Annales Fennici Mathematici
Volumen 49, 2024, 601–620

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. We prove a number of general results about such equations and provide some applications. 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.

Muodollisten potenssisarjojen funktionaaliyhtälöistä

Tiivistelmä. Olkoon k algebrallisesti suljettu kunta, jonka karakteristika on nolla, ja $k[[z]]$ sen muodollisten potenssisarjojen rengas. Tässä tutkimuksessa tarkastellaan puoliryhmässä $z^2k[[z]]$ asetettuja yhtälöitä, kun puoliryhmälaskutoimituksena on kuvausten yhdistely. Työssä todistetaan näitä yhtälöitä koskevia yleisiä tuloksia ja esitellään joitakin sovelluksia. Erityisesti vastataan Horwitzin ja Rubelin esittämään "parillisten" potenssisarjojen hajotelmia koskevaan kysymykseen. Lisäksi osoitetaan, että jokainen oikealta keskiarvoistuva puoliryhmän $z^2k[[z]]$ alipuoliryhmä on jonkin monomien alipuoliryhmän liittoluokka.

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 $A(z) = \sum_{n\geq 0} c_n z^n$ of $k[[z]]$, we define its *order* by the formula $\operatorname{ord} A = \min\{n \geq 0 \mid c_n \neq 0\}$. We 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 of $k[[z]]$ 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*.

The group $k_1[[z]]$ has been intensively studied (see e.g. [2, 3, 4, 9, 20, 21, 22, 25, 35, 40, 41]). In this paper, we focus on the less studied semigroup Γ with an emphasis on equations in Γ. In other words, we study functional equations in formal powers series of order at least two. An example of such an equation is simply the equation

$$A = A_1 \circ A_2 \circ \cdots \circ A_r, \quad r \geq 2, \tag{1}$$

where $A \in \Gamma$ is a given and $A_1, A_2, \dots, A_r \in \Gamma$ are unknown, describing the ways in which an element A of Γ can be represented as a composition of other elements of Γ. Although the problem of characterizing solutions of (1) is fundamental, we were unable to find relevant references in the literature, and provide an answer in this paper. Specifically, we describe *equivalence classes* of decompositions (1), where two decompositions

$$A = A_1 \circ A_2 \circ \cdots \circ A_k \quad \text{and} \quad A = \widehat{A}_1 \circ \widehat{A}_2 \circ \cdots \circ \widehat{A}_m, \tag{2}$$

https://doi.org/10.54330/afm.149373
2020 Mathematics Subject Classification: Primary 30D05, 39B12.
Key words: Functional equations, formal power series, Böttcher's equation, semigroup amenability.
This research was supported by ISF Grant No. 1092/22.

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

$$A_1 = \widehat{A}_1 \circ \mu_1^{-1}, \quad A_i = \mu_{i-1} \circ \widehat{A}_i \circ \mu_i^{-1}, \quad 1 < i < k, \quad \text{and} \quad A_k = \mu_{k-1} \circ \widehat{A}_k. \tag{3}$$

Let us recall that for every $A \in \Gamma$ of order n 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 Böttcher function is not defined in a unique way; however, if β_A is some Böttcher function, then any other Böttcher function has the form $\beta_A \circ \varepsilon z$, where $\varepsilon^{n-1} = 1$. In this notation, our main result concerning equation (1) is the following.

Theorem 1.1. *Let $A \in \Gamma$ be a formal power series of order n, and β_A some Bötcher function. Then every decomposition*

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

of A into a composition of elements $A_1, A_2, \dots, A_r$ of Γ is equivalent to the decomposition

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

Thus, equivalence classes of decompositions of A are in a one-to-one correspondence with ordered factorizations of n.

The main motivation for writing this paper was to construct in the formal power series setting an analogue of the decomposition theory of *rational functions*. Correspondingly, the definition of the equivalency of decompositions of elements of Γ given above mimics the corresponding definition from the decomposition theory of rational functions, in which two decompositions (2) of a rational function of degree at least two A into compositions of rational functions of degree at least two $A_1, A_2, \dots, A_k$ and $\widehat{A}_1, \widehat{A}_2, \dots, \widehat{A}_m$ are considered as equivalent if (3) holds for some Möbius transformations μ_i, $1 \le i \le k-1$. As expected, the results obtained in this paper differ significantly from the corresponding results for rational functions, generally being simpler. For instance, even for polynomial decompositions, the analogue of Theorem 1.1, obtained by Ritt [38], is substantially more complex. On the other hand, for arbitrary rational functions, such an analogue is not known, and typical results in the area primarily concern either decompositions of specific types of functions or functional equations of a particular form (see e.g. [1, 7, 15, 16, 26, 27, 28, 29, 30, 39]).

The main method in the study of decompositions of rational functions is the monodromy method, which involves examining the monodromy group associated with a given rational function. On the other hand, the primary technical tool in the study of equations in formal power series is the Böttcher functions. Our approach consists in the systematic use along with the Böttcher functions what we call the *transition functions*. By definition, the transitions functions for $A \in \Gamma$ are elements φ_A of $k_1[[z]]$ satisfying

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

For $A \in \Gamma$ of order n there exist exactly n transition functions forming a cyclic group with respect to the operation of composition. We will call this group the *transition group* and denote it by G_A. Although the transition groups are quite simple from a group-theoretic perspective, they turn out to be very convenient for studying equations in Γ since the relative position of these groups within $k_1[[z]]$

reflects the mutual compositional properties of the corresponding elements of Γ. We illustrate this statement with the following two results, which we consider among the main results of the paper.

The first result concerns the functional equation $F = X \circ A$, where F, A are given and X is unknown.

Theorem 1.2. *Let $A \in k_n[[z]]$, $n \geq 2$, and $F \in k_{nm}[[z]]$, $m \geq 1$. Then the equation*

$$F = X \circ A$$

has a solution in $X \in k_m[[z]]$ if and only if $G_A \subseteq G_F$. In particular, for $A, B \in \Gamma$ of the same order the equality $G_A = G_B$ holds if and only if $B = \mu \circ A$ for some $\mu \in k_1[[z]]$

The second result concerns the functional equation $X \circ A = Y \circ B$, where A, B are given and X, Y are unknown.

Theorem 1.3. *Let $A, B \in \Gamma$. Then the equation*

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

has a solution in $X, Y \in zk[[z]]$ if and only if

$$\varphi_A \circ \varphi_B = \varphi_B \circ \varphi_A$$

for all $\varphi_A \in G_A$ and $\varphi_B \in G_B$.

Along with decompositions of general elements of Γ, we study decompositions of elements of a special form. Specifically, we address the following problem posed by Horwitz and Rubel in [19]: 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? Some partial results on this problem and its modifications, concerning decompositions of entire functions or polynomials, were obtained in the papers [6, 5, 19, 18].

In this paper, we provide a complete solution to the problem of Horwitz and Rubel in the case where h and f, g are elements of Γ. In fact, along with *even* formal power series, that is, 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. Specifically, we prove the following result.

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 any decomposition $A = A_1 \circ A_2$, where $A_1, A_2 \in \Gamma$, there exist $\mu \in k_1[[z]]$ and $R_1, R_2 \in k[[z]]$ such that*

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

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 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 $\mu^{-1} \circ A_2$ is odd and $A_1 \circ \mu$ is even. On the other hand, if $A = A_1 \circ A_2$ is odd, then Theorem 1.4 implies that there exists $\mu \in k_1[[z]]$ such that $A_1 \circ \mu$ and $\mu^{-1} \circ A_2$ are both odd (see Corollary 6.5).

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*, meaning that it admits a finitely additive probability measure μ defined on all 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

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

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 [33] that a *finitely* generated subsemigroup of Γ is right amenable if and only if it is conjugate to a subsemigroup of $\mathcal{Z}^U$. However, 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 $\mathcal{Z}$.*

Moreover, we show that the conclusion of Theorem 1.5 holds already under the assumption that S is *right reversible*, which is a weaker condition than the assumption that S is right amenable (see Theorem 7.2). We deduce these results from the following statement of independent interest.

Theorem 1.6. *Let $A, B \in \Gamma$ be formal power series, and β_A, β_B some Bötcher functions. Then the equation*

$$X \circ A^{\circ l} = Y \circ B^{\circ s} \tag{4}$$

has a solution in $X, Y \in zk[[z]]$ for all $s, l \geq 1$ if and only if $\beta_A = \beta_B \circ cz$ for some $c \in k^*$.

Notice that Theorem 1.6 includes the characterization of commuting elements of Γ in terms of their Böttcher functions, as obtained by Dorfer and Woracek [13]. Specifically, it implies that $A, B \in \Gamma$ commute if and only if $\beta_A = \beta_B \circ \varepsilon z$ for some ε satisfying

$$\varepsilon^{(\operatorname{ord} A - 1)(\operatorname{ord} B - 1)} = 1$$

(see Corollary 7.1).

This paper is organized as follows. In the second section, after recalling several elementary facts about the semigroup $k[[z]]$ 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 decompositions of elements of Γ, and 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 [36] 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, and prove Theorem 1.3 and Theorem 1.6. Finally, we establish the aforementioned necessary condition for the right amenability and the right reversibility of subsemigroups of Γ.

2. Böttcher functions

2.1. Lemmata about formal power series. In this paper, k always denotes an algebraically closed field of characteristic zero. Notice that the number of nth roots of unity in such k equals n for every $n \geq 1$. We will denote by U_n the group of nth roots of unity in k, and by U_n^P the subset of U_n consisting of primitive nth roots of unity.

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 [12]. 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 $\mu_1 = \varepsilon\mu_2$ for some $\varepsilon \in U_n$.

Proof. Since

$$\mu_1^n - \mu_2^n = \prod_{\varepsilon \in U_n} (\mu_1 - \varepsilon\mu_2),$$

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*

$$\mu \circ az = bz \circ \mu. \tag{5}$$

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

$$\mu \circ \varepsilon z = \varepsilon^r z \circ \mu \tag{6}$$

for some $\varepsilon \in U_n^P$ 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 (5) and (6). □

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

$$z^n \circ \mu = \mu \circ z^n, \quad n \geq 2, \tag{7}$$

if and only if $\mu = \varepsilon z^m$ for some $\varepsilon \in U_{n-1}$ and $m \geq 0$.

Proof. Setting $m = \operatorname{ord} \mu$ and substituting $\mu = \sum_{i=m}^{\infty} c_i z^i$ into (7) 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*

$$z^n \circ \mu_1 = \mu_2 \circ z^n, \quad n \geq 2, \tag{8}$$

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

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

Proof. The identity

$$z^n \circ z^r R(z^n) = z^r R^n(z) \circ z^n \tag{9}$$

is checked by a direct calculation. To prove the "only if" part, we observe that for any $\varepsilon_n \in U_n^P$ equality (8) implies the equality

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

Therefore, by Lemma 2.1, there exists 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 (8) 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 (8) 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 power series $\beta_A \in k_1[[z]]$ such that the equality

$$A \circ \beta_A = \beta_A \circ z^n \tag{10}$$

holds. It is well known that such a function exists and is defined in a unique way up to the change $\beta_A \to \beta_A \circ \varepsilon z$, where $\varepsilon \in U_{n-1}$. In the context of complex dynamics, this fact is widely used and goes back to Böttcher (see [8], [37], [24]). For the proof in the algebraic setting, see [23, Hilffsatz 4]. Notice that the map

$$A \to \beta_X^{-1} \circ A \circ \beta_X, \tag{11}$$

where X is a fixed element of Γ, is a semigroup automorphism of Γ.

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*

$$A_1 \circ X = A_2 \circ X \tag{12}$$

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 (12) 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

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

Since (11) is an isomorphism, this implies in turn that $A_1 = A_2$. □

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 (10). 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 solutions of the equation*

$$A \circ X = Y \circ z^n \tag{13}$$

in $X, Y \in zk[[z]]$ are given by the formulas

$$X = \beta_A \circ z^r R(z^n), \quad Y = \beta_A \circ z^r R^n(z), \tag{14}$$

where $R \in k[[z]]$ and $0 \le r \le n-1$. Furthermore, if $X = Y$, then solutions of (13) *are given by the formula*

$$X = \beta_A \circ \varepsilon z^l, \quad \varepsilon \in U_{n-1},$$

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

Proof. The fact that X and Y defined by (14) satisfy (13) follows from equalities (9) and (10). On the other hand, if (13) holds, then taking an arbitrary Böttcher function β_A and substituting $\beta_A \circ z^n \circ \beta_A^{-1}$ for A in (13), 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 (14) hold by Lemma 2.4.

Furthermore, if $X = Y$, then (14) 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 $\varepsilon \in U_{n-1}$ and $m \ge 0$. Therefore,

$$X = z^r R(z^n) = \varepsilon z^l,$$

where

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

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 solutions of the equation*

$$A \circ X = Y \circ B \tag{15}$$

in $X, Y \in zk[[z]]$ *are given by the formulas*

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

where $R \in k[[z]]$ *and* $0 \leq r \leq n-1$. *Furthermore, if* $X = Y$, *then solutions of* (15) *are given by the formula*

$$X = \beta_A \circ \varepsilon z^l \circ \beta_B^{-1}, \quad \varepsilon \in U_{n-1},$$

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

Proof. For an arbitrary Böttcher function β_B, equality (15) is equivalent to the equality

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

Thus, the theorem follows from Theorem 2.6. □

3. Transition functions

Let $A \in \Gamma$ be a formal power series of order n. We recall that we defined transition functions for A as formal series φ_A satisfying

$$A \circ \varphi_A = A. \tag{16}$$

It is clear that such series necessarily belong to $k_1[[z]]$ and form a group, which we denote by G_A.

The following two lemmas are modifications of the results of Section 2 in [17] characterizing solutions of (16) in the analytical setting.

Lemma 3.1. *Let* $A \in \Gamma$ *be a formal power series, and* β_A *some Böttcher function. Then*

$$G_A = \{\beta_A \circ \varepsilon z \circ \beta_A^{-1} \mid \varepsilon \in U_n\}. \tag{17}$$

Proof. It follows from equality (10) that for every $\varepsilon \in U_n$ we have

$$A \circ \beta_A = A \circ \beta_A \circ \varepsilon z,$$

implying that

$$A = A \circ (\beta_A \circ \varepsilon z \circ \beta_A^{-1}).$$

On the other hand, if equality (16) 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 $\beta_A^{-1} \circ \varphi_A \circ \beta_A = \varepsilon z$ for some $\varepsilon \in U_n$. □

For a formal power series $\varphi \in k_1[[z]]$, we denote by $|\varphi|$ the order of φ in the group $k_1[[z]]$. Thus, $|\varphi|$ equals the minimum number d such that $\varphi^{\circ d} = z$, if such a number exists, and $|\varphi|$ equals ∞, if $\varphi^{\circ d}$ is distinct from z for every $d \geq 1$.

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

Proof. Since the functions defined by (17) satisfy $\varphi_A^{\circ n} = z$, 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 lemma follows immediately from Lemma 3.1.

Lemma 3.3. *Let $A \in \Gamma$. Then G_A is a cyclic group of order n, whose generators are $\beta_A \circ \varepsilon_n z \circ \beta_A^{-1}$, where $\varepsilon_n \in U_n^P$.* □

The following lemma relates the transition group for $A \in \Gamma$ with the transition groups for $A^{\circ l}$, $l \geq 1$, and

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

Lemma 3.4. *Let $A \in \Gamma$ be a formal power series of order n, and β_A some Böttcher function. Then*

$$G_{A^{\circ l}} = \{\beta_A \circ \varepsilon z \circ \beta_A^{-1} \mid \varepsilon \in U_{nl}\}, \quad l \geq 1, \tag{18}$$

and

$$G_{A_\mu} = \mu^{-1} \circ G_A \circ \mu, \quad \mu \in k_1[[z]]. \tag{19}$$

Proof. Equality (18) follows from Lemma 3.1 and the fact that β_A remains a Böttcher function for $A^{\circ l}$, $l \geq 1$. On the other hand, since $\operatorname{ord} A = \operatorname{ord} A_\mu = n$, equality (19) follows from the equality

$$A_\mu \circ (\mu^{-1} \circ \varphi_A \circ \mu) = A_\mu, \quad \varphi_A \in G_A,$$

which is obtained by a direct calculation. □

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

Theorem 3.5. *Let $A \in \Gamma$ and $X_1, X_2 \in zk[[z]]$. Then the equality*

$$A \circ X_1 = A \circ X_2 \tag{20}$$

holds if and only if

$$X_2 = \varphi_A \circ X_1$$

for some $\varphi_A \in G_A$.

Proof. The "if" part is obvious. On the other hand if equality (20) 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

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

for some $\varepsilon \in U_n$ by Lemma 2.1. Therefore,

$$X_2 = \beta_A \circ \varepsilon z \circ \beta_A^{-1} \circ X_1 = \varphi_A \circ X_1$$

by Lemma 3.1. □

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*

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

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

$$z^m \circ \beta_F^{-1} \circ \beta_A = z^r R(z^n). \tag{22}$$

Furthermore, if (22) *holds, then* (21) *has a unique solution* X *given by the formula*

$$X = \beta_F \circ z^r R^n(z) \circ \beta_A^{-1}. \tag{23}$$

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 (21), 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

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

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

In the other direction, (22) implies that

$$\begin{aligned} F &= \beta_F \circ z^{nm} \circ \beta_F^{-1} = \beta_F \circ z^n \circ z^m \circ \beta_F^{-1} = \beta_F \circ z^n \circ z^r R(z^n) \circ \beta_A^{-1} \\ &= \beta_F \circ z^r R^n(z) \circ z^n \circ \beta_A^{-1} = \beta_F \circ z^r R^n(z) \circ \beta_A^{-1} \circ A. \end{aligned}$$

Thus, (21) holds for X given by (23). Finally, the function X is defined by formula (23) in a unique way by Theorem 2.5. □

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

$$F = A \circ X \tag{24}$$

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

$$\beta_A^{-1} \circ \beta_F \circ z^m = z^r L^n(z). \tag{25}$$

Furthermore, if (25) *holds, then* (24) *has* n *solutions given by the formula*

$$X = \beta_A \circ \varepsilon z \circ z^r L(z^n) \circ \beta_F^{-1}, \quad \varepsilon \in U_n.$$

Proof. Equality (24) 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

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

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

In the other direction, (25) implies that

$$\begin{aligned} F &= \beta_F \circ z^{nm} \circ \beta_F^{-1} = \beta_F \circ z^m \circ z^n \circ \beta_F^{-1} = \beta_A \circ z^r L^n(z) \circ z^n \circ \beta_F^{-1} \\ &= \beta_A \circ z^n \circ z^r L(z^n) \circ \beta_F^{-1} = A \circ \beta_A \circ z^r L(z^n) \circ \beta_F^{-1}. \end{aligned}$$

Thus, (24) holds for

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

Finally, by Theorem 3.5 and Lemma 3.1, any other solution of (23) has the form

$$\begin{aligned} X &= \varphi_A \circ \beta_A \circ z^r L(z^n) \circ \beta_F^{-1} = \beta_A \circ \varepsilon z \circ \beta_A^{-1} \circ \beta_A \circ z^r L(z^n) \circ \beta_F^{-1} \\ &= \beta_A \circ \varepsilon z \circ z^r L(z^n) \circ \beta_F^{-1}, \quad \varepsilon \in U_n. \end{aligned}$$

□

Proof of Theorem 1.2. If $F = X \circ A$, then for any $\varphi_A \in G_A$ we have

$$F \circ \varphi_A = X \circ A \circ \varphi_A = X \circ A = F,$$

implying that $G_A \subseteq G_F$.

In the other direction, the equality $F \circ \widehat{\varphi}_A = F$ for some generator $\widehat{\varphi}_A$ of G_A implies that

$$\beta_F \circ z^{nm} \circ \beta_F^{-1} \circ \beta_A \circ \varepsilon_n z \circ \beta_A^{-1} = \beta_F \circ z^{nm} \circ \beta_F^{-1} \tag{26}$$

for some Böttcher functions β_A, β_F and $\varepsilon_n \in U_n^P$. It is clear that equality (26) implies the equalities

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

and

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

In turn, the last equality implies 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 (22) holds. Therefore, the equality $F = X \circ A$ holds for some $X \in k_m[[z]]$ by Theorem 4.1. □

For brevity, we will say that $A \in \Gamma$ is a *compositional right factor* of $F \in \Gamma$ if there exists $X \in zk[[z]]$ such that $F = X \circ A$. Compositional left factors are defined similarly.

Corollary 4.3. *Let $F \in \Gamma$ be a formal power series, and $A, B \in \Gamma$ some compositional right factors of F. Then any $\varphi_A \in G_A$ and $\varphi_B \in G_B$ commute.*

Proof. By Theorem 1.2, any $\varphi_A \in G_A$ and $\varphi_B \in G_B$ are elements of the commutative group G_F. □

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

Corollary 4.4. *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 system*

$$A = \widetilde{A} \circ W, \quad B = \widetilde{B} \circ W, \tag{27}$$

has a solution in $\widetilde{A} \in k_{n/d}[[z]]$, $\widetilde{B} \in k_{m/d}[[z]]$, and $W \in k_d[[z]]$ if and only if the intersection of the groups G_A and G_B contains a group of order d.

Proof. Assume that (27) holds and let $\widehat{\varphi}_W$ be a generator of G_W. Then by the "only if" part of Theorem 1.2

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

for some generator $\widehat{\varphi}_A$ of G_A and some generator $\widehat{\varphi}_B$ of G_B. Thus, $G_A \cap G_B$ contains a cyclic group of order d generated by $\widehat{\varphi}_W$.

In the other direction, if $G_A \cap G_B$ contains a group of order d, and φ is its generator, then

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

for some generator $\widehat{\varphi}_A$ of G_A and some generator $\widehat{\varphi}_B$ of G_B. On the other hand, since $|\varphi| = d$, it follows from Lemma 3.2 that $\varphi = \widehat{\varphi}_W$ for some $W \in k_d[[z]]$. Using now the "if" part of Theorem 1.2, we conclude that (27) 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 4.5. *Let $A, C, D \in \Gamma$ be formal power series. Then the equation*

$$A \circ C = X \circ D \tag{28}$$

has a solution in $X \in k[[z]]$ if and only if for any $\varphi_D \in G_D$ there exists $\varphi_A \in G_A$ such that

$$C \circ \varphi_D = \varphi_A \circ C. \tag{29}$$

Proof. If for any $\varphi_D \in G_D$ equality (29) holds for some $\varphi_A \in G_A$, then for any $\varphi_D \in G_D$ we have

$$A \circ C \circ \varphi_D = A \circ \varphi_A \circ C = A \circ C.$$

Therefore, $G_D \subseteq G_{A \circ C}$ and hence (28) has a solution by Theorem 1.2.

In the other direction, equality (28) implies that

$$A \circ C = A \circ C \circ \varphi_D.$$

Thus, (29) holds by Theorem 3.5. □

5. Equivalency classes of decompositions of formal power series

In this section, we prove Theorem 1.1 and deduce from it a corollary, which can be considered as an analogue of the result of Engstrom [14] about polynomial solutions of the equation $A \circ C = B \circ D$.

Proof of Theorem 1.1. Let

$$A = A_1 \circ A_2 \circ \cdots \circ A_r \tag{30}$$

be a decomposition of $A \in \Gamma$ with

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

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 for $A = z^n$ every decomposition (30) is equivalent to the decomposition

$$z^n = z^{n_1} \circ z^{n_2} \circ \cdots \circ z^{n_r}. \tag{31}$$

We prove the last statement by induction on r.

Clearly, $G_{z^n} = \{\varepsilon z \mid \varepsilon \in U_n\}$. Since $|G_{A_r}| = n_r$ and G_{A_r} is a subgroup of G_{z^n} by Theorem 1.2, this implies that $G_{A_r} = \{\varepsilon z \mid \varepsilon \in U_{n_r}\}$. Thus, $G_{A_r} = G_{z^{n_r}}$, implying by Theorem 1.2 that

$$A_r = \mu_{r-1} \circ z^{n_r} \tag{32}$$

for some $\mu_{r-1} \in k_1[[z]]$. Hence, 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 (32) and

$$z^{n_1 n_2 \ldots n_{r-1}} = A_1 \circ A_2 \ldots (A_{r-1} \circ \mu_{r-1}). \tag{33}$$

By the induction assumption, the decomposition in the right part of (33) is equivalent to the decomposition $z^{n_1} \circ z^{n_2} \circ \cdots \circ z^{n_{r-1}}$, and in virtue of (32) this implies that for $A = z^n$ every decomposition (30) is equivalent to decomposition (31). □

Corollary 5.1. *Assume that* $A, B, C, D \in \Gamma$ *satisfy*

$$A \circ C = B \circ D.$$

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

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

Proof. Let us set

$$\begin{aligned} &F = A \circ C = B \circ D, \\ &n = \operatorname{ord} F, \quad a = \operatorname{ord} A, \quad b = \operatorname{ord} B, \quad c = \operatorname{ord} C, \quad d = \operatorname{ord} D, \\ &u = \gcd(a, b), \quad v = \gcd(c, d). \end{aligned}$$

Taking a Bötcher function β_F and applying Theorem 1.1, we see that there exist $\nu, \mu \in k_1[[z]]$ such that

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

and

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

Therefore, the statement of the corollary is true for

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

and

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

6. Formal power series with symmetries

6.1. Characterizations of formal powers series with symmetries. The following result characterizes elements of Γ 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* $A \in \Gamma$. *Then* A *has the form* $A = z^r R(z^m)$ *for some* $R \in k[[z]]$ *and integers* $m \geq 2$, $r \geq 0$ *if and only if any Bötcher function* β_A *has the form* $\beta_A = zL(z^m)$ *for some* $L \in k_0[[z]]$.

Proof. Assume that for some Bötcher function β_A the equality $\beta_A = zL(z^m)$ holds. Then β_A commutes with $\varepsilon_m z$ for any $\varepsilon_m \in U_m^P$, whence

$$\begin{aligned} (A \circ \varepsilon_m z) \circ \beta_A = A \circ \beta_A \circ \varepsilon_m z = \beta_A \circ z^n \circ \varepsilon_m z = \beta_A \circ \varepsilon_m^n z \circ z^n \\ = \varepsilon_m^n z \circ \beta_A \circ z^n = (\varepsilon_m^n z \circ A) \circ \beta_A. \end{aligned}$$

Therefore,

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

implying by Lemma 2.2 that $A = z^r R(z^m)$.

In the other direction, let us assume that $A = z^r R(z^m)$ and set $\widehat{A} = z^r R^m(z)$. Since

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

for any Bötcher function β_A we have

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

where $n = \operatorname{ord} A$, implying by Theorem 2.6 that

$$z^m \circ \beta_A = \beta_{\widehat{A}} \circ \varepsilon z^m = (\beta_{\widehat{A}} \circ \varepsilon z) \circ z^m$$

for some Bötcher function $\widehat{\beta}_A$ and $\varepsilon \in U_{n-1}$. 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 $L \in k_0[[z]]$. □

Notice that if some Bötcher function has the form $\beta_A = zL(z^m)$, then all Bötcher functions have such a form.

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

Theorem 6.2. *Let $A \in \Gamma$. Then A has the form $A = \mu \circ z^r R(z^m)$ for some $\mu \in k_1[[z]]$, $R \in k[[z]]$, and integers $m \geq 2$, $r \geq 0$ if and only if any transition function φ_A has the form $\varphi_A = zM(z^m)$ for some $M \in k_0[[z]]$.*

Proof. Let us fix $\varepsilon_m \in U_m^P$. If some $\varphi_A \in G_A$ has the form $\varphi_A = zM(z^m)$, then φ_A commutes with $\varepsilon_m z$, implying that

$$A \circ \varepsilon_m z = A \circ \varphi_A \circ \varepsilon_m z = (A \circ \varepsilon_m z) \circ \varphi_A.$$

Thus, φ_A belongs to $G_{A \circ \varepsilon_m z}$. Therefore, if any $\varphi_A \in G_A$ has the above form, then $G_A = G_{A \circ \varepsilon_m z}$, implying by Theorem 1.2 that

$$A \circ \varepsilon_m z = \nu \circ A \tag{34}$$

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

Since (34) 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 (34) we conclude that $A = R(z^m)$ for some $R \in k[[z]]$. On the other hand, if $d > 1$, then $\nu = \varphi_F$ for some $F \in k_d[[z]]$ by Lemma 3.2, and hence

$$\nu = \beta_F \circ \varepsilon z \circ \beta_F^{-1}$$

for some Bötcher function β_F and $\varepsilon \in U_d$ by Lemma 3.1. Moreover, since d divides m, the equalities $\varepsilon = \varepsilon_m^r$ and

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

hold for some r, $0 \leq r \leq m-1$. Substituting the right part of the last equality for ν in (34), we see that

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

Hence, by Lemma 2.2,

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

for some $R \in k[[z]]$. Thus, the equality $A = \mu \circ z^r R(z^m)$ holds for $\mu = \beta_F$.

In the other direction, if $A = \mu \circ z^r R(z^m)$, then applying Corollary 4.3 to the function

$$F = \widehat{A} \circ z^m = z^m \circ \mu^{-1} \circ A,$$

where $\widehat{A} = z^r R^m(z)$, we conclude that any $\varphi_A \in G_A$ commutes with $\varphi_{z^m} = \varepsilon_m z$. Therefore, any φ_A has the form $\varphi_A = zM(z^m)$ by Lemma 2.2. □

Corollary 6.3. *Let $A \in \Gamma$. Then A has a compositional right factor $C \in \Gamma$ of the form $C = z^r R(z^m)$ for some $R \in k[[z]]$ and integers $m \geq 2$, $r \geq 0$ if and only if some transition function $\varphi_A \neq z$ has the form $\varphi_A = zM(z^m)$ for some $M \in k_0[[z]]$.*

Proof. If A has such a factor, then by Theorem 1.2 the group G_A contains the non-trivial group G_C as a subgroup. Moreover, all elements of the last group have the form $zM(z^m)$ by Theorem 6.2.

In the other direction, let us assume that some transition function $\varphi_A \neq z$ has the form $\varphi_A = zM(z^m)$ and set $d = |\varphi_A|$. By Lemma 3.2, $\varphi_A = \varphi_C$ for some $C \in \Gamma$ of order d, and it is clear that $G_C = \langle \varphi_A \rangle$. Thus, $A = B \circ C$ for some $B \in zk[[z]]$ by Theorem 1.2. Moreover, since any iterate of a series of the form $zM(z^m)$ also has such form, it follows from $G_C = \langle \varphi_A \rangle$ by Theorem 6.2 that C has the form $\mu \circ z^r R(z^m)$ for some $\mu \in k_1[[z]]$. Finally, changing B to $B \circ \mu$, we may assume that $C = z^r R(z^m)$. □

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 us fix $\varepsilon_m \in U_m^P$. Let

$$A = A_1 \circ A_2, \tag{35}$$

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 4.3, we see that any $\varphi_{A_2} \in G_{A_2}$ commutes with the transition function $\varphi_{z^m} = \varepsilon_m z$. Thus, any $\varphi_{A_2} \in G_{A_2}$ has the form $zM(z^m)$ for some $M \in k_0[[z]]$ by Lemma 2.2, and hence

$$A_2 = \mu \circ z^{r_2} R_2(z^m) \tag{36}$$

for some $\mu \in k_1[[z]]$, $R_2 \in k[[z]]$, 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

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

implying that

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

and

$$A_1 \circ \mu \circ \varepsilon_m^{r_2} z = \varepsilon_m^r z \circ A_1 \circ \mu.$$

Since $\varepsilon_m^{r_2}$ is a primitive $\frac{m}{\gcd(r_2,m)}$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,

$$A_1 = z^{r_1} R_1(z^{\frac{m}{\gcd(r_2,m)}}) \circ \mu^{-1}. \tag{37}$$

Finally, it follows from (35) and (36), (37) that $r_1 r_2 \equiv r \pmod{m}$. □

Notice that in general the series A_1 in a decomposition $A = A_1 \circ A_2$ of a symmetric series A is "less symmetric" than A. Moreover, if $r_2 = 0$, then A_1 may be not symmetric at all. Nevertheless, the following statement is true.

Corollary 6.4. *Let $A \in \Gamma$ be a formal power series of the form $A = z^r R(z^m)$, where $R \in k[[z]]$ and $m \geq 2$, $r \geq 1$ are integers such that $\gcd(r, m) = 1$. Then for any decomposition $A = A_1 \circ A_2$, where $A_1, A_2 \in \Gamma$, there exist $R_1, R_2 \in k[[z]]$ and $\mu \in k_1[[z]]$ 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 (36), (37) 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

$$\frac{m}{\gcd(r_2, m)} = m, \tag{38}$$

the series A_1 has the required form. □

Corollary 6.5. *Let $A \in \Gamma$ be an even formal power series. Then for any decomposition $A = A_1 \circ A_2$, where $A_1, A_2 \in \Gamma$, either A_2 is even, or there exists $\mu \in k_1[[z]]$ such that $\mu^{-1} \circ A_2$ is odd and $A_1 \circ \mu$ 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 $\mu^{-1} \circ A_2$ is odd and $A_1 \circ \mu$ is even by (38). On the other hand, if A is odd, then $m = 2$ and $r \equiv 1 \pmod 2$. Thus, the corollary follows from Corollary 6.4. □

It was shown by Reznick in [36] that if $A \in zk[[z]]$ is a formal power series such that some iterate of A has the form $A^{\circ s} = z^r R(z^m)$ 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 6.6. *Let $A \in \Gamma$. Then some iterate $A^{\circ s}$, $s \geq 1$, has the form $A^{\circ s} = z^r R(z^m)$ 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 integer $r_0 \geq 0$.*

Proof. The "if" part is obvious. To prove the "only if" part we observe that if β_A is some Böttcher function for A, then β_A remains a Böttcher function for $A^{\circ s}$, $s \geq 1$. Thus, if $A^{\circ s} = z^r R(z^m)$ for some $s \geq 1$, the "only if" part of Theorem 6.1 implies that $\beta_A = zL(z^m)$ for some $L \in k_0[[z]]$. Using now the "if" part, we conclude that A has the required form. □

Let us mention that for every $m \geq 2$ there exist series $A \in \Gamma$ that do not have the form $\mu \circ z^r R(z^m)$ for some $\mu \in k_1[[z]]$ but have compositional right factors of this form. Indeed, arguing as in the proof of Theorem 1.4, one can easily see that a composition of series $A = A_1 \circ z^{r_2} R_2(z^m)$ with $\gcd(r_2, m) = 1$ has the form $\mu \circ z^r R(z^m)$ for some $\mu \in k_1[[z]]$ if and only if A_1 has the form $\mu \circ z^{r_1} R_1(z^m)$. Thus, if A_1 does not have such a form, the same is true for A.

Notice that for series A as above some transition functions have the form $zM(z^m)$ and some do not. Indeed, all functions φ_A cannot have the form $zM(z^m)$ by Theorem 6.2, but some of them have this form by Corollary 6.3. Since G_A is a cyclic group, this gives us examples of series of order one for which Theorem 6.6 is not true.

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 and Theorem 1.6.

Proof of Theorem 1.3. If

$$X \circ A = Y \circ B, \tag{39}$$

has a solution, then setting

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

and applying Corollary 4.3, we see that

$$\varphi_A \circ \varphi_B = \varphi_B \circ \varphi_A \tag{40}$$

for all $\varphi_A \in G_A$ and $\varphi_B \in G_B$.

To prove the "if" part, let us observe that Lemma 3.4 implies that condition (40) is equivalent to the condition that

$$\varphi_{A_\mu} \circ \varphi_{B_\mu} = \varphi_{B_\mu} \circ \varphi_{A_\mu}$$

for all $\varphi_{A_\mu} \in G_{A_\mu}$ and $\varphi_{B_\mu} \in G_{B_\mu}$ for some $\mu \in k_1[[z]]$. Similarly, equation (39) has a solution for A and B if and only if it has a solution for A_μ and B_μ for some $\mu \in k_1[[z]]$. Thus, conjugating A and B by $\mu = \beta_A$, without loss of generality we can assume that $A = z^n$, $n \geq 2$.

Applying Lemma 2.2 to equality (40) for $\varphi_A = \varphi_{z^n} = \varepsilon_n z$, where $\varepsilon_n \in U_n^P$, we see that any $\varphi_B \in G_B$ has the form $\varphi_B = zM(z^n)$ for some $M \in k_0[[z]]$. By Theorem 6.2, this yields that B has the form $B = \mu \circ z^r R(z^n)$ for some $\mu \in k_1[[z]]$, $R \in k[[z]]$, and $r \geq 0$. Therefore, equality (39) holds for

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

Proof of Theorem 1.6. Let us set $n = \operatorname{ord} A$, $m = \operatorname{ord} B$. If (4) has a solution in $X, Y \in zk[[z]]$ for all $s, l \geq 1$, then by Theorem 1.3 the transition functions

$$\varphi_{A^{\circ l}} = \beta_A \circ \varepsilon_{nl} z \circ \beta_A^{-1}, \quad \varphi_{B^{\circ s}} = \beta_B \circ \varepsilon_{ms} z \circ \beta_B^{-1}, \quad s, l \geq 1, \tag{41}$$

where $\varepsilon_{nl} \in U_{nl}^P$ and $\varepsilon_{ms} \in U_{ms}^P$, commute, implying that

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

Fixing now l and ε_{nl} and applying Lemma 2.2, we see that for every $s \geq 1$ there exists $R_s \in k[[z]]$ such that

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

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 $l\geq 1$ and $\varepsilon_{nl}\in U_{nl}^P$, using again Lemma 2.2, we conclude that for every $l\geq 1$ there exists $M_l\in k_0[[z]]$ such that

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

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

In the other direction, it is easy to see that if $\beta_A=\beta_B\circ cz$ for some $c\in k^*$, then for all $s,l\geq 1$ transition functions (41) commute, implying by Theorem 1.3 that (4) has a solution. □

Theorem 1.6 implies the following result, obtained by Dorfer and Woracek (see [13, Proposition 3.11]).

Corollary 7.1. *Let $A,B\in\Gamma$ be formal power series, and β_A, β_B some Bötcher functions. Then A and B commute if and only if $\beta_A=\beta_B\circ\varepsilon z$ for some ε satisfying*

$$\varepsilon^{(\operatorname{ord}A-1)(\operatorname{ord}B-1)}=1.$$

Proof. Let us set $n=\operatorname{ord}A$, $m=\operatorname{ord}B$. If A and B commute, then for all $s,l\geq 1$ the iterates $A^{\circ l}$ and $B^{\circ s}$ also commute, implying that (4) has the solution $X=B^{\circ s}$, $Y=A^{\circ l}$. Thus, $\beta_A=\beta_B\circ cz$ for some $c\in k^*$ by Theorem 1.6. Furthermore, since

$$A=\beta_B\circ cz\circ z^n\circ c^{-1}z\circ\beta_B^{-1},\quad B=\beta_B\circ z^m\circ\beta_B^{-1}, \tag{42}$$

it follows from the commutativity of A and B that

$$c^{-(n-1)}=c^{-(n-1)m}.$$

On the other hand, if $\beta_A=\beta_B\circ cz$ for some c satisfying $c^{(n-1)(m-1)}=1$, then (42) implies that A and B commute. □

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

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

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 [34], 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 [10, 11, 32]. Some analogues of the results of these papers for finitely generated subsemigroups of Γ were obtained in the paper [33], mentioned in the introduction. The approach of [33] relies on the results of [31], for which the assumption that S is finitely generated is essential. Theorem 1.6 provides another approach to the problem, which works equally well for infinitely generated subsemigroups of Γ. Specifically, Theorem 1.6 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 all $s, l \geq 1$, we can apply the right reversibility condition to the elements $A^{\circ l}$ and $B^{\circ s}$ of S concluding that there exist $X, Y \in S$ such that equality (4) holds. Therefore, by Theorem 1.6, for every $B \in S$ the equality $\beta_A = \beta_B \circ cz$ holds for some $c \in k^*$, implying that

$$\begin{aligned}\beta_A^{-1} \circ B \circ \beta_A = (\beta_B \circ cz)^{-1} \circ B \circ (\beta_B \circ cz) = c^{-1}z \circ \beta_B^{-1} \circ (B \circ \beta_B) \circ cz \\ = c^{-1}z \circ \beta_B^{-1} \circ (\beta_B \circ z^m) \circ cz = c^{m-1}z^m,\end{aligned}$$

where $m = \operatorname{ord} B$. Thus, the semigroup $\beta_A^{-1} \circ S \circ \beta_A$ is a subsemigroup of $\mathcal{Z}$. □

References

[1] Avanzi, R., and U. Zannier: The equation $f(X) = f(Y)$ in rational functions $X = X(t)$, $Y = Y(t)$. - Compos. Math. 139:3, 2003, 263–295.

[2] Babenko, I., and S. Bogatyi: Amenability of the substitution group of formal power series. - Izv. Math. 75:2, 2011, 239–252.

[3] Babenko, I., and S. Bogatyi: Algebra, geometry and topology of the substitution group of formal power series. - Russian Math. Surveys 68:1, 2013, 1–68

[4] Baker, I.: Permutable power series and regular iteration. - J. Aust. Math. Soc. 2, 1961-62, 265–294.

[5] Beardon, A.: Even and odd entire functions. - J. Aust. Math. Soc. 74:1, 2003, 19–24.

[6] Beardon, A., and T. W. Ng: On Ritt's factorization of polynomials. - J. London Math. Soc. (2) 62:1, 2000, 127–138.

[7] Bogatyrev, A.: Rational functions admitting double decompositions. - Trans. Moscow Math. Soc. 2012, 2012, 161–165.

[8] Böttcher, L.: Beiträge zur Theorie der Iterationsrechnung. - Bull. Kasan Math. Soc. 14, 1905, 176 (in Russian).

[9] Brudnyi, A.: Subgroups of the group of formal power series with the big powers condition. - C. R. Math. Acad. Sci. Soc. R. Can. 41:2, 2019, 20–31.

[10] Cabrera, C., and P. Makienko: Amenability and measure of maximal entropy for semigroups of rational maps. - Groups Geom. Dyn. 15:4, 2021, 1139–1174.

[11] Cabrera, C., and P. Makienko: On amenability and measure of maximal entropy for semigroups of rational maps: II. - Internat. J. Algebra Comput. 33:6, 2023, 1099–1125.

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

[13] Dorfer, G., and H. Woracek: Formal power series and some theorems of J. F. Ritt in arbitrary characteristic. - Monatsh. Math. 127, 1999, 277–293.

[14] Engstrom, H.: Polynomial substitutions. - Amer. J. Math. 63, 1941, 249–255.

[15] Eremenko, A.: Some functional equations connected with the iteration of rational functions. - Leningrad Math. J. 1, 1990, 905–919.

[16] Fuchs, C., and U. Zannier: Composite rational functions expressible with few terms. - J. Eur. Math. Soc. (JEMS) 14:1, 2012, 175–208.

[17] Hansen, L., and H. Shapiro: Graphs and functional equations. - Ann. Acad. Sci. Fenn. Ser. A I Math. 18:1, 1993, 125–146.

[18] Horwitz, A.: Even compositions of entire functions and related matters. - J. Aust. Math. Soc. Ser. A 63:2, 1997, 225–237.

[19] Horwitz, A., and L. Rubel: When is the composition of two power series even? - J. Aust. Math. Soc. Ser. A 56:3, 1994, 415–420.

[20] Jabłoński, W., and L. Reich: A new approach to the description of one-parameter groups of formal power series in one indeterminate. - Aequationes Math. 87, 2014, 247–284.

[21] Jennings, S. A.: Substitution groups of formal power series. - Canad. J. Math. 6, 1954, 325–340.

[22] Johnson, D. L.: The group of formal power series under substitution. - J. Aust. Math. Soc. Ser. A 45:3, 1988, 296–302.

[23] Kautschitsch, H.: Über vertauschbare Potenzreihen. - Math. Nachr. 88, 1979, 207–217.

[24] Milnor, J.: Dynamics in one complex variable. - Ann. of Math. Stud. 160, Princeton Univ. Press, Princeton, NJ, 2006.

[25] Muckenhoupt, B.: Automorphisms of formal power series under substitution. - Trans. Amer. Math. Soc. 99:3, 1961, 373–383.

[26] Muzychuk, M., and F. Pakovich: Jordan–Hölder theorem for imprimitivity systems and maximal decompositions of rational functions. - Proc. Lond. Math. Soc. (3) 102:1, 2011, 1–24.

[27] Ng, T., and M. X. Wang: Ritt's theory on the unit disk. - Forum Math. 25:4, 2013, 821–851.

[28] Pakovich, F.: Prime and composite Laurent polynomials. - Bull. Sci. Math. 133, 2009, 693–732.

[29] Pakovich, F.: On semiconjugate rational functions. - Geom. Funct. Anal. 26, 2016, 1217–1243.

[30] Pakovich, F.: Commuting rational functions revisited. - Ergodic Theory Dynam. Systems 41:1, 2021, 295–320.

[31] Pakovich, F.: Sharing a measure of maximal entropy in polynomial semigroups. - Int. Math. Res. Not. IMRN 2022:18, 2022, 13829–13840.

[32] Pakovich, F.: On amenable semigroups of rational functions. - Trans. Amer. Math. Soc. 375:11, 2022, 7945–7979.

[33] Pakovich, F.: Right amenability in semigroups of formal power series. - arXiv:2208.04640v2 [math.DS], 2023.

[34] Paterson, A.: Amenability. - Math. Surveys Monogr. 29, Amer. Math. Soc., Providence, RI, 1988.

[35] Reich, L.: Families of commuting formal power series, semicanonical forms and iterative roots. - Ann. Math. Sil. 8, 1994, 189–201.

[36] Reznick, B.: When is the iterate of a formal power series odd? - J. Aust. Math. Soc. Ser. A 28:1, 1979, 62–66.

[37] Ritt, J.: On the iteration of rational functions. - Trans. Amer. Math. Soc. 21, 1920, 348–356.

[38] Ritt, J.: Prime and composite polynomials. - Trans. Amer. Math. Soc. 23, 1922, 51–66.

[39] Ritt, J.: Permutable rational functions. - Trans. Amer. Math. Soc. 25, 1923, 399–448.

[40] Scheinberg, S.: Power series in one variable. - J. Math. Anal. Appl. 31, 1970, 321–333.

[41] Schwaiger, J.: Roots of formal power series in one variable. - Aequationes Math. 29, 1985, 40–43.

Received 30 November 2023 • Accepted 30 September 2024 • Published online 31 October 2024

Fedor Pakovich
Department of Mathematics
Ben Gurion University of the Negev
P.O.B. 653, Be'er Sheva 8410501, Israel
pakovich@math.bgu.ac.il