ON SYMMETRIES OF ITERATES OF RATIONAL FUNCTIONS

FEDOR PAKOVICH

Abstract. Let $A$ be a rational function of degree $n \geq 2$. Let us denote by $G(A)$ the group of Möbius transformations $\sigma$ such that $A \circ \sigma = \nu \circ A$ for some Möbius transformations $\nu$, and by $\Sigma(A)\text{ and } \text{Aut}(A)$ the subgroups of $G(A)$ consisting of $\sigma$ such that $A \circ \sigma = A$ and $A \circ \sigma = \sigma \circ A$, correspondingly. In this paper, we study sequences of the above groups arising from iterating $A$. In particular, we show that if $A$ is not conjugate to $z^n$, then the orders of the groups $G_{p,q}$, $k \geq 2$, are finite and uniformly bounded in terms of $n$ only.

We also prove a number of results about the groups $\Sigma_{p,q} = \bigcup_{k=1}^{n-1} \Sigma(A^{\circ k})$ and $\text{Aut}_{p,q}(A) = \bigcup_{k=1}^{n-1} \text{Aut}(A^{\circ k})$, which are especially interesting from the dynamical perspective.

1. Introduction

Let $A$ be a rational function of degree $n \geq 2$. In this paper, we study a variety of different subgroups of $\text{Aut}(\mathbb{C}P^1)$ related to $A$, and more generally to a dynamical system defined by iterating $A$. Specifically, let us define $\Sigma(A)$ and $\text{Aut}(A)$ as the groups of Möbius transformations $\sigma$ 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 $\text{Aut}(A)$ 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 $\text{Aut}(A)$ are finite and therefore belong to the well-known list $A_4, S_4, A_5, C_1, D_2$ of finite subgroups of $\text{Aut}(\mathbb{C}P^1)$.

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

$$A \circ \sigma = \nu \circ A$$

for some Möbius transformations $\nu$. It is easy to see that $G(A)$ is indeed a group, and that $\nu$ is defined in a unique way by $\sigma$. Furthermore, the map

$$\gamma_A : \sigma \rightarrow \nu$$

is a homomorphism from $G(A)$ to the group $\text{Aut}(\mathbb{C}P^1)$, whose kernel coincides with $\Sigma(A)$. We will denote the image of $\gamma_A$ by $\overline{G}(A)$. It was shown in the paper [15] that unless

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

for some $\alpha, \beta \in \text{Aut}(\mathbb{C}P^1)$ 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. 1092/22.
In this paper, we study the dynamical analogues of the groups $\Sigma(A)$ and $\text{Aut}(A)$ defined by the formulas
\[ \Sigma_\infty(A) = \bigcup_{k=1}^{\infty} \Sigma(A^c_k), \quad \text{Aut}_\infty(A) = \bigcup_{k=1}^{\infty} \text{Aut}(A^c_k). \]
Since
\[ \Sigma(A) \subseteq \Sigma(A^{c^2}) \subseteq \Sigma(A^{c^3}) \subseteq \ldots \subseteq \Sigma(A^{c^k}) \subseteq \ldots, \]
and
\[ \text{Aut}(A^{c^k}) \subseteq \text{Aut}(A^{c^r}), \quad \text{Aut}(A^{c^2}) \subseteq \text{Aut}(A^{c^r}) \]
for any common multiple $r$ of $k$ and $l$, the sets $\Sigma_\infty(A)$ and $\text{Aut}_\infty(A)$ are groups. While it is not clear a priori that the groups $\Sigma_\infty(A)$ and $\text{Aut}_\infty(A)$ 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 $\text{Aut}_\infty(A)$ 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 $G(A^{c^k})$, $k \geq 1$, defined by iterating $A$.

Our main result about the groups $G(A^{c^k})$, $k \geq 1$, can be formulated as follows.

**Theorem 1.1.** Let $A$ be a rational function of degree $n \geq 2$ that is not conjugate to $z^{\pm n}$. Then the orders of the groups $G(A^{c^k})$, $k \geq 2$, are finite and uniformly bounded in terms of $n$ only.

In addition to Theorem 1.1, we prove a number of more precise results about the groups $\Sigma_\infty(A)$ and $\text{Aut}_\infty(A)$ 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 concerning the groups $\text{Aut}_\infty(A)$ is following.

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

Notice that since Möbius transformations $\nu$ such that
\[ \nu(c(A)) \subseteq c(A^{c^2}) \]
can be described explicitly, Theorem 1.2 provides us with a concrete subset of $\text{Aut}(\mathbb{CP}^1)$ containing the group $\text{Aut}_\infty(A)$.

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

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 $\mu$ 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, 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 $\Sigma_\nu(A)$ is following.

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

Notice that in some cases Theorem 1.3 permits to describe the group $\Sigma_\nu(A)$ 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 yields the following statement.

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

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

Finally, along with the groups $G(A^k), k \geq 1$, we consider their “local” versions. Specifically, let $z_0 \in \mathbb{C}P^1$ be a fixed point of $A$. For a point $z_1 \in \mathbb{C}P^1$ distinct from $z_0$, we define $G(A, z_0, z_1)$ as the subgroup of $G(A)$ consisting of M"obius transformations $\sigma$ such that $\sigma(z_0) = z_0$ and $\sigma(z_1) = z_1$. For these groups, we prove the following statement.

**Theorem 1.5.** Let $A$ be a rational function of degree $n \geq 2$ that is not conjugate to $z^{\pm n}$. Assume that $z_0 \in \mathbb{C}P^1$ is a fixed point of $A$, and $z_1 \in \mathbb{C}P^1$ is a point distinct from $z_0$. Then $G(A^k, z_0, z_1), k \geq 1$, are finite cyclic groups equal to each other.

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

$$A^k \circ \sigma = \sigma \circ A^k, \quad k \geq 1,$$

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

The paper is organized as follows. In the second section, we establish basic properties of the group $G(A)$ and provide a method for its calculation. In the third section, we briefly discuss relations between the groups $\Sigma_\nu(A)$, $\text{Aut}_\nu(A)$ 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 (4) holds for any M"obius transformation $\nu$ that belongs to $\hat{G}(A^k)$ for some $k \geq 1$. 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 $\text{Aut}_\nu(A)$ and $\Sigma_\nu(A)$. 

2. Groups $G(A)$

Let $A$ be a rational function of degree $n \geq 2$, and $G(A)$, $\hat{G}(A)$, $\Sigma(A)$, $\text{Aut}(A)$ 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 $\alpha, \beta \in \text{Aut}(\mathbb{CP}^1)$, then

$$(7) \quad G(A') = \beta^{-1} \circ G(A) \circ \beta, \quad \hat{G}(A') = \alpha \circ \hat{G}(A) \circ \alpha^{-1}.$$  

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

$$(8) \quad p\hat{G}(pA) = G(pA)/\Sigma(pA),$$

the equality

$$(9) \quad |G(A)| = |\hat{G}(A)|/|\Sigma(A)|$$

holds whenever the groups involved are finite.

**Lemma 2.1.** Let $A$ be a rational function of degree $n \geq 2$. 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 by $\sigma$ to the fiber $A^{-1}(\nu_\sigma(c))$.

iii) Every $\nu \in \hat{G}(A)$ maps $c(A)$ to $c(A)$.

**Proof.** Since (1) implies that

$$\text{mult}_z A \cdot \text{mult}_z \sigma = \text{mult}_{A(z)} \nu_\sigma \cdot \text{mult}_z A$$

the first statement follows from the fact that $\sigma$ and $\nu_\sigma$ are one-to-one.

Further, it is clear that (1) implies

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

Changing now $\sigma^{-1}$ to $\sigma$ 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 $\sigma$ is one-to-one, and that $c$ is a critical value of $A$ if and only $|A^{-1}(c)| < n$. □

We say that a rational function $A$ of degree $n \geq 2$ is a quasi-power if there exist $\alpha, \beta \in \text{Aut}(\mathbb{CP}^1)$ 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 $z \rightarrow cz^{\pm 1}, \ c \in \mathbb{C}\setminus\{0\}$. Therefore, by (7), for any quasi-power $A$ the groups $G(A)$ and $\hat{G}(A)$ are infinite.

**Lemma 2.2.** 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 $A^2$ is a quasi-power if and only if $A$ is conjugate to $z^n$. 


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
\[ A'^2 = \alpha \circ z^n \circ \beta \circ \alpha \circ z^n \circ \beta \]
has only two critical values if and only if \( \beta \circ \alpha \) maps the set \( \{0, \infty\} \) to itself. Therefore, \( A'^2 \) is a quasi-power if and only if \( \beta \circ \alpha = cz^{\pm 1}, \; c \in \mathbb{C}\backslash\{0\} \), that is, if and only if
\[ A = \alpha \circ z^n \circ \beta = \alpha \circ z^n \circ cz^{\pm 1} \circ \alpha^{-1} = \alpha \circ c^n z^{\pm n} \circ \alpha^{-1}. \]

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 \( \text{Aut}(\mathbb{C}P^1) \). We recall that a rational function \( \theta_G \) is called an invariant function for \( G \) if the equality \( \theta_G(x) = \theta_G(y) \) holds for \( x, y \in \mathbb{C}P^1 \) 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 \( \theta_G \rightarrow \mu \circ \theta_G \), where \( \mu \in \text{Aut}(\mathbb{C}P^1) \). Obviously, \( \theta_G \) has degree equal to the order of \( G \). Invariant functions for finite subgroups of \( \text{Aut}(\mathbb{C}P^1) \) were first found by Klein in his book [4].

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

**Proof.** Since for a finite subgroup \( G \) of \( \text{Aut}(\mathbb{C}P^1) \) the set of rational functions \( F \) such that \( F \circ \sigma = F \) for every \( \sigma \in G \) is a subfield of \( \mathbb{C}(z) \), it follows easily from the Lüroth theorem that any such a function \( F \) is a rational function in \( \theta_G \). Thus, \( \deg F \) is divisible by \( \deg \theta_G = |G| \). In particular, setting \( G = \Sigma(A) \), we see that the degree of \( A \) is divisible by \( |\Sigma(A)| \), and \( \deg A = |\Sigma(A)| \) 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 \( \text{Aut}(\mathbb{C}P^1) \) there exist rational functions for which \( \Sigma(A) = G \). Similarly, for every finite subgroup \( G \) of \( \text{Aut}(\mathbb{C}P^1) \) there exist rational functions for which \( \text{Aut}(A) = G \).

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).

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 \( n \geq 2 \) that is not a quasi-power. Then the group \( G(A) \) is isomorphic to one of the five finite rotation groups of the sphere \( A_4, S_4, A_5, C_1, D_{2l} \), and the order of any element of \( G(A) \) does not exceed \( n \). In particular, \( |G(A)| \leq \max\{60, 2n\} \).

**Proof.** Any element of the group \( \text{Aut}(\mathbb{C}P^1) \cong \text{PSL}_2(\mathbb{C}) \) is conjugate either to \( z \rightarrow z + 1 \) or to \( z \rightarrow \lambda z \) for some \( \lambda \in \mathbb{C}\backslash\{0\} \). Thus, making the change
\[ A \rightarrow \mu_1 \circ A \circ \mu_2, \quad \sigma \rightarrow \mu_2^{-1} \circ \sigma \circ \mu_2, \quad \nu_\sigma \rightarrow \mu_1 \circ \nu_\sigma \circ \mu_1^{-1} \]
for convenient \( \mu_1, \mu_2 \in \text{Aut}(\mathbb{C}P^1) \), without loss of generality we may assume that \( \sigma \) and \( \nu_\sigma \) in (1) have one of the two forms above.

We observe first that the equality
\[ A(z + 1) = \lambda A(z), \quad \lambda \in \mathbb{C}\backslash\{0\}, \]
is impossible. Indeed, if $A$ has a finite pole, then (10) 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 (10) implies that $A$ has infinitely many zeroes. Similarly, the equality

$$A(z + 1) = A(z) + 1$$

is impossible if $A$ has a finite pole. On the other hand, if $A$ is a polynomial of degree $n \geq 2$, then we obtain a contradiction comparing the coefficients of $z^{n-1}$ on the left and the right sides of equality (11).

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 on the left and the right sides of the equality

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

we conclude that this equality is impossible either. Thus, equality (1) for a non-identity $\sigma$ reduces to the equality

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

Comparing now coefficients on the left and the right sides of (12) and taking into account that $A \neq az^n$, $a \in \mathbb{C}$, by the assumption, we conclude that $\lambda_1$ is a root of unity. Furthermore, if $d$ is the order of $\lambda_1$, then $\lambda_2 = \lambda_1^r$ for some $0 \leq r \leq d - 1$, 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 $0 \leq r < d = 1$, then $d \leq n$, unless either $R \in \mathbb{C}\setminus\{0\}$ or $R = a/z$ for some $a \in \mathbb{C}\setminus\{0\}$. Since for such $R$ the function $A$ is a quasi-power, we conclude that the order of $\lambda_1$ 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. Since $\Sigma(A)$ is finite by Theorem 2.3, this implies that $G(A)$ is finite because of the isomorphism (8).

Remark 2.5. Using some non-trivial group-theoretic results about subgroups of $\text{GL}_2(\mathbb{C})$, 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 $\text{GL}_2(\mathbb{C})$ has finite order. Alternatively, one can use the Burnside theorem (see e.g. [1], (36.1)), which states that any subgroup of $\text{GL}_2(\mathbb{C})$ of bounded period is finite. Indeed, assume that $G(A)$ is infinite. Then its lifting $\overline{G(A)} \subset \text{SL}_2(\mathbb{C}) \subset \text{GL}_2(\mathbb{C})$ 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 of $\overline{G(A)}$ is bounded by $2N$. The contradiction obtained proves the finiteness of $G(A)$.

Corollary 2.6. Let $A$ be a rational function of degree $n \geq 2$. Then $\Sigma(A)$ and $\text{Aut}(A)$ 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 \( n \geq 2 \). 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 \( \text{Aut}(\mathbb{CP}^1) \) 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 \( n \geq 2 \) 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 \( |G(A)| \leq 2^n \) do exist. Indeed, it is easy to see that for any function of the form

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

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

\[
z \rightarrow \frac{1}{z}, \quad z \rightarrow \varepsilon_n z,
\]

where \( \varepsilon_n = e^{\frac{2\pi i}{n}} \). Thus, for \( n \) big enough, \( G(A) = D_{2n} \), by Theorem 2.4. 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

\[
A = \frac{z^4 + 8z^3 + 8z - 8}{z - 1}.
\]

One can check that \( A \) has three critical values \( 1, 9, \) and \( \infty \), and that

\[
A - 1 = \frac{1}{8} \frac{z^3(z+8)}{z-1}, \quad A - 9 = \frac{1}{8} \frac{(z^2 + 4z - 8)^2}{z - 1}.
\]

Since the multiplicities of \( A \) at the preimages of \( 1, 9, \) and \( \infty \) are

\[
\text{mult}_0 A = 3, \quad \text{mult}_{-8} A = 1, \quad \text{mult}_{-2+2\sqrt{3}} A = 2, \quad \text{mult}_{-2-2\sqrt{3}} A = 2,
\]

and

\[
\text{mult}_{\infty} A = 3, \quad \text{mult}_1 A = 1,
\]

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

\[
(13) \quad \sigma(0) = 0, \quad \sigma(\infty) = \infty, \quad \sigma(-8) = -8, \quad \sigma(1) = 1,
\]

or

\[
(14) \quad \sigma(0) = \infty, \quad \sigma(\infty) = 0, \quad \sigma(-8) = 1, \quad \sigma(1) = -8.
\]

Moreover, in addition, either

\[
(15) \quad \sigma(-2 + 2\sqrt{3}) = -2 - 2\sqrt{3}, \quad \sigma(-2 - 2\sqrt{3}) = -2 + 2\sqrt{3},
\]
or
\[ \sigma(-2 + 2\sqrt{3}) = -2 + 2\sqrt{3}, \quad \sigma(-2 - 2\sqrt{3}) = -2 - 2\sqrt{3}. \]

Clearly, condition (13) implies that \( \sigma = z \), while the unique transformation satisfying (14) is
\[ \sigma = -8/z, \]
and this transformation satisfies (15). Furthermore, the corresponding \( \nu_\sigma \) must satisfy
\[ \nu_\sigma(1) = \infty, \quad \nu_\sigma(\infty) = 1, \quad \nu_\sigma(9) = 9, \]
implying that
\[ \nu_\sigma = \frac{z + 63}{z - 1}. \]

Therefore, (1) can hold only for \( \sigma \) and \( \nu_\sigma \) given by formulas (16) and (17), and a direct calculation shows that (1) is indeed satisfied. Thus, the group \( G \) is a cyclic group of order two.

Notice that to verify whether a given Möbius transformation \( \sigma \) belongs to \( G \) 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 \( g = \nu \circ f \) for some Möbius transformation \( \nu \). Thus, a Möbius transformation \( \sigma \) belongs to \( G \) if and only if
\[ S(A)(z) = S(A \circ \sigma)(z). \]

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

**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 \( \Sigma(B) \) contains the transformations \( z \to -z \) and \( z \to 1/z \), which generate the Klein four-group \( V_4 = D_4 \), implying that \( \Sigma(B) = D_4 \) 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 \( \sigma \) of order \( k > 4 \), whose fixed points coincide with fixed points of \( z \to iz \). The second case is impossible, since any Möbius transformation \( \sigma \) fixing 0 and \( \infty \) has the form \( cz \), \( c \in \mathbb{C}\{0\} \), and it is easy to see that such \( \sigma \) 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 \( \mu = \frac{1}{iz} \), generating together with \( z \to iz \) and \( z \to 1/z \) the group \( S_4 \), equality (1) holds for \( \nu = \frac{z + 1}{-3z - 1} \). Thus, \( G(B) \cong S_4 \).
3. Groups $\Sigma_x(A)$, $\text{Aut}_x(A)$ 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 $n \geq 2$ there exists a unique probability measure $\mu_A$ 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 $\mu_A$ can be described as follows. For $a \in \mathbb{CP}^1$ let $z^k_i(a)$, $i = 1, \ldots, n^k$, be the roots of the equation $A^k(z) = a$ counted with multiplicity, and $\mu_{A,k}(a)$ the measure defined by

$$\mu_{A,k}(a) = \frac{1}{n^k} \sum_{i=1}^{n^k} \delta_{z^k_i(a)}.$$  \hfill (18)

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 $\mu_A$. Notice that this description of $\mu_A$ implies that $\mu_A = \mu_B$ whenever $A$ and $B$ share an iterate.

The measure $\mu_A$ 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 also 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 $\Sigma_x(A)$, $\text{Aut}_x(A)$ and the measure of maximal entropy are described by the following two statements.

Lemma 3.1. Let $A$ be a rational function of degree $n \geq 2$. Then $\sigma \in \text{Aut}_x(A)$ if and only if $A$ and $\sigma^{-1} \circ A \circ \sigma$ have a common iterate. In particular, if $\sigma \in \text{Aut}_x(A)$, then $A$ and $\sigma^{-1} \circ A \circ \sigma$ share the measure of maximal entropy.

Proof. The proof is trivial, given that rational functions sharing an iterate share a measure of maximal entropy. \hfill $\square$

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

Proof. The equality

$$A^l = A^l \circ \sigma, \quad l \geq 1,$$

implies that for any $k \geq l$ and $a \in \mathbb{CP}^1$ the transformation $\sigma$ maps the set of roots of the equation $A^k(z) = a$ to itself. Thus, for any set $S \subset \mathbb{CP}^1$ we have

$$|S \cap A^{-k}(a)| = |\sigma(S) \cap A^{-k}(a)|, \quad k \geq l, \quad a \in \mathbb{CP}^1,$$

implying that any $\sigma \in \Sigma_x(A)$ is $\mu_A$-invariant since $\mu_A$ is a limit of (18).

Let now $S$ be a Borel set on which $A \circ \sigma$ is injective. Then $A$ is injective on $\sigma(S)$, implying that

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

Thus, $\mu_A$ is the balanced measure for $A \circ \sigma$, and hence $\mu_A = \mu_{A \circ \sigma}$. \hfill $\square$

It was proved by Levin ([5], [6]) that for any rational function $A$ of degree $n \geq 2$ that is 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 $A$. Levin’s theorem combined with Lemma 3.1 and Lemma 3.2 implies the following result.
Theorem 3.3. Let $A$ be a rational function of degree $n \geq 2$ that is not conjugate to $z^{\pm n}$. Then the groups $\text{Aut}_x(A)$ and $\Sigma_x(A)$ are finite.

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

$$\sigma^{-1} \circ A \circ \sigma, \quad \sigma \in \text{Aut}_x(A),$$

is finite. On the other hand, the equality

$$\sigma^{-1} \circ A \circ \sigma = \sigma'^{-1} \circ A \circ \sigma', \quad \sigma' \in \text{Aut}(\mathbb{C}P^1),$$

implies that $\sigma' \circ \sigma^{-1} \in \text{Aut}(A)$. Thus, the finiteness of set (19) implies that there exist $\sigma_1, \sigma_2, \ldots, \sigma_l$ such that any $\sigma' \in \text{Aut}_x(A)$ has the form

$$\sigma' = \hat{\sigma} \circ \sigma_k,$$

for some $\hat{\sigma} \in \text{Aut}(A)$ and $k, 1 \leq k \leq l$. Since $\text{Aut}(A)$ is finite, this implies that $\text{Aut}_x(A)$ is also finite.

Similarly, it follows from Lemma 3.2 and Levin’s theorem that the set of functions $A \circ \sigma, \quad \sigma \in \Sigma_x(A)$, is finite, implying the finiteness of $\Sigma_x(A)$ since the equality

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

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

4. Groups $\widehat{G}(A^{\geq k})$ and $\text{Aut}_x(A)$

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

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

that is, as the set of Möbius transformation $\nu$ such that the equality

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

holds for some Möbius transformation $\mu$ and $k \geq 1$. 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 $A_1, A_2, \ldots, A_k$ and $B_1, B_2, \ldots, B_k$, $k \geq 2$, be rational functions of degree $n \geq 2$ such that

$$A_1 \circ A_2 \circ \cdots \circ A_k = B_1 \circ B_2 \circ \cdots \circ B_k.$$

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

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

$$\left|f^{-1}(T)\right| \leq \left|T\right|d.$$

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

$$2d - 2 = \sum_{z \in \mathbb{C}P^1} (\text{mult}_z f - 1)$$
implies that
\[ \sum_{z \in f^{-1}(T)} (\text{mult}_z f - 1) \leq 2d - 2. \]
Therefore,
\[ |f^{-1}(T)| = \sum_{z \in f^{-1}(T)} 1 \geq \sum_{z \in f^{-1}(T)} \text{mult}_z f - 2d = (|T| - 2)d + 2. \tag{23} \]

Let us denote by \( F \) the rational function defined by any of the parts of equality (21). 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 (22) that
\[ |F^{-1}\{c\}| \leq (n - 1)n^{k-1}. \tag{24} \]
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 (23) that
\[ |F^{-1}\{c\}| \geq (n^2 - 2)n^{k-2} + 2. \tag{25} \]
It follows now from (24) and (25) 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, \( c(A_1) \subseteq c(B_1 \circ B_2) \). \( \square \)

Theorem 4.1 implies the following statement.

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

**Proof.** Let \( \nu \) be an element of \( S(A) \). In case \( \nu \in \hat{G}(A) \), the statement of the theorem follows from Lemma 2.1, iii), since \( c(A) \subseteq c(A^{n^2}) \) by the chain rule. Similarly, if \( \nu \) belongs to \( \hat{G}(A^{n^2}) \), then \( \nu(c(A^{n^2})) = c(A^{n^2}) \), implying that
\[ \nu(c(A)) \subseteq \nu(c(A^{n^2})) = c(A^{n^2}). \]
Therefore, we may assume that \( \nu \in \hat{G}(A^{nk}) \) for some \( k \geq 3 \). Since equality (20) has the form (21) with
\[ A_1 = \nu \circ A, \quad A_2 = A_3 = \cdots = A_k = A, \]
and
\[ B_1 = B_2 = \cdots = B_{k-1} = A, \quad B_k = A \circ \mu, \]
applying Theorem 4.1 we conclude that \( c(\nu \circ A) \subseteq c(A^{n^2}) \). Taking into account that for any rational function \( A \) the equality
\[ c(\nu \circ A) = \nu(c(A)) \]
holds, this implies that \( \nu(c(A)) \subseteq c(A^{n^2}) \). \( \square \)

**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 \( \bigcup_{i=2}^{\infty} \hat{G}(A^{nk}) \) 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 \( \nu(c(A)) \subseteq c(A^{n^2}) \) 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 the first part of Lemma 2.2. Moreover, since \( |c(A)| \) and \( |c(A^{n^2})| \) 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 \( A^{n^2} \) is not a quasi-power by the second part of Lemma 2.2. To prove the finiteness of \( \bigcup_{i=2}^{\infty} \tilde{G}(A^{i k}) \) in this case, it is enough to show that for every \( \nu \in \tilde{G}(A^{i k}), k \geq 2 \), the inclusion

\[
\nu(c(A^{i k})) \subseteq c(A^{i 4})
\]

holds, and this can be done by a modification of the proof of Theorem 4.2. Indeed, equality (20) implies the equality

\[
\nu \circ A^{i 2 k} = A^{i k} \circ \mu \circ A^{k}
\]

which can be rewritten for \( k \geq 4 \) in the form (21) with

\[
A_1 = \nu \circ A^{i 2}, \quad A_2 = A_3 = \cdots = A_k = A^{i 2},
\]

and

\[
B_1 = \cdots = B_2 = A^{i 2}, \quad B_{k+1} = \mu \circ A^{i 2}, \quad B_{k+2} = \cdots = B_k = A^{i 2},
\]

if \( k \) is even, or

\[
B_1 = \cdots = B_{k+1} = A^{i 2}, \quad B_{k+1} = A \circ \mu \circ A, \quad B_{k+2} = \cdots = B_k = A^{i 2},
\]

if \( k \) is odd. Therefore, if \( \nu \) belongs to \( \tilde{G}(A^{i k}) \) for some \( k \geq 4 \), then applying Theorem 4.1, we conclude that (26) holds. On the other hand, if \( \nu \) belongs to \( \tilde{G}(A^{i 3}) \), then \( \nu(c(A^{i 2})) = c(A^{i 2}) \), by Lemma 2.1, iii), implying (26) by the chain rule. Similarly, if \( \nu \) belongs to \( \tilde{G}(A^{i 3}) \), then \( \nu(c(A^{i 3})) = c(A^{i 3}) \), implying that

\[
\nu(c(A^{i 2})) \subseteq \nu(c(A^{i 3})) = c(A^{i 3}) \subseteq c(A^{i 4}).
\]

Theorem 4.3 implies the following result.

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

Proof. The theorem is a direct corollary of Theorem 4.3.

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

**Proof of Theorem 1.2.** The boundedness of the set \( \bigcup_{i=2}^{\infty} \text{Aut}(A^{i k}) \) in terms of \( n \) for \( A \) that is not conjugate to \( z^n \) follows from Theorem 4.3. On the other hand, \( \text{Aut}(A) \) is finite and bounded in terms of \( n \) by Corollary 2.6. This proves the first part of the theorem. Finally, since the set \( S(A) \) contains the group \( \text{Aut}_{\infty}(A) \), the second part of the theorem follows from Theorem 4.2 (the assumption that \( A \) is not conjugate to \( z^n \) is actually redundant).
5. Groups $\Sigma_x(A)$ and $G(A^k)$

Let $A$ and $B$ be rational functions of degree at least two. We recall that the function $B$ is said to be \textit{semiconjugate} to the function $A$ if there exists a non-constant rational function $X$ such that the equality

\begin{equation}
A \circ X = X \circ B
\end{equation}

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

\[
\begin{array}{ccc}
\mathbb{C}P^1 & \xrightarrow{B} & \mathbb{C}P^1 \\
X & \downarrow & X \\
\mathbb{C}P^1 & \xrightarrow{A} & \mathbb{C}P^1
\end{array}
\]

The simplest examples of semiconjugate rational functions are provided by equivalent rational functions defined in the introduction. Indeed, it follows from equalities (5) that the diagrams

\[
\begin{array}{ccc}
\mathbb{C}P^1 & \xrightarrow{A} & \mathbb{C}P^1 \\
V & \downarrow & V \\
\mathbb{C}P^1 & \xrightarrow{\tilde{A}} & \mathbb{C}P^1
\end{array}
\]

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 (27) satisfying $\mathbb{C}(X, B) = \mathbb{C}(z)$, called \textit{primitive}, can be described in terms of group actions on $\mathbb{C}P^1$ or $\mathbb{C}$, implying strong restrictions on a possible form of $A, B$ and $X$. On the other hand, an arbitrary solution of equation (27) 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

\[B = \tilde{B} \circ W, \quad X = \tilde{X} \circ W\]

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

\[
\begin{array}{ccc}
\mathbb{C}P^1 & \xrightarrow{B} & \mathbb{C}P^1 \\
W & \downarrow & W \\
\mathbb{C}P^1 & \xrightarrow{W \circ \tilde{B}} & \mathbb{C}P^1 \\
\tilde{X} & \downarrow & \tilde{X} \\
\mathbb{C}P^1 & \xrightarrow{\tilde{A}} & \mathbb{C}P^1
\end{array}
\]

commutes. Thus, the triple $A, \tilde{X}, W \circ \tilde{B}$ is another solution of (27). This new solution is not necessarily primitive, however $\deg \tilde{X} < \deg X$. 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 (27) there exist rational functions $X_0, B_0, U$ such that $X = X_0 \circ U$, the diagram

\begin{equation}
\begin{array}{ccc}
\mathbb{CP}^1 & \xrightarrow{B} & \mathbb{CP}^1 \\
U & \downarrow & U \\
\mathbb{CP}^1 & \xrightarrow{B_0} & \mathbb{CP}^1 \\
X_0 & \downarrow & X_0 \\
\mathbb{CP}^1 & \xrightarrow{A} & \mathbb{CP}^1
\end{array}
\end{equation}

(28)

commutes, the triple $A, X_0, B_0$ is a primitive solution of (27), and $B_0 \sim B$.

The following theorem is essentially the second 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 $n \geq 2$. Then for every $\sigma \in \Sigma_E(A)$ the relation $A \circ \sigma \sim A$ holds.

**Proof.** Let $\sigma$ be an element of $\Sigma_E(A)$. Then

\begin{equation}
A^{\circ k} = A^{\circ k} \circ \sigma
\end{equation}

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

\begin{equation}
\begin{array}{ccc}
\mathbb{CP}^1 & \xrightarrow{A \circ \sigma} & \mathbb{CP}^1 \\
\downarrow A^{(k-1)} & & \downarrow A^{(k-1)} \\
\mathbb{CP}^1 & \xrightarrow{A} & \mathbb{CP}^1
\end{array}
\end{equation}

we see that to prove the theorem it is enough to show that in diagram (28), corresponding to the solution

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

of (27), 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 (27), the solution $A^{\circ l}, X, B^{\circ l}$, $l \geq 1$, is also primitive (see [16], Lemma 2.5). Second, a solution $A, X, B$ of (27) 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 see that the triple $A^{\circ (k-1)}, X_0, B_0^{\circ (k-1)}$ is a primitive solution of (27), and the algebraic curve

\begin{equation}
A^{\circ (k-1)}(x) - X_0(y) = 0
\end{equation}

(30)

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 (30). Moreover, if $\deg X_0 > 1$, then this component is proper. Therefore, $\deg X_0 = 1$. □
The following result proves the first part of Theorem 1.3 and thus finishes the proof of this theorem.

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

**Proof.** Let us observe first that it is enough to prove the theorem under the assumption that $A$ is not a quasi-power. Indeed, if $A$ is a quasi-power but is not conjugate to $z^{\pm n}$, then $A^{\pm 2}$ is not a quasi-power by Lemma 2.2. Therefore, if the theorem is true for functions that are not quasi-powers, then for any $A$ that is not conjugate to $z^{\pm n}$, the group $\Sigma_{x}(A^{\pm 2})$ is finite and bounded in terms of $n$, implying by (3) that the same is true for the group $\Sigma_{x}(A)$.

Assume now that $A$ is not a quasi-power. Then $G(A)$ is finite by Theorem 2.4. Let us recall that in view of equality (6) 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

\begin{equation}
|\Sigma_{x}(A)| \leq |G(A)|N_{A}.
\end{equation}

By Theorem 5.1, for any $\sigma \in \Sigma_{x}(A)$ 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 $\alpha \in \text{Aut}(\mathbb{C}P^{1})$, implying that

$$A \circ \sigma \circ \alpha \circ \sigma_{0}^{-1} = \alpha \circ A.$$

This is possible only if $\alpha$ belongs to the group $\hat{G}(A)$, and, in addition, $\sigma \circ \alpha \circ \sigma_{0}^{-1}$ belongs to the preimage of $\alpha$ under homomorphism (2). Therefore, for any fixed $\sigma_{0}$, there could be at most $|\hat{G}(A)|$ such $\alpha$, and for each $\alpha$ there could be at most $|\text{Ker} \gamma_{A}|$ elements $\sigma \in \Sigma_{x}(A)$ such that

$$\gamma_{A}(\sigma \circ \alpha \circ \sigma_{0}^{-1}) = \alpha.$$

Thus, (31) follows from (9).

It was 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 yields in particular that for a given rational function $B$ of degree $n \geq 2$ the number of conjugacy classes of rational functions $A$ such that (27) 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 implies that for non-special $A$ the number $N_{A}$ is bounded in terms of $n$. Moreover, it is easy to see that the same is true also for $A$ conjugate to $z^{\pm n}$ or $\pm T_{n}$, since any decomposition of $z^{n}$ has the form

$$z^{n} = (z^{d} \circ \mu) \circ (\mu^{-1} \circ z^{n/d})$$

where $\mu \in \text{Aut}(\mathbb{C}P^{1})$ and $d|n$, while any decomposition of $T_{n}$ has the form

$$T_{n} = (T_{d} \circ \mu) \circ (\mu^{-1} \circ T_{n/d})$$

where $\mu \in \text{Aut}(\mathbb{C}P^{1})$ and $d|n$.  

The above shows that to finish the proof of Theorem 5.2 we only must prove that the group $\Sigma_x(A)$ is finite and bounded in terms of $n$ if $A$ is a Lattés map. To prove the last statement, we recall that if $A$ is a Lattés map, then there exists an orbifold $O = (\mathbb{C}P^1, \nu)$ of zero Euler characteristic such that $A : O \to O$ is a covering map between orbifolds (see [10], [13] for more detail). Since this implies that $A^{\pm k} : O \to O$, $k \geq 1$, also is a covering map (see [11], Corollary 4.1), it follows from equality (29) that $\sigma : O \to O$ is a covering map (see [11], Corollary 4.2 and Lemma 4.1). As $\sigma$ is of degree one, the last condition simply means that $\sigma$ permutes points of the support of $O$. Since the support of an orbifold $O = (\mathbb{C}P^1, \nu)$ of zero Euler characteristic contains either three or four points, this implies that $\Sigma_x(A)$ is finite and uniformly bounded for any Lattés map $A$.

**Proof of Theorem 1.4.** If $\sigma \in \Sigma_x(A)$, then
\begin{equation}
A \circ \sigma \sim A,
\end{equation}
by Theorem 5.1. On the other hand, since for any indecomposable function $A$ the number $N_A$ obviously is equal to one, condition (32) is equivalent to the condition that
\begin{equation}
A \circ \sigma = \beta \circ A \circ \beta^{-1}
\end{equation}
for some $\beta \in \text{Aut}(\mathbb{C}P^1)$. Clearly, equality (33) implies that $\beta$ belongs to $\hat{G}(A)$. Therefore, if $\hat{G}(A)$ is trivial, then (32) is satisfied only if $A \circ \sigma = A$, that is, only if $\sigma$ belongs to $\Sigma_x(A)$. Thus, $\Sigma(A) = \Sigma_x(A)$, whenever $\hat{G}(A)$ is trivial.

Furthermore, it follows from equality (33) that $\sigma \circ \beta$ belongs to the preimage of $\beta$ under homomorphism (2). On the other hand, if $G(A) = \text{Aut}(A)$, this preimage consists of $\beta$ only. Therefore, in this case $\sigma \circ \beta = \beta$, implying that $\sigma$ is the identity map. Thus, the group $\Sigma_x(A)$ is trivial, whenever $G(A) = \text{Aut}(A)$.

The following theorem implies Theorem 1.1 from the introduction.

**Theorem 5.3.** Let $A$ be a rational function of degree $n \geq 2$. Then the orders of the groups $G(A^{\pm k})$, $k \geq 1$, are finite and uniformly bounded in terms of $n$ only, unless $A$ is a quasi-power. Furthermore, the orders of the groups $G(A^{\pm k})$, $k \geq 2$, 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 $\hat{G}(A^{\pm k})$, $k \geq 1$, and $\Sigma(A^{\pm k})$, $k \geq 1$, are finite and uniformly bounded in terms of $n$ only. Therefore, by (9), the orders of the groups $G(A^{\pm k})$, $k \geq 1$, also are finite and uniformly bounded. Similarly, the groups $G(A^{\pm k})$, $k \geq 2$, are finite and uniformly bounded in terms of $n$ only, unless $A$ is conjugate to $z^{\pm n}$.

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

**Proof.** For $A$ not conjugate to $z^{\pm n}$, the corollary follows from Theorem 5.3 since there exist only finitely many groups of any given order. Moreover, actually the groups $G(A^{\pm k})$, $k \geq 2$, belong to the list $A_4$, $S_4$, $A_5$, $C_l$, $D_{2l}$, by Theorem 2.4. On the other hand, if $A$ is conjugate to $z^{\pm n}$, then all the groups $G(A^{\pm k})$, $k \geq 1$, consist of the transformations $z \to c z^{\pm 1}$, $c \in \mathbb{C} \setminus \{0\}$.

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

**Example 5.5.** Let us consider the function
\[ A = x + \frac{27}{x^3}.\]
A calculation shows that, in addition to the critical value $\infty$, this function has critical values $\pm 4$ and $\pm 4i$, and
\[
A \pm 4 = \frac{(x^2 \mp 2x + 3)(x \pm 3)^2}{x^3},
\]
\[
A \pm 4i = \frac{(x^2 \mp 2ix - 3)(\pm x + 3i)^2}{x^3}.
\]
Since the above equalities imply that $\text{mult}_0 A = 3$, 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. This implies easily that $G(A)$ is a cyclic group of order two, and $G(A) = \text{Aut}(A)$. Finally, since $\text{mult}_0 A = 3$, 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 $z \rightarrow -z$. 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 $z \rightarrow -z$ and $z \rightarrow 1/z$. In particular, $\Sigma(A^{\circ 2})$ is larger than $\Sigma(A)$. Moreover, since
\[
A^{\circ 3} = -\frac{(z^4 - 1)^2}{z^8 + 6z^4 + 1},
\]
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 $\sigma$ of order $l > 4$ such that $\mu_1$ is an iterate of $\sigma$. 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, the fixed points of $\sigma$ are zero and infinity. Since $A$ is indecomposable, it follows from Theorem 5.1 that to exclude the second case it is enough to show that if $\sigma = cz$, $c \in \mathbb{C}\setminus\{0\}$, satisfies
\[
A \circ \sigma = \beta \circ A \circ \beta^{-1}, \quad \beta \in \text{Aut}(\mathbb{CP}^1),
\]
then $\sigma$ is an iterate of $\mu_1$. Since critical points of the function on the left side of (34) coincide with critical points of the function on the right side, the Möbius
transformation $\beta$ necessarily has the form $\beta = dz^{\pm 1}$, $d \in \mathbb{C}\setminus\{0\}$. Thus, equation (34) 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

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

One can check that 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 (see the next section).

6. Groups $G(A, z_0, z_1)$

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 $i = j (\text{mod } l)$. 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 $r$, $1 \leq r \leq l$. 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 $f^s$ is homozygous mod $l$, then $f^{ks}(z) = z$ for some integer $s \geq 1$. Our proof of Theorem 1.5 relies on this result.

**Proof of Theorem 1.5.** Without loss of generality, we can assume that $z_0 = 0$ and $z_1 = \infty$. 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 every element of $G(A, 0, \infty)$ has the form $z \to \varepsilon z$, where $\varepsilon$ is a root of unity, and $G(A, 0, \infty)$ is a finite cyclic group, whose order is equal to the maximum number $n$ such that $f_A$ is homozygous mod $n$. Since $f_A^{\pm k} = f_A^{-k}$, this implies that

$$G(A, 0, \infty) \subseteq G(A^{\pm k}, 0, \infty), \quad k \geq 1.$$ 

Moreover, if $G(A^{\pm k}, 0, \infty)$ is strictly larger than $G(A, 0, \infty)$ for some $k > 1$, then there exists $n_0$ such that $f_A$ is hybrid mod $n_0$ but $f_A^{\pm k}$ is homozygous mod $n_0$. Therefore, by the Reznick theorem, the equality $f_A^{\pm ks} = z$ holds for some $s \geq 1$. However, in this case by the analytical continuation $A^{\pm ks} = z$ for all $z \in \mathbb{C} \setminus \{0, \infty\}$, in contradiction with $n \geq 2$. Thus, the groups $G(A^{\pm k}, 0, \infty)$, $k \geq 1$, are equal.

Notice that the groups $G(A^{\pm k}, 0, z_1)$, $k \geq 1$, are equal even if $A$ is conjugate to $z^{\pm n}$. Indeed, for $A = z^{\pm n}$ these groups are trivial, unless $\{z_0, z_1\} = \{0, \infty\}$, while in the last case all these groups consist of the transformations $z \to cz^{\pm 1}$, $c \in \mathbb{C}\setminus\{0\}$.

Let us emphasize that since iterates $A^{\pm k}$, $k > 1$, have in general more fixed points than $A$, it may happen that $G(A^{\pm k}, z_0, z_1)$, $k > 1$, is non-trivial, while $G(A, z_0, z_1)$ is not defined, so that the equality $G(A^{\pm k}, z_0, z_1) = G(A, z_0, z_1)$ 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
\[ A^{g2} = -\frac{2z^2}{z^4 + 1}, \]
and the group $G(A^{g2}, 0, \infty)$ is a cyclic group of order four. Let us remark that Theorem 1.5 gives another proof of the fact that $\Sigma_{\sigma}(A)$ cannot contain an element $\sigma = cz, c \in \mathbb{C}\setminus\{0\}$, of order $l > 4$. Indeed, such $\sigma$ must belong to the group $G(A^{2k}, 0, \infty)$ for some $k \geq 1$, and hence to the group $G(A^{2k}, 0, \infty)$. However, $G(A^{2k}, 0, \infty)$ is equal to $G(A^{g2}, 0, \infty) = C_4$ by Theorem 1.5 applied to $A^{g2}$.

Under certain conditions, Theorem 1.5 permits to estimate the order of the groups $\text{Aut}_{\infty}(A)$ and $\Sigma_{\sigma}(A)$ and even to describe these groups explicitly.

**Theorem 6.1.** Let $A$ be a rational function of degree $n \geq 2$ that is not conjugate to $z^{\pm n}$. Assume that for some $k \geq 1$ the group $\text{Aut}(A^{\pm k})$ contains an element $\sigma$ of order at least six with fixed points $z_0$ and $z_1$ such that $z_0$ is a fixed point of $A^{\pm k}$. Then the inequality $|\text{Aut}_{\infty}(A)| \leq 2|G(A^{\pm k}, z_0, z_1)|$ holds. Similarly, if $\sigma$ as above is contained in $\Sigma(A^{\pm k})$, then $|\Sigma_{\sigma}(A)| \leq 2|G(A^{\pm k}, z_0, z_1)|$.

**Proof.** Since the maximal order of a cyclic subgroup in the groups $A_4, S_4, A_5$ is five, it follows from Corollary 2.6 that if $\text{Aut}(A^{\pm k})$ contains an element $\sigma$ of order $r > 5$, then either $\text{Aut}_{\infty}(A) = C_5$ or $\text{Aut}_{\infty}(A) = D_{2s}$, where $r|s$. Moreover, if $\sigma_{\infty}$ is an element of order $s$ in $\text{Aut}_{\infty}(A)$, then $\sigma$ is an iterate of $\sigma_{\infty}$. In particular, fixed points of $\sigma_{\infty}$ coincide with fixed points of $\sigma$.

To prove the theorem, we only must show that the inequality
\[ (35) \quad s > |G(A^{\pm k}, z_0, z_1)| \]
is impossible. Assume the inverse. Since $\sigma_{\infty}$ belongs to $\text{Aut}(A^{k'})$ for some $k' \geq 1$, it belongs to $\text{Aut}(A^{2kk'})$ and $G(A^{2kk'}, z_0, z_1)$. Therefore, if (35) holds, then the group $G(A^{2kk'}, z_0, z_1)$ contains an element of order greater than $|G(A^{\pm k}, z_0, z_1)|$, in contradiction with the equality
\[ G(A^{2kk'}, z_0, z_1) = G(A^{\pm k}, z_0, z_1), \]
provided by Theorem 1.5 applied to $G(A^{\pm k})$. The proof of the inequality for $|\Sigma_{\sigma}(A)|$ is similar. \qed

**Example 6.2.** Let us consider the function
\[ A = z \frac{z^6 - 2}{2z^6 - 1} \]
It is easy to see that $\text{Aut}(A)$ contains the dihedral group $D_{12}$ generated by the transformations
\[ z \rightarrow e^{\frac{2\pi}{12}} z, \quad z \rightarrow \frac{1}{z}. \]
Since zero is a fixed point of $A$ and $G(A, 0, \infty) = C_6$, it follows from Theorem 6.1 that
\[ \text{Aut}_{\infty}(A) = \text{Aut}(A) = D_{12}. \]

Although the group $\text{Aut}(A^{\pm k})$ does not necessarily contain an element that belongs to $G(A^{\pm k}, z_0, z_1)$, it always contains an element that belongs to $G(A^{2k}, z_0, z_1)$. More generally, the following statement holds.
Lemma 6.3. Let $A$ be a rational function of degree $n \geq 2$, and $\sigma \notin \Sigma(A^{2k})$ a Möbius transformation such that the equality
\begin{equation}
A^{2k} \circ \sigma = \sigma^{cl} \circ A^{2k},
\end{equation}
holds for some $l \geq 1$. Then at least one of the fixed points $z_0, z_1$ of $\sigma$ is a fixed point of $A^{2k}$, and if $z_0$ is such a point, then $\sigma \in G(A^{2k}, z_0, z_1)$.

Proof. Clearly, equality (36) implies the equalities
\[
\sigma^{cl}(A^{2k}(z_0)) = A^{2k}(z_0), \quad \sigma^{cl}(A^{2k}(z_1)) = A^{2k}(z_1).
\]
However, since $\sigma^{cl}$ is not the identity map, it has only two fixed points $z_0, z_1$. Therefore, $A^{2k}\{z_0, z_1\} \subseteq \{z_0, z_1\}$, implying that at least one of the points $z_0, z_1$ is a fixed point of $A^{2k}$. Finally, if $z_0$ is such a point, then $\sigma \in G(A^{2k}, z_0, z_1)$. □

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

Theorem 6.4. Let $A$ be a rational function of degree $n \geq 2$ that is not conjugate to $z^\pm n$. Assume that for some $k \geq 1$ the group $\text{Aut}(A^{2k})$ contains an element $\sigma$ of order at least six with fixed points $z_0, z_1$. Then $|\text{Aut}_{\Sigma}(A)| \leq 2|G(A^{2k}, z_0, z_1)|$, where $z_0$ is a fixed point of $\sigma$ that is also a fixed point of $A^{2k}$. □

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 69 (2001), no. 3-4, 432-33.

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

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

[8] 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.

[9] F. Pakovich, On semiconjugate rational functions, Geom. Dedic., 26 (2016), 1217-1243.

[10] F. Pakovich, Reconstructing rational functions, Int. Math. Res. Not., 2019, no. 7, 1921-1935.

[11] F. Pakovich, On generalized Latbes maps, J. Anal. Math., 142 (2020), no. 1, 1-39.

[12] H. Ye, Rational functions with identical measure of maximal entropy, Adv. Math. 268 (2015), 373-395.