ON SYMMETRIES OF ITERATES OF RATIONAL FUNCTIONS

FEDOR PAKOVICH

Abstract. Let A be a rational function of degree $n \geqslant 2$. Let us 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 $\mathrm{Aut}(A)$ the subgroups of $G(A)$, consisting of σ such that $A \circ \sigma = A$ and $A \circ \sigma = \sigma \circ A$, correspondingly. A dynamical system defined by iterating A gives rise sequences of the above groups, and in this paper we study these sequences. In particular, we show that if A is not conjugate to $z^{\pm n}$, then the sequence $G(A^{\circ k})$, $k \geqslant 2$, contains only finitely many non-isomorphic groups, and the orders of these groups are uniformly bounded in terms of n only. We also prove a number of results about the groups $\Sigma_\infty(A) = \cup_{k=1}^{\infty} \Sigma(A^{\circ k})$ and $\mathrm{Aut}_\infty(A) = \cup_{k=1}^{\infty} \mathrm{Aut}(A^{\circ k})$, which are especially interesting from the dynamical perspective.

1. Introduction

Let A be a rational function of degree $n \geqslant 2$. In this paper, we study a variety of different subgroups of $\mathrm{Aut}(\mathbb{CP}^1)$ related to A, and more generally to a dynamical system defined by iterating 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 $A^{\circ k}$, $k \geqslant 1$, while elements of $\mathrm{Aut}(A)$ permute fixed points of $A^{\circ k}$, $k \geqslant 1$. 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 [15] 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 and No. 1092/22.

In this paper, we study 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.* 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 theorem of Levin ([5], [6]) about rational functions sharing the measure of maximal entropy. However, the Levin theorem does 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 in this direction. More generally, we study the totality of the groups $G(A^{\circ k})$, $k \geqslant 1$, defined by iterating A.

Our main result can be formulated as follows.

Theorem 1.1. *Let A be a rational function of degree $n \geqslant 2$ that is not conjugate to $z^{\pm n}$. Then the sequence $G(A^{\circ k})$, $k \geqslant 2$, contains only finitely many non-isomorphic groups. Furthermore, the orders of these groups are finite and uniformly bounded in terms of n only.*

We also prove a number of results about the groups $\Sigma_\infty(A)$ and $\mathrm{Aut}_\infty(A)$ allowing us in certain cases to calculate these groups explicitly. For a rational function A, let us denote by $c(A)$ the set of its critical values. Our main result about the groups $\mathrm{Aut}_\infty(A)$ is following.

Theorem 1.2. *Let A be a rational function of degree $n \geqslant 2$ that is not conjugate to $z^{\pm n}$. Then every $\nu \in \mathrm{Aut}_\infty(A)$ maps the set $c(A)$ to the set $c(A^{\circ 2})$. Furthermore, the group $\mathrm{Aut}_\infty(A)$ is finite and its order is bounded in terms of n only.*

Notice that since Möbius transformations ν such that

$$\nu\big(c(A)\big) \subseteq c(A^{\circ 2}) \tag{5}$$

can be described explicitly, Theorem 1.2 provides us with a concrete finite subset of $\mathrm{Aut}(\mathbb{CP}^1)$ containing the group $\mathrm{Aut}_\infty(A)$.

To formulate our main results concerning groups $\Sigma(A)$, let us introduce some definitions. Let A be a rational function. Then a rational function $\widetilde{A}$ is called an *elementary transformation* of A if there exist rational functions U and V such that

$$A = U \circ V \quad \text{and} \quad \widetilde{A} = V \circ U. \tag{6}$$

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

$$A = (A \circ \mu^{-1}) \circ \mu \tag{7}$$

holds, the equivalence class $[A]$ of a rational function A is a union of conjugacy classes. Moreover, by the results of the papers [12], [15], the number of conjugacy classes in $[A]$ is finite, unless A is a flexible Lattès map.

In this notation, our main result about the groups $\Sigma_\infty(A)$ is following.

Theorem 1.3. *Let A be a rational function of degree $n \geqslant 2$ that is not conjugate to $z^{\pm n}$. Then for every $\sigma \in \Sigma_\infty(A)$ the relation $A \circ \sigma \sim A$ holds. Moreover, the order of the group $\Sigma_\infty(A)$ is finite and bounded in terms of n only.*

Notice that in some cases Theorem 1.3 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, the number of conjugacy classes in the equivalence class $[A]$ obviously is equal to one, and Theorem 1.3 implies the following statement.

Theorem 1.4. *Let A be an indecomposable rational function of degree $n \geqslant 2$ that is not conjugate to $z^{\pm n}$. Then $\Sigma_\infty(A) = \Sigma(A)$, whenever the group $\widehat{G}(A)$ is trivial. Furthermore, the group $\Sigma_\infty(A)$ is trivial, whenever $G(A) = \mathrm{Aut}(A)$.*

Notice that Theorem 1.4 implies in particular that if A is indecomposable and the group $G(A)$ is trivial, then $\Sigma_\infty(A)$ is also trivial.

Finally, along with the groups $G(A^{\circ k})$, $k \geqslant 1$, 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. Let us 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

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

for some $l \geqslant 1$. We prove the following statement.

Theorem 1.5. *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 $k \geqslant 1$.*

Notice that every element $\sigma \in \mathrm{Aut}(A^{\circ k})$, $k \geqslant 1$, belongs to $G(A^{\circ 2k}, z_0, z_1)$ for some z_0, z_1. Indeed, the equality

$$A^{\circ k} \circ \sigma = \sigma \circ A^{\circ k}, \qquad k \geqslant 1,$$

implies that $A^{\circ k}$ sends the set of fixed points of σ to itself. Therefore, at least one of these points z_0, z_1 is a fixed point of $A^{\circ 2k}$, and, if z_0 is such a point, then $\sigma \in G(A^{\circ 2k}, z_0, z_1)$. In view of this relation between $\mathrm{Aut}(A^{\circ k})$ and $G(A^{\circ 2k}, z_0, z_1)$, Theorem 1.5 allows us in some cases to estimate the order of the group $\mathrm{Aut}_\infty(A)$ and even to describe this group explicitly.

The paper is organized as follows. In the second section, we establish basic properties of the group $G(A)$. 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 briefly discuss relations between the groups $\Sigma_\infty(A)$, $\mathrm{Aut}_\infty(A)$ and the measure of maximal entropy for A. In particular, we deduce the finiteness of these groups from the results of Levin ([5], [6]),

In the fourth section, we prove Theorem 1.2. Moreover, we prove that (5) holds for any Möbius transformation ν that belongs to $\widehat{G}(A^{\circ k})$ for some $k \geqslant 1$. In the fifth section, using results about semiconjugate rational functions from the papers [11], [15], we prove Theorem 1.3 and Theorem 1.4. We also prove a slightly more general version of Theorem 1.1. Finally, in the sixth section, we deduce Theorem 1.5 from the result of Reznick ([17]) about iterates of formal power series, and provide some applications of Theorem 1.5 concerning the groups $\mathrm{Aut}_\infty(A)$ and $\Sigma_\infty(A)$.

2. Groups $G(A)$

Let A be a rational function of degree $n \geqslant 2$, and $G(A)$, $\widehat{G}(A)$, $\Sigma(A)$, $\mathrm{Aut}(A)$ the groups defined in the introduction. 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

$$G(A') = \beta^{-1} \circ G(A) \circ \beta, \qquad \widehat{G}(A') = \alpha \circ \widehat{G}(A) \circ \alpha^{-1}. \tag{8}$$

In particular, the groups $G(A)$ and $G(A')$ are isomorphic. Notice also that since

$$\widehat{G}(A) \cong G(A)/\Sigma(A), \tag{9}$$

the equality

$$|G(A)| = |\widehat{G}(A)||\Sigma(A)| \tag{10}$$

holds whenever $G(A)$ is finite.

Lemma 2.1. *Let A be a rational function of degree $n \geqslant 2$. Then the following statements are true.*

- *i) For every $z \in \mathbb{CP}^1$ and $\sigma \in G(A)$ the multiplicity of A at z is equal to the multiplicity of A at $\sigma(z)$.*
- *ii) For every $c \in \mathbb{CP}^1$ and $\sigma \in G(A)$ the fiber $A^{-1}\{c\}$ is mapped to the fiber $A^{-1}\{\nu_\sigma(c)\}$ by σ.*
- *iii) Every $\nu \in \widehat{G}(A)$ maps $c(A)$ to $c(A)$.*

Proof. Since (1) implies that

$$\mathrm{mult}_{\sigma(z)}(A) \cdot \mathrm{mult}_z(\sigma) = \mathrm{mult}_{A(z)}(\nu) \cdot \mathrm{mult}_z(A)$$

the first statement follows from the fact that σ and ν are one-to-one.

Further, it is clear that (1) implies

$$\sigma^{-1}(A^{-1}(c)) = A^{-1}(\nu_\sigma^{-1}(c)).$$

Changing now σ^{-1} to σ and taking into account that $\nu_\sigma^{-1} = \nu_{\sigma^{-1}}$, we obtain the second statement.

Finally, the third statement follows from the second one, taking into account that

$$|A^{-1}\{c\}| = |A^{-1}\{\nu_\sigma(c)\}|$$

since σ is one-to-one and that c is a critical value of A if and only $|A^{-1}\{c\}| < n$. $\square$

We say that a rational function A of degree $n \geqslant 2$ is *a quasi-power* if there exist $\alpha, \beta \in \mathrm{Aut}(\mathbb{CP}^1)$ such that

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

It is easy to see using Lemma 2.1 that the group $G(z^n)$ consists of the transformations $z \to cz^{\pm 1}$, $c \in \mathbb{C}\backslash\{0\}$. Therefore, by (8), for any quasi-power A the groups $G(A)$ and $\widehat{G}(A)$ are infinite.

Lemma 2.2. *A rational function A of degree $n \geqslant 2$ 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 the function

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

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

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

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

Let G be a finite subgroup of $\mathrm{Aut}(\mathbb{CP}^1)$. We 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. Invariant functions for finite subgroups of $\mathrm{Aut}(\mathbb{CP}^1)$ were first found by Klein in his book [4].

Theorem 2.3. *Let A be a rational function of degree $n \geqslant 2$. Then $|\Sigma(A)|$ is a divisor of n. Moreover, $|\Sigma(A)| = n$ if and only if A is an invariant function for $\Sigma(A)$.*

Proof. It is easy to see that for a finite subgroup G of $\mathrm{Aut}(\mathbb{CP}^1)$ the set of rational functions F such that $F \circ \sigma = F$ for every $\sigma \in G$ is a subfield of $\mathbb{C}(z)$. Therefore, by the Lüroth theorem, any such a function F is a rational function in θ_G, implying that $\deg F$ is divisible by $|G|$. In particular, setting $G = \Sigma(A)$, we see that the degree of A is divisible by $|\Sigma(A)|$. Moreover, $\deg A = |\Sigma(A)|$ if and only if A is an invariant function for $\Sigma(A)$. □

The existence of invariant functions implies that for every finite subgroup G of $\mathrm{Aut}(\mathbb{CP}^1)$ there exist rational functions for which $\Sigma(A) = G$. Similarly, for every finite subgroup G of $\mathrm{Aut}(\mathbb{CP}^1)$ there exist rational functions for which $\mathrm{Aut}(A) = G$. A description of such functions in terms of homogenous invariant polynomials for G was obtained by Doyle and McMullen in [2]. Notice that rational functions with non-trivial automorphism groups are closely related to *generalized Lattès maps* (see [13] for more detail and examples).

The following result was proved in [15]. For the reader convenience we provide a simpler proof.

Theorem 2.4. *Let A be a rational function of degree $n \geqslant 2$ that is not a quasi-power. Then the group $G(A)$ is isomorphic to 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, $|G(A)| \leqslant \max\{60, 2n\}$.*

Proof. Any 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 $\lambda \in \mathbb{C}\setminus\{0\}$. 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 equality

$$A(z + 1) = \lambda A(z), \qquad \lambda \in \mathbb{C}\setminus\{0\}, \tag{11}$$

is impossible. Indeed, if A has a finite pole, then (11) implies that A has infinitely many poles. On the other hand, if A does not have finite poles, then A has a finite zero, and (11) implies that A has infinitely many zeroes. Similarly, the equality

$$A(z+1) = A(z) + 1 \tag{12}$$

is impossible if A has a finite pole. On the other hand, if A is a polynomial of degree $n \geqslant 2$, then we obtain a contradiction comparing the coefficients of z^{n-1} in left and the right sides of equality (12).

For the argument below, instead of considering A as a ratio of two polynomials, it is more convenient to assume that A is represented by its convergent Laurent series at zero or infinity. Comparing for such a representation the free terms in of the left and the right sides of the equality

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

we conclude that this equality is impossible either. Thus, equality (1) for a non-identical σ reduces to the equality

$$A(\lambda_1 z) = \lambda_2 A(z), \quad \lambda_1 \in \mathbb{C}\backslash\{0, 1\}, \quad \lambda_2 \in \mathbb{C}\backslash\{0\}. \tag{13}$$

Comparing now coefficients in the left and the right sides of (13) and taking into account that $A \neq az^{\pm n}$, $a \in \mathbb{C}$, by the assumption, we conclude that λ_1 is a root of unity. Furthermore, if d is the order of λ_1, then $\lambda_2 = \lambda_1^r$ for some $0 \leqslant r \leqslant d-1$, implying that A/z^r is a rational function in z^d. On the other hand, it is easy to see that if $A = z^r R(z^d)$, where $R \in \mathbb{C}(z)$ and $0 \leqslant r \leqslant d-1$, then $d \leqslant n$, unless either $R \in \mathbb{C}\backslash\{0\}$ or $R = a/z^d$ for some $a \in \mathbb{C}\backslash\{0\}$. Since for such R the function A is a quasi-power, we conclude that the order of λ_1 and hence the order of any element of $G(A)$ does not exceed n.

To finish the proof we only must show that $G(A)$ is finite. By Lemma 2.2, A has at least three critical values. On the other hand, by Lemma 2.1, iii), every $\nu \in \widehat{G}(A)$ maps $c(A)$ to $c(A)$. Since any Möbius transformation is defined by its values at any three points, this implies that $\widehat{G}(A)$ is finite. In turn, this implies that $G(A)$ is finite in view of the isomorphism (9) taking into account that $\Sigma(A)$ is finite by Theorem 2.3. □

Remark 2.5. Using some non-trivial group-theoretic results about subgroups of $\mathrm{GL}_{\mathrm{k}}(\mathbb{C})$, one can deduce the finiteness of $G(A)$ directly from the fact that the order of any element of $G(A)$ does not exceed n. Namely, the proof given in the paper [15] uses the Schur theorem (see e.g. [1], (36.2)), which states that any finitely generated periodic subgroup of $\mathrm{GL}_{\mathrm{k}}(\mathbb{C})$ has finite order. Alternatively, one can use the Burnside theorem (see e.g. [1], (36.1)), which states that any subgroup of $\mathrm{GL}_{\mathrm{k}}(\mathbb{C})$ of bounded period is finite. Indeed, assume that $G(A)$ 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 $G(A)$.

Corollary 2.6. *Let A be a rational function of degree $n \geqslant 2$. Then the groups $\Sigma(A)$ and $\mathrm{Aut}(A)$ are finite groups whose order does not exceed* $\max\{60, 2n\}$.

Proof. If A is a not a quasi-power, then the corollary follows from Theorem 2.4. On the other hand, it is easy to see that if A is a quasi-power, then the corresponding groups are cyclic groups of order n and $n-1$ correspondingly. □

Let us mention the following specification of Theorem 2.4.

Theorem 2.7. *Let A be a rational function of degree $n \geqslant 2$. Assume that there exists a point $z_0 \in \mathbb{CP}^1$ such that the multiplicity of A at z_0 is distinct from the multiplicity of A at any other point $z \in \mathbb{CP}^1$. Then $G(A)$ is a finite cyclic group, and z_0 is a fixed point of its generator.*

Proof. It follows from the assumption that A is not a quasi-power. Therefore, $G(A)$ is finite. Moreover, every element of $G(A)$ fixes z_0 by Lemma 2.1, i). On the other hand, a unique finite subgroup of $\mathrm{Aut}(\mathbb{CP}^1)$ whose elements share a fixed point is cyclic. $\square$

In turn, Theorem 2.7 implies the following well-known corollary.

Corollary 2.8. *Let P be a polynomial of degree $n \geqslant 2$ that is not a quasi-power. Then $G(P)$ is a finite cyclic group generated by a polynomial.*

Proof. Since P is a not a quasi-power, the multiplicity of P at infinity is distinct from the multiplicity of P at any other point of $\mathbb{CP}^1$. Moreover, since every element of $G(P)$ fixes infinity, $G(P)$ consist of polynomials. $\square$

Notice that functions A of degree n with $|G(A)| = 2n$ do exist. Indeed, it is easy to see that for any function of the from

$$A = \frac{z^n - a}{az^n - 1}, \quad a \in \mathbb{C}\backslash\{0\},$$

the group $G(A)$ contains the dihedral group D_{2n}, generated by

$$z \to \frac{1}{z}, \qquad z \to \varepsilon_n z,$$

where $\varepsilon_n = e^{\frac{2\pi i}{n}}$. In particular, by Theorem 2.4, $G(A) = D_{2n}$ for n big enough. On the other hand, for small n, functions A of degree n with $|G(A)| > 2n$ do exist as well (see for instance Example 2.10 below).

Lemma 2.1 provides us with a method for practical calculation of $G(A)$, at least if the degree of A is small enough. We illustrate it with the following example.

Example 2.9. 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

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

Since the multiplicities of A at the preimages of 1, 9, and ∞ are

$$\mathrm{mult}_0 A = 3, \quad \mathrm{mult}_{-8} A = 1, \quad \mathrm{mult}_{-2+2\sqrt{3}} A = 2, \quad \mathrm{mult}_{-2-2\sqrt{3}} A = 2,$$

and

$$\mathrm{mult}_\infty A = 3, \quad \mathrm{mult}_1 A = 1,$$

Lemma 2.1 implies that for any $\sigma \in G(A)$ either

$$\sigma(0) = 0, \quad \sigma(\infty) = \infty, \quad \sigma(-8) = -8, \quad \sigma(1) = 1, \tag{14}$$

or

$$\sigma(0) = \infty, \quad \sigma(\infty) = 0, \quad \sigma(-8) = 1, \quad \sigma(1) = -8. \tag{15}$$

Moreover, in addition, either

$$\sigma(-2 + 2\sqrt{3}) = -2 - 2\sqrt{3}, \quad \sigma(-2 - 2\sqrt{3}) = -2 + 2\sqrt{3}, \tag{16}$$

or

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

Clearly, condition (14) implies that $\sigma = z$, while the unique transformation satisfying (15) is

$$\sigma=-8/z, \tag{17}$$

and this transformation satisfies (16). Furthermore, the corresponding ν_σ must satisfy

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

implying that

$$\nu_\sigma=\frac{z+63}{z-1}. \tag{18}$$

Therefore, (1) can hold only for σ and ν_σ given by formulas (17) and (18), 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.

Notice that to verify whether a given Möbius transformation σ belongs to $G(A)$ one can use the Schwarz derivative. Let us recall that for a function f meromorphic on a domain $D\subset\mathbb{C}$ the Schwarz derivative is defined by

$$S(f)(z)=\frac{f'''}{f'}-\frac{3}{2}\left(\frac{f''}{f'}\right)^2.$$

The characteristic property of the Schwarz derivative is that for two functions f and g meromorphic on D the equality $S(f)(z)=S(g)(z)$ holds if and only if

$$g\ =\ \frac{a\,f+b}{c\,f+d}\ \text{for some}\ \begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{GL}_2(\mathbb{C}).$$

Thus, a Möbius transformation σ belongs to $G(A)$ if and only if

$$S(A)(z)=S(A\circ\sigma)(z).$$

We finish this section by another example of calculation of $G(A)$.

Example 2.10. 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 $\Sigma(A)$ contains the transformations $z\to -z$ and $z\to 1/z$, which generate the Klein four-group $V_4=D_4$. Thus, $\Sigma(B)=D_4$, by Theorem 2.3. Furthermore, it is clear that $G(B)$ contains the transformation $z\to iz$, implying 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 $G(B)=S_4$, or $G(B)$ is a dihedral group containing an element σ of order $k>4$, whose fixed points coincide with fixed points of $z\to iz$. The second case is impossible, since any Möbius transformation σ fixing 0 and ∞ has the form cz, $c\in\mathbb{C}\backslash\{0\}$, and it is easy to see that such σ belongs to $G(B)$ if and only if it is a power of $z\to iz$. On the other hand, a direct calculation shows that for the transformation $\mu=\frac{z+i}{z-i}$, generating together with $z\to iz$ and $z\to 1/z$ the group S_4, equality (1) holds for $\nu=\frac{-z+1}{-3z-1}$. Summarizing, we see that $G(B)\cong S_4$, $\widehat{G}(B)\cong D_6$, $\Sigma(B)\cong D_4$, and $\mathrm{Aut}(B)$ is trivial.

3. Groups $\Sigma_\infty(A)$, $\mathrm{Aut}_\infty(A)$ and the measure of maximal entropy

Let us recall that by the results of Freire, Lopes, Mañé ([3]) and Lyubich ([8]), for every rational function A of degree $n \geqslant 2$ 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.

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 $\mu_{A,k}(a)$ 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 $\mu_{A,k}(a)$, $k \geqslant 1$, 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 [7]), leading to characterizations of such functions in terms of functional equations (see [7], [14], [18]).

The relations between the groups $\Sigma_\infty(A)$, $\mathrm{Aut}_\infty(A)$ and the measure of maximal entropy are described by the following two statements.

Lemma 3.1. *Let A be a rational function of degree at least two. Then $\sigma \in \mathrm{Aut}_\infty(A)$ if and only if A and $\sigma^{-1} \circ A \circ \sigma$ have a common iterate. In particular, if $\sigma \in \mathrm{Aut}_\infty(A)$, then A and $\sigma^{-1} \circ A \circ \sigma$ share the measure of maximal entropy.*

Proof. The proof follows easily from the definitions. □

Lemma 3.2. *Let A be a rational function of degree $n \geqslant 2$. Then for every $\sigma \in \Sigma_\infty(A)$ the functions A and $A \circ \sigma$ share the measure of maximal entropy.*

Proof. Let us show first that any $\sigma \in \Sigma_\infty(A)$ is μ_A-invariant. Since the equality

$$A^{\circ l} = A^{\circ l} \circ \sigma, \quad l \geqslant 1,$$

implies that for any $k \geqslant 1$ 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:

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

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

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

holds, implying that

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

Let now 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 $\mu_A = \mu_{A \circ \sigma}$. □

It was proved by Levin ([5], [6]) that for any rational function A of degree $n \geqslant 2$ that is not conjugate to $z^{\pm n}$ there exist at most finitely many rational functions B of any given degree $d \geqslant 2$ sharing the measure of maximal entropy with A. The Levin theorem combined Lemma 3.1 and Lemma 3.2 implies the following result.

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

Proof. Since $\sigma \in \mathrm{Aut}_\infty(A)$ implies that A and $\sigma^{-1} \circ A \circ \sigma$ share the measure of maximal entropy by Lemma 3.1, it follows from the Levin theorem that the set of functions

$$\sigma^{-1} \circ A \circ \sigma, \qquad \sigma \in \mathrm{Aut}_\infty(A), \tag{19}$$

is finite. On the other hand, the equality

$$\sigma \circ A \circ \sigma^{-1} = \sigma' \circ A \circ \sigma'^{-1} \tag{20}$$

implies that $\sigma'^{-1} \circ \sigma \in \mathrm{Aut}(A)$. Thus, for any $\sigma \in \mathrm{Aut}_\infty(A)$ there exist at most finitely many $\sigma' \in \mathrm{Aut}_\infty(A)$ satisfying (20), and hence the finiteness of the set (19) implies the finiteness of the set $\mathrm{Aut}_\infty(A)$.

Similarly, it follows from Lemma 3.2 and the Levin theorem that the set of functions

$$A \circ \sigma, \qquad \sigma \in \Sigma_\infty(A),$$

is finite, implying the finiteness of $\Sigma_\infty(A)$, since the equality

$$A \circ \sigma = A \circ \sigma'$$

implies that $\sigma'^{-1} \circ \sigma \in \Sigma(A)$. □

4. Groups $\mathrm{Aut}_\infty(A)$ and $\widehat{G}(A^{\circ k})$

Let A be a rational function of degree $n \geqslant 2$. We define the set $S(A)$ 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 the equality

$$\nu \circ A^{\circ k} = A^{\circ k} \circ \mu \tag{21}$$

holds for some Möbius transformation μ and $k \geqslant 1$. The next several results provide a characterization of elements of $S(A)$, and show that $S(A)$ is finite and bounded in terms of n, unless A is a quasi-power.

We start from the following statement.

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

$$A_1 \circ A_2 \circ \cdots \circ A_k = B_1 \circ B_2 \circ \cdots \circ B_k. \tag{22}$$

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

$$|f^{-1}(T)| \leqslant |T| d. \tag{23}$$

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

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

Therefore,

$$|f^{-1}(T)| = \sum_{z\in f^{-1}\{T\}} 1 \geqslant \sum_{z\in f^{-1}\{T\}} \deg_z f - 2d + 2 = (|T| - 2)d + 2. \tag{24}$$

Let us denote by F the rational function defined by any of the parts of equality (22). 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 $|A_1^{-1}\{c\}| \leqslant n - 1$, it follows from (23) that

$$|F^{-1}\{c\}| \leqslant (n-1)n^{k-1}. \tag{25}$$

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 (24) that

$$|F^{-1}\{c\}| \geqslant (n^2 - 2)n^{k-2} + 2. \tag{26}$$

It follows now from (25) and (26) that

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

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

Theorem 4.1 implies the following statement.

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

Proof. Let ν be an element of $S(A)$. In case $\nu \in \widehat{G}(A)$, the statement of the theorem follows from Lemma 2.1, iii), 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 $k \geqslant 2$. Since equality (21) has the form (22) 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 $c(\nu \circ A) \subseteq c(A^{\circ 2})$. Taking into account that for every rational function A the equality

$$c(\nu \circ A) = \nu\big(c(A)\big)$$

holds, this implies that $\nu\big(c(A)\big) \subseteq c(A^{\circ 2})$. □

Theorem 4.3. *Let A be a rational function of degree $n \geqslant 2$. Then the set $S(A)$ is finite and bounded in terms of n, unless A is a quasi-power. Furthermore, the set $S(A)\backslash\widehat{G}(A)$ 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. Thus, the finiteness of $S(A)$ in case A is not a quasi-power follows from Lemma 2.2. 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.

Further, if A is not conjugate to $z^{\pm n}$, then its second iterate $A^{\circ 2}$ is not a quasi-power by Lemma 2.2. To prove the finiteness of $S(A)\backslash\widehat{G}(A)$ in this case, it is enough to show that for every $\nu \in S(A)\backslash\widehat{G}(A)$ the inclusion

$$\nu\big(c(A^{\circ 2})\big) \subseteq c(A^{\circ 4}) \tag{27}$$

holds, and this can be done by a modification of the proof of Theorem 4.2. Indeed, equality (21) implies the equality

$$\nu \circ A^{\circ 2k} = A^{\circ k} \circ \mu \circ A^{\circ k}$$

which can be rewritten for $k \geqslant 4$ in the form (22) with

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

and

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

if k is even, or

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

if k is odd. Therefore, if σ belongs to $\widehat{G}(A^{\circ k})$ for some $k \geqslant 4$, then applying Theorem 4.1, we conclude that (27) holds. On the other hand, if σ belongs to $\widehat{G}(A^{\circ 2})$, then $\nu\big(c(A^{\circ 2})\big) = c(A^{\circ 2})$, by Lemma 2.1, iii), implying by the chain rule that (27) holds. Similarly, if σ belongs to $\widehat{G}(A^{\circ 3})$, then $\nu\big(c(A^{\circ 3})\big) = c(A^{\circ 3})$, implying that

$$\nu\big(c(A^{\circ 2})\big) \subseteq \nu\big(c(A^{\circ 3})\big) = c(A^{\circ 3}) \subseteq c(A^{\circ 4}). \qquad \square$$

Theorem 4.3 implies the following result.

Theorem 4.4. *Let A be a rational function of degree $n \geqslant 2$. Then the orders of the groups $\widehat{G}(A^{\circ k})$, $k \geqslant 1$, are finite and uniformly bounded in terms of n only, unless A is a quasi-power. Furthermore, the orders of the groups $\widehat{G}(A^{\circ k})$, $k \geqslant 2$, are finite and uniformly bounded in terms of n only, unless A is conjugate to $z^{\pm n}$.*

Proof. Since every group $\widehat{G}(A^{\circ k})$, $k \geqslant 1$, is contained in $S(G)$, while every group $\widehat{G}(A^{\circ k})$, $k \geqslant 2$, is contained in $S(A)\backslash\widehat{G}(A)$ the theorem is a direct corollary of Theorem 4.3. $\square$

Finally, Theorem 4.2 and Theorem 4.3 imply Theorem 1.2 from the introduction.

Proof of Theorem 1.2. Since the set $S(A)$ contains the group $\mathrm{Aut}_\infty(A)$, the first part of the theorem follows from Theorem 4.2 (the assumption that A is not conjugate to z^n is actually redundant). In the same way, the boundedness of the set $\mathrm{Aut}_\infty(A)\backslash\mathrm{Aut}(A)$ in terms of n for A that is not conjugate to z^n follows from Theorem 4.3. Finally, the group $\mathrm{Aut}(A)$ is finite and bounded in terms of n by Theorem 2.4. $\square$

5. Groups $\Sigma_\infty(P)$ and $G(A^{\circ k})$

Let A and B be rational functions of degree at least two. We 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 the equality

$$A \circ X = X \circ B \tag{28}$$

holds. Usually, we will write this condition in the form of a commuting diagram

$$\begin{tikzcd} \mathbb{CP}^1 \arrow[r, "B"] \arrow[d, "X"'] & \mathbb{CP}^1 \arrow[d, "X"] \\ \mathbb{CP}^1 \arrow[r, "A"] & \mathbb{CP}^1. \end{tikzcd}$$

The simplest examples of semiconjugate rational functions are provided by equivalent rational functions defined in the introduction. Indeed, it follows from equalities (6) that the diagrams

$$\begin{tikzcd} \mathbb{CP}^1 \arrow[r, "A"] \arrow[d, "V"'] & \mathbb{CP}^1 \arrow[d, "V"] \\ \mathbb{CP}^1 \arrow[r, "\widetilde{A}"] & \mathbb{CP}^1 \end{tikzcd} \qquad \begin{tikzcd} \mathbb{CP}^1 \arrow[r, "\widetilde{A}"] \arrow[d, "U"'] & \mathbb{CP}^1 \arrow[d, "U"] \\ \mathbb{CP}^1 \arrow[r, "A"] & \mathbb{CP}^1 \end{tikzcd}$$

commutes, implying inductively that if A is equivalent to B, then A is semiconjugate to B, and B is semiconjugate to A.

A comprehensive description of semiconjugate rational functions was obtained in the papers [11], [12], [13]. In particular, it was shown in [11] that solutions A, X, B of (28) 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. On the other hand, an arbitrary solution of equation (28) can be reduced 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

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

for some rational functions $\widetilde{X}$ and $\widetilde{B}$ satisfying $\mathbb{C}(\widetilde{X}, \widetilde{B}) = \mathbb{C}(z)$. Moreover, it is easy to see that the diagram

$$\begin{tikzcd} \mathbb{CP}^1 \arrow[r, "B"] \arrow[d, "W"'] & \mathbb{CP}^1 \arrow[d, "W"] \\ \mathbb{CP}^1 \arrow[r, "W \circ \widetilde{B}"] \arrow[d, "\widetilde{X}"'] & \mathbb{CP}^1 \arrow[d, "\widetilde{X}"] \\ \mathbb{CP}^1 \arrow[r, "A"] & \mathbb{CP}^1 \end{tikzcd}$$

commutes. Thus, the triple $A, \widetilde{X}, W \circ \widetilde{B}$ is another solution of (28). This new solution is not necessary primitive, however $\deg \widetilde{X} < \deg X$. Therefore, continuing in this way, after a finite number of similar transformations we will arrive to a primitive solution. In more detail, the above argument shows that for any rational functions A, X, B satisfying (28) there exist rational functions X_0, B_0, U such that $X = X_0 \circ U$, the diagram

$$\begin{tikzcd} \mathbb{CP}^1 \arrow[r, "B"] \arrow[d, "U"'] & \mathbb{CP}^1 \arrow[d, "U"] \\ \mathbb{CP}^1 \arrow[r, "B_0"] \arrow[d, "X_0"'] & \mathbb{CP}^1 \arrow[d, "X_0"] \\ \mathbb{CP}^1 \arrow[r, "A"] & \mathbb{CP}^1 \end{tikzcd} \tag{29}$$

commutes, the triple A, X_0, B_0 is a primitive solution of (28), and $B_0 \sim B$.

The following theorem is essentially the first part of Theorem 1.3 from the introduction but without the assumption that A is not conjugate to z^n, which is redundant in this case.

Theorem 5.1. *Let A be a rational function of degree $n \geqslant 2$. Then for every $\sigma \in \Sigma_\infty(A)$ the relation $A \circ \sigma \sim A$ holds.*

Proof. Let σ be an element of $\Sigma_\infty(A)$. Then

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

for some $k \geqslant 1$. Writing this equality as the semiconjugacy

$$\begin{tikzcd} \mathbb{CP}^1 \arrow[r, "A\circ\sigma"] \arrow[d, "A^{\circ(k-1)}"] & \mathbb{CP}^1 \arrow[d, "A^{\circ(k-1)}"] \\ \mathbb{CP}^1 \arrow[r, "A"] & \mathbb{CP}^1 \end{tikzcd},$$

we see that to prove the theorem it is enough to show that in diagram (29), corresponding to the solution

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

of (28), the function X_0 has degree one. The proof of the last statement is similar to the proof of Theorem 2.3 in [16] and follows from the following two facts. First, for any primitive solution A, X, B of (28), the solution $A^{\circ l}, X, B^{\circ l}$, $l \geqslant 1$, is also primitive (see [16], Lemma 2.5). Second, a solution A, X, B of (28) is primitive if and only if the algebraic curve

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

is irreducible (see [16], Lemma 2.4). Using these facts we conclude that the triple $A^{\circ(k-1)}, X_0, B_0^{\circ(k-1)}$ is a primitive solution of (28), and the algebraic curve

$$A^{\circ(k-1)}(x) - X_0(y) = 0 \tag{31}$$

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 (31). Moreover, the assumption $\deg X_0 > 1$ implies that this component is proper. The contradiction obtained proves that $\deg X_0 = 1$. $\square$

The following result proves the second part of Theorem 1.3 and thus finishes the proof of this theorem.

Theorem 5.2. *Let A be a rational function of degree $n \geqslant 2$ that is not conjugate to $z^{\pm n}$. Then the order of the group $\Sigma_\infty(A)$ is finite and bounded in terms of n.*

Proof. 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 2.2. Therefore, if the theorem is true for functions which are not quasi-powers, then for any A that 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 $\Sigma_\infty(A)$.

Let us recall that in view of equality (7) the equivalence class $[A]$ is a union of conjugacy classes. Denoting the number of these conjugacy classes by N_A, let us show that if N_A is finite, then

$$|\Sigma_\infty(A)| \leqslant |G(A)|N_A. \tag{32}$$

By Theorem 5.1, for any $\sigma_0 \in \Sigma_\infty(A)$ the function $A \circ \sigma_0$ 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 $\widehat{G}(A)$, 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 $|\mathrm{Ker}\,\gamma_A|$ elements $\sigma \in G(A)$ such that

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

Thus, (32) follows from (10).

It is proved in [12] that N_A is infinite if and only if A is a flexible Lattès map. However, the proof given in [12] uses the theorem of McMullen ([9]) about isospectral rational functions, which is not effective. Therefore, the result of [12] does not imply that N_A is bounded in terms of n. Nevertheless, we can use the main result of [15], which states that for a given rational function B of degree n the number of conjugacy classes of rational functions A such that (28) 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, 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 $\pm T_n$.

It is easy to see using the explicit formula

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

that the group $\Sigma(\pm T_n)$ is either trivial or equal to C_2, depending on the parity of n. Therefore, since $T_n^{\circ k} = T_{n^{\circ k}}$, $k \geqslant 1$, the order of $\Sigma_\infty(\pm T_n)$ is at most two.

Finally, if A is a Lattès map, then there exists 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 [10], [13] for more detail). Since this implies that $A^{\circ k} : \mathcal{O} \to \mathcal{O}$, $k \geqslant 1$, also is a covering map (see [11], Corollary 4.1), equality (30) implies that $\sigma : \mathcal{O} \to \mathcal{O}$ is a covering map (see [11], 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. $\square$

Proof of Theorem 1.4. If $\sigma \in \Sigma_\infty(A)$, then

$$A \circ \sigma \sim A, \tag{33}$$

by Theorem 5.1. On the other hand, since for any indecomposable function A the number N_A obviously is equal to one, condition (33) is equivalent to the condition that

$$A \circ \sigma = \beta \circ A \circ \beta^{-1} \tag{34}$$

for some $\beta \in \mathrm{Aut}(\mathbb{CP}^1)$. Clearly, equality (34) implies that β belongs to $\widehat{G}(A)$. Therefore, if $\widehat{G}(A)$ is trivial, then (33) 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 (34) 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 $G(A) = \mathrm{Aut}(A)$. $\square$

The following two theorems imply Theorem 1.1 from the introduction.

Theorem 5.3. *Let A be a rational function of degree $n \geqslant 2$. Then the orders of the groups $G(A^{\circ k})$, $k \geqslant 1$, are finite and uniformly bounded in terms of n only, unless A is a quasi-power. Furthermore, the orders of the groups $G(A^{\circ k})$, $k \geqslant 2$, are finite and uniformly bounded in terms of n only, unless A is conjugate to $z^{\pm n}$.*

Proof. If A is not a quasi-power, then, by Theorem 4.4 and Theorem 5.2, the orders of the groups $\widehat{G}(A^{\circ k})$, $k \geqslant 1$, and $\Sigma(A^{\circ k})$, $k \geqslant 1$, are finite and uniformly bounded in terms of n only. Therefore, by (10), the orders of the groups $G(A^{\circ k})$, $k \geqslant 1$, also are finite and uniformly bounded. Similarly, the groups $G(A^{\circ k})$, $k \geqslant 2$, are finite and uniformly bounded in terms of n only, unless A is conjugate to $z^{\pm n}$. $\square$

Theorem 5.4. *Let A be a rational function of degree $n \geqslant 2$. Then the sequence $G(A^{\circ k})$, $k \geqslant 1$, contains only finitely many non-isomorphic groups.*

Proof. If A is a not conjugate to $z^{\pm n}$, then the theorem follows from Theorem 5.3, since there exist only finitely many groups of any given order. On the other hand, if A is conjugate to $z^{\pm n}$, then all the groups $G(A^{\circ k})$, $k \geqslant 1$, are equal and consist of the transformations $z \to cz$, $c \in \mathbb{C}\setminus\{0\}$. $\square$

We finish this section by two examples of calculation of the group $\Sigma_\infty(A)$.

Example 5.5. Let us consider the function

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

A calculation show that, in addition to the critical value ∞, this function has critical values 4 and $4i$, and

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

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

Since the above equalities imply that $\mathrm{mult}_0 A = 3$, while at any other point of $\mathbb{CP}^1$ the multiplicity of A is at most two, it follows from Theorem 2.7 that $G(A)$ is a cyclic group, whose generator has zero as a fixed point. Moreover, 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, $G(A) = \mathrm{Aut}(A)$. Finally, since $\mathrm{mult}_0 A = 3$, 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 1.4.

Example 5.6. Let us consider the function

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

Since A is a quasi-power, $\Sigma(A)$ 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 2.10. 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 2.10, 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 $l > 4$ such that σ_1 is an iterate of σ. The first case is impossible, for otherwise Theorem 2.3 implies that for k satisfying $\Sigma_\infty(A) = \Sigma(A^{\circ k})$ the number $\deg A^{\circ k} = 2^k$ is divisible by $|S_4| = 24$. On the other hand, in the second case, fixed points of σ must be zero and infinity. Therefore, by Theorem 5.1, taking into account that A is indecomposable, to exclude the second case it is enough to show that if $\sigma = cz$, $c \in \mathbb{C}\backslash\{0\}$, satisfies

$$A \circ \sigma = \beta \circ A \circ \beta^{-1}, \quad \beta \in \mathrm{Aut}(\mathbb{CP}^1), \tag{35}$$

then σ is an iterate of μ_1. Since critical points of the function in the left side of (35) coincide with critical points of the function in the right side, the Möbius transformation β necessarily has the form $\beta = dz^{\pm 1}$, $d \in \mathbb{C}\backslash\{0\}$. Thus, equation (35) reduces to the equations

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

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 5.1 it is also possible to use Theorem 1.5.

6. Groups $G(A, z_0)$

Following [17], 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 $i \equiv j(\text{mod } l)$. If f is not homozygous mod l, it is called *hybrid* mod l. Obviously, the condition that f is homozygous mod l 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, $1 \leqslant r \leqslant l$. In particular, if f is homozygous mod l, then any iterate of f is homozygous mod l. The inverse is not true. However, the following statement proved by Reznick ([17]) holds: 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 $s \geqslant 1$. Our proof of Theorem 1.5 relies on this result.

Proof of Theorem 1.5. If $A=z^{\pm n}$, then the theorem is true, since the groups $G(A^{\circ k}, z_0, z_1)$, $k \geqslant 1$, are trivial, unless $\{z_0, z_1\}=\{0,\infty\}$, while in the last case all these groups are equal and consist of the transformations $z \to cz$, $c \in \mathbb{C}\backslash\{0\}$. Therefore, we can assume that A is not conjugate to $z^{\pm n}$. In addition, without loss of generality, we can assume that $z_0=0$, $z_1=\infty$. Notice that the definition of $G(A, z_0, z_1)$ implies that

$$G(A, z_0, z_1) \subseteq G(A^{\circ k}, z_0, z_1), \qquad k \geqslant 1.$$

Let f_A be the Taylor series of the function A at zero. Arguing as in the proof of Theorem 2.4, we see that the above assumptions imply that $G(A, 0, \infty)$ is a finite cyclic group, and every element of $G(A, 0, \infty)$ has the form $z \to \varepsilon z$, where ε is a root of unity. Moreover, a primitive n-root of unity ε belongs to $G(A, 0, \infty)$ if and only if f_A is homozygous mod n. Since $f_{A^{\circ k}}=f_A^{\circ k}$, this implies that if $G(A^{\circ k}, 0, \infty)$ is strictly larger than $G(A, 0, \infty)$, then there exists n_0 such that f_A is hybrid mod n_0 but $f_A^{\circ k}$ is homozygous mod n_0. Therefore, by the Reznick theorem, the equality $f_A^{\circ ks}=z$ holds for some $s \geqslant 1$. However, this is impossible, since the equality $A^{\circ ks}=z$ implies by the analytical continuation that $A^{\circ ks}=z$ for all $z \in \mathbb{CP}^1$, in contradiction with $n \geqslant 2$. $\square$

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. For example, for the function

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

from Example 5.6 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 two. Notice Theorem 1.5 gives another proof of the fact that $\Sigma_\infty(A)$ cannot contain an element $\sigma = cz$, $c \in \mathbb{C}\backslash\{0\}$, of order $l > 4$. Indeed, such σ must belong to the group $G(A^{\circ k},0,\infty)$ for some $k \geqslant 1$, and hence to the group $G(A^{\circ 2k},0,\infty)$. However, $G(A^{\circ 2k},0,\infty)$ is equal to $G(A^{\circ 2},0,\infty) = C_2$ by Theorem 1.5 applied to $A^{\circ 2}$.

Any Möbius transformation σ that belongs to the group $\mathrm{Aut}_\infty(A)$ or to the group $\Sigma_\infty(A)$ satisfies the equality

$$A^{\circ k} \circ \sigma = \sigma^{\circ l} \circ A^{\circ k}, \tag{36}$$

where $k \geqslant 1$ and l equals zero or one. This fact combined with Theorem 1.5 permits under certain conditions to estimate the order of the groups $\mathrm{Aut}_\infty(A)$ and $\Sigma_\infty(A)$ and even to describe these groups explicitly.

Theorem 6.1. *Let A be a rational function of degree $n \geqslant 2$ that is not conjugate to $z^{\pm n}$. Assume that for some $k \geqslant 1$ the group $\mathrm{Aut}(A^{\circ k})$ contains an element σ of order at least six with fixed points z_0, z_1 such that z_0 is a fixed point of $A^{\circ k}$. Then the inequality $|\mathrm{Aut}_\infty(A)| \leqslant 2|G(A^{\circ k}, z_0, z_1)|$ holds. In case the group $\Sigma(A^{\circ k})$ contains an element σ as above, the same inequality holds for $|\Sigma_\infty(A)|$.*

Proof. Since the maximal order of a cyclic subgroup in the groups A_4, S_4, A_5 is five, it follows from Theorem 2.4 that if $\mathrm{Aut}(A^{\circ k})$ contains an element σ of order $r > 5$, then either $\mathrm{Aut}_\infty(A) = C_s$ or $\mathrm{Aut}_\infty(A) = D_{2s}$, where $r|s$. Moreover, if σ_∞ is an element of order s in $\mathrm{Aut}_\infty(A)$, then σ is an iterate of σ_∞. In particular, fixed points of σ_∞ coincide with fixed points of σ.

To prove the theorem we only must show that the inequality

$$s > |G(A^{\circ k}, z_0, z_1)| \tag{37}$$

is impossible. Assume the inverse. Since σ_∞ belongs to $\mathrm{Aut}(A^{\circ k'})$ for some $k' \geqslant 1$, it belongs to $\mathrm{Aut}(A^{\circ kk'})$ and $G(A^{\circ kk'}, z_0, z_1)$. Therefore, if (37) holds, 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 1.5 applied to $G(A^{\circ k})$. The proof of the inequality for $|\Sigma_\infty(A)|$ is similar. □

Example 6.2. 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 zero is a fixed point of A and $G(A,0,\infty) = C_6$, it follows from Theorem 6.1 that

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

Equality (36) does not necessarily imply that a fixed point of σ is a fixed point of $A^{\circ k}$. For example, for a rational function A of the form $A = R(z^d)$, where $d \geqslant 2$ and $R \in \mathbb{C}(z)$, fixed points of $\sigma = e^{\frac{2\pi i}{d}} z$ satisfying (36) are zero and infinity, and these points are not fixed points of A, unless they are fixed points of R. Nevertheless, the following statement holds.

Lemma 6.3. *Let A be a rational function of degree $n \geqslant 2$, and $\sigma \notin \Sigma(A^{\circ k})$ a Möbius transformation such that* (36) *holds for some $l \geqslant 1$. 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. Clearly, equality (36) implies the equalities

$$\sigma^{\circ l}(A^{\circ k}(z_0)) = A^{\circ k}(z_0), \quad \sigma^{\circ l}(A^{\circ k}(z_1)) = A^{\circ k}(z_1).$$

On the other hand, since $\sigma^{\circ l}$ is not the identical map, it has only two fixed points z_0, z_1. Therefore, $A^{\circ k}\{z_0, z_1\} \subseteq \{z_0, z_1\}$, implying that at least one of the points z_0, z_1 is a fixed point of $A^{\circ 2k}$. Finally, if z_0 is such a point, then $\sigma \in G(A^{\circ 2k}, z_0, z_1)$, since equality (36) implies the equality

$$A^{\circ 2k} \circ \sigma = \sigma^{\circ l^2} \circ A^{\circ 2k}. \qquad \square$$

Combining Theorem 6.1 with Lemma 6.3 we obtain the following result.

Theorem 6.4. *Let A be a rational function of degree $n \geqslant 2$ that is not conjugate to $z^{\pm n}$. Assume that for some $k \geqslant 1$ the group $\mathrm{Aut}(A^{\circ k})$ contains an element σ of order at least six with fixed points z_0, z_1. Then $|\mathrm{Aut}_\infty(A)| \leqslant 2|G(A^{\circ 2k}, z_0, z_1)|$, where z_0 is a fixed point of σ that is also a fixed point of $A^{\circ 2k}$.* $\square$

References

[1] C. W. Curtis, I. Reiner, *Representation theory of finite groups and associative algebras,* Pure and Appl. Math., vol. 11, Interscience, New York, 1962.

[2] P. Doyle, C. McMullen, *Solving the quintic by iteration,* Acta Math. 163 (1989), no. 3-4, 151-180.

[3] A. Freire, A. Lopes, R. Mañé, *An invariant measure for rational maps*, Bol. Soc. Brasil. Mat. 14 (1983), no. 1, 45-62.

[4] F. Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, New York: Dover Publications, (1956).

[5] G. Levin, *Symmetries on Julia sets,* Math. Notes 48 (1990), no. 5-6, 1126-1131.

[6] G. Levin, *Letter to the editors*, Math. Notes 69 (2001), no. 3-4, 432-33.

[7] G. Levin, F. Przytycki, *When do two rational functions have the same Julia set?*, Proc. Amer. Math. Soc. 125 (1997), no. 7, 2179-2190.

[8] M. Ljubich, *Entropy properties of rational endomorphisms of the Riemann sphere*, Ergodic Theory Dynam. Systems 3 (1983), no. 3, 351-385.

[9] C. McMullen, *Families of rational maps and iterative root-finding algorithms,* Ann. of Math., 125, No. 3 (1987), 467-493.

[10] 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.

[11] F. Pakovich, *On semiconjugate rational functions,* Geom. Funct. Anal., 26 (2016), 1217-1243.

[12] F. Pakovich, *Recomposing rational functions,* Int. Math. Res. Not., 2019, no. 7, 1921-1935.

[13] F. Pakovich, *On generalized Latès maps,* J. Anal. Math., 142 (2020), no. 1, 1–39.

[14] F. Pakovich, *On rational functions sharing the measure of maximal entropy*, Arnold Math. J., 6, 387–396 (2020).

[15] F. Pakovich, *Finiteness theorems for commuting and semiconjugate rational functions,* Conform. Geom. Dyn., 24 (2020), 202-229.

[16] F. Pakovich, *Commuting rational functions revisited*, Ergodic Theory Dynam. Systems, 41 (2021), no. 1, 295 - 320.

[17] B. Reznick, *When is the iterate of a formal power series odd?*, J. Austral. Math. Soc. Ser. A 28 (1979), no. 1, 62-66.

[18] 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
Email address: pakovich@math.bgu.ac.il