Commuting rational functions revisited

FEDOR PA KovICH

Department of Mathematics, Ben Gurion University, P.O. Box 653, Beer Sheva, 8410501, Israel
(e-mail: pakovich@math.bgu.ac.il)

(Received 15 February 2019 and accepted in revised form 12 June 2019)

Abstract. Let \( B \) be a rational function of degree at least two that is neither a Lattès map nor conjugate to \( z^{\pm n} \) or \( \pm T_n \). We provide a method for describing the set \( C_B \) consisting of all rational functions commuting with \( B \). Specifically, we define an equivalence relation \( \sim_B \) on \( C_B \) such that the quotient \( C_B/\sim_B \) possesses the structure of a finite group \( G_B \), and describe generators of \( G_B \) in terms of the fundamental group of a special graph associated with \( B \).

Key words: commuting rational functions, the Ritt theorem, common iterates
2010 Mathematics Subject Classification: 30D05 (Primary); 37F10 (Secondary)

1. Introduction
In this paper, we study commuting rational functions, that is rational solutions of the functional equation

\[ B \circ X = X \circ B. \]

More precisely, we fix a function \( B \in \mathbb{C}(z) \) of degree at least two and study the set \( C_B \) consisting of all \( X \in \mathbb{C}(z) \) such that (1) holds.

Functional equation (1) has been investigated previously by Julia [3] and Fatou [2]. In particular, they showed that commuting rational functions \( X \) and \( B \) of degree at least two have the same Julia set \( J = J(X) = J(B) \). Using Poincaré functions, Julia and Fatou proved that if \( X \) and \( B \) have no iterate in common and \( J \neq \mathbb{C}P^1 \), then, up to a conjugacy, \( X \) and \( B \) are either powers or Chebyshev polynomials. The assumption \( J \neq \mathbb{C}P^1 \) was removed by Ritt [13], who used a topological-algebraic method. Ritt proved that solutions of (1) having no iterate in common reduce to powers, to Chebyshev polynomials, or to Lattès maps. A proof of the Ritt theorem based on modern dynamical methods was given by Eremenko [1].
All the above results assume that $X$ and $B$ have no iterate in common. However, commuting rational functions $X$ and $B$ such that

$$B^{ol} = X^{ok}$$

(2)

for some $l, k \geq 1$ also exist. The simplest examples of such functions can be obtained by setting

$$X = R^{ol_1}, \quad B = R^{ol_2},$$

where $R$ is an arbitrary rational function and $l_1, l_2 \geq 1$. More generally, denoting by Aut($R$) the group of Möbius transformations commuting with $R$, we can set

$$X = \mu_1 \circ R^{ol_1}, \quad B = \mu_2 \circ R^{ol_2},$$

(3)

where $\mu_1$ and $\mu_2$ are elements of Aut($R$) commuting between themselves. However, it has been shown already by Ritt [13] that commuting rational functions satisfying (2) are not exhausted by functions of the form (3). Although Ritt’s method provides some insight into the structure of commuting rational functions $X$ and $B$ satisfying (2), it does not permit the description of this class of functions in an explicit way, and Ritt concluded his paper by saying: ‘we think that the example given above makes it conceivable that no great order may reign in this class’.

Functional equation (1) is a particular case of the functional equation

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

(4)

where $A$ and $B$ are rational functions of degree at least two. In case that (4) is satisfied for some rational function $X$ of degree at least two, the function $B$ is called semiconjugate to the function $A$. Semiconjugate rational functions were investigated in the recent papers [5, 6, 8–10]. In particular, it was shown in [6] that solutions of (4) 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 $X$. Any solution of (4) reduces to a primitive one by a certain iterative process, and the quantitative aspects of this reduction were studied in [5]. In particular, it was shown in [5] that if a rational function $B$ is not special, that is, if $B$ is neither a Lattès map nor conjugate to $z^{\pm n}$ or $\pm T_n$, then solutions of equations (1) and (4) obey some finiteness conditions.

Specifically, with regards to equation (1), it was shown in [5] that if $B$ is not special, then there exist finitely many rational functions $X_1, X_2, \ldots, X_r$ such that $X$ commutes with $B$ if and only if

$$X = X_j \circ B^{ok}$$

for some $j, 1 \leq j \leq r$, and $k \geq 0$. Moreover, the number $r$ and the degrees of $X_j, 1 \leq j \leq r$, can be bounded by numbers depending on deg $B$ only. Note that this result immediately implies the Ritt theorem. Indeed, if $X$ commutes with $B$, then any iterate $X^{ol}, l \geq 1$, does. Thus, by the Dirichlet box principle, there exist distinct $l_1, l_2$ such that

$$X^{ol_1} = X_j \circ B^{ok_1}, \quad X^{ol_2} = X_j \circ B^{ok_2}$$

for the same $j$ and some $k_1, k_2 \geq 0$. Therefore, if, say, $l_2 > l_1$, then

$$X^{ol_2} = X^{ol_1} \circ B^{ok_2 - k_1},$$

implying that (2) holds for $l = l_2 - l_1$ and $k = k_2 - k_1$, since $X$ and $B$ commute.
In this paper, we provide a method for describing the set $C_B$ for non-special $B$. For such $B$, essentially all the information about $C_B$ provided by the Ritt method reduces to the fact that any element of $C_B$ has a common iterate with $B$. Thus, new approaches and techniques are needed, and we develop them in this paper. Our main results are as follows. First, for any non-special rational function $B$, we define an equivalence relation $\sim_B$ on the set $C_B$ such that the quotient $C_B/\sim_B$ possesses the structure of a finite group $G_B$. Second, we describe generators of this group in terms of the fundamental group of a special graph associated with $B$, providing a method for describing $C_B$. Finally, we calculate $G_B$ for several classes of rational functions. Note that our method of describing $C_B$ reduces the problem to the easier problem of finding all functional decompositions $F = U \circ V$ for finitely many rational functions $F$.

In more detail, for a non-special rational function $B$, we define an equivalence relation $\sim_B$ on the set $C_B$, setting $A_1 \sim_B A_2$ if

$$A_1 \circ B^{l_1} = A_2 \circ B^{l_2}$$

for some $l_1 \geq 0$, $l_2 \geq 0$, and show that the multiplication of classes induced by the functional composition of their representatives provides $C_B/\sim_B$ with the structure of a finite group $G_B$. The group structure on $C_B/\sim_B$ offers a new look at the problem of describing $C_B$, and permits the characterization of properties of $C_B$ in group theoretic terms. For example, the group $G_B$ is trivial if and only if any element of $C_B$ is an iterate of $B$, while $G_B$ is isomorphic to $\text{Aut}(B)$ if and only if any element of $C_B$ can be represented in the form $X = \mu \circ B^k$, where $\mu \in \text{Aut}(B)$ and $k \geq 0$.

We describe generators of $G_B$ using a special finite graph $\Gamma_B$ defined as follows. Let $B$ be a rational function. We say that a rational function $\hat{B}$ is an elementary transformation of $B$ if there exist rational functions $U$ and $V$ such that $B = V \circ U$ and $\hat{B} = U \circ V$. We say that rational functions $B$ and $A$ are equivalent and write $A \sim B$ if there exists a chain of elementary transformations between $B$ and $A$ (this equivalence relation should not be confused with the previous one where the subscript $B$ is used). Since for any Möbius transformation $\mu$ the equality

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

holds, the equivalence class $[B]$ of a rational function $B$ is a union of conjugacy classes. Moreover, by the result of [9], the class $[B]$ consists of finitely many conjugacy classes, unless $B$ is a flexible Lattès map. The graph $\Gamma_B$ is defined as a multigraph whose vertices are in a one-to-one correspondence with some fixed representatives $B_i$ of conjugacy classes in $[B]$, and whose multiple edges connecting the vertices corresponding to $B_i$ to $B_j$ are in a one-to-one correspondence with solutions of the system

$$B_i = V \circ U, \quad B_j = U \circ V$$

in rational functions. In these terms, the main result of the paper about the group $G_B$ is a construction of a group epimorphism from the fundamental group of the graph $\Gamma_B$ to the group $G_B$.

The paper is organized as follows. In §2, we describe the set $C_B$ in terms of elementary transformations. In §3, we define the group $G_B$. In §§4 and 5, we define the graph $\Gamma_B$.
and construct a group epimorphism from $\pi_1(\Gamma_B)$ to $G_B$. We also show that if $A \sim B$, then the groups $G_A$ and $G_B$ are isomorphic. Note that this implies, in particular, that if $A$ is a rational function such that the group $\text{Aut}(A)$ is non-trivial, then for any rational function $B \sim A$ the group $G_B$ is also non-trivial, even though $\text{Aut}(B)$ can be trivial. In the last case, functions of degree one in $C_A$ give rise to functions of higher degree in $C_B$ through the isomorphism $G_A \cong G_B$.

In §6, we calculate the group $G_B$ for certain classes of rational functions, and consider some examples. Specifically, we show that for a wide class of rational functions, which we call generically decomposable, $G_B$ is isomorphic to $\text{Aut}(B)$. We also show that for a polynomial $B$ the group $G_B$ is metacyclic. Finally, we discuss in detail the example of commuting rational functions $B$ and $X$ satisfying condition (2) from the paper of Ritt [13]. In particular, we calculate the group $G_B$ that turns out to be a cyclic group of order three. We also provide a different example of this kind.

2. The set $C_B$ and elementary transformations

Let $B$ be a rational function of degree at least two. We denote by $C_B$ the set of all rational functions commuting with $B$.

**Lemma 2.1.** The set $C_B$ is closed with respect to the operation of composition, that is, $A_1, A_2 \in C_B$ implies $A_1 \circ A_2 \in C_B$. Furthermore, if $A \circ U \in C_B$ and $U \in C_B$, then $A \in C_B$.

**Proof.** Indeed, if $A_1, A_2 \in C_B$, then

$$A_1 \circ A_2 \circ B = A_1 \circ B \circ A_2 = B \circ A_1 \circ A_2.$$  

On the other hand, if $A \circ U \in C_B$ and $U \in C_B$, then

$$B \circ A \circ U = A \circ U \circ B = A \circ B \circ U,$$

implying that

$$B \circ A = A \circ B.$$

We emphasize that we allow to elements of $C_B$ to have degree one, that is to Möbius transformations. All Möbius transformations commuting with $B$ obviously form a group denoted by $\text{Aut}(B)$ and called the *symmetry group* of $B$. Since any $\mu \in \text{Aut}(B)$ maps periodic points of $B$ of order $l \geq 1$ to themselves, and any Möbius transformation is defined by its values at any three points, the symmetry group of any rational function is finite. In particular, $\text{Aut}(B)$ is one of the five well-known finite rotation groups of the sphere: $A_4$, $S_4$, $A_5$, $C_n$, $D_{2n}$. Note that the property of $\mu \in \text{Aut}(B)$ to map periodic points of $B$ to periodic points can be used for a practical description of $\text{Aut}(B)$.

Let $B$ be a rational function. A rational function $\widehat{B}$ is called an *elementary transformation* of $B$ if there exist rational functions $U$ and $V$ such that $B = V \circ U$ and $\widehat{B} = U \circ V$. We say that rational functions $B$ and $A$ are *equivalent* and write $A \sim B$ if there exists a chain of elementary transformations between $B$ and $A$. Since for any Möbius transformation $\mu$ the equality

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

Downloaded from https://www.cambridge.org/core. 31 Dec 2020 at 07:53:34, subject to the Cambridge Core terms of use.
Commuting rational functions revisited

holds, the equivalence class \([B]\) of a rational function \(B\) is a union of conjugacy classes. Thus, the relation \(\sim\) can be considered as a weaker form of the classical conjugacy relation. The equivalence class \([B]\) contains infinitely many conjugacy classes if and only if \(B\) is a flexible Lattès map [9].

The following lemma is obtained by a direct calculation (see [10, Lemma 3.1]).

**Lemma 2.2.** Let

\[ L : B \rightarrow B_1 \rightarrow B_2 \rightarrow \cdots \rightarrow B_s \]  

be a sequence of elementary transformations, and \(U_i, V_i, 1 \leq i \leq s\), rational functions such that

\[ B = V_1 \circ U_1, \quad B_i = U_i \circ V_i, \quad 1 \leq i \leq s, \]

and

\[ U_i \circ V_i = V_{i+1} \circ U_{i+1}, \quad 1 \leq i \leq s - 1. \]

Then the functions

\[ U = U_s \circ U_{s-1} \circ \cdots \circ U_1, \quad V = V_1 \circ \cdots \circ V_{s-1} \circ V_s \]

make the diagram

\[
\begin{array}{ccc}
\mathbb{CP}^1 & \xrightarrow{B} & \mathbb{CP}^1 \\
U \downarrow & & U \downarrow \\
\mathbb{CP}^1 & \xrightarrow{B_s} & \mathbb{CP}^1 \\
V \downarrow & & V \downarrow \\
\mathbb{CP}^1 & \xrightarrow{B} & \mathbb{CP}^1 \\
\end{array}
\]

commutative and satisfy the equalities

\[ V \circ U = B_s^\circ, \quad U \circ V = B_s^\circ. \]

It follows from Lemma 2.2, that any sequence of elementary transformations (5) such that \(B_s = B\) gives rise to a rational function \(U\) commuting with \(B\), and the main result of this section states that for non-special \(B\) any element of \(C_B\) can be obtained in this way.

**Theorem 2.3.** Let \(B\) be a non-special rational function of degree at least two. Then a rational function \(X\) belongs to \(C_B\) if and only if there exists a sequence of elementary transformation (5) such that \(B_s = B\) and \(X = U_s \circ U_{s-1} \circ \cdots \circ U_1\).

The proof of Theorem 2.3 uses the following two lemmas which are particular cases of [6, Lemma 2.1] and [5, Theorem 2.18], respectively. For the reader’s convenience, we provide short independent proofs. We recall that a solution \(A, X, B\) of (4) is called *primitive* if \(\mathbb{C}(X, B) = \mathbb{C}(z)\). We also mention that for an arbitrary solution \(A, X, B\) of (4) the equality

\[ \deg A = \deg B \]  

holds.
LEMMA 2.4. A solution \( A, X, B \) of (4) is primitive if and only if the algebraic curve

\[ A(x) - X(y) = 0 \]  

(8)

is irreducible.

Proof. By the Lüroth theorem, there exists a rational function \( W \) such that \( \mathbb{C}(X, B) = \mathbb{C}(W) \), implying that the equalities

\[ X = X' \circ W, \quad B = B' \circ W \]  

(9)

hold for some rational functions \( X' \) and \( B' \) with \( \mathbb{C}(X', B') = \mathbb{C}(z) \). Clearly, \( x = X'(t) \), \( y = B'(t) \) is a generically one-to-one parametrization of some irreducible component

\[ C : F(x, y) = 0 \]

of (8). Furthermore, since the degree of the projection of \( C \) on \( x \) (respectively, \( y \)) is equal to \( \deg X' \) (respectively, \( \deg B' \)) the equalities

\[ \deg_x F = \deg B', \quad \deg_y F = \deg X' \]  

(10)

hold. If \( \mathbb{C}(X, B) = \mathbb{C}(z) \), then \( \deg W = 1 \), and it follows from equalities (9), (10), and (7) that the curve \( C \) coincides with curve (8), implying that (8) is irreducible. On the other hand, if \( \mathbb{C}(X, B) \neq \mathbb{C}(z) \), then \( \deg W > 1 \), and equalities (9), (10), and (7) imply that \( C \) is a proper component of (8). \( \square \)

LEMMA 2.5. Let \( A, X, B \) be a primitive solution of (4). Then for any \( l \geq 1 \), the solution \( A^l, X, B^l \) is also primitive.

Proof. The proof is by induction on \( l \). For \( l = 1 \), the lemma is trivially true. Assume that it is true for all \( k \leq l \). By Lemma 2.4, this implies that the algebraic curve

\[ C_k : A^{\circ k}(x) - X(y) = 0 \]

is irreducible for all \( k \leq l \), and

\[ R_k : x = X(t), \quad y = B^{\circ k}(t) \]

is its generically one-to-one parametrization.

Let \( P_1, P_2 \) be arbitrary rational functions satisfying the equality

\[ A^{\circ(l+1)} \circ P_1 = X \circ P_2. \]  

(11)

Since the curve \( C_l \) is irreducible and \( R_l \) is its generically one-to-one parametrization, the equality

\[ A^{\circ(l+1)} \circ P_1 = A^{\circ l} \circ (A \circ P_1) = X \circ P_2 \]

implies that

\[ A \circ P_1 = X \circ W, \quad P_2 = B^{\circ l} \circ W \]

for some \( W \in \mathbb{C}(z) \). Furthermore, since the curve \( C_1 \) is also irreducible, it follows from the first of these equalities that

\[ P_1 = X \circ U, \quad W = B \circ U \]
Commuting rational functions revisited

for some $U \in \mathbb{C}(z)$. Thus, any pair of rational functions $P_1, P_2$ satisfying (11) has the form

$$P_1 = X \circ U, \quad P_2 = B^{o(l+1)} \circ U$$

for some $U \in \mathbb{C}(z)$. In particular, this implies that if the equalities

$$X = P_1 \circ W, \quad B^{o(l+1)} = P_2 \circ W$$

hold for some $P_1, P_2, W \in \mathbb{C}(z)$, then $\deg W = 1$, since $P_1, P_2$ in (12) satisfy (11). Therefore, $\mathbb{C}(X, B^{o(l+1)}) = \mathbb{C}(z)$, that is, $A^{o(l+1)}, X, B^{o(l+1)}$ is a primitive solution. □

Proof of Theorem 2.3. The sufficiency follows from Lemma 2.2. In the other direction, assume that $X \in C_B$. If $X$ is a M"obius transformation, then the sequence

$$B = (B \circ X^{-1}) \circ X \rightarrow X \circ (B \circ X^{-1}) = B$$

is as required. Thus, assume that $\deg X \geq 2$.

We observe first that there exist a sequence (5) and a commutative diagram

$$\begin{array}{c}
\mathbb{C}\mathbb{P}^1 \quad \xrightarrow{B} \quad \mathbb{C}\mathbb{P}^1 \\
\downarrow U \quad \quad \quad \downarrow U \\
\mathbb{C}\mathbb{P}^1 \quad \xrightarrow{B_s} \quad \mathbb{C}\mathbb{P}^1 \\
\downarrow X_0 \quad \quad \quad \downarrow X_0 \\
\mathbb{C}\mathbb{P}^1 \quad \xrightarrow{B} \quad \mathbb{C}\mathbb{P}^1
\end{array}$$

such that $U$ is defined by (6), the equality $X = X_0 \circ U$ holds, and the triple $B, X_0, B_s$ is a primitive solution of (4). Indeed, if $B, X, B$ is a primitive solution of (4), we can set $U = z$, $X_0 = X$, and $B_s = B$. Otherwise, $\mathbb{C}(X, B) = \mathbb{C}(W)$ for some $W$ with $\deg W > 1$, and substituting equalities (9) in (4) we see that the diagram

$$\begin{array}{c}
\mathbb{C}\mathbb{P}^1 \quad \xrightarrow{B} \quad \mathbb{C}\mathbb{P}^1 \\
\downarrow W \quad \quad \quad \downarrow W \\
\mathbb{C}\mathbb{P}^1 \quad \xrightarrow{W \circ B'} \quad \mathbb{C}\mathbb{P}^1 \\
\downarrow X' \quad \quad \quad \downarrow X' \\
\mathbb{C}\mathbb{P}^1 \quad \xrightarrow{B} \quad \mathbb{C}\mathbb{P}^1
\end{array}$$

commutes. If the solution $B, X', W \circ B'$ of (4) is primitive, we are done. Otherwise, we can apply the above transformation to this solution. Since $\deg X' < \deg X$, it is clear that after a finite number of steps we obtain a sequence of elementary transformations (5) and functions $U, X_0, B_s$ as required.

To prove Theorem 2.3, we only must show that $\deg X_0 = 1$. Indeed, in this case changing $U_s$ to $X_0 \circ U_s$ and $B_s$ to $X_0 \circ B_s \circ X_0^{-1}$, without loss of generality we may assume that $X_0 = z$, so that $B_s = B$ and (5) is the sequence required. Assume, in contrast, that $\deg X_0 > 1$. By Lemma 2.5, for any $l \geq 1$ the triple $B^{ol}, X_0, B_s^{ol}$ is a primitive solution.
of (4). On the other hand, by the Ritt theorem, there exist \( k \) and \( l \) such that equality (2) holds. Thus,

\[
B^{ol} = X^{ok} = X_0 \circ (U \circ X^{ok-1}),
\]

implying that the curve

\[
(U \circ X^{ok-1})(x) - y = 0
\]
is a component of the curve

\[
B^{ol}(x) - X_0(y) = 0.
\]

Moreover, this component is proper because \( \deg X_0 > 1 \). Since, by Lemma 2.4, this contradicts the fact that \( B^{ol}, X_0, B^{ol}_s \) is a primitive solution of (4), we conclude that \( \deg X_0 = 1 \). \( \square \)

3. The group \( G_B \)

Define an equivalence relation on the set \( C_B \), setting \( A_1 \sim A_2 \) if

\[
A_1 \circ B^{ol_1} = A_2 \circ B^{ol_2}
\]
for some \( l_1 \geq 0, l_2 \geq 0 \) (in order to distinguish this relation from the relation \( \sim \) introduced in the previous section we use the subscript \( B \)). It is easy to see that \( \sim \) is really an equivalence relation. Indeed, \( \sim \) is clearly reflexive and symmetric. Furthermore, if equalities (13) and

\[
A_2 \circ B^{on_1} = A_3 \circ B^{on_2}
\]
hold, and \( n_1 \geq l_2 \), then

\[
A_1 \circ B^{ol_1(n_1+n_2-l_2)} = A_2 \circ B^{on_1} = A_3 \circ B^{on_2},
\]
implying that \( A_1 \sim A_3 \). Similarly, if \( l_2 \geq n_1 \), then

\[
A_3 \circ B^{ol_2(n_2+l_2-n_1)} = A_2 \circ B^{ol_2} = A_1 \circ B^{ol_1}.
\]

Lemma 3.1. Let \( A \) be an equivalence class of \( \sim \). For any \( n \geq 1 \), the class \( A \) contains at most one rational function of degree \( n \). Furthermore, if \( A_0 \in A \) is a function of minimal possible degree, then any \( A \in A \) has the form \( A = A_0 \circ B^{ol_1} \), \( l \geq 1 \). Alternatively, the function \( A_0 \) can be described as a unique function in \( A \) that is not a rational function in \( B \).

Proof. If \( \deg A_1 = \deg A_2 \) in (13), then \( l_1 = l_2 \), implying that \( A_1 = A_2 \). Furthermore, if

\[
A \circ B^{ol_1} = A_0 \circ B^{ol_2}
\]
and \( l_1 > l_2 \), then

\[
A_0 = A \circ B^{ol_1(l_2-l_1)},
\]
implying that \( \deg A < \deg A_0 \) in contradiction with the assumption. Therefore, \( l_1 \leq l_2 \) and, hence,

\[
A = A_0 \circ B^{ol_1(l_2-l_1)}.
\]
Moreover, $A_0$ is not a rational function in $B$, since if $A_0 = A' \circ B$, then $A'$ commutes with $B$ by Lemma 2.1, implying that $A' \sim A_0$ and $\deg A' < \deg A_0$. On the other hand, if $A$ is an other function in the class $A$ that is not a rational function in $B$, then (14) implies that $l_1 = l_2$ and $A = A_0$. \hfill \Box

For a rational function $B$, we denote by $G_{B}$ the set of equivalence classes of $\sim_{B}$ on $C_B$. We define a binary operation on the set $G_B$ as follows. If $A_1$ and $A_2$ are equivalence classes of $\sim_{B}$, and $A_1 \in A_1$ and $A_2 \in A_2$ are their representatives, then $A_1 \cdot A_2$ is defined as the equivalence class containing $A_1 \circ A_2$. It is easy to see that this operation is well defined. Indeed, assume that $A_1 \sim A_1'$ and $A_2 \sim A_2'$. Then

$$A_1 \circ B^{l_1} = A_1' \circ B^{l_1'}$$

and

$$A_2 \circ B^{l_2} = A_2' \circ B^{l_2'},$$

implying that

$$A_1 \circ B^{l_1} \circ A_2 \circ B^{l_2} = A_1' \circ B^{l_1'} \circ A_2' \circ B^{l_2'}.$$  \hspace{1cm} (15)

Since $A_1, A_2 \in C_B$, equality (15) implies that

$$A_1 \circ A_2 \circ B^{l_1 + l_2} = A_1' \circ A_2' \circ B^{l_1' + l_2'},$$

and, hence,

$$A_1 \circ A_2 \sim B_{B} A_1' \circ A_2'.$$

**Theorem 3.2.** The set $G_B$ equipped with the operation $\cdot$ is a finite group.

**Proof.** By definition, if $A_i \in A_i, \ 1 \leq i \leq 3$, then $(A_1 \cdot A_2) \cdot A_3$ and $A_1 \cdot (A_2 \cdot A_3)$ are classes containing the functions $(A_1 \circ A_2) \circ A_3$ and $A_1 \circ (A_2 \circ A_3)$, respectively. On the other hand,

$$(A_1 \circ A_2) \circ A_3 = A_1 \circ (A_2 \circ A_3),$$

since $\circ$ is an associative operation on the set of rational functions. Therefore, the classes $(A_1 \cdot A_2) \cdot A_3$ and $A_1 \cdot (A_2 \cdot A_3)$ coincide, and, hence, the operation $\cdot$ satisfies the associativity axiom.

Clearly, the class $e$ containing the function $z$ and consisting of all iterates of $B$ serves as the unit element. Moreover, for any class $X$ there exists a class $X^{-1}$ such that

$$X \cdot X^{-1} = X^{-1} \circ X = e.$$  \hspace{1cm} (16)

Indeed, by Theorem 2.3, for any $X \in X$ there exists a sequence of elementary transformation (5) such that

$$X = U_s \circ U_{s-1} \circ \cdots \circ U_1.$$ 

Further, it follows from Lemma 2.2 that the function

$$Y = V_s \circ V_{s-1} \circ \cdots \circ V_1$$
belongs to $C_B$, and the functions $X$ and $Y$ satisfy

$$X \circ Y = Y \circ X = B^s.$$  

Therefore, condition (16) holds for $X^{-1}$ defined as the class containing the rational function $Y$.

Finally, by the result of [5] cited in the introduction, there exist at most finitely many rational functions $A \in C_B$ which are not rational functions in $B$, implying by Lemma 3.1 that the group $G_B$ is finite. □

Note that the above proof provides a method for the actual finding $X^{-1}$. On the other hand, merely the existence of the inverse element follows from the Ritt theorem. Indeed, since for any $X \in \mathcal{X}$ there exist $l, k \geq 1$ such that (2) holds, for any class $X$ there exists $k$ such that $X^k = e$, implying that (16) holds for $X^{-1} = X^{k-1}$. Note also that the Ritt theorem by itself does not imply that the group $G_B$ is finite, although it does imply that any its element has finite order.

For $X \in C_B$, we denote by $X$ the element of $G_B$ corresponding to the equivalence class of $\sim_B$ containing $X$.

**Lemma 3.3.** The map $\mu \to \mu$ is a group monomorphism from the group $\text{Aut}(B)$ to the group $G_B$.

**Proof.** Since functions from $\text{Aut}(B)$ have degree one, it follows from Lemma 3.1 that $\mu_1 = \mu_2$ if and only if $\mu_1 = \mu_2$. Therefore, the map $\tau : \mu \to \mu$ is injective, and it is easy to see that $\tau$ is a homomorphism of groups. □

We denote the image of $\text{Aut}(B)$ in $G_B$ under the group monomorphism $\mu \to \mu$ by $\text{Aut}_G(B)$.

**Lemma 3.4.** The following conditions are equivalent.

1. Any $X \in C_B$ has the form $X = \mu \circ B^{ol}$ for some $\mu \in \text{Aut}(B)$ and $l \geq 0$.
2. Any $X \in C_B$ of degree at least two is a rational function in $B$.
3. The group $G_B$ coincides with $\text{Aut}_G(B)$.

**Proof.** It is easy to see that (1) and (3) are equivalent, and that (1) implies (2). Assume now that (2) holds, and let $X \in C_B$ be a function of degree at least two. By the assumption, $X = R_1 \circ B$ for some $R \in \mathbb{C}(z)$. Moreover, since by Lemma 2.1 the function $R_1$ belongs to $C_B$, using (2) again we conclude that either $R_1 \in \text{Aut}(B)$, or there exists $R_2 \in \mathbb{C}(z)$ such that $R_1 = R_2 \circ B$ and $R_2 \in C_B$. It is clear that continuing this process we will eventually obtain a representation $X = \mu \circ B^l$ for some $\mu \in \text{Aut}(B)$ and $l \geq 1$. □

**4. The graph $\Gamma_B$**

Let $B$ be a rational function of degree at least two. Define $\Gamma_B$ as a multigraph whose vertices are in a one-to-one correspondence with some fixed representatives of conjugacy classes in $[B]$, and whose multiple edges connecting vertices corresponding to representatives $B_i$ and $B_j$ are in a one-to-one correspondence with solutions of the system

$$B_i = V \circ U, \quad B_j = U \circ V$$  \hspace{1cm} (17)
in rational functions. Note that $\Gamma_B$ have loops. They correspond to solutions of
\[ B_i = U \circ V = V \circ U. \]

**Lemma 4.1.** The graph $\Gamma_B$ does not depend on the choice of representatives of conjugacy classes in $[B]$.

**Proof.** Indeed, for any M"obius transformations $\alpha$ and $\beta$, to a solution $U, V$ of system (17) corresponds a solution
\[ U' = \beta \circ U \circ \alpha^{-1}, \quad V' = \alpha \circ V \circ \beta^{-1} \]
(18) of the system
\[ \alpha \circ B_i \circ \alpha^{-1} = V' \circ U', \quad \beta \circ B_j \circ \beta^{-1} = U' \circ V'. \]
(19)
Furthermore, it is easy to see that formulas (18) provide a one-to-one correspondence between solutions of (17) and (19).

**Theorem 4.2.** Let $B$ a rational function of degree at least two. Then the graph $\Gamma_B$ is finite, unless $B$ is a flexible Lattès map.

**Proof.** By the main result of the paper [9], the class $[B]$ contains infinitely many conjugacy classes if and only if $B$ is a flexible Lattès map. Therefore, if $B$ is not such a map, the graph $\Gamma_B$ contains only finitely many vertices.

Let us show now that the number of edges connecting two vertices is finite. Recall that two decompositions
\[ B = V \circ U, \quad B = V' \circ U' \]
(20) of a rational function $B$ into compositions of rational functions are called equivalent if there exists a M"obius transformation $\mu$ such that
\[ V' = V \circ \mu^{-1}, \quad U' = \mu \circ U. \]
(21)
It is well known that equivalence classes of decompositions of $B$ are in one-to-one correspondence with imprimitivity systems of the monodromy group $\text{Mon}(B)$ of $B$. In particular, there exist at most finitely many such classes. Therefore, to prove the finiteness of the number of edges adjacent to the vertices corresponding to $B_i$ and $B_j$ it is enough to show that for any fixed solution $U, V$ of (17) there exist only finitely many solutions $U'$, $V'$ of (17) such that decompositions (20) are equivalent. Since equalities (21) combined with the equality
\[ U \circ V = U' \circ V' \]
imply the equality
\[ U \circ V = \mu \circ U \circ V \circ \mu^{-1}, \]
the last statement follows from the finiteness of the group $\text{Aut}(U \circ V)$. 

Since in this paper we consider only non-special rational functions $B$, the corresponding graphs $\Gamma_B$ are always finite by Theorem 4.2. Note that the results of [5] imply that the number of vertices of $\Gamma_B$ can be bounded by a number depending on $\deg B$ only (see [5, Remark 5.2]). Nevertheless, there exists no absolute bound for the number of vertices.
of \( \Gamma_B \), and it is easy to construct rational functions \( B \) of degree \( n \) for which the graph \( \Gamma_B \) contains \( \approx \log_2 n \) vertices (see [6, p. 1241]).

We always assume that the representative of the conjugacy class of the function \( B \) in \( \Gamma_B \) is the function \( B \) itself. Abusing notation, in the following we call the functions \( B_j \) simply ‘vertices’ of \( \Gamma_B \). Note that for each vertex \( B_j \) of \( \Gamma_B \) there exists at least one loop starting and ending at \( B \) that corresponds to the solution

\[
B = B \circ z = z \circ B
\]

of (17). More generally, the solutions

\[
B = (\mu^{-1} \circ B) \circ \mu = \mu \circ (\mu^{-1} \circ B), \quad \mu \in \text{Aut}(B),
\]

give rise to \( |\text{Aut}(B)| \) loops.

**Example 1.** Assume that \( B \) is an *indecomposable* rational function. By definition, this means that the equality \( B = V \circ U \) implies that at least one of the functions \( U \) and \( V \) has degree one. In this case, the equivalence class \([B]\) obviously consists of a unique conjugacy class. Thus, \( \Gamma_B \) has a unique vertex, and all edges of \( \Gamma_B \) are loops corresponding to solutions of

\[
B = U \circ V = V \circ U
\]

such that one of the functions \( U, V \) has degree one. Assuming without loss of generality that \( \text{deg } U = 1 \), we see that

\[
B \circ U = U \circ V \circ U = U \circ B,
\]

implying that \( U \in \text{Aut}(B) \). Therefore, \( \Gamma_B \) has the form shown in Figure 1, and the number of loops of \( \Gamma_B \) is equal to \( |\text{Aut}(B)| \).

**Example 2.** Assume now that a rational function \( B \) has, up to equivalency (21), a unique decomposition \( B = V \circ U \) into a composition of rational functions of degree at least two, and that the same is true for the function \( B_1 = U \circ V \). In this case, graph \( \Gamma_B \) may have two distinct forms. Namely, if \( B_1 \) and \( B \) are not conjugate, then \( \Gamma_B \) has the form shown in Figure 2, where all loops correspond to some automorphisms. Note that for such \( B \) and \( B_1 \) the groups \( \text{Aut}(B) \) and \( \text{Aut}(B_1) \) are isomorphic (see Lemma 6.3), implying that \( B \) and \( B_1 \) have the same number of attached loops.
On the other hand, if $B_1$ is conjugate to $B$, then without loss of generality we may assume that $B_1 = B$, so that

$$B = V \circ U = U \circ V. \quad (24)$$

In this case, the graph $\Gamma_B$ has one vertex and $|\text{Aut}(B)| + 1$ loops corresponding to (23) and (24). Note that since by the assumption the decompositions in (24) are equivalent, the equalities

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

hold for some Möbius transformation $\mu$, implying that

$$B = V \circ U = \mu \circ U \circ \mu^{-1}. \quad (25)$$

Thus, up to a composition with a Möbius transformation $\mu$, the function $B$ is the second iterate of some rational function $U$. Moreover, since

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

the transformation $\mu$ belongs to $\text{Aut}(U)$.

**Example 3.** Set

$$B = -\frac{2z^2}{z^4 + 1} = -\frac{2}{z^2 + 1/z^2}. \quad (26)$$

The function $B$ is an invariant for the finite automorphism group of $\mathbb{C}P^1$ generated by the transformations

$$z \rightarrow \frac{1}{z}, \quad z \rightarrow -z,$$

and its monodromy group $\text{Mon}(B)$ is the Klein four group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ having three proper imprimitivity systems. The corresponding decompositions of $B$ are

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

and

$$B = \frac{z^2 - 1}{z^2 + 1} \circ \frac{z^2 - 1}{z^2 + 1}. \quad (25)$$

Using, for example, the ‘Maple’ system, one can check that the function

$$B_1 = \frac{z^2 + 1}{z} \circ -\frac{2}{z^2 - 2} = -\frac{1}{2} \frac{z^4 - 4z^2 + 8}{z^2 - 2} \quad (26)$$

has three critical values in $\mathbb{C}P^1$, and the corresponding permutations in $\text{Mon}(B_1)$ can be identified with the permutations (12)(34), (1243), and (14) in $S_4$. On the other hand, the function

$$B_2 = \frac{z^2 - 1}{z} \circ -\frac{2}{z^2 + 2} = \frac{1}{2} \frac{z^2(z^2 + 4)}{z^2 + 2} \quad (27)$$

has four critical values, and the corresponding permutations in $\text{Mon}(B_2)$ can be identified with (12)(34), (23), (12)(34), and (14). Since $B_1$ and $B_2$ have a different number of critical values, they are not conjugate. Furthermore, it is easy to see that the both groups $\text{Mon}(B_1)$ and $\text{Mon}(B_2)$ have a unique proper imprimitivity system $\{1, 4\}, \{2, 3\}$,
corresponding to decompositions (26) and (27), implying, in particular, that $B$ is not conjugate to $B_1$ or $B_2$. Finally, one can check by a direct calculations, solving the system

$$\frac{az + b}{cz + d} \circ B = B \circ \frac{az + b}{cz + d}$$

in $a, b, c, d$, that the functions $B, B_1, B_2$ have no automorphisms. Summing up, we conclude that the graph $\Gamma_B$ has the form shown on Figure 3.

5. The epimorphism $\pi_1(\Gamma_B) \to G_B$

Considering the graph $\Gamma_B$ as a one-dimensional CW complex in $\mathbb{R}^3$, we can provide each edge of $\Gamma_B$, including loops, with two opposite orientations. With each oriented edge $e$ of $\Gamma_B$, we associate a rational function $\mathcal{F}(e)$ as follows. Assume first that $e$ corresponds to solution (17) with different $B_i$ and $B_j$. Then we set $\mathcal{F}(e) = U$, if the initial point of $e$ is $B_i$ and the final point is $B_j$, and $\mathcal{F}(e) = V$, if the orientation is opposite. For a loop, we simply set the value of $\mathcal{F}$ equal to $U$ for one of the two corresponding oriented edges, and equal to $V$ for the opposite oriented edge. For an oriented path

$$l = e_ne_{n-1} \ldots e_1,$$

set

$$\mathcal{F}(l) = \mathcal{F}(e_n) \circ \mathcal{F}(e_{n-1}) \circ \cdots \circ \mathcal{F}(e_1).$$

We emphasize that since we always compose functions from right to left, we follow this convention also for a concatenation of paths. Thus, a path obtained by a concatenation of the paths $l_1$ and $l_2$ is denoted by

$$l = l_2l_1,$$

and the above definition implies that

$$\mathcal{F}(l) = \mathcal{F}(l_2) \circ \mathcal{F}(l_1).$$

(28)

As usual, we denote the path $l$ traversed in the opposite direction by $l^{-1}$.

By construction, oriented paths from $B$ to $B_s$ correspond to sequences of elementary transformation (5). Furthermore, in the notation of Lemma 2.2, if

$$\mathcal{F}(l) = U_s \circ U_{s-1} \circ \cdots \circ U_1,$$

then

$$\mathcal{F}(l^{-1}) = V_1 \circ \cdots \circ V_{s-1} \circ V_s.$$
LEMMA 5.1. Let \( l \) be an oriented path in \( \Gamma_B \) from the vertex \( B \) to a vertex \( B_s \) consisting of \( k \) oriented edges. Then

\[
B_s \circ \mathcal{F}(l) = \mathcal{F}(l) \circ B,
\]

and

\[
\mathcal{F}(l^{-1}) \circ \mathcal{F}(l) = B^o_k, \quad \mathcal{F}(l) \circ \mathcal{F}(l^{-1}) = B'_s \circ k.
\]  \( □ \) (30)

If \( l \) is a closed path in \( \Gamma_B \) starting and ending at \( B \), then (29) implies that the function \( \mathcal{F}(l) \) commutes with \( B \), while equalities (30) reduce to the equalities

\[
\mathcal{F}(l^{-1}) \circ \mathcal{F}(l) = \mathcal{F}(l) \circ \mathcal{F}(l^{-1}) = B^o_k.
\]  (31)

Thus, we obtain a map \( \phi_B : l \rightarrow \mathcal{F}(l) \) from the set of closed paths starting and ending at \( B \) to the set \( C_B \).

THEOREM 5.2. The map \( \phi_B : l \rightarrow \mathcal{F}(l) \) descends to an epimorphism of groups \( \Phi_B : \pi_1(\Gamma_B, B) \rightarrow G_B \).

Proof. Let \( \Gamma \) be a graph. Recall that an oriented path \( l \) in \( \Gamma \) is called reduced if no two successive oriented edges in \( l \) are opposite orientations of the same edge. Paths of the form \( e^{-1}e \), where \( e \) is an oriented edge are called spurs. Paths \( l \) and \( l' \) are called equivalent if \( l' \) is obtained from \( l \) by a finite number of insertions and removals of spurs between successive oriented edges or at the endpoints. In these terms, the fundamental group \( \pi_1(\Gamma, V) \) of the graph \( \Gamma \) can be defined as the set of equivalence classes of paths that begin and end at some fixed vertex \( V \) of \( \Gamma \), equipped with the product of classes defined in an obvious way (see e.g. [14, §2.1.6]).

To prove that the map \( \phi_B \) descends to a map from \( \pi_1(\Gamma_B, B) \) to \( G_B \), we must show that whenever closed paths \( l \) and \( l' \) in \( \Gamma_B \) that start and end at \( B \) are equivalent, the rational functions \( \mathcal{F}(l) \) and \( \mathcal{F}(l') \) are in the same equivalence class of \( C_B \). Since any path is equivalent to a path with no spurs, for this purpose it is enough to show that if \( l' \) is obtained from \( l \) by an insertion of a spur, then \( \mathcal{F}(l) \sim \mathcal{F}(l') \). Assume that

\[
l' = l_2e^{-1}el_1,
\]

where \( l_1 \) is a path from \( B \) to \( B_s \), and \( l_2 \) is a path from \( B_s \) to \( B \) (one of the paths \( l_1 \) and \( l_2 \) can be empty in which case \( B_s = B \)). Then

\[
\mathcal{F}(l') = \mathcal{F}(l_2) \circ B_s \circ \mathcal{F}(l_1),
\]

by (28) and (31). It follows now from (29) that

\[
\mathcal{F}(l') = \mathcal{F}(l_2) \circ \mathcal{F}(l_1) \circ B = \mathcal{F}(l) \circ B,
\]

implying that \( \mathcal{F}(l) \sim \mathcal{F}(l') \). Thus, \( \phi_B \) descends to a map \( \Phi_B : \pi_1(\Gamma_B, B) \rightarrow G_B \), and (28) implies that \( \Phi_B \) is a homomorphism of groups.

Finally, it follows from Theorem 2.3 that \( \Phi_B \) is an epimorphism. Indeed, by Theorem 2.3, any \( X \in C_B \) can be obtained from a sequence of elementary transformations (5). Moreover, we can change if necessary each of rational functions \( B_i, \ 1 \leq i \leq s - 1 \), appearing in (5) to any desired representative of its conjugacy class, consecutively.
changing the function \( U_i \) to \( \alpha_i \circ U_i \), the function \( B_i \) to \( \alpha_i \circ B_i \circ \alpha_i^{-1} \), and the function \( U_{i+1} \) to \( \alpha_i^{-1} \circ U_{i+1} \) for a convenient Möbius transformation \( \alpha_i \). Therefore, for any \( X \in C_B \), there exists a closed path \( l \) starting and ending at \( B \) such that \( \mathcal{F}(l) = X \), implying that \( \Phi_B : \pi_1(\Gamma_B, B) \to G_B \) is an epimorphism.

**Theorem 5.3.** Let \( A \) and \( B \) be equivalent rational functions. Then \( G_B \cong G_A \).

*Proof.* Assuming that \( A \) and \( B \) are vertices of \( \Gamma_B \), take a path \( s \) from \( A \) to \( B \) in \( \Gamma_B \). Since the map \( \psi : l \to s^{-1}ls \), from the set of closed paths starting and ending at \( B \) to the set of closed paths starting and ending at \( A \), descends to an isomorphism of the fundamental groups

\[
\Psi : \pi_1(\Gamma_B, B) \to \pi_1(\Gamma_B, A),
\]

it follows from Theorem 5.2 that we only need to prove the equality

\[
\Psi(\ker \Phi_B) = \ker \Phi_A. \tag{32}
\]

Let \( l_0 \) be a path starting and ending at \( B \) such that \( \mathcal{F}(l_0) = B^k \), \( k \geq 1 \), and let \( k_0 = \psi(l_0) \). Then

\[
\mathcal{F}(k_0) = \mathcal{F}(s^{-1}) \circ \mathcal{F}(l_0) \circ \mathcal{F}(s) = \mathcal{F}(s^{-1}) \circ B^k \circ \mathcal{F}(s),
\]

implying by (29) and (30) that

\[
\mathcal{F}(k_0) = \mathcal{F}(s^{-1}) \circ \mathcal{F}(s) \circ A^{k} = A^{k} \circ A^{k} = A^{2k}
\]

for some \( k, l \geq 1 \). This implies that

\[
\Psi(\ker \Phi_B) \subseteq \ker \Phi_A.
\]

Similarly, considering the isomorphism inverse to \( \Psi \) we obtain that

\[
\Psi^{-1}(\ker \Phi_A) \subseteq \ker \Phi_B.
\]

This proves equality (32). \( \square \)

6. **Examples of groups \( G_B \)**

6.1. **Functions with \( G_B = \text{Aut}_G(B) \).** The simplest application of Theorem 5.2 is the following result.

**Theorem 6.1.** Let \( B \) be an indecomposable non-special rational function of degree at least two. Then \( G_B = \text{Aut}_G(B) \). Equivalently, \( X \in C_B \) if and only if \( X = \mu \circ B^l \) for some \( \mu \in \text{Aut}(B) \) and \( l \geq 1 \).

*Proof.* Since \( \Gamma_B \) has a unique vertex and \( |\text{Aut}(B)| \) loops corresponding to automorphisms of \( B \) (see Example 1), it follows easily from Theorem 5.2 that \( G_B \) is generated by \( \mu \), \( \mu \in \text{Aut}(B) \). Thus, \( G_B = \text{Aut}_G(B) \). The second statement follows from Lemma 3.4. \( \square \)

Note that Theorem 6.1 implies that for a ‘random’ rational function \( B \), the group \( G_B \) is trivial, since such a function is indecomposable and has no automorphisms.

Theorem 6.1 can be extended to a wide class of decomposable rational functions. Recall that a functional decomposition

\[
B = U_r \circ U_{r-1} \circ \cdots \circ U_1 \tag{33}
\]
of a rational function $B$ is called maximal if all $U_1, U_2, \ldots, U_r$ are indecomposable and of degree greater than one. The number $r$ is called the length of the maximal decomposition (33). Two decompositions (maximal or not) having an equal number of terms

$$F = F_r \circ F_{r-1} \circ \cdots \circ F_1 \quad \text{and} \quad F = G_r \circ G_{r-1} \circ \cdots \circ G_1$$

are called equivalent if either $r = 1$ and $F_1 = G_1$ or $r \geq 2$ and there exist Möbius transformations $\mu_i, 1 \leq i \leq r - 1$, such that

$$F_r = G_r \circ \mu_{r-1}, \quad F_i = \mu_i^{-1} \circ G_i \circ \mu_{i-1}, \quad 1 < i < r, \quad \text{and} \quad F_1 = \mu_1^{-1} \circ G_1.$$

Note that all maximal decompositions of a polynomial have the same length [11], but this is not true for arbitrary rational functions (see e.g. [4]).

We say that a rational function $B$ having a maximal decomposition (33) is generically decomposable if the following conditions are satisfied:

- each of the functions

$$B_i = (U_i \circ \cdots \circ U_2 \circ U_1) \circ (U_r \circ U_{r-1} \circ \cdots \circ U_{i+1}), \quad 0 \leq i \leq r - 1,$$

has a unique equivalence class of maximal decompositions;
- the functions $B_i, 0 \leq k \leq r - 1$, are pairwise not conjugate.

For a graph $\Gamma_B$, define $\Gamma_B^0$ as a graph obtained from $\Gamma_B$ by removing all loops that correspond to automorphisms. For example, for the graph $\Gamma_B$ from Example 3 the graph $\Gamma_B^0$ is shown in Figure 4. Recall that a complete graph is a graph in which every pair of distinct vertices is connected by a unique edge. The complete graph on $n$ vertices is denoted by $K_n$.

**Lemma 6.2.** Assume that a non-special rational function $B$ having a maximal decomposition of length $r$ is generically decomposable. Then $\Gamma_B^0$ is the complete graph $K_r$.

**Proof.** Let (33) be a maximal decomposition of $B$. Since all the functions $B_i, 0 \leq i \leq r - 1$, are equivalent and pairwise not conjugate, the graph $\Gamma_B$ contains at least $r$ vertices. Observe now that any decomposition $B = V \circ U$ of $B$ into a composition of two rational functions of degree at least two has the form

$$V = (U_r \circ U_{r-1} \circ \cdots \circ U_{i+1}) \circ \mu, \quad U = \mu^{-1} \circ (U_i \circ \cdots \circ U_2 \circ U_1), \quad 0 \leq i \leq r - 1,$$

where $\mu$ is a Möbius transformation. Indeed, concatenating arbitrary maximal decompositions of $U$ and $V$ we must obtain a maximal decomposition equivalent to

![Figure 4. The form of $\Gamma_B^0$ in Example 3.](image-url)
Since the same argument holds for any $1 \leq k \leq r - 1$, and there exists exactly one edge connecting $B_0$ and $B_1$, $1 \leq k \leq r - 1$. Since the same argument holds for any $B_i$, $0 \leq k \leq r - 1$, we conclude that $\Gamma_B^0$ is the complete graph $K_r$. 

**Proof.** In view of formula (28), it is enough to prove the lemma for the case where $l$ is an oriented edge. If $l$ is a loop, then by Lemma 6.2, it corresponds to a solution of (17) of the form

$$B_i = (\mu_0^{-1} \circ B_i) \circ \mu_0 = \mu_0 \circ (\mu_0^{-1} \circ B_i), \quad \mu_0 \in \text{Aut}(B_i).$$

Thus, either $\mathcal{F}(l) = \mu_0$ or $\mathcal{F}(l) = \mu_0^{-1} \circ B_i$, and it is easy to see that in these cases equality (35) holds for the automorphisms

$$\alpha(\mu) = \mu_0 \circ \mu \circ \mu_0^{-1}, \quad \alpha(\mu) = \mu_0^{-1} \circ \mu \circ \mu_0,$$

respectively.

Assume now that $l$ is an oriented edge from a vertex $B_{i_1} = V \circ U$ to a different vertex $B_{i_2} = U \circ V$. Let us observe that for any $\mu \in \text{Aut}(B_{i_1})$ the decompositions $B_{i_1} = V \circ U$ and

$$B_{i_1} = (\mu^{-1} \circ V) \circ (U \circ \mu)$$

are equivalent, since for arbitrary maximal decompositions of $U$ and $V$ the corresponding induced maximal decompositions of $B_{i_1}$ are equivalent. Therefore, for any $\mu \in \text{Aut}(B_{i_1})$, there exists a Möbius transformation $\alpha = \alpha(\mu)$ such that

$$\mu^{-1} \circ V = V \circ \alpha(\mu)^{-1}, \quad U \circ \mu = \alpha(\mu) \circ U.$$

Furthermore, since

$$B_{i_2} = U \circ V = U \circ \mu \circ \mu^{-1} \circ V = \alpha(\mu) \circ U \circ V \circ \alpha(\mu)^{-1},$$

the transformation $\alpha(\mu)$ belongs to $\mu \in \text{Aut}(B_{i_2})$, and it is easy to see that $\mu \rightarrow \alpha(\mu)$ is a group homomorphism from $\text{Aut}(B_{i_1})$ to $\text{Aut}(B_{i_2})$.

Finally, if

$$v \rightarrow \beta(v)$$

is a homomorphism from $\text{Aut}(B_{i_2})$ to $\text{Aut}(B_{i_1})$, defined by the conditions

$$v^{-1} \circ U = U \circ \beta(v)^{-1}, \quad V \circ v = \beta(v) \circ V,$$

and $\mu \in \text{Aut}(B_{i_1})$, then

$$V \circ U \circ \mu = V \circ \alpha(\mu) \circ U = \beta(\alpha(\mu)) \circ V \circ U.$$
Since
\[ V \circ U \circ \mu = \mu \circ V \circ U, \]
this implies that \( \beta \circ \alpha \) is the identical mapping of \( \text{Aut}(B_{i_1}) \), and hence \( \mu \to \alpha(\mu) \) is an isomorphism.

\[ \square \]

**Theorem 6.4.** Let \( B \) be a non-special generically decomposable rational function. Then \( G_B = \text{Aut}_G(B) \). Equivalently, \( X \in C_B \) if and only if \( X = \mu \circ B^l \) for some \( \mu \in \text{Aut}(B) \) and \( l \geq 1 \).

**Proof.** Let (33) be a maximal decomposition of \( B \). For convenience, define rational functions \( U_i \) for \( i \geq r \), setting \( U_i \). Let us recall that any decomposition \( B = V \circ U \), where \( U \) and \( V \) are functions of degree at least two, has the form (34), and a similar statement holds for all \( B_i, 0 \leq i \leq r - 1 \). Therefore, for the oriented edge \( e \) from a vertex \( B_{i_1} \) to a different vertex \( B_{i_2} \) the equality \( F(e) = U_{i_2} \circ \cdots \circ U_{i_1+2} \circ U_{i_1+1} \)
holds, implying inductively by (28) that for an arbitrary path \( l \) with no loops from \( B_{i_1} \) to \( B_{i_2} \) the equality \( F(l) = U_{i_2+rk} \circ \cdots \circ U_{i_1+2} \circ U_{i_1+1} = B_{i_2}^{ok} \circ U_{i_2} \circ \cdots \circ U_{i_1+2} \circ U_{i_1+1} \)
holds for some \( k \geq 1 \). In particular, if \( l \) is a closed path starting and ending at \( B \) and containing no loops, then \( F(l) = B^{ok}, k \geq 1 \), implying that the image of \( l \) under the homomorphism \( \Phi_B \) from Theorem 5.2 is the unit element. Further, if \( l \) contains a loop, then either \( F(l) = U_{kr} \circ \cdots \circ U_{i+1} \circ v \circ U_i \circ \cdots \circ U_1 \),
or \( F(l) = U_{kr} \circ \cdots \circ U_{i+1} \circ (v^{-1} \circ B_i) \circ U_i \circ \cdots \circ U_1 \)
for some \( k \geq 1, 0 \leq i \leq r - 1 \), and \( v \in \text{Aut}(B_i) \). Therefore, by Lemmas 6.3 and 5.1, either \( F(l) = \mu \circ B^{ok} \),
or \( F(l) = \mu \circ B^{ok(k+1)} \)
for some \( \mu \in \text{Aut}(B) \). Finally, if \( l \) contains several loops, then repeatedly using Lemmas 6.3 and 5.1, we conclude that \( F(l) = \mu \circ B^{oxs} \)
for some \( \mu \in \text{Aut}(B) \) and \( s \geq 1 \). Thus, \( G_B = \text{Aut}_G(B) \). \( \square \)

**Corollary 6.5.** Let \( B \) be a non-special rational function of degree at least two such that \( G_B \) is strictly larger than \( \text{Aut}_G(B) \). Then there exists \( A \sim B \) such that either \( A \) can be represented as a composition of two commuting rational functions of degree at least two, or \( A \) has more than one class of maximal decompositions.
Proof. By Theorem 6.4, it is enough to show that if any \( A \sim B \) has a unique equivalence class of maximal decompositions and cannot be represented as a composition of two commuting rational functions of degree at least two, then for the function \( B \) the both conditions defining generically decomposable rational functions are satisfied. For the first condition, this is obvious. For the second condition, this is also true. Indeed, if say \( B_0 = B \) is conjugate to \( B_i \) and \( \mu \) is a Möbius transformation such that

\[
(U_r \circ \cdots \circ U_{i+1}) \circ \mu \circ (U_i \circ \cdots \circ U_1) = (U_r \circ \cdots \circ U_{i+1}) \circ \mu^{-1},
\]

then for the functions

\[
N = \mu \circ (U_i \circ \cdots \circ U_1), \quad M = (U_r \circ \cdots \circ U_{i+1}) \circ \mu^{-1}
\]

the equality

\[
B = M \circ N = N \circ M \quad (36)
\]

holds. \( \square \)

Note that whenever \( B \) is a composition of two commuting rational functions of degree at least two, the group \( G_B \) is strictly larger than \( \text{Aut}_G(B) \). Indeed, equality (36) implies easily that the functions \( N \) and \( M \) belong to \( C_B \). Moreover, their images in \( G_B \) are not trivial and do not belong to \( \text{Aut}_G(B) \), since

\[
1 < \deg M < \deg B, \quad 1 < \deg N < \deg B.
\]

In particular, if \( B = T^s \), where \( s > 1 \), the group \( G_B \) contains a cyclic group of order \( s \) whose intersection with \( \text{Aut}_G(B) \) is trivial.

Finally, note that the group \( G_B \) can be strictly larger than \( \text{Aut}_G(B) \) even if \( B \) is not a composition of commuting functions, and that the relation \( A \sim B \) does not imply, in general, the equality \( \text{Aut}_G(A) \cong \text{Aut}_G(B) \) (see §6.3).

6.2. The group \( G_B \) for polynomial \( B \). Before stating the theorem describing groups \( G_B \) for polynomial \( B \) let us recall several results.

First, for a non-special polynomial \( B \) of degree at least two, the set \( C_B \) consists of polynomials. Indeed, (1) yields that

\[
B^{-1}(X^{-1}(\infty)) = X^{-1}(\infty), \quad (37)
\]

implying that \( X^{-1}(\infty) \) contains at most two points. Furthermore, considering instead of \( B \) and \( X \) the functions

\[
X \to \mu \circ X \circ \mu^{-1}, \quad B \to \mu \circ B \circ \mu^{-1}
\]

for a convenient Möbius transformation \( \mu \), without loss of generality one can assume that either \( X^{-1}(\infty) = \{\infty\} \) or \( X^{-1}(\infty) = \{\infty, 0\} \). In the first case, \( X \) is a polynomial. On the other hand, in the second case, (37) implies that \( B \) is conjugate to \( z^n \), contradicting the assumption that \( B \) is not special.

Second, the symmetry group \( \text{Aut}(B) \) of a non-special polynomial \( B \) of degree at least two is cyclic. Indeed, unless \( B \) is conjugate to \( z^n \), for any \( \mu \in \text{Aut}(B) \) necessarily \( \mu^{-1}(\infty) = \{\infty\} \), implying that \( \mu \) is a polynomial. By a polynomial conjugation, we can
always assume that the coefficient of \( z^{\deg B - 1} \) is zero, and it is clear that \( \mu = az + b \) may commute with such \( B \) only if \( b = 0 \). Furthermore, it is easy to see that \( \text{Aut}(B) \) is a cyclic rotation group of order \( n \), where \( n \) is the maximal number such that

\[
B = zR(z^n)
\]

for some polynomial \( R \).

Third, a polynomial \( B \) is special if and only if \( B \) is conjugate to \( z^n \) or \( \pm T_n \), since it is well known that a polynomial cannot be a Latt`es map.

In addition, we need the following result (see [7, Theorem 1.3]).

**Theorem 6.6.** Let \( A \) and \( B \) be fixed non-special polynomials of degree at least two, and let \( \mathcal{E}(A, B) \) be the set of all polynomials of degree at least two \( X \) such that \( A \circ X = X \circ B \). Then, either \( \mathcal{E}(A, B) \) is empty, or there exists \( X_0 \in \mathcal{E}(A, B) \) such that a polynomial \( X \) belongs to \( \mathcal{E}(A, B) \) if and only if \( X = \hat{A} \circ X_0 \) for some polynomial \( \hat{A} \) commuting with \( A \).

Recall that a group \( G \) is called metacyclic if it has a normal cyclic subgroup \( H \) such that \( G/H \) is a cyclic group.

**Theorem 6.7.** Let \( B \) be a polynomial of degree at least two not conjugate to \( z^n \) or \( \pm T_n \), \( n \geq 2 \). Then the group \( G_B \) is metacyclic.

**Proof.** Applying Theorem 6.6 for \( A = B \) and arguing as in Lemma 3.4, we see that any rational function \( X \) that belongs to \( C_B = \mathcal{E}(B, B) \) has the form \( X = \mu \circ X_0^{\ell_0} \), where \( \mu \in \text{Aut}(B) \) and \( l \geq 1 \). In particular, \( B = \mu \circ X_0^{\ell_0} \) for some \( l_0 \geq 1 \) and \( \mu \in \text{Aut}(B) \). Moreover, the degree of any element of \( C_B \) is a power of \( d_0^l \) coincides with the set \( S_{1,l} = \{ \mu \circ X_0^l \mid \mu \in \text{Aut}(B) \} \).

Let us observe now that if

\[
X_0^{\ell_0} \circ \mu_1 = X_0^{\ell_0} \circ \mu_2,
\]

where \( \mu_1, \mu_2 \in \text{Aut}(B) \), then \( \mu_1 = \mu_2 \). Indeed, (38) implies that

\[
X_0^{\ell_0} \circ (\mu_1 \circ \mu_2^{-1}) = X_0^{\ell_0}.
\]

Therefore, since \( B^{\ell_0} = v \circ X_0^{\circ(l_0)} \) for some \( v \in \text{Aut}(B) \),

\[
B^{\ell_0} \circ (\mu_1 \circ \mu_2^{-1}) = B^{\ell_0},
\]

implying that \( \mu_1 = \mu_2 \). Thus, for \( l \geq 0 \) the set \( S_{2,l} = \{ X_0^l \circ \mu \mid \mu \in \text{Aut}(B) \} \) has the same cardinality as the set \( S_{1,l} \). Since \( S_{2,l} \) is contained in \( C_B \), this implies that \( S_{1,l} = S_{2,l} \).

The above analysis shows that the right cosets of \( \text{Aut}_G(B) \) in \( G \) have the form

\[
X_0^l \text{Aut}_G(B), \quad 0 \leq l < l_0,
\]

the left cosets have the form

\[
\text{Aut}_G(B)X_0^l, \quad 0 \leq l < l_0,
\]

and any right coset of \( \text{Aut}_G(B) \) in \( G \) is a left coset. Thus, \( \text{Aut}_G(B) \) is a normal subgroup in \( G_B \), and the group \( G_B/\text{Aut}_G(B) \) is a cyclic group of order \( l_0 \) generated by \( X_0 \). Since \( \text{Aut}(B) \) is also a cyclic group, we conclude that the group \( G_B \) is metacyclic. □
Note that Theorem 6.7 can be deduced from the Ritt theorem [12, 13] saying that any commuting non-special polynomials $X$ and $B$ can be represented in the form (3). Nevertheless, the Ritt theorem does not imply Theorem 6.7 immediately, since $R$ in (3) \textit{a priori} depends on $X$, and the further analysis is needed.

6.3. \textit{The group $G_B$ for the Ritt example.} Let $B$ be a rational function of degree at least two. Denote by $\hat{\text{Aut}}(B)$ the group consisting of M"{o}bius transformations $\mu$ such that

$$B \circ \mu = v \circ B$$

for some M"{o}bius transformations $v$. Like the group $\text{Aut}(B)$, the group $\hat{\text{Aut}}(B)$ is a finite rotation group of the sphere (see [5, \S 4]). More generally, denote by $\hat{C}_B$ the set of rational functions $X$ such that $B \circ X = Y \circ B$ for some rational function $Y$. Clearly, $\text{Aut}(B)$ is a subgroup of $\hat{\text{Aut}}(B)$, and $C_B \subseteq \hat{C}_B$.

Let

$$V = \frac{z^2 + 2}{z + 1}, \quad U = \frac{z^2 - 4}{z - 1}, \quad \mu = \epsilon z,$$

where $\epsilon^3 = 1$. In [13], Ritt showed that the rational functions

$$B = V \circ U, \quad X = V \circ \mu \circ U$$

commute but no one of them is a rational function of the other. In particular, this implies that there is no $R$ such that

$$B = \mu_1 \circ R^{l_1}, \quad X = \mu_2 \circ R^{l_2}$$

for some M"{o}bius transformations $\mu_1, \mu_2$, and $l_1, l_2 \geq 1$. More generally, for any function $C$ such that $C(\epsilon z) = \epsilon C(z)$, the functions

$$B' = V \circ C \circ U, \quad X' = V \circ \mu \circ C \circ U$$

commute, but no one of them is a rational function of the other.

The Ritt statement follows from the following more general observation.

\textbf{Lemma 6.8.} Let $W \in C_{U \circ V}$, but $W \not\in \hat{C}_V$. Then the functions $V \circ U$ and $V \circ W \circ U$ commute but the latter is not a rational function of the former. Furthermore, the same conclusion holds for the functions $V \circ C \circ U$ and $V \circ W \circ C \circ U$, where $C$ is any function commuting with $W$.

\textit{Proof.} Indeed, we have

$$(V \circ C \circ U) \circ (V \circ W \circ C \circ U) = V \circ C \circ (U \circ V \circ W) \circ C \circ U$$

$$= V \circ C \circ (W \circ U \circ V) \circ C \circ U = (V \circ C \circ W \circ U) \circ (V \circ C \circ U)$$

$$= (V \circ W \circ C \circ U) \circ (V \circ C \circ U).$$

On the other hand, if

$$V \circ W \circ C \circ U = R \circ V \circ C \circ U$$

for some rational function $R$, then

$$V \circ W = R \circ V,$$

contradicting the assumption that $W \not\in \hat{C}_V$. \hfill \Box
The Ritt statement is obtained from Lemma 6.8 for \( W = \mu \). Indeed,

\[
U \circ V = \frac{z(z^3 - 8)}{(z^3 + 1)},
\]

implying that \( \mu \in \text{Aut}(U \circ V) \). On the other hand, the assumption that

\[
V \circ \mu = \nu \circ V \tag{39}
\]

for some Möbius transformation \( \nu \) leads to a contradiction. Namely, (39) implies that \( \nu(\infty) = \infty \). Therefore, \( \nu = az + b, a, b \in \mathbb{C} \), and, hence, if (39) holds, then the functions \( V \) and

\[
V \circ \mu = \frac{\varepsilon^2 z^2 + 2}{\varepsilon z + 1}
\]

have the same set of poles. However, this is not true.

Let us calculate the group \( G_B \). Again using the assistance of a computer one can check that the function

\[
B = V \circ U = \frac{z^4 - 6z^2 - 4z + 18}{(z^2 + z - 5)(z - 1)}
\]

has four critical values and the corresponding permutations in \( \text{Mon}(B) \) can be identified with the permutations (13), (12)(34), (13), and (12)(34) in \( S_4 \), while the function

\[
B_1 = U \circ V = \frac{z(z^3 - 8)}{(z^3 + 1)}
\]

has three critical values and the corresponding permutations in \( \text{Mon}(B_1) \) can be identified with (12)(34), (13)(24), and (14)(23). In particular, \( B_1 \) and \( B \) are not conjugate since they have a different number of critical values. Moreover, one can check that the group \( \text{Aut}(B) \) is trivial while \( \text{Aut}(B_1) \) is a cyclic group of order three generated by \( \mu \).

It is easy to see that \( \text{Mon}(B) \) has a unique imprimitivity system \( \{1, 3\}, \{2, 4\} \), corresponding to the decomposition \( B = V \circ U \) while \( \text{Mon}(B_1) \) has three imprimitivity systems

\[
\{1, 3\}, \{2, 4\}, \quad \{1, 2\}, \{3, 4\}, \quad \{1, 4\}, \{2, 3\},
\]

corresponding to the decompositions

\[
B_1 = U \circ V, \quad B_1 = (\mu^{-1} \circ U) \circ (V \circ \mu), \quad B_1 = (\mu^{-2} \circ U) \circ (V \circ \mu^2).
\]

Summing up, we see that the graph \( \Gamma_B \) has the form shown in Figure 5, where the edges connecting \( B \) and \( B_1 \) correspond to the solutions

\[
B = (V \circ \mu^{i-1}) \circ (\mu^{-(i-1)} \circ U), \quad B_1 = (\mu^{-(i-1)} \circ U) \circ (V \circ \mu^{i-1}), \quad 1 \leq i \leq 3,
\]

of system (17), the loops attached to \( B_1 \) correspond to the solutions

\[
B_1 = (\mu^{-i-1} \circ B_1) \circ \mu^{-i-1} = \mu^{i-1} \circ (\mu^{-i-1} \circ B_1), \quad 1 \leq i \leq 3,
\]

and the loop attached to \( B \) corresponds to the solution (22).

The fundamental group of \( \Gamma_B \) can be easily calculated by the well-known method using the spanning tree (see e.g. [14, §4.1.2]). Namely, choosing a fixed orientation on each of edges of \( \Gamma_B \) as shown in Figure 6, and considering the edge \( l_1 \) together with vertices \( B \) and
implies that the group $G$ we obtain has at least three elements. On the other hand, we have

and it follows from Lemma 3.1 that

we obtain

implying that the images of the functions

in the group $G_B$ generate $G_B$. Since

and

it follows from Lemma 3.1 that $g_1, g_2, g_3$ represent different classes in $C_B/ \sim_B$, so that $G_B$ has at least three elements. On the other hand, we have

and

Therefore, $G_B = \mathbb{Z}/3\mathbb{Z}$.

In turn, the set $C_B$ can be described as follows: $X \in C_B$ if and only if

or

Indeed, by Lemma 3.1, it is enough to check that the functions (40) are not rational functions in $B$. Assume say that $g_1 = R \circ B$. Then it follows from (41) that $R$ is a Möbius transformation. Moreover, $R \in \text{Aut}(B)$ by Lemma 2.1. However, since $\text{Aut}(B)$ is trivial and $g_1 \neq B$, this is impossible.

Note that since $G_B \cong G_{B_1}$ by Theorem 5.3 and $\text{Aut}_G(B_1) = \mathbb{Z}/3\mathbb{Z}$, we have

Note also that since $G_B \cong G_{B_1}$, the non-triviality of $\text{Aut}(B_1)$ already implies the non-triviality of $G_B$. Moreover, since $B$ has no automorphisms, we can conclude that the set $C_B$ contains functions of degree greater than one that are not iterates of $B$. 

\begin{figure}[h]
\centering
\includegraphics[width=0.5\textwidth]{\figDir/figure5.pdf}
\caption{The form of $\Gamma_B$ in the Ritt example.}
\end{figure}
6.4. The group $G_B$ for $B = -2z^2/(z^4 + 1)$. Since equality (25) implies that the function

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

commutes with $B$, the group $G_B$ clearly contains a cyclic group of order two generated by $W$. Moreover, it is easy to see that in fact $G_B = \mathbb{Z}/2\mathbb{Z}$. Indeed, providing edges of the graph $\Gamma_B$ with orientations shown in Figure 7, we see that $\pi_1(\Gamma_B, B)$ is a free group of rank four with generators

$$c, \quad t, \quad l_i^{-1}e_i l_i, \quad i = 1, 2,$$

and assuming that

$$\mathcal{F}(c) = \mathcal{F}(e_1) = \mathcal{F}(e_2) = z, \quad \mathcal{F}(t) = W,$$

we see that $G_B$ is generated by the $W$. Similarly, one can conclude that $G_{B_1}$ is generated by $X$, where

$$X = \mathcal{F}(l_1 t l_1^{-1}) = \frac{z^2 + 1}{z} \circ \frac{z^2 - 1}{z^2 + 1} \circ -\frac{2}{z^2 - 2}.$$

The above functions $B_1$ and $X$ provide an example of commuting rational functions similar to that constructed by Ritt. Namely, set

$$V = \frac{z^2 + 1}{z}, \quad U = -\frac{2}{z^2 - 2}.$$

Then $W$ commutes with $U \circ V = W^{\circ 2}$, but $W \notin \hat{C}_V$. Indeed, assume the inverse, and let $S$ be the rational function defined by any of the sides of the equality

$$\frac{z^2 + 1}{z} \circ \frac{z^2 - 1}{z^2 + 1} = R \circ \frac{z^2 + 1}{z}, \quad \text{(42)}$$

where $R \in \mathbb{C}(z)$. Then substituting $z$ by $1/z$ in the right-hand side of (42), we obtain that $S \circ 1/z = S$. However, substituting $z$ by $1/z$ in the left-hand side, we obtain

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

The contradiction obtained shows that $W \notin \hat{C}_V$. Therefore, by Lemma 6.8, the rational function

$$X = V \circ W \circ U$$

commutes with $B_1 = V \circ U$, but is not a rational function in $B_1$. Note that in distinction with the Ritt example, the non-triviality of $G_{B_1}$ is explained by the existence in the class $[B_1]$ of a function that is an iterate.
Acknowledgements. The author is grateful to the Max-Planck-Institut für Mathematik for the hospitality and support. This research was supported by the ISF (grant number 1432/18).

REFERENCES


