Solution of the polynomial moment problem

M. Muzychuk, F. Pakovich

November 26, 2007

1 Introduction

In this paper we solve the following "polynomial moment problem": *for a complex polynomial $P(z)$ and distinct complex numbers a, b to describe polynomials $q(z)$ such that*

$$\int_a^b P^i(z)q(z)\mathrm{d}z = 0 \tag{1}$$

for all integer $i \geq 0$.

The polynomial moment problem was posed in the series of papers [2]-[5] in connection with the center problem for the Abel differential equation

$$\frac{\mathrm{d}y}{\mathrm{d}z} = p(z)y^2 + q(z)y^3 \tag{2}$$

with polynomial coefficients $p(z), q(z)$ in the complex domain. For given complex numbers a, b the center problem for the Abel equation is to find necessary and sufficient conditions on $p(z), q(z)$ which imply the equality $y(b) = y(a)$ for any solution $y(z)$ of (2) with $y(a)$ small enough. This problem is closely related to the classical Center-Focus problem of Poincare and has been studied in many recent papers (see e.g. [1]-[9], [26]).

The center problem for the Abel equation is connected with the polynomial moment problem in several ways. For example, it was shown in [4] that for the parametric version

$$\frac{\mathrm{d}y}{\mathrm{d}z} = p(z)y^2 + \varepsilon q(z)y^3$$

of (2) the "infinitesimal" center conditions with respect to ε reduce to moment equations (1) with $P(z) = \int p(z)\mathrm{d}z$. On the other hand, it was shown in [7] that "at infinity" (under an appropriate projectivization of the parameter space) the system of equations on the coefficients of $q(z)$, describing the center set of (2) for fixed $p(z)$, also reduces to (1). Many other results concerning connections between the center problem and the polynomial moment problem can be found in [7]. These results convince that a thorough description of solutions of system (1) is an important step in understanding of the center problem for the Abel equation.

There exists a natural condition on $P(z)$ and $Q(z)=\int q(z)\mathrm{d}z$ which reduces equations (1), (2) to similar equations with respect to polynomials of lesser degrees. Namely, suppose that there exist non-linear polynomials $\tilde{P}(z)$, $\tilde{Q}(z)$, $W(z)$ such that

$$P(z)=\tilde{P}(W(z)), \qquad Q(z)=\tilde{Q}(W(z)). \tag{3}$$

Then performing the change of variable $w=W(z)$ we see that

$$\int_a^b P^i(z)q(z)\mathrm{d}z=\int_{W(a)}^{W(b)}\tilde{P}^i(w)\tilde{Q}'(w)\mathrm{d}w. \tag{4}$$

Similarly, equation (2) transforms to the equation

$$\frac{\mathrm{d}\tilde{y}}{\mathrm{d}w}=\tilde{P}'(w)\tilde{y}^2+\tilde{Q}'(w)\tilde{y}^3 \tag{5}$$

and any solution $y(z)$ of equation (2) is the pull-back

$$y(z)=\tilde{y}(W(z)) \tag{6}$$

of a solution $\tilde{y}(w)$ of equation (5).

Furthermore, if the polynomial $W(z)$ in (3) satisfies the equality

$$W(a)=W(b) \tag{7}$$

then in view of (6) equation (2) has a center. Similarly, in view of (4) condition (7) implies that $Q(z)$ is a solution of system (1). This justifies the following definition: a center for equation (2) or a solution of system (1) is called *reducible* if there exist polynomials $\tilde{P}(z)$, $\tilde{Q}(z)$, $W(z)$ such that conditions (3), (7) hold. The main conjecture concerning the center problem for the Abel equation ("the composition conjecture"), supported by the results obtained in the papers cited above, states that any center for the Abel equation is reducible (see [7] and the bibliography there).

By analogy with the composition conjecture it was suggested ("the composition conjecture" for the polynomial moment problem) that, under the additional assumption $P(a)=P(b)$, any solution of (1) is reducible. This conjecture was shown to be true in many cases. For instance, if a,b are not critical points of $P(z)$ ([9]), if $P(z)$ is indecomposable ([16]), and in some other special cases (see [20], [19], [22]). Nevertheless, in general the composition conjecture for the polynomial moment problem fails to be true. Namely, if for a given polynomial $P(z)$ several reducible solutions of (1) exist then it may happen that the sum of these solutions is an irreducible solution ([15]). The simplest explicit example of an irreducible solution of (1) obtained in this way has the following form:

$$P(z)=T_6(z), \quad q(z)=T_2'(z)+T_3'(z), \quad a=-\sqrt{3}/2, \quad b=\sqrt{3}/2,$$

where $T_n(z)$ is the n-th Chebyshev polynomial (recall that $T_n(z)=T_{n/d}(T_d(z))$ for any $d|n$).

It was conjectured in [17] that actually *any* irreducible solution of (1) is a sum of reducible ones. In view of the fact that all compositional factors $W(z)$ of a polynomial $P(z)$ can be defined explicitely such a description of irreducible solutions of (1) would be very convenient, especially for applications to the Abel equation (cf. [7]). However, until now this conjecture was verified only for the case $P(z) = T_n(z)$ which is rather special (see [18]).

Explicit necessary and sufficient conditions for a polynomial $q(z)$ to be a solution of (1) were constructed in [20]. Set $n = \deg P(z)$ and denote by $P_i^{-1}(z)$, $1 \leq i \leq n$, the branches of the algebraic function $P^{-1}(z)$. It was shown in [20] that there exists a system of equations

$$\sum_{i=1}^{n} f_{s,i} Q(P_i^{-1}(z)) = 0, \qquad 1 \leq s < n, \tag{8}$$

with $f_{s,i}$ taking values in the set $\{0, -1, 1\}$, such that (1) holds if and only if (8) holds. Moreover, this system was constructed explicitly with the use of a special planar tree λ_P which represents the monodromy group G_P of the algebraic function $P^{-1}(z)$ in a combinatorial way. By construction, points a, b are vertices of λ_P and system (8) reflects the combinatorics of the path connecting a, b on λ_P.

A finite system of equations (8) is more convenient for a study than the initial infinite system of equatons (1). In particular, in many cases the analysis of (8) permits to conclude that for given $P(z), a, b$ any solution of (1) is reducible (see [20]). In this paper we develop the necessary algebraic and analytic techniques in order to describe the solutions of (8) in general case and, as a corollary, prove the conjecture above. So, our main result is the following theorem.

Theorem. *A non-zero polynomial $q(z)$ is a solution of system (1) if and only if $Q(z) = \int q(z)\mathrm{d}z$ can be represented as a sum of polynomials $Q_j(z)$ such that*

$$P(z) = \tilde{P}_j(W_j(z)), \quad Q_j(z) = \tilde{Q}_j(W_j(z)), \quad \textit{and} \quad W_j(a) = W_j(b) \tag{9}$$

for some polynomials $\tilde{P}_j(z), \tilde{Q}_j(z), W_j(z)$.

Note that since conditions of the theorem impose no restrictions on the values of $P(z)$ at the points a, b the theorem implies in particular that non-zero solutions of (1) exist if and only if the equality $P(a) = P(b)$ holds.

The paper is organized as follows. In the second section we give a brief account of definitions and results related to the polynomial moment problem and prove an extended version of criterion (8). Besides, we introduce the "module of relations" $M_{P,a,b}$ connected with (8). By definition, $M_{P,a,b}$ is a subspace of $\mathbb{Q}^n$ generated by the vectors

$$(f_{s,\sigma(1)}, f_{s,\sigma(2)}, \dots, f_{s,\sigma(n)})$$

for all s, $1 \leq s < n$, and $\sigma \in G_P$. Notice that, by construction, $M_{P,a,b}$ is an invariant subspace of $\mathbb{Q}^n$ with respect to the permutation representation of the group G_P.

Since $P(z)$ is a polynomial, the group G_P contains a cycle of lenght equal to the degree of G_P. Such groups possess a number of remarkable properties and have a developped theory which goes back to Schur. In the third section of the paper, written entirely in the framework of the group theory, we show that for any permutation group G of degree n, containing a cycle of lenght n, the subspaces of $\mathbb{Q}^n$ which are invariant with respect to the permutation representation of G can be described explicitely via the imprimitivity systems of G only. We believe that this result is new and interesting by itself.

Finally, in the fourth section, using the description of G_P-invariant subspaces of $\mathbb{Q}^n$ and the Puiseux expansions technique, we describe all *rational* functions $Q(z)$ such that a function defined near infinity by the equality

$$H(t) = \int_a^b \frac{Q(z)P'(z)dz}{P(z)-t}.$$

is rational. The solution of the polynomial moment problem is obtained as a corollary of this description since in the case when $Q(z)$ is a polynomial the rationality of $H(t)$ turns out to be equivalent to system (1).

Acknowledgments. The authors are grateful to L. Gavrilov, M. Klin, and Y. Yomdin for discussions. The second author also would like to thank the Max Planck Institut für Mathematik for its support and hospitality.

2 Preliminaries

2.1 Criterion for $H(t)$ to be rational

Unless stated otherwise, in this paper $P(z)$ denotes a polynomial while $Q(z)$ denotes a rational function such that

$$Q(a) = Q(b) = 0. \tag{10}$$

In particular, we suppose that condition (10) holds when we use the notation $Q(z) = \int q(z)\mathrm{d}z$ for a primitive of a solution of the polynomial moment problem (in view of (1) taken for $i = 0$ the values of any primitive of $q(z)$ at points a, b coincide).

For a curve $\Gamma_{a,b} \subset \mathbb{C}$ connecting points a and b and $P(z), Q(z)$ as above we will denote by $H(t) = H(P, Q, \Gamma_{a,b}, t)$ a function defined near infinity by the equality

$$H(t) = \int_{\Gamma_{a,b}} \frac{Q(z)P'(z)dz}{P(z)-t}. \tag{11}$$

After the change of variable $z \to P(z)$ the integral above becomes the Cauchy type integral

$$\int_{\gamma} \frac{g(z)dz}{z-t}\,, \tag{12}$$

where $\gamma = P(\Gamma_{a,b})$ and $g(z)$ is an algebraic function obtained by the analytic continuation of a germ of the algebraic function $g(z) = Q(P^{-1}(z))$ along γ

(see the paper [19] for the general theory of Cauchy type integrals of algebraic functions). Integral representation (12) defines a collection of univalent regular functions $I_i(t)$, where each $I_i(t)$ is defined in a domain U_i of the complement of γ in $\mathbb{CP}^1$ and, by definition, $H(t)$ coincides with a function which corresponds to a domain containing infinity.

Lemma 2.1. *Let $P(z), q(z)$ be polynomials, a, b be distinct complex numbers, and $Q(z) = \int q(z)\mathrm{d}z$. Then the following conditions are equivalent:*

1) the equalities

$$\int_a^b P^i(z)q(z)\mathrm{d}z = 0,$$

hold for all $i \geq 0$,

2) the equalities

$$\int_a^b P^i(z)Q(z)P'(z)\mathrm{d}z = 0,$$

hold for all $i \geq 0$,

3) the function $H(t)$ vanishes identically for any path $\Gamma_{a,b}$ connecting the points a and b.

Proof. It may be verified by a direct calculation (see [20], p. 753) that

$$\frac{dH(t)}{dt} = \frac{Q(a)}{P(a)-t} - \frac{Q(b)}{P(b)-t} + \tilde{H}(t), \tag{13}$$

where

$$\tilde{H}(t) = \int_a^b \frac{q(z)dz}{P(z)-t}.$$

Now the lemma follows from the fact that the integrals appearing in conditions 1) and 2) of the lemma are coefficients of the Taylor expansions near infinity of the functions $\tilde{H}(t)$, $H(t)$ respectively. □

The lemma 2.1 shows that the polynomial moment problem is equivalent to the problem of description of polynomials $Q(z)$ for which $H(t) \equiv 0$ and it was shown in [20] that $H(t) \equiv 0$ if and only if $Q(z)$ satisfies a certain system of equation (8).

In this paper we will allow $Q(z)$ to be a rational function and will investigate conditions under which $H(t)$ is a rational function. The motivation for such a setting is the fact that from the algebraic point of view it is more natural to investigate all rational solutions $Q(z)$ of system (8) not only polynomial ones. In general, such solutions lead to rational $H(t)$. On the other hand, as we will see below if $Q(z)$ is a polynomial then the property of $H(t)$ to be rational is equivalent to the condition that $H(t)$ vanishes identically.

Observe that the property of $H(t)$ to be rational does not depend on the choice of the integration path $\Gamma_{a,b}$ (we always will assume that $\Gamma_{a,b}$ does not contain the poles of $Q(z)$). This is the corollary of the following lemma.

Lemma 2.2. *For any closed integration path $\Gamma \subset \mathbb{C}$ a function $\hat{H}(t)$ defined near infinity by the integral*

$$\hat{H}(t) = \int_{\Gamma} \frac{Q(z)P'(z)dz}{P(z)-t}.$$

is rational.

Proof. Indeed, since Γ is closed, $\hat{H}(t)$ is equal to a linear combination of the residues, multiplied by $2\pi i$, of a function

$$h(t) = \frac{Q(z)P'(z)}{P(z)-t}$$

in some bounded domain U of $\mathbb{C}$. Since $P(z)$ is a polynomial, for t close to infinity a function

$$\frac{P'(z)}{P(z)-t}$$

is holomorphic in U. On the other hand, if $\alpha \in U$ is a pole of order d of $Q(z)$ then setting

$$Q(z) = \frac{\tilde{Q}(z)}{(z-\alpha)^d},$$

where $\tilde{Q}(z)$ is a rational function holomorphic at α, we see that the residue of $h(t)$ at α is equal to

$$\frac{1}{(d-1)\,!} \lim_{z\to\alpha} \frac{\mathrm{d}^{d-1}}{\mathrm{d}z^{d-1}} \left\{ \frac{\tilde{Q}(z)P'(z)}{P(z)-t} \right\}.$$

This implies that $\hat{H}(t)$ is rational. $\square$

In order to obtain a transparent criterion for $H(t)$ to be a rational function it is convenient to choose $\Gamma_{a,b}$ as a path connecting the corresponding vertices on a special tree λ_P, embedded into the Riemann sphere, defined as follows (see [20]). Let $c_1, c_2, ..., c_k$ be the set of all finite branching points of the algebraic function $P^{-1}(z)$ (this set obviously coincides with the set of all finite critical values of the map $P(z)$) and let c be a non-branching point. Draw a star S joining c with $c_1, c_2, ..., c_k$ by non intersecting arcs $\gamma_1, \gamma_2, ..., \gamma_k$ and define λ_P as the preimage of S under the map $P(z) : \mathbb{C} \to \mathbb{C}$ (see Fig. 1). By definition, vertices of λ_P are preimages of the points c_s, $1 \leq s \leq k$, and c, while edges of λ_P are preimages of the arcs γ_s, $1 \leq s \leq k$. Furthermore, we will mark the preimages of the point c_s, $1 \leq s \leq k$, by the number s. It is not difficult to show that λ_P is connected and has no cycles. Therefore, λ_P is a plane tree. The set of all edges of λ_P adjacent to a non-marked vertex w is called a *star* of λ_P centered at w.

Let $U \subset \mathbb{C}$ be a simply connected domain containing the set $S \backslash \{c_1, c_2, ..., c_k\}$ but not containing the points $\{c_1, c_2, ..., c_k\}$. The set of stars of λ_P is naturally

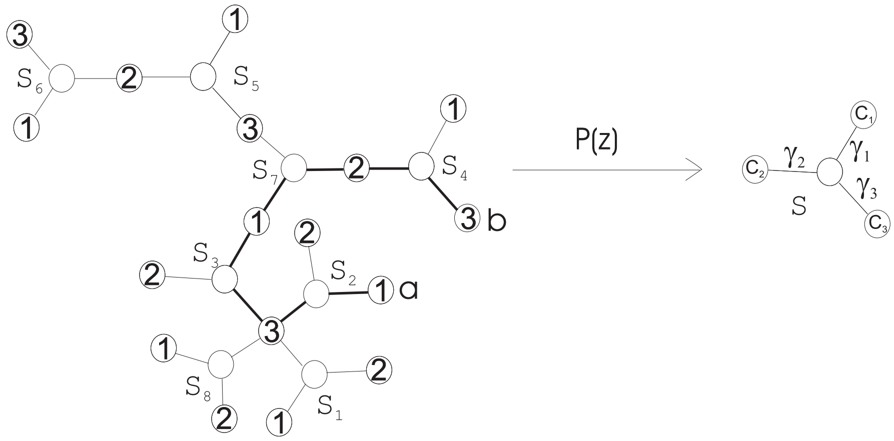

Figure 1

identified with the set of single-valued branches $P_i^{-1}(z)$, $1 \leq i \leq n$, of the algebraic function $P^{-1}(z)$ defined in U. We will label the star which corresponds to the branch $P_i^{-1}(z)$, $1 \leq i \leq n$, by the symbol S_i. Observe that, since $P(z)$ is a polynomial, the element of the monodromy group G_P of the algebraic function $P^{-1}(z)$ corresponding to the loop around infinity is a cycle of length n. We always will assume that the numeration of branches $P_i^{-1}(z)$, $1 \leq i \leq n$, is chosen in such a way that this cycle coincides with the cycle $(12...n)$ (this numeration is defined uniquely up to the choice of $P_0(z)$).

The tree constructed above is known under the name of "constellation" and is very useful for the combinatorial analysis of the group G_P (see [13] for further details and other versions of this construction). Since however the points a, b are vertices of so constructed λ_P only if $P(a)$ and $P(b)$ are critical values of $P(z)$, in case if $P(a)$ or $P(b)$ (or both of them) is not a critical value of $P(z)$ we modify the construction as follows: take as $c_1, c_2, ..., c_k$ all finite critical values of $P(z)$ complemented by $P(a)$ or $P(b)$ (or by both of them) and as above set $\lambda_P = P^{-1}\{S\}$, where S is the star connecting c with $c_1, c_2, ..., c_k$ (we suppose that c is chosen distinct from $P(a), P(b)$). Clearly, λ_P is still connected and has no cycles. Furthermore, the points a, b are vertices of λ_P. Since λ_P is connected and has no cycles there exists a unique oriented path $\mu_{a,b} \subset \lambda_P$ with the starting point a and the ending point b.

By construction, if we choose $\mu_{a,b}$ as a new way of integration then after the change of variable $z \to P(z)$ integral (12) reduces to the sum of integrals

$$H(t) = \sum_{s=1}^{k} \int_{\gamma_s} \frac{\varphi_s(z)}{z-t} \, \mathrm{d}z, \tag{14}$$

where $\varphi_s(z)$, $1 \leq s \leq k$, are linear combinations of the functions $Q(P_i^{-1}(z))$,

$1 \leq i \leq n$. More precisely,

$$\varphi_s(z) = \sum_{i=1}^{n} f_{s,i} Q(P_i^{-1}(z)), \tag{15}$$

where $f_{s,i} \neq 0$ if and only if the path $\mu_{a,b}$ contains an edge e of λ_P such that e is adjacent to an s-vertex v_s and is contained in the star S_i. Furthermore, if when crossing S_i the vertex v_s is followed by the center of S_i then $f_{s,i} = -1$ otherwise $f_{s,i} = 1$. For example, for the graph λ_P shown on Fig. 1 and the path $\mu_{a,b} \subset \lambda_P$ pictured by the fat line we have:

$$\varphi_1(z) = -Q(P_2^{-1}(z)) + Q(P_3^{-1}(z)) - Q(P_7^{-1}(z)),$$
$$\varphi_2(z) = Q(P_7^{-1}(z)) - Q(P_4^{-1}(z)),$$
$$\varphi_3(z) = Q(P_2^{-1}(z)) - Q(P_3^{-1}(z)) + Q(P_4^{-1}(z)).$$

Theorem 2.1. *Let $P(z) \in \mathbb{C}[z]$, $Q(z) \in \mathbb{C}(z)$, and $a, b \in \mathbb{C}$, $a \neq b$. Then $H(t)$ is a rational function if and only if $\varphi_s(z) \equiv 0$ for any s, $1 \leq s \leq k$.*

Proof. Let us suppose at first that λ_P does not contain poles of $Q(z)$. In this case representation (14) is well defined. This implies in particular that the function $H(t)$ extends to a function analytic in the domain $\mathbb{CP}^1 \setminus S$. Furthermore, since a small deformation of $S \setminus \{c_1, c_2, \dots, c_k\}$ does not change the germ of $H(t)$ near infinity, it is easy to see that we can continue $H(t)$ analytically to any point of $\mathbb{CP}^1 \setminus \{c_1, c_2, \dots, c_k\}$.

If z_0 is an interior point of some γ_s, $1 \leq s \leq k$, then by the well-known boundary property of Cauchy type integrals we have:

$$\lim_{t \to z_0}{}^{+} H(t) - \lim_{t \to z_0}{}^{-} H(t) = \varphi_s(t_0), \tag{16}$$

where the limits are taken respectively for t tending to z_0 from the "left" and from the "right" parts of γ_s. Clearly, if $H(t)$ is a rational function then the limits above coincide for any z_0 and hence $\varphi_s(z) \equiv 0$. On the other hand, if

$$\varphi_s(z) \equiv 0, \qquad 1 \leq s \leq k, \tag{17}$$

then it follows directly from formula (14) that $H(t) \equiv 0$.

Suppose now that λ_P contains some poles of $Q(z)$. First of all observe that performing in case of necessity a small deformation of $S \setminus \{c_1, c_2, \dots, c_k\}$ we may assume that these poles are located only at the preimages of the points $c_1, c_2, \dots, c_k$. Deform now the path $\mu_{a,b}$ as follows. First, construct for each s, $1 \leq s \leq k$, a small loop δ_s around c_s. Then for each pole $x \in \mu_{a,b}$ for which $P(x) = s$, $1 \leq s \leq k$, replace a small part of $\mu_{a,b}$ near x by a part ω_x of the connectivity component of the preimage $P^{-1}(\delta_s)$ which bounds the domain containing x (see Fig. 2).

By construction, for the function $H(t)$ corresponding to so defined new way of integration we have:

$$H(t) = \sum_{s=1}^{k} \int_{\gamma_s} \frac{\varphi_s(z)}{z - t}\,\mathrm{d}z + \sum_{s}^{k} \int_{l_s} \frac{g_s(z)}{z - t}\,\mathrm{d}z + \sum_{s}^{k} \int_{\delta_s} \frac{h_s(z)}{z - t}\,\mathrm{d}z,$$

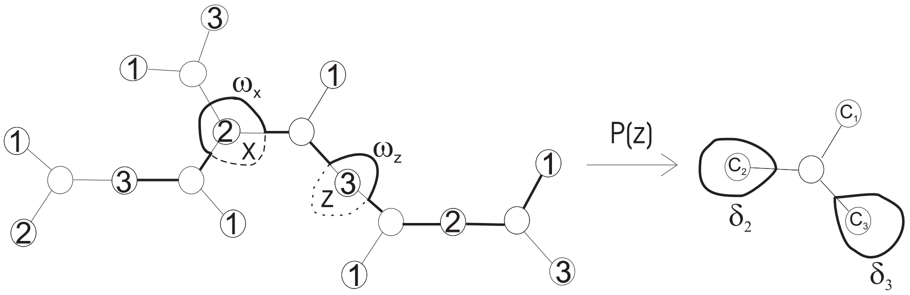

Figure 2

where l_s is the part of S which is inside of the domain bounded by δ_s, $g_s(z)$ are some linear combinations of the branches of $P^{-1}(z)$, and $h_s(z)$ are analytic continuations of $g_s(z)$ along δ_s. Observe now that we can take the loops δ_s as close to the corresponding c_s, $1 \leq s \leq k$, as we want. This implies that the function $H(t)$ can have singularities only at the points $c_1, c_2, \dots, c_k$. Furthermore, in view of (16), this implies that $H(t)$ does not ramify at c_s, $1 \leq s \leq k$, if and only if condition (17) holds. In particular, condition (17) is necessary for the rationality of $H(t)$. On the other hand, since condition (17) implies that $H(t)$ does not ramify at c_s, $1 \leq s \leq k$, in order to prove the sufficiency of (17) we only must show that Laurent series expansions of $H(t)$ near c_s can not contain an infinite number of negative degree terms.

So, suppose that condition (17) holds. Then we have:

$$H(t) = \sum_{s}^{k} \int_{l_s} \frac{g_s(z)}{z-t}\,\mathrm{d}z + \sum_{s}^{k} \int_{\delta_s} \frac{h_s(z)}{z-t}\,\mathrm{d}z. \tag{18}$$

Any integral form the second sum in (18) induces two analytic functions $I_s^+(t)$ and $I_s^-(t)$ defined outside and inside of δ_x respectively from which the function $I_s^+(t)$ gives a contribution to $H(t)$. $I_s^+(t)$ and $I_s^-(t)$ are connected in a neighborhood of δ_x by the boundary formula

$$I_s^+(t) = I_s^-(t) + h_s(t). \tag{19}$$

Defining the analytic continuation of $I_s^+(t)$ as the analytic continuation of the right side of this equality we see that $I_s^+(t)$ can be continued analytically inside of the domain bounded by δ_x with the point c_s removed. Furthermore, it follows from (19) that at c_s the analytic continuation of $I_s^+(t)$ can have only finite number of negative degree terms in its Puiseux expansion.

On the other hand, it is known (see [19], Theorem 3.4) that in a neighborhood of the end point z_0 of a non-closed integration way l the Cauchy type integral of an algebraic function $g(z)$ bounded on l has the form

$$\int_l \frac{g(z)}{z-t}\,\mathrm{d}z = u(t)\log(t-z_0) + v(t), \tag{20}$$

where $u(t)$ is a function analytic at z_0 and $v(t)$ is a bounded function which has a finite ramification at z_0. In particular, the s-th integral from the first sum in (18) near c_s, $1 \leq s \leq k$, has the form

$$u_s(t)\log(t - c_s) + v_s(t), \tag{21}$$

where $u_s(t)$ is a function analytic at c_s and $v_s(t)$ is a bounded function which has a finite ramification at c_s.

Since other integrals from (18) are holomorphic or have a finite ramification at c_s, we see that if $H(t)$ has no ramification at c_s then $u_s(t) \equiv 0$ near c_s. Therefore, formulas (19), (21) imply that $H(t)$ can have only finite number of negative degree terms in its Puiseux expansion near c_s, $1 \leq s \leq k$. Since $H(t)$ has no ramification at c_s, $1 \leq s \leq k$, we conclude that c_s is a pole of $H(t)$ at worst. This proves the sufficiency of condition (17). $\square$

Note that the above construction shows that if $Q(z)$ is a polynomial then $H(t)$ is a rational function if and only if $H(t) \equiv 0$. Indeed, in this case $H(t)$ does not depend on the integration path. On the other hand, as we saw, for the path $\mu_{a,b}$ the rationality of $H(t)$ implies that $H(t) \equiv 0$. More generally, if $Q(z)$ is a rational function which does not have poles on the set $P^{-1}\{c_1, c_2, \dots, c_k\}$ then the rationality of $H(t)$ for some path $\Gamma_{a,b}$ implies that for the path $\mu_{a,b}$ the corresponding function $H(t)$ vanishes.

2.2 Subspace $M_{P,a,b}$

The simplest form of the equality $\varphi_s(z) = 0$, $1 \leq s \leq k$, is the equality

$$Q(P_{i_1}^{-1}(z)) = Q(P_{i_2}^{-1}(z)) \tag{22}$$

for some $i_1 \neq i_2$, $1 \leq i_1, i_2 \leq n$. Furthermore, such an equality has the clear functional meaning.

For $P(z), Q(z) \in \mathbb{C}(z)$ denote by $d(Q(P^{-1}(z)))$ the degree of the algebraic function $Q(P^{-1}(z))$ that is the number of its different branches.

Lemma 2.3. *Let $P(z), Q(z) \in \mathbb{C}(z)$. Then*

$$d(Q(P^{-1}(z))) = \deg P(z)/[\mathbb{C}(z) : \mathbb{C}(P, Q)].$$

Proof. See e. g. [16], lemma 1. $\square$

Notice that, since by the Lüroth theorem any subfield of $\mathbb{C}(z)$ has the form $\mathbb{C}(W(z))$ for some $W(z) \in \mathbb{C}(z)$, lemma 2.3 implies that equality (22) holds if and only if

$$P(z) = \tilde{P}(W(z)), \qquad Q(z) = \tilde{Q}(W(z)) \tag{23}$$

for some $\tilde{P}(z), \tilde{Q}(z), W(z) \in \mathbb{C}(z)$ with $\deg W(z) > 1$.

For any element σ of the monodromy group G_P of the algebraic function $P^{-1}(z)$ the equality $\varphi_s(z) = 0$, $1 \leq s \leq k$, implies by the analytic continuation the equality

$$\sum_{i=1}^{n} f_{s,i} Q(P^{-1}_{\sigma(i)}(z)) = 0.$$

Changing σ by σ^{-1} we see that theorem 2.1 implies that $H(t)$ is a rational function if and only if

$$\sum_{i=1}^{n} f_{s,\sigma(i)} Q(P^{-1}_{i}(z)) = 0$$

for any $\sigma \in G_P$ and s, $1 \leq s \leq k$.

Denote by $M_{P,a,b}$ the subspace of $\mathbb{Q}^n$ generated by the vectors

$$(f_{s,\sigma(1)}, f_{s,\sigma(2)}, \, \dots \, , f_{s,\sigma(n)})$$

for all s, $1 \leq s \leq k$, and $\sigma \in G_P$. Abusing notation we usually will not distinguish an element of $M_{P,a,b}$ and the corresponding equation connecting branches of $Q(P^{-1}(z))$. For example, instead of the notation

$$(0, 0, \, \dots \, , 1, \, \dots \, , 0, 0, \, \dots \, , -1, \, \dots \, , 0, 0) \tag{24}$$

for an element of $M_{P,a,b}$ we will use simply equality (22).

It turns out that $M_{P,a,b}$ always contains certain specific elements the form of which depends only on the local behavior of $P(z)$ near points a, b. Denote by $P^{-1}_{a_1}(z)$, $P^{-1}_{a_2}(z), \dots, P^{-1}_{a_{d_a}}(z)$ (resp. $P^{-1}_{b_1}(z)$, $P^{-1}_{b_2}(z)$, ... , $P^{-1}_{b_{d_b}}(z)$) the branches of $P^{-1}(z)$ in U which map points close to $P(a)$ (resp. $P(b)$) to points close to a (resp. b). In particular, d_a (resp. d_b) equals the multiplicity of the point a (resp. b) with respect to $P(z)$.

Proposition 2.1. *Suppose that $P(a) = P(b)$. Then $M_{P,a,b}$ contains the element*

$$\frac{1}{d_a} \sum_{s=1}^{d_a} Q(P^{-1}_{a_s}(z)) = \frac{1}{d_b} \sum_{s=1}^{d_b} Q(P^{-1}_{b_s}(z)). \tag{25}$$

On the other hand, if $P(a) \neq P(b)$ then $M_{P,a,b}$ contains the elements

$$\frac{1}{d_a} \sum_{s=1}^{d_a} Q(P^{-1}_{a_s}(z)) = 0, \qquad \frac{1}{d_b} \sum_{s=1}^{d_b} Q(P^{-1}_{b_s}(z)) = 0. \tag{26}$$

Proof. Can be deduced from theorem 2.1 exactly in the same way as it was done in [20], proposition 4.1, for the case when $Q(z)$ is a polynomial, or from the properties of Cauchy type integrals of algebraic functions (see [19], Corollary 3.9). $\square$

The proposition below, proved in [20] with the use of some topological considerations related to the topology of sphere (see the "Monodromy Lemma", p.

766) describes some specific property of the mutual position on the unit circle of the sets

$$V(a) = \{\varepsilon_n^{a_1}, \varepsilon_n^{a_2}, ..., \varepsilon_n^{a_{d_a}}\} \qquad \text{and} \qquad V(b) = \{\varepsilon_n^{b_1}, \varepsilon_n^{b_2}, ..., \varepsilon_n^{b_{d_b}}\},$$

where $\varepsilon_n = exp(2\pi i/n)$ (recall our convention about the numeration of branches of $P^{-1}(z)$).

Let us introduce the following definitions. Say that two sets of points X, Y on the unit circle S^1 are *disjointed* if there exist $s_1, s_2 \in S^1$ such that all points from X are on the one of two connected components of $S^1 \setminus \{s_1, s_2\}$ while all points from Y are on the other one. Say that X, Y are *almost disjointed* if $X \cap Y$ consists of a single point s_1 and there exists a point $s_2 \in S^1$ such that all points from $X \setminus s_1$ are on the one of two connected components of $S^1 \setminus \{s_1, s_2\}$ while all points from $Y \setminus s_1$ are on the other one.

Proposition 2.2. *The sets $V(a)$ and $V(b)$ are disjointed or almost disjointed. Furthermore, if $P(a) = P(b)$ then $V(a)$ and $V(b)$ are disjointed.* $\square$

Remark. A general algebraic approach to linear relations between roots of algebraic equations was developped in the papers [10], [11]. In particular, it follows from Theorem 1 of [11] that a necessary and sufficient condition for the existence of at least one solution of (17), such that the functions $Q(P_i^{-1}(z))$, $1 \leq i \leq n$, are distinct between themselves, is that the subspace $M_{P,a,b}$ does not contain elements of the form (24). An equivalent form of this condition is that the subspace $M_{P,a,b}$ does not contain any of subspaces $V_d^{\perp}$, $d \in D(G_P)$, which are defined below. Notice however that the method of [11] does not provide any information about the description or the actual finding of these solutions.

3 Permutation representations of groups containing a full cycle

3.1 Invariant subspaces and the centralizer ring

The construction of $M_{P,a,b}$ implies that $M_{P,a,b}$ is an invariant subspace of $\mathbb{Q}^n$ with respect to the so called *permutation representation* of the group G_P on $\mathbb{Q}^n$. By definition, the permutation representation of a transitive permutation group $H \subseteq S_n$ on $\mathbb{Q}^n$ is a homomorphism $R_H : H \rightarrow GL_n(\mathbb{Q})$ which associates to $h \in H$ a matrix $R_H(h)$ for which $r_{i,j} = 1$ if $j = i^h$ and 0 otherwise. In other words,

$$R_H(h) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_{1^h} \\ x_{2^h} \\ \vdots \\ x_{n^h} \end{pmatrix}.$$

Note that $\mathbb{Q}^n$ admits a R_H-invariant scalar product $(x, y) := \sum_{i=1}^n x_i y_i$.

The goal of this section is to provide a full description of the invariant subspaces of $\mathbb{Q}^n$ with respect to the permutation action of G_P. More general, we classify all invariant subspaces of $\mathbb{Q}^n$ with respect to the permutation representation of an arbitrary group $G \subseteq S_n$ containing the cycle $(1, ..., n)$. In the following G will always denote such a group.

Recall that a subset B of $X = \{1, 2, \ldots, n\}$ is called a *block* ([25]) of a transitive permutation group $H \subseteq S_n$ if for each $h \in H$ the set B^h is either disjoint or equal to B. For a block B the set $\mathcal{B} := \{B^h \mid h \in H\}$ forms a partition of X into a disjoint union of blocks of equal cardinality which is called an *imprimitivity system* of H. Each permutation group $H \subseteq S_n$ has two *trivial* imprimitivity systems: one formed by singletones and another formed by the whole X. A permutation group is called *primitive* if it has only trivial imprimitivity systems. Otherwise it is called *imprimitive*.

For each $d \,|\, n$ we denote by V_d the subspace of $\mathbb{Q}^n$ consisting of d-periodic vectors. The fact that the group G contains the cycle $(1, ..., n)$ implies easily the followng statement.

Lemma 3.1. *Any imprimitivity system for G coincides with the residue classes modulo d for some $d \,|\, n$. Furthermore, for given d such classes form an imprimitivity system for G if and only if the subspace V_d is G-invariant.* $\square$

Denote by $D(G)$ the set of all divisors of n for which V_d is G-invariant. Clearly, $1, n \in D(G)$. Notice that $D(G)$ is a lattice with respect to the operations $\wedge, \vee$, where $d \wedge f := \gcd(d, f)$ and $d \vee f := \operatorname{lcm}(d, f)$. Indeed, for an element $x \in X$ the intersection of two blocks containing x and corresponding to $d, f \in D(G)$ is a block which corresponds to $d \vee f$. On the other hand, the intersection of two invariant subspaces V_d, V_f is an invariant subspace which is equal to $V_{d\wedge f}$.

Say that $d \in D(G)$ covers $f \in D(G)$ if $f \,|\, d$, $f < d$, and there is no $x \in D(G)$ such that $f < x < d$ and $f|x$, $x|d$. Now we are ready to formulate the main result of this section.

Theorem 3.1. *Each R_G-irreducible subspace of $\mathbb{Q}^n$ has the form*

$$U_d := V_d \cap \left(V_{f_1}^{\perp} \cap ... \cap V_{f_\ell}^{\perp}\right),$$

where $d \in D(G)$ and $f_1, ..., f_\ell$ is a complete set of elements of $D(G)$ covered by d. Every R_G-invariant subspace of $\mathbb{Q}^n$ is a direct sum of some U_d's.

The proof of this theorem splits in several steps and is given below. We start from recalling some basics facts of the representations theory which we will use afterwards (see e.g. [12]).

First, any representation of a finite group H over a field k of characteristic not dividing $|G|$ is completely reducible that is a direct sum of irreducible subrepresentations (Maschke's theorem). Furthermore, irreducible subspaces of a completely reducible representation $T : H \to GL_n(k)$ are in one to one correspondence with minimal idempotents of the *centralizer ring* $V_k(H)$. Recall that $V_k(H)$ consists of all matrices $A \in M_n(k)$ which commute with every

$T(h), h \in H$, and that a non-zero matrix E is called idempotent if $E^2 = E$. Furthermore, two idempotents E, F are called *orthogonal* if $EF = FE = 0$ and an idempotent $E \in V_k(H)$ is called minimal if it can not be presented as a sum of two orthogonal idempotents from $V_k(H)$. Under this notation the correspondence above is obtained as follows: to a minimal idempotent $E \in V_k(H)$ corresponds an irreducible subspace $V = \mathsf{Im}\{E\}$.

In general, the decompositon of a completely reducible representation into a sum of irreducible subrepresentations is not uniquely defined. Nevertheless, if

$$V = V_1^{\oplus a_1} \oplus \cdots \oplus V_r^{\oplus a_r} \tag{27}$$

is a decomposition such that V_i, $1 \leq i \leq r$, are non-isomorphic irreducible subrepresentations then the factors $V_i^{\oplus a_i}$, $1 \leq i \leq r$, are defined uniquely. They correspond to the minimal idempotents of the *center* $C(V_k(H))$ of $V_k(H)$. The centralizer ring $V_k(H)$ is commutative if and only if all the multiplicities of irreducible subrepresentations equal 1. For such representations irreducible invariant subspaces simply correspond to minimal idempotents of $V_k(H)$.

For any group G as above the ring $V_{\mathbb{Q}}(G)$ is isomorphic to a subring of the group algebra of a cyclic group (see Proposition 3.3 below) and therefore is commutative. Summing up we obtain.

Proposition 3.1. *An R_G-invariant subspace $W \subset \mathbb{Q}^n$ is irreducible if and only if there exists a minimal idempotent $E \in V_{\mathbb{Q}}(G)$ such that $\mathsf{Im}\{E\} = W$. Every R_G-invariant subspace is a direct sum of some W's.*

For each transitive permutation group $H \subseteq S_n$ we can construct some special basis of $V_{\mathbb{C}}(H)$ via orbits of the stabilizer H_1 of the point 1 as follows. To each orbit Δ of H_1 associate a matrix V^{Δ}, where $V^{\Delta}_{i,j} = 1$ if there exist $h \in H$, $\delta \in \Delta$ such that $1^h = j$, $\delta^h = i$, and $V^{\Delta}_{i,j} = 0$ otherwise. In particular, for the first column of V^{Δ} the equality $V^{\Delta}_{i,1} = 1$ holds if and only if $i \in \Delta$. It turns out that the matrices V^{Δ} form a basis of $V_{\mathbb{C}}(H)$ ([25], Theorem 28.4). Furthermore, since by construction the matrices V^{Δ} are contained in $M_n(\mathbb{Q})$ they form a basis of $V_{\mathbb{Q}}(H)$. We summarize the properties of V^{Δ} in the proposition below (see [25], §28).

Proposition 3.2. *The matrices V^{Δ} satisfy the following conditions:*

(1) V^{Δ} form a basis of the algebra $V_{\mathbb{Q}}(H)$ as of a $\mathbb{Q}$-module,

(2) If $\Delta_1 \neq \Delta_2$ then the ones of Δ_1 and Δ_2 do not occure in the same place. On the other hand, $\sum_{\Delta} V^{\Delta}$ is a matrix all the entries of which are ones.

(3) For each orbit Δ there exists an orbit Γ such that $(V^{\Delta})^T = V^{\Gamma}$.

Notice that the property (3) implies that for the first row V^{Δ} the equality $V^{\Delta}_{1,j} = 1$ holds if and only if $j \in \Gamma$. Furthermore, it is easy to see that the mapping $\Delta \to \Gamma$ defines an involution on the set of orbits of G_1.

3.2 Schur rings

3.2.1 Isomorphism between $S_{\mathbb{Q}}(G)$ and $V_{\mathbb{Q}}(G)$

In order to construct the minimal idempotents of $V_{\mathbb{Q}}(G)$ we will use so called *Schur rings* introduced by Schur in his classical paper [24] for the investigation of permutation groups $G \subseteq S_n$ containing a regular subgroup C of degree n. Since in this paper C always will be a cyclic group, in the following we will restrict our attention to this case only (see [25] for the account of the Schur method in the general case).

The idea of the Schur approach can be described as follows. Suppose that G contains the cycle $c := (1, ..., n)$. Then elements of the set $\{1, 2, \ldots, n\}$ can be identified with elements of the cyclic group C generated by c as follows: to the element i corresponds the element of C which transforms 1 to i. Therefore, we can consider G as a permutation group on its subgroup C. After such an identification we can "multiply" elements of the set $\{1, 2, \ldots, n\}$ and this multiplication is agreed with the action of G in the following sense: if $h, g \in H$ then $h^g = hg$. Furthermore, identifying any two subsets of $\{1, 2, \ldots, n\}$ with the corresponding elements of the group algebra $\mathbb{Q}[C]$ we can define their "product" as the product of these element in $\mathbb{Q}[C]$. The remarkable result of Schur is that under such a multiplication the orbits of the stabilizer G_1 form a basis of some subalgebra of $\mathbb{Q}[C]$. To make this statement precise let us introduce the following definition.

For $T \subseteq C$ denote by $T^{(-1)}$ the set of elements of C inverse to the elements of T and by $\underline{T}$ the formal sum $\sum_{h \in T} h$. The elements of $\mathbb{Q}[C]$ of the form $\underline{T}$ for some $T \subseteq C$ are called *simple quantities* ([25]).

Definition 3.1. *A subalgebra $\mathcal{A}$ of the group algebra $\mathbb{Q}[C]$ is called a Schur ring or an S-ring over C if it satisfies the following axioms:*

(S1) $\mathcal{A}$ as a $\mathbb{Q}$-module has a basis consisting of simple quantities $\underline{T_0}, \ldots, \underline{T_d}$, where $T_0 = \{e\}$,

(S2) $T_i \cap T_j = \emptyset$ for $i \neq j$ and $\bigcup_{j=0}^{d} T_j = C$,

(S3) For each $i \in \{0, 1, \ldots, d\}$ there exists $i' \in \{0, 1, \ldots, d\}$ such that $T_{i'} = T_i^{(-1)}$.

It is not hard to prove that (S1) and (S2) imply that the basis $\underline{T_0}, \ldots, \underline{T_d}$ is unique. This basis is called the *standard basis* of $\mathcal{A}$. The number $d+1$ is called the *rank* of $\mathcal{A}$. The sets T_i, $0 \leq i \leq d$, are called the *basic sets* of $\mathcal{A}$ and the notation $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_d} \rangle$ will be used if $\mathcal{A}$ is an S-ring over C whose basic sets are $T_0, \ldots, T_d$. We also write $\mathsf{Basic}(\mathcal{A})$ for the set $\{T_0, \ldots, T_d\}$. Notice that if $\tilde{\mathcal{A}}$ is an S-ring which is a subring of $\mathcal{A}$ then its basic sets are some unions of basic sets of $\mathcal{A}$. There are two *trivial* S-rings, namely $\langle \underline{e}, \underline{C \setminus \{e\}} \rangle$ and $\mathbb{Q}[C]$.

Proposition 3.3. *To any group G corresponds a Schur ring $S_{\mathbb{Q}}(G)$ the basic sets of which are the orbits of the stabilizer G_1. Moreover, $S_{\mathbb{Q}}(G)$ and $V_{\mathbb{Q}}(G)$ are isomorphic as $\mathbb{Q}$-algebras.*

The proposition 3.3 is a particular case of Theorem 28.8 in [25]. It implies in particular that in order to describe the minimal idempotents of $V_{\mathbb{Q}}(G)$ it is enough to describe the ones of $S_{\mathbb{Q}}(G)$. Since however for this propose an explicit construction of the isomorphism between $S_{\mathbb{Q}}(G)$ and $V_{\mathbb{Q}}(G)$ is needed, below we give a short proof of proposition 3.3 which is based on proposition 3.2

Proof of proposition 3.3. First of all observe that since G contains c each matrix $M \in V_{\mathbb{Q}}(G)$ is necessarily a *circulant* that is each row vector of M is rotated one element to the right relative to the preceding row vector, in other words

$$M_{i,j} = M_{1,j-i+1 \bmod n}. \tag{28}$$

Define now a mapping $\psi : V_{\mathbb{Q}}(G) \to \mathbb{Q}[C]$ by the formula

$$\psi(M) := \sum_{j=1}^{n} M_{1,j} c^{j-1}$$

and show that ψ is an algebra monomorphism. Indeed, for any $M, N \in V_{\mathbb{Q}}(G)$ we have:

$$\psi(MN) = \sum_{\ell=1}^{n} (MN)_{1,\ell} c^{\ell-1} = \sum_{\ell=1}^{n} \sum_{i=1}^{n} M_{1,i} N_{i,\ell} c^{\ell-1} =$$
$$= \sum_{\ell=1}^{n} \sum_{i=1}^{n} M_{1,i} N_{1,\ell-i+1} c^{\ell-1} = \sum_{i=1}^{n} \sum_{j=1}^{n} M_{1,i} N_{1,j} c^{i+j-2} =$$
$$= \left(\sum_{i=1}^{n} M_{1,i} c^{i-1} \right) \left(\sum_{j=1}^{n} N_{1,j} c^{j-1} \right) = \psi(M)\psi(N).$$

Thus ψ is an algebra homomorphism. Furthermore, ψ is injective since any matrix $M \in V_{\mathbb{Q}}(G)$ is defined by its first row in view of (28).

Clearly, the image of $V_{\mathbb{Q}}(G)$ is a subalgebra $S_{\mathbb{Q}}(G)$ of $\mathbb{Q}[C]$. Furthermore, by construction the basis of this subalgebra consists of the orbits of the stabilizer G_1. The properties S1, S2 of $S_{\mathbb{Q}}(G)$ are obvious. Finally, since any matrix from $V_{\mathbb{Q}}(G)$ is a circulant, it follows from the third part of proposition 3.2 that $\Delta^{(-1)} = \Gamma$. $\square$

For d dividing n denote by C_d a unique subgroup of C of order d. For a Schur ring $\mathcal{A}$ denote by $D(\mathcal{A})$ a set of all divisors of n for which $\underline{C_d} \in \mathcal{A}$.

Lemma 3.2. *$d \in D(G) \iff n/d \in D(S_{\mathbb{Q}}(G))$.*

Proof. Let $d \in D(G)$. Then $C_{n/d}$ under the identification of the set $\{1, 2, \ldots, n\}$ with C corresponds to the set $X = \{1, d+1, 2d+1, \ldots, n-d+1\}$ and therefore is a block of G containing 1. It follows that $C_{n/d}$ is a union of some G_1-orbits, say $T_0, ..., T_\ell$. Hence $\underline{C_{n/d}} = \underline{T_0} + \underline{T_1} + \cdots + \underline{T_\ell}$ and therefore $\underline{C_{n/d}} \in S_{\mathbb{Q}}(G)$.

Let now $n/d \in D(S_{\mathbb{Q}}(G))$. Then $\psi^{-1}(\underline{C_{n/d}}) \in V_{\mathbb{Q}}(G)$. It follows from the definition of ψ that $\psi^{-1}(\underline{C_{n/d}})$ is a circulant matrix M such that $M_{1,i} = 1$ if

$i \in X$ and 0 otherwise. Since $M \in V_{\mathbb{Q}}(G)$ the subspace $\mathrm{Im}(M)$ is G-invariant. On the other hand, it is easy to see that $\mathrm{Im}(M) = V_d$. Therefore, $d \in D(G)$ by lemma 3.1. $\square$

3.2.2 Rational S-rings

The automorphism group of C is isomorphic to the multiplicative group $\mathbb{Z}_n^*$. To the element $m \in \mathbb{Z}_n^*$ corresponds the automorphism $g \mapsto g^m, g \in C$. Extending this action onto $\mathbb{Q}[C]$ by linearity we obtain an action of $\mathbb{Z}_n^*$ on the group algebra $\mathbb{Q}[C]$:

$$\alpha = \sum_{g \in C} \alpha_g g \quad \longrightarrow \quad \alpha^{(m)} := \sum_{g \in C} \alpha_g g^m.$$

An element $\alpha \in \mathbb{Q}[C]$ is called *rational* if $\alpha = \alpha^{(m)}$ for any $m \in \mathbb{Z}_n^*$. Note that the mappings $\alpha \mapsto \alpha^{(m)}$, $m \in \mathbb{Z}_n^*$, are automorphisms of $\mathbb{Q}[C]$. Moreover, these mappings are also automorphisms of any S-ring $\mathcal{A}$ over C (see [25], Theorem 23.9). In particular, for each $m \in \mathbb{Z}_n^*$ and $T \subseteq C$ we have

$$T \in \mathsf{Basic}(\mathcal{A}) \iff T^{(m)} \in \mathsf{Basic}(\mathcal{A}),$$

where for a subset $T \subset C$ by $T^{(m)}$ is denoted the set of m-th powers of T.

Recall that the set of all irreducible complex representations of C consists of n one-dimensional representations (characters) $\chi_0, ..., \chi_{n-1}$ where

$$\chi_i(c^j) := e^{2\pi ij/n}, \quad 0 \le i, j \le n-1.$$

We will keep the same notation for the extensions of $\chi_0, ..., \chi_{n-1}$ on $\mathbb{Q}[C]$. The rational elements of an S-rings $\mathcal{A}$ admit the following characterization.

Lemma 3.3. *An element $\alpha \in \mathbb{Q}[C]$ is rational if and only if $\chi_i(\alpha) \in \mathbb{Q}$ for any i, $0 \le i \le n-1$.*

Proof. For an element $\alpha = \sum_{i=1}^n h_i c^i$ of $\mathbb{Q}[C]$ the condition that $\chi_i(\alpha) \in \mathbb{Q}$ for any i, $0 \le i \le n-1$, is equivalent to the condition that $\chi_i(\alpha)$, $0 \le i \le n-1$, is invariant with respect to the action of the Galois group Γ of the extension $(\mathbb{Q}(e^{2\pi i/n}) : \mathbb{Q})$. The group Γ is isomorphic $\mathbb{Z}_n^*$. Namely, to the element $m \in \mathbb{Z}_n^*$ corresponds the element $\sigma_m \in \Gamma$ which transforms $e^{2\pi i/n}$ to $e^{2\pi im/n}$. We have:

$$\sigma_m(\chi_i(\alpha)) = \sigma_m(\chi_i(\sum_{j=1}^n h_j c^j)) = \sigma_m(\sum_{j=1}^n h_j e^{2\pi ij/n}) =$$

$$= \sum_{j=1}^n h_j e^{2\pi imj/n} = \chi_i(\sum_{j=1}^n h_j c^{mj}) = \chi_i(\alpha^{(m)}).$$

Therefore, for i, $0 \le i \le n-1$, and $m \in \mathbb{Z}_n^*$ the equality $\chi_i(\alpha) = \sigma_m(\chi_i(\alpha))$ is equivalent to the equality $\chi_i(\alpha) = \chi_i(\alpha^{(m)})$. Since for $\alpha, \beta \in \mathbb{Q}[C]$ the equality $\chi_i(\alpha) = \chi_i(\beta)$ holds for any i, $0 \le i \le n-1$, if and only if $\alpha = \beta$, we conclude that $\chi_i(\alpha) \in \mathbb{Q}$ for any i, $0 \le i \le n-1$, if and only if α is rational. $\square$

An S-ring $\mathcal{A}$ is called *rational* if all its elements are rational. Clearly, $\mathcal{A}$ is rational if and only if $T^{(m)} = T$ for all $T \in \mathsf{Basic}(\mathcal{A})$ and $m \in \mathbb{Z}_n^*$. Any rational S-ring is a subring of some universal rational S-ring W. To construct W observe that the orbits of the action of $\mathbb{Z}_n^*$ on C are parametrized by the divisors of n as follows: an orbit O_m, $m|n$, consists of all generators of the group C_m. It turns out that the vector space spanned by $\underline{O_m}$, $m|n$, is a rational S-ring W ([24]). Furthermore, any rational S-ring $\mathcal{A}$ is a subring of W. Indeed, since any element of the standard basis of a rational S-ring $\mathcal{A}$ is invariant with respect to the action of $\mathbb{Z}_n^*$, such an element is a union of some O_m, $m|n$. Therefore, $\mathcal{A}$ is a subring of W.

Denote by D_n the lattice of all divisors of n with respect to the operations $\wedge, \vee$. The statement below describes the rational S-rings.

Proposition 3.4. *([14]) An S-ring $\mathcal{A}$ over C is rational if and only if there exists a sublattice D of D_n with $1, n \in D$ such that $\underline{C_d}$, $d \in D$, is a basis of $\mathcal{A}$.*

Notice that the basis $\underline{C_d}$, $d \in D$, is not a standard basis of $\mathcal{A}$ in the sense of definition 3.1.

To any S-ring $\mathcal{A}$ one can associate a rational S-ring $\mathring{\mathcal{A}}$, called the *rational closure* of $\mathcal{A}$, which is constructed as follows. Introduce an equivalence relation on $\mathsf{Basic}(\mathcal{A})$ setting $S \sim T$ if there exists $m \in \mathbb{Z}_n^*$ such that $S = T^{(m)}$. For $T \in \mathsf{Basic}(\mathcal{A})$ set $\mathring{T} := \bigcup\{T^{(m)} \,|\, m \in \mathbb{Z}_n^*\}$ and denote by $\mathring{\mathcal{A}}$ the vector space spanned by $\underline{\mathring{T}}, T \in \mathsf{Basic}(\mathcal{A})$.

Proposition 3.5. *([24]) $\mathring{\mathcal{A}}$ is an S-ring consisting of all rational elements of $\mathcal{A}$.*

The proposition 3.4 allows us to describe a rational closure of an arbitrary S-ring.

Proposition 3.6. *Let $\mathcal{A}$ be an S-ring over C. Then $\underline{C_d}\,, d \in D(\mathcal{A})$, is a basis of $\mathring{\mathcal{A}}$.*

Proof. By proposition 3.4 $\mathring{\mathcal{A}}$ is spanned by vectors $\underline{C_d}$, $d \in D$, for a certain sublattice D of D_n. It remains to prove that $D = D(\mathcal{A})$. The inclusion $D \subseteq D(\mathcal{A})$ follows from the following line

$$d \in D \implies \underline{C_d} \in \mathring{\mathcal{A}} \subseteq \mathcal{A} \implies \underline{C_d} \in \mathcal{A} \implies d \in D(\mathcal{A}).$$

Vice versa, pick an arbitrary $f \in D(\mathcal{A})$. Then $\underline{C_f} \in \mathcal{A}$. Furthermore, since

$$\underline{C_f} = \sum_{t \in D_f} \underline{O_t}\ ,$$

the element $\underline{C_f}$ is rational and therefore $\underline{C_f} \in \mathring{\mathcal{A}}$. This means that $\underline{C_f}$ is a linear combination of $\underline{C_d}$, $d \in D$. Therefore, in order to prove that $\overline{C_f = C_d}$ for suitable $d \in D$ it is enough to show that the simple quantities $\underline{C_d}$, $\overline{d} \in D_n$, are linearly independent.

In order to prove the last statement observe that if

$$\sum_d l_d \underline{C_d} = 0 \tag{29}$$

and M is a maximal number d for which $l_d \neq 0$ then any element u of C which generates C_M can not be an element of C_d for $d < M$. But then u appears in the left part of equality (29) with coefficient $l_d \neq 0$. This is a contradicition and therefore $\underline{C_d}$, $d \in D_n$, are linearly independent. $\square$

3.3 Proof of theorem 3.1

It follows from

$$\underline{C_d} \cdot \underline{C_f} = (d \wedge f)\underline{C_{d\vee f}}$$

that the elements $\sigma_d := \frac{1}{d}\underline{C_d}, d \in D(\mathcal{A})$, are idempotents of the algebra $\mathcal{A}$. Nevertheless, they are not pairwise orthogonal since

$$\sigma_f \sigma_d = \sigma_d \sigma_f = \sigma_{f\vee d}. \tag{30}$$

Similarly to the definition given above for the elements of $D(G)$ say that for an S-ring $\mathcal{A}$ the element $d \in D(\mathcal{A})$ covers the element $f \in D(\mathcal{A})$ if $f \,|\, d$, $f < d$, and there is no $x \in D(\mathcal{A})$ such that $f < x < d$ and $f|x$, $x|d$.

Proposition 3.7. *An element of an S-ring $\mathcal{A}$ over C is a minimal idempotent of $\mathcal{A}$ if and only if it has the form*

$$\epsilon_d = \sigma_d \prod_{i=1}^{\ell}(1 - \sigma_{f_\ell}), \tag{31}$$

where $d \in D(\mathcal{A})$ and $f_1, ..., f_\ell$ is a complete set of elements of $D(\mathcal{A})$ covering d.

Proof. Let us show first that $\epsilon_d, d \in D(\mathcal{A})$, are pairwise orthogonal idempotenets. Since each σ_d, $d \in D_n$, is an idempotent, we have:

$$\epsilon_d^2 = \sigma_d^2 \prod_{i=1}^{\ell}(1 - \sigma_{f_\ell})^2 = \sigma_d \prod_{i=1}^{\ell}(1 - 2\sigma_{f_\ell} + \sigma_{f_\ell}^2) = \sigma_d \prod_{i=1}^{\ell}(1 - \sigma_{f_\ell}) = \epsilon_d.$$

Therefore, in order to show that ϵ_d is an idempotent we only must check that $\epsilon_d \neq 0$. In view of (30), after opening the brackets in (31) we obtain a linear combination of σ_f in which σ_d appears with the coefficient one. Since σ_d, $d \in D_n$, are linearly independent this implies that $\epsilon_d \neq 0$.

Let us check now the orthogonality. Take two distinct $m, d \in D(\mathcal{A})$, where it is assumed that $d < m$, and consider the product $\epsilon_d \epsilon_m$. Let $f_1, ..., f_\ell$ and $n_1, ..., n_k$ be complete sets of elements of $D(\mathcal{A})$ which cover d and m respectively. By (30) we have:

$$\epsilon_d \epsilon_m = \sigma_d \prod_{i=1}^{\ell}(1 - \sigma_{f_i}) \cdot \sigma_m \prod_{j=1}^{k}(1 - \sigma_{n_j}) = \sigma_d \sigma_m \prod_{i=1,j=1}^{i=\ell,j=k}(1 - \sigma_{f_i})(1 - \sigma_{n_j}) =$$

$$= \sigma_{d\vee m} \prod_{i=1,j=1}^{i=\ell,j=k} (1-\sigma_{f_i})(1-\sigma_{n_j}) \tag{32}$$

Since $d \,|\, d\vee m$ and $d < d\vee m$, there exists an element $f_i \in D(\mathcal{A})$ which covers d and divides $d\vee m$. For such an element $(1-\sigma_{f_i})\sigma_{d\vee m} = 0$ and this implies the vanishing of the right-hand side of (32).

Since the idempotents $\epsilon_d, d \in D(\mathcal{A})$, are pairwise orthogonal they are linearly independent elements of $\mathcal{A}$. Furthermore, since $\epsilon_d \in \mathring{\mathcal{A}}$ for any $d \in D(\mathcal{A})$ and

$$\dim(\mathring{\mathcal{A}}) = |D(\mathcal{A})| \tag{33}$$

by proposition 3.6, the idempotents $\epsilon_d, d \in D(\mathcal{A})$, form a basis of $\mathring{\mathcal{A}}$ which consists of pairwise orthogonal idempotents. This implies that any minimal idempotent ϵ of $\mathring{\mathcal{A}}$ coincides with some $\epsilon_d, d \in D(\mathcal{A})$. Indeed, since $\epsilon_d, d \in D(\mathcal{A})$, form a basis of $\mathring{\mathcal{A}}$ there exist numbers $a_d, d \in D(\mathcal{A})$, such that $\epsilon = \sum_{d\in D(\mathcal{A})} a_d\epsilon_d$. But, since ϵ is an idempotent, for any $d \in D(\mathcal{A})$ the coefficient a_d equals either 1 or 0. Therefore, if ϵ is minimal then $\epsilon = \epsilon_d$ for some $d \in D(\mathcal{A})$.

Finally, observe that the sets of minimal idempotents of $\mathring{\mathcal{A}}$ and $\mathcal{A}$ coincide. Indeed, if ϵ is any idempotent of $\mathcal{A}$ then $\epsilon^2 = \epsilon$ implies that $\chi_i(\epsilon) \in \{0,1\}$, $0 \le i \le n-1$. Therefore, by proposition 3.5, $\epsilon \in \mathring{\mathcal{A}}$. If now ϵ is minimal in $\mathcal{A}$ then obviously it is also minimal in $\mathring{\mathcal{A}}$. On the other hand, any minimal idempotent of $\mathring{\mathcal{A}}$ remains a minimal idempotent in $\mathcal{A}$ since all idempotents of $\mathcal{A}$ are contained in $\mathring{\mathcal{A}}$. $\square$

Proof of theorem 3.1. By proposition 3.1 any R_G-irreducible invariant subspace W of $\mathbb{Q}^n$ corresponds to a minimal idempotent $E \in V_{\mathbb{Q}}(G)$ such that $\mathsf{Im}\{E\} = W$. Furthermore, since ψ is an isomorphism between $V_{\mathbb{Q}}(G)$ and $R_{\mathbb{Q}}(G)$, the matrix $\psi(E)$ is a minimal idempotent of $R_{\mathbb{Q}}(G)$ and therefore, by proposition 3.7, $\psi(E) = \epsilon_d$ for some $d \in D(R_{\mathbb{Q}}(G))$. Thus W is R_G-irreducible invariant subspace of $\mathbb{Q}^n$ if and only if there exist $d \in D(R_{\mathbb{Q}}(G))$ such that

$$W = \mathsf{Im}\{\psi^{-1}(\epsilon_d)\} = \mathsf{Im}\left\{\psi^{-1}(\sigma_d)\Pi_{i=1}^{\ell}(I - \psi^{-1}(\sigma_{f_\ell}))\right\}. \tag{34}$$

Observe now that if two idempotent matrices A, B commute then for the matrix $C = AB = BA$ the equality

$$\mathsf{Im}\{C\} = \mathsf{Im}\{A\} \cap \mathsf{Im}\{B\}$$

holds. Indeed, it is clear that

$$\mathsf{Im}\{C\} \subseteq \mathsf{Im}\{A\} \cap \mathsf{Im}\{B\}.$$

On the other hand, if $z \in \mathsf{Im}\{A\} \cap \mathsf{Im}\{B\}$ then $z = Ax = By$ for some vectors x, y and

$$Az = A(Ax) = Ax = z, \quad Bz = B(By) = By = z. \tag{35}$$

It follows that $Cz = A(Bz) = Az = z$ and hence $z \in \mathsf{Im}\{C\}$. Since proposition 3.3 implies that $V_{\mathbb{Q}}(G)$ is commutative it follows now from (34) that

$$W = \mathsf{Im}\left\{\psi^{-1}(\sigma_d)\right\} \cap \left(\bigcap_{i=1}^{\ell} \mathsf{Im}\left\{(I - \psi^{-1}(\sigma_{f_\ell}))\right\}\right).$$

It was observed in the proof of proposition 3.2 that $\mathsf{Im}(\psi^{-1}(\sigma_d)) = V_{n/d}$. Furthermore, since the image of any idempotent matrix consists of its invariant vectors we have $\mathsf{Im}\{I - \psi^{-1}(\sigma_d)\} = \mathsf{Ker}\{\psi^{-1}(\sigma_d)\}$. On the other hand, since the matrix $\psi^{-1}(\sigma_d)$ is symmetric, $\mathsf{Ker}\{\psi^{-1}(\sigma_d)\} = \mathsf{Im}\{\psi^{-1}(\sigma_d)\}^{\perp}$. Therefore,

$$W = V_{n/d} \cap V_{n/f_1}^{\perp} \cap ... \cap V_{n/f_\ell}^{\perp}.$$

Finally, proposition 3.2 implies that $n/d \in D(G)$ and that $n/f_1, ..., n/f_\ell$ is a complete set of elements of $D(G)$ covered by n/d. Hence, $W = U_{n/d}$.

Remark. If G does not contain a full cycle then theorem 3.1 fails to be true. Indeed, consider an action of the group S_5 on two element subsets of $\{1, 2, 3, 4, 5\}$ and its permutation representation on $\mathbb{Q}^{10}$. One can verify that this action is primitive. On the other hand, the subspace $V_1^{\perp}$ is reducible since irreducible representations of S_5 have dimensions 1,4,5, or 6.

Notice also that theorem 3.1 is not true for representations over $\mathbb{C}$. In order to see this it is enough to consider any cyclic group.

4 Description of rational $Q(z)$ for which $H(t)$ is rational

4.1 Factorisations of $P(z)$ and imprimitivity sytems of G_P

Let

$$F(z) = A(B(z)) \tag{36}$$

be a factorisation of a rational function into a composition of two rational functions. Say that factoriasation (36) is equivalent to an other factoriasation $F(z) = \tilde{A}(\tilde{B}(z))$ if

$$\tilde{A}(z) = A(\sigma(z)), \quad \tilde{B}(z) = \sigma^{-1}(B(z)),$$

for some Möbius transformation $\sigma(z)$. In this subsection we briefly recall the correspondence between the equivalence classes of factorisations of a rational function $F(z)$ and imprimitivity systems of the monodromy group H of the algebraic function $F^{-1}(z)$. For this purpose first of all notice that the blocks of H containing the branch $F_1^{-1}(z)$ are in one-to-one correspondence with the subgroups of H containing the stabiliser H_1 of $F_1^{-1}(z)$. Namely, for a subgroup $\Gamma \supseteq H_1$ the corresponding block is the orbit of Γ containing $F_1^{-1}(z)$ (see [25], Theorem 7.5).

Suppose now that $F(z)$ is a rational function of degree n and let $F_j^{-1}(z)$, $j \in J$, be a block of H of cardinality d containing $F_1^{-1}(z)$. Let $\Gamma_J \supseteq H_1$ be a subgroup of H corresponding to this block. By the Galois correspondence the invariant subfield of Γ_J in the field generated by all the branches of $F^{-1}(z)$ is a subfield K_J of $\mathbb{C}(F_1^{-1}(z))$ such that

$$[\mathbb{C}(F_1^{-1}(z)) : K_J] = [\Gamma_J : H_1] = d.$$

By Lüroth's theorem any subfield of $\mathbb{C}(F_1^{-1}(z))$ has the form $\mathbb{C}(R(F_1^{-1}(z)))$ for some rational function $R(z)$. Since

$$d(R(F_1^{-1}(z))) = [K_J : \mathbb{C}(z)] = [\mathbb{C}(F_1^{-1}(z)) : \mathbb{C}(z)]/[\mathbb{C}(F_1^{-1}(z)) : K_J] = n/d$$

it follows now from lemma 2.3 that equality (36) holds for some rational functions $A(z)$, $B(z)$ such that $\deg A(z) = n/d$, $\deg B(z) = d$. Furthermore, $K_J = \mathbb{C}(A_1^{-1}(z))$, where $A_1^{-1}(z))$ is a branch of $A^{-1}(z)$. Since $A_1^{-1}(z)$ is a generator of the field K_J it follows that the function $A(z)$ is defined uniquely up to a composition with some Möbius transformation $\sigma(z)$.

In other direction, if (36) holds for some rational functions $A(z)$, $B(z)$, $\deg A(z) = n/d$, $\deg B(z) = d$, then for a suitable choice of the branch $A_1^{-1}(z)$ the field $\mathbb{C}(A_1^{-1}(z))$ is a subfield of $\mathbb{C}(F_1^{-1}(z))$ and

$$[\mathbb{C}(F_1^{-1}(z)) : \mathbb{C}(A_1^{-1}(z))] = d.$$

If now Γ is a group correponding to the field $\mathbb{C}(A_1^{-1}(z))$ under the Galois correspondence then $H_1 \subseteq \Gamma$ and the orbit of Γ containing $F_1^{-1}(z)$ is a block of cardinality d.

Notice that for the polynomial rational functions the corresponding imprimitivity systems have especially simple structure. Indeed, for a polynomial $P(z)$ of degree n its monodoromy group G_P contains a cycle of length n which is by our convention the cycle $(12...n)$. Therefore, by lemma 3.1 any system of blocks of G_P coincides with the system of residues by modulo d for some $d|n$.

This fact implies easily that if $P(z) = A(B(z))$ for some rational functions $A(z), B(z)$ then there exists a Möbius transformation $\sigma(z)$ such that $A \circ \sigma$ and $\sigma^{-1} \circ B$ are polynomials. Another corollary of this fact is that the equality

$$A(B(z)) = C(D(z)) \tag{37}$$

for some $A(z), B(z), C(z), D(z) \in \mathbb{C}(z)$ with $\deg A(z) = \deg C(z)$ implies that $A(z) = C(\sigma(z))$ for some Möbius transformation $\sigma(z)$.

4.2 Geometry of $M_{P,a,b}$

The description of G-invariant irreducible subspaces of $\mathbb{Q}^n$, given in the third section, together with proposition 2.2 imply the following important geometric property of $M_{P,a,b}$.

Set $W = V_{f_1}^{\perp} \cap ... \cap V_{f_\ell}^{\perp}$, where $f_1, ..., f_\ell$ is the set of all elements of $D(G_P)$ distinct from n, that is, in notation of theorem 3.1, $W = U_n$.

Theorem 4.1. *The subspace $M_{P,a,b}$ contains the subspace W.*

Proof. Indeed, since by construction $M_{P,a,b}$ is a G_P-invariant subspace of $\mathbb{Q}^n$, theorem 3.1 implies that either $M_{P,a,b}$ contains W or is orthogonal to W. In the last case $M_{P,a,b}$ also would be orthogonal to the complexification $W^{\mathbb{C}}$ of W. Therefore, in order to prove the proposition it is enough to find vectors $\vec{w} \in W^{\mathbb{C}}$ and $\vec{v} \in M_{P,a,b}$ such that $(\vec{v}, \vec{w}) \neq 0$.

Set
$$\vec{w}_i = (1, \varepsilon_n^i, \varepsilon_n^{2i}, \dots, \varepsilon_n^{(n-1)i}),$$
$0 \leq i \leq n-1$, where $\varepsilon_n = exp(2\pi\sqrt{-1}/n)$. It is easy to see that the vectors $\vec{w}_i$, $0 \leq i \leq n-1$, form an orthogonal basis of $\mathbb{C}^n$. Furthermore, for $d|n$ the set of the vectors $\vec{w}_j$ for which $(n/d)\,|\,j$ is a basis of $V_d^{\mathbb{C}}$. It follows that for any $f \in D(G_P)$, $f \neq n$, the vector $\vec{w}_1$ is orthogonal to $V_f^{\mathbb{C}}$ and therefore $\vec{w}_1 \in W^{\mathbb{C}}$. Set $w = w_1$.

Consider now two cases. Suppose first that $P(a) = P(b)$. In this case let $\vec{v}$ be the vector corresponding to equation (25). Then $(\vec{v}, \vec{w}) \neq 0$. Indeed, the equality $(\vec{v}, \vec{w}) = 0$ is equivalent to the equality

$$\sum_{s=1}^{d_a} \varepsilon_n^{a_s}/d_a = \sum_{s=1}^{d_b} \varepsilon_n^{b_s}/d_b$$

which in its turn is equivalent to the statement that the mass centers of the sets $V(a)$ and $V(b)$ coincide. But this contradicts to proposition 2.2 since the mass center of a system of points in $\mathbb{C}$ is inside of the convex envelope of this system and therefore the mass centers of disjointed sets must be distinct.

Similarly, if $P(a) \neq P(b)$ then $(\vec{v}, \vec{w}) \neq 0$ for at least one vector $\vec{v}$ of two vectors corresponding to equations (26). Indeed, otherwise we have:

$$\sum_{s=1}^{d_a} \varepsilon_n^{a_s}/d_a = 0, \qquad \sum_{s=1}^{d_b} \varepsilon_n^{b_s}/d_b = 0.$$

But this again contradicts the monodromy lemma since the fact that the sets $V(a)$ and $V(b)$ are almost disjointed implies that at least on of these sets is contained in an open half plane bounded by a line passing through the origin and therefore has the mass center distinct from zero. $\square$

4.3 Puiseux expansions of $Q(P^{-1}(z))$

In view of our convention about the numeration of branches of $Q(P^{-1}(z))$, for z close to infinity the branch $Q(P_i^{-1}(z))$, $1 \leq i \leq n$, is represented by a converging series

$$Q(P_i^{-1}(z)) = \sum_{k=m}^{\infty} s_k \varepsilon_n^{(i-1)k} z^{-\frac{k}{n}}, \tag{38}$$

where $z^{\frac{1}{n}}$ denotes some fixed branch of the algebraic function inverse to z^n. Therefore, any relation of the form

$$\sum_{i=1}^{n} f_i Q(P_i^{-1}(z)) = 0, \qquad f_i \in \mathbb{C}, \tag{39}$$

is equivalent to the system

$$\sum_{i=1}^{n} f_i s_k \varepsilon_n^{k(i-1)} = 0, \quad k \geq -m. \tag{40}$$

This fact together with theorem 4.1 imply the following statement (cf. [20], Theorem 4.1).

Proposition 4.1. *Let $Q(z)$ be a rational function such that the function $H(t)$ is rational. Then for any non-zero coefficient s_k, $k \geq m$, of series* (38) *there exists $f_l \in D(G_P)$, $f_l \neq n$, such that $(n/f_l) \,|\, k$.*

Proof. Indeed, if $s_k \neq 0$ then it follows from (40) that the vector $\vec{w}_k$ is orthogonal to $M^{\mathbb{C}}_{P,a,b}$. By theorem 4.1 this implies that $\vec{w}_k$ is a linear combinations of vectors $\vec{w}_j$, $(n/f_l) \,|\, j$, $f_l \in D(G_P)$. Since the vectors $\vec{w}_i$, $1 \leq i \leq n$, are linearly independent it follows that $\vec{w}_k \in V^{\mathbb{C}}_{f_l}$ for some $f_l \in D(G_P)$ and therefore $(n/f_l) \,|\, k$. $\square$

For $f \in D(G_P)$, $f \neq n$, and $Q(z) \in \mathbb{C}(z)$ set

$$\psi_{Q,f}(z) = \sum_{\substack{j \\ j \equiv 0 \bmod n/f}} s_j \left(z^{\frac{1}{n}}\right)^j,$$

where s_j, $j \geq m$, are coefficients of series (38) and define $\Psi_{Q,f}(z)$ as a complete analytic continuation of the germ defined by the series $\psi_{Q,f}(z)$ near infinity. Let $P(z) = A(B(z))$, $\deg A(z) = f$, be a factorisation of $P(z)$ corresponding to f, where it is assumed that $A(z), B(z)$ are polynomials.

Lemma 4.1. *There exists $R(z) \in \mathbb{C}(z)$ such that $\Psi_{Q,f}(z) = R(A^{-1}(z))$.*

Proof. Indeed, by a direct calculation we have:

$$\left(\frac{n}{f}\right) \psi_f(z) = Q(P_1^{-1}(z)) + Q(P_{f+1}^{-1}(z)) + Q(P_{2f+1}^{-1}(z)) + \dots + Q(P_{n-f+1}^{-1}(z)).$$

Furthermore, the collection of branches appearing in the right side of this formula is precisely a block of the imprimitivity system I of G_P corresponding to the factorisation $P(z) = A(B(z))$. It follows that the function $\psi_{Q,f}(z)$ is invariant with respect to the action of the subgroup $\Gamma \supseteq H_1$ of G_P corresponding to I. Therefore, $\psi_{Q,f}(z) \in \mathbb{C}(A_1^{-1}(z))$ for some branch $A_1^{-1}(z)$ of $A^{-1}(z)$ and hence $\Psi_{Q,f}(z) = R(A^{-1}(z))$ for some rational function $R(z)$. $\square$

4.4 Main theorem

Now we are ready to describe solutions of the following problem which generalises the polynomial moment problem: *for a given polynomial $P(z)$ and distinct complex numbers a, b to describe rational functions $Q(z)$ for which a function defined near infinity by the equality*

$$H(t) = \int_{\Gamma_{a,b}} \frac{Q(z)P'(z)dz}{P(z) - t}, \tag{41}$$

is rational.

First of all observe that if there exist polynomials $\tilde{P}(z), W(z)$ and a rational function $\tilde{Q}(z)$ such that equalities (3) and (7) hold then it follows from lemma 2.2 after the change of variable $z \rightarrow W(z)$ that $H(t)$ is a rational function. By analogy with the definition above say that in this case the solution $Q(z)$ is *reducible*.

Theorem 4.2. *The function $H(z)$ is rational if and only if $Q(z)$ can be represented as a sum of rational functions $Q_j(z)$ such that*

$$P(z) = \tilde{P}_j(W_j(z)), \quad Q_j(z) = \tilde{Q}_j(W_j(z)), \quad \textit{and} \quad W_j(a) = W_j(b) \tag{42}$$

for some polynomials $\tilde{P}_j(z), W_j(z)$ and rational functions $\tilde{Q}_j(z)$.

Proof. The proof is by induction on the number $i(P)$ of imprimitivity systems of G_P.

If $i(P) = 2$, that is if G_P has only trivial imprimitivity systems and $P(z)$ is indecomposable, then by proposition 4.1 for any non-zero coefficient s_j, $j \geq m$, of the expansion (38) we have $n|j$. It follows that all the functions $Q(P_i^{-1}(z))$, $1 \leq i \leq n$, are equal between themselves and therefore by lemma 2.3 there exists a rational function $R(z)$ such that $Q(z) = R(P(z))$.

In order to show now that $P(a) = P(b)$ observe that otherwise after the change of variable $z = P(z)$ we would obtain that $R(z)$ is orthogonal to all powers of z on the segment $[P(a), P(b)]$. Setting now in proposition 2.1

$$P(z) = z, \quad Q(z) = R(z), \quad a = P(a), \quad b = P(b)$$

we see that any of relations (26) reduces to the equality $R(z) = 0$ (of course instead of proposition 2.1 we simply can use the Weierstrass theorem). Therefore, for $i(P) = 2$ all solutions of (41) are reducible (cf. [16], Theorem 1 and [20], Theorem 5.3).

Suppose now that the theorem is proved for all $P(z)$ with $i(P) < n$ and let $Q(z)$ be a solution of (41) for a polynomial $P(z)$ of degree n. If $Q(z) = R(P(z))$ for some rational function $R(z)$ then one can show as above that $P(a) = P(b)$ and hence $Q(z)$ is reducible. Otherwise there exists a non-zero coefficient s_{j_1}, $j_1 \geq m$, of expansion (38) such that j_1 is not a multiple of n. By proposition 4.1 this implies that there exists $f_1 \in D(G_P)$, $f_1 \neq 1$, such that $(n/f_1) \,|\, j_1$. Furthermore, by lemma 4.1 if

$$P(z) = A_1(B_1(z)), \quad A_1(z), B_1(z) \in \mathbb{C}[z], \quad \deg A_1(z) = f_1,$$

is a decomposition corresponding to f_1 then $\Psi_{Q,f_1}(z) = R_1(A_1^{-1}(z))$ for some rational function $R_1(z)$.

Setting $S_1(z) = R_1(B_1(z))$ we see that $\Psi_{Q,f_1}(z) = S_1(P^{-1}(z))$ and

$$Q(P^{-1}(z)) = S_1(P^{-1}(z)) + T_1(P^{-1}(z)),$$

where $T_1(z) = Q(z) - S_1(z)$ is a rational function. Furthermore, since by construction the intersection of the supports of the Puiseux expansions near infinity of the functions $S_1(P^{-1}(z))$ and $T_1(P^{-1}(z))$ is empty, it follows from theorem 2.1 that both functions

$$H_1(t)=\int_{\Gamma_{a,b}}\frac{S_1(z)P'(z)dz}{P(z)-t}\,,\qquad F_1(t)=\int_{\Gamma_{a,b}}\frac{T_1(z)P'(z)dz}{P(z)-t}\,,$$

are rational in a neighborhood of infinity. Moreover, the construction implies that the Puiseux expansion of $F_1(t)$ contains no non-zero coefficients with indices which are multiple of $n|f_1$

If $F_1(t)\neq 0$ then there exist a non-zero coefficient $s_{j_2},\ j_2\geq m$, of the expansion (38) and $f_2\in D(G_P),\ f_2\neq f_1$, such that $(n/f_2)\,|\,j_2$. Furthermore, if

$$P(z)=A_2(B_2(z)),\quad A_2(z),B_2(z)\in\mathbb{C}[z],\quad \deg A_2=f_2,$$

then $\Psi_{T_1,f_2}(z)=R_2(A_2^{-1}(z))$ for some rational function $R_2(z)$. Setting $S_2(z)=R_2(B_2(z))$ we conclude as above that

$$T_1(P^{-1}(z))=S_2(P^{-1}(z))+T_2(P^{-1}(z)),$$

where $T_2(z)=T_1(z)-S_2(z)$ is a rational function, and that the functions

$$H_2(t)=\int_{\Gamma_{a,b}}\frac{S_2(z)P'(z)dz}{P(z)-t}\,,\qquad F_2(t)=\int_{\Gamma_{a,b}}\frac{T_2(z)P'(z)dz}{P(z)-t}\,,$$

are rational in a neighborhood of infinity. Furthermore, the Puiseux expansion of $F_2(t)$ contains no non-zero coefficients with indices which are multiple of $n|f_1$ or $n|f_2$.

It is clear that continuing in this way we will arrive after a finite number of steps to a decomposition of the function $Q(z)$ into a sum of rational functions

$$Q(z)=S_1(z)+S_2(z)+\cdots+S_r(z)$$

such that the functions

$$H_s(t)=\int_{\Gamma_{a,b}}\frac{S_s(z)P'(z)dz}{P(z)-t}\,,\qquad 1\leq s\leq r,$$

are rational in a neighborhood of infinity and

$$P_s(z)=A_s(B_s(z)),\qquad S_s(z)=R_s(B_s(z)),\qquad 1\leq s\leq r,$$

for some $R_s(z)\in\mathbb{C}(z)$, and $A_s(z),B_s(z)\in\mathbb{C}[z]$, $1\leq s\leq r$.

Since

$$H_s(t)=\int_{\Omega_{B_s(a),B_s(b)}}\frac{R_s(z)A_s'(z)dz}{A_s(z)-t},\qquad 1\leq s\leq r,$$

where $\Omega_{B_s(a),B_s(b)}=B_s(\Gamma_{a,b})$ and obviously $i(A_s)<i(P)$ it follows from the induction assumption that for each s, $1\leq s\leq r$, either $B_s(a)=B_s(b)$ or there exist rational functions $R_{s,1}(z),R_{s,2}(z),\ldots,R_{s,j_s}(z)$ such that

$$R_s(z)=R_{s,1}(z)+R_{s,2}(z)+\cdots+R_{s,j_s}(z)$$

and

$$R_{s,e}(z) = \tilde{R}_{s,e}(U_{s,e}(z)), \quad A_s(z) = \tilde{A}_{s,e}(U_{s,e}(z)), \quad U_{s,e}(B_s(a)) = U_{s,e}(B_s(b)),$$

for some $\tilde{R}_{s,e}(z) \in \mathbb{C}(z)$ and $\tilde{A}_{s,e}(z), U_{s,e}(z) \in \mathbb{C}[z]$, $1 \leq e \leq j_s$.

Setting now $Q_j(z)$ equal to the corresponding $R_{s,e}(B_s(z))$ (or just $R_s(B_s(z))$ if $B_s(a) = B_s(b)$) we see that one can represent $Q(z)$ as a sum of rational functions

$$Q(z) = Q_1(z) + Q_2(z) + \cdots + Q_t(z)$$

such that for j, $1 \leq j \leq t$,

$$P(z) = \tilde{P}_j(W_j(z)), \quad Q_j(z) = \tilde{Q}_j(W_j(z)), \quad \text{and} \quad W_j(a) = W_j(b), \tag{43}$$

where $\tilde{Q}_j(z) \in \mathbb{C}(z)$ and $\tilde{P}_j(z), W_j(z) \in \mathbb{C}[z]$ are defined as follows: $\tilde{P}_j(z)$ equals $\tilde{A}_{s,e}(z)$ or $A_s(z)$, $\tilde{Q}_j(z)$ equals $\tilde{R}_{s,e}(z)$ or $R_s(z)$, and $W_j(z)$ equals $U_{s,e}(B_s(z))$ or $B_s(z)$. $\square$

Notice that theorem 4.2 implies the theorem stated in the introduction. Indeed, as it was remarked after the proof of theorem 2.1, in the case when $Q(z)$ is a polynomial the function $H(t)$ is rational if and only if $H(t) \equiv 0$. The desired theorem follows now from lemma 2.1 taking into account that if $Q(z)$ is a polynomial then $Q_j(z)$ also are polynomials.

References

[1] M. Blinov, M. Briskin, Y. Yomdin, *Local center conditions for a polynomial Abel equation and cyclicity of its zero solution*, in "Complex analysis and dynamical systems II", Contemp. Math., AMS, Providence, RI, 2005, 65-82.

[2] M. Briskin, J.-P. Francoise, Y. Yomdin, *Une approche au probleme du centre-foyer de Poincare,* C. R. Acad. Sci., Paris, Ser. I, Math. 326, No.11, 1295-1298 (1998).

[3] M. Briskin, J.-P. Francoise, Y. Yomdin, *Center conditions, compositions of polynomials and moments on algebraic curve*, Ergodic Theory Dyn. Syst. **19**, no 5, 1201-1220 (1999).

[4] M. Briskin, J.-P. Francoise, Y. Yomdin, *Center condition II: Parametric and model center problems*, Isr. J. Math. **118**, 61-82 (2000).

[5] M. Briskin, J.-P. Francoise, Y. Yomdin, *Center condition III: Parametric and model center problems*, Isr. J. Math. **118**, 83-108 (2000).

[6] M. Briskin, J.-P. Francoise, Y. Yomdin, *Generalized moments, center-focus conditions and compositions of polynomials,* in "Operator theory, system theory and related topics", Oper. Theory Adv. Appl., **123**, 161–185 (2001).

[7] M. Briskin, N. Roytvarf, Y. Yomdin, *Center conditions at infinity for Abel differential equation*, preprint.

[8] M. Briskin, Y. Yomdin, *Tangential version of Hilbert 16th problem for the Abel equation*, Mosc. Math. J., **5**, (2005), no. 1, 23-53.

[9] C. Christopher, *Abel equations: composition conjectures and the model problem*, Bull. Lond. Math. Soc. **32**, No.3, 332-338 (2000).

[10] K. Girstmair, *Linear dependence of zeros of polynomials and construction of primitive elements*, Manuscripta Math. 39 (1982), no. 1, 81–97.

[11] K. Girstmair, *Linear relations between roots of polynomials*, Acta Arith. 89, No.1, 53-96 (1999)

[12] A. Kirillov, *Elements of the theory of representations,* Grundlehren der mathematischen Wissenschaften. 220, Springer-Verlag. (1976).

[13] S. Lando, A. Zvonkin, *Graphs on surfaces and their applications*, Encyclopaedia of Mathematical Sciences, 141. Low-Dimensional Topology, II. Springer-Verlag, Berlin, 2004.

[14] M.E. Muzychuk, *The structure of rational Schur rings over cyclic groups,* Europ. J. of Combin., 14 (1993), 479-490.

[15] F. Pakovich, *A counterexample to the "Composition Conjecture"*, Proc. AMS, 130, no. 12 (2002), 3747-3749.

[16] F. Pakovich, *On the polynomial moment problem*, Math. Research Letters **10**, (2003), 401-410.

[17] F. Pakovich, *Polynomial moment problem*, Addendum to the paper *Center Problem for Abel Equation, Compositions of Functions, and Moment Conditions* by Y. Yomdin, Mosc. Math. J., **3** (2003), no. 3, 1167-1195.

[18] F. Pakovich, *On polynomials orthogonal to all powers of a Chebyshev polynomial on a segment*, Isr. J. Math, Vol. 142 (2004), pp. 273–283.

[19] F. Pakovich, N. Roytvarf and Y. Yomdin. *Cauchy type integrals of Algebraic functions,* Isr. J. Math., Vol. 144 (2004), pp. 221-291.

[20] F. Pakovich, *On polynomials orthogonal to all powers of a given polynomial on a segment*, Bull. Sci. Math. 129 (2005), no. 9, 749–774.

[21] J. Ritt, *Prime and composite polynomials,* Trans. Amer. Math. Soc. **23**, no. 1, 51–66 (1922).

[22] N. Roytvarf, *Generalized moments, composition of polynomials and Bernstein classes*, in "Entire functions in modern analysis. B.Ya. Levin memorial volume", Isr. Math. Conf. Proc. **15**, 339-355 (2001).

[23] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and Its Applications **77**, Cambridge University Press, 2000.

[24] I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*, Sitzungsber. Preuß. Akad. Wiss., Phys.-Math. Kl. 1933, No.18/20, 598-623 (1933).

[25] H. Wielandt, *Finite permutation groups,* New York and London: Academic Press, 1964.

[26] Y. Yomdin, *Center Problem for Abel Equation, Compositions of Functions, and Moment Conditions*, Mosc. Math. J., **3** (2003), no. 3, 1167-1195.