Annales Mathematicae Silesianae 8. Katowice 1994, 189–201

Prace Naukowe Uniwersytetu Śląskiego nr 1444

FAMILIES OF COMMUTING FORMAL POWER SERIES, SEMICANONICAL FORMS AND ITERATIVE ROOTS

LUDWIG REICH

Abstract. We consider for a given formal power series $F(x) = \rho x + c_2 x^2 + \dots, \rho \neq 0$, with complex coefficients and for a given integer $N > 1$ the functional equation $G^N = F$ where G is again a formal series (G is called an iterative root of F). If ρ is a root of 1 and F is not conjugate to its linear part we derive a criterion for the existence of solutions G and describe the general solution. Representations of the coefficients of G by means of universal polynomials are given, also in the case where ρ is not a root of 1 (where existence is almost trivial). Our main tools are maximal families of commuting series (i.e. the Aczél–Jabotinsky equation of third type) and semicanonical forms.

1. Introduction. Much is known about iterative roots of formal power series $F(x) = \rho x + c_2 x^2 + \dots$, $\rho \neq 0$, over $\mathbb{C}$. By an iterative root G of order N of F we understand a formal series $G(x) = \sigma x + d_2 x^2 + \dots$, such that

$$G^N = F, \tag{1}$$

where G^N is defined in the sense of iteration theory. This means that $G^N = G^{N-1} \circ G$, $G^1 = G$, $\circ$ being the substitution in the ring $\mathbb{C}[\![x]\!]$ of formal series over $\mathbb{C}$. Some important results on existence and construction of solutions G of (1) are nicely collected in the monograph [2] (Ch. 11.6). But also the theory of semicanonical forms of formal power series transformations (also in several indeterminates), as developped by J. Schwaiger and the author, leads to criteria about existence of iterative roots which are in our present

Received May 10, 1994.
AMS (1991) subject classification: Primary 39B12, 13F25.

situation of power series in one indeterminate rather explicit (see [8], [7], [5]). Last but not least, the theory of families of commuting formal series and its relations to the Aczél–Jabotinsky differential equations of third type is also closely connected with the functional equation (1), as pointed out in [4].

So the present paper has the following task. We want to apply our theory of families of commuting series and the theory of normal forms to present the known results on (1) in a systematic and rather short way in two cases: a) In $F(x) = \rho x + c_2x^2 + \dots$, the "multiplier" ρ is a root od unity (possibly 1) and F is *not* conjugate to its linear part ρx. b) In $F(x)$ the multiplier ρ is *not* a root of unity. But we will also go beyond these results which are known in most cases, and we will show how the coefficients of solutions G of (1) can be expressed as universal polynomials in the coefficients of F. (The notion "universal" will be made precise in Section 4.)

The most interesting case is certainly a) where the full power of the theory of families of commuting power series is needed. Here, in general, for a given N, F does not have an iterative root of order N. Furthermore, if for given F and N a solution of (1) exists, then the total number is finite, and we will describe the set of solutions in great detail (Section 2). We will prove this result as a consequence of a basic criterion on the existence of solutions of (1) when F and N are given, and which is formulated in terms of elementary number theory. Only three integers are involved. Let ρ be $\rho = e^{2\pi ik/m}$, $m > 1$ and such that $F^{\tilde{m}}(x) = x + d_{m+1}x^{m+1} + \dots$, where $\tilde{m} = m/\gcd(k, m)$, $d_{m+1} \neq 0$. (We will see that this m exists, $m > 1$ and is uniquely determined by F.) Then the criterion (in Theorem 1) refers to m, k and N only.

In case b) we have a different picture. For each F and each N, in this situation, there exist solutions of (1), their number is finite, and we will again give a detailed description of the set of all solutions (Section 3). Our note will not cover the cases of iterative roots of the series $F(x) = x$ and more generally series $F(x) = \rho x + \dots$, where ρ is a root of unity and F is conjugate to its linear part ρx (and which are exactly the iterative roots of x). These cases are somewhat different in the sense that for each F and each N there is a continuum of solutions for which 1-1 parametrizations can be given. Moreover, the problem of finding groups or families of commuting series with respect to substitution in the set of all iterative roots of $F(x) = x$ turns out to be an interesting question. Hence these cases will be the topic of a separate paper.

2. Iterative roots of series $F(x) = \rho x + c_2x^2 + \dots$, where ρ is a root of unity and F is not linearizable. This case is the most interesting one. We know from [4] that $F(x) = \rho x + c_2x^2 + \dots$, where ρ is a root of unity and $F(x)$ is not conjugate to ρx is contained in a unique maximal family $\mathcal{F}$ of commuting (invertible) formal power series. This family $\mathcal{F}$ is on the other side, the set of all solutions of a unique normalized Aczél-Jabotinsky equation of the third type. Those equations, from the point of view of formal series, are studied in [3].

Now assume that G is an iterative root of order N of F, i.e.

$$G^N = F. \tag{1}$$

Then clearly $G \circ F = F \circ G$ and therefore by what has been said above $G \in \mathcal{F}$. Now it is known from [4] and from [3] that $\mathcal{F}$ can be assumed to be in its normal form. This means that each $\phi \in \mathcal{F}$ (hence in particular F and G) is of the form

$$\phi(x) = \sigma x + \varphi_{m+1} x^{m+1} + \sum_{j\geq 2} \varphi_{jm+1} x^{jm+1}, \qquad \sigma = e^{2\pi i \frac{l}{m}},$$

in particular

$$F(x) = \rho x + c_{m+1} x^{m+1} + \sum_{j\geq 2} c_{jm+1} x^{jm+1},$$

where $\rho = e^{2\pi i \frac{k}{m}}$, $c_{m+1} \neq 0$.

Furthermore it is known that there exists an isomorphism Θ of the abelian group $\mathcal{F}$ onto a group of (2,2)-matrices, namely

$$\Theta(\phi) = \begin{pmatrix} \sigma & \varphi_{m+1} \\ 0 & \sigma \end{pmatrix},$$

i.e.

$$\Theta(\mathcal{F}) = \left\{ \begin{pmatrix} \sigma & \varphi_{m+1} \\ 0 & \sigma \end{pmatrix} \middle| \ \sigma^m = 1, \ \varphi_{m+1} \in \mathbf{C} \right\}.$$

The group operation on $\mathcal{F}$ is clearly the substitution of formal series. Now, the equation $G^N = F$ is therefore equivalent to the matrix equation

$$\begin{pmatrix} \sigma & \varphi_{m+1} \\ 0 & \sigma \end{pmatrix}^N = \begin{pmatrix} \sigma & c_{m+1} \\ 0 & \rho \end{pmatrix}. \tag{2}$$

We introduce $\rho_0 = e^{\frac{2\pi i}{m}}$, and observe that for each $N \in \mathbf{Z}$

$$\begin{pmatrix} \sigma & \varphi_{m+1} \\ 0 & \sigma \end{pmatrix}^N = \begin{pmatrix} \sigma^N & N\sigma^{N-1}\varphi_{m+1} \\ 0 & \sigma^N \end{pmatrix}. \tag{3}$$

Therefore (1) and (2) are equivalent to

$$\rho_0^{Nl} = \rho_0^k, \quad c_{m+1} = N\rho_0^{(N-1)l}\varphi_{m+1}. \tag{4}$$

If the first equation (4) has a solution $l \in \mathbb{Z}$ then $\varphi_{m+1} = \frac{1}{N}\rho_0^{-(N-1)l}c_{m+1}$ always, therefore it is sufficient to consider $\rho_0^{Nl} = \rho_0$, which is equivalent to

$$Nl \equiv k(\mathrm{mod}\ m). \tag{5}$$

It is well known from elementary number theory that (5) has a solution if and only if

$$\gcd(N,m)|k.$$

If this is the case, then from (5) we deduce

$$\frac{N}{\gcd(N,m)}l \equiv \frac{k}{\gcd(N,m)}\left(\mathrm{mod}\frac{m}{\gcd(N,m)}\right). \tag{6}$$

Since $\gcd\left(\frac{N}{\gcd(N,m)}, \frac{m}{\gcd(N,m)}\right) = 1$, (6) has a unique solution l_0 mod $\frac{m}{\gcd(N,m)}$ and we get all solutions of (5) (mod m) by

$$l_\mu = l_0 + \mu\frac{m}{\gcd(N,m)}(\mathrm{mod}\ m), \qquad \mu = 0, 1, \ldots, \gcd(N,m) - 1. \tag{7}$$

For each μ we obtain a solution

$$\begin{pmatrix} \rho_0^{l_\mu} & \varphi_{m+1}^{(\mu)} \\ 0 & \rho_0^{l_\mu} \end{pmatrix}, \qquad \mu = 0, \ldots, \gcd(N,m) - 1 \tag{8}$$

of the matrix equation (2), where

$$\varphi_{m+1}^{(\mu)} = \frac{1}{N}\rho_0^{-(N-1)l_\mu}c_{m+1}.$$

By

$$G_\mu := \Theta^{-1}\begin{pmatrix} \rho_0^{l_\mu} & \varphi_{m+1}^{(\mu)} \\ 0 & \rho_0^{l_\mu} \end{pmatrix}, \qquad \mu = 0, \ldots, \gcd(N,m) - 1 \tag{9}$$

we find all solutions of (1). If G_λ, G_μ, are two solutions of (1), then G_λ, $G_\mu \in \mathcal{F}$ and therefore they commute, and we find

$$\left(G_\lambda \circ G_\mu^{-1}\right)^N(x) = G_\lambda^N \circ G_\lambda^{-N}(x) = F \circ F^{-1}(x) = \mathrm{id}(x).$$

This means that $G_\lambda \circ G_\mu^{-1}$ is an iterative root of id of order N, which lies in $\mathcal{F}$. Conversely, if $W \in \mathcal{F}$ and $W^N(x) = \mathrm{id}(x)$, then $G_\lambda \circ W = W \circ G_\lambda$. Therefore $(G_\lambda \circ W)^N = F$. We determine all roots of identity, of order N, which are in $\mathcal{F}$. Since $\Theta(\mathrm{id}) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, we deduce from (3) that for W

$$\Theta(W) = \begin{pmatrix} \sigma & 0 \\ 0 & \sigma \end{pmatrix} \qquad \text{with} \quad \sigma^m = 1,$$

and conversely, so that the matrix representation of the roots of order N of id in $\mathcal{F}$ is characterized by

$$\begin{pmatrix} \sigma & 0 \\ 0 & \sigma \end{pmatrix}^N = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

with $\sigma^m = 1$. Hence, if $\sigma = e^{2\pi i \frac{r}{m}}$ we get $Nr \equiv 0 \ (\mathrm{mod}\ m)$ and $\frac{N}{\gcd(N,m)} r \equiv 0 \left(\mathrm{mod} \frac{m}{\gcd(N,m)}\right)$, and hence $r \equiv 0 \left(\mathrm{mod} \frac{m}{\gcd(N,m)}\right)$, and $r = r_\mu = \mu \cdot \frac{m}{\gcd(N,m)}$, $\mu = 0, \ldots, \gcd(N,m) - 1$. The set (8) is also given by

$$\begin{pmatrix} \rho_0^{l_0} & \varphi_{m+1}^{(0)} \\ 0 & \rho_0^{l_0} \end{pmatrix} \cdot \begin{pmatrix} \rho_0^{\mu \frac{m}{\gcd(N,m)}} & 0 \\ 0 & \rho_0^{\mu \frac{m}{\gcd(N,m)}} \end{pmatrix},$$

$\mu = 0, \ldots, \gcd(N,m)$, or by applying Θ^{-1}:

$$G_\mu = G_0 \circ W_\mu, \quad W_\mu = \Theta^{-1} \begin{pmatrix} \rho_0^{r_\mu} & 0 \\ 0 & \rho_0^{r_\mu} \end{pmatrix}.$$

We summarize these results in

THEOREM 1. *Let $F(x) = \rho x + \tilde{c}_2 x^2 + \ldots \rho = \rho_0^k$, $\rho_0 = \exp \frac{2\pi i}{m}$, $m > 1$, which is not conjugate to its linear part, and let its semicanonical form be*

$$H(x) = \rho x + c_{m+1} x^{m+1} + \sum_{j \geq 2} c_{jm+1} x^{jm+1}$$

with $c_{m+1} \neq 0$. (This initial jet $\rho x + c_{m+1} x^{m+1}$ is an invariant of F, see [5].) Then:

(i) *F has an iterative root G of order $N, G^N = F$, if and only if*

$$\gcd(N, m) | k. \tag{10}$$

(ii) *Each iterative root G of F belongs to the unique maximal family $\mathcal{F}$ of formal series containing F, and so all roots of F commute.*

(iii) *If F has an iterative root G_0 of order N then the set of all solutions of $G^N = F$ is given by*

$$G_\mu = G_0 \circ W_\mu, \quad \mu = 0, \dots, \gcd(N,m) - 1,$$

where W_μ runs through all roots of id *of order N which belong to $\mathcal{F}$. This set forms a cyclic group of order* $\gcd(N,m)$.

It is now useful to study some special cases.

A. Suppose firstly that $k = m$, i.e. $F(x) = x + \tilde{c}_2 x^2 + \dots = x + \tilde{c}_{m+1} x^{m+1} + \dots$, $\tilde{c}_{m+1} \neq 0$. Then condition (10) is fulfilled, and F has therefore iterative roots of order N for each N. This could also be deduced from the fact that F is embeddable in exactly one analytic iteration group $(F_t)_{t \in \mathbb{C}}$, $F_t(x) = x + \tilde{c}_{m+1}(t) x^{m+1} + \dots$, and $F_{1/N}(x) = x + \tilde{c}_{m+1}\left(\frac{1}{N}\right) x^{m+1} \cdots$ is therefore one of the roots of order N.

If moreover $\gcd(N,m) > 1$ then according to Theorem 1 the general solution of $G^N = F$ is

$$\left\{ F_{1/N} \circ W_\mu \mid \quad \mu = 0, \dots, \gcd(N,m) - 1 \right\}$$

where W_μ is defined as above.

B. Suppose that $\gcd(N,m) = 1$. Then (10) is also true, $F(x)$ has exactly one iterative root of order N.

3. Iterative roots of series $F(x) = \rho x + c_2 x^2 + \dots$, where ρ is not a root of unity. We deduce from the theory of families of commuting power series [4] that F is again contained in a unique maximal family $\mathcal{F}$, which is in this case

$$\mathcal{F} = \left\{ T^{-1}(\sigma T x) \mid \quad \sigma \in \mathbb{C}^* \right\}.$$

Let σ be an arbitrary solution of

$$\sigma^N = \rho.$$

Then there are N distinct solutions G_σ of $G^N = F$, and they can be written as

$$G_{\sigma_\mu} = G_{\sigma_0} \cdot W_\mu, \qquad \mu = 0, \dots, N-1,$$

where $\sigma_\mu = \sigma_0 \cdot \eta^\mu, \eta = \exp\left(\frac{2\pi i}{N}\right)$, and σ_0 is a fixed solution of $\sigma_0^N = \rho$.

The roots of F belong to the unique maximal family $\mathcal{F}$ containing F, and hence they all commute. Moreover, in the above representation the series W_μ

form the set of all iterative roots of id which belong to $\mathcal{F}$. This set is a cyclic group of order N and $W_\mu = T^{-1}(\eta^\mu Tx)$, where T is the uniquely determined automorphism $T(x) = x + t_2x^2 + \ldots$ such that $T^{-1} \circ F \circ T(x) = \rho x$.

Assume now that $G(x) = \sigma x + \ldots$ solves the equation $G^N = F$. Then $G \circ F = F \circ G$, so $G \in \mathcal{F}$, and $G(x) = T^{-1}(\sigma Tx)$, $\sigma^N = \rho$. Conversely, if $\sigma^N = \rho$, then $T^{-1}(\sigma Tx)$ is an iterative root of order N of F. So we get (similarly to Theorem 1)

THEOREM 2. *Suppose that in $F(x) = \rho x + c_2x^2 + \ldots \rho$ is not a root of unity. Hence let $T(x) = x + tx^2 + \ldots$ be the unique power series such that $F(x) = T^{-1}(\rho T(x))$.*

Then F has iterative roots of order N for each N, namely

$$G_\sigma(x) = T^{-1}(\sigma Tx),$$

where σ runs through the solutions of $\sigma^N = \rho$.

All iterative roots of F of order N belong to the unique maximal family of commuting formal series containing F and each iterative root has the form given above.

4. Coefficients of iterative roots $F^{1/N}(x)$ represented as universal polynomials, when F is not conjugate to its linear part. We start out with a series $F(x) = \rho x + c_2x^2 + \ldots$, in case a) again. Before formulating our result about the coefficients of iterative roots of fixed order N as values of certain universal polynomials we have to discuss once more in detail the integers m and k, used in Section 1 (Introduction), as well as in Theorem 1. Assume that $\rho = e^{2\pi i\tilde{k}/\tilde{m}}$, where $\tilde{m} \geq 1$, $\gcd(\tilde{k}, \tilde{m}) = 1$. Then clearly the iterate of F of order $\tilde{m}$ has multiplier 1. But we can say much more (cf. [5]).

LEMMA. *If $F(x) = \rho x + c_2x^2 + \ldots$, with $\rho = \exp(2\pi i\tilde{k}/\tilde{m})$, $\tilde{m} \geq 1$, gcd $(h, \tilde{m}) = 1$, and F is not conjugate to its linear part, then there exist integers k and m $(m \geq 1)$, such that $\rho = \exp(2\pi ik/m)$ and $F^{\tilde{m}}(x) = x + d_{m+1}x^{m+1} + \ldots$, where $d_{m+1} \neq 0$ and $\tilde{m}|m$.*

PROOF. Clearly, $F^{\tilde{m}}(x)$ has multiplier 1 and $\tilde{m}$ is the least positive integer ν, such that $F^\nu(x)$ has this property. Now we are going to show that $F^{\tilde{m}}(x) \neq x$. From the theory of semicanonical forms (cf. [8]) it is known that there exists a transformation $S(x) = x + s_2x^2 + \ldots$ transforming F by conjugation to a semicanonical form $S^{-1} \circ F \circ S(x) = \rho x + \sum_{\nu \geq 1} \tilde{c}_{\nu\tilde{m}+1}x^{\nu\tilde{m}+1}$.

Since $S^{-1} \circ F \circ S$ cannot be linear (by assumption) there is a minimal ν_0 with $\tilde{c}_{\nu_0\tilde{m}+1} \neq 0$, i.e. $S^{-1} \circ F \circ S(x) = \rho x + \tilde{c}_{\nu_0\tilde{m}+1}x^{\nu_0\tilde{m}+1} + \ldots$. For each $l \in \mathbf{N}$ we calculate the l-th iterate as

$$(S^{-1} \circ F \circ S)^l(x) = \rho^l x + l\rho^{l-1}\tilde{c}_{\nu_0\tilde{m}+1}x^{\nu_0\tilde{m}+1} + \ldots,$$

from which $F^{\widetilde{m}}(x) = x + d_{m+1}x^{m+1} + \dots$, with $d_{m+1} \neq 0$, and $\widetilde{m}|m$ immediately follows. This proves the Lemma. $\square$

It is obvious that, fixing $\widetilde{m}$ and m, for the set of all series F as considered in the Lemma there exists a universal sequence $(P_\mu)_{\mu \geq m+1}$ of polynomials such that $d_{m+j} = P_{m+j}(\rho, c_2, \dots, c_{m+j})$, $j \geq 1$. We denote by $\mathcal{F}_{k,m}$ the set of all formal series $F(x) = \rho x + c_2x^2 + \dots$, $\rho = \exp\left(2\pi i\widetilde{k}/\widetilde{m}\right)$, $\gcd(\widetilde{k}, \widetilde{m}) = 1$ for which the same numbers k and m are determined by the Lemma, and let $N \in \mathbf{N}$ be fixed such that F has an iterative root of order N. We recall that in Theorem 1 we proved a necessary and sufficient condition (involving k, m and N) for the existence of such a root W of F. Then we are going to prove

THEOREM 3. *Let the family $\mathcal{F}_{k,m}$ be defined as above, and let N be a positive integer. Then for $\mathcal{F}_{k,m}$ and N there exists a sequence $(Q_\mu)_{\mu \geq 2}$ of polynomials with the following property: If $F(x) = \rho x + c_2x^2 + \dots$ has an iterative root $W(x) = \sigma x + u_2x^2 + \dots$, of order N, then*

$$u_j = Q_j\left(\sigma; \rho, c_2, \dots, c_j, \frac{1}{P_{m+1}(\rho, c_2, \dots, c_{m+1})}\right),$$

$j = 2, 3, \dots$, where $P_{m+1}(\rho, c_2, \dots, c_{m+1}) \neq 0$ is the coefficient of x^{m+1} in $F^{\widetilde{m}}(x)$, according to the Lemma.

PROOF. We denote now $F^{\widetilde{m}}(x)$ by $\phi(x) = x + d_{m+1}x^{m+1} + \dots$, $d_{m+1} \neq 0$. Then it is well known ([1]) that ϕ is embeddable in exactly one analytic iteration group $(\phi_t)_{t \in \mathbb{C}}$, $\phi_1 = \phi$. The coefficients of the series $\phi_t(x)$ are polynomials in t and the parameters $d_{m+1}, d_{m+2}, \dots$ hence also polynomials in t and in $\rho, c_2, c_3, \dots$. In particular

$$\phi_t(x) = x + d_{m+1}tx^{m+1} + \dots$$

Moreover, we deduce from [3] that each ϕ_t is a solution of the formal Aczél--Jabotinsky differential equation of the third type

$$(G \circ \Psi)(x) = \frac{d\Psi}{dx} \cdot G(x), \tag{11}$$

where $G(x) = \frac{\partial \phi_t}{\partial t}(x)|_{t=0} = g_{m+1}x^{m+1} + \dots$ with $g_{m+1} := d_{m+1}$. From the structure of the coefficients of $\phi_t(x)$ we deduce that each g_{m+j} is a polynomial in $\rho, c_2, \dots, c_{m+j}$, these polynomials being universal for fixed k and m (or equivalently $\widetilde{m}$ and m). In Section 1 we had already extensively used that all iterative roots of $F(x)$ belong also to the set of all solutions $\Psi(x) = \sigma x + b_2x^2 + \dots$ of (11), and we are now going to consider in detail expressions for the coefficients of solutions of (11), as developped in [3]. It is clear that equation (11) has exactly the same solutions Ψ as the normalized equation

$$(12) \qquad (\widehat{G} \circ \Psi)(x) = \frac{d\Psi}{dx} \cdot \widehat{G}(x),$$

with $\widehat{G}(x) = x^{m+1} + \frac{g_{m+2}}{g_{m+1}} x^{m+2} + \dots$. In both cases it follows from [3] that the coefficients of an individual solution Ψ of (11) or (12) can be fixed by prescribing the multiplier σ being an m-th root of unity and b_{m+1}. All other coefficients b_l are polynomials in $\sigma, b_{m+1} \frac{g_{m+2}}{g_{m+1}}, \dots, \frac{g_{m+l}}{g_{m+1}}$. Moreover, one can easily find expressions for b_l as linear forms in $\frac{g_{m+2}}{g_{m+1}}, \dots, \frac{g_{m+l}}{g_{m+1}}$ with coefficients polynomials in $\sigma, b_2, \dots, b_{l-1}$. For our purposes we have also to consider the transformation of Aczél-Jabotinsky equations (in their normalized form), see again [3].

If $S(x) = x + s_2 x^2 + \dots$, then the set $S^{-1} \circ \Psi \circ S(x)$, where Ψ runs through all solutions of (12) is the set of all solutions of the equation

$$(13) \qquad (\widetilde{G} \circ \widetilde{\Psi}) = \frac{d\widetilde{\Psi}}{dx} \cdot \widetilde{G}(x),$$

with $(\widetilde{G})(x) := \left(\frac{dS}{dx}\right)^{-1} \cdot (\widetilde{G} \circ S)(x)$. This type of transformation can be used to introduce certain normal forms for Aczél-Jabotinsky equations. In our case it is sufficient to transform G in (11) to the simplified form $\widetilde{G}(x) = x^{m+1} + \widetilde{g}_{2m+1} x^{2m+1} + \dots$. A "Koeffizientenvergleich" as in [3] yields that this can be achieved by a transformation $S(x) = x + s_2 x^2 + \dots$, which is unique if we require

$$s_{m+j} = 0, \qquad j \geq 1.$$

Moreover, the coefficients $s_2, \dots, s_m$, are polynomials in $\frac{g_{m+2}}{g_{m+1}}, \dots, \frac{g_{2m}}{g_{m+1}}$, and the same holds for the coefficients of the inverse transformation $S^{-1}(x)$ and for $\left(\frac{dS}{dx}\right)^{-1}$, and eventually for the coefficients of $\widetilde{G}(x)$ since $\widetilde{G}$ is given by (13). Since the coefficients $\widetilde{b}_l$ of $\widetilde{\Psi}$ are linear in the coefficients $\widetilde{g}_\mu$, $\mu \leq l$, of $\widetilde{G}$, we see that each solution $\widetilde{\Psi}$ of (12) has the special structure

$$\widetilde{\Psi}(x) = \sigma x + \widetilde{b}_{m+1} x^{m+1} + \widetilde{b}_{m+2} x^{m+2} + \dots,$$

and hence we get that the coefficients $\widetilde{b}_{m+r}$, $r \geq 1$, are polynomials in $\sigma, \widetilde{b}_{m+1}$ and in $\frac{g_{m+2}}{g_{m+1}}, \dots, \frac{g_{m+r}}{g_{m+1}}$, hence eventually they are polynomials in $\sigma, \widetilde{b}_{m+1}, \rho, c_2, \dots, c_{m+1}$ and $1/P_{m+1}(\rho, c_2, \dots, c_{m+1})$, namely

$$(14) \qquad \widetilde{b}_{m+r} = Q^*_{m+r}\left(\sigma, \widetilde{b}_{m+1}, \rho, c_2, \dots, c_{m+r}, \frac{1}{P_{m+1}(\rho, c_2, \dots, c_{m+1})}\right) \qquad (r \geq 1).$$

Now let W be an iterative root of order N of F. As already men--tioned, F is a solution of (11), and so $\widetilde{F} = S^{-1} \circ F \circ S$ is a solution of (13). The same holds for W and $\widetilde{W} = S^{-1} \circ W \circ S$ resp. Let $\widetilde{F}(x)$ be $\widetilde{F}(x) = \rho x + \widetilde{c}_{m+1}x^{m+1} + \dots$ ($\widetilde{c}_{m+1} \neq 0$), and observe that $\widetilde{c}_{m+1}$ is a polynomial in $\rho, c_2, \dots, c_{m+1}, \frac{g_{m+2}}{g_{m+1}}, \dots, \frac{g_{2m}}{g_{m+1}}$, hence also in $\rho, c_2, \dots, c_{m+1}$, $\frac{1}{P_{m+1}(c_2,\dots,c_{m+1})}$. Moreover, the coefficients of W are given according (14) by $\gamma_{m+r} = Q^*_{m+r}\left(\sigma, \frac{1}{N\sigma^{N-1}}\widetilde{c}_{m+1}, \rho, c_2, \dots, c_{m+r}, \frac{1}{P_{m+1}(\rho, c_2,\dots,c_{m+1})}\right)$, and hence

$$\widetilde{\gamma}_{m+r} = Q^{**}_{m+r}\left(\sigma, \rho, c_2, \dots, c_{m+r}, \frac{1}{P_{m+1}(c_2, \dots, c_{m+1})}\right),$$

where now the sequence (Q^{**}_μ) depends on k, m and N and σ is the multiplier of W, satisfying $\sigma^N = \rho$.

Indeed, to obtain the coefficients of the root $\widetilde{W}$ of $\widetilde{F}$ we have to insert in (14) on the second place the coefficient of x^{m+1} in $\widetilde{W}$. But $\widetilde{W}(x)$, being a solution of (13) has the form $\widetilde{W(x)} = \sigma x + \widetilde{\gamma}_{m+1}x^{m+1} + \dots$ and its N-th iterate is therefore $\widetilde{W}^N(x) = \sigma^N x + N\sigma^{N-1}\widetilde{\gamma}_{m+1}x^{m+1} \dots$. So we find $\widetilde{\gamma}_{m+1} = \frac{1}{N\sigma^{N-1}}\widetilde{c}_{m+1}$.

In the final step of the proof we return to $F = S \circ \widetilde{F} \circ S^{-1}$ and $W = S \circ \widetilde{W} \circ S^{-1}$. This shows, by what we know about $S, \widetilde{W}$ and S^{-1} that the coefficients of W are now polynomials in $\sigma, \rho, c_2, \dots, c_{m+1}, \frac{1}{P_{m+1}(c_2,\dots,c_{m+1})}$ and in $\frac{g_{m+k}}{g_{m+1}}$. Putting this together we get

$$u_r = Q_r\left(\sigma, \rho, c_2, \dots, c_r, \frac{1}{P_{m+1}(c_2, \dots, c_{m+1})}\right)$$

the sequence $(Q_r)_{r\geq 2}$ depending on k, m and N. This proves Theorem 3. □

5. Coefficients of iterative roots $F^{1/N}(x)$, when F is conjugate to its linear part and not an iterative root of x. We now want to give explicit expressions of the coefficients of the solutions $G_\mu(x) = T^{-1}(\sigma_\mu Tx)$ of $G^N = F$, where F is conjugate to its linear part ρx and not an iterative root of x (case b)).

We start from $\rho T(x) = T(F(x))$, $T(x) = x + t_2x^2 + \dots$, and easily find ($k \geq 2$)

$$\begin{aligned}(\rho - \rho^k)t_k &= \widetilde{R}_k(\rho, c_2, \dots, c_k;\ t_2, \dots, t_{k-1}) \\ &= c_k + R_k(\rho, c_2, \dots, c_{k-1},\ t_2, \dots, t_{k-1})\end{aligned}$$

with a universal polynomial $\widetilde{R}_k$ over $\mathbf{Z}$. Therefore, by induction

$$t_k = E_k\left(\frac{1}{\rho - \rho^\lambda}\middle|\quad \lambda \leq k;\ \rho, c_2, \dots, c_k\right),$$

Forming $T^{-1}(x) = \sum_{l\geq 2} \tau_l x^l$, we see that

$$\tau_l = \theta_l(t_2, \dots, t_l), \quad l \geq 2$$

with universal polynomials θ_l over $\mathbf{Z}$, and so, by what preceeds also

$$\tau_l = \widetilde{\theta}_l \left(\frac{1}{\rho - \rho^\lambda} \middle| \quad \lambda \leq l, \quad \rho, c_2, \dots, c_l \right)$$

with universal polynomials $\widetilde{\theta}_l$ over $\mathbf{Z}$. Therefore we get eventually from

$$G_\mu(x) = T^{-1}(\sigma_\mu T(x)) = \sigma_\mu x + d_2^{(\mu)} x^2 + \dots$$

$$d_j^{(\mu)} \equiv P_j^{(\mu)} \left(\frac{1}{\rho - \rho^l} \middle| \quad 2 \leq j \leq \lambda; \quad \rho, c_2, \dots, c_j \right), \qquad j \geq 2$$

with universal polynomials $P_j^{(n)}$ in the arguments over $\mathbf{Z}$.

There is a different method to construct such representations of the coefficients $d_j^{(\mu)}$. Notice that in our situation, when ρ is not a root of unity, $F(x) = \rho x + c_2 x^2 + \dots$ can be embedded into an analytic iteration group $(F_t)_{t\in\mathbb{C}}$, $F_t(x) = \mathrm{e}^{\lambda t} x + \rho_2(t)x^2 + c_2 x^2 + \dots$, where λ is a determination of $\ln \rho$, and that to each λ there is exactly one such embedding (see [6]). Furthermore it is well known in iteration theory that to each analytic embedding $(F_t)_{t\in\mathbb{C}}$ there exists exactly one formal differential equation

$$\text{(15)} \qquad \frac{dy}{dt} = H(y), \quad H(y) = \lambda y + h_2 y^2 + \dots$$

with the following property: The unique formal solution $y = F_t(x) = \mathrm{e}^{\lambda t} x + \rho_2(t)x^2 + \dots$ of (15) satisfies the boundary condition $F_1(x) = F(x)$. This yields the following (necessary and sufficient) conditions for $H(y)$ and $F_t(x)$: $\lambda = \ln \rho$ and

$$\text{(16)} \qquad \begin{cases} \varphi_\nu'(t) = \lambda \varphi_\nu(t) + Q_\nu(\mathrm{e}^{\lambda t}, \varphi_2(t), \dots, \varphi_{\nu-1}(t), h_2, \dots, h_\nu), \\ \varphi_\nu(0) = 0, \varphi_\nu(1) = c_\nu, \qquad \text{for } \nu \geq 2, \end{cases}$$

where Q_ν, are universal polynomials over $\mathbf{Z}$. Using that ρ is not a root of unity one sees that the system (16) can be solved in a unique way, and we find eventually (by induction over ν)

$$\text{(17)} \qquad \varphi_\nu(t) = \phi_\nu \left(\mathrm{e}^{\lambda t}, \frac{1}{\rho - \rho^l}, \ 2 \leq l \leq \nu; \ \rho, c_2, \dots, c_\nu \right)$$

with polynomials ϕ_ν over $\mathbf{Z}$, universal for all series F in case b).

We omit here the details of the calculation, similar calculations can be found in [6].

Putting $t = \frac{1}{N}$ we get in (17)

$$\phi_\nu\left(e^{\lambda/N};\ \frac{1}{\rho-\rho^l},\ 2\le l\le\nu;\ \rho, c_2, \dots, c_\nu\right)$$

the coefficients of the element $F_{\frac{1}{N}}$, of the analytic iteration of F belonging to the choice of λ of $\ln\rho$. This $F_{\frac{1}{N}}$, is clearly an iterative root of F of order N.

As final step we have to show that all iterative roots of F can be found by this procedure. Let $G(x) = \sigma x + d_2x^2 + \dots$ be an iterative root of F of order N. Then σ is also not a root of unity and hence G can be embedded into a unique analytic iteration group $(G_s)_{s\in\mathbb{C}}$ belong to a fixed choice μ of $\ln\sigma$. From $\sigma^N = \rho$ we deduce that $N\mu$ is a certain choice of $\ln\rho$. Since $G^N = G_1^N = F$ we obtain from $(G_s)_{s\in\mathbb{C}}$ an analytic iteration of F belonging to $N\mu$ by the following change of the group parameter:

$$F_t := G_{tN} = (G_t)^N.$$

So everything is proved, and we may summarize in

THEOREM 4. *Let $F(x)$ be a formal series $\rho x + c_2x^2 + \dots$, where ρ is not a root of unity (case* b)*). Let $N \in \mathbf{N}$ be given and assume $\sigma^N = \rho$ for $\sigma \in \mathbb{C}$. Then there exists a sequence Q_ν of polynomials over $\mathbf{Z}$ (universal for series in case* b)*) with the following property: $G(x) = \sigma x + d_2x^2 + \dots$ is an iterative root of order N of F if and only if*

$$d_\nu = Q_\nu\left(\frac{1}{\rho-\rho^l},\ 2\le l\le\nu;\ \rho, c_2, \dots, c_\nu\right),$$

for $\nu \ge 2$.

REFERENCES

[1] I.N. Baker, *Permutable power series and regular iteration*, Journal Australian Math. Society **2** (1962), 265-294.

[2] M. Kuczma, B. Choczewski and R. Ger, *Iterative Functional Equations*, Encyclopedia of Mathematics and its Applications, vol. 32. Cambridge University Press, Cambridge 1990.

[3] L. Reich, *On a differential equation in iteration theory in rings of formal power series in one variable*, in: *Iteration Theory and Its Functional Equations* (Eds. R. Liedl et al.), Lecture Notes in Mathematics, vol. 1163, 135-148, Springer, 1985.

[4] L. Reich, *On families of commuting formal power series*, Berichte der Mathematisch-statistischen Sektion in der Forschungsgesellschaft Joanneum Graz **294** (1988), 1-18.

[5] L. Reich, *On power series transformations in one indeterminate having iterative roots of given order and with given multiplier*, in: *J.P Lampreia, J. Llibre et al. (Eds.), European Conference on Iteration Theory (ECIT 1991)*, World Scientific, Singapore 1992, 210-217.

[6] L. Reich, J. Schwaiger, *Über einen Satz von Sthl. Sternberg in der Theorie der analytischen Iterationen*, Monatshefte Math. **83** (1977), 207-221.

[7] J. Schwaiger, *Roots of power series in one variable*, Aequationes Math. **29** (1985), 40-43.

[8] J. Schwaiger, L. Reich, *Über Lösungen der Funktionalgleichung $F \circ T = T \circ G$ für formale Potenzreihen*, Aequationes Math. **20** (1980), 224-243.

INSTITUT FÜR MATHEMATIK
DER UNIVERSITÄT GRAZ
HEINRICHSTRASSE 36
A-8010 GRAZ, AUSTRIA