F. Pakovich (2017) "Recomposing Rational Functions,"
International Mathematics Research Notices, Vol. 2019, No. 7, pp. 1921–1935
Advance Access Publication August 13, 2017
doi: 10.1093/imrn/rnx172

Recomposing Rational Functions

Fedor Pakovich*

Department of Mathematics, Ben Gurion University of the Negev, P.O.B. 653, Beer Sheva, 8410501, Israel

**Correspondence to be sent to: e-mail: pakovich@math.bgu.ac.il*

Let A be a rational function. For any decomposition of A into a composition of rational functions $A = U \circ V$ the rational function $\widetilde{A} = V \circ U$ is called an elementary transformation of A, and rational functions A and B are called equivalent if there exists a chain of elementary transformations between A and B. This equivalence relation naturally appears in the complex dynamics as a part of the problem of describing of semiconjugate rational functions. In this paper we show that for a rational function A its equivalence class $[A]$ contains infinitely many conjugacy classes if and only if A is a flexible Lattès map. For flexible Lattès maps $\mathcal{L} = \mathcal{L}_j$ induced by the multiplication by 2 on elliptic curves with given j-invariant we provide a very precise description of $[\mathcal{L}]$. Namely, we show that any rational function equivalent to $\mathcal{L}_j$ necessarily has the form $\mathcal{L}_{j'}$ for some $j' \in \mathbb{C}$, and that the set of $j' \in \mathbb{C}$ such that $\mathcal{L}_{j'} \sim \mathcal{L}_j$ coincides with the orbit of j under the correspondence associated with the classical modular equation $\Phi_2(x, y) = 0$.

1 Introduction

Let B be a rational function of degree at least two. The function B is called semiconjugate to a rational function A if the equality

$$A \circ X = X \circ B \tag{1}$$

Received October 25, 2016; Revised April 24, 2017; Accepted June 29, 2017
Communicated by Prof. Umberto Zannier

holds for some rational function X. In case if X is invertible, A and B are called conjugate. In terms of dynamical systems, condition (1) means that the dynamical system $A^{\circ k}$, $k \geq 1$, on $\mathbb{CP}^1$ is a factor of the dynamical system $B^{\circ k}$, $k \geq 1$. The semiconjugacy is not a symmetric relation. However, if B is semiconjugate to A, and C is semiconjugate to B, then C is semiconjugate to A, since equalities (1) and $B \circ W = W \circ C$ imply the equality

$$A \circ (X \circ W) = (X \circ W) \circ C.$$

In the recent paper [10] equation (1) was investigated at length. Roughly speaking, the main result of [10] states that (1) holds in two cases. In the first case, the corresponding functions A and B are either Lattès maps, or functions which can be considered as analogues of Lattès maps related to automorphism groups of $\mathbb{CP}^1$ instead of automorphism groups of $\mathbb{C}$. In the second case, the functions A and B do not possess any special properties, however they are equivalent with respect to an equivalence relation $\sim$ on the set of rational functions defined as follows. For any decomposition $A = U \circ V$, where U and V are rational functions, the rational function $\widetilde{A} = V \circ U$ is called an *elementary transformation* of A, and rational functions A and B are called *equivalent* if there exists a chain of elementary transformations between A and B. For a rational function A we will denote its equivalence class by $[A]$.

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

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

implying inductively that whenever $A \sim B$ there exists X such that (1) holds, and there exists Y such that

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

Therefore, if $A \sim B$, each of the dynamical systems $A^{\circ k}$, $k \geq 1$, and $B^{\circ k}$, $k \geq 1$, is a factor of the other one, meaning that these systems have "similar" dynamics. Furthermore, since for any invertible rational function W the equality

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

holds, each equivalence class $[A]$ is a union of conjugacy classes. Thus, the relation $\sim$ can be considered as a weaker form of the classical conjugacy relation.

The main result of this article is the following statement.

Theorem 1.1. Let F be a rational function. Then its equivalence class $[F]$ contains infinitely many conjugacy classes if and only if F is a flexible Lattès map. □

Simplest examples of flexible Lattès maps are rational functions $\mathcal{L}$ induced by the multiplication by 2 on elliptic curves. Such a function can be defined by the equality

$$\wp(2z) = \mathcal{L} \circ \wp(z), \tag{2}$$

where $\wp(z)$ is the Weierstrass function associated with some lattice M of rank two in $\mathbb{C}$. Two such functions corresponding to lattices M and M' are conjugate if and only if the elliptic curves $\mathbb{C}/M$ and $\mathbb{C}/M'$ are isomorphic. So, abusing the notation, we will denote by $\mathcal{L}_j$ any Lattès map induced by the multiplication by 2 on an elliptic curve with given j-invariant.

In order to describe conjugacy classes in $[\mathcal{L}_j]$ it is convenient to use the notion of correspondence $\mathcal{F}$ associated with an affine algebraic curve $F(x, y) = 0$. By definition, for $x_0 \in \mathbb{C}$ an image of x_0 under $\mathcal{F}$ is any point $y_0 \in \mathbb{C}$ such that $F(x_0, y_0) = 0$. More generally, $y_0 \in \mathbb{C}$ is an image of $x_0 \in \mathbb{C}$ under the kth iteration of $\mathcal{F}$ if there exists a sequence $x_0, x_1, \dots, x_k = y_0$ such that (x_{i-1}, x_i), $i = 1, \dots k$, is a point on $F(x, y) = 0$. Considering the totalities of all images and preimages of a point x_0 we can define its forward, backwards, and full orbit under $\mathcal{F}$. If $F(x, y)$ is symmetric, that is $F(x, y) = F(y, x)$, all these orbits coincide, so we can use simply the term orbit.

In the above notation, our main result about $[\mathcal{L}_j]$ is following.

Theorem 1.2. Any rational function equivalent to $\mathcal{L}_j$, $j \in \mathbb{C}$, has the form $\mathcal{L}_{j'}$, $j' \in \mathbb{C}$. Furthermore, the set of $j' \in \mathbb{C}$ such that $\mathcal{L}_{j'} \sim \mathcal{L}$ coincides with the orbit of j under the correspondence associated with the classical modular equation $\Phi_2(x, y) = 0$. □

Notice that although the expression for the curve $\Phi_2(x, y) = 0$ is quite bulky it has a very simple parametrization by rational functions which goes back to Klein [2], implying that $\mathcal{L}_{j'} \sim \mathcal{L}_j$ if and only if j and j' are in the same orbit of the multivalued function

$$\mathcal{F} = \beta \circ \frac{1}{z} \circ \beta^{-1}, \tag{3}$$

where β is a rational function of degree three,

$$\beta(z) = 64\,\frac{(z+4)^3}{z^2}.$$

The article has the following structure. In the second section we show that the condition $A \sim B$ implies that A and B are isospectral, and deduce the “only if” part of Theorem 1.1 from the fundamental result of McMullen [4] about isospectral rational functions. In the third section we relate functional decompositions of flexible Lattès maps with isogenies between elliptic curves, and prove the “if” part of Theorem 1.1. Finally, in the fourth section we describe explicitly all functional decompositions of $\mathcal{L}_j$ and prove Theorem 1.2.

2 Equivalence and Isospectrality

Let F be a rational function. Recall that two decompositions of F into compositions of rational functions $F = U \circ V$ and $F = U' \circ V'$ are called *equivalent* if there exists a Möbius transformation μ such that

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

Clearly, elementary transformations corresponding to equivalent decompositions are conjugate. Since equivalence classes of decompositions of F are in a one-to-one correspondence with imprimitivity systems of the monodromy group G_F of F, this implies in particular that the number of conjugacy classes of rational functions obtained from F by elementary transformations is finite, and that the number of conjugacy classes in $[F]$ is at most countable.

Recall that a rational function A is called *a flexible Lattès map* if there exist an elliptic curve $\mathcal{C}$ and morphisms $\varphi : \mathcal{C} \to \mathcal{C}$ and $\pi : \mathcal{C} \to \mathbb{CP}^1$ such that the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\varphi} & \mathcal{C} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{CP}^1 & \xrightarrow{A} & \mathbb{CP}^1 \end{array}, \tag{4}$$

commutes, π has degree two and satisfies $\pi(z) = \pi(-z)$, and $\varphi = nz + \beta$, where $n \in \mathbb{Z}$ and $\beta \in \mathcal{C}$ (see [14, Section 6.5] and [6]). In fact, β necessarily satisfies the condition $2\beta = 0$ on $\mathcal{C}$. Moreover, changing $\pi(z)$ to $\pi'(z) = \pi(z + \beta)$, we see that the condition $\pi'(z) = \pi'(-z)$ still holds, while (4) holds for $\varphi' = nz + \beta'$, where $\beta' = n\beta$. Thus, if n is even, we may assume that $\beta = 0$. The complex structure of $\mathcal{C}$ is completely defined by the conjugacy class of A, that is, if $A', \mathcal{C}', \pi', \varphi'$ is another collection as above and A is conjugate to A', then $\mathcal{C}$ is isomorphic to $\mathcal{C}'$ (see e.g., [14, Theorem 6.46]). Abusing the notation, we will denote by A_j any Lattès map satisfying (4) for $\mathcal{C}$ with given j-invariant.

Assuming that $\mathcal{C}$ is written in the Weierstrass form

$$\mathcal{C}: \; y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{C}, \tag{5}$$

a prototypical example of a Lattès map is obtained for $\varphi = 2z$ and $\pi(x, y) = x$. In this case,

$$A = \frac{z^4 - 2az^2 - 8bz + a^2}{4z^3 + 4az + 4b}. \tag{6}$$

Notice that if M is a lattice of rank two in $\mathbb{C}$ such that $\mathcal{C} = \mathbb{C}/M$ and $\wp(z)$ is the corresponding Weierstrass function, then the function A is defined by the condition $\wp(2z) = A \circ \wp(z)$. For $\mathcal{C}$ given by (5), $A = A_j$, where

$$j = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Let F be a rational function of degree d. By definition, the *multiplier spectrum* of F is a function which assigns to each $s \geq 1$ the unordered list of multipliers at all $d^s + 1$ fixed points of $F^{\circ s}$ taken with appropriate multiplicity. Two rational functions are called *isospectral* if they have the same multiplier spectrum. For example, all the functions from family (6) have the same multiplier spectrum (see e.g., [14, Example 6.49]). Nevertheless, by the following result of McMullen such a situation is exceptional (see [4, 6, 14]).

Theorem 2.1 (McMullen). The conjugacy class of any rational function F which is not a flexible Lattès map is defined up to finitely many choices by its multiplier spectrum. □

The equivalence $\sim$ and the isospectrality are closely related as the following lemma shows.

Lemma 2.1. Let U and V be rational functions. Then the rational functions $U \circ V$ and $V \circ U$ are isospectral. □

Proof. Since the equality

$$(U \circ V)^{\circ l}(z_0) = z_0$$

implies the equality

$$(V \circ U)^{\circ l}(z_1) = z_1,$$

where $z_1 = V(z_0)$, the function V maps periodic points of $U \circ V$ to periodic points of $V \circ U$. Furthermore, the period of z_1 divides the period of z_0. Similarly, U maps periodic points of $V \circ U$ to periodic points of $U \circ V$. Since the composition $U \circ V$ maps bijectively periodic points of $U \circ V$ of period l to themselves, this implies that V maps bijectively periodic points of $U \circ V$ of period l to periodic points of $V \circ U$ of period l.

Further, since by the chain rule

$$((U \circ V)^{\circ l})'(z_0) = ((U \circ V)^{\circ l-1} \circ U)'(z_1) \circ V'(z_0)$$

and

$$((V \circ U)^{\circ l})'(z_1) = V'((U \circ V)^{\circ l-1} \circ U)(z_1)) \circ ((U \circ V)^{\circ l-1} \circ U)'(z_1),$$

it follows from

$$((U \circ V)^{\circ l-1} \circ U)(z_1) = z_0$$

that

$$((U \circ V)^{\circ l})'(z_0) = ((V \circ U)^{\circ l})'(z_1).$$

Finally, observe that the multiplicity of a fixed point z_0 of $(U \circ V)^{\circ l}$ equals the multiplicity of the fixed point $z_1 = V(z_0)$ of $(V \circ U)^{\circ l}$. Indeed, since the multiplicity of a fixed point is an analytic invariant (see [1, Proposition 7]), this is true whenever $V'(z_0) \neq 0$. On the other hand, if $V'(z_0) = 0$, then $((U \circ V)^{\circ l})'(z_0) = 0$ and $((V \circ U)^{\circ l})'(z_1) = 0$, implying that both multiplicities under consideration are equal to one. ■

Corollary 2.1. Let A and B be rational functions such that $A \sim B$. Then A and B are isospectral. □

Proof. By definition, $A \sim B$ if B is obtained from A by a chain of elementary transformations. On the other hand, any such transformation leads to an isospectral function by Lemma 2.1. ■

It is clear that the McMullen theorem combined with Corollary 2.1 proves the "only if" part of Theorem 1.1. Notice however that the number of conjugacy classes in an equivalence class $[F]$ can be arbitrary large (see [10]). The proof of the "if" part of Theorem 1.1 is given in the next section.

Notice that isospectral A and B are not necessary equivalent. Say, all functions (6) cannot be equivalent since any equivalence class contains at most countably many conjugacy classes. Nevertheless, to our best knowledge all known examples of isospectral rational functions are obtained either from flexible Lattès maps, or from rigid Lattès maps (see [4, 6, 14]), or else from elementary transformations. Thus, it is still possible that if A and B are not Lattès maps, then the fact that A and B are isospectral implies that $A \sim B$. A comprehensive description of relations between the isospectrality and the equivalence $\sim$ seems to be a very interesting problem.

Notice also that if A is a *polynomial*, then the finiteness of $[A]$ can be established without using the McMullen theorem; see Corollary 5.8 in [11], and also the article [5] using the notion of "skew twist equivalence" which essentially coincides with the equivalence $\sim$ in the setting considered here. The approach of the article [5] is based on the theory of decomposition of polynomials developed by Ritt [12], while the method of [11] relies on the results of [9] about polynomials sharing preimages of compact sets. However, methods of both these articles are restricted to the polynomial case only.

3 Proof of Theorem 1.1

Consider first flexible Lattès maps $A = A_j$ defined by the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{nz} & \mathcal{C} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{CP}^1 & \xrightarrow{A} & \mathbb{CP}^1 \end{array} \tag{7}$$

where $n \in \mathbb{Z}$. In order to prove that $[A_j]$ contains infinitely many conjugacy classes we will use the relation between functional decompositions of A_j and isogenies between elliptic curves. We start from recalling some basic definitions and results concerning isogenies and the modular equation. Abusing the notation, below we will use the symbol j in two possible meanings: for a value of the elliptic modular function $j(\tau)$ of weight zero for $SL(2,\mathbb{Z})$ on the upper half-plane $\mathbb{H}$, and for a value of the j-invariant of elliptic curve $\mathcal{C} = \mathbb{C}/L_\tau$, where L_τ is a lattice in $\mathbb{C}$ generated by 1 and $\tau \in \mathbb{H}$.

Let $\mathcal{C}$ and $\widetilde{\mathcal{C}}$ be elliptic curves over $\mathbb{C}$. An *isogeny* between $\mathcal{C}$ and $\widetilde{\mathcal{C}}$ is a nonconstant morphism $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ which sends the identity element of the group $\mathcal{C}$ to the identity element of the group $\widetilde{\mathcal{C}}$. Such a morphism is necessarily a homomorphism of groups. A kernel Γ of a non-zero isogeny $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ is a subgroup of finite order in $\mathcal{C}$, and for any subgroup of finite order Γ there exists a unique isogeny $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ such that $\ker \psi = \Gamma$. For any elliptic curve $\mathcal{C}$ and integer n the multiplication by n on $\mathbb{C}$ projects to an isogeny

$[n] : \mathcal{C} \to \mathcal{C}$ of degree n^2 with the kernel consisting of points whose order divides n. Furthermore, for any isogeny $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ of degree n there exists a unique *dual* isogeny $\widehat{\psi} : \widetilde{\mathcal{C}} \to \mathcal{C}$ such that

$$\widehat{\psi} \circ \psi = [n] \tag{8}$$

on $\mathcal{C}$, and

$$\psi \circ \widehat{\psi} = [n] \tag{9}$$

on $\widetilde{\mathcal{C}}$ (for the proofs of the above facts see e.g., [13, Chapter III]). An isogeny whose kernel is a cyclic group of order n is called n-cyclic.

Below, we mostly will consider specific n-cyclic isogenies defined as follows. Let $\mathcal{C}_1 = \mathbb{C}/L_\tau$ be an elliptic curve and n an integer. Then the multiplication by n on $\mathbb{C}$ projects to an n-cyclic isogeny

$$\psi_n : \mathcal{C}_1 \to \mathcal{C}_2, \tag{10}$$

where $\mathcal{C}_2 = \mathbb{C}/L_{n\tau}$. The dual isogeny

$$\widehat{\psi}_n : \mathcal{C}_2 \to \mathcal{C}_1 \tag{11}$$

is the projection of the identical map on $\mathbb{C}$.

There exists a polynomial in two variable

$$\Phi_n(x, y) = 0 \tag{12}$$

with integer coefficients, called the *modular equation*, having the following property: if $\mathcal{C}_1$ and $\mathcal{C}_2$ are two elliptic curves with j-invariant j_1 and j_2, then an n-cyclic isogeny $\mathcal{C}_1 \to \mathcal{C}_2$ exists if and only if (j_1, j_2) is a point of curve (12) (see [3, Chapter 5]). In particular, since (10) is an n-cyclic isogeny between elliptic curves with j-invariants $j(\tau)$ and $j(n\tau)$, for any $\tau \in \mathbb{H}$ the equality

$$\Phi_n(j(\tau), j(n\tau)) = 0 \tag{13}$$

holds.

Let $\mathcal{C}$ be an elliptic curve and $A = A_j$ a Lattès map satisfying (7). Further, let Γ be a subgroup of $\mathcal{C}$ and $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ an isogeny such that $\ker \psi = \Gamma$. Since ψ is a homomorphism, the equality $\psi(-x) = -\psi(x)$ holds, implying that there exists a rational function V_Γ such that the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\psi} & \widetilde{\mathcal{C}} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \widetilde{\pi}} \\ \mathbb{CP}^1 & \xrightarrow{V_\Gamma} & \mathbb{CP}^1 \end{array}$$

commutes. Similarly, for the dual isogeny $\widehat{\psi} : \widetilde{\mathcal{C}} \to \mathcal{C}$ there exists a rational function U_Γ such that the diagram

$$\begin{array}{ccc} \widetilde{\mathcal{C}} & \xrightarrow{\widehat{\psi}} & \mathcal{C} \\ \downarrow{\scriptstyle \widetilde{\pi}} & & \downarrow{\scriptstyle \pi} \\ \mathbb{CP}^1 & \xrightarrow{U_\Gamma} & \mathbb{CP}^1 \end{array}$$

commutes. Thus, to any subgroup Γ of $\mathcal{C}$ corresponds a decomposition

$$A_j = U_\Gamma \circ V_\Gamma. \tag{14}$$

In particular, the equality

$$\widehat{\psi}_n \circ \psi_n = [n]$$

gives rise to a decomposition

$$A_j = U_n \circ V_n. \tag{15}$$

Notice that explicit expressions for U_Γ and V_Γ can be deduced from Vélu's formulas for isogenies $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ with given $\mathcal{C}$ and $\ker \psi$ (see [15]).

Equality (9) implies that an elementary transformation of A_j corresponding to decomposition (14) also is a flexible Lattès map $A_{j'}$, where j' is j-invariant of $\widetilde{\mathcal{C}}$. Furthermore, if Γ is a cyclic group of order n, then the corresponding values of j' are described by the condition that (j, j') is a point of (12). Clearly, in order to prove that $[A_j]$ has infinitely many conjugacy classes it is enough to prove that we can obtain infinitely many conjugacy classes using chains of elementary transformations arising from decompositions (15) only. Moreover, since conjugate Lattès maps correspond to isomorphic elliptic curves and isogeny (10) corresponds to the point $(j(\tau), j(n\tau))$ on (12), it is enough to show that for any $\tau \in \mathbb{H}$ the sequence $j(n^k\tau)$ takes infinitely many values.

In order to prove the last statement recall that the Fourier expansion for $j(\tau)$ in $q = e^{2\pi i\tau}$ is

$$j(\tau) = \frac{1}{q} + 744 + 196884q + \cdots .$$

Further,

$$q_k = e^{2\pi i(n^k\tau)} \to 0, \quad \text{as} \quad k \to \infty,$$

since $\Im(\tau) > 0$. Therefore,

$$j(n^k\tau) \to \infty, \quad \text{as} \quad k \to \infty,$$

implying that $j(n^k\tau)$ takes infinitely many distinct values. This proves the "if" part of Theorem 1.1 for Lattès maps A given by (7).

Consider now flexible Lattès maps $\widetilde{A} = \widetilde{A}_j$ defined by the diagram

$$\begin{tikzcd} \mathcal{C} \arrow[r, "nz+\beta"] \arrow[d, "\pi"] & \mathcal{C} \arrow[d, "\pi"] \\ \mathbb{CP}^1 \arrow[r, "\widetilde{A}"] & \mathbb{CP}^1 \end{tikzcd}, \tag{16}$$

where $n \in \mathbb{Z}$ is odd and β is a point of order two on $\mathcal{C}$. For $c \in \mathbb{C}$ set $\varphi_c = z + c$. Since $2\beta = 0$ and n is odd,

$$nz + \beta = nz \circ \varphi_\beta \tag{17}$$

on $\mathcal{C}$. Further, since $\varphi_\beta(-z) = -\varphi_\beta(z)$ on $\mathcal{C}$, there exists a Möbius transformation μ which makes the diagram

$$\begin{tikzcd} \mathcal{C} \arrow[r, "\varphi_\beta"] \arrow[d, "\pi"] & \mathcal{C} \arrow[d, "\pi"] \\ \mathbb{CP}^1 \arrow[r, "\mu"] & \mathbb{CP}^1 \end{tikzcd}$$

commutative. Therefore, the Lattès map $\widetilde{A} = \widetilde{A}_j$ and the Lattès map $A = A_j$ defined by diagram (7) are related by the equality

$$\widetilde{A}_j = A_j \circ \mu, \tag{18}$$

where μ is a Möbius transformation.

Clearly, an elementary transformation $A_j \to A_{j'}$ corresponding to decomposition (15) induces an elementary transformation

$$U_n \circ V_n \circ \mu \to V_n \circ \mu \circ U_n \tag{19}$$

of $\widetilde{A}_j$. Moreover, since the composition

$$\mathcal{C}_2 \xrightarrow{\widehat{\psi}_n} \mathcal{C}_1 \xrightarrow{\varphi_\beta} \mathcal{C}_1$$

equals the composition

$$\mathcal{C}_2 \xrightarrow{\varphi_{n\beta}} \mathcal{C}_2 \xrightarrow{\widehat{\psi}_n} \mathcal{C}_1,$$

and $\varphi_{n\beta}(-z) = -\varphi_{n\beta}(z)$ on $\mathcal{C}_2$, considering the commutative diagram

$$\begin{tikzcd}
\mathcal{C}_2 \arrow[r, "\widehat{\psi}_n"] \arrow[d, "\pi_2"] & \mathcal{C}_1 \arrow[r, "\varphi_\beta"] \arrow[d, "\pi_1"] & \mathcal{C}_1 \arrow[r, "\psi_n"] \arrow[d, "\pi_1"] & \mathcal{C}_2 \arrow[d, "\pi_2"] \\
\mathbb{CP}^1 \arrow[r, "U_n"] & \mathbb{CP}^1 \arrow[r, "\mu"] & \mathbb{CP}^1 \arrow[r, "V_n"] & \mathbb{CP}^1
\end{tikzcd}$$

we see that

$$(V_n \circ \mu) \circ U_n = V_n \circ U_n \circ \mu',$$

where μ' is a Möbius transformation satisfying

$$\begin{tikzcd}
\mathcal{C}_2 \arrow[r, "\varphi_{n\beta}"] \arrow[d, "\pi_2"] & \mathcal{C}_2 \arrow[d, "\pi_2"] \\
\mathbb{CP}^1 \arrow[r, "\mu'"] & \mathbb{CP}^1 .
\end{tikzcd}$$

Thus, if $A_j \to A_{j'}$ is the elementary transformation corresponding to decomposition (15), then the elementary transformation of $\widetilde{A}_j$ in the right part of (19) is a Lattès map $\widetilde{A}_{j'}$ defined by the diagram

$$\begin{tikzcd}
\mathcal{C}_2 \arrow[r, "nz+\beta'"] \arrow[d, "\pi_2"] & \mathcal{C}_2 \arrow[d, "\pi_2"] \\
\mathbb{CP}^1 \arrow[r, "\widetilde{A}_{j'}"] & \mathbb{CP}^1 ,
\end{tikzcd}$$

where $\beta' = n\beta$ is a points of order two on $\mathcal{C}_2$. Therefore, a chain of elementary transformations

$$A_j \to A_{j_1} \to A_{j_2} \to \dots$$

with infinitely many different j arising from decompositions (15) induces a similar chain

$$\widetilde{A}_j \to \widetilde{A}_{j_1} \to \widetilde{A}_{j_2} \to \dots .$$

This finishes the proof of Theorem 1.1.

4 Decompositions of $\mathcal{L}_j$

In this section, we provide some explicit formulas illustrating constructions from the previous section in the simplest case where considered Lattès maps are defined by the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{2z} & \mathcal{C} \\ \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi} \\ \mathbb{CP}^1 & \xrightarrow{\mathcal{L}} & \mathbb{CP}^1, \end{array} \tag{20}$$

and prove Theorem 1.2. In order to reduce the number of parameters, we will write elliptic curves in the Legendre form

$$\mathcal{E}_\lambda : y^2 = x(x-1)(x-\lambda), \qquad \lambda \in \mathbb{C} \setminus \{0,1\}. \tag{21}$$

When working with the explicit expression for $\mathcal{L} = \mathcal{L}_j$ we will use the notation

$$L_\lambda = \frac{1}{4}\,\frac{\left(z^2-\lambda\right)^2}{z\,(z-1)\,(z-\lambda)}.$$

So, $L_\lambda = \mathcal{L}_j$, where

$$j = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}.$$

The next result describes explicitly all equivalence classes of decompositions of L_λ.

Theorem 4.1. Any decomposition of L_λ into a composition of rational functions of degree greater than one is equivalent to one of the following decompositions

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

$$L_\lambda(z) = \left(\frac{1}{4}\,\frac{z^2+2z+1}{z+1-\lambda}\right)\circ\left(z+\frac{1-\lambda}{z-1}\right) \tag{22}$$

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

These decompositions are not equivalent and have form (14), where Γ runs over cyclic subgroups of order two in $\mathcal{C}$. □

Proof. Recall that equivalence classes of decompositions of a rational function F are in a one-to-one correspondence with imprimitiivity systems of the monodromy group G_F of F. Namely, if z_0 is a non-critical value of F, and G_F is realized as a permutation group acting on the set $F^{-1}\{z_0\}$, then to an equivalence class of a decomposition $F = U\circ V$, corresponds an imprimitivity system of G_F consisting of $d = \deg A$ blocks $V^{-1}\{t_i\}$, $1\le i\le d$, where $\{t_1,t_2,\dots,t_d\} = U^{-1}\{z_0\}$.

It is clear that for any decomposition $L_\lambda = U\circ V$ with $\deg U > 1$, $\deg V > 1$ the equalities $\deg V = 2$, $\deg U = 2$ hold. Therefore, if c is a non-critical value of $L_\lambda(z)$ and G_{L_λ} is realized as a permutation group acting on $L_\lambda^{-1}\{c\} = \{z_0,z_1,z_2,z_3\}$, then to each equivalence class of decompositions of L_λ corresponds a block of size two containing the point z_0, say. Since there might be at most three such blocks, namely, $\{z_0,z_1\}$, $\{z_0,z_2\}$, and $\{z_0,z_3\}$, there exist at most three non-equivalent decompositions of L_λ.

Prove now that the decompositions

$$L_\lambda = C_i\circ D_i,\quad i=1,2,3,$$

given by formulas (22) are not equivalent. Since the set

$$L_\lambda^{-1}\{\infty\} = \{\infty,0,1,\lambda\}$$

consists of four different points, the point $c=\infty$ is a non-critical value of L_λ and we can assume that G_{L_λ} acts on the set $L_\lambda^{-1}\{\infty\}$. Furthermore,

$$C_1^{-1}\{\infty\} = \{\lambda+1,\infty\},\quad C_2^{-1}\{\infty\} = \{\lambda-1,\infty\},\quad C_3^{-1}\{\infty\} = \{1-\lambda,\infty\},$$

implying that the blocks containing the point $z_0=\infty$ of the corresponding imprimitivity systems are

$$\{0,\infty\},\quad \{1,\infty\},\quad \{\lambda,\infty\}. \tag{23}$$

Since these blocks are different, decompositions (22) are not equivalent.

Similarly, decompositions (14), where Γ runs over cyclic subgroups of order two, are not equivalent, and in fact reduce to decompositions (14). Indeed, since any element of the function field of $\mathcal{E}_\lambda$ has the form $p(x)+q(x)y$, where p and q are rational functions, it follows from $\pi(-z) = \pi(z)$ and $\deg \pi = 2$ that $\pi = \mu \circ x$ for some Möbius transformation π. Thus, without loss of generality we may assume that $\pi = x$. Since π maps the unit element of $\mathcal{C}$ to infinity, it follows from (20) that π is a bijection between points of order two on $\mathcal{C}$ and the set $L_\lambda^{-1}\{\infty\}$, implying that the blocks containing $z_0 = \infty$ corresponding to decompositions (14) are exactly the sets listed in (23), that is the blocks corresponding to decompositions (22). ■

Notice that the images of the isogenies corresponding to left parts of decompositions (22) do not have Legendre form (21). Therefore, elementary transformations corresponding to decompositions (22) are not *equal* to functions $L_\lambda(z)$ but only *conjugate* to such functions.

Corollary 4.1. Any elementary transformations of the function $\mathcal{L}_j$, $j \in \mathbb{C}$, has the form $\mathcal{L}_{j'}$, $j' \in \mathbb{C}$, where values of j' are defined by the condition $\Phi_2(j, j') = 0$. □

Proof. Indeed, if $L_\lambda = U \circ V$ is a decomposition such that one of the functions U and V is invertible, then the corresponding elementary transformation leads to a function conjugate to L_λ. On the other hand, any decomposition of L_λ into a composition of rational functions of degree greater than one is equivalent to one of decompositions (22). ■

Clearly, Corollary 4.1 implies Theorem 1.2. Furthermore, since the modular equation $\Phi_2(x, y) = 0$ is given by the equation

$$\begin{aligned} -x^2y^2 + x^3 + y^3 + 2^4 \cdot 3 \cdot 31\, xy(x+y) + 3^4 \cdot 5^3 \cdot 4027\, xy \\ - 2^4 \cdot 3^4 \cdot 5^3(x^2+y^2) + 2^8 \cdot 3^7 \cdot 5^6(x+y) - 2^{12} \cdot 3^9 \cdot 5^9 = 0 \quad (24) \end{aligned}$$

and can be parametrized by the rational functions

$$x = 64\,\frac{(j+4)^3}{j^2}, \qquad y = 64\,\frac{(j+4)^3}{j^2} \circ \frac{1}{j},$$

the correspondence $\mathcal{F}$ associated with (24) has form (3).

References

[1] Buff, X. and A. Epstein. “A parabolic Pommerenke-Levin-Yoccoz inequality.” *Fund. Math.* 172, no. 3 (2002): 249–89.

[2] Klein, F. “Ueber die Transformation der elliptischen Functionen und die Auflösung der Gleichungen fünften Grades.” *Math. Ann.* 14 (1879): 111–72.

[3] Lang, S. *Elliptic Functions. Graduate Texts in Mathematics* 112. New York: Springer, 1987.

[4] McMullen, C. “Families of rational maps and iterative root-finding algorithms.” *Ann. Math.* 125, no. 3 (1987): 467–93.

[5] Medvedev, A. and T. Scanlon. “Invariant varieties for polynomial dynamical systems.” *Ann Math*. 179, no. 1 (2014): 81–177.

[6] Milnor, J. On Lattès maps. In *Dynamics on the Riemann Sphere. A Bodil Branner Festschrift,* edited by P. Hjorth and C. L. Petersen, 9–43. European Mathematical Society, 2006.

[7] Muzychuk, M. and F. Pakovich. “Jordan-Holder theorem for imprimitivity systems and maximal decompositions of rational functions.” *Proc. Lond. Math. Soc*. 102, no. 1 (2011): 1–24.

[8] Milnor, J. *Dynamics in One Complex Variable*. Princeton Annals in Mathematics 160. Princeton, NJ: Princeton University Press, 2006.

[9] Pakovich, F. “On polynomials sharing preimages of compact sets, and related questions.” *Geom. Funct. Anal*. 18, no. 1 (2008): 163–83.

[10] Pakovich, F. “On semiconjugate rational functions.” *Geom. Funct. Anal*. 26, no. 4 (2016): 1217–43.

[11] Pakovich, F. “Polynomial semiconjugacies, decompositions of iterations, and invariant curves.” *Ann. Sc. Norm. Super. Pisa Cl. Sci. (5)*, to appear.

[12] Ritt, J. “Prime and composite polynomials.” *Trans. Amer. Math. Soc*. 23 (1922): 51–66.

[13] Silverman, J. *The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics* 106. New York: Springer, 1986.

[14] Silverman, J. *The Arithmetic of Dynamical Systems. Graduate Texts in Mathematics* 241. New York: Springer, 2007.

[15] Vélu, J. “Isogénies entre courbes elliptiques.” *CR Acad. Sci. Paris Seér.* A-B 273, (1971): A238-41.