(t), \sigma), f)$

Input: A $\Pi\Sigma$-field $(\mathbb{F}(t), \sigma)$ over a computable constant field, $f \in \mathbb{F}(t)^*$.

Output: A solution $f', g \in \mathbb{F}(t)$ for the Problem *MPE*

(1) Compute a σ-factorization $f = u\, f_1 \dots f_k$ where $f_i = \prod_{j=0}^{n_i} \sigma^j(h_i^{m_{ij}})$.

(2) for all $1 \leq i \leq k$ and all $1 \leq j \leq n_i$ compute $g_{ij} := \prod_{l=0}^{j-1} \sigma^l(h_i^{m_{ij}})$.
(3) for all $1 \leq i \leq k$ compute $m_i := \sum_{l=1}^{n_i} m_{ij}$.
(4) RETURN $f' := u \prod_{l=1}^{k} h_i^{m_i}$ and $g := \prod_{i=1}^{k} \prod_{j=1}^{n_i} g_{ij}$.

Corollary 4.2. *Algorithm 4.1 is correct.*

Proof: Since $\mathbb{K}$ is computable, the σ-factorization of f can be computed. By Lemma 4.4 we have $\sigma^j(h_i^{m_{ij}}) = h_i^{m_{ij}} \frac{\sigma(g_{ij})}{g_{ij}}$, and hence $f = \frac{\sigma(g)}{g} f'$. By Lemma 4.3 f' is σ-reduced, and hence by Theorem 4.1 the degrees of numerator and denominator of f' are minimal. □

Example 4.4. In Example 4.1 the σ-factorization of f is $h^{-1} \sigma(h^2) \sigma^2(h) \sigma^3(h^{-1})$ for $h = \sigma(t)$. Following the strategy of Algorithm 4.1 we compute g and f' from Example 4.2 as $g = \big[1\big]^{-1} \big[h\big]^2 \big[h\,\sigma(h)\big]^1 \big[h\,\sigma(h)\,\sigma^2(h)\big]^{-1}$ and $f' = h^{-1+2+1-1} = \sigma(t)$.

Remark 4.2. We want to mention that Algorithm 4.1 returns just one of many f', g that solve Problem *MPE*. Actually for $f_i = \prod_{j=1}^{n_i} \sigma^j(h_i^{m_{ij}})$ Lemma 4.4 tells us, how any factor of the numerator can be eliminated with any factor of the denominator in f_i.

Corollary 4.3. *Let $(\mathbb{F}(t), \sigma)$ be a ΠΣ-field over a computable $\mathbb{K}$ and $f \in \mathbb{F}(t)^*$. If there are a $g \in \mathbb{F}(t)$ and an $f' \in \mathbb{F}$ with $f = \frac{\sigma(g)}{g} f'$, Algorithm 4.1 will compute such g and f'.*

Proof: This is follows by the minimal degrees of the numerator and denominator in f'. □

Example 4.5. Let $(\mathbb{K}(x), \sigma)$ be the ΠΣ-field over $\mathbb{K}$ with $\sigma(x) = x + 1$ and $f = \frac{(-x-2)(x+8)}{(x+5)^2}$. Then Algorithm 4.1 computes $g = \frac{(x+5)(x+6)(x+7)}{(x+2)(x+3)(x+4)}$ with $f = (-1) \frac{\sigma(g)}{g}$, which gives (3).

Remark 4.3. Let $(\mathbb{F}, \sigma)$ be a ΠΣ-field over a computable $\mathbb{K}$ with $\mathbb{F} = \mathbb{K}(t_1, \dots, t_e)$, and let $(\mathbb{F}(p), \sigma)$ be a Π-extension of $(\mathbb{F}, \sigma)$ with $f := \frac{\sigma(p)}{p} \in \mathbb{F}$. Then we want to emphasize that if there exists a Π-extension $(\mathbb{F}(p'), \sigma)$ of $(\mathbb{F}, \sigma)$ with $f' = \frac{\sigma(p')}{p'} \in \mathbb{K}(t_1, \dots, t_{e-1})$ which is $\mathbb{F}$-isomorphic to $(\mathbb{F}(p), \sigma)$, Algorithm 4.1 will find such an extension. Moreover it is important to mention that this simplification can be applied recursively. Hence one can find an $\mathbb{F}$-isomorphic Π-extension $(\mathbb{F}(p'), \sigma)$ of $(\mathbb{F}, \sigma)$ with $\frac{\sigma(p')}{p'} \in \mathbb{K}(t_1, \dots, t_i)$ where i is minimal.

5. Representation of a (q-)hypergeometric term with a Π-extension

In this section we will analyze which kind of (q-)hypergeometric terms can be represented in ΠΣ-fields. A sequence given by $h(n)$ is a *(q-)hypergeometric term* over $\mathbb{K}$, if for some $n \geq k_0$ on its quotient $h(n+1)/h(n)$ can be represented as rational function in $\mathbb{K}(n)$ (resp. $\mathbb{K}(q^n)$). In other words, a (q-)hypergeometric term $h(n)$ can be written as a product $h(n) = \prod_{k=k_0}^{n} f(k)$ where $f(k)$ can be represented as a rational function in k (resp. q^k). In the sequel it will turn out that only those (q-)hypergeometric terms cannot be expressed in a ΠΣ-field that are of the type $\gamma^n\, r(n)$ where $\gamma \neq 1$ is a root of unity and $r(n)$ is a rational function in n. Note that with the results of the previous section one can compute such a γ and $r(n)$, if $h(n) = \prod_{k=0}^{n} f(k)$ can be expressed as $\gamma^n\, r(k)$; see Corollary 4.3 and Example 4.5. In this context it is important to mention that generalizations [Sch01] of the algorithms in [Kar81, Sch02c] enable to search for solutions of linear difference equations involving objects like γ^n; although there are still open problems, these algorithms implemented in the summation package *Sigma* [Sch00] were successfully applied in various concrete examples like for instance in [Sch01, Sch03a].

Lemmas 5.1 and 5.2 provide some shortcuts for the central Lemma 5.3.

Lemma 5.1. *Let $(\mathbb{K}(t), \sigma)$ be a ΠΣ-field over $\mathbb{K}$, and let $\alpha \in \mathbb{K}^*$ be a root of unity. If there exists an $n > 0$ and a $g \in \mathbb{K}(t)$ with $\frac{\sigma(g)}{g} = \alpha^n$ then $g \in \mathbb{K}^*$ and $\alpha^n = 1$.*

Proof: Since α is a root of unity, we can find an $r \geq 1$ with $\alpha^r = 1$. Suppose there exists an $n > 0$ and a $g \in \mathbb{K}(t)$ with $\frac{\sigma(g)}{g} = \alpha^n$ Hence $1 = \alpha^{nr} = \frac{\sigma(g^r)}{g^r}$ and therefore $g^r \in \mathbb{K}$. Since $\mathbb{K}(t)$ is a field of rational functions, it follows that $g \in \mathbb{K}$. Therefore $1 = \frac{\sigma(g)}{g} = \alpha^n$. □

Lemma 5.2. *Let $\mathbb{K}$ be a field and $g, h \in \mathbb{K}^*$. If $g^n = h^n$ for some $n \in \mathbb{Z}$ then $g = v\,h$ for some $v \in \mathbb{K}^*$ with $v^n = 1$*

Proof: Since $1 = \frac{g^n}{h^n} = \left(\frac{g}{h}\right)^n$, we have $v := \frac{g}{h} \in \mathbb{K}^*$ with $v^n = 1$ and hence $g = v\,h$. □

Lemma 5.3. *Let $(\mathbb{K}(t), \sigma)$ be a Σ-extension of $(\mathbb{K}, \sigma)$ with constant field $\mathbb{K}$, $\alpha \in \mathbb{K}(t)^*$ and $n > 0$. Then there is a $g \in \mathbb{K}(t)$ with $\frac{\sigma(g)}{g} = \alpha^n$ iff there is a $g' \in \mathbb{K}(t)$ with $\frac{\sigma(g')}{g'} = v\,\alpha$ for some $v \in \mathbb{K}^*$ with $v^n = 1$.*

Proof: The direction from right to left is immediate by taking $g := g'^n$. We consider the proof direction from left to right. If α is a root of unity, we may apply Lemma 5.1, and it follows that $\alpha^n = 1$. Hence we can choose $g' := 1$ and $v := \alpha^{n-1}$ with $v^n = 1$ which shows that $1 = \alpha\,v = \frac{\sigma(g')}{g'}$. Otherwise suppose that $\alpha^n \neq 1$ and hence that $g \notin \mathbb{K}$. We can write g in form of its σ-factorization $g = u\,g_1 \cdots g_k$, $k > 0$, where $u \in \mathbb{K}^*$, $\gcd(g_i, \sigma^l(g_j)) = 1$ for all $i \neq j$, and $l \in \mathbb{Z}$ and

$$g_i = \prod_{j=0}^{r_i} \sigma^j(h_i)^{m_{ij}} \neq 1 \tag{7}$$

where $h_i \in \mathbb{K}[t] \setminus \mathbb{K}$ is irreducible and $m_{ij} \in \mathbb{Z}$. Then it follows that $\frac{\sigma(g)}{g} = \alpha^n$ holds only, if for all $1 \leq i \leq k$ and all $0 \leq j \leq r_i - 1$ we have that $n \mid (m_{i,j+1} - m_{i,j})$ and $n \mid m_{i,r_i}$. But because of $n \mid m_{i,r_i}$ and $n \mid (m_{i,r_i} - m_{i,r_i-1})$, it follows that $n \mid m_{i,r_i-1}$. Applying this argument r_i times proves that $n \mid m_{ij}$ for all $1 \leq i \leq k$ and all $1 \leq j \leq r_i$. Hence $g_i = g_i'^n$ for $g_i' := \prod_{j=0}^{r_i} \sigma^j(h_i)^{m_{ij}/n} \in \mathbb{K}[t]$ for all $1 \leq i \leq k$. But this proves that there exists a $g' \in \mathbb{K}(t)$ with $g = u\,g'^n$. Since $u \in \mathbb{K}^*$, $\sigma(u) = u$ and therefore $\alpha^n = \frac{\sigma(g)}{g} = \frac{\sigma(g'^n)}{g'^n} = \left(\frac{\sigma(g')}{g'}\right)^n$. Together with Lemma 5.2 the statement is proven. □

A direct consequence of Lemma 5.3 and Theorem 2.1 shows

Theorem 5.1. *Let $(\mathbb{K}(t), \sigma)$ be a $\Pi\Sigma$-field over $\mathbb{K}$ where $\sigma(t) = t + 1$. Then there exists a Π-extension $(\mathbb{K}(t)(p), \sigma)$ of $(\mathbb{K}(t), \sigma)$ with $\alpha := \frac{\sigma(p)}{p} \in \mathbb{K}$ if and only if there do not exist a $g \in \mathbb{K}(t)$ and a root of unity $v \in \mathbb{K}^*$ with $\frac{\sigma(g)}{g} = v\,\alpha$.*

Now consider the hypergeometric term $h(n) = \prod_{k=k_0}^{n} f(k)$ with $f(n) \in \mathbb{K}(n)$ and the $\Pi\Sigma$-field $(\mathbb{K}(n), \sigma)$ over $\mathbb{K}$ with $\sigma(n) = n + 1$. Moreover suppose that there does not exist a Π-extension $(\mathbb{K}(n)(p), \sigma)$ with $\sigma(p) = \alpha\,p$. Under this assumption we obtain immediately, how $h(n)$ must look like. By Theorem 5.1 there exists a root of unity γ and an $r(n) \in \mathbb{K}(n)$ such that $\frac{r(n+1)}{r(n)} = \gamma\,f(n)$. Hence for $g(n) := (1/\gamma)^n\,r(n)$, $1/\gamma$ a root of unity, it follows that $\frac{g(n+1)}{g(n)} = f(n)$. Therefore from a fixed k_1 on and constant $c \in \mathbb{K}^*$ we have that

$$h(n) = c\,g(n) = c\,(1/\gamma)^n\,r(n), \quad n \geq k_1.$$

In particular this gives two cases: **(1)** $\gamma = 1$, i.e., $h(n) = r(n)$ can be rephrased in the $\Pi\Sigma$-field $(\mathbb{K}(n), \sigma)$. **(2)** $\gamma \neq 1$, i.e., $h(n)$ cannot be represented in a $\Pi\Sigma$-field.

Finally we turn to the q-hypergeometric case.

Lemma 5.4. *Let $(\mathbb{K}(t),\sigma)$ be a Π-extension of $(\mathbb{K},\sigma)$ with $\sigma(t)=a\,t$ and constant field $\mathbb{K}$, $\alpha\in\mathbb{K}(t)^*$ and $n>0$. Then there is a $g\in\mathbb{K}(t)$ with $\frac{\sigma(g)}{g}=\alpha^n$ if and only if there is a $g'\in\mathbb{K}(t)$ with $\frac{\sigma(g')}{g'}=v\,b\,\alpha$ where $v\in\mathbb{K}^*$ with $v^n=1$ and $b^n=a^z$ for some $b\in\mathbb{K}$ and $z\in\mathbb{Z}$.*

Proof: The direction from right to left is immediate by taking $g:=g'^n\,t^z$. So we turn to the other proof direction. If α is a root of unity, we follow the proof of Lemma 5.3. Otherwise suppose that $\alpha^n\neq 1$, and hence $g\notin\mathbb{K}$. We can write g in its σ-factorization form $g=u\,t^z\,g_1\cdots g_k$ where $u\in\mathbb{K}^*$, $z\in\mathbb{Z}$, $\gcd(g_i,\sigma^l(g_j))=1$ for all $i\neq j$ and $l\in\mathbb{Z}$, and (7) where $h_i\in\mathbb{K}[t]\setminus\mathbb{K}$ is irreducible, $t\nmid h_i$ and $m_{ij}\in\mathbb{Z}$. If $k=0$, $g=u\,t^z$. Otherwise, suppose $k>0$. Then following the argumentation of Lemma 5.3, $\frac{\sigma(g)}{g}=\alpha^n$ holds only, if $n\mid m_{ij}$ for all $1\leq i\leq k$ and all $1\leq j\leq r_i$. Hence $g_i=g_i'^n$ for $g_i'=\prod_{j=0}^{r_i}\sigma^j(h_i)^{m_{ij}/n}$. But this proves that there exists a $g'\in\mathbb{K}(t)$ with $g=u\,t^z\,g'^n$ for $k=0$ or $k>0$. Since $u\in\mathbb{K}^*$, $\sigma(u)=u$ and therefore $\alpha^n=\frac{\sigma(g)}{g}=a^z\frac{\sigma(g'^n)}{g'^n}=a^z\big(\frac{\sigma(g')}{g'}\big)^n$. Take $b:=\frac{\alpha\,g'}{\sigma(g')}\in\mathbb{K}(t)$. Then $b^n=a^z\in\mathbb{K}^*$, therefore $b\in\mathbb{K}^*$, and hence $\alpha^n=\big(b\,\frac{\sigma(g')}{g'}\big)^n$. Thus the lemma is proven by Lemma 5.2. □

Lemma 5.5. *Let $\mathbb{K}(q)$ be a rational function field, $b\in\mathbb{K}(q)^*$ and $n>0$. Then $b^n=q^z$ for some $z\in\mathbb{Z}$ if and only if $b=u\,q^r$ for some $r\in\mathbb{Z}$ and $u\in\mathbb{K}^*$ with $u^n=1$.*

Proof: The implication from right to left follows immediately. For the other proof direction suppose first that $z=0$. Then $b^n=1$, therefore $b\in\mathbb{K}^*$, and setting $u:=b$ and $r:=0$ shows this implication. Now suppose that $z>0$ and $b^n=q^z$. If $b\in\mathbb{K}(q)\setminus\mathbb{K}[q]$ then $b^n\notin\mathbb{K}[q]$, a contradiction. Hence $b\in\mathbb{K}[q]$. Since $z>0$, $b\in\mathbb{K}[q]\setminus\mathbb{K}$, and therefore $r:=\deg(b)>0$. Moreover, it follows that $\deg(b)\,n=z>0$. Thus we can write $b^n=(q^r)^n$. Therefore by Lemma 5.2 $b=q^r\,u$ for some $u\in\mathbb{K}(q)^*$ with $u^n=1$. Hence $u\in\mathbb{K}^*$ which proves this case. Otherwise, if $z<0$, consider $(\frac{1}{b})^n=q^{-z}$. Then by the same argumentation, it follows that $\frac{1}{b}=q^r\,u$ for some $r\geq 0$ and $u\in\mathbb{K}^*$ with $u^n=1$. Thus $b=q^{-r}\,\frac{1}{u}$ with $\big(\frac{1}{u}\big)^n=1$. □

A direct consequence of Theorem 2.1, Lemma 5.4, and Lemma 5.5 gives

Theorem 5.2. *Let $(\mathbb{K}(q)(t),\sigma)$ be a ΠΣ-field over $\mathbb{K}(q)$, q transcendental over $\mathbb{K}$, where $\sigma(t)=q\,t$. Then there exists a Π-extension $(\mathbb{K}(q)(t)(p),\sigma)$ of $(\mathbb{K}(q)(t),\sigma)$ with $\alpha=\frac{\sigma(p)}{p}\in\mathbb{K}(q)$ if and only if there do not exist a $g\in\mathbb{K}(t)$ and a root of unity $v\in\mathbb{K}^*$ with $\frac{\sigma(g)}{g}=v\,\alpha$.*

6. Hypergeometric terms in ΠΣ-fields and certain difference rings extensions

In the end of Subsection 2.2 it is indicated that the construction of Π-extensions for a given nested product/sum expression might lead to problems. In the sequel this fact will be illustrated in more details. Assume that we want to find the right hand side of the identity

$$\sum_{k=0}^{n}\frac{(2^k+3k-4)4^k}{(2^k+k)(2^k+2k-2)}=\frac{2^n+2(4^n)+n}{2^n+n}\tag{8}$$

with our difference field machinery. As in Subsection 2.2 indicated, we try to construct a ΠΣ-field in which the summand $f(k)$ can be represented. In our concrete example we start with the constant field $\mathbb{Q}$ and build up a ΠΣ-field that enables to formulate the sequences given by $k\to 4^k\to 2^k$. In order to represent the summation object k with its shift $S\,k=k+1$, we first construct the Σ-extension $(\mathbb{Q}(x),\sigma)$ of $(\mathbb{Q},\sigma)$ with $\sigma(x)=x+1$; Theorem 2.1 ensures that this is indeed a Σ-extension. Next we try to formulate the sequence given by 4^k in $(\mathbb{Q}(x),\sigma)$. Since there does not exist an $n>0$ such that $4^n\in\mathrm{H}_{(\mathbb{Q}(x),\sigma)}$, it follows by Theorem 2.1 that we can adjoin 4^k to our difference field in form of a Π-extension $(\mathbb{Q}(x)(p),\sigma)$ of $(\mathbb{Q}(x),\sigma)$ with

$\sigma(p) = 4\,p$. Next we want to express the product $2^k = \prod_{l=1}^{k} 2$ in this difference field. We check algorithmically that there does not exist a $g \in \mathbb{F}$ with $\sigma(g) = 2\,g$. On the other side we fail to adjoin this product in form of a Π-extension by Theorem 2.1, since $2^2 = \frac{\sigma(p)}{p} \in \mathrm{H}_{(\mathbb{Q}(x)(p),\sigma)}$. Loosely speaking, one can avoid this problem by adjoining 2^k before 4^k, i.e. constructing the Π-extension $(\mathbb{Q}(x)(p'),\sigma)$ with $\sigma(p') = 2\,p'$ and afterwards rephrase 4^n as $t_1'^2 \in \mathbb{Q}(x)(p')$. Then the indefinite summation problem can be posed as follows: find a $g' \in \mathbb{Q}(x)(p')$ with $\sigma(g') - g' = \frac{p'^2(p'+3x-4)}{(p'+p')(p'+2p'-2)}$. For instance with our package *Sigma* [Sch00] we compute the solution $g' = p'^2/(p' + 2x - 2)$ which means that $g(k) = (2^k)^2/((2^k) + 2k - 2)$ is a solution of $g(k+1) - g(k) = f(k)$. With telescoping we immediately obtain the right hand side from (8). Intuitively one can avoid many such problems, if one splits products into smallest possible atomics, like $\prod_{l=1}^{k}(4l) = \big(\prod_{l=1}^{k} 2\big)^2 \prod_{l=1}^{k} l$; adjoining objects like $k!$ or 2^k cannot cause anymore problems. But dealing with $\prod_{l=1}^{k}(-4l) = \big(\prod_{l=1}^{k} -2\big)^2 \prod_{l=1}^{k} l = \big(\prod_{l=1}^{k} 2\big)^2 \prod_{l=1}^{k} -l$ might cause problems, if afterwards one also needs $k!$ and 2^k. Actually, one could handle also such kind of problems, if one allows difference ring extensions like $(-1)^k$; then one could split the above product into $\prod_{l=1}^{k}(-4l) = (-1)^k\big(\prod_{l=1}^{k} 2\big)^2 \prod_{l=1}^{k} l$. Summarizing, splitting products into smaller parts enables to construct a $\Pi\Sigma$-field for a given multisum expression in many instances. In particular, if one fails to represent such an expression in a $\Pi\Sigma$-field, one can try to extract a product γ^k where γ a root of unity such that all other products can be rephrased in a Π-extension. As already emphasized in the beginning of Section 5, terms like γ^n can be treated at least partially algorithmically to solve linear difference equations.

The above considerations will be formalized in Theorem 6.2 and Corollary 6.1 for the $\Pi\Sigma$-field $(\mathbb{K}(x),\sigma)$ over $\mathbb{K}$ with $\sigma(x) = x + 1$. In order to achieve this, we will suppose that the constant field is given as the quotient field of a unique factorization domain $\mathbb{U}$. Throughout this section the factorization in a unique factorization domain $\mathbb{U}[x]$ will play a major role. So for $\mathbb{U} := \mathbb{Z}$ the complete factorization of $6x^3 + 6x^2 - 6x - 6$ is $2 \cdot 3(x + 1)^2(x - 1)$ and for $\mathbb{U} := \mathbb{Z}[i]$ it is $-i(i + 1)^2 3(x + 1)^2(x - 1)$. We want to emphasize that in this section we understand under the factorization $f \in \mathbb{U}[x]$ not only the factorization of polynomials over $\mathbb{U}$, but also the factorization of the content in $\mathbb{U}$ of an element in $\mathbb{U}[x]$. Moreover recall that each element $f \in \mathbb{K}(x)$ can be represented in the form $f = \prod_{i=1}^{n} f_i^{m_i}$ where the $f_i \in \mathbb{U}[x]$ are irreducible, pairwise prime and $m_i \in \mathbb{Z}$; if $m_i \geq 0$, $f \in \mathbb{U}[x]$. An irreducible element $f \in \mathbb{U}[x]$ is an $\mathbb{U}[x]$-*factor* in $g \in \mathbb{U}[x]$ (resp. $g \in \mathbb{K}(x)$), if there exists an i and a unit $u \in \mathbb{U}^*$ such that $g = u\,f_i$. So for instance in $2\,x \in \mathbb{Z}[x]$ we have that 2 and x are $\mathbb{Z}[x]$-factors. Similarly 2, 3 and x are $\mathbb{Z}[x]$-factors in $\frac{2}{3x} \in \mathbb{Q}(x)$.

In the sequel we will consider the following subclass of $\Pi\Sigma$-fields; for examples see Remark 3.2.

Property 6.1. Let $\mathbb{U}$ be a unique factorization domain where all units are roots of unity, $\mathbb{K}$ be its quotient field, and $(\mathbb{K}(x),\sigma)$ be the $\Pi\Sigma$-field with $\sigma(x) = x + 1$ over $\mathbb{K}$.

First we show some important properties for $\mathbb{U}[x]$ that are related to Subsection 2.3.

Proposition 6.1. *Let $(\mathbb{K}(x),\sigma)$ be a $\Pi\Sigma$-field with Property 6.1. Then $(\mathbb{K}(x),\sigma)$ is a difference ring extension of the difference ring $(\mathbb{U}[x],\sigma)$ with $\sigma(x) = x + 1$. Moreover, if $f \in \mathbb{U}[x]$ is irreducible, $\sigma^k(f)$ is irreducible for any $k \in \mathbb{Z}$.*

Proof: Recall that $\mathbb{K}(x)$ is the quotient field of $\mathbb{K}[x]$. Since $\mathbb{K}$ is the quotient field of $\mathbb{U}$, $\mathbb{K}(x)$ is the quotient field of $\mathbb{U}[x]$. Hence $\mathbb{U}[x]$ is a subring of $\mathbb{K}(x)$. Since $\sigma^k(f) \in \mathbb{U}[x]$ for any $f \in \mathbb{U}[x]$ and $k \in \mathbb{Z}$, $(\mathbb{Q}(x),\sigma)$ is a difference ring extension of $(\mathbb{U}[x],\sigma)$. Now let $f \in \mathbb{U}[x]$ be irreducible and suppose that $\sigma^k(f)$ is reducible for some $k \in \mathbb{Z}$, i.e., we find $f_1, f_2 \in \mathbb{U}[t]$ with $\sigma^k(f) = f_1\,f_2$ where the f_i are not units. Hence $f = \sigma^{-k}(f_1)\,\sigma^{-k}(f_2)$ where

$\sigma^{-k}(f_1), \sigma^{-k}(f_2) \in \mathbb{U}[x]$. In particular this means that also the $\sigma^{-k}(f_i)$ cannot be units, since otherwise $\sigma^{-k}(f_i) \in \mathbb{U}$, and hence $\sigma^{-k}(f_i) = f_i$, a contradiction. But this means that we find a nontrivial factorization $f = \sigma^{-k}(f_1)\,\sigma^{-k}(f_2)$, a contradiction. Consequently $\sigma^k(f)$ is irreducible for any $k \in \mathbb{Z}$. □

Definition 6.1. Let $(\mathbb{U}[x], \sigma)$ be a difference ring with $\sigma(x) = x + 1$ where $\mathbb{U}$ is a unique factorization domain. $f \in \mathbb{U}[x]$ is σ-prime to $g \in \mathbb{U}[x]$, if $\gcd(\sigma^k(f), g) = 1$ for all $k \in \mathbb{Z}$.

Note that $f \in \mathbb{U}[x]$ is σ-prime to $g \in \mathbb{U}[x]$ if and only if g is σ-prime to f; in short we will just say that f, g are σ-prime, or not σ-prime.

Lemma 6.1. *Let $(\mathbb{K}(x), \sigma)$ be a ΠΣ-field over a semi-computable $\mathbb{K}$ with Property 6.1 and $f, g \in \mathbb{U}[x]$ be irreducible. Then one can decide algorithmically if f, g are σ-prime.*

Proof: By Proposition 6.1 $\sigma^k(f) \in \mathbb{U}[x]\setminus\mathbb{U}$ is irreducible for any $k \in \mathbb{Z}$. Hence f, g are σ-prime iff there does not exist a $k \in \mathbb{Z}$ with $\frac{\sigma^k(f)}{g} \in \mathbb{K}$. Thus the lemma holds by Theorem 2.3. □

Lemma 6.2, which is closely related to Lemma 4.4, gives the main tool to express an atomic product in the already constructed Π-extension.

Lemma 6.2. *Let $(\mathbb{K}(x), \sigma)$ be a ΠΣ-field with Property 6.1 and $(\mathbb{K}(x)(p_1, \dots, p_e), \sigma)$ be a Π-extension of $(\mathbb{K}(x), \sigma)$ with $\alpha_i := \frac{\sigma(p_i)}{p_i} \in \mathbb{U}[x]$ irreducible. If $f \in \mathbb{U}[x]$ is irreducible but not σ-prime with an α_j, $1 \le j \le e$, there is a $g \in \mathbb{K}(x)^*$ with $f = u\,\frac{\sigma(g\,t_j)}{g\,t_j}$ for some root of unity u. If $\mathbb{K}$ is semi-computable, such a g and u can be computed.*

Proof: Since f, α_j are not σ-prime, we can write $f = u\,\sigma^k(\alpha_j)$ for a $k \in \mathbb{Z}$ and a unit $u \in \mathbb{U}$. If $k \ge 0$, take $g := \prod_{i=0}^{k-1} \sigma^i(\alpha_j)$. Then $u\,\frac{\sigma(g\,t_j)}{g\,t_j} = u\,\frac{\prod_{i=1}^{k} \sigma^i(\alpha_j)}{\prod_{i=0}^{k-1} \sigma^i(\alpha_j)}\alpha_j = u\,\sigma^k(\alpha_j) = f$. If $k < 0$, take $g := \prod_{i=1}^{-k} \frac{1}{\sigma^{-i}(\alpha_j)}$. Then $u\,\frac{\sigma(g\,t_j)}{g\,t_j} = u\,\frac{\prod_{i=1}^{-k} \sigma^{-i}(\alpha_j)}{\prod_{i=0}^{-k+1} \sigma^{-i}(\alpha_j)}\,\alpha_j = u\,\sigma^k(\alpha_j) = f$. If $\mathbb{K}$ is semi-computable, k can be computed by Theorem 2.3, and hence also u and g. □

Lemma 6.3 and 6.4 are needed to prove Theorem 6.1 which gives a criterion if certain hypergeometric terms can be represented with a Π-extension.

Lemma 6.3. *Let $(\mathbb{K}(x), \sigma)$ be a ΠΣ-field with Property 6.1. Suppose that the $\alpha_1, \dots, \alpha_e \in \mathbb{U}[x]$, $e \ge 1$, are irreducible and pairwise σ-prime. Then for $m_i \in \mathbb{Z}$, not all m_i zero, there does not exist a $u \in \mathbb{K}(x)$ such that $\frac{\sigma(u)}{u} = \alpha_1^{m_1} \dots \alpha_e^{m_e}$.*

Proof: Suppose there exists such a $u \in \mathbb{K}(x)$. Take any j, $1 \le j \le e$, with $m_j \ne 0$. First suppose that $\alpha_j \in \mathbb{U}$. Write $u = \prod_{j=1}^{r} p_i^{n_i}$ in its prime factorization with $p_i \in \mathbb{U}[x]$. If $p_i \notin \mathbb{U}$, $\alpha_j \nmid p_i$. Since $\sigma(p_i) \notin \mathbb{U}$ is also prime, $\alpha_j \nmid \sigma(p_i)$. Otherwise, if $p_i \in \mathbb{U}$, $\frac{\sigma(p_i)}{p_i} = 1$. Hence α_j cannot be a $\mathbb{U}[x]$-factor in $\frac{\sigma(u)}{u}$, a contradiction to $m_j \ne 0$. Therefore we may suppose that $\alpha_j \in \mathbb{U}[x] \setminus \mathbb{U}$ with $m_j \ne 0$. Now let $m \in \mathbb{Z}$ be maximal such that the irreducible $\sigma^m(\alpha_j) \in \mathbb{U}[X]$ is a $\mathbb{U}[x]$-factor in u. Then it follows that $\sigma^{m+1}(\alpha_j) \in \mathbb{U}[X]$ is a $\mathbb{U}[x]$-factor of $\sigma(u)$ but not of u. Therefore $\sigma^{m+1}(\alpha_j)$ must be a $\mathbb{U}[x]$-factor in $\frac{\sigma(u)}{u}$. Since the α_i are pairwise σ-prime, it follows that $\sigma^{m+1}(\alpha_j) = \alpha_j$, and hence $m = -1$. Now let $l \in \mathbb{Z}$ be minimal such that $\sigma^l(\alpha_j) \in \mathbb{U}[X]$ is a $\mathbb{U}[x]$-factor in u. Clearly $l \le m = -1$. Moreover $\sigma^l(\alpha_j)$ is a $\mathbb{U}[x]$-factor in u but not in $\sigma(u)$, otherwise l is not minimal. Therefore $\sigma^l(\alpha_j)$ must be also a $\mathbb{U}[x]$-factor in $\frac{\sigma(u)}{u}$. Since the α_i are pairwise σ-prime, it follows that $\sigma^l(\alpha_j) = \alpha_j$, and hence $l = 0$, a contradiction to $l < -1$. □

Lemma 6.4. *Let $(\mathbb{K}(x),\sigma)$ be a $\Pi\Sigma$-field with Property 6.1 and $(\mathbb{K}(x)(p_1,\dots,p_e),\sigma)$ be a Π-extension of $(\mathbb{K}(x),\sigma)$ with $\alpha_i := \frac{\sigma(p_i)}{p_i} \in \mathbb{U}[x]$ irreducible. Then the α_i are pairwise σ-prime.*

Proof: Suppose that α_i, α_j are not σ-prime for some $i < j$. Since the α_i are irreducible, by Lemma 6.2 there is a $g \in \mathbb{K}(x)$ and a unit $u \in \mathbb{U}$ with $\frac{\sigma(g)}{g} = u\,\alpha_j$. By assumption u is a root of unity and thus $u^m = 1$ for some $m > 0$. Hence $\frac{\sigma(g^m)}{g^m} = \alpha_j^m$, and thus $(\mathbb{F}(p_1,\dots,p_{j-1})(p_j),\sigma)$ is not a Π-extension of $(\mathbb{F}(p_1,\dots,p_{j-1}),\sigma)$ by Theorem 2.1, a contradiction. □

Lemma 6.5. *Let $(\mathbb{F}(t_1,\dots,t_e),\sigma)$ be a $\Pi\Sigma$-extension of $(\mathbb{F},\sigma)$ where for any Π-extension t_i we have $\frac{\sigma(t_i)}{t_i} \in \mathbb{F}^*$. If there is a $g \in \mathbb{F}(t_1,\dots,t_e)^*$ with $\frac{\sigma(g)}{g} \in \mathbb{F}$ then $g = w\,t_1^{k_1}\cdots t_e^{k_e}$ where $w \in \mathbb{F}^*$ and $k_i \in \mathbb{Z}$. In particular, $k_i = 0$, if t_i is a Σ-extension.*

Proof: We proof the corollary by induction on n. For $e = 0$ nothing has to be proven. Now suppose that the corollary holds for $e \geq 0$ and consider a $\Pi\Sigma$-extension $(\mathbb{E}(t_{e+1}),\sigma)$ of $(\mathbb{E},\sigma)$ with $\mathbb{E} = \mathbb{F}(t_1,\dots,t_e)$. Let $g \in \mathbb{E}(t_{e+1})$ such that $\alpha := \frac{\sigma(g)}{g} \in \mathbb{F}$. Applying Theorem 2.2 we get $g = w\,t_{e+1}^{k_{e+1}}$ where $w \in \mathbb{E}$ with $k_{e+1} \in \mathbb{Z}$. In particular, if t_{e+1} is a Σ-extension, it follows that $k_{e+1} = 0$, and hence $g \in \mathbb{E}$. By the induction assumption this case is proven. Otherwise, if t_{e+1} is a Π-extension, we have $\alpha = \frac{\sigma(g)}{g} = \frac{\sigma(w)}{w} f^{k_{e+1}}$ with $f := \frac{\sigma(t_{e+1})}{t_{e+1}} \in \mathbb{F}$ and thus $\frac{\sigma(w)}{w} = \frac{\alpha}{f^{k_{e+1}}} \in \mathbb{F}$. Together with the induction assumption the corollary is proven. □

Theorem 6.1. *Let $(\mathbb{K}(x),\sigma)$ be a $\Pi\Sigma$-field with Property 6.1 and $(\mathbb{K}(x)(p_1,\dots,p_e),\sigma)$ be a Π-extension of $(\mathbb{K}(x),\sigma)$ with $\alpha_i := \frac{\sigma(p_i)}{p_i} \in \mathbb{U}[x]$ irreducible. Moreover let $\alpha \in \mathbb{U}[x]$ be irreducible. Then there exists a Π-extension $(\mathbb{K}(x)(p_1,\dots,p_e)(p),\sigma)$ of $(\mathbb{K}(x)(p_1,\dots,p_e),\sigma)$ with $\sigma(p) = \alpha\,p$ if and only if α is σ-prime with all the α_i.*

Proof: By Lemma 6.4 all the α_i are pairwise σ-prime. In particular, if $(\mathbb{K}(x)(p_1,\dots,p_e)(p),\sigma)$ is a Π-extension of $(\mathbb{K}(x)(p_1,\dots,p_e),\sigma)$ with $\sigma(p) = \alpha\,p$, also α is σ-prime with all the α_i. This proves the direction form left to right. Conversely, suppose that there does not exist such a Π-extension. Then by Theorem 2.1 there exists a $g \in \mathbb{F}$ and $n > 0$ such that $\frac{\sigma(g)}{g} = \alpha^n$. By Lemma 6.5 we have $g = w\,p_1^{k_1}\cdots p_e^{k_e}$ for some $w \in \mathbb{K}(x)$ with $k_i \in \mathbb{Z}$. Hence $\frac{\sigma(w)}{w} = \alpha^n\,\alpha_1^{-k_1}\cdots\alpha_e^{-k_e}$ where $n > 0$ and $\alpha,\alpha_1,\dots,\alpha_e \in \mathbb{U}[x]$ are irreducible. Now suppose that α is σ-prime with all the α_i. Then we may apply Lemma 6.3, and it follows that there does not exist a $w \in \mathbb{K}(x)^*$, a contradiction. Hence α is not σ-prime with one of the α_i which proves the theorem. □

Together with Lemma 6.1, Lemma 6.2 and Theorem 6.1 one finally can design Π-extensions in which one can represent arbitrary hypergeometric terms up to the multiplication with a root of unit.

Theorem 6.2. *Let $(\mathbb{K}(x),\sigma)$ be a $\Pi\Sigma$-field with Property 6.1 and $\alpha_1,\dots,\alpha_r \in \mathbb{K}(x)^*$. Then there exists a Π-extension $(\mathbb{E},\sigma)$ of $(\mathbb{F},\sigma)$ with the following property: for all $1 \leq i \leq r$ there is a $g_i \in \mathbb{E}$ and a root of unity $u_i \in \mathbb{U}^*$ with $\alpha_i = u_i\,\frac{\sigma(g_i)}{g_i}$. If $\mathbb{K}$ is semi-computable and one can factorize in $\mathbb{U}[x]$, such a Π-extension together with the u_i and g_i can be constructed.*

Proof: Write $\alpha_i = w_i \prod_{j=1}^{\lambda} f_j^{m_{ij}}$ where the $f_j \in \mathbb{U}[x]$ are irreducible and pairwise prime, $m_{ij} \in \mathbb{Z}$ and w_j a root of unity. We will show by induction on λ that there exists a Π-extension $(\mathbb{E},\sigma)$ of $(\mathbb{K}(x),\sigma)$ such that for all f_j there exists a $g_j \in \mathbb{E}$ and a root of unity $u_j \in \mathbb{U}^*$ with $\frac{\sigma(g_j)}{g_j} = u_j\,f_j$. Moreover, the extension $\mathbb{E} = \mathbb{F}(p_1\dots,p_e)$ will be constructed in such a way that all $\frac{\sigma(p_i)}{p_i} \in \mathbb{U}[x]$ are irreducible, more precisely we will have that $\frac{\sigma(p_i)}{p_i} \in \{f_1,\dots,f_\lambda\}$.

Given this result, it will follow that $\frac{\sigma(h_i)}{h_i} = v_i\,\alpha_i$ for the root of unity $v_i := w_i\,\prod_{j=1}^{\lambda} u_j^{m_{ij}}$ and $h_i := \prod_{j=1}^{\lambda} g_j^{m_{ij}} \in \mathbb{E}$, which will prove the first part of the theorem.
First we consider the base case $\lambda = 1$. By Lemma 6.3 there do not exist a $g \in \mathbb{K}(x)$ and an $n > 0$ such that $\frac{\sigma(g)}{g} = f_1^n$. Hence by Theorem 2.1 we can construct a Π-extension $(\mathbb{K}(x)(p_1), \sigma)$ of $(\mathbb{K}(x), \sigma)$ with $\frac{\sigma(p_1)}{p_1} = f_1$. Now suppose that for an s with $\lambda > s \geq 1$ we already have constructed a Π-extension $(\mathbb{E}, \sigma)$ of $(\mathbb{K}(x), \sigma)$ with the above assumptions. If f_{s+1} is σ-prime with all the $\frac{\sigma(p_i)}{p_i}$ for $1 \leq i \leq e$, by Theorem 6.1 we can construct a Π-extension $(\mathbb{E}(p_{e+1}), \sigma)$ of $(\mathbb{E}, \sigma)$ with $\frac{\sigma(p_{e+1})}{p_{e+1}} = f_{s+1}$ and we can set $g_{s+1} := p_{e+1}$. Applying our induction assumption together with the property of f_{s+1} the property still holds that $\frac{\sigma(p_i)}{p_i} \in \{f_1, \dots, f_{s+1}\}$ for all $1 \leq i \leq e+1$, i.e., $\frac{\sigma(p_i)}{p_i}$ is irreducible. Otherwise, if f_{e+1} is not σ-prime to one of the $\frac{\sigma(p_i)}{p_i}$, there exists by Lemma 6.2 a $g \in \mathbb{E}$ and a root of unity u such that $\frac{\sigma(g)}{g} = u\,f_{s+1}$. This proves the first part of the theorem.
Now suppose that $\mathbb{K}$ is semi-computable and one can compute the prime factorization in $\mathbb{U}[x]$. Hence the prime factorizations for the $\alpha_i = w_i\,\prod_{j=1}^{\lambda} f_j^{m_{ij}}$ can be computed. Moreover, by Lemma 6.1 one can check algorithmically if f_{s+1} is σ-prime with all the α_i. In particular, in case of existence, one compute such a $g \in \mathbb{E}$ and u as stated above with $\frac{\sigma(g)}{g} = u\,f_{s+1}$ by Lemma 6.2. This finishes the constructive part of the theorem. □

So far the above theorem proposes to split all products into atomics and to adjoin them (up to a root of unit) in form of Π-extension. It is important to mention that one can avoid to adjoin unnecessary products, if one first simplifies the given products as suggested in Corollary 4.3.

Next we show that hypergeometric terms can be expressed with one additional difference ring extension. For this result we need the following lemma; for a proof see [Sch01, Lemma 3.6.2].

Lemma 6.6. *Let $(\mathbb{F}, \sigma)$ a difference field and $1 \neq \gamma \in \mathbb{F}$ be a k-th root of unity. Then there is a difference ring extension $(\mathbb{F}[y], \sigma)$ of $(\mathbb{F}, \sigma)$ with $y \notin \mathbb{F}$, $\mathrm{const}_\sigma\mathbb{F}[y] = \mathrm{const}_\sigma\mathbb{F}$, $\sigma(y) = \gamma\,y$ and $y^k = 1$.*

Corollary 6.1. *Let $(\mathbb{K}(x), \sigma)$ be a ΠΣ-field with Property 6.1. Then for $\alpha_1, \dots, \alpha_r \in \mathbb{K}(x)^*$ there exists a Π-extension $(\mathbb{E}, \sigma)$ of $(\mathbb{K}(x), \sigma)$ and a difference ring extension $(\mathbb{E}[y], \sigma)$ of $(\mathbb{E}, \sigma)$ with $y^k = 1$, $\frac{\sigma(y)}{y} \in \mathbb{K}$ and $\mathrm{const}_\sigma\mathbb{E}[y] = \mathbb{K}$ with the following property: for all $1 \leq i \leq r$ there is a $g \in \mathbb{E}[y]$ with $\frac{\sigma(g)}{g} = \alpha_i$.*

Proof: Let γ be a k-th root of unity that generates the cyclic group of units in $\mathbb{U}$. Obviously, $k > 1$. By Theorem 6.2 there is a Π-extension $(\mathbb{E}, \sigma)$ of $(\mathbb{K}(x), \sigma)$, $g_i \in \mathbb{E}^*$ and roots of unity $u_i \in \mathbb{U}$ with $\frac{\sigma(g_i)}{g_i}\,u_i = \alpha_i$. Moreover by Lemma 6.6 there is a difference ring extension $(\mathbb{E}[y], \sigma)$ of $(\mathbb{E}, \sigma)$ with $y^m = 1$, $\sigma(y) = \gamma\,y$ and $\mathrm{const}_\sigma\mathbb{E}[y] = \mathbb{K}$. Since γ is a generator of the roots of unity, there exist $n_i \geq 0$ with $u_i = \gamma^{n_i}$. With $g_i' := g_i\,y^{n_i}$ we have $\frac{\sigma(g_i')}{g_i'} = \gamma^{n_i}\,\frac{\sigma(g_i)}{g_i} = \alpha_i$. □

Contrary, to split product extensions into atomics clearly increases the algorithmic complexity to deal with Problems *LDE* and *GOH*. In general, if one has given a Π-extension $(\mathbb{F}(p_1, \dots, p_e), \sigma)$ of $(\mathbb{F}, \sigma)$, one might merge extensions to just one Π-extension.

Proposition 6.2. *Let $(\mathbb{F}(t_1, \dots, t_e), \sigma)$ be a Π-extension of $(\mathbb{F}, \sigma)$ with $\alpha_i := \frac{\sigma(t_i)}{t_i}$ and $u \in \mathbb{F}$ a root of unity. Then there exists a Π-extension $(\mathbb{F}(t), \sigma)$ of $(\mathbb{F}, \sigma)$ with $\sigma(t) = \big(u\,\prod_{i=1}^{e} \alpha_i\big)t$.*

Proof: Suppose such a Π-extension $(\mathbb{F}(t), \sigma)$ of $(\mathbb{F}, \sigma)$ does not exist. Then by Theorem 2.1 we have $\frac{\sigma(g)}{g} = (u\,\prod_{i=1}^{e} \alpha_i)^n$ for some $n > 0$, $g \in \mathbb{F}$. Let $k > 0$ such that $u^k = 1$ and take $m := n\,k$

and $g' := g^k$. Then $\frac{\sigma(g')}{g'} = (\prod_{i=1}^{e} \alpha_i)^m$ and hence $\frac{1}{\alpha_e^m} = \frac{\sigma(g')}{g'} \prod_{i=1}^{e-1} \alpha_i^m = \frac{\sigma(g'\, t_1^m \dots t_{e-1}^m)}{g'\, t_1^m \dots t_{e-1}^m}$. Thus $\alpha_e^m \in \mathrm{H}_{(\mathbb{E},\sigma)}$ with $\mathbb{E} := \mathbb{F}(t_1, \dots, t_{e-1})$, a contradiction by Theorem 2.1. $\square$

References

[AB00] S.A. Abramov and M. Bronstein. Hypergeometric dispersion and the orbit problem. In *ISSAC'00*. ACM Press, 2000.

[AP02] S. Abramov and M. Petkovšek. Rational normal forms and minimal decompositions of hypergeometric terms. *J. Symbolic Comput.*, 33(5):521–543, 2002.

[Bro00] M. Bronstein. On solutions of linear ordinary difference equations in their coefficient field. *J. Symbolic Comput.*, 29(6):841–877, June 2000.

[CLZ00] J. Cai, R.J. Lipton, and Y. Zalcstein. The complexity of the $a\ b\ c$ problem. *Electron. J. Combin.*, 29(6):1878–1888, 2000.

[DPSW03] K. Driver, H. Prodinger, C. Schneider, and J. A. C Weideman. Padé approximations to the logarithm II: Identities, recurrences, and symbolic computation. *Submitted*, 2003.

[Ge93a] G. Ge. *Algorithms related to the multiplicative representation of algebraic numbers*. PhD thesis, Department of Mathematics, University of California at Berkeley, Berkeley, CA, 1993.

[Ge93b] G. Ge. Testing equalities of multiplicative representations in polynomial time. In *Proceedings Foundation of Computer Science*, pages 422–426, 1993.

[Kar81] M. Karr. Summation in finite terms. *J. ACM*, 28:305–350, 1981.

[Kar85] M. Karr. Theory of summation in finite terms. *J. Symbolic Comput.*, 1:303–315, 1985.

[KL86] R. Kannan and R. Lipton. Polynomial-time algorithm for the orbit problem. *Journal of the ACM*, 33(4):808–821, October 1986.

[Mas88] D.W. Masser. *New Advances in Transcendence Theory*, chapter Linear relations on algebraic groups, pages 248–262. Cambridge University Press, UK, 1988.

[MW94] Y.K. Man and F.J. Wright. Fast polynomial dispersion computation and its applications to indefinite summation. In J. von zur Gathen and M. Giesbrecht, editors, *Proc. ISSAC'94*, pages 175–180. ACM Press, 1994.

[PS03] P. Paule and C. Schneider. Computer proofs of a new family of harmonic number identities. *Adv. in Appl. Math.*, 2003. To appear.

[PWZ96] M. Petkovšek, H. S. Wilf, and D. Zeilberger. $A = B$. A. K. Peters, Wellesley, MA, 1996.

[PZ89] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*. Encyclopedia of mathematics and its applications. Cambridge University Press, Cambridge, 1989.

[Sch00] C. Schneider. An implementation of Karr's summation algorithm in Mathematica. *Sém. Lothar. Combin.*, S43b:1–10, 2000.

[Sch01] C. Schneider. Symbolic summation in difference fields. Technical Report 01-17, RISC-Linz, J. Kepler University, November 2001. PhD Thesis.

[Sch02a] C. Schneider. A collection of degree bounds to solve parameterized linear difference equations in $\Pi\Sigma$-fields. Technical Report 02-05, RISC-Linz, J. Kepler University, July 2002. Submitted.

[Sch02b] C. Schneider. A collection of denominator bounds to solve parameterized linear difference equations in $\Pi\Sigma$-fields. Technical Report 02-04, RISC-Linz, J. Kepler University, July 2002. Submitted.

[Sch02c] C. Schneider. Solving parameterized linear difference equations in $\Pi\Sigma$-fields. Technical Report 02-03, RISC-Linz, J. Kepler University, July 2002. Submitted.

[Sch03a] C. Schneider. A note of the number of rhombus tilings of a symmetric hexagon and symbolic summation. 2003. Submitted.

[Sch03b] C. Schneider. Single nested sum extensions in $\Pi\Sigma$-fields. 2003. In preparation.

[Sim84] C. C. Sims. *Abstract algebra, A computational approach*. John Wiley & Sons, New York, 1984.

[Win96] F. Winkler. *Polynomial Algorithms in Computer Algebra*. Texts and Monographs in Symbolic Computation. Springer, Wien, 1996.

[Zei90] D. Zeilberger. A fast algorithm for proving terminating hypergeometric identities. *Discrete Math.*, 80(2):207–211, 1990.

(C. Schneider) Johann Radon Institute for Computational and Applied Mathematics (RICAM), Johannes Kepler University Linz, A–4040 Linz, Austria,

E-mail address: `Carsten.Schneider@oeaw.ac.at`