FUNCTIONAL EQUATIONS IN FORMAL POWER SERIES

FEDOR PAKOVICH

Abstract. Let k be an algebraically closed field of characteristic zero, and $k[[z]]$ the ring of formal power series over k. In this paper, we study equations in the semigroup $z^2k[[z]]$ with the semigroup operation being composition. In particular, we answer a question of Horwitz and Rubel about decompositions of "even" formal power series. We also show that every right amenable subsemigroup of $z^2k[[z]]$ is conjugate to a subsemigroup of the semigroup of monomials.

1. Introduction

Let k be an algebraically closed field of characteristic zero, and $k[[z]]$ the ring of formal power series over k. For an element $A(z)=\sum_{n\geq 0}c_nz^n$ of $k[[z]]$, we define its *order* by the formula $\operatorname{ord}A=\min\{n\geq 0\,|\,c_n\neq 0\}$. We will denote by $k_n[[z]]$, $n\geq 0$, the subset of $k[[z]]$ consisting of formal power series of order n, and by Γ the subset consisting of formal power series of order at least two. If A and B are elements of $k[[z]]$ with $\operatorname{ord}B\geq 1$, then the operation $A\circ B$ of *composition* of A and B is well defined. In particular, with respect to this operation the set $k_1[[z]]$ is a *group*, and the set Γ is a *semigroup*.

Equations in the group $k_1[[z]]$ and its group-theoretic properties have been intensively studied (see e. g. [1], [2], [6], [14], [15], [16], [19], [24], [28], [29]). In contrast, in this paper we study equations in the semigroup Γ. In other words, we study functional equations in formal powers series of order at least two. One of such equations is simply the equation $A=A_1\circ A_2\circ\cdots\circ A_r$, $r\geq 2$, where A is a given element of Γ, and $A_1,A_2,\dots,A_r$ are unknown elements of Γ. Stated differently, the problem is to describe the ways in which an element A of Γ can be represented as a composition $A=A_1\circ A_2\circ\cdots\circ A_r$ of other elements of Γ. Although this question is of a fundamental nature, we were unable to find relevant references in the literature, and provide an answer in this paper. Specifically, we describe *equivalence classes* of such decomposition, where two decompositions

$$A=A_1\circ A_2\circ\cdots\circ A_k\quad\text{ and }\quad A=\widehat{A}_1\circ\widehat{A}_2\circ\cdots\circ\widehat{A}_m,$$

are considered as equivalent if $k=m$ and there exist elements μ_i, $1\leq i\leq k-1$, of $k_1[[z]]$ such that

$$A_1=\widehat{A}_1\circ\mu_1^{-1},\quad A_i=\mu_{i-1}\circ\widehat{A}_i\circ\mu_i^{-1},\quad 1<i<k,\quad\text{and}\quad A_k=\mu_{k-1}\circ\widehat{A}_k.$$

Since for every $A\in\Gamma$ there exists an element β_A of $k_1[[z]]$, called the *Böttcher function*, such that

$$\beta_A^{-1}\circ A\circ\beta_A=z^n,$$

the problem of describing equivalency classes of decompositions of $A\in\Gamma$ in the obvious sense reduces to the case $A=z^n$. Our main result in this context is following.

Theorem 1.1. *Every decomposition*

$$z^n = A_1 \circ A_2 \circ \cdots \circ A_r, \quad r \geq 2,$$

of the formal power series z^n, $n \geq 2$, into a composition of elements of Γ is equivalent to the decomposition

$$z^n = z^{\operatorname{ord} A_1} \circ z^{\operatorname{ord} A_2} \circ \cdots \circ z^{\operatorname{ord} A_r}.$$

Our approach to the study of equations in Γ consists in the systematic use, along with the Böttcher functions, what we call the *transition functions*. By definition, the transitions functions associated with $A \in \Gamma$ are elements φ_A of $k_1[[z]]$ satisfying the condition

$$A \circ \varphi_A = A.$$

If $\operatorname{ord} A = n$, then there exist exactly n transition functions associated with A. Moreover, all these functions are iterates of the *primitive* transition function $\widehat{\varphi}_A$, defined by the formula

$$\widehat{\varphi}_A = \beta_A \circ \varepsilon_n z \circ \beta_A^{-1},$$

where $\varepsilon_n = e^{\frac{2\pi i}{n}}$ and β_A is a Böttcher function.

Transition functions turn out to be extremely convenient for studying equations in Γ due to the following two results, which we consider as some of the main results of the paper. The first result relates the primitive transition function of an element F of Γ with the primitive transition functions of "compositional right factors" of F, where by a compositional right factor of F we mean any element A of Γ such that $F = X \circ A$ for some $X \in zk[[z]]$.

Theorem 1.2. *Let $A \in k_n[[z]]$, $n \geq 2$, and $F \in k_{nm}[[z]]$, $m \geq 1$, be formal power series. Then the following conditions are equivalent:*

1) *The equality*
$$F = X \circ A$$
holds for some formal power series $X \in k_m[[z]]$.
2) *The equality*
$$F \circ \widehat{\varphi}_A = F$$
holds.
3) *The equality*
$$\widehat{\varphi}_A = \widehat{\varphi}_F^{\circ m}$$
holds.

The second result relating transition functions with functional equations is the following statement.

Theorem 1.3. *Let $A, B \in \Gamma$ be formal power series. Then the equation*

$$X \circ A = Y \circ B$$

has a solution in formal power series $X, Y \in zk[[z]]$ if and only if the equality

$$\widehat{\varphi}_A \circ \widehat{\varphi}_B = \widehat{\varphi}_B \circ \widehat{\varphi}_A$$

holds.

Notice that, in distinction with the Böttcher function β_A, the transition function $\widehat{\varphi}_A$ does not define A in a unique way. However, Theorem 1.1 implies that if $\widehat{\varphi}_A = \widehat{\varphi}_B$ for $A, B \in \Gamma$ of the same order, then the equality $B = \mu \circ A$ holds for some $\mu \in k_1[[z]]$.

Another result of this paper concerns the following problem posed in [12]. If h is the composition of two formal power series f and g, and if h is even, what can be said about f and g ? In particular, is it true that f or g must be even ? Some partial results, in particular, in the context of decompositions of entire functions or polynomials, were obtained in the papers [3], [4], [12], [13]. In this paper, we provide an answer in the case where f, g and h are elements of Γ. In fact, along with "even" formal power series having the form $R(z^2)$ for some $R \in k[[z]]$, we also consider "odd" series having the form $zR(z^2)$ and, more generally, "symmetric" series having the form $z^r R(z^m)$, where $m \geq 2$, $r \geq 0$ are integers.

Theorem 1.4. *Let $A \in \Gamma$ be a formal power series of the form $A = z^r R(z^m)$, where $R \in k[[z]]$ and $m \geq 2$, $r \geq 0$ are integers. Then for every decomposition $A = A_1 \circ A_2$ of A into a composition of formal power series $A_1, A_2 \in \Gamma$ there exist $\mu \in k_1[[z]]$ and $R_1, R_2 \in k[[z]]$ such that*

$$A_1 = z^{r_1} R_1(z^{\frac{m}{\gcd(r_2, m)}}) \circ \mu^{-1}, \qquad A_2 = \mu \circ z^{r_2} R_2(z^m)$$

for some integers $r_1, r_2 \geq 0$ satisfying the condition $r_1 r_2 \equiv r \pmod{m}$.

Notice that Theorem 1.4 implies in particular that if $A = A_1 \circ A_2$ is even, then either A_2 is even, or there exists $\mu \in k_1[[z]]$ such that $A_1 \circ \mu$ is even. On the other hand, Theorem 1.4 implies that if $A = A_1 \circ A_2$ is odd, then there exists $\mu \in k_1[[z]]$ such that $A_1 \circ \mu$ and $\mu^{-1} \circ A_2$ are odd.

As an application of our results about functional equations in Γ, we provide a handy necessary condition for a subsemigroup of Γ to be right amenable. Let us denote by $\mathcal{Z}$ the subsemigroup of Γ consisting of monomials az^n, where $a \in k^*$ and $n \geq 2$, and by $\mathcal{Z}^U$ the subsemigroup consisting of all monomials of the form ωz^n, $n \geq 2$, where ω is a root of unity. We say that two subsemigroups S_1 and S_2 of Γ are *conjugate* if there exists a formal power series $\alpha \in k_1[[z]]$ such that

$$\alpha \circ S_1 \circ \alpha^{-1} = S_2.$$

It was shown in [22] that a *finitely* generated subsemigroup of Γ is right amenable if and only if it is conjugate to a subsemigroup of $\mathcal{Z}^U$. Still, it was observed that an *infinitely* generated right amenable subsemigroup of Γ is not necessarily conjugate to a subsemigroup of $\mathcal{Z}^U$. In this paper, we prove the following result.

Theorem 1.5. *Every right amenable subsemigroup S of Γ is conjugate to a subsemigroup of $\mathcal{Z}$.*

This paper is organized as follows. In the second section, after recalling several elementary facts about the semigroup $k_1[[z]]$, we discuss Bötcher functions and some of their immediate applications to functional equations. In the third section, we introduce transition functions and establish their basic properties. In the fourth section, we solve the functional equations

$$F = A \circ X \quad \text{and} \quad F = X \circ A,$$

where $F, A \in \Gamma$ are given and $X \in zk[[z]]$ is unknown, in terms of the corresponding Böttcher functions. We also prove Theorem 1.2 and several of its corollaries.

In the fifth section, we apply the obtained results to questions concerning decompositions of elements of Γ. In particular, we prove Theorem 1.1. In the sixths section, we characterize "symmetric" series in terms of their Bötcher and transition functions, and prove Theorem 1.4. We also reprove the result of Reznick ([25]) stating that if an iterate of $A \in \Gamma$ is symmetric, then A is also symmetric. In the seventh section, we consider the functional equation

$$X \circ A = Y \circ B,$$

where $A, B \in \Gamma$ are given and $X, Y \in zk[[z]]$ are unknown. We start by proving Theorem 1.3. Then we deduce from it a description of pairs $A, B \in \Gamma$ such that the functional equation

$$X \circ A^{\circ k} = Y \circ B^{\circ l}$$

has a solution for all $k, l \geq 1$. Finally, we prove Theorem 1.5. Moreover, we show that its conclusion holds already under the assumption that S is right reversible, which is weaker than the assumption that S is right amenable.

2. Böttcher functions

2.1. **Lemmata about formal power series.** In this paper, k always denotes an algebraically closed field of characteristic zero. In particular, k contains all roots of unity, for which we use the notation

$$\varepsilon_n = e^{\frac{2\pi i}{n}}, \quad n \geq 1.$$

For elementary properties of the ring of formal power series $k[[z]]$ and the semigroup $zk[[z]]$ under the composition operation $\circ$, we refer the reader to the first paragraph of [9]. In particular, we will use the fact that $k[[z]]$ is an integer domain and that an element A of $zk[[z]]$ is invertible with respect to $\circ$ if and only if A belongs to $k_1[[z]]$. Below we collect some further simple facts about $k[[z]]$.

Lemma 2.1. *Formal power series $\mu_1, \mu_2 \in k[[z]]$ satisfy the equality*

$$z^n \circ \mu_1 = z^n \circ \mu_2, \quad n \geq 2,$$

if and only if $\mu_1 = \varepsilon \mu_2$, where $\varepsilon^n = 1$.

Proof. Since

$$\mu_1^n - \mu_2^n = (\mu_1 - \mu_2)(\mu_1 - \varepsilon_n \mu_2)(\mu_1 - \varepsilon_n^2 \mu_2) \dots (\mu_1 - \varepsilon_n^{n-1} \mu_2),$$

the lemma follows from the fact that $k[[z]]$ is an integer domain. □

Lemma 2.2. *Let $\mu \in k[[z]] \setminus k$ and $a, b \in k^*$ satisfy the equality*

$$\mu \circ az = bz \circ \mu. \tag{1}$$

Then $b = a^r$ for some $r \in \mathbb{N}$. Furthermore, either $\mu = cz^r$, $r \geq 1$, for some $c \in k^*$, or a is a root of unity. Finally, μ satisfies the equality

$$\mu \circ \varepsilon z = \varepsilon^r z \circ \mu \tag{2}$$

for some primitive nth root of unity ε and r, $0 \leq r \leq n-1$, if and only if there exists a formal power series $R \in k[[z]]$ such that $\mu = z^r R(z^n)$.

Proof. The proof is obtained by a comparison of coefficients in the left and the right parts of (1) and (2). □

Lemma 2.3. *A formal power series $\mu \in k[[z]]$ satisfies the equality*

$$z^n \circ \mu = \mu \circ z^n, \quad n \geq 2, \tag{3}$$

if and only if $\mu = \varepsilon z^m$ for some $(n-1)$th root of unity ε and $m \geq 0$.

Proof. Setting $m = \operatorname{ord} \mu$ and substituting $\mu = \sum_{i=m}^{\infty} c_i z^i$ into (3) we see that $c_m^n = c_m$. Furthermore, if $\mu \neq c_m z^m$ we obtain a contradiction as follows. Let $l > m$ be the minimum number such that $c_l \neq 0$. Then

$$\mu = c_m z^m + c_l z^l + \text{higher terms},$$

implying that

$$\mu \circ z^n = c_m z^{mn} + c_l z^{ln} + \text{higher terms}.$$

On the other hand,

$$z^n \circ \mu = c_m^n z^{mn} + n c_m^{n-1} c_l z^{m(n-1)+l} + \text{higher terms}.$$

Since

$$m(n-1) + l < l(n-1) + l = ln,$$

this is impossible, and hence $\mu = c_m z^m$. □

Lemma 2.4. *Formal power series $\mu_1, \mu_2 \in k[[z]] \setminus k$ satisfy the equality*

$$z^n \circ \mu_1 = \mu_2 \circ z^n, \quad n \geq 2, \tag{4}$$

if and only if there exist $R \in k[[z]]$ and r, $0 \leq r \leq n-1$, such that

$$\mu_1 = z^r R(z^n), \qquad \mu_2 = z^r R^n(z).$$

Proof. The identity

$$z^n \circ z^r R(z^n) = z^r R^n(z) \circ z^n \tag{5}$$

is checked by a direct calculation. To prove the "only if" part, we observe that equality (4) implies the equality

$$z^n \circ \mu_1 = z^n \circ (\mu_1 \circ \varepsilon_n z).$$

Therefore, by Lemma 2.1, there exist r, $0 \leq r \leq n-1$, such that

$$\mu_1 \circ \varepsilon_n z = \varepsilon_n^r z \circ \mu_1,$$

implying by Lemma 2.2 that $\mu_1 = z^r R(z^n)$ for some $R \in k[[z]]$. It follows now from (4) that

$$\mu_2 \circ z^n = z^n \circ \mu_1 = z^{rn} R^n(z^n) = z^r R^n(z) \circ z^n,$$

implying that $\mu_2 = z^r R^n(z)$. □

Notice that the representation $\mu_2 = z^r R^n(z)$ appearing in Lemma 2.4 defines the series R only up to a multiplication by an nth root of unity. Accordingly, to μ_2 correspond n different μ_1 such that (4) holds.

2.2. **Böttcher functions and the equation $A\circ X=Y\circ B$.** Let $A\in\Gamma$ be a formal power series of order n. Then the corresponding Böttcher function is defined as a formal series $\beta_A\in k_1[[z]]$ such that the equality

$$A\circ\beta_A=\beta_A\circ z^n \tag{6}$$

holds. It is known that such a function exists and is defined in a unique way up to the change $\beta_A(z)\to\beta_A(\varepsilon z)$, where $\varepsilon^{n-1}=1$. In the context of complex dynamics, this fact is widely used and goes back to Böttcher (see [5], [26], [18]). For the proof in the algebraic setting, see [17] (Hilffsatz 4).

Among other things, the existence of Böttcher functions yields the following statement.

Theorem 2.5. *Let $A_1,A_2\in k[[z]]$ and $X\in zk[[z]]$ be formal power series. Then the equality*

$$A_1\circ X=A_2\circ X \tag{7}$$

holds if and only $A_1=A_2$.

Proof. In case X is invertible in the semigroup $zk[[z]]$, the statement is clear. Otherwise setting $n=\operatorname{ord}X$ and conjugating (7) by β_X, we obtain the equality

$$(\beta_X^{-1}\circ A_1\circ\beta_X)\circ z^n=(\beta_X^{-1}\circ A_2\circ\beta_X)\circ z^n,$$

which obviously implies that

$$\beta_X^{-1}\circ A_1\circ\beta_X=\beta_X^{-1}\circ A_2\circ\beta_X.$$

In turn, this implies that $A_1=A_2$ since β_A is invertible in $zk[[z]]$ □

Using Böttcher functions, one can provide a solution in $X,Y\in zk[[z]]$ of the functional equation

$$A\circ X=Y\circ B,$$

where A and B are given elements of Γ of the same order, generalizing equation (6). We start by considering the following particular case.

Theorem 2.6. *Let $A\in\Gamma$ be a formal power series of order n, and β_A some Böttcher function. Then formal power series $X,Y\in zk[[z]]$ satisfy the equality*

$$A\circ X=Y\circ z^n \tag{8}$$

if and only if there exist $R\in k[[z]]$ and r, $0\le r\le n-1$, such that

$$X=\beta_A\circ z^rR(z^n),\qquad Y=\beta_A\circ z^rR^n(z). \tag{9}$$

Furthermore, if $X=Y$, then solutions of (8) *are given by the formula*

$$X=\beta_A\circ\varepsilon_{n-1}^kz^l,\qquad 0\le k\le n-2,$$

where $l=\operatorname{ord}X$.

Proof. The "if" part is obtained from equalities (5) and (6). In the other direction, taking an arbitrary Böttcher function β_A and substituting $\beta_A\circ z^n\circ\beta_A^{-1}$ for A in (8), we obtain

$$\beta_A\circ z^n\circ\beta_A^{-1}\circ X=Y\circ z^n,$$

implying that

$$z^n\circ(\beta_A^{-1}\circ X)=(\beta_A^{-1}\circ Y)\circ z^n.$$

Thus, equalities (9) hold for some $R\in k[[z]]$ and r, $0\le r\le n-1$, by Lemma 2.4.

Furthermore, if $X = Y$, then (9) implies that

$$z^r R(z^n) = z^r R^n(z).$$

In turn, this yields that R commutes with z^n, implying by Lemma 2.3 that $R = \varepsilon z^m$, where $\varepsilon^{n-1} = 1$ and $m \geq 0$. Thus, there exists k, $0 \leq k \leq n-2$, such that

$$z^r R(z^n) = \varepsilon_{n-1}^k z^l,$$

where

$$l = \operatorname{ord} z^r R(z^n) = \operatorname{ord} X. \qquad \square$$

Theorem 2.6 implies the following more general statement.

Theorem 2.7. *Let $A, B \in \Gamma$ be formal power series of the same order n, and β_A, β_B some Böttcher functions. Then $X, Y \in zk[[z]]$ satisfy the equality*

$$A \circ X = Y \circ B \tag{10}$$

if and only if there exist $R \in k[[z]]$ and r, $0 \leq r \leq n-1$, such that

$$X = \beta_A \circ z^r R(z^n) \circ \beta_B^{-1}, \qquad Y = \beta_A \circ z^r R^n(z) \circ \beta_B^{-1}.$$

Furthermore, if $X = Y$, then solutions of (10) *are given by the formula*

$$X = \beta_A \circ \varepsilon_{n-1}^k z^l \circ \beta_B^{-1}, \qquad 0 \leq k \leq n-2,$$

where $l = \operatorname{ord} X$.

Proof. For an arbitrary Böttcher function β_B, equality (10) is equivalent to the equality

$$A \circ (X \circ \beta_B) = (Y \circ \beta_B) \circ z^n.$$

Thus, the theorem follows Theorem 2.6. $\square$

3. Transition functions

Let $A \in \Gamma$ be a formal power series of order n. We recall that a transition function corresponding to A is defined as a formal series φ_A such that the equality

$$A \circ \varphi_A = A \tag{11}$$

holds. It is clear that such a series necessarily belongs to $k_1[[z]]$. In the context of *analytical* functions, transition functions were defined in the paper [11], and the following two lemmas are algebraic counterparts of the results of Section 2 in [11].

Lemma 3.1. *Let $A \in \Gamma$ be a formal powes series of order n, and β_A some Böttcher function. Then there are exactly n transition functions corresponding to A, and they are defined by the formula*

$$\varphi_A = \beta_A \circ \varepsilon_n^k z \circ \beta_A^{-1}, \qquad 0 \leq k \leq n-1. \tag{12}$$

Proof. It follows from equality (6) that

$$A \circ \beta_A = A \circ \beta_A \circ \varepsilon_n^k z, \qquad 0 \leq k \leq n-1,$$

implying that

$$A = A \circ (\beta_A \circ \varepsilon_n^k z \circ \beta_A^{-1}), \qquad 0 \leq k \leq n-1.$$

On the other hand, if equality (11) holds, then conjugating its parts by β_A, we obtain

$$z^n \circ (\beta_A^{-1} \circ \varphi_A \circ \beta_A) = z^n,$$

implying by Lemma 2.1 that

$$\beta_A^{-1} \circ \varphi_A \circ \beta_A = \varepsilon_n^k z$$

for some k, $0 \leq k \leq n-1$. Finally, since β_A is invertible in $zk[[z]]$, to different roots of unity ε_n^k, $0 \leq k \leq n-1$, correspond different functions (12). □

For a formal power series $\varphi \in k_1[[z]]$, we will denote by $|\varphi|$ the minimum number d such that $\varphi^{\circ d} = z$. In case $\varphi^{\circ d}$ is distinct from z for every $d \geq 1$, we set $|\varphi| = \infty$. In other words, d is the order of φ in the group $k_1[[z]]$.

Lemma 3.2. *Let $\varphi \in k_1[[z]]$ be a formal power series with $|A| = d$. Then $\varphi = \varphi_A$ for some formal power series $A \in \Gamma$ if and only if $1 < d < \infty$. Moreover, in the last case there exists $A \in k_d[[z]]$ such that $\varphi = \varphi_A$.*

Proof. Since the functions defined by formula (12) satisfy $\varphi_A^{\circ d} = z$, the "only if" part follows from Lemma 3.1. On the other hand, if $1 < d < \infty$, then setting

$$A = z \cdot \varphi \cdot \varphi^{\circ 2} \cdot \ldots \cdot \varphi^{\circ (d-1)},$$

we see that $A \in k_d[[z]]$ and the equality $A \circ \varphi = A$ holds. □

The following statement is a counterpart of Theorem 2.5 for the functional equation $A \circ X_1 = A \circ X_2$.

Theorem 3.3. *Let $A \in \Gamma$ and $X_1, X_2 \in zk[[z]]$ be formal power series. Then the equality*

$$A \circ X_1 = A \circ X_2 \tag{13}$$

holds if and only if

$$X_2 = \varphi_A \circ X_1$$

for some transition function φ_A.

Proof. The "if" part is obvious. On the other hand if equality (13) holds, then conjugating its parts by β_A we obtain

$$z^n \circ (\beta_A^{-1} \circ X_1 \circ \beta_A) = z^n \circ (\beta_A^{-1} \circ X_2 \circ \beta_A),$$

implying that

$$\beta_A^{-1} \circ X_2 \circ \beta_A = \varepsilon_n^k z \circ \beta_A^{-1} \circ X_1 \circ \beta_A$$

for some k, $0 \leq r \leq n-1$, by Lemma 2.1. Therefore,

$$X_2 = \beta_A \circ \varepsilon_n^k z \circ \beta_A^{-1} \circ X_1 = \varphi_A \circ X_1,$$

by Lemma 3.1. □

We will use the notation $\widehat{\varphi}_A$ for the transition function given by the formula

$$\widehat{\varphi}_A = \beta_A \circ \varepsilon_n z \circ \beta_A^{-1}.$$

We will call this transition function *primitive*. Notice that $\widehat{\varphi}_A$ does not depend on the choice of β_A. The following lemma follows immediately from Lemma 3.1.

Lemma 3.4. *Let $A \in \Gamma$ be a formal power series. Then every transition function φ_A is an iterate of $\widehat{\varphi}_A$.* □

We finish this section by the following lemma.

Lemma 3.5. *Let $A \in \Gamma$ be a formal power series of order n. Then for every $l \geq 1$ the equality*

$$\widehat{\varphi}_{A^{\circ l}} = \beta_A \circ \varepsilon_{nl} z \circ \beta_A^{-1} \tag{14}$$

holds. On the other hand, if

$$A_\mu = \mu^{-1} \circ A \circ \mu, \qquad \mu \in k_1[[z]],$$

then

$$\widehat{\varphi}_{A_\mu} = \mu^{-1} \circ \widehat{\varphi}_A \circ \mu. \tag{15}$$

Proof. Equality (14) follows from the fact that β_A remains a Böttcher function for $A^{\circ l}$, $l \geq 1$. On the other hand, since the leading coefficient of $\mu^{-1} \circ \widehat{\varphi}_A \circ \mu$ equals ε_n, equality (15) follows from the equality

$$A_\mu \circ (\mu^{-1} \circ \widehat{\varphi}_A \circ \mu) = A_\mu,$$

which is obtained by a direct calculation. □

4. Functional equations $F = A \circ X$ and $F = X \circ A$

The next two results provide solutions of the functional equations $F = A \circ X$ and $F = X \circ A$, where $F, A \in \Gamma$ are given and $X \in zk[[z]]$ is unknown, in terms of the corresponding Böttcher functions β_F and β_A.

Theorem 4.1. *Let $A \in k_n[[z]]$, $n \geq 2$, and $F \in k_{nm}[[z]]$, $m \geq 1$, be formal power series, and β_A, β_F some Böttcher functions. Then the equation*

$$F = X \circ A \tag{16}$$

has a solution $X \in k_m[[z]]$ if and only if there exist $R \in k[[z]]$ and r, $0 \leq r \leq n-1$ such that

$$z^m \circ \beta_F^{-1} \circ \beta_A = z^r R(z^n). \tag{17}$$

Furthermore, if (17) holds, then (16) has a unique solution X given by the formula

$$X = \beta_F \circ z^r R^n(z) \circ \beta_A^{-1}. \tag{18}$$

Proof. Substituting $\beta_F \circ z^{nm} \circ \beta_F^{-1}$ for F and $\beta_A \circ z^n \circ \beta_A^{-1}$ for A to (16), we obtain the equality

$$\beta_F \circ z^{nm} \circ \beta_F^{-1} = X \circ \beta_A \circ z^n \circ \beta_A^{-1},$$

which in turn implies the equality

$$z^n \circ (z^m \circ \beta_F^{-1} \circ \beta_A) = (\beta_F^{-1} \circ X \circ \beta_A) \circ z^n,$$

Thus, the "only if" part follows from Lemma 2.4.

In the other direction, (17) implies that

$$F = \beta_F \circ z^{nm} \circ \beta_F^{-1} = \beta_F \circ z^n \circ z^m \circ \beta_F^{-1} = \beta_F \circ z^n \circ z^r R(z^n) \circ \beta_A^{-1} =$$

$$= \beta_F \circ z^r R^n(z) \circ z^n \circ \beta_A^{-1} = \beta_F \circ z^r R^n(z) \circ \beta_A^{-1} \circ A.$$

Thus, (16) holds for X given by (18). Finally, the function X is defined by formula (18) in a unique way by Theorem 2.5. □

Theorem 4.2. *Let $A \in k_n[[z]]$, $n \geq 2$, and $F \in k_{nm}[[z]]$, $m \geq 1$, be formal power series, and β_A, β_F some Böttcher functions. Then the equation*

$$F = A \circ X \tag{19}$$

has a solution $X \in k_m[[z]]$ if and only if there exist $L \in k[[z]]$ and r, $0 \leq r \leq n-1$, such that

$$\beta_A^{-1} \circ \beta_F \circ z^m = z^r L^n(z). \tag{20}$$

Furthermore, if (20) *holds, then* (19) *has n solutions given by the formula*

$$X = \beta_A \circ \varepsilon_n^k z \circ z^r L(z^n) \circ \beta_F^{-1}, \quad 0 \leq k \leq n-1.$$

Proof. Equality (19) implies the equality

$$\beta_F \circ z^{nm} \circ \beta_F^{-1} = \beta_A \circ z^n \circ \beta_A^{-1} \circ X,$$

which in turn implies the equality

$$(\beta_A^{-1} \circ \beta_F \circ z^m) \circ z^n = z^n \circ (\beta_A^{-1} \circ X \circ \beta_F).$$

Thus, the "only if" part follows from Lemma 2.4.

In the other direction, (20) implies that

$$F = \beta_F \circ z^{nm} \circ \beta_F^{-1} = \beta_F \circ z^m \circ z^n \circ \beta_F^{-1} = \beta_A \circ z^r L^n(z) \circ z^n \circ \beta_F^{-1} =$$

$$= \beta_A \circ z^n \circ z^r L(z^n) \circ \beta_F^{-1} = A \circ \beta_A \circ z^r L(z^n) \circ \beta_F^{-1}$$

Thus, (19) holds for

$$X = \beta_A \circ z^r L(z^n) \circ \beta_F^{-1}.$$

Finally, by Theorem 3.3 and Lemma 3.1, any other solution of (18) has the form

$$X = \varphi_A \circ \beta_A \circ z^r L(z^n) \circ \beta_F^{-1} = \beta_A \circ \varepsilon_n^k z \circ \beta_A^{-1} \circ \beta_A \circ z^r L(z^n) \circ \beta_F^{-1} =$$

$$= \beta_A \circ \varepsilon_n^k z \circ z^r L(z^n) \circ \beta_F^{-1}, \quad 0 \leq k \leq n-1. \qquad \square$$

Proof of Theorem 1.2. If

$$F = X \circ A, \tag{21}$$

then

$$F \circ \widehat{\varphi}_A = X \circ A \circ \widehat{\varphi}_A = X \circ A = F.$$

Thus, 1) $\Rightarrow$ 2).

In the other direction, equality

$$F \circ \widehat{\varphi}_A = F$$

implies the equalities

$$\beta_F \circ z^{nm} \circ \beta_F^{-1} \circ \beta_A \circ \varepsilon_n z \circ \beta_A^{-1} = \beta_F \circ z^{nm} \circ \beta_F^{-1}$$

and

$$z^{nm} \circ \beta_F^{-1} \circ \beta_A \circ \varepsilon_n z = z^{nm} \circ \beta_F^{-1} \circ \beta_A.$$

Therefore,

$$z^n \circ (z^m \circ \beta_F^{-1} \circ \beta_A \circ \varepsilon_n z) = z^n \circ (z^m \circ \beta_F^{-1} \circ \beta_A),$$

implying by Lemma 2.1 that

$$(z^m \circ \beta_F^{-1} \circ \beta_A) \circ \varepsilon_n z = \varepsilon_n^r z \circ (z^m \circ \beta_F^{-1} \circ \beta_A)$$

for some r, $0 \le r \le n-1$. It follows now from Lemma 2.2 that there exists $R \in k[[z]]$ such that (17) holds. Thus, (21) holds for some $X \in k_m[[z]]$ by Theorem 4.1. Hence, 2) $\Rightarrow$ 1).

Further, if 2) holds, then $\widehat{\varphi}_A$ is a transition function for F. Therefore, $\widehat{\varphi}_A$ is an iterate of $\widehat{\varphi}_F$ by Lemma 3.4, and the comparison of coefficients shows that 3) holds. Finally, 3) obviously implies 2). □

Corollary 4.3. *Let $A, B \in \Gamma$ be formal power series of the same order. Then the equality*

$$\widehat{\varphi}_A = \widehat{\varphi}_B$$

holds if and only if

$$B = \mu \circ A$$

for some $\mu \in k_1[[z]]$.

Proof. The corollary follows from Theorem 1.2 for $m = 1$ and $F = B$. □

Corollary 4.4. *Let $F \in \Gamma$ be a formal power series, and $A, B \in \Gamma$ some compositional right factors of F. Then any transition functions φ_A and φ_B commute.*

Proof. By Theorem 1.2, the both functions φ_A and φ_B are iterates of $\widehat{\varphi}_F$. Hence, they commute. □

The following corollary provides a criterion for two elements of Γ to have "a common compositional right factor" in Γ.

Corollary 4.5. *Let $A \in k_n[[z]]$, $B \in k_m[[z]]$, $n, m \ge 2$, be formal power series and $d \ge 2$ a common divisor of n and m. Then the equalities*

$$A = \widetilde{A} \circ W, \qquad B = \widetilde{B} \circ W, \tag{22}$$

hold for some series $\widetilde{A} \in k_{n/d}[[z]]$, $\widetilde{B} \in k_{m/d}[[z]]$, and $W \in k_d[[z]]$ if and only if the equality

$$\widehat{\varphi}_A^{\circ n/d} = \widehat{\varphi}_B^{\circ m/d} \tag{23}$$

holds.

Proof. If (22) holds, then it follows from Theorem 1.2 that

$$\widehat{\varphi}_W = \widehat{\varphi}_A^{\circ n/d}, \quad \widehat{\varphi}_W = \widehat{\varphi}_B^{\circ m/d},$$

implying (23).

In the other direction, denoting by φ the series defined by any of the parts of equality (23), we see that $|\varphi| = d$, implying by Lemma 3.2 that there exists $W \in k_d[[z]]$ such that $\varphi = \widehat{\varphi}_W$. It follows now from

$$\widehat{\varphi}_A^{\circ n/d} = \widehat{\varphi}_B^{\circ m/d} = \widehat{\varphi}_W$$

by Theorem 1.2 that (22) holds. □

We finish this section by the following result, providing a criterion for a formal power series $D \in \Gamma$ to be a compositional right factor of a composition of formal power series $A, C \in \Gamma$.

Theorem 4.6. *Let $A, C, D \in \Gamma$ be formal power series. Then the equation*

$$A \circ C = X \circ D \tag{24}$$

has a solution $X \in k[[z]]$ if and only if the equality

$$C \circ \widehat{\varphi}_D = \widehat{\varphi}_A \circ C \tag{25}$$

holds.

Proof. Equality (25) implies that

$$A \circ C \circ \widehat{\varphi}_D = A \circ \widehat{\varphi}_A \circ C = A \circ C.$$

Therefore, (24) has a solution by Theorem 1.2.

In the other direction, equality (24) implies that

$$A \circ C = A \circ C \circ \widehat{\varphi}_D.$$

Thus, (25) holds by Theorem 3.3. □

5. Decompositions of formal power series

Let $A \in \Gamma$ be a formal power series. Then A is called *indecomposable* if the equality $A = A_1 \circ A_2$, where A_1, A_2 are formal power series, implies that at least one of the series A_1, A_2 is of order one. A formal power series $A \in \Gamma$ that is not indecomposable is called *decomposable*. Let us recall that an *ordered factorization* of an integer $n \geq 2$ is a representation of n as an ordered product of factors greater than one, where two representations are considered identical if they contain the same factors in the same order. Every decomposition

$$A = A_1 \circ A_2 \circ \cdots \circ A_r$$

of a formal power series $A \in \Gamma$ into a composition of formal power series $A_1, A_2, \dots, A_r \in \Gamma$ gives rise to an ordered factorization

$$\operatorname{ord} A = \operatorname{ord} A_1 \cdot \operatorname{ord} A_2 \cdot \ \dots \ \cdot \operatorname{ord} A_r,$$

and the following slightly extended version of Theorem 1.1 from the introduction shows that equivalence classes of decompositions of A are in a one-to-one correspondence with ordered factorizations of $\operatorname{ord} A$.

Theorem 5.1. *Let $A \in \Gamma$ be a formal power series of order n, and β_A some Bötcher function. Then every decomposition*

$$A = A_1 \circ A_2 \circ \cdots \circ A_r \tag{26}$$

of A into a composition of elements of Γ is equivalent to the decomposition

$$A = (\beta_A \circ z^{\operatorname{ord} A_1}) \circ z^{\operatorname{ord} A_2} \circ \cdots \circ (z^{\operatorname{ord} A_r} \circ \beta_A^{-1}). \tag{27}$$

Thus, equivalence classes of decompositions of F are in a one-to-one correspondence with ordered factorizations of n. In particular, F is indecomposable if and only if n is a prime number.

Proof. Let us set

$$\operatorname{ord} A_k = n_k, \quad 1 \leq k \leq r.$$

Since

$$\beta_A^{-1} \circ A \circ \beta_A = z^n = (\beta_A^{-1} \circ A_1) \circ A_2 \circ \cdots \circ (A_r \circ \beta_A),$$

to prove the theorem it is enough to show that every decomposition (26) of $A = z^n$ is equivalent to the decomposition

$$z^n = z^{n_1} \circ z^{n_2} \circ \cdots \circ z^{n_r}. \tag{28}$$

We prove the last statement by induction on r.

Since $\widehat{\varphi}_{z^n} = \varepsilon_n z$, it follows from Theorem 1.2 that

$$\widehat{\varphi}_{A_r} = \widehat{\varphi}_A^{\circ \frac{n}{n_r}} = \varepsilon_{n_r} z = \widehat{\varphi}_{z^{n_r}},$$

implying by Corollary 4.3 that

$$A_r = \mu_{r-1} \circ z^{n_r} \tag{29}$$

for some $\mu_{r-1} \in k_1[[z]]$. Thus, if $r = 2$, we have:

$$z^{n_1 n_2} = A_1 \circ \mu_1 \circ z^{n_2},$$

implying by Theorem 2.5 that $A_1 = z^{n_1} \circ \mu_1^{-1}$. On the other hand, if $r > 2$, then in a similar way we obtain the equalities (29) and

$$z^{n_1 n_2 \dots n_{r-1}} = A_1 \circ A_2 \dots (A_{r-1} \circ \mu_1).$$

By the induction assumption, the decomposition in the right part of the last equality is equivalent to the decomposition $z^{n_1} \circ z^{n_2} \circ \cdots \circ z^{n_{r-1}}$, and in view of (29) this implies that decompositions (26) and (28) are equivalent. □

Notice that Theorem 5.1 implies that decompositions (27) for *different* β_A are equivalent. In the explicit form, this equivalence is given by the formula

$$A = (\beta_A \circ \varepsilon z \circ z^{n_1}) \circ z^{n_2} \circ \cdots \circ z^{n_{r-1}} \circ (z^{n_r} \circ \varepsilon^{-1} z \circ \beta_A^{-1}) =$$

$$= (\beta_A \circ z^{n_1} \circ \varepsilon^{n_2 n_3 \dots n_r} z) \circ \prod_{i=2}^{r-1} \left(\varepsilon^{-n_i \dots n_r} z \circ z^{n_i} \circ \varepsilon^{n_{i+1} \dots n_r} z\right) \circ (\varepsilon^{-n_r} \circ z^{n_r} \circ \beta_A^{-1}),$$

where ε is an $(n-1)$th root of unity.

Theorem 5.2. *Let $A, B, C, D \in \Gamma$ be formal power series such that*

$$A \circ C = B \circ D. \tag{30}$$

Then there exist formal power series $U, V, \widetilde{A}, \widetilde{C}, \widetilde{B}, \widetilde{D} \in zk[[z]]$, where

$$\operatorname{ord} U = \operatorname{GCD}(\operatorname{ord} A, \operatorname{ord} B), \quad \operatorname{ord} V = \operatorname{GCD}(\operatorname{ord} C, \operatorname{ord} D),$$

such that

$$A = U \circ \widetilde{A}, \quad B = U \circ \widetilde{B}, \quad C = \widetilde{C} \circ V, \quad D = \widetilde{D} \circ V,$$

and

$$\widetilde{A} \circ \widetilde{C} = \widetilde{B} \circ \widetilde{D}.$$

In particular, if $\operatorname{ord} A = \operatorname{ord} B$ then the decompositions $A \circ C$ and $B \circ D$ are necessarily equivalent.

Proof. Let us set

$$F = A \circ C = B \circ D,$$

$$n = \operatorname{ord} F, \quad a = \operatorname{ord} A, \quad b = \operatorname{ord} B, \quad c = \operatorname{ord} C, \quad d = \operatorname{ord} D,$$

$$u = \gcd(a, b), \quad v = \gcd(c, d).$$

Applying Theorem 5.1, we see that there exist formal powers series $\nu, \mu \in k_1[[z]]$ such that

$$A = \beta_F \circ z^a \circ \nu^{-1}, \quad C = \nu \circ z^c \circ \beta_F^{-1},$$

and

$$B = \beta_F \circ z^b \circ \mu^{-1}, \quad C = \mu \circ z^d \circ \beta_F^{-1}.$$

Therefore, the statement of the theorem is true for

$$U = \beta_F \circ z^u, \quad V = z^v \circ \beta_F^{-1}$$

and

$$\widetilde{A} = z^{\circ \frac{a}{u}} \circ \nu^{-1}, \quad \widetilde{C} = \nu \circ z^{\circ \frac{c}{v}},$$
$$\widetilde{B} = z^{\circ \frac{b}{u}} \circ \mu^{-1}, \quad \widetilde{D} = \mu \circ z^{\circ \frac{d}{v}}.$$ □

Notice that Theorem 1.1 can be considered as a formal power series analogue of the Ritt theory of polynomial decompositions ([27]), while Theorem 5.2 is an analogue of the result of Engstrom ([10]) about polynomial solutions of (30).

6. Formal power series with symmetries

6.1. **Characterizations of formal powers series with symmetries.** The following result characterizes formal powers series of the form $A = z^r R(z^m)$, where $R \in k[[z]]$ and $m \geq 2$, $r \geq 0$ are integers, in terms of the corresponding Bötcher functions.

Theorem 6.1. *Let $A \in \Gamma$ be a formal power series of order n, β_A some Bötcher function, and m, $2 \leq m \leq n$, an integer. Then A has the form $A = z^r R(z^m)$, where $R \in k[[z]]$ and $r \geq 0$, if and only if there exists $L \in k_0[[z]]$ such that $\beta_A = zL(z^m)$.*

Proof. Since equality (6) implies the equality

$$A \circ \beta_A \circ \varepsilon_m z = \beta_A \circ z^n \circ \varepsilon_m z,$$

if $\beta_A = zL(z^m)$, then

$$(A \circ \varepsilon_m z) \circ \beta_A = A \circ \beta_A \circ \varepsilon_m z = \beta_A \circ z^n \circ \varepsilon_m z = \beta_A \circ \varepsilon_m^n z \circ z^n =$$
$$= \varepsilon_m^n z \circ \beta_A \circ z^n = (\varepsilon_m^n z \circ A) \circ \beta_A,$$

implying that

$$A \circ \varepsilon_m z = \varepsilon_m^n z \circ A.$$

Since $\varepsilon_m^n = \varepsilon_m^r$ for some r satisfying $0 \leq r \leq m-1$, it follows now from Lemma 2.2 that $A = z^r R(z^m)$.

In the other direction, let us assume that $A = z^r R(z^m)$, where $R \in k[[z]]$ and $r \geq 0$, and set $\widehat{A} = z^r R^m(z)$. Since

$$\widehat{A} \circ z^m = z^m \circ A,$$

we have:

$$\widehat{A} \circ (z^m \circ \beta_A) = z^m \circ A \circ \beta_A = (z^m \circ \beta_A) \circ z^n,$$

implying by Theorem 2.6 that

$$z^m \circ \beta_A = \beta_{\widehat{A}} \circ z^m.$$

By Lemma 2.4, this implies that $\beta_A = z^l L(z^m)$, where $L \in k[[z]]$ and $0 \leq l \leq m-1$. Finally, since $\beta_A \in k_1[[z]]$, we conclude that $l = 1$ and $L \in k_0[[z]]$. □

The following result is a counterpart of Theorem 6.1 in the context of transition functions.

Theorem 6.2. *Let $A \in \Gamma$ be a formal power series of order n, and m, $2 \leq m \leq n$, an integer. Then A has the form $A = \mu \circ z^r R(z^m)$, where $R \in k[[z]]$, $\mu \in k_1[[z]]$, and $r \geq 0$, if and only if $\widehat{\varphi}_A = zM(z^m)$ for some $M \in k_0[[z]]$.*

Proof. Since

$$A \circ \widehat{\varphi}_A = A,$$

if $\widehat{\varphi}_A = zM(z^m)$, then

$$A \circ \varepsilon_m z = A \circ \widehat{\varphi}_A \circ \varepsilon_m z = (A \circ \varepsilon_m z) \circ \widehat{\varphi}_A.$$

Thus, $\widehat{\varphi}_A$ is the primitive transition function for the formal power series $A \circ \varepsilon_m z$, implying by Corollary 4.3 that

$$A \circ \varepsilon_m z = \nu \circ A \tag{31}$$

for some $\nu \in k_1[[z]]$. Furthermore, since the last equality implies that

$$A \circ (\varepsilon_m z)^{\circ l} = \nu^{\circ l} \circ A, \quad l \geq 1,$$

the number $d = |\nu|$ is finite and divides m. If $d = 1$, that is, if $\nu = z$, then applying Lemma 2.2 to equality (31) we conclude that $A = R(z^m)$ for some $R \in k[[z]]$. On the other hand, if $d > 1$, then by Lemma 3.2 there exists $F \in k_d[[z]]$ such that $\nu = \varphi_F$. Moreover, since d divides m, Lemma 3.1 yields that

$$\nu = \beta_F \circ \varepsilon_m^k \circ \beta_F^{-1}$$

for some k, $0 \leq k \leq m-1$. Substituting the right part of this equality for ν to (31), we conclude that

$$(\beta_F^{-1} \circ A) \circ \varepsilon_m z = \varepsilon_m^k z \circ (\beta_F^{-1} \circ A).$$

Thus,

$$\beta_F^{-1} \circ A = z^k R(z^m),$$

where $R \in k[[z]]$ and $0 \leq k \leq m-1$, by Lemma 2.2, and hence the equality $A = \mu \circ z^r R(z^m)$ holds for $\mu = \beta_F$ and $r = k$.

In the other direction, let us assume that $A = z^r R(z^m)$, where $R \in k[[z]]$ and $r \geq 0$. Then applying Corollary 4.4 to the function

$$F = \widehat{A} \circ z^m = z^m \circ A,$$

where $\widehat{A} = z^r R^m(z)$, we conclude that the transition functions $\widehat{\varphi}_{z^m} = \varepsilon_m z$ and $\widehat{\varphi}_A$ commute, implying by Lemma 2.2 that $\widehat{\varphi}_A = zM(z^m)$ for some $M \in k_0[[z]]$. □

6.2. **Decompositions of formal powers series with symmetries.** Below, we provide some applications of Theorem 6.1 and Theorem 6.2. We start by proving Theorem 1.4.

Proof of Theorem 1.4. Let

$$A = A_1 \circ A_2, \tag{32}$$

be a decomposition of A with $A_1, A_2 \in \Gamma$. Considering the equality

$$\widehat{A} \circ z^m = (z^m \circ A_1) \circ A_2,$$

where $\widehat{A} = z^r R^m(z)$, and using Corollary 4.4, we conclude that the transition functions $\widehat{\varphi}_{z^m} = \varepsilon_m z$ and $\widehat{\varphi}_{A_2}$ commute. Therefore, $\widehat{\varphi}_{A_2} = zM(z^m)$ for some $M \in k_0[[z]]$ by Lemma 2.2. Thus,

$$A_2 = \mu \circ z^{r_2} R_2(z^m) \tag{33}$$

for some $R_2 \in k[[z]]$, $\mu \in k_1[[z]]$, and $r_2 \geq 0$, by Theorem 6.2.

Furthermore, it follows from the equality

$$z^r R(z^m) = (A_1 \circ \mu) \circ z^{r_2} R_2(z^m)$$

that

$$(A_1 \circ \mu) \circ z^{r_2} R_2(z^m) \circ \varepsilon_m z = \varepsilon_m^r z \circ (A_1 \circ \mu) \circ z^{r_2} R_2(z^m),$$

implying that

$$(A_1 \circ \mu) \circ \varepsilon_m^{r_2} z \circ z^{r_2} R_2(z^m) = \varepsilon_m^r z \circ (A_1 \circ \mu) \circ z^{r_2} R_2(z^m).$$

Therefore,

$$(A_1 \circ \mu) \circ \varepsilon_m^{r_2} z = \varepsilon_m^r z \circ (A_1 \circ \mu),$$

by Theorem 2.5. Since $\varepsilon_m^{r_2}$ is an $\frac{m}{\gcd(r_2,m)}$th root of unity, it follows now from Lemma 2.2 that

$$A_1 \circ \mu = z^{r_1} R_1(z^{\frac{m}{\gcd(r_2,m)}})$$

for some $R_1 \in k[[z]]$ and $r_1 \geq 0$. Thus,

$$A_1 = z^{r_1} R_1(z^{\frac{m}{\gcd(r_2,m)}}) \circ \mu^{-1}. \tag{34}$$

Finally, it follows from (32) and (33), (34) that $r_1 r_2 \equiv r \pmod m$. □

Notice that since any composition of series A_1 and A_2 given by formulas (33), (34) has the form $z^r R(z^m)$, the series A_1 in a decomposition $A = A_1 \circ A_2$ may be "less" symmetric than A. In fact, if $r_2 = 0$, then A_1 may be not symmetric at all. Nevertheless, the following statement is true.

Corollary 6.3. *Let $A \in \Gamma$ be a formal power series of the form $A = z^r R(z^m)$, where $R \in k[[z]]$ and $m \geq 2$, $r \geq 1$ are integers such that $\gcd(r, m) = 1$. Then for every decomposition $A = A_1 \circ A_2$ of A into a composition of formal power series $A_1, A_2 \in \Gamma$ there exist $\mu \in k_1[[z]]$ and formal power series R_1 and R_2 such that*

$$A_1 = z^{r_1} R_1(z^m) \circ \mu^{-1}, \qquad A_2 = \mu \circ z^{r_2} R_2(z^m)$$

for some integers $r_1, r_2 \geq 1$ such that $\gcd(r_1, m) = 1$ and $\gcd(r_2, m) = 1$.

Proof. Since the numbers r_1, r_2 appearing in formulas (33), (34) satisfy the condition $r_1 r_2 \equiv r \pmod m$, it follows from $\gcd(r, m) = 1$ that $\gcd(r_1, m) = 1$ and $\gcd(r_2, m) = 1$. Moreover, since $\gcd(r_2, m) = 1$ implies that

$$\frac{m}{\gcd(r_2, m)} = m, \tag{35}$$

the series A_1 has the required form. □

We will say that a formal power series $A \in \Gamma$ is "even" if $A = R(z^2)$ for some $R \in k[[z]]$, and "odd" if $A = zR(z^2)$ for some $R \in k[[z]]$.

Corollary 6.4. *Let $A \in \Gamma$ be an even formal power series, and $A = A_1 \circ A_2$ a decomposition of A into a composition of formal power series $A_1, A_2 \in \Gamma$. Then either A_2 is even, or there exists $\mu \in k_1[[z]]$ such that $A_1 \circ \mu$ is even. On the other hand, if A is odd, then there exists $\mu \in k_1[[z]]$ such that $A_1 \circ \mu$ and $\mu^{-1} \circ A_2$ are odd.*

Proof. If A is even, then $m = 2$ and $r \equiv 0 \pmod 2$. Therefore, the condition $r_1 r_2 \equiv r \pmod m$ implies that either $r_2 \equiv 0 \pmod 2$, in which case A_2 is even, or $r_2 \equiv 1 \pmod 2$ but $r_1 \equiv 0 \pmod 2$, in which case $A_1 \circ \mu$ is even since equality (35) holds. On the other hand, if A is odd, then $m = 2$ and $r \equiv 1 \pmod 2$. Thus, the corollary follows from Corollary 6.3. □

It was shown by Reznick in [25] that if $A \in zk[[z]]$ is a formal power series such that some iterate of A has the form $A^{\circ k} = z^r R(z^m)$ for some $R \in zk[[z]]$ and integers $m \geq 2$, $r \geq 0$, then either A itself has a similar form, or $\operatorname{ord} A = 1$ and $|A|$ is finite. We finish this section by showing that the part of the Reznick result concerning formal power series of order at least two is an immediate corollary of Theorem 6.1.

Theorem 6.5. *Let $A \in \Gamma$ be a formal power series, and m, $2 \leq m \leq n$, an integer. Then some iterate $A^{\circ k}$, $k \geq 1$, has the form $A^{\circ k} = z^r R(z^m)$ for some $R \in k[[z]]$ and integers $m \geq 2$, $r \geq 0$ if and only if $A = z^{r_0} R_0(z^m)$ for some $R_0 \in k[[z]]$ and $r_0 \geq 0$.*

Proof. The "if" part is obvious. To prove the "only if" part we observe that if $A^{\circ k} = z^r R(z^m)$ for some $R \in k[[z]]$ and integers $m \geq 2$, $r \geq 0$, then by the "only if" part of Theorem 6.1 for any Böttcher function $\beta_{A^{\circ k}}$ the equality $\beta_{A^{\circ k}} = zL(z^m)$ holds for some $L \in k_0[[z]]$. Since the uniqueness of the Böttcher function implies that for any Böttcher function β_A the equality $\beta_A = \beta_{A^{\circ k}} \circ \varepsilon z$ holds for some ε satisfying $\varepsilon^{k \operatorname{ord} A} = \varepsilon$, using now the "if" part of Theorem 6.1, we conclude that A has the required form. □

7. Functional equation $X \circ A = Y \circ B$ and reversibility

7.1. **Functional equation $X \circ A = Y \circ B$.** We start this section by proving Theorem 1.3.

Proof of Theorem 1.3. If

$$X \circ A = Y \circ B, \tag{36}$$

has a solution, then setting

$$F = X \circ A = Y \circ B$$

and applying Corollary 4.4, we conclude that the equality

$$\widehat{\varphi}_A \circ \widehat{\varphi}_B = \widehat{\varphi}_B \circ \widehat{\varphi}_A \tag{37}$$

holds.

Assume now that (37) holds. Let us observe that Lemma 3.5 implies that $\widehat{\varphi}_A$ and $\widehat{\varphi}_B$ commute if and only if $\widehat{\varphi}_{A_\mu}$ and $\widehat{\varphi}_{B_\mu}$ commute for some $\mu \in k_1[[z]]$. Similarly, equation (36) has a solution for A and B if and only if it has a solution for A_μ and B_μ. Thus, conjugating A and B by $\mu = \beta_A$, without loss of generality we can assume that $A = z^n$, $n \geq 2$.

Since $\widehat{\varphi}_{z^n} = \varepsilon_n z$, equality (37) implies by Lemma 2.2 that $\widehat{\varphi}_A = zM(z^n)$ for some $M \in k_0[[z]]$. By Theorem 6.2, this yields that B has the form $B = \mu \circ z^r R(z^n)$, where $R \in k[[z]]$, $\mu \in k_1[[z]]$, and $0 \leq r \leq n-1$. Therefore, equality (36) holds for

$$X = z^r R^n(z), \quad Y = z^n \circ \mu^{-1}.$$ □

Using Theorem 1.3, we prove the following result.

Theorem 7.1. *Let $A, B \in \Gamma$ be formal power series. Assume that for every $k, l \geq 1$ there exist formal power series $X, Y \in zk[[z]]$ satisfying*

$$X \circ A^{\circ l} = Y \circ B^{\circ k}. \tag{38}$$

Then $\beta_A = \beta_B \circ cz$ for some $c \in k^*$.

Proof. Let us set $n = \operatorname{ord} A$, $m = \operatorname{ord} B$. By Theorem 1.3, for every $k, l \geq 1$ the equality

$$\widehat{\varphi}_{A^{\circ l}} \circ \widehat{\varphi}_{B^{\circ k}} = \widehat{\varphi}_{B^{\circ k}} \circ \widehat{\varphi}_{A^{\circ l}}$$

holds. Since

$$\widehat{\varphi}_{A^{\circ l}} = \beta_A \circ \varepsilon_{nl} z \circ \beta_A^{-1}, \quad \widehat{\varphi}_{B^{\circ k}} = \beta_B \circ \varepsilon_{mk} z \circ \beta_B^{-1}$$

by Lemma 3.5, this implies that

$$(\beta_B^{-1} \circ \beta_A \circ \varepsilon_{nl} z \circ \beta_A^{-1} \circ \beta_B) \circ \varepsilon_{mk} z = \varepsilon_{mk} z \circ (\beta_B^{-1} \circ \beta_A \circ \varepsilon_{nl} z \circ \beta_A^{-1} \circ \beta_B).$$

Fixing now l and applying Lemma 2.2, we see that for every $k \geq 1$ there exists $R_k \in k[[z]]$ such that

$$\beta_B^{-1} \circ \beta_A \circ \varepsilon_{nl} z \circ \beta_A^{-1} \circ \beta_B = z R_k(z^{mk}).$$

Clearly, this is possible only if

$$\beta_B^{-1} \circ \beta_A \circ \varepsilon_{nl} z \circ \beta_A^{-1} \circ \beta_B = cz,$$

for some $c \in k^*$, and comparing coefficients in the parts of this equality we conclude that

$$\beta_B^{-1} \circ \beta_A \circ \varepsilon_{nl} z \circ \beta_A^{-1} \circ \beta_B = \varepsilon_{nl} z.$$

The last equality implies that $\beta_B^{-1} \circ \beta_A$ commutes with $\varepsilon_{nl} z$. Since this is true for every $l \geq 1$, using again Lemma 2.2, we obtain that for every $l \geq 1$ there exists $M_l \in k_0[[z]]$ such that

$$\beta_B^{-1} \circ \beta_A = z M_l(z^{nl}),$$

implying that $\beta_A = \beta_B \circ cz$ for some $c \in k^*$. □

7.2. **Right reversibility of subsemigroups of Γ.** Let us recall that a semigroup S is called *right amenable* if it admits a finitely additive probability measure μ defined on all the subsets of S such that for all $a \in S$ and $T \subseteq S$ the equality

$$\mu(Ta^{-1}) = \mu(T)$$

holds, where the set Ta^{-1} is defined by the formula

$$Ta^{-1} = \{s \in S \,|\, sa \in T\}.$$

A semigroup S is called *right reversible* if for all $a, b \in S$ the left ideals Sa and Sb have a non-empty intersection, that is, if for all $a, b \in S$ there exist $x, y \in S$ such that $xa = yb$. It is well known and follows easily from the definition (see [23], Proposition 1.23) that every right amenable semigroup is right reversible.

The problems of describing right reversible and right amenable semigroups of polynomials and rational functions have been studied in the recent papers [7], [8], [21]. Some analogues of the results of these papers for finitely generated subsemigroups of Γ were obtained in the paper [22], mentioned in the introduction. The approach of [22] relies on results of [20], for which the assumption that S is finitely generated is essential. Theorem 7.1 provides another approach to the problem, which works equally well for infinitely generated subsemigroups of Γ. Specifically,

Theorem 7.1 implies the following result, which contains Theorem 1.5 from the introduction.

Theorem 7.2. *Every right reversible subsemigroup S of Γ is conjugate to a subsemigroup of $\mathcal{Z}$. In particular, every right amenable subsemigroup S of Γ is conjugate to a subsemigroup of $\mathcal{Z}$.*

Proof. Let us fix an arbitrary element A of S. Then for every $B \in S$ and $k, l \geq 1$, we can apply the right reversibility condition to the elements $A^{\circ l}$ and $B^{\circ k}$ of S concluding that there exists $X, Y \in S$ such that equality (38) holds. Therefore, by Theorem 7.1, for every $B \in S$ the equality $\beta_A = \beta_B \circ cz$ holds for some $c \in k^*$. Let us observe now that for every $B \in S$ and $c \in k^*$ the equality

$$B \circ \beta_B = \beta_B \circ z^m,$$

where $m = \deg B$, implies the equality

$$B \circ \beta_B \circ cz = \beta_B \circ z^m \circ cz = \beta_B \circ cz \circ c^{m-1} z^m.$$

Thus,

$$\beta_A^{-1} \circ B \circ \beta_A = c^{m-1} z^m,$$

and therefore the semigroup $\beta_A^{-1} \circ S \circ \beta_A$ is a subsemigroup of $\mathcal{Z}$. □

References

[1] I. Babenko, S. Bogatyi, *Amenability of the substitution group of formal power series*, Izv. Math. 75 (2011), no. 2, 239-252.

[2] I. Babenko, S. Bogatyi, *Algebra, geometry and topology of the substitution group of formal power series*, Russian Math. Surveys 68 (2013), no. 1, 1-68

[3] A. Beardon, T. W. Ng, *On Ritt's factorization of polynomials*, J. London Math. Soc. (2) 62 (2000), no. 1, 127-138.

[4] A. Beardon, *Even and odd entire functions*, J. Austral. Math. Soc., 74(1) , 19-24, (2003).

[5] L. Böttcher, *Beiträge zur Theorie der Iterationsrechnung* (russian), Bull. Kasan Math. Soc. 14 (1905), 176.

[6] A. Brudnyi, *Subgroups of the group of formal power series with the big powers condition*, C. R. Math. Acad. Sci. Soc. R. Can. 41 (2019), no. 2, 20-31.

[7] Cabrera C., Makienko P., *Amenability and measure of maximal entropy for semigroups of rational map*, Groups Geom. Dyn. 15 (2021), no. 4, 1139-1174.

[8] Cabrera C., Makienko P., *Amenability and measure of maximal entropy for semigroups of rational map: II*, arXiv:2109.11601.

[9] H. Cartan, *Elementary theory of analytic functions of one or several complex variables,* Addison-Wesley Publishing Company, Palo Alto, Reading (MA), London, 1963.

[10] H. Engstrom, *Polynomial substitutions,* Amer. J. Math. 63, 249-255 (1941).

[11] L. Hansen, H. Shapiro, *Graphs and functional equations*, Ann. Acad. Sci. Fenn. Ser. A I Math. 18 (1993), no. 1, 125-146.

[12] A. Horwitz, L. Rubel, *When is the composition of two power series even?* J. Austral. Math. Soc. Ser. A 56 (1994), no. 3, 415-420.

[13] A. Horwitz, *Even compositions of entire functions and related matters*, J. Austral. Math. Soc. Ser. A 63 (1997), no. 2, 225–237.

[14] W. Jabloński, L. Reich, *A new approach to the description of one-parameter groups of formal power series in one indeterminate,* Aequationes Mathematicae, 87 (2014), 247 - 284.

[15] S. A. Jennings, *Substitution groups of formal power series*, Canad. J. Math. 6 (1954), 325-340.

[16] D. L. Johnson, *The group of formal power series under substitution*, J. Austral. Math. Soc. Ser. A 45:3 (1988), 296-302.

[17] H. Kautschitsch, *Über vertauschbare Potenzreihen,* Math. Nachr. 88 (1979), 207-217.

[18] J. Milnor, *Dynamics in one complex variable*, Princeton Annals in Mathematics 160. Princeton, NJ: Princeton University Press (2006).

[19] B. Muckenhoupt, *Automorphisms of formal power series under substitution*, Trans. Amer. Math. Soc. 99:3 (1961), 373-383.
[20] F. Pakovich, *Sharing a measure of maximal entropy in polynomial semigroups, Int. Math. Res. Not.,* doi:10.1093/imrn/rnab076.
[21] F. Pakovich, *On amenable semigroups of rational functions,* Trans. Amer. Math. Soc., to appear.
[22] F. Pakovich, *Right amenability in semigroups of formal power series,* arXiv:2208.04640.
[23] A. Paterson, *Amenability*, Mathematical Surveys and Monographs, 29. American Mathematical Society, Providence, RI, 1988.
[24] L. Reich, *Families of Commuting Formal Power Series, Semicanonical Forms and Iterative Roots,* Annales Mathematicae Silesianae (Katowice), 8 (1994), 189 - 201. [
[25] B. Reznick, *When is the iterate of a formal power series odd?* J. Austral. Math. Soc. Ser. A 28 (1979), no. 1, 62-66.
[26] J. Ritt, *On the iteration of rational functions,* Trans. Amer. Math. Soc. 21 (1920), 348-356.
[27] J. Ritt, *Prime and composite polynomials*, American M. S. Trans. 23, 51-66 (1922).
[28] S. Scheinberg, *Power Series in One Variable,* Journal of Mathematical Analysis and Applications, 31 (1970), 321 - 333.
[29] J. Schwaiger, *Roots of formal power series in one variable,* Aequationes Mathematicae, 29 (1985), 40 - 43.

Department of Mathematics, Ben Gurion University of the Negev, Israel
Email address: pakovich@math.bgu.ac.il