arXiv:2006.08154v1 [math.DS] 15 Jun 2020

ON SYMMETRIES OF ITERATES OF RATIONAL FUNCTIONS

FEDOR PAKOVICH

Abstract. Let A be a rational function of degree $n \geq 2$. We denote by $G(A)$ the group of Möbius transformations σ such that $A \circ \sigma = \nu \circ A$ for some Möbius transformations ν, and by $\Sigma(A)$ and $\mathrm{Aut}(A)$ subgroups of $G(A)$, consisting of Möbius transformations σ such that $A \circ \sigma = A$ and $A \circ \sigma = \sigma \circ A$, correspondingly. We show that, unless A has a very special form, the orders of the groups $G(A^{\circ k})$, $k \geq 1$, are finite and uniformly bounded in terms of n only. We also prove a number of results allowing us in some cases to calculate explicitly the groups $\Sigma_\infty(A) = \cup_{k=1}^{\infty} \Sigma(A^{\circ k})$ and $\mathrm{Aut}_\infty(A) = \cup_{k=1}^{\infty} \mathrm{Aut}(A^{\circ k})$, especially interesting from the dynamical perspective. In addition, we prove that the number of rational functions B of degree d sharing an iterate with A is finite and bounded in terms of n and d only.

1. Introduction

Let A be a rational function of degree $n \geq 2$. In this paper, we study a variety of different subgroups of $\mathrm{Aut}(\mathbb{CP}^1)$ related to A, and more generally to the dynamical system defined by the iteration of A. Specifically, let us define $\Sigma(A)$ and $\mathrm{Aut}(A)$ as the groups of Möbius transformations σ such that $A \circ \sigma = A$ and $A \circ \sigma = \sigma \circ A$, correspondingly. Notice that elements of $\Sigma(A)$ permute points of any fiber of A, and more generally of any fiber of $A^{\circ k}$, $k \geq 1$, while elements of $\mathrm{Aut}(A)$ permute fixed points of $A^{\circ k}$, $k \geq 1$. Since any Möbius transformation is defined by its values at any three points, this implies in particular that the groups $\Sigma(A)$ and $\mathrm{Aut}(A)$ are finite and therefore belong to the well-known list A_4, S_4, A_5, C_l, D_{2l} of finite subgroups of $\mathrm{Aut}(\mathbb{CP}^1)$.

The both groups $\Sigma(A)$ and $\mathrm{Aut}(A)$ are subgroups of the group $G(A)$ defined as the group of Möbius transformations σ such that

$$A \circ \sigma = \nu \circ A \tag{1}$$

for some Möbius transformations ν. It is easy to see that $G(F)$ is indeed a group and that the map

$$\gamma_A : \sigma \to \nu_\sigma \tag{2}$$

is a homomorphism from $G(A)$ to the group $\mathrm{Aut}(\mathbb{CP}^1)$, whose kernel coincides with $\Sigma(A)$. We will denote the image of γ_F by $\widehat{G}(A)$. It was shown in the paper [22] that, unless

$$A = \alpha \circ z^n \circ \beta \tag{3}$$

for some $\alpha, \beta \in \mathrm{Aut}(\mathbb{CP}^1)$, the group $G(A)$ is also finite and its order is bounded in terms of degree of A.

This research was supported by ISF Grant No. 1432/18.

In this paper, we are mostly interested in the dynamical analogues of the groups $\Sigma(A)$ and $\mathrm{Aut}(A)$ defined by the formulas

$$\Sigma_\infty(A) = \cup_{k=1}^{\infty}\Sigma(A^{\circ k}), \qquad \mathrm{Aut}_\infty(A) = \cup_{k=1}^{\infty}\mathrm{Aut}(A^{\circ k}).$$

Since

$$\Sigma(A) \subseteq \Sigma(A^{\circ 2}) \subseteq \Sigma(A^{\circ 3}) \subseteq \dots \subseteq \Sigma(A^{\circ k}) \subseteq \dots \tag{4}$$

and

$$\mathrm{Aut}(A^{\circ k}) \subseteq \mathrm{Aut}(A^{\circ r}), \qquad \mathrm{Aut}(A^{\circ l}) \subseteq \mathrm{Aut}(A^{\circ r})$$

for any common multiple r of k and l, the sets $\Sigma_\infty(A)$ and $\mathrm{Aut}_\infty(A)$ are *groups*. Moreover, these groups preserve the Julia set J_A of A.

While it is not clear a priori that the groups $\Sigma_\infty(A)$ and $\mathrm{Aut}_\infty(A)$ are finite, for A not conjugated to $z^{\pm n}$ their finiteness can be deduced from the results of Levin ([10], [11]) about rational functions sharing the measure of maximal entropy. However, these results do not permit to describe the groups $\Sigma_\infty(A)$ and $\mathrm{Aut}_\infty(A)$ or to estimate their orders, and the main goal of this paper is to prove some results providing such information. More generally, we show that the orders of the groups $G(A^{\circ k})$, $k \geq 1$, are finite and uniformly bounded in terms of n only, unless A has a very special form. We also prove a number of results allowing us in certain cases to calculate the groups $\Sigma_\infty(A)$ and $\mathrm{Aut}_\infty(A)$ explicitly.

To formulate our results precisely let us introduce some definitions. Let A be a rational function. A rational function $\widetilde{A}$ is called an *elementary transformation* of A if there exist rational functions U and V such that $A = U \circ V$ and $\widetilde{A} = V \circ U$. We say that rational functions A and A' are *equivalent* and write $A \sim A'$ if there exists a chain of elementary transformations between A and A'. Since for any Möbius transformation μ the equality

$$A = (A \circ \mu^{-1}) \circ \mu$$

holds, the equivalence class $[A]$ of a rational function A is a union of conjugacy classes. Moreover, the number of conjugacy classes in $[A]$, which we denote by N_A, is finite, unless A is a flexible Lattès map ([18]). We denote by $c(A)$ the set of critical values of A, and by $S(A)$ the union

$$S(A) = \cup_{i=1}^{\infty}\widehat{G}(A^{\circ k}).$$

Notice that the set $S(A)$ contains the group $\mathrm{Aut}_\infty(A)$. In this notation, our main results can be summarized in the form of the following theorem.

Theorem 1.1. *Let A be a rational function of degree $n \geq 2$. Then any $\nu \in S(A)$ maps the set $c(A)$ to the set $c(A^{\circ 2})$. On the other hand, for any $\sigma \in \Sigma_\infty(A)$ the relation $A \circ \sigma \sim A$ holds. Furthermore, the sequence $G(A^{\circ k})$, $k \geq 1$, contains only finitely many non-isomorphic groups, and, unless $A = \alpha \circ z^n \circ \beta$ for some $\alpha, \beta \in \mathrm{Aut}(\mathbb{CP}^1)$, the orders of these groups are finite and uniformly bounded in terms of n only.*

The set of Möbius transformations ν satisfying $\nu\big(c(A)\big) \subseteq c(A^{\circ 2})$ can be described explicitly. Moreover, this set is finite, unless A has the form (3). Therefore, Theorem 1.1 provides us with a finite subset of $\mathrm{Aut}(\mathbb{CP}^1)$ containing the set $S(A)$ and in particular the group $\mathrm{Aut}_\infty(A)$.

The set of Möbius transformations σ satisfying $A\circ\sigma\sim A$ also can be described explicitly, providing us with a subset of $\mathrm{Aut}(\mathbb{CP}^1)$ containing the group $\Sigma_\infty(A)$. Indeed, if $N_A=1$, then the condition $A\circ\sigma\sim A$ reduces to the condition that

$$A\circ\sigma=\beta\circ A\circ\beta^{-1} \tag{5}$$

for some $\beta\in\mathrm{Aut}(\mathbb{CP}^1)$. Since equality (5) implies that β belongs to $\widehat{G}(A)$, while $\sigma\circ\beta$ belongs to the preimage of β under the homomorphism (2), we see that, whenever $G(A)$ is finite, there exist only finitely many transformations σ satisfying (5). Moreover, such transformations can be calculated explicitly once the group $G(A)$ is known. Similarly, for $N_A>1$, we can describe transformations σ satisfying $A\circ\sigma\sim A$, describing representatives $A_1,A_2,\dots,A_{N_A}$ of conjugacy classes in $[A]$ and the corresponding groups $G(A_1),G(A_2),\dots,G(A_{N_A})$.

In some cases, Theorem 1.1 permits to describe the group $\Sigma_\infty(A)$ completely. Specifically, assume that A is *indecomposable*, that is cannot be represented as a composition of two rational functions of degree at least two. In this case, obviously, $N_A=1$. On the other hand, if the group $\widehat{G}(A)$ is trivial, that is, if $G(A)=\Sigma(A)$, then equality (5) is possible only if $\sigma\in\Sigma(A)$. Therefore, for an indecomposable rational function A with trivial group $\widehat{G}(A)$, the equality $\Sigma_\infty(A)=\Sigma(A)$ holds. In particular, if the group $G(A)$ is trivial, then the group $\Sigma_\infty(A)$ is also trivial. Similarly, if $G(A)=\mathrm{Aut}(A)$, then equality (5) is possible only if σ is the identical map. Thus, $\Sigma_\infty(A)$ is trivial whenever A is indecomposable and $G(A)=\mathrm{Aut}(A)$.

Along with the groups $G(A^{\circ k})$, $k\geq 1$, we consider their "local" versions. Specifically, let z_0 be a fixed point of A, and z_1 a point of $\mathbb{CP}^1$ distinct from z_0. We define $G(A,z_0,z_1)$ as the subgroup of $G(A)$ consisting of Möbius transformations σ such that $\sigma(z_0)=z_0$, $\sigma(z_1)=z_1$, and $\nu_\sigma=\sigma^{\circ k}$ for some $k\geq 1$. We prove the following statement.

Theorem 1.2. *Let A be a rational function of degree at least two, z_0 a fixed point of A, and z_1 a point of $\mathbb{CP}^1$ distinct from z_0. Then $G(A^{\circ k},z_0,z_1)=G(A,z_0,z_1)$ for all $k\geq 1$.*

Notice that the groups $G(A^{\circ k},z_0,z_1)$, $k\geq 1$, are related to the groups $\mathrm{Aut}(A^{\circ k})$, $k\geq 1$. Indeed, the equality

$$A^{\circ k}\circ\sigma=\sigma\circ A^{\circ k},\qquad k\geq 1, \tag{6}$$

implies that $A^{\circ k}$ sends the set of fixed points of σ to itself. Therefore, at least one of the fixed points z_0, z_1 of σ is a fixed point of $A^{\circ 2k}$, and, if z_0 is such a point, then $\sigma\in G(A^{\circ 2k},z_0,z_1)$. Due to this connection, Theorem 1.2 allows us in some cases to estimate the order of the group $\mathrm{Aut}_\infty(A)$, and even to describe this group explicitly.

Finally, we prove the following result of independent interest.

Theorem 1.3. *There exists a function $\varphi:\mathbb{N}\times\mathbb{N}\to\mathbb{R}$ such that for any rational function A of degree n, not conjugate to $z^{\pm n}$, there exist at most $\varphi(n,d)$ rational functions B of degree d sharing an iterate with A.*

Let us mention that since equality (6) is equivalent to the equality

$$A^{\circ k}=(\sigma\circ A\circ\sigma^{-1})^{\circ k},$$

Theorem 1.3 is a generalization of the statement about the boundedness of the group $\mathrm{Aut}_\infty(A)$ in terms of n.

The paper is organized as follows. In the second section, we establish basic properties of the group $G(A)$ used throughout the rest of the paper. In particular, we prove the finiteness of $G(A)$ for A not of the form (3), and provide a method for calculating $G(A)$. In the third section, we discuss relations between the group $G(A)$ and the group $\Omega(A)$ consisting of Möbius transformations preserving the Julia set J_A of A. In particular, we show that the set of Möbius transformations σ such that

$$A^{\circ k} \circ \sigma = \sigma^{\circ l} \circ A^{\circ k}$$

for some $k \geq 1$ and $l \geq 1$ is a subset of $\Omega(A)$. We also deduce the finiteness of $\Sigma_\infty(A)$ and $\mathrm{Aut}_\infty(A)$ from the results of [10], [11].

In the fourth section, we prove that any $\nu \in S(A)$ maps the set $c(A)$ to the set $c(A^{\circ 2})$. In the fifth section, using some general results about semiconjugate rational functions from the papers [17], [22], we show that for any $\sigma \in \Sigma_\infty(A)$ the relation $A \circ \sigma \sim A$ holds, and prove the remaining statements from Theorem 1.1. In the sixth section, we deduce Theorem 1.2 from the result of Reznick ([24]) about iterates of formal power series, and provide some applications concerning the group $\mathrm{Aut}_\infty(A)$. Finally, in the seventh section, using a result about functional decompositions of iterates of rational functions from the paper [23], we prove Theorem 1.3.

2. Groups $G(A)$

Let A be a rational function of degree $n \geq 2$. Recall that the group $G(A)$ is defined as the group of Möbius transformations σ such that equality (1) holds for some Möbius transformation ν. Notice that if rational functions A and A' are related by the equality

$$\alpha \circ A \circ \beta = A'$$

for some $\alpha, \beta \in \mathrm{Aut}(\mathbb{CP}^1)$, then

$$G(A') = \beta^{-1} \circ G(A) \circ \beta, \qquad \widehat{G}(A') = \alpha \circ \widehat{G}(A) \circ \alpha^{-1}.$$

In particular, the groups $G(A)$ and $G(A')$ are isomorphic. We say that a rational function A of degree $n \geq 2$ is *a quasi-power* if there exist $\alpha, \beta \in \mathrm{Aut}(\mathbb{CP}^1)$ such that

$$A = \alpha \circ z^n \circ \beta.$$

Lemma 2.1. *A rational function A of degree $n \geq 2$ is a quasi-power if and only if it has only two critical values. If A is a quasi-power, then $A^{\circ 2}$ is a quasi-power if and only if A is conjugate to $z^{\pm n}$.*

Proof. The first part of the lemma is well-known and follows easily from the Riemann-Hurwitz formula. To prove the second, we observe that the chain rule implies that

$$A^{\circ 2} = \alpha \circ z^n \circ \beta \circ \alpha \circ z^n \circ \beta$$

has only two critical values if and only if $\beta \circ \alpha$ maps the set $\{0, \infty\}$ to itself. Therefore, $A^{\circ 2}$ is a quasi-power if and only if $\beta \circ \alpha = cz^{\pm 1}$, $c \in \mathbb{C} \setminus \{0\}$, that is, if and only if

$$A = \alpha \circ z^n \circ cz^{\pm 1} \circ \alpha^{-1} = \alpha \circ c^n z^{\pm n} \circ \alpha^{-1}.$$

Since $c^n z^{\pm n}$ is conjugate to $z^{\pm n}$, the last condition is equivalent to the condition that A is conjugate to $z^{\pm n}$. □

The following result was proved in [22]. Since some ideas of the proof are used in the rest of the paper, we repeat the arguments.

Theorem 2.2. *Let A be a rational function of degree $n \geq 2$, which is not a quasi-power. Then the group $G(A)$ is one of the five finite rotation groups of the sphere A_4, S_4, A_5, C_l, D_{2l}, and the order of any element of $G(A)$ does not exceed n. In particular, $|G(A)| \leq \max\{60, 2n\}$.*

Proof. Any non-identical element of the group $\mathrm{Aut}(\mathbb{CP}^1) \cong \mathrm{PSL}_2(\mathbb{C})$ is conjugate either to $z \to z+1$ or to $z \to \lambda z$ for some $\lambda \in \mathbb{C} \setminus \{0, 1\}$. Thus, making the change

$$A \to \mu_1 \circ A \circ \mu_2, \quad \sigma \to \mu_2^{-1} \circ \sigma \circ \mu_2, \quad \nu_\sigma \to \mu_1 \circ \nu_\sigma \circ \mu_1^{-1}$$

for convenient μ_1, $\mu_2 \in \mathrm{Aut}(\mathbb{CP}^1)$, without loss of generality we may assume that σ and ν in (1) have one of the two forms above.

We observe first that the equalities

$$A(z+1) = \lambda A(z), \quad \lambda \in \mathbb{C} \setminus \{0, 1\}, \tag{7}$$

and

$$A(z+1) = A(z) + 1 \tag{8}$$

are impossible. Indeed, if A has a finite pole, then any of these equalities implies that A has infinitely many poles. On the other hand, if A is a polynomial of degree $n \geq 2$, then we obtain a contradiction comparing the coefficients of z^n in the left and the right sides of equality (7), and the coefficients of z^{n-1} in left and the right sides of equality (8), correspondingly.

Furthermore, comparing the free terms in the Laurent series at infinity of the left and the right sides of the equality

$$A(\lambda z) = A(z) + 1, \quad \lambda \in \mathbb{C} \setminus \{0, 1\},$$

we conclude that this equality is impossible either. Thus,

$$A(\lambda_1 z) = \lambda_2 A(z), \quad \lambda_1, \lambda_2 \in \mathbb{C} \setminus \{0, 1\}. \tag{9}$$

Comparing coefficients in the left and the right sides of (9) and taking into account that $A \neq z^{\pm n}$ by the assumption, we conclude that λ_1 is a root of unity. Furthermore, the order of the transformation $z \to \lambda_1 z$ in the group $G(A)$ does not exceed the maximum number d such that A can be represented in the form

$$A = z^r R(z^d), \quad R \in \mathbb{C}(z), \quad 0 \leq r \leq d-1. \tag{10}$$

In particular, the order of any element of $G(A)$ does not exceed n. Indeed, since $A \neq z^{\pm n}$, the function R in (10) has a zero or a pole distinct from 0 and ∞, implying that $d \leq n$.

The finiteness of $G(A)$ follows now from the Burnside theorem (see e.g. [6], (36.1)), which states that any subgroup of $\mathrm{GL_k}(\mathbb{C})$ of bounded period is finite. Indeed, if $G(A) \subset \mathrm{PSL}_2(\mathbb{C})$ is infinite, then its lifting $\overline{G(A)} \subset \mathrm{SL}_2(\mathbb{C}) \subset \mathrm{GL}_2(\mathbb{C})$ is also infinite. On the other hand, if the order of any element of $G(A)$ is bounded by n, then the order of any element $\overline{G(A)}$ is bounded by $2n$. The contradiction obtained proves the finiteness of $G(A)$. It is also possible to use the classification of finite subgroups of $\mathrm{Aut}(\mathbb{CP}^1)$ combined with the Schur theorem (see e.g. [6], (36.2)), which states that any finitely generated periodic subgroup of $\mathrm{GL_k}(\mathbb{C})$ has finite order (cf. [22]). $\square$

Notice that Theorem 2.2 obviously implies that, unless A is a quasi-power,

$$|G(A)| = |\widehat{G}(A)||\Sigma(A)|. \tag{11}$$

In particular, $\widehat{G}(A)$ is finite.

The following result, while simple, is extremely useful.

Theorem 2.3. *Let A be a rational function of degree $n \geq 2$. Then every $\nu \in \widehat{G}(A)$ maps $c(A)$ to $c(A)$. Furthermore, if $\nu(c_1) = c_2$ for some $c_1, c_2 \in c(A)$, then any $\sigma \in \gamma_A^{-1}\{\nu\}$ maps the fiber $A^{-1}\{c_1\}$ to the fiber $A^{-1}\{c_2\}$ preserving the local multiplicities of points.*

Proof. It follows directly from (1) that if $\nu(c) = c'$ for some $c, c' \in \mathbb{CP}^1$, then any $\sigma \in \gamma_A^{-1}\{\nu\}$ maps the fiber $A^{-1}\{c\}$ to the fiber $A^{-1}\{c'\}$. Moreover, since σ and ν are one-to-one, applying the chain rule to (1), we see that σ preserves the local multiplicities of points. Finally, again using that σ is one-to-one, we see that the fibers $A^{-1}\{c\}$ and $A^{-1}\{c'\}$ have the same cardinality, implying that σ maps $c(A)$ to $c(A)$. □

Notice that Theorem 2.3, along with Theorem 2.2, implies the finiteness of the group $G(A)$ for rational functions A, which are not quasi-powers. Indeed, since $c(A)$ is finite and any Mobius transformation is defined by its values at any three points, Theorem 2.3 implies that the group $G(A)$ is finite, unless A has only two critical values. On the other hand, by Lemma 2.1, A has only two critical values if and only if A is a quasi-power. Notice also that Theorem 2.3 implies that for $A = z^{\pm n}$ the group $G(A)$ consists of the transformations $cz^{\pm 1}$, $c \in \mathbb{C} \setminus \{0\}$.

Although Theorem 2.3 does not provide us with a bound for orders of elements of the group $G(A)$, it gives a method for practical calculation of $G(A)$, especially useful if A has a relatively small number of critical values. We illustrate it with the following example.

Example 2.4. Let us consider the function

$$A = \frac{1}{8}\,\frac{z^4 + 8\,z^3 + 8\,z - 8}{z - 1}.$$

One can check that A has three critical values 1, 9, and ∞, and that

$$A - 1 = \frac{1}{8}\,\frac{z^3\,(z + 8)}{z - 1}, \qquad A - 9 = \frac{1}{8}\,\frac{\left(z^2 + 4\,z - 8\right)^2}{z - 1}.$$

Taking into account that the multiplicity of the pole ∞ is 3, while the multiplicity of the pole 1 is 1, in correspondence with Theorem 2.3 we conclude that for any $\sigma \in G(A)$ either

$$\sigma(0) = 0, \quad \sigma(\infty) = \infty, \quad \sigma(-8) = -8, \quad \sigma(1) = 1, \tag{12}$$

or

$$\sigma(0) = \infty, \quad \sigma(\infty) = 0, \quad \sigma(-8) = 1, \quad \sigma(1) = -8. \tag{13}$$

Moreover, in addition, either

$$\sigma(-2 + 2\sqrt{3}) = -2 - 2\sqrt{3}, \quad \sigma(-2 - 2\sqrt{3}) = -2 + 2\sqrt{3}, \tag{14}$$

or

$$\sigma(-2 + 2\sqrt{3}) = -2 + 2\sqrt{3}, \quad \sigma(-2 - 2\sqrt{3}) = -2 - 2\sqrt{3}.$$

Clearly, condition (12) implies that $\sigma = z$, while the unique transformation satisfying (13) is

$$\sigma = -8/z, \tag{15}$$

and this transformation satisfies (14). Furthermore, the corresponding ν_σ must satisfy

$$\nu_\sigma(1) = \infty, \quad \nu_\sigma(\infty) = 1, \quad \nu_\sigma(9) = 9,$$

implying that

$$\nu_\sigma = \frac{z+63}{z-1}. \tag{16}$$

Therefore, (1) can hold only for σ and ν_σ given by formulas (15) and (16), and the direct calculation shows that (1) is indeed satisfied. Thus, the groups $G(A)$ and $\widehat{G}(A)$ are cyclic groups of order two, while the groups $\Sigma(A)$ and $\mathrm{Aut}(A)$ are trivial.

To reduce the found symmetry to the "visible" form (10) one need use the transformations

$$\mu_1 = \frac{z+7}{z-9}, \quad \mu_2 = \frac{2\,i\sqrt{2}z + 2\,i\sqrt{2}}{-z+1}$$

for which

$$\mu_1 \circ \frac{z+63}{z-1} \circ \mu_1^{-1} = -z, \quad \mu_2^{-1} \circ -8/z \circ \mu_2 = -z$$

and

$$\mu_1 \circ A \circ \mu_2 = 4\,\frac{z\left(\left(i\sqrt{2}+1\right)z^2 - i\sqrt{2}+1\right)}{\left(2\,i\sqrt{2}+1\right)z^4 + 6\,z^2 - 2\,i\sqrt{2}+1}.$$

Let G be a finite subgroup of $\mathrm{Aut}(\mathbb{CP}^1)$. Recall that a rational function $\theta = \theta_G$ is called an *invariant function* for G if the equality $\theta_G(x) = \theta_G(y)$ holds for $x, y \in \mathbb{CP}^1$ if and only if there exists $\sigma \in G$ such that $\sigma(x) = y$. Such a function always exists and is defined in a unique way up to the transformation $\theta \to \mu \circ \theta$, where $\mu \in \mathrm{Aut}(\mathbb{CP}^1)$. Obviously, θ_G has degree equal to the order of G. Moreover, the Lüroth theorem implies that any rational function g such that $g(x) = g(y)$ whenever $\sigma(x) = y$ for some $\sigma \in G$ is a rational function in θ_G.

The above implies that the equality $\Sigma(A) = G$ is equivalent to the requirement that A is a rational function in θ_G, but is not a rational function in $\theta_{G'}$ for any finite subgroup G' of $\mathrm{Aut}(\mathbb{CP}^1)$ satisfying $G \subset G'$. On the other hand, a description of rational functions A such that $\mathrm{Aut}(A) = G$ can be done in terms of homogenous invariant polynomials for G. This description was obtained by Doyle and McMullen in [7]. Notice that rational functions with non-trivial automorphism groups are closely related to *generalized Lattès maps* (see [19] for more detail and examples).

Example 2.5. Let us consider the function

$$B = -\frac{2z^2}{z^4+1} = -\frac{2}{z^2 + \frac{1}{z^2}}.$$

It is easy to see that B is an invariant function for the Klein four-group $V_4 = D_4$, generated by the transformations $z \to -z$ and $z \to 1/z$. Thus, $\Sigma(B) = D_4$. Furthermore, it is clear that $G(B)$ contains the transformation $\mu_1 = iz$, satisfying $B \circ \mu_1 = \nu_1 \circ B$ for $\nu_1 = -z$, so that $G(B)$ contains D_8.

The groups A_4, A_5, and C_l do not contain D_8. Therefore, if D_8 is a proper subgroup of $G(B)$, then either $G(B)$ is a dihedral group containing an element σ of order $k > 4$, whose fixed points coincide with fixed points of μ_1, or $G(B) = S_4$. The first case is impossible, since σ must have the form cz, $c \in \mathbb{C} \setminus \{0\}$, and it is easy to see that such σ belongs to $G(B)$ if and only if it is a power of μ_1. On the other hand, a direct calculation shows that for the transformation $\mu_2 = \frac{z+i}{z-i}$, generating together with $\mu_1 = iz$ and $\delta = 1/z$ the group S_4, the equality $B \circ \mu_2 = \nu_2 \circ B$ holds for $\nu_2 = \frac{-z+1}{-3z-1}$. Summarizing, we see that $G(B) = S_4$, $\widehat{G}(B) = D_6$, $\Sigma(B) = D_4$, and $\mathrm{Aut}(B)$ is trivial.

We conclude this section with the following specification of Theorem 2.2 and Theorem 2.3.

Theorem 2.6. *Let A be a rational function of degree $n \geq 2$. Assume that there exists a point $z_0 \in \mathrm{Aut}(\mathbb{CP}^1)$ such that the local multiplicity of A at z_0 is distinct from the local multiplicity of A at any other point $z \in \mathrm{Aut}(\mathbb{CP}^1)$. Then $G(A)$ is a finite cyclic group, and z_0 is a fixed point of the generator of $G(A)$.*

Proof. Indeed, it is easy to see that A is not a quasi-power, implying that $G(A)$ is finite. Moreover, any element of $G(A)$ fixes z_0. On the other hand, a unique finite subgroup of $\mathrm{Aut}(\mathbb{CP}^1)$ whose elements share a fixed point is cyclic. $\square$

Corollary 2.7. *Let P be a polynomial of degree $n \geq 2$, which is not a quasi-power. Then $G(P)$ is a finite cyclic group, generated by a polynomial.*

Proof. Since the local multiplicity of P at infinity is n, the corollary follows from Theorem 2.6, taking into account that P is a not a quasi-power.

Another way to prove Corollary 2.7 is to conjugate P to a *normal* polynomial, that is, to a polynomial of the form

$$z^n + a_{n-2}z^{n-2} + \cdots + a_0, \tag{17}$$

where $a_n = 1$ and $a_{n-1} = 0$ (see [3] for more detail). Indeed, if P is not a quasi-power, then the both groups $G(P)$ and $\widehat{G}(A)$ consist of polynomials. On the other hand, one can easily see that if (1) holds for a polynomial of the form (17) and polynomials $\sigma = az + b$, $\nu_\sigma = cz + d$, then $b = 0$ and a is a root of unity. $\square$

3. Symmetries of Julia sets

Let A be a rational function of degree at least two. In this section, we discuss relations between the group $G(A)$ and the group of symmetries of the Julia set J_A of A. We start from the polynomial case where the situation is well understood, although the notion of symmetry is more restrictive than the one considered in this paper.

Let us denote by $\mathcal{E}$ the group of all *Euclidean isometries of* $\mathbb{C}$, that is, the group of polynomials of degree one $\mu = az + b$, $a, b \in \mathbb{C}$, with $|a| = 1$. For a polynomial P we denote by $E(P)$ the group consisting of $\mu \in \mathcal{E}$ such that $\mu(J_A) = J_A$.

The following result was proved in [3].

Theorem 3.1. *Let P be a polynomial of degree at least two. Then $\mu \in \mathcal{E}$ belongs to $E(P)$ if and only if $P \circ \mu = \mu^{\circ l} \circ P$ for some $l \geq 1$.* $\square$

In one direction, the proof is easy. Indeed, let μ be a rotation about some point ζ such that

$$P \circ \mu = \mu^{\circ l} \circ P \tag{18}$$

for some $l \geq 1$. Then for any $k \geq 1$ the equality

$$P^{\circ k} = \mu^{\circ r} \circ P^{\circ k}$$

holds for some $r \geq 1$, and

$$|(P^{\circ k} \circ \mu)(z) - \zeta| = |(\mu^{\circ r} \circ P^{\circ k})(z) - \zeta| = |P^{\circ k}(z) - \zeta|$$

in the metric of $\mathbb{C}$. Since the Julia set J_P of a polynomial P is the boundary of the set $F_\infty(P)$ consisting of the points of $\mathbb{CP}^1$ with unbounded orbit, this implies that $z \in J_P$ if and only if $\mu(z) \in J_P$. Therefore, $\mu(J_P) = J_P$.

The proof in the inverse direction is more complicated and makes use the Bötcher function. Alternatively, one can use the main result of the paper [16]. Specifically, it follows from Corollary 1 in [16] that if $K \subset \mathbb{C}$ is an arbitrary compact set containing more than one point such that $P^{-1}(K) = K$, and μ is a polynomial of degree one such that $\mu(K) = K$, then there exists a polynomial of degree one ν such that

$$P \circ \mu = \nu \circ P$$

and $\nu(K) = K$. Using now the analysis of the previous section, it is easy to see that $\nu = \mu^{\circ s}$ for some $s \geq 1$. Notice that the problem of describing the group $E(P)$ for polynomial P is closely related to the problem of describing commuting polynomials and polynomials sharing the Julia set (see [1], [2], [3], [4], [16], [25]).

By Corollary 2.7, for a polynomial P, not conjugate to z^n, any Möbius transformation μ, satisfying (18), is a polynomial. On the other hand, any polynomial Möbius transformation μ preserving J_P is an isometry of $\mathbb{C}$, since for a polynomial P the set J_P is compact, and hence μ maps the disc of minimum radius containing J_P to itself. Thus, the assumption that μ is an isometry of $\mathbb{C}$ is appropriate in Theorem 3.1, and the above proof uses this assumption. Our next result generalizes the “if” part of Theorem 3.1 in two directions. First, we allow P to be an arbitrary rational function. Second, we do not assume that considered Möbius transformations necessarily are isometries of $\mathbb{C}$ or $\mathbb{CP}^1$.

For a rational function A we denote by $\Omega(A)$ the subgroup of $\text{Aut}(\mathbb{CP}^1)$ consisting of Möbius transformations such that $\mu(J_A) = J_A$, and by $\Gamma(A)$ the set of Möbius transformations σ such that

$$A \circ \sigma = \sigma^{\circ l} \circ A$$

for some $l \geq 0$. Finally, we define the set $\Gamma_\infty(A)$ by the formula

$$\Gamma_\infty(A) = \bigcup_{i=1}^{\infty} \Gamma(A^{\circ k}).$$

Notice that $\Gamma_\infty(A)$ contains the both groups $\Sigma_\infty(A)$ and $\text{Aut}_\infty(A)$.

Theorem 3.2. *Let A be a rational function of degree at least two. Then the set $\Gamma_\infty(A)$ is a subset of $\Omega(A)$.*

Proof. Let σ be an element of $\Gamma_\infty(P)$, satisfying the equality

$$A^{\circ k} \circ \sigma = \sigma^{\circ l} \circ A^{\circ k} \tag{19}$$

for some $k \geq 1$ and $l \geq 0$, and let C_σ be the cyclic subgroup of $\text{Aut}(\mathbb{CP}^1)$, generated by σ. Clearly, (19) implies that for any $s \geq 1$ the equality

$$A^{\circ ks} \circ \sigma = \sigma^{\circ r} \circ A^{\circ ks}$$

holds for some $r \geq 1$. On the other hand, since $\sigma \in G(A^{\circ k})$, the group C_σ is finite by Theorem 2.2. Therefore, there exist $\sigma' \in C_\sigma$ and integers s_1 and s_2 such that the equalities

$$A^{\circ ks_1} \circ \sigma = \sigma' \circ A^{\circ ks_1} \tag{20}$$

and

$$A^{\circ ks_2} \circ \sigma' = \sigma' \circ A^{\circ ks_2} \tag{21}$$

hold.

Since equality (21) is equivalent to the equality

$$A^{\circ ks_2} = (\sigma' \circ A \circ \sigma'^{-1})^{\circ ks_2},$$

we see that

$$J_A = J_{A^{\circ ks_2}} = J_{(\sigma' \circ A \circ \sigma'^{-1})^{\circ ks_2}} = J_{\sigma' \circ A \circ \sigma'^{-1}},$$

implying that $\sigma'(J_A) = J_A$. It follows now from $A^{-1}(J_A) = J_A$ and (20) that $\sigma^{-1}(J_A) = J_A$. □

In distinction with the polynomial case, the problem of describing rational functions sharing the Julia set is still not solved in the complete generality (see [10], [11], [12] for available results). The structure of the group $\Omega(A)$ is also not known. In particular, to our best knowledge, it is not known whether any element of $\Omega(A)$ has finite order, unless J_A is a circle, a segment, or the whole sphere (see [5], [11] for partial results). Thus, understanding to what extent Theorem 3.2 has a converse is a challenging problem. Nevertheless, the results of [10], [11] imply that for any rational function A of degree $n \geq 2$, not conjugate to $z^{\pm n}$, there exist at most finitely many rational functions B of any given degree $d \geq 2$ sharing the *measure of maximal entropy* with A. This fact can be used for proving the finiteness of the groups $\Sigma_\infty(A)$ and $\mathrm{Aut}_\infty(A)$. We provide such a proof below.

Let us recall that by the results of Freire, Lopes, Mañé ([9]) and Lyubich ([13]), for any rational function A of degree $n \geq 2$ there exists a unique probability measure μ_A on $\mathbb{CP}^1$, which is invariant under A, has support equal to the Julia set J_A, and achieves maximal entropy $\log n$ among all A-invariant probability measures. Since J_A coincides with the support of μ_A, rational functions sharing the measure of maximal entropy share the Julia sets. However, the inverse is not true in general. The measure μ_A can be described as follows. For $a \in \mathbb{CP}^1$ let $z_i^k(a)$, $i = 1, \dots, n^k$, be the roots of the equation $A^{\circ k}(z) = a$ counted with multiplicity, and $\mu_{A,k}(a)$ be the measure defined by

$$\mu_{A,k}(a) = \frac{1}{n^k} \sum_{i=1}^{n^k} \delta_{z_i^k(a)}.$$

Then for every $a \in \mathbb{CP}^1$ with two possible exceptions, the sequence $\mu_{A,k}(a)$, $k \geq 1$, converges in the weak topology to μ_A. The measure μ_A is characterized by the balancedness property that

$$\mu_A(A(S)) = \mu_A(S) \deg A$$

for any Borel set S on which A is injective. Notice that for rational functions A and B the property to have the same measure of maximal entropy can be expressed in algebraic terms (see [12]), leading to characterizations of such functions in terms of functional equations (see [12], [21], [26]).

Theorem 3.3. *Let A be a rational function of degree $n \geq 2$, not conjugate to $z^{\pm n}$. Then the groups $\Sigma_\infty(A)$ and $\mathrm{Aut}_\infty(A)$ are finite.*

Proof. Assume that $\sigma \in \mathrm{Aut}_\infty(A)$. Then the functions A and $\sigma^{-1} \circ A \circ \sigma$ have a common iterate and hence share the measure of maximal entropy. Therefore, by the results of [10], [11], the set

$$\sigma^{-1} \circ A \circ \sigma, \qquad \sigma \in \mathrm{Aut}_\infty(A),$$

is finite. On the other hand, the equality

$$\sigma \circ A \circ \sigma^{-1} = \sigma' \circ A \circ \sigma'^{-1} \tag{22}$$

implies that $\sigma'^{-1} \circ \sigma \in \mathrm{Aut}(A)$. Thus, for any given $\sigma \in \mathrm{Aut}_\infty(A)$ there could be at most finitely many $\sigma' \in \mathrm{Aut}_\infty(A)$ satisfying (22), implying the finiteness of $\mathrm{Aut}_\infty(A)$.

To prove the finiteness of $\Sigma_\infty(A)$, let us observe first that any $\sigma \in \Sigma_\infty(A)$ is μ_A-invariant. Indeed, since the equality

$$A^{\circ l} = A^{\circ l} \circ \sigma,$$

where $\sigma \in \mathrm{Aut}(\mathbb{CP}^1)$ and $l \geq 1$, implies that for any $k \geq 1$ the transformation σ maps the set of roots of the equation $A^{\circ kl}(z) = a$, $a \in \mathbb{CP}^1$, to itself, we have:

$$\sigma_* \mu_{A,kl}(a) = \mu_{A,kl}(a), \qquad k \geq 1.$$

Therefore, for any function f continuous on $\mathbb{CP}^1$ and $k \geq 1$ the equality

$$\int f \circ \sigma d\mu_{A,kl}(a) = \int f d\mu_{A,kl}(a)$$

holds, implying that

$$\int f \circ \sigma d\mu = \int f d\mu.$$

Further, let us show that that for any $\sigma \in \Sigma_\infty(A)$ the equality $\mu_A = \mu_{A\circ\sigma}$ holds. Let S be a Borel set on which $A \circ \sigma$ is injective. Then A is injective on $\sigma(S)$, implying that

$$\mu_A\big((A \circ \sigma)(S)\big) = \mu_A\big(A(\sigma(S)\big) = n\mu_A\big(\sigma(S)\big) = n\mu_A(S).$$

Thus, μ_A is the balanced measure for $A\circ\sigma$ and hence $\mu_A = \mu_{A\circ\sigma}$. Now the finiteness of $\Sigma_\infty(A)$ can be established similarly to the finiteness of $\mathrm{Aut}_\infty(A)$, using instead of the finiteness of $\mathrm{Aut}(A)$ the finiteness of $\Sigma(A)$. □

We conclude this section with the following result.

Theorem 3.4. *Let P be a polynomial of degree $n \geq 2$. Then $\Gamma(P^{\circ k}) = \Gamma(P)$, $k \geq 1$.*

Proof. Without loss of generality, we can assume that P has the normal form (17). It is easy to see that then any iterate of P also has the normal form. In particular, fixed points of any element of $\Gamma(P^{\circ k})$, $k \geq 1$, are zero and infinity. If $P = z^n$, then any of the sets $\Gamma(P^{\circ k})$, $k \geq 1$, coincides with the group $cz^{\pm 1}$, $c \in \mathbb{C} \setminus \{0\}$, and the theorem is true. Thus, we can assume that $P \neq z^n$, implying that $P^{\circ k}$, $k \geq 1$, is not a power. As it was observed in the proof of Corollary 2.7, in this case any element of $\Gamma(P^{\circ k})$, $k \geq 1$, is a polynomial belonging to $\mathcal{E}$. Thus, $\Gamma(P^{\circ k}) = E(P^{\circ k})$, $k \geq 1$, by Theorem 3.1. On the other hand, $E(P^{\circ k}) = E(P)$, $k \geq 1$, since $J_{P^{\circ k}} = J_P$, $k \geq 1$. Therefore, $\Gamma(P^{\circ k}) = \Gamma(P)$, $k \geq 1$.

Another proof of the theorem can be obtained as follows. Let us observe that for a polynomial P in the normal form, not equal to z^n, the cardinality of $\Gamma(P)$ equals the maximum number $d = d(P)$ such that P can be represented in the form (10), where R is a *polynomial*. Therefore, to prove the theorem it is enough to prove the following statement: if some iterate of a polynomial $P \neq z^n$, has the form $P^{\circ k} = z^l Q(z^d)$, for some l, $0 \leq l \leq d-1$, and $Q \in \mathbb{C}[z]$, then there exist r, $0 \leq r \leq d-1$, and $R \in \mathbb{C}[z]$ such that $P = z^r R(z^d)$.

To prove the last statement, we recall that for an arbitrary rational function F its functional decompositions $F = U \circ V$ considered up to the equivalency

$$U \to U \circ \mu, \qquad V \to \mu^{-1} \circ V, \qquad \mu \in \mathrm{Aut}(\mathbb{CP}^1),$$

are in a one-to-one correspondence with imprimitivity systems of the monodromy group of F. Since the monodromy group of a polynomial P of degree n contains a cycle of length n, this implies that for any two decompositions $P = U \circ V$ and $P = U' \circ V'$, where U, V, U', V' are polynomials such that $\deg U = \deg U'$ and $\deg V = \deg V'$, there exists a Möbius transformation μ such that

$$U = U' \circ \mu, \qquad V = \mu^{-1} \circ V'$$

(for a purely algebraic proof of this fact, see [8]). Therefore, if $P^{\circ k} = z^l Q(z^d)$, then it follows from the equality

$$z^l Q(z^d) = P^{\circ (k-1)} \circ P = (\varepsilon^{-l} P^{\circ (k-1)}) \circ (P \circ \varepsilon z),$$

where $\varepsilon = e^{\frac{2\pi i}{d}}$, that there exists a Möbius transformation μ such that

$$P \circ \varepsilon z = \mu \circ P, \qquad \varepsilon^{-l} P^{\circ (k-1)} = P^{\circ (k-1)} \circ \mu^{-1}. \tag{23}$$

Clearly, μ is a polynomial. Moreover, since $P^{\circ (k-1)}$ has the normal form, the second equality in (23) implies that $\mu(0) = 0$. Since $P \neq z^n$, it follows now from the first equality in (23) that there exist r, $0 \leq r \leq d-1$, and $R \in \mathbb{C}[z]$ such that $P = z^r R(z^d)$. □

Notice that neither the statement of Theorem 3.4, nor the statement about polynomials, used in the second proof of Theorem 3.4, are true for rational functions (see Example 6.2 below).

4. Sets $S(A)$

Let A be a rational function of degree $n \geq 2$. Recall that the set $S(A)$ is defined as the union

$$S(A) = \cup_{i=1}^{\infty} \widehat{G}(A^{\circ k}),$$

that is, as the set of Möbius transformation ν such that

$$\nu \circ A^{\circ k} = A^{\circ k} \circ \mu \tag{24}$$

for some Möbius transformation μ and $k \geq 1$. In this section we provide a characterization of elements of $S(A)$, and prove that $S(A)$ is finite and bounded in terms of n, unless A is a quasi-power.

We use the following statement.

Theorem 4.1. *Let $A_1, A_2, \dots, A_k$, $k \geq 2$, and $B_1, B_2, \dots, B_k$, $k \geq 2$, be rational functions of degree $n \geq 2$ such that*

$$A_1 \circ A_2 \circ \cdots \circ A_k = B_1 \circ B_2 \circ \cdots \circ B_k. \tag{25}$$

Then $c(A_1) \subseteq c(B_1 \circ B_2)$.

Proof. Let f be a rational function of degree d and $T \subset \mathbb{CP}^1$ a finite set. It is clear that the cardinality of the preimage $f^{-1}(T)$ satisfies the upper bound

$$|f^{-1}(T)| \leq |T|d. \tag{26}$$

To obtain the lower bound, we observe that the Riemann-Hurwitz formula

$$2d-2 = \sum_{z \in \mathbb{CP}^1} (\deg_z f - 1)$$

implies that

$$\sum_{z \in f^{-1}(T)} (\deg_z f - 1) \leq 2d-2.$$

Therefore,

$$|f^{-1}(T)| = \sum_{z \in f^{-1}\{T\}} 1 \geq \sum_{z \in f^{-1}\{T\}} \deg_z f - 2d + 2 = (|T|-2)d + 2. \tag{27}$$

Let us denote by F the rational function defined by any of the parts of equality (25). Assume that c is a critical value of A_1 such that $c \notin c(B_1 \circ B_2)$. Clearly,

$$|F^{-1}\{c\}| = |(A_2 \circ \cdots \circ A_k)^{-1}\{A_1^{-1}\{c\}\}|.$$

Therefore, since $c \in c(A_1)$ implies that $|A_1^{-1}\{c\}| \leq n-1$, it follows from (26) that

$$|F^{-1}\{c\}| \leq (n-1)n^{k-1}. \tag{28}$$

On the other hand,

$$|F^{-1}\{c\}| = |(B_3 \circ \cdots \circ B_k)^{-1}\{(B_1 \circ B_2)^{-1}\{c\}\}|.$$

Since the condition $c \notin c(B_1 \circ B_2)$ is equivalent to the equality $|(B_1 \circ B_2)^{-1}\{c\}| = n^2$, this implies by (27) that

$$|F^{-1}\{c\}| \geq (n^2-2)n^{k-2} + 2. \tag{29}$$

It follows now from (28) and (29) that

$$(n^2-2)n^{k-2} + 2 \leq (n-1)n^{k-1},$$

or equivalently that $n^{k-1} + 2 \leq 2n^{k-2}$. However, this leads to a contradiction since $n \geq 2$ implies that $n^{k-1} + 2 \geq 2n^{k-2} + 2$. Therefore, $c(A_1) \subseteq c(B_1 \circ B_2)$. □

Theorem 4.1 implies the following statement, which is essentially the first statement of Theorem 1.1.

Theorem 4.2. *Let A be a rational function of degree $n \geq 2$. Then for any $\nu \in S(A)$ the inclusion $\nu\big(c(A)\big) \subseteq c(A^{\circ 2})$ holds.*

Proof. Let ν be an element of $S(A)$. In case if $\nu \in \widehat{G}(A)$, the statement of the theorem follows from Theorem 2.3, since $c(A) \subseteq c(A^{\circ 2})$ by the chain rule. Therefore, we may assume that $\nu \in \widehat{G}(A^{\circ k})$ for some $k \geq 2$. Since equality (24) has the form (25) with

$$A_1 = \nu \circ A, \qquad A_2 = A_3 = \cdots = A_k = A,$$

and

$$B_1 = B_2 = \cdots = B_{k-1} = A, \qquad B_k = A \circ \mu,$$

applying Theorem 4.1 we conclude that

$$\nu\big(c(A))\big) = c(\nu \circ A) \subseteq c(A^{\circ 2}).$$

□

The next result is an extended version of the statement about the finiteness of $S(A)$.

Theorem 4.3. *Let A be a rational function of degree $n \geq 2$. Then the set $S(A)$ is finite and bounded in terms of n, unless A is a quasi-power. Furthermore, the set $S(A) \setminus \widehat{G}(A)$ is finite and bounded in terms of n, unless A is conjugate to $z^{\pm n}$.*

Proof. Since any Möbius transformation is defined by its values at any three points, the condition $\nu\big(c(A)\big) \subseteq c(A^{\circ 2})$ is satisfied only for finitely many Möbius transformations whenever A has at least three critical values, implying by Lemma 2.1 the finiteness of $S(A)$ in case if A is not a quasi-power. Moreover, since $|c(A)|$ and $|c(A^{\circ 2})|$ are bounded in terms of n, the set $S(A)$ is also bounded in terms of n.

If A is a quasi-power, but is not conjugate to $z^{\pm n}$, then its second iterate $A^{\circ 2}$ is not a quasi-power by Lemma 2.1, and the finiteness of $S(A) \setminus \widehat{G}(A)$ can be obtained by a modification of the proof of Theorem 4.2. Indeed, if σ belongs to $\widehat{G}(A^{\circ 2})$ or $\widehat{G}(A^{\circ 3})$, then $\nu\big(c(A^{\circ 2})\big) \subseteq c(A^{\circ 2})$ and $\nu\big(c(A^{\circ 3})\big) \subseteq c(A^{\circ 3})$, by Theorem 2.3. On the other hand, if σ belongs to $\widehat{G}(A^{\circ k})$ for some $k \geq 4$, then equality (24) implies the equality

$$\nu \circ A^{\circ 2k} = A^{\circ k} \circ \mu \circ A^{\circ k}, \quad k \geq 4.$$

Applying now Theorem 4.1 to equality (25) with

$$A_1 = \nu \circ A^{\circ 2}, \qquad A_2 = A_3 = \dots = A_k = A^{\circ 2},$$

and

$$B_1 = \dots = B_{\frac{k}{2}} = A^{\circ 2}, \quad B_{\frac{k}{2}+1} = \mu \circ A^{\circ 2}, \quad B_{\frac{k}{2}+2} = \dots = B_k = A^{\circ 2},$$

if k is even, or

$$B_1 = \dots = B_{\frac{k-1}{2}} = A^{\circ 2}, \quad B_{\frac{k-1}{2}+1} = A \circ \mu \circ A, \quad B_{\frac{k-1}{2}+2} = \dots = B_k = A^{\circ 2},$$

if k is odd, we conclude that $\nu\big(c(A^{\circ 2})\big) \subseteq c(A^{\circ 4})$. □

Finally, the next result is a corollary of Theorem 4.3.

Theorem 4.4. *Let A be a rational function of degree $n \geq 2$. Then the group $\mathrm{Aut}_\infty(A)$ is finite and bounded in terms of n, unless A is conjugate to $z^{\pm n}$.*

Proof. Since $\mathrm{Aut}(A^{\circ k})$, $k \geq 1$, is a subgroup of $\widehat{G}(A^{\circ k})$, $k \geq 1$, the boundedness of the set $\mathrm{Aut}_\infty(A) \setminus \mathrm{Aut}(A)$ in terms of n for A not conjugate to z^n follows from Theorem 4.3. On the other hand, it is easy to see that the group $\mathrm{Aut}(A)$ is always finite and bounded in terms of n. □

5. Groups $\Sigma_\infty(P)$

Recall that the group $\Sigma_\infty(A)$ is defined by the formula

$$\Sigma_\infty(A) = \cup_{k=1}^{\infty} \Sigma(A^{\circ k}).$$

Thus, $\Sigma_\infty(P)$ consists of Möbius transformations ν such that the equality

$$A^{\circ k} = A^{\circ k} \circ \sigma \tag{30}$$

holds for some $k \geq 1$. In this section, we prove analogues of Theorem 4.2 and Theorem 4.4 for the group $\Sigma_\infty(A)$. Then we prove an extended version of the statement about the groups $G(A^{\circ k})$, $k \geq 1$, from Theorem 1.1.

Let A and B be rational functions of degree at least two. Recall that the function B is said to be *semiconjugate* to the function A if there exists a non-constant rational function X such that

$$A \circ X = X \circ B. \tag{31}$$

A description of semiconjugate rational functions was obtained in the paper [17]. In particular, it was shown in [17] that solutions of (31) satisfying $\mathbb{C}(X, B) = \mathbb{C}(z)$, called *primitive*, can be described in terms of group actions on $\mathbb{CP}^1$ or $\mathbb{C}$, implying strong restrictions on a possible form of A, B and X.

Non-primitive solutions of (31) can be reduced to primitive one by *elementary transformations*. Let A be a rational function. We say that a rational function $\widetilde{A}$ is an elementary transformation of A if there exist rational functions U and V such that $A = U \circ V$ and $\widetilde{A} = V \circ U$. We say that rational functions A and A' are *equivalent* and write $A \sim A'$ if there exists a chain of elementary transformations between A and A'. Since for any Möbius transformation μ the equality

$$A = (A \circ \mu^{-1}) \circ \mu$$

holds, the equivalence class $[A]$ of a rational function A is a union of conjugacy classes. Moreover, the equivalence class $[A]$ contains only *finitely many* conjugacy classes, unless A is a flexible Lattès map (see [18]). We denote the number of conjugacy classes in the equivalence class $[A]$ by N_A.

Notice that for a rational function A, which is not a flexible Lattès map, describing the equivalence class $[A]$ comes down to describing functional decompositions of finitely many rational functions F. Thus, $[A]$ can be described effectively, at least for small degrees of A. Notice also that according to results of the recent paper [20], the problem of describing rational functions commuting with a given rational function A to a large extent reduces to describing the class $[A]$.

Example 5.1. Let us consider the function B from Example 2.5. The monodromy group of B is isomorphic to $V_4 = D_4$. It has three proper imprimitivity systems, and one can check that the corresponding decompositions of B are

$$B = \frac{z^2-1}{z^2+1} \circ \frac{z^2-1}{z^2+1}, \qquad B = -\frac{2}{z^2-2} \circ \frac{z^2+1}{z}, \qquad B = -\frac{2}{z^2+2} \circ \frac{z^2-1}{z}.$$

These decompositions provide us with the functions

$$B_1 = B = \frac{z^2-1}{z^2+1} \circ \frac{z^2-1}{z^2+1} = -\frac{2z^2}{z^4+1},$$

$$B_2 = \frac{z^2+1}{z} \circ -\frac{2}{z^2-2} = -\frac{1}{2}\,\frac{z^4-4\,z^2+8}{z^2-2},$$

$$B_3 = \frac{z^2-1}{z} \circ -\frac{2}{z^2+2} = \frac{1}{2}\,\frac{z^2\left(z^2+4\right)}{z^2+2}.$$

from the equivalence class $[B]$. Moreover, analyzing the monodromy groups of B_2 and B_3 one can show that the both groups have a unique proper imprimitivity system corresponding to the above decompositions, implying that the equivalence class $[B]$ contains exactly three conjugacy classes, which are represented by the functions B_1, B_2, and B_3 (see [20], Example 3, for more detail).

The connection between the relation $\sim$ and semiconjugacy is straightforward. Namely, for $\widetilde{A}$ and A as above we have:

$$\widetilde{A} \circ V = V \circ A, \qquad \text{and} \qquad A \circ U = U \circ \widetilde{A},$$

implying inductively that whenever $A \sim A'$ there exists X such that (31) holds, and there exists Y such that

$$A' \circ Y = Y \circ A$$

holds.

An arbitrary solution of equation (31) reduces to a primitive one by a sequence of elementary transformations as follows. By the Lüroth theorem, the field $\mathbb{C}(X, B)$ is generated by some rational function W. Therefore, if $\mathbb{C}(X, B) \neq \mathbb{C}(z)$, then there exists a rational function W of degree greater than one such that

$$B = \widetilde{B} \circ W, \quad X = \widetilde{X} \circ W \tag{32}$$

for some rational functions $\widetilde{X}$ and $\widetilde{B}$ satisfying $\mathbb{C}(\widetilde{X}, \widetilde{B}) = \mathbb{C}(z)$. Substituting now (32) in (31) we see that the triple $A, \widetilde{X}, W \circ \widetilde{B}$ is another solution of (31). This new solution is not necessary primitive, however $\deg \widetilde{X} < \deg X$, and hence after a finite number of similar transformations we will arrive to a primitive solution. Thus, for any solution A, X, B of (31) there exist rational functions X_0, B_0, U such that $X = X_0 \circ U$, the diagram

$$\begin{array}{ccc} \mathbb{CP}^1 & \xrightarrow{B} & \mathbb{CP}^1 \\ {\scriptstyle U}\downarrow & & \downarrow{\scriptstyle U} \\ \mathbb{CP}^1 & \xrightarrow{B_0} & \mathbb{CP}^1 \\ {\scriptstyle X_0}\downarrow & & \downarrow{\scriptstyle X_0} \\ \mathbb{CP}^1 & \xrightarrow{A} & \mathbb{CP}^1 \end{array} \tag{33}$$

commutes, the triple A, X_0, B_0 is a primitive solution of (31), and the rational function B_0 is obtained from the rational function B by a sequence of elementary transformations.

Theorem 5.2. *Let A be a rational function of degree $n \geq 2$. Then for any $\sigma \in \Sigma_\infty(A)$ the relation $A \circ \sigma \sim A$ holds.*

Proof. Let σ be an element of $\Sigma_\infty(A)$. Writing equality (30) as the semiconjugacy

$$\begin{array}{ccc} \mathbb{CP}^1 & \xrightarrow{A\circ\sigma} & \mathbb{CP}^1 \\ \downarrow{\scriptstyle A^{\circ(k-1)}} & & \downarrow{\scriptstyle A^{\circ(k-1)}} \\ \mathbb{CP}^1 & \xrightarrow{A} & \mathbb{CP}^1\,, \end{array} \tag{34}$$

we see that to prove the theorem it is enough to show that in diagram (33), constructed for the solution

$$A = A, \qquad X = A^{\circ(k-1)}, \qquad B = A \circ \sigma$$

of (31), the equality $\deg X_0 = 1$ holds. The proof of this fact is similar to the proof of Theorem 2.3 in [20] and relies on the following two facts. First, for any primitive solution A, X, B of (31), the solution $A^{\circ l}, X, B^{\circ l}$, $l \geq 1$, is also primitive (see [20], Lemma 2.5). Second, a solution A, X, B of (31) is primitive if and only if the algebraic curve

$$A(x) - X(y) = 0$$

is irreducible (see [20], Lemma 2.4).

Assume now that for the primitive solution A, X_0, B_0 of (31), provided by diagram (33) for the semiconjugacy (34), the inequality $\deg X_0 > 1$ holds. Then the triple $A^{\circ(k-1)}, X_0, B_0^{\circ(k-1)}$ is also a primitive solution of (31), and hence the algebraic curve

$$A^{\circ(k-1)}(x) - X_0(y) = 0 \tag{35}$$

is irreducible. However, the equality

$$A^{\circ(k-1)} = X_0 \circ U,$$

implies that the curve

$$U(x) - y = 0$$

is a component of (35). Moreover, the assumption $\deg X_0 > 1$ implies that this component is proper. The contradiction obtained proves the theorem. □

Theorem 5.3. *Let A be a rational function of degree $n \geq 2$. Then the order of the group $\Sigma_\infty(A)$ is finite and bounded in terms of n, unless A is conjugate to $z^{\pm n}$.*

Proof. Let us observe first that without loss of generality we may assume that A is not a quasi-power, and therefore that $G(A)$ is finite. Indeed, if A is a quasi-power but is not conjugate to $z^{\pm n}$, then $A^{\circ 2}$ is not a quasi-power by Lemma 2.1. Therefore, if the theorem is true for functions which are not quasi-powers, then for any A, which is not conjugate to $z^{\pm n}$, the group $\Sigma_\infty(A^{\circ 2})$ is finite and bounded in terms of n, implying by (4) that the same is true for the group $\Sigma_\infty(A)$.

Assume first that the number N_A is finite. Let us show that in this case the inequality

$$|\Sigma_\infty(A)| \leq |G(A)| N_A \tag{36}$$

holds. By Theorem 5.2, for any $\sigma \in \Sigma_\infty(A)$ the function $A \circ \sigma$ belongs to one of N_A conjugacy classes in the equivalence class $[A]$. Furthermore, if $A \circ \sigma_0$ and $A \circ \sigma$ belong to the same conjugacy class, then

$$A \circ \sigma = \alpha \circ A \circ \sigma_0 \circ \alpha^{-1}$$

for some $\alpha \in \mathrm{Aut}(\mathbb{CP}^1)$, implying that

$$A \circ \sigma \circ \alpha \circ \sigma_0^{-1} = \alpha \circ A.$$

This is possible only if α belongs to the group $\widehat{G}(P)$, and, in addition, $\sigma \circ \alpha \circ \sigma_0^{-1}$ belongs to the preimage of α under homomorphism (2). Therefore, for any fixed σ_0 there could be at most $|\widehat{G}(A)|$ such α, and for each α there could be at most $|\mathrm{Ker}\, \varphi_A|$ elements $\sigma \in G(A)$ such that

$$\varphi(\sigma \circ \alpha \circ \sigma_0^{-1}) = \alpha.$$

Thus, (36) follows from (11).

It is proved in [18] that N_A is infinite if and only if A is a flexible Lattès map. However, the proof given in [18] uses the theorem of McMullen ([14]) about isospectral rational functions, which is not effective. Therefore, the result of [18] does not imply that N_A is bounded in terms of n. Nevertheless, we can use the main result of [22], which states that for a given rational function B of degree n the number of conjugacy classes of rational functions A such that (31) holds for some rational function X is finite and bounded in terms of n, unless B is *special*, that is, unless B is either a Lattès map or it is conjugate to $z^{\pm n}$ or $\pm T_n$. Since $A \sim A'$ implies that A is semiconjugate to A', this result implies in particular that for a non-special A the number N_A is bounded in terms of n. Thus, in view of inequality (36), the theorem is true whenever A is not special.

To finish the proof we only must show that the group $\Sigma_\infty(A)$ is finite and bounded in terms of n if A is a Lattès map or is conjugate to $\pm T_n$. Using the explicit formula

$$T_n = \frac{n}{2} \sum_{k=0}^{[n/2]} (-1)^k \frac{(n-k-1)!}{k!(n-2k)!} (2x)^{n-2k},$$

it is easy to see that the group $\Sigma(\pm T_n)$ is either trivial or equal to C_2, depending on the parity of n. Therefore, since $T_n^{\circ k} = T_{n^{\circ k}}$, the order of $\Sigma_\infty(\pm T_n)$ is at most two.

Finally, assume that A is a Lattès map. There are several possible ways to characterize such maps, one of which is to postulate the existence of an orbifold $\mathcal{O} = (\mathbb{CP}^1, \nu)$ of zero Euler characteristic such that $A : \mathcal{O} \to \mathcal{O}$ is a covering map between orbifold (see [15], [19] for more detail). Since this implies that $A^{\circ k} : \mathcal{O} \to \mathcal{O}$, $k \geq 1$, also is a covering map (see [17], Corollary 4.1), equality (30) implies that $\sigma : \mathcal{O} \to \mathcal{O}$ is a covering map (see [17], Corollary 4.1 and Lemma 4.2). As σ is of degree one, the last condition simply means that σ permute points of the support of $\mathcal{O}$. Since the support of an orbifold $\mathcal{O} = (\mathbb{CP}^1, \nu)$ of zero Euler characteristic contains either three or four points, this implies that $\Sigma_\infty(A)$ is finite and uniformly bounded for any Lattès map A. This finishes the proof. □

The next result combined with the results of this and the precedent section finishes the proof of Theorem 1.1 from the introduction.

Theorem 5.4. *Let A be a rational function of degree $n \geq 2$. Then the sequence $G(A^{\circ k})$, $k \geq 1$, contains only finitely many non-isomorphic groups, and, unless A is a quasi-power, orders of these groups are finite and uniformly bounded in terms of n only. Furthermore, orders of $G(A^{\circ k})$, $k \geq 2$, are finite and uniformly bounded in terms of n only, unless A is conjugate to $z^{\pm n}$.*

Proof. By Theorem 4.3 and Theorem 5.3, the orders of the groups $\widehat{G}(A^{\circ k})$, $k \geq 1$, and $\Sigma(A^{\circ k})$, $k \geq 1$, are finite and uniformly bounded in terms of n only, unless A is a quasi-power. Therefore, by (11), the orders of the groups $G(A^{\circ k})$, $k \geq 1$, also are finite and uniformly bounded in terms of n only, unless A is a quasi-power. In particular, the sequence $G(A^{\circ k})$, $k \geq 1$, contains only finitely many non-isomorphic groups, since there exist only finitely many groups of any given order. In the same way, we obtain that the groups $G(A^{\circ k})$, $k \geq 2$, are finite and uniformly bounded in terms of n only, unless A is conjugate to $z^{\pm n}$.

Finally, even if A is a quasi-power, the first statement of the theorem remains true. Indeed, if A is not conjugate to $z^{\pm n}$, this is a corollary of the already proved part of the theorem. On the other hand, if A is conjugate to $z^{\pm n}$, then all the groups $G(A^{\circ k})$, $k \geq 1$, are isomorphic to the group $cz^{\pm 1}$, $c \in \mathbb{C} \setminus \{0\}$. □

We recall that a rational function A is called *indecomposable* if A cannot be represented as a composition of two rational functions of degree at least two. Thus, all decompositions of A reduce to the decompositions

$$A = (A \circ \mu) \circ \mu^{-1}, \qquad A = \mu \circ (\mu^{-1} \circ A),$$

where $\mu \in \mathbb{CP}^1$, implying that $N_A = 1$. We conclude this section with a result about the group $\Sigma_\infty(A)$ for an indecomposable A and some examples.

Theorem 5.5. *Let A be an indecomposable rational function of degree at least two. Then $\Sigma_\infty(A) = \Sigma(A)$ whenever the group $\widehat{G}(A)$ is trivial. In particular, the group $\Sigma_\infty(A)$ is trivial whenever the group $G(A)$ is trivial. Furthermore, the group $\Sigma_\infty(A)$ is trivial whenever $G(A) = \mathrm{Aut}(A)$.*

Proof. Assume that a Möbius transformation σ belongs to $\Sigma_\infty(A)$. Then by Theorem 5.2 the relation

$$A \circ \sigma \sim A \tag{37}$$

holds. On the other hand, since $N_A = 1$, condition (37) is equivalent to the condition that

$$A \circ \sigma = \beta \circ A \circ \beta^{-1} \tag{38}$$

for some $\beta \in \mathrm{Aut}(\mathbb{CP}^1)$. Clearly, equality (38) implies that β belongs to $\widehat{G}(A)$. Therefore, if $\widehat{G}(A)$ is trivial, then (38) is satisfied only if $A \circ \sigma = A$, that is, only if σ belongs to $\Sigma(A)$. Thus, $\Sigma(A) = \Sigma_\infty(A)$ whenever $\widehat{G}(A)$ is trivial.

Furthermore, it follows from equality (38) that $\sigma \circ \beta$ belongs to the preimage of β under the homomorphism (2). On the other hand, if $G(A) = \mathrm{Aut}(A)$, this preimage consists of β only. Therefore, in this case $\sigma \circ \beta = \beta$, implying that σ is the identical map. Thus, the group $\Sigma_\infty(A)$ is trivial whenever $G(A) = \mathrm{Aut}(A)$. □

Example 5.6. Let us consider the function

$$A = x + \frac{27}{x^3}.$$

In addition to the critical value ∞, it has critical values 4 and $4i$, whose ramifications are defined by the equalities

$$A - 4 = \frac{\left(x^2 + 2\,x + 3\right)(x-3)^2}{x^3},$$

$$A - 4i = \frac{\left(x^2 + 2\,ix - 3\right)(-x + 3\,i)^2}{x^3}.$$

Since the above equalities imply that the local multiplicity of A at the point zero is three, while at any other point of $\mathbb{CP}^1$ the local multiplicity of A is at most two, it follows from Theorem 2.6 that $G(A)$ is a cyclic group, whose generator has zero as a fixed point. Since $G(A)$ obviously contains the transformation $\sigma = -z$, the second fixed point of this generator must be infinity, implying easily that $G(A)$ is a cyclic group of order two. Clearly, $G(A) = \mathrm{Aut}(A)$. Moreover, since there is a point where the local multiplicity of A is three, it follows from the chain rule that the equality $A = A_1 \circ A_2$, where A_1 and A_2 are rational function of degree two is impossible. Therefore, A is indecomposable, and hence the group $\Sigma_\infty(A)$ is trivial by Theorem 5.5.

Example 5.7. Let us consider the quasi-power

$$A=\frac{z^2-1}{z^2+1}.$$

It is clear that $\Sigma(A)$ is a cyclic group of order two, generated by the transformation $z\to -z$. A calculation shows that the second iterate

$$A^{\circ 2}=-\frac{2z^2}{z^4+1}$$

is the function B from Example 2.5. Thus, $\Sigma(A^{\circ 2})$ is the dihedral group D_4, generated by the transformation $z\to -z$ and $z\to 1/z$. In particular, $\Sigma(A^{\circ 2})$ is larger than $\Sigma(A)$. Moreover, since

$$A^{\circ 3}=-\frac{\left(z^4-1\right)^2}{z^8+6\,z^4+1},$$

we see that $\Sigma(A^{\circ 3})$ contains the dihedral group D_8, generated by the transformation $\mu_1=iz$ and $\mu_2=1/z$, and hence $\Sigma(A^{\circ 3})$ is larger than $\Sigma(A^{\circ 2})$.

Let us show that

$$\Sigma_\infty(A)=\Sigma(A^{\circ 3})=D_8.$$

As in Example 2.5, we see that if $\Sigma_\infty(A)$ is larger than D_8, then either $\Sigma_\infty(A)=S_4$, or $\Sigma_\infty(A)$ is a dihedral group containing an element σ of order $l>4$, whose fixed points are zero and infinity. It is not hard to see that the first case is impossible. Indeed, let $k\geq 1$ be an index such that $\Sigma_\infty(A)=\Sigma(A^{\circ k})$, and let θ be an invariant rational function for the group $\Sigma_\infty(A)$. Then $A^{\circ k}$ is a rational function in θ, implying that $\deg A^{\circ k}$ is divisible by $\deg\theta$. Therefore, assuming that $\Sigma_\infty(A)=S_4$, we arrive at a contradictory conclusion that $\deg A^{\circ k}=2^k$ is divisible by

$$\deg\theta=|S_4|=24.$$

By Theorem 5.2, to prove that $\Sigma_\infty(A)$ cannot be a dihedral group larger than D_8, it is enough to show that if $\sigma=cz$, $c\in\mathbb{C}\setminus\{0\}$, satisfies

$$A\circ\sigma=\beta\circ A\circ\beta^{-1},\quad \beta\in \mathrm{Aut}(\mathbb{CP}^1),\tag{39}$$

then σ is a power of μ_1. Since critical points of the function in the left side of (39) coincide with critical points of the function in the right side, the Möbius transformation β necessarily has the form $\beta=dz^{\pm 1}$, $d\in\mathbb{C}\setminus\{0\}$. Thus, equation (39) reduces to the equations

$$\frac{c^2z^2-1}{c^2z^2+1}=\frac{1}{d}\frac{d^2z^2-1}{d^2z^2+1},$$

and

$$\frac{c^2z^2-1}{c^2z^2+1}=\frac{d\left(d^2+z^2\right)}{d^2-z^2}.$$

Solutions of the first equation are $d=1$ and $c=\pm 1$, while solutions of the second are $d=-1$ and $c=\pm i$. This proves the necessary statement.

Notice that instead of Theorem 5.2 it is also possible to use Theorem 1.2 (see Example 6.2 below).

6. Groups $G(A, z_0)$

Following [24], we say that a formal power series $f(z) = \sum_{i=1}^{\infty} a_i z^i$ having zero as a fixed point is *homozygous* mod l if the inequalities $a_i \neq 0$ and $a_j \neq 0$ imply the equality $i \equiv j (\text{mod } l)$. Obviously, this condition is equivalent to the condition that $f = z^r g(z^l)$ for some formal power series $g = \sum_{i=0}^{\infty} b_i z^i$ and integer r, $1 \leq r \leq l$. In particular, if f is homozygous mod l, then any iterate of f is homozygous mod l. If f is not homozygous mod l, it is called *hybrid* mod l. It is easy to see that unless $f = cz^r$, $c \in \mathbb{C}$, $r \geq 1$, there exists a number $N = N(f)$ such that f homozygous mod l if and only if l is a divisor of N.

The following result was proved by Reznick in the paper [24] by methods of local dynamics.

Theorem 6.1. *If a formal power series $f(z) = \sum_{i=1}^{\infty} a_i z^i$ is hybrid* mod l *and $f^{\circ k}$ is homozygous* mod l *then $f^{\circ ks}(z) = z$ for some integer $s \geq 1$.*

Let z_0 be a fixed point of a rational function A, and z_1 a point of $\mathbb{CP}^1$ distinct from z_0. We recall that the group $G(A, z_0, z_1)$ is defined as the subgroup of $G(A)$ consisting of Möbius transformations σ such that $\sigma(z_0) = z_0$, $\sigma(z_1) = z_1$, and $\nu_\sigma = \sigma^{\circ k}$ for some $k \geq 1$. Clearly, the definition implies that

$$G(A, z_0, z_1) \subseteq G(A^{\circ k}, z_0, z_1), \quad k \geq 1,$$

while Theorem 1.2 from the introduction states that in fact all the inclusions above are equalities.

Proof of Theorem 1.2. If $A = z^n$, then the theorem is true, since the groups $G(A^{\circ k}, z_0, z_1)$, $k \geq 1$, are trivial, unless $\{z_0, z_1\} = \{0, \infty\}$, while all the groups $G(A^{\circ k}, 0, \infty)$, $k \geq 1$, coincide with the group cz, $c \in \mathbb{C} \setminus \{0\}$. Therefore, we can assume that A is not conjugate to z^n. In addition, without loss of generality, we can assume that $z_0 = 0$, $z_1 = \infty$.

Let us observe that

$$|G(A, 0, \infty)| = N(f_A), \tag{40}$$

where f_A stands for the Taylor series of the function A at zero. Indeed, $N(f_A)$ is equal to the number of roots of unity ε such that

$$f_A(\varepsilon z) = \varepsilon^k f_A(z)$$

for some $k \geq 1$ in the ring of formal series. However, since f_A converges in a neighborhood U of zero, this number equals to the number of roots of unity ε such that

$$A(\varepsilon z) = \varepsilon^k A(z)$$

in U. Finally, by the analytical continuation, the last number coincides with the number $d(A)$.

Since $f_{A^{\circ k}} = f_A^{\circ k}$, it follows from (40) that if $G(A, 0, \infty) = C_e$, $e \geq 1$, while $G(A^{\circ k}, 0, \infty) = C_l$, $l \geq 1$, where l is a proper multiple of e, then f_A is hybrid mod l, while $f_A^{\circ k}$ is homozygous mod l. Therefore, by Theorem 6.1, the equality $f_A^{\circ ks} = z$ holds for some $s \geq 1$. However, this is impossible since the local equality $A^{\circ ks} = z$ implies by the analytical continuation that $A^{\circ ks} = z$ globally, in contradiction with the assumption that $n \geq 2$. $\square$

Let us emphasize that since the iterates $A^{\circ k}$, $k>1$, have in general more fixed points than A, it may happen that $G(A^{\circ k}, z_0, z_1)$, $k>1$, is non-trivial, while $G(A, z_0, z_1)$ is *not defined*, so that the equality $G(A^{\circ k}, z_0, z_1) = G(A, z_0, z_1)$ does not make sense.

Example 6.2. Let us consider the function

$$A = \frac{z^2-1}{z^2+1}$$

from Example 5.7. Clearly, zero is not a fixed point for A and hence the group $G(A, 0, \infty)$ is not defined. However, zero is a fixed point for

$$A^{\circ 2} = -\frac{2z^2}{z^4+1},$$

and the group $G(A^{\circ 2}, 0, \infty)$ is a cyclic group of order four.

The rational function A provides a counterexample to the generalization of Theorem 3.4 to rational functions. Indeed, since

$$A = \frac{z-1}{z+1} \circ z^2,$$

the group $G(A)$ consists of the transformations $cz^{\pm 1}$, $c \in \mathbb{C} \setminus \{0\}$, implying easily that the set $\Gamma(A)$ contains only the functions $\pm z$. On the other hand, $\Gamma(A^{\circ 2})$ contains the group $G(A^{\circ 2}, 0, \infty) = C_4$.

In addition, on the example of the function A one can see that the statement about polynomials, used in the second proof of Theorem 3.4, is not true for rational functions. Indeed, A is not conjugate to z^2, and $A^{\circ 2}$ has the form $z^2 Q(z^4)$, where $Q \in \mathbb{C}(z)$. However, A cannot be represented in the form $z^r R(z^4)$, where $R \in \mathbb{C}(z)$ and $r \geq 0$.

Finally, notice that Theorem 1.2 can be used to obtain another proof of the fact that the group $\Sigma_\infty(A)$ cannot contain an element $\sigma = cz$, $c \in \mathbb{C} \setminus \{0\}$, of order $l>4$, given in Example 5.7. Indeed, such σ would belong to the group $G(A^{\circ k}, 0, \infty)$ for some $k \geq 1$, and hence to the group $G(A^{\circ 2k}, 0, \infty)$. However, $G(A^{\circ 2k}, 0, \infty)$ is equal to $G(A^{\circ 2}, 0, \infty) = C_4$ by Theorem 1.2 applied to $A^{\circ 2}$.

Theorem 1.2 implies the following result, which in some cases permits to estimate the orders of $\mathrm{Aut}_\infty(A)$ and $\Sigma_\infty(A)$, and even to describe these groups explicitly.

Theorem 6.3. *Let A be a rational function of degree at least two, not conjugate to $z^{\pm n}$. Assume that for some $k \geq 1$ the group $\mathrm{Aut}(A^{\circ k})$ contains an element σ of order $l>5$ with fixed points z_0, z_1 such that z_0 is a fixed point of $A^{\circ k}$. Then $|\mathrm{Aut}_\infty(A)| \leq 2|G(A^{\circ k}, z_0, z_1)|$. Similarly, if the group $\Sigma(A^{\circ k})$ contains an element σ satisfying the above properties, then $|\Sigma_\infty(A)| \leq 2|G(A^{\circ k}, z_0, z_1)|$.*

Proof. Since the maximal order of a cyclic subgroup in the groups A_4, S_4, A_5 is five, it follows from Theorem 4.4 that if $\mathrm{Aut}(A^{\circ k})$ contains an element σ of order $l>5$, then either $\mathrm{Aut}_\infty(A) = C_r$ or $\mathrm{Aut}_\infty(A) = D_{2r}$, where $l|r$. Moreover, fixed points of σ coincide with fixed points of the element of order r in $\mathrm{Aut}_\infty(A)$. We denote this element by σ_∞.

To prove the theorem we must show that $r \leq |G(A^{\circ k}, z_0, z_1)|$. Since the transformation σ_∞ belongs to $\mathrm{Aut}(A^{\circ k'})$ for some $k' \geq 1$, it belongs to $G(A^{\circ kk'}, z_0, z_1)$.

Therefore, if $r > |G(A^{\circ k}, z_0, z_1)|$, then the group $G(A^{\circ kk'}, z_0, z_1)$ contains an element of order greater than $|G(A^{\circ k}, z_0, z_1)|$, in contradiction with the equality

$$G(A^{\circ kk'}, z_0, z_1) = G(A^{\circ k}, z_0, z_1),$$

provided by Theorem 1.2 applied to $G(A^{\circ k})$. The proof of the estimate for $|\Sigma_\infty(A)|$ is similar. □

Example 6.4. Let us consider the function

$$A = z\frac{z^6 - 2}{2z^6 - 1}.$$

It is easy to see that $\mathrm{Aut}(A)$ contains the dihedral group D_{12}, generated by the transformations

$$z \to e^{\frac{2\pi i}{6}} z, \qquad z \to 1/z.$$

Since $G(A, 0, \infty) = C_6$ and zero is a fixed point of A, it follows from Theorem 6.3 that

$$\mathrm{Aut}_\infty(A) = \mathrm{Aut}(A) = D_{12}.$$

It is clear that for any fixed point z_0 of $A^{\circ k}$, $k \geq 1$, and $z_1 \in \mathbb{CP}^1$ the group $G(A^{\circ k}, z_0, z_1)$ belongs to the set $\Gamma(A^{\circ k})$. However, it is not true in general that any element of $\Gamma(A^{\circ k})$, $k \geq 1$, belongs to $G(A^{\circ k}, z_0, z_1)$ for some z_0, z_1, since equality (19) does not necessary imply that a fixed point of σ is a fixed point of $A^{\circ k}$. For example, for any rational function A of the form $A = R(z^d)$, where $d \geq 2$ and $R \in \mathbb{C}(z)$, the group $\Sigma(A) \subseteq \Gamma(A)$ contains the cyclic group generated by the transformation $z \to e^{\frac{2\pi i}{d}} z$. However, elements of this group do not belong to $G(A, z_0, z_1)$, unless zero or infinity is a fixed point of R. Nevertheless, the following statement holds.

Lemma 6.5. *Let A be a rational function of degree $n \geq 2$, and $\sigma \in \Gamma(A^{\circ k}) \backslash \Sigma(A^{\circ k})$. Then at least one of fixed points z_0, z_1 of σ is a fixed point of $A^{\circ 2k}$, and, if z_0 is such a point, then $\sigma \in G(A^{\circ 2k}, z_0, z_1)$.*

Proof. Let z_0, z_1 be fixed points of σ satisfying (19). Since $\sigma^{\circ l}$ is not the identical map, (19) implies that

$$A^{\circ k}\{z_0, z_1\} \subseteq \{z_0, z_1\}.$$

Therefore, at least one of the points z_0, z_1 is a fixed point of $A^{\circ 2k}$, and, if z_0 is such a point, then $\sigma \in G(A^{\circ 2k}, z_0, z_1)$ since $G(A^{\circ k}, z_0, z_1) \subseteq G(A^{\circ 2k}, z_0, z_1)$. □

To illustrate Lemma 6.5, consider the function

$$A = z\frac{z^2 - 2}{2z^2 - 1}$$

and the transformation $\sigma = 1/z$ which belongs to $\mathrm{Aut}(A)$. The fixed points ± 1 of σ are not fixed points of A, but they are fixed points of the second iterate $A^{\circ 2}$.

Finally, combining Theorem 6.3 with Lemma 6.5 we obtain the following result.

Theorem 6.6. *Let A be a rational function of degree at least two, not conjugate to $z^{\pm n}$. Assume that for some $k \geq 1$ the group $\mathrm{Aut}(A^{\circ k})$ contains an element σ of order $l > 5$ with fixed points z_0, z_1. Then $|\mathrm{Aut}_\infty(A)| \leq 2|G(A^{\circ 2k}, z_0, z_1)|$, where z_0 is a fixed point of σ, which is also a fixed point of $A^{\circ 2k}$.* □

7. Rational functions sharing an iterate

In this section, we prove Theorem 1.3. Our proof is based on the result from [23], which states roughly speaking that if a rational function X is "a compositional left factor" of *some* iterate of a rational function A, then X is already a compositional left factor of $A^{\circ N}$, where N is bounded in terms of degrees of A and X. More precisely, the following statement holds ([23]).

Theorem 7.1. *There exists a function $\varphi : \mathbb{N} \times \mathbb{N} \to \mathbb{R}$ with the following property. For any rational functions A and X such that the equality*

$$A^{\circ r} = X \circ R \tag{41}$$

holds for some rational function R and $r \geq 1$, there exist $N \leq \varphi(\deg A, \deg X)$ and a rational function R' such that

$$A^{\circ N} = X \circ R'$$

and $R = R' \circ A^{\circ(r-N)}$, if $r > N$. In particular, for every positive integer d, up to the change $X \to X \circ \mu$, where μ is a Möbius transformation, there exist at most finitely many rational functions X of degree d such that (41) holds for some rational function R and $r \geq 1$.

Before proving Theorem 1.3 we prove the following two statements of independent interest.

Theorem 7.2. *Let X be a rational function of degree at least two, and ν a Möbius transformation. Then $\nu \circ X$ shares an iterate with X if and only if $\nu \in \mathrm{Aut}_\infty(X)$.*

Proof. Assume that

$$X^{\circ k} \circ \nu = \nu \circ X^{\circ k}$$

for some $k \geq 1$. Then for any $l \geq 1$ the equality

$$(\nu \circ X)^{\circ kl} = \nu^{\circ l} \circ X^{\circ kl}$$

holds. Since ν has finite order by Theorem 4.4, this implies that

$$(\nu \circ X)^{\circ kr} = X^{\circ kr},$$

where r is the order of ν.

Assume now that

$$(\nu \circ X)^{\circ k} = X^{\circ k}, \qquad k \geq 1. \tag{42}$$

Clearly, equality (42) implies the equality

$$(\nu \circ X)^{\circ(k-1)} \circ \nu = X^{\circ(k-1)}, \qquad k \geq 1. \tag{43}$$

Composing now X with the both parts of equality (43), we obtain the equality

$$(X \circ \nu)^{\circ k} = X^{\circ k}, \qquad k \geq 1. \tag{44}$$

Finally, using (42) and (44), we have:

$$X^{\circ k} \circ \nu = (\nu \circ X)^{\circ k} \circ \nu = \nu \circ (X \circ \nu)^{\circ k} = \nu \circ X^{\circ k},$$

implying that

$$\nu \in \mathrm{Aut}(X^{\circ k}) \subseteq \mathrm{Aut}_\infty(A).$$

□

Theorem 7.3. *Let X be a rational function of degree $d \geq 2$ not conjugate to $z^{\pm d}$. Then the number of Möbius transformations ν such that X and $\nu \circ X$ share an iterate is finite and bounded in terms of d. Similarly, the number of Möbius transformations μ such that X and $X \circ \mu$ share an iterate is finite and bounded in terms of d.*

Proof. The first part of the theorem follows from Theorem 7.2 and Theorem 4.4. Assume now that μ_i, $1 \leq i \leq N$, are distinct Möbius transformations such that

$$X^{\circ n_i} = (X \circ \mu_i)^{\circ n_i}$$

for some n_i, $1 \leq i \leq N$. Clearly, this implies that

$$X^{\circ M} = (X \circ \mu_i)^{\circ M}, \qquad 1 \leq i \leq N,$$

where $M = \mathrm{LCM}(n_1, n_2, \dots, n_N)$. Therefore,

$$(X \circ \mu_i)^{\circ M} \circ X = X^{\circ (M+1)}, \qquad 1 \leq i \leq N,$$

and hence

$$X \circ (\mu_1 \circ X)^{\circ M} = X \circ (\mu_2 \circ X)^{\circ M} = \dots = X \circ (\mu_N \circ X)^{\circ M}. \tag{45}$$

Since the preimage $X^{-1}\{z_0\}$, $z_0 \in \mathbb{CP}^1$, contains at most d distinct points, equality (45) yields that among rational functions $(\mu_i \circ X)^{\circ M}$, $1 \leq i \leq N$, there are at most d distinct. On the other hand, it follows from the first part of the theorem that for any fixed $\mu_0 \in \mathrm{Aut}(\mathbb{CP}^1)$ the number of $\mu \in \mathrm{Aut}(\mathbb{CP}^1)$ such that

$$(\mu \circ X)^{\circ M} = (\mu_0 \circ X)^{\circ M}$$

is finite and bounded by some constant $s = s(d)$ depending on d only. Thus, the number N satisfies the estimate $N \leq s(d)d$. □

Proof of Theorem 1.3. By Theorem 7.1, there exist finitely many rational functions $X_1, X_2, \dots, X_s$ of degree d, where $s = s(n, d)$ depends on n and d only, such that, whenever a rational function B of degree d shares an iterate with A, there exists i, $1 \leq i \leq s$, such that $B = X_i \circ \mu$ for some $\mu \in \mathrm{Aut}(\mathbb{CP}^1)$. Changing X_i to $X_i \circ \mu$ for some μ such that $X_i \circ \mu$ shares an iterate with A, without loss of generality we may assume that $X_1, X_2, \dots, X_s$ share an iterate with A. Since A shares an iterate with a function conjugate to $z^{\pm d}$, if and only if A is conjugate to $z^{\pm n}$, the functions $X_1, X_2, \dots, X_s$ are not conjugate to $z^{\pm d}$.

Since any two rational functions sharing an iterate with A share an iterate between themselves, it follows from the second part of Theorem 7.3 that for any fixed X_i, $1 \leq i \leq s$, there are at most $k = k(d)$ Möbius transformations μ such that X_i and $X_i \circ \mu$ share an iterate with A. Therefore, the number of rational functions of degree d sharing an iterate with A is at most $s(n, d)k(d)$. □

References

1. P. Atela, J. Hu, *Commuting polynomials and polynomials with same Julia set,* Internat. J. Bifur. Chaos Appl. Sci. Engrg. 6 (1996), no. 12A, 2427–2432
2. I. Baker, A. Eremenko, *A problem on Julia sets,* Ann. Acad. Sci. Fennicae (series A.I. Math.) 12 (1987), 229–236.
3. A. Beardon, *Symmetries of Julia sets,* Bull. Lond. Math. Soc. 22, No.6, 576-582 (1990).
4. A. Beardon, *Polynomials with identical Julia sets,* Complex Variables, Theory Appl. 17, No.3-4, 195-200 (1992).

5. D. Boyd, *Translation invariant Julia sets,* Proc. Amer. Math. Soc. 128 (2000), no. 3, 803-812.
6. C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras,* Pure and Appl. Math., vol. 11, Interscience, New York, 1962.
7. P. Doyle, C. McMullen, *Solving the quintic by iteration,* Acta Math. 163 (1989), no. 3-4, 151-180.
8. H. Engstrom, *Polynomial substitutions,* Amer. J. Math. 63, 249-255 (1941).
9. A. Freire, A. Lopes, R. Mañé, *An invariant measure for rational maps*, Bol. Soc. Brasil. Mat. 14 (1983), no. 1, 45-62.
10. G. Levin, *Symmetries on Julia sets,* Math. Notes 48 (1990), no. 5-6, 1126-1131.
11. G. Levin, *Letter to the editors*, Math. Notes 69 (2001), no. 3-4, 432-33.
12. G. Levin, F. Przytycki, *When do two rational functions have the same Julia set?*, Proc. Amer. Math. Soc. 125 (1997), no. 7, 2179-2190.
13. M. Ljubich, *Entropy properties of rational endomorphisms of the Riemann sphere*, Ergodic Theory Dynam. Systems 3 (1983), no. 3, 351-385.
14. C. McMullen, *Families of rational maps and iterative root-finding algorithms,* Ann. of Math., 125, No. 3 (1987), 467-493.
15. J. Milnor, *On Lattès maps,* Dynamics on the Riemann Sphere. Eds. P. Hjorth and C. L. Petersen. A Bodil Branner Festschrift, European Mathematical Society, 2006, pp. 9-43.
16. F. Pakovich, *On polynomials sharing preimages of compact sets, and related questions*, Geom. Funct. Anal., 18, No. 1, 163-183 (2008).
17. F. Pakovich, *On semiconjugate rational functions,* Geom. Funct. Anal., 26 (2016), 1217-1243.
18. F. Pakovich, *Recomposing rational functions,* Int. Math. Res. Not., 2019, no. 7, 1921-1935.
19. F. Pakovich, *On generalized Latès maps,* J. Anal. Math., accepted.
20. F. Pakovich, *Commuting rational functions revisited*, Ergodic Theory Dynam. Systems, accepted.
21. F. Pakovich, *On rational functions sharing the measure of maximal entropy*, Arnold Math. J., accepted.
22. F. Pakovich, *Finiteness theorems for commuting and semiconjugate rational functions,* arxiv:1604:04771.
23. F. Pakovich, *Invariant curves for endomorphisms of* $\mathbb{P}^1 \times \mathbb{P}^1$, arxiv:1904:10952.
24. B. Reznick, *When is the iterate of a formal power series odd?*, J. Austral. Math. Soc. Ser. A 28 (1979), no. 1, 62-66.
25. W. Schmidt, N. Steinmetz, *The polynomials associated with a Julia set,* Bull. London Math. Soc. 27 (1995), no. 3, 239–241.
26. H. Ye, *Rational functions with identical measure of maximal entropy*, Adv. Math. 268 (2015), 373-395.

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