

RATIONAL FUNCTIONS ADMITTING DOUBLE DECOMPOSITIONS

A. B. BOGATYRĚV

ABSTRACT. Ritt (1922) studied the structure of the set of complex polynomials with respect to composition. A polynomial $P(x)$ is said to be indecomposable if it can be represented as $P = P_1 \circ P_2$ only if either P_1 or P_2 is a linear function. A decomposition $P = P_1 \circ P_2 \circ \dots \circ P_r$ is said to be maximal if all the P_j are indecomposable polynomials that are not linear. Ritt proved that any two maximal decompositions of the same polynomial have the same length r , the same (unordered) set $\{\deg(P_j)\}$ of the degrees of the composition factors, and can be connected by a finite chain of transformations each of which consists in replacing the left-hand side of the double decomposition

$$(1) \quad R_1 \circ R_2 = R_3 \circ R_4$$

by its right-hand side. Solutions of this functional equation are indecomposable polynomials of degree greater than 1, and Ritt listed all of them explicitly.

Up until now, analogues of Ritt's theory for rational functions have only been constructed for some special classes of these functions, for instance, for Laurent polynomials (Pakovich, 2009). In this note we describe a certain class of double decompositions (1) with rational functions $R_j(x)$ of degree greater than 1. In essence, the rational functions described below were discovered by ZolotarĚv as solutions of a certain optimization problem (1932). However, the double decomposition property for these functions remained little known because they had an awkward parametric representation. Below we give a representation for ZolotarĚv fractions (possibly new), which resembles the well-known representation for Chebyshev polynomials. These, by the way, are a special limit case of ZolotarĚv fractions.

§ 1. ZOLOTARĚV FRACTIONS AND THEIR COMPOSITION PROPERTY

A purely imaginary parameter $\tau \in i\mathbb{R}_+$ defines the rectangle $\Pi(\tau)$ of size $2 \times |\tau|$:

$$\Pi(\tau) := \{u \in \mathbb{C} : |\operatorname{Re} u| \leq 1, 0 \leq \operatorname{Im} u \leq |\tau|\}.$$

The conformal map $x_\tau(u)$ taking this rectangle to the upper half-plane and fixing the three points $u = \pm 1, 0$ has the following simple form:

$$x_\tau(u) = \operatorname{sn}(K(\tau)u|\tau)$$

in terms of the elliptic sine sn and the complete elliptic integral K . It is easy to deduce from the reflection principle for a conformal map that the parametric representation

$$R(u) := x_\tau(u); \quad x(u) := x_{n\tau}(u), \quad u \in \mathbb{C}, \quad n \in \mathbb{N},$$

defines a rational function R of degree n in the argument x depending parametrically on τ :

$$Z_n(x|\tau) := R(u(x)) = x_\tau \circ x_{n\tau}^{-1}.$$

2010 *Mathematics Subject Classification.* Primary 30D05; Secondary 33E05.

Key words and phrases. Ritt theory, composition factors, ZolotarĚv fraction, elliptic functions, lattices.

This research was supported by the Russian Foundation for Basic Research (grant no. 10-01-00407) and by the programme “Modern Problems of Theoretical Mathematics” of the Division of Mathematical Sciences of the Russian Academy of Sciences.

This rational function is known as a ZolotarĚv fraction. It follows directly from the definition that ZolotarĚv fractions satisfy the following composition property:

$$(2) \quad Z_{mn}(x|\tau) = Z_m(Z_n(x|m\tau)|\tau), \quad m, n \in \mathbb{N}.$$

As the parameter τ tends to zero, ZolotarĚv fractions, modified by suitable fractional linear transformations, become the classical Chebyshev polynomials, and the classical composition property of Chebyshev polynomials appears as a consequence of formula (2) given above. Interchanging n and m in formula (2) we observe that ZolotarĚv fractions of composite degrees have double decompositions of the form (1). We generalize this construction in the following section.

§ 2. THE CONSTRUCTION

Let L be a lattice of rank two in the plane of a complex variable u . We denote the group of translations of the plane by elements of this lattice by the same letter L . We let L^+ denote the extension of the group L by the element of order two corresponding to the transformation $u \rightarrow -u$. The extended group acts discontinuously on the complex plane, so that the orbit space is well defined and has the natural complex structure

$$\mathbb{C}/L^+ = \mathbb{C}P^1.$$

On this Riemann sphere we can introduce a global coordinate, say,

$$x(u) = \wp(u|L) := u^{-2} + \sum_{0 \neq v \in L} ((u-v)^{-2} - v^{-2}), \quad u \in \mathbb{C}.$$

Traditionally, (some) basis in the lattice L is used as the second argument of the Weierstrass function, although the function depends only on the lattice itself as a whole.

If our lattice L contains a sublattice L_\bullet of full rank, then the corresponding extended group L_\bullet^+ is a subgroup of L^+ , and therefore every orbit of the group L_\bullet^+ is contained in some orbit of the group L^+ . Thus a holomorphic map of one sphere onto the other appears:

$$(3) \quad \mathbb{C}/L_\bullet^+ \rightarrow \mathbb{C}/L^+,$$

which can be identified with a rational function, once we have fixed a global complex coordinate on each sphere. In this fashion we obtain a parametrically defined rational function $R_{L:L_\bullet}(x)$ of degree $|L : L_\bullet|$:

$$(4) \quad R_{L:L_\bullet}(x_\bullet(u)) := x(u), \quad x_\bullet(u) := \wp(u|L_\bullet),$$

which is the general form of rational functions with extremality number $g = 1$ in the terminology of [6]. In order to obtain a ZolotarĚv fraction of modulus $\tau \in i\mathbb{R}_+$, we must take the lattice $L = \text{Span}_{\mathbb{Z}}\{4, 2\tau\}$ and its sublattice $L_\bullet = \text{Span}_{\mathbb{Z}}\{4, 2n\tau\}$. Then $R_{L:L_\bullet}(x)$ coincides with $Z_n(x|\tau)$ up to normalization (that is, up to pre- and post-composition with fractional linear functions).

Suppose that we have two sublattices L_\bullet and L_\circ of full rank in the lattice L . Their intersection $L_{\bullet\circ} := L_\bullet \cap L_\circ$ is a sublattice of full rank in both L_\bullet and L_\circ . Indeed, $L_{\bullet\circ}$ contains the sublattice $|L : L_\bullet||L : L_\circ|L$ of full rank. Under these conditions the following double decomposition holds:

$$(5) \quad R_{L:L_{\bullet\circ}} = R_{L:L_\bullet} \circ R_{L_\bullet:L_{\bullet\circ}} = R_{L:L_\circ} \circ R_{L_\circ:L_{\bullet\circ}}.$$

Not all relations of the form (5) are independent. In what follows we shall show that an arbitrary double decomposition (5) follows from the same relations for sublattices L_\bullet , L_\circ of prime indices in L .

§ 3. SUBLATTICES OF PRIME INDEX

If we are given a basis of a lattice L , then a basis of a sublattice L_\bullet can be obtained using a 2×2 integer matrix Q . A different choice of bases results in multiplying Q by invertible integer matrices (that is, with determinant ± 1) on the left and on the right. The index of the sublattice L_\bullet in the lattice L is denoted by $|L : L_\bullet|$ and is defined to be equal to $|\det Q|$; it is independent of the choice of bases in the lattice and the sublattice. If we are given a sequence of sublattices $L \supset L_\bullet \supset L_{\bullet\bullet}$, then their indices satisfy the chain rule: $|L : L_{\bullet\bullet}| = |L : L_\bullet| |L_\bullet : L_{\bullet\bullet}|$.

Lemma 1. *Any sublattice L_\bullet of prime index p in L has the following representation:*

$$(6) \quad L_\bullet = \text{Span}_{\mathbb{Z}}\{pL, e\},$$

where e is an arbitrary element in $L_\bullet \setminus pL$. Conversely, the right-hand side of (6) is a sublattice of prime index p in L if $e \notin pL$.

Proof. Let $Q \in \text{GL}_2(\mathbb{Z})$ be a matrix that takes a basis of L to a basis of L_\bullet . The matrix $(\det Q) \cdot Q^{-1}$ is integer-valued and, consequently, L_\bullet contains a sublattice pL of index $p = \det Q$. Consider the chain of sublattices

$$pL \subset \text{Span}_{\mathbb{Z}}\{pL, e\} \subset L_\bullet.$$

The prime index $p = |L_\bullet : pL|$ is equal to the product of indices $|L_\bullet : \text{Span}\{\dots\}|$ and $|\text{Span}\{\dots\} : pL|$; consequently, one of them is equal to 1. In other words, the middle lattice in the chain coincides either with the left- or the right-hand lattice. The choice of the element e tells us that the middle lattice of the chain is strictly larger than pL . \square

Corollary 1. *Suppose that $L_\bullet \neq L_\circ$ are two sublattices of L of the same prime index p . Then $L_\bullet \cap L_\circ = pL$.*

Proof. Every sublattice of L of index p contains pL . If the intersection $L_\bullet \cap L_\circ$ contains at least one element $e \notin pL$, then each of the two sublattices can be reconstructed using (6), and consequently they coincide. \square

Corollary 2. *Suppose that L_\bullet and L_\circ are two sublattices of L with different prime indices p_\bullet and p_\circ , respectively. Then their intersection has the following representation:*

$$(7) \quad L_\bullet \cap L_\circ = \text{Span}_{\mathbb{Z}}\{p_\bullet p_\circ L, p_\bullet e_\circ, p_\circ e_\bullet\},$$

where e_* is an arbitrary element of $L_* \setminus p_* L$, where the index $*$ is equal to \bullet or \circ .

Proof. We denote the lattice on the right-hand side of (7) by $L_{\bullet\circ}$ and claim that it is a sublattice of L_\bullet of index p_\circ . Indeed, (6) implies the representation

$$L_{\bullet\circ} = \text{Span}_{\mathbb{Z}}\{p_\circ L_\bullet, p_\bullet e_\circ\},$$

and it remains to verify that $p_\bullet e_\circ \notin p_\circ L_\bullet$. If this was not the case, then we would have $p_\bullet e_\circ \in p_\bullet L \cap p_\circ L = p_\bullet p_\circ L$ and $e_\circ \in p_\circ L$, contrary to our choice of the element e_\circ . We can verify that $L_{\bullet\circ}$ is similarly a sublattice of L_\circ of index p_\bullet . Thus, $L_{\bullet\circ}$ is a sublattice of the intersection $L_\bullet \cap L_\circ$. The index of $L_\bullet \cap L_\circ$ in L is a multiple of both numbers p_\bullet and p_\circ , that is, at least $p_\bullet p_\circ$. On the other hand,

$$p_\bullet p_\circ = |L : L_{\bullet\circ}| = |L : L_\bullet \cap L_\circ| |L_\bullet \cap L_\circ : L_{\bullet\circ}|.$$

Hence (7) follows. \square

Combining Corollaries 1 and 2 we obtain the following lemma.

Lemma 2. *Suppose that L_\bullet and L_\circ are two sublattices of L of prime indices p_\bullet and p_\circ , respectively, and let $L_{\bullet\circ} := L_\bullet \cap L_\circ$ be their intersection. If $L_\bullet \neq L_\circ$, then $|L_\bullet : L_{\bullet\circ}| = p_\circ$ and $|L_\circ : L_{\bullet\circ}| = p_\bullet$. In the opposite case, if $L_\bullet = L_\circ$, then $|L_\bullet : L_{\bullet\circ}| = |L_\circ : L_{\bullet\circ}| = 1$.*

We now can list all the sublattices of L of a given prime index p . The quotient of any lattice (6) by its sublattice pL consists of p elements $\{je\}$, $j = 0, \dots, p-1$, and is naturally included in the quotient L/pL consisting of p^2 elements. For different sublattices L_\bullet , the quotients L_\bullet/pL intersect only in the zero element of L/pL . Consequently, there exist exactly $(p^2 - 1)/(p - 1) = p + 1$ sublattices in L of given prime index p . One can verify that they are represented, for example, by the following change of basis matrices Q for any fixed basis in L :

$$\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}, \quad j = 0, p - 1, \quad \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

§ 4. SUBLATTICES OF COMPOSITE INDEX

We fix an arbitrary lattice L of rank 2 and sublattices L_* , L^* of full rank.

For suitable bases in the lattices L and L_* , the change of basis matrix Q_* is diagonal (to prove this we use the Smith canonical form for integer matrices). By decomposing the elements of Q_* into products of prime numbers we obtain a representation of this matrix as a product of integer matrices with prime determinants. Thus we obtain a chain of nested lattices $L := L_0 \supset L_1 \supset L_2 \supset \dots \supset L_r =: L_*$ with consecutive prime indices $p_j := |L_{j-1} : L_j|$. The same argument applied to the second sublattice L^* gives another filtration $L := L^0 \supset L^1 \supset L^2 \supset \dots \supset L^s =: L^*$ with prime indices $p^k := |L^{k-1} : L^k|$.

We consider the sublattices $L_j^k := L_j \cap L^k$ that naturally fill the following rectangular table:

$$(8) \quad \begin{array}{ccccccc} L^s & \leftarrow & L_1^s & \leftarrow & L_2^s & \leftarrow & \dots & \leftarrow & L_r^s = L_* \cap L^* := L_*^* \\ \downarrow & & \downarrow & & \downarrow & & & & \downarrow \\ \vdots & & \vdots & & \vdots & & & & \vdots \\ \downarrow & & \downarrow & & \downarrow & & & & \downarrow \\ L^2 & \leftarrow & L_1^2 & \leftarrow & \dots & \leftarrow & \dots & \leftarrow & L_r^2 \\ \downarrow & & \downarrow & & \downarrow & & & & \downarrow \\ L^1 & \leftarrow & L_1^1 & \leftarrow & L_2^1 & \leftarrow & \dots & \leftarrow & L_r^1 \\ \downarrow & & \downarrow & & \downarrow & & & & \downarrow \\ L & \leftarrow & L_1 & \leftarrow & L_2 & \leftarrow & \dots & \leftarrow & L_r \end{array}$$

where arrows denote embeddings. Indeed,

$$L_{j-1}^k \cap L_j^{k-1} := (L_{j-1} \cap L^k) \cap (L_j \cap L^{k-1}) = (L_j \cap L_{j-1}) \cap (L^k \cap L^{k-1}) = L_j \cap L^k =: L_j^k.$$

Applying Lemma 2 successively to the elementary squares of table (8) starting at the bottom left and moving to the right along rows, and upwards along columns, we obtain the following.

Corollary 3. *Adjacent sublattices in table (8) either coincide or have prime index: $|L_{j-1}^k : L_j^k| \in \{1, p_j\}$; $|L_j^{k-1} : L_j^k| \in \{1, p^k\}$.*

Theorem 1. *Any double decomposition (5) is a consequence of relations of the same type for sublattices L_\bullet, L_\circ of prime index.*

Proof of Theorem 1. Consider all possible paths from L_*^* to L going via the arrows of table (8). Every path corresponds to a filtration of the initial lattice L , and consequently, also to a decomposition of the rational function $R_{L:L_*^*}(x)$ into prime composition factors (which may be identity elements). A change of path resulting from bypassing an elementary square in the table differently (see Figure 1) results in two adjacent terms of the decomposition being replaced on the basis of the double decomposition relation (5),

$$R_{L_j^k:L_{j+1}^k} \circ R_{L_{j+1}^k:L_{j+1}^{k+1}} = R_{L_j^k:L_j^{k+1}} \circ R_{L_j^{k+1}:L_{j+1}^{k+1}},$$

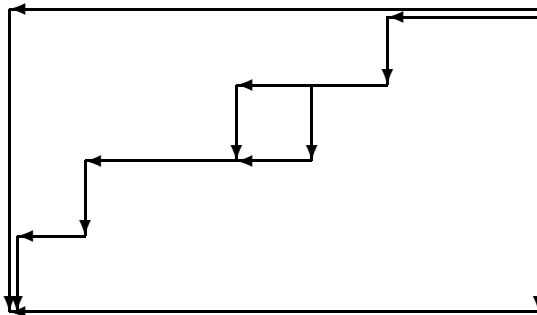


FIGURE 1. Deformation of paths in the table

corresponding to sublattices with prime indices. The path going along the upper and left sides of the table can be transformed into the path going over the right and lower sides by such elementary replacements. \square

REFERENCES

- [1] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66. MR1501189
- [2] F. Pakovich, *Prime and composite Laurent polynomials*, Bull. Sci. Math. **133** (2009), 693–732. MR2557404 (2011c:30075)
- [3] F. Pakovich, *On semiconjugate rational functions*, Preprint, arXiv:1108.1900v2.
- [4] E. I. Zolotarëv, *Application of elliptic functions to questions about functions which deviate least or most from zero (1877)*, Complete collection of works of E. I. Zolotarëv, vol. 2. Academy of Sciences of USSR, Leningrad, 1932, 1–59. (Russian)
- [5] N. I. Achieser, *Lectures on the theory of approximation*, Nauka, Moscow, 1965; English transl., *Theory of approximation*, Dover Publications, New York, 1992.
- [6] A. V. Bogatyřev, *Chebyshev representation of rational functions*, Mat. Sb. **201** (2010), no. 11, 19–40; English transl., Sb. Math. **201** (2010), no. 11–12, 1579–1598. MR2768552 (2011k:30047)

INSTITUTE OF COMPUTATIONAL MATHEMATICS OF THE RUSSIAN ACADEMY OF SCIENCES
E-mail address: gourmet@inm.ras.ru

Translated by E. KHUKHRO
 Originally published in Russian