Proceedings of the London Mathematical Society Advance Access published March 31, 2009

doi:10.1112/plms/pdp010

Solution of the polynomial moment problem

F. Pakovich and M. Muzychuk

Abstract

In this paper we give a solution of the following 'polynomial moment problem' which arose about 10 years ago in connection with Poincaré's center-focus problem: for a given polynomial $P(z)$ to describe polynomials $q(z)$ orthogonal to all powers of $P(z)$ on a segment $[a, b]$.

1. *Introduction*

In this paper we solve the following 'polynomial moment problem': *for given* $P(z) \in \mathbb{C}[z]$ *and distinct* $a, b \in \mathbb{C}$ *to describe* $q(z) \in \mathbb{C}[z]$ *such that*

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

for all $i \geqslant 0$.

The polynomial moment problem was posed in the series of papers [3–6] in connection with the center problem for the Abel differential equation

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

with polynomial coefficients $p(z), q(z)$ in the complex domain. For given $a, b \in \mathbb{C}$ the center problem for the Abel equation is to find necessary and sufficient conditions on $p(z), q(z)$ that 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 Poincaré and has been studied in many recent papers (see, for example, [1–9, 28]).

The center problem for the Abel equation is connected with the polynomial moment problem in several ways. For example, it was shown in [5] that for the parametric version

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

of (2) the 'infinitesimal' center conditions with respect to ε reduce to moment equations (1) with $P(z) = \int p(z)\,dz$. On the other hand, it was shown in [8] 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 relations between the center problem and the polynomial moment problem can be found in [8]. These results convince that a thorough description of solutions of system (1) is an important step in the understanding of the center problem for the Abel equation.

There exists a natural condition on $P(z)$ and $Q(z) = \int q(z)\,dz$, that reduces equations (1), (2) to similar equations with respect to polynomials of smaller degrees. Namely, suppose that there exist polynomials $\tilde{P}(z)$, $\tilde{Q}(z)$, $W(z)$ with $\deg W(z) > 1$ such that

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

Received 24 October 2007; revised 4 February 2009.

2000 *Mathematics Subject Classification* 30E99 (primary), 34C99, 20C05, 12F10 (secondary).

The research of the first author was supported by the ISF grant no. 979/07.

Then after the change of variable $w = W(z)$, equations (1) transform to the equations

$$\int_{W(a)}^{W(b)} \tilde{P}^i(w)\tilde{Q}'(w)\,dw = 0, \tag{4}$$

while equation (2) transforms to the equation

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

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

$$W(a) = W(b), \tag{6}$$

then the Cauchy theorem implies that the polynomial $\tilde{Q}'(w)$ is a solution of system (4) and hence the polynomial $q(z) = Q'(z)$ is a solution of system (1). Similarly, since any solution $y(z)$ of equation (2) is the pull-back

$$y(z) = \tilde{y}(W(z)) \tag{7}$$

of a solution $\tilde{y}(w)$ of equation (5), if $W(z)$ satisfies (6), then equation (2) has a center. 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), (6) hold. The main conjecture concerning the center problem for the Abel equation ('the composition conjecture for the Abel equation'), supported by the results obtained in the papers cited above, states that any center for the Abel equation is reducible (see [**8**] and the bibliography therein).

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 $P(z)$ (see [**9**]), if $P(z)$ is indecomposable (see [**19**]), and in some other special cases (see, for example, [**5**, **22**, **23**, **25**]). Nevertheless, in general the composition conjecture for the polynomial moment problem fails to be true. Namely, it was shown in [**18**] that if $P(z)$ has several 'compositional right factors' $W(z)$ such that $W(a) = W(b)$, then it may happen that the sum of reducible solutions corresponding to these factors is a non-reducible solution.

It was conjectured in [**20**] that actually *any* non-reducible solution of (1) is a sum of reducible ones. Since compositional factors $W(z)$ of a polynomial $P(z)$ can be defined explicitly, such a description of non-reducible solutions of (1) would be very helpful, especially for applications to the Abel equation (cf. [**8**]). However, until now this conjecture was verified only in a single special case (see [**21**]).

Meanwhile, another necessary and sufficient condition for a polynomial $q(z)$ to be a solution of (1) was constructed in [**22**]. Namely, it was shown in [**22**] that there exists a finite system of equations

$$\sum_{i=1}^{n} f_{s,i} Q(P_i^{-1}(z)) = 0, \quad f_{s,i} \in \mathbb{Z}, \quad 1 \leqslant s \leqslant k, \tag{8}$$

where $Q(z) = \int q(z)\,dz$ and $P_i^{-1}(z)$, $1 \leqslant i \leqslant n$, are branches of the algebraic function $P^{-1}(z)$, such that (1) holds if and only if (8) holds. Moreover, this system was constructed explicitly using a special planar tree λ_P that 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 and b on λ_P.

A finite system of equations (8) is more convenient for a study than initial infinite system of equations (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 [**22**]). In this paper we develop necessary algebraic and analytic techniques that allow us to describe solutions of (8) in the general case

and to prove that any solution of (1) is a sum of reducible ones. More precisely, our main result is as follows.

THEOREM 1.1. *A non-zero polynomial $q(z)$ is a solution of system* (1) *if and only if $Q(z) = \int q(z)\,dz$ 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. Indeed, if $P(a) = P(b)$, then for any $\tilde{Q}(z) \in \mathbb{C}[z]$ the polynomial $Q(z) = \tilde{Q}(P(z))$ is a solution of (1) since we can set $W(z) = P(z)$ in (3), (6). On the other hand, if $Q(z)$ is a solution of (1) then equalities (9) imply that $P(a) = P(b)$.

The paper is organized as follows. In Section 2 we give a detailed account of definitions and previous results related to the polynomial moment problem. In particular, starting from system (8), we introduce a linear subspace $M_{P,a,b}$ of $\mathbb{Q}^n$ generated by the vectors

$$(f_{s,\sigma(1)}, f_{s,\sigma(2)}, \dots, f_{s,\sigma(n)}), \quad \sigma \in G_P, \ \ 1 \leqslant s \leqslant k,$$

and study its basic properties.

It follows from the definition that $M_{P,a,b}$ is invariant with respect to the permutation matrix representation of the group G_P. In Section 3, written entirely in the framework of the group theory, we describe a general structure of such subspaces. More generally, we describe subspaces of $\mathbb{Q}^n$ invariant with respect to the permutation matrix representation of a permutation group G of degree n, containing a cycle of length n. Roughly speaking, we show that the structure of invariant subspaces of $\mathbb{Q}^n$ for such G depends on imprimitivity systems of G only. We believe that this result is new and interesting by itself.

Finally, in Section 4, using the description of G_P-invariant subspaces of $\mathbb{Q}^n$ and results and techniques of [**22**], we prove Theorem 1.1.

2. *Preliminaries*

In this section we collect basic definitions and results concerning the polynomial moment problem. In order to make the paper self-contained, we outline the proofs of the main statements.

2.1. *Criterion for $\hat{H}(t) \equiv 0$*

For $P(z), Q(z) \in \mathbb{C}[z]$ and a path $\Gamma_{a,b} \subset \mathbb{C}$, connecting different points a, b of $\mathbb{C}$, let $H(t) = H(P, Q, \Gamma_{a,b}, t)$ be a function defined on $\mathbb{CP}^1 \setminus P(\Gamma_{a,b})$ by the integral

$$H(t) = \int_{\Gamma_{a,b}} \frac{Q(z)P'(z)\,dz}{P(z) - t}. \tag{10}$$

Note that although integral (10) depends on $\Gamma_{a,b}$ the Cauchy theorem implies that if $\tilde{\Gamma}_{a,b} \subset \mathbb{C}$ is another path connecting a and b, then for all t close enough to infinity the equality

$$H(P, Q, \tilde{\Gamma}_{a,b}, t) = H(P, Q, \Gamma_{a,b}, t)$$

holds. Therefore the Taylor expansion of $H(t)$ at infinity and the corresponding germ $\hat{H}(t)$ do not depend on the choice of $\Gamma_{a,b}$.

After the change of variable $z \to P(z)$, integral (10) transforms to the Cauchy-type integral

$$H(t) = \int_{\gamma} \frac{g(z)dz}{z-t}, \tag{11}$$

where $\gamma = P(\Gamma_{a,b})$ and $g(z)$ is obtained by the analytic continuation along γ of a germ of the algebraic function $Q(P^{-1}(z))$. Clearly, integral representation (11) defines an analytic function in each domain of the complement of γ in $\mathbb{CP}^1$. Note that for any choice of $\Gamma_{a,b}$ the function defined in the domain containing infinity is the analytic continuation of the germ $\hat{H}(t)$.

LEMMA 2.1 [22]. *Assume that $P(z)$, $q(z) \in \mathbb{C}[z]$ and $a, b \in \mathbb{C}$, $a \neq b$, satisfy*

$$\int_{\Gamma_{a,b}} P^i(z)q(z)\,dz = 0, \quad i \geqslant 0, \tag{12}$$

and let $Q(z)$ be a polynomial defined by the equalities

$$Q(z) = \int q(z)\,dz, \quad Q(a) = 0. \tag{13}$$

Then for the germ $\hat{H}(t)$ defined near infinity by integral (10), the equality $\hat{H}(t) \equiv 0$ holds.

Proof. Indeed, for all $i \geqslant 1$, by integration by parts we have

$$\int_{\Gamma_{a,b}} P^i(z)q(z)\,dz = P^i(b)Q(b) - P^i(a)Q(a) - i\int_{\Gamma_{a,b}} P^{i-1}(z)Q(z)P'(z)\,dz. \tag{14}$$

Furthermore, $Q(a) = 0$ implies $Q(b) = 0$ in view of (12) taken for $i = 0$. Therefore, if (12) holds then all the integrals appearing in the right part of (14) vanish. On the other hand, these integrals are coefficients of the Taylor expansion of $-\hat{H}(t)$ at infinity. □

Lemma 2.1 shows that the polynomial moment problem reduces to the problem of finding conditions on $Q(z)$ under which the equality $\hat{H}(t) \equiv 0$ holds. On the other hand, we will show below (Corollary 2.5) that if $\hat{H}(t) \equiv 0$ holds for some polynomial $Q(z)$, then (12) holds for $q(z) = Q'(z)$. A condition of a general character for $\hat{H}(t)$ to vanish was given in the paper [23] in the context of the theory of Cauchy-type integrals of algebraic functions. Subsequently, in the paper [22] a construction, which permits to obtain conditions for vanishing of $\hat{H}(t)$ in a very explicit form, was proposed. Briefly, the idea of [22] is to choose the integration path $\Gamma_{a,b}$ in such a way that its image under the mapping $P(z) : \mathbb{CP}^1 \to \mathbb{CP}^1$ does not divide the Riemann sphere.

The construction of the paper [22] uses a special graph λ_P, embedded into the Riemann sphere, defined as follows (see [22]). Let S be a 'star' joining a non-critical value c of a polynomial $P(z)$ of degree n with all its *finite* critical values $c_1, c_2, \ldots, c_k$ by non-intersecting oriented arcs $\gamma_1, \gamma_2, \ldots, \gamma_k$. Define λ_P as a preimage of S under the map $P(z) : \mathbb{CP}^1 \to \mathbb{CP}^1$ (see Figure 1). More precisely, define vertices of λ_P as preimages of the points c and c_s, $1 \leqslant s \leqslant k$, and edges of λ_P as preimages of the arcs γ_s, $1 \leqslant s \leqslant k$. Furthermore, for each s, $1 \leqslant s \leqslant k$, mark vertices of λ_P that are preimages of the point c_s by the number s. Finally, define a *star* of λ_P as a subset of edges of λ_P consisting of edges adjacent to some non-marked vertex.

By construction, the restriction of $P(z)$ on $\mathbb{CP}^1 \setminus \lambda_P$ is a covering of the topological punctured disk $\mathbb{CP}^1 \setminus \{S \cup \infty\}$, and therefore $\mathbb{CP}^1 \setminus \lambda_P$ is a disjointed union of punctured disks (see, for example, [11]). Moreover, since the preimage of infinity under $P(z)$ consists of a unique point, $\mathbb{CP}^1 \setminus \lambda_P$ consists of a unique disk and hence the graph λ_P is a tree.

Set $C = \{c_1, c_2, \ldots, c_k\}$, and let $U \subset \mathbb{C}$ be a simply connected domain such that $S \setminus C \subset U$ and $U \cap C = \emptyset$. Then in U there exist n single-valued analytic branches of the algebraic function

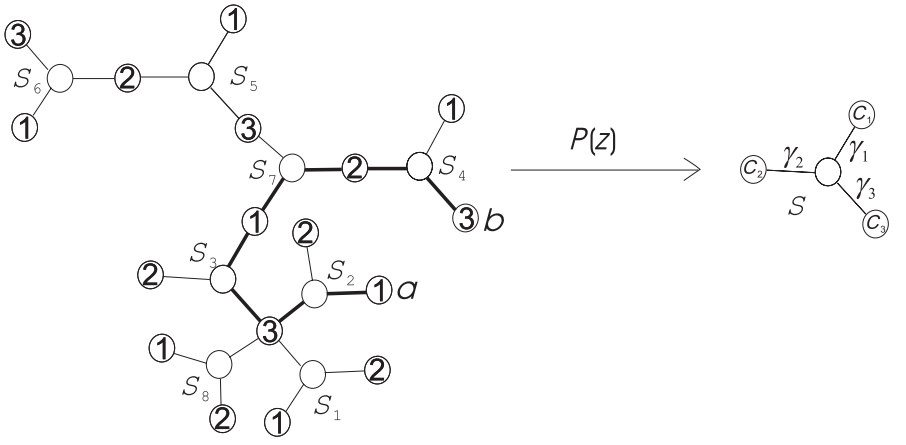

FIGURE 1.

$P^{-1}(z)$ inverse to $P(z)$. We will denote these branches by $P_i^{-1}(z)$, $1 \leqslant i \leqslant n$. The stars of λ_P may be naturally identified with branches of $P^{-1}(z)$ in U as follows: to the branch $P_i^{-1}(z)$, $1 \leqslant i \leqslant n$, corresponds the star S_i, $1 \leqslant i \leqslant n$, such that $P_i^{-1}(z)$ maps bijectively the interior of S to the interior of S_i.

Under the analytic continuation along a closed curve, the set $P_i^{-1}(z)$, $1 \leqslant i \leqslant n$, transforms to itself. This induces a homomorphism

$$\pi_1(\mathbb{CP}^1 \setminus \{C \cup \infty\}, c) \longrightarrow S_n \tag{15}$$

whose image G_P is called the monodromy group of $P(z)$. Note that if ω_∞ and ω_i, $1 \leqslant i \leqslant k$, are loops around ∞ and c_i, $1 \leqslant i \leqslant k$, respectively, such that $\omega_1\omega_2 \dots \omega_k\omega_\infty = 1$ in $\pi_1(\mathbb{CP}^1 \setminus \{C \cup \infty\}, c)$, then the elements g_i, $1 \leqslant i \leqslant k$, of G_P, which are the images of ω_i, $1 \leqslant i \leqslant k$, under homomorphism (15), generate G_P and satisfy the equality $g_1 g_2 \dots g_k g_\infty = 1$, where g_∞ is the element of G_P which is the image of ω_∞.

Keeping in mind the identification of the set of stars of λ_P with the set of branches of $P^{-1}(z)$, the permutation g_s, $1 \leqslant s \leqslant k$, can be identified with a permutation $\hat{g}_s$, $1 \leqslant s \leqslant k$, acting on the set of stars of λ_P in the following way: $\hat{g}_s$ sends the star S_i, $1 \leqslant i \leqslant n$, to the 'next' star under a counterclockwise rotation around the vertex of S_i colored by the sth color. For example, for the tree shown in Figure 1 we have: $g_1 = (1)(2)(37)(4)(5)(6)(8)$, $g_2 = (1)(2)(3)(47)(56)(8)$, $g_3 = (1238)(4)(57)(6)$. Note that since $P(z)$ is a polynomial, the permutation g_∞ is a cycle of length n. We will always assume that the numeration of branches of $P^{-1}(z)$ in U is chosen in such a way that g_∞ coincides with the cycle $(1\,2\,\dots\,n)$. Clearly, such a numeration is defined uniquely up to a choice of $P_1^{-1}(z)$.

The tree constructed above is known under the name of 'constellation' or 'cactus' and is closely related to what is called a 'dessin d'enfant' (see [**15**] for further details and other versions of this construction). The Riemann existence theorem implies that a polynomial $P(z)$ is defined by $c_1, c_2, \dots, c_k$ and λ_P up to a composition $P(z) \to P(\mu(z))$, where $\mu(z)$ is a linear function.

It follows from the definition that the points a and b are vertices of λ_P if and only if $P(a)$ and $P(b)$ are critical values of $P(z)$. For our purposes, however, it is more convenient to define the tree λ_P so that the points a, b would always be its vertices. Thus, in the case where $P(a)$ or $P(b)$ (or both of them) is not a critical value of $P(z)$, we modify the construction as follows. Define $c_1, c_2, \dots, c_k$ as the set of all finite critical values of $P(z)$ *supplemented* by $P(a)$ or $P(b)$ (or by both of them), and set as above $\lambda_P = P^{-1}\{S\}$, where S is a star connecting c with

$c_1, c_2, \dots, c_k$ (we suppose that c is chosen distinct from $P(a), P(b)$). Clearly, λ_P is still a tree and the points a, b are vertices of λ_P.

Since λ_P is connected and has no cycles, there exists a unique oriented path $\mu_{a,b} \subset \lambda_P$ joining the point a with the point b. Furthermore, it follows from the definition of λ_P that if we set $\Gamma_{a,b} = \mu_{a,b}$, then after the change of variable $z \to P(z)$ integral (10) reduces to the sum of integrals

$$H(t) = \sum_{s=1}^{k} \int_{\gamma_s} \frac{\varphi_s(z)}{z - t}\, dz, \tag{16}$$

where each $\varphi_s(z)$, $1 \leqslant s \leqslant k$, is a linear combination of the functions $Q(P_i^{-1}(z))$, $1 \leqslant i \leqslant n$, in U. Namely,

$$\varphi_s(z) = \sum_{i=1}^{n} f_{s,i} Q(P_i^{-1}(z)), \tag{17}$$

where $f_{s,i} \neq 0$ if and only if the path $\mu_{a,b}$ goes through the star S_i across its s-vertex. Furthermore, if when going along $\mu_{a,b}$ the s-vertex of S_i 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 in Figure 1 and the path $\mu_{a,b} \subset \lambda_P$ represented by the thick line, we have

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

Note that the number k in (16) coincides with the number of critical values s of $P(z)$ such that the path $\Gamma_{a,b}$ passes through at least one vertex colored by the sth color. Also note that equations (17) are linearly dependent. Indeed, for each i, $1 \leqslant i \leqslant n$, such that there exists an index s, $1 \leqslant s \leqslant k$, with $f_{s,i} \neq 0$ there exist exactly two such indices s_1, s_2, and $c_{s_1,i} = -c_{s_2,i}$. Therefore the equality

$$\sum_{s=1}^{k} \varphi_s(t) = 0$$

holds in U.

THEOREM 2.2 [**22**]. *Let $P(z), Q(z) \in \mathbb{C}[z]$ and let $a, b \in \mathbb{C}$, $a \neq b$. Then $\hat{H}(t) \equiv 0$ if and only if $\varphi_s(z) \equiv 0$ for any s, $1 \leqslant s \leqslant k$.*

Proof. Formula (16) defines the analytic continuation of $\hat{H}(t)$ to the domain $\mathbb{CP}^1 \setminus S$. In particular, $\hat{H}(t) \equiv 0$ if and only if $H(t) \equiv 0$ in $\mathbb{CP}^1 \setminus S$. On the other hand, by the well-known boundary property of Cauchy-type integrals (see, for example, [**16**]), for any s, $1 \leqslant s \leqslant k$, and any interior point z_0 of γ_s we have

$$2\pi\sqrt{-1}\,\varphi_s(z_0) = \lim_{t \to z_0}{}^{+}\, H(t) - \lim_{t \to z_0}{}^{-}\, H(t), \tag{18}$$

where the limits are taken when t approaches z_0 from the 'right' (respectively 'left') side of γ_s. Therefore, if $H(t) \equiv 0$ in $\mathbb{CP}^1 \setminus S$, then the limits in (18) equal zero and hence $\varphi_s(z) \equiv 0$ for any s, $1 \leqslant s \leqslant k$.

Finally, if

$$\varphi_s(z) \equiv 0, \quad 1 \leqslant s \leqslant k, \tag{19}$$

then it follows directly from formula (16) that $H(t) \equiv 0$. □

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

For any element $\sigma \in G_P$, the equality $\varphi_s(z) = 0$, $1 \leqslant s \leqslant k$, implies by the analytic continuation the equality

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

Therefore, replacing σ by σ^{-1} we see that Theorem 2.2 implies that $\hat{H}(t) \equiv 0$ if and only if for any $\sigma \in G_P$ and s, $1 \leqslant s \leqslant k$, the equality

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

holds.

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

$$(f_{s,\sigma(1)}, f_{s,\sigma(2)}, \dots, f_{s,\sigma(n)}), \quad 1 \leqslant s \leqslant k, \ \ \sigma \in G_P.$$

Abusing the notation, we will usually not distinguish an element of $M_{P,a,b}$ and the corresponding equation connecting branches of $Q(P^{-1}(z))$. For example, instead of using the notation

$$(0, 0, \dots, 1, \dots, 0, 0, \dots, -1, \dots, 0, 0) \tag{20}$$

for an element of $M_{P,a,b}$ we will simply use the equality

$$Q(P_{i_1}^{-1}(z)) = Q(P_{i_2}^{-1}(z)), \tag{21}$$

for corresponding $i_1 \neq i_2$, $1 \leqslant i_1, i_2 \leqslant n$.

Equality (21) is the simplest example of the equality $\varphi_s(z) = 0$, $1 \leqslant s \leqslant k$, and is equivalent to the statement that $P(z)$ and $Q(z)$ have a non-trivial 'compositional right factor' (cf. [**9**, **19**, **22**, **23**, **25**]).

LEMMA 2.3. *Let $P(z), Q(z) \in \mathbb{C}[z]$. Then the equalities*

$$P(z) = \tilde{P}(W(z)), \quad Q(z) = \tilde{Q}(W(z)) \tag{22}$$

hold for some $\tilde{P}(z), \tilde{Q}(z), W(z) \in \mathbb{C}[z]$ with $\deg W(z) > 1$ if and only if equality (21) holds for some $i_1 \neq i_2$, $1 \leqslant i_1, i_2 \leqslant n$. Furthermore, $Q(z) = \tilde{Q}(P(z))$ for some $\tilde{Q}(z) \in \mathbb{C}[z]$ if and only if all the functions $Q(P_i^{-1}(z))$, $1 \leqslant i \leqslant n$, are equal between themselves.

Proof. Let $d(Q(P^{-1}))$ be the number of *different* functions in the collection of functions $Q(P_i^{-1}(z))$, $1 \leqslant i \leqslant n$. Since any algebraic relation over $\mathbb{C}$ between $Q(p^{-1}(z))$ and z, where $p^{-1}(z)$ is a branch of the algebraic function $P^{-1}(z)$ in U, supplies an algebraic relation between $Q(z)$ and $P(z)$, and vice versa, we have

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

Therefore

$$[\mathbb{C}(z) : \mathbb{C}(Q,P)] = n/d(Q(P^{-1})). \tag{23}$$

It follows now from the Lüroth theorem that $d(Q(P^{-1})) < n$ if and only if (22) holds for some *rational* functions $\tilde{P}(z)$, $\tilde{Q}(z)$, $W(z)$ with $\deg W(z) > 1$. Furthermore, if $d(Q(P^{-1})) = 1$ then (23) implies that $Q(z) = \tilde{Q}(P(z))$ for some $\tilde{Q}(z) \in \mathbb{C}(z)$.

Observe now that, since $P(z)$, $Q(z)$ are polynomials, without loss of generality we may assume that $\mathbb{C}(Q,P) = \mathbb{C}(W)$ for some *polynomial* $W(z)$. Indeed, since $P(z)$ is a polynomial,

the equality $P(z)=U(V(z))$, where $U(z)$, $V(z)$ are rational functions, implies that $U(z)$ has a unique pole and that the preimage of this pole under $V(z)$ consists of infinity alone. This implies that $V(z)=\mu(W(z))$ for some polynomial $W(z)$ and Möbius transformation $\mu(z)$, and it is clear that the fields $\mathbb{C}(V(z))$ and $\mathbb{C}(W(z))$ coincide. Finally, if $W(z)$ is a polynomial, then obviously $\tilde{P}(z)$, $\tilde{Q}(z)$ are also polynomials. □

Since (22) implies that

$$\int_a^b P^i(z)q(z)\,dz=\int_{W(a)}^{W(b)}\tilde{P}^i(W)\tilde{Q}'(W)\,dW,$$

Lemma 2.3 shows that if the subspace $M_{P,a,b}$ contains an element of the form (21), then any solution $q(z)$ of the polynomial moment problem for $P(z)$ is either reducible or the 'pull-back' $q(z)=\tilde{q}(W(z))W'(z)$ of a solution $\tilde{q}(z)$ of the polynomial moment problem for a compositional left factor $\tilde{P}(z)$ of $P(z)$ and the points $\tilde{a}=W(a)$ and $\tilde{b}=W(b)$.

If a,b are not critical points of $P(z)$, then $M_{P,a,b}$ always contains elements of the form (21). In general case, however, a more delicate conclusion is true. Denote by $P_{a_1}^{-1}(z)$, $P_{a_2}^{-1}(z),\dots,P_{a_{d_a}}^{-1}(z)$ (respectively $P_{b_1}^{-1}(z)$, $P_{b_2}^{-1}(z),\dots,P_{b_{d_b}}^{-1}(z)$) branches of $P^{-1}(z)$ in U which map points close to $P(a)$ (respectively to $P(b)$) to points close to a (respectively b). In particular, the number d_a (respectively d_b) equals the multiplicity of the point a (respectively b) with respect to $P(z)$. The proposition below was proved in [23] and by a different method in [22]. Below we give a proof following [22].

Proposition 2.4 [22, 23]. *If $P(a)=P(b)$ then $M_{P,a,b}$ contains the element*

$$\frac{1}{d_a}\sum_{s=1}^{d_a}Q(P_{a_s}^{-1}(z))=\frac{1}{d_b}\sum_{s=1}^{d_b}Q(P_{b_s}^{-1}(z)). \tag{24}$$

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

$$\frac{1}{d_a}\sum_{s=1}^{d_a}Q(P_{a_s}^{-1}(z))=0,\quad \frac{1}{d_b}\sum_{s=1}^{d_b}Q(P_{b_s}^{-1}(z))=0. \tag{25}$$

Proof. Suppose first that $P(a)=P(b)$. Without loss of generality assume that $P(a)=P(b)=c_1$ and consider the relation

$$\varphi_1(z)=\sum_{i=1}^{n}f_{1,i}Q(P_i^{-1}(z))=0$$

corresponding to c_1. Let i, $1\leqslant i\leqslant n$, be an index such that $f_{1,i}\neq 0$ and let x be a vertex of the star S_i such that $P(x)=c_1$. It follows from the definition of $\varphi_i(z)$, $1\leqslant i\leqslant k$, that if $x\neq a,b$, then there exists an index j such that x is also a vertex of the star S_j and $f_{1,j}=-f_{1,i}$. Furthermore, we have $j=g_1^l(i)$ for some natural number l (see Figure 2). Therefore, $\varphi_1(z)$ has the form

$$\begin{aligned}\varphi_1(z)=&-Q(P_{i_a}^{-1}(z))+Q(P_{i_1}^{-1}(z))-Q(P_{g_1^{l_1}(i_1)}^{-1}(z))+\ldots+Q(P_{i_r}^{-1}(z))-Q(P_{g_1^{l_r}(i_r)}^{-1}(z))\\&+Q(P_{i_b}^{-1}(z))=0,\end{aligned}$$

where i_a (respectively i_b) is an index such that $a\subset S_{i_a}$ (respectively $b\subset S_{i_b}$), $i_1,i_2,\dots,i_r$ are some other indices, and $l_1,l_2,\dots,l_r$ are some natural numbers.

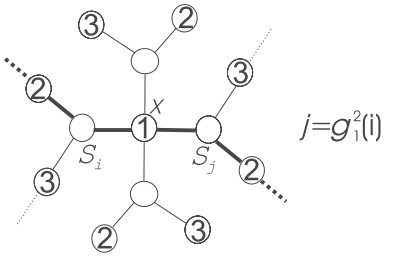

FIGURE 2.

For each $s \geqslant 0$ the equality

$$-Q(P^{-1}_{g_1^s(i_a)}(z)) + Q(P^{-1}_{g_1^s(i_1)}(z)) - Q(P^{-1}_{g_1^{l_1+s}(i_1)}(z)) + \ldots + Q(P^{-1}_{g_1^s(i_r)}(z)) - Q(P^{-1}_{g_1^{l_r+s}(i_r)}(z)) + Q(P^{-1}_{g_1^s(i_b)}(z)) = 0$$

holds by the analytic continuation of the equality $\varphi_1(z) = 0$. Now summing these equalities from $s = 0$ to $s = r - 1$, where r is the order of the element g_1 in the group G_P, and taking into account that for any i, $1 \leqslant i \leqslant n$, and any natural number l we have

$$\sum_{s=0}^{r-1} Q(P^{-1}_{g_1^s(i)}(z)) = \sum_{s=0}^{r-1} Q(P^{-1}_{g_1^{l+s}(i)}(z)),$$

we obtain equality (24).

In order to prove the proposition in the case where $P(a) \neq P(b)$, it is enough to examine in a similar way the relations $\varphi_1(z) = 0$ and $\varphi_2(z) = 0$, where $P(a) = c_1$, $P(b) = c_2$. □

COROLLARY 2.5. *Let $P(z), Q(z) \in \mathbb{C}[z]$ and let $a, b \in \mathbb{C}$, $a \neq b$. Then $\hat{H}(t) \equiv 0$ implies that (12) holds for $q(z) = Q'(z)$.*

Proof. Indeed, if $P(a) = P(b)$, then equating the limits of both parts of equality (24) as z approaches $P(a) = P(b)$, we see that $Q(a) = Q(b)$. On the other hand, if $P(a) \neq P(b)$, then it follows from equalities (25), in a similar way, that $Q(a) = Q(b) = 0$. In both cases it follows from (14) that (12) holds. □

Recall that we assume that the numeration of branches $P_i^{-1}(z)$, $1 \leqslant i \leqslant n$, in U is chosen in such a way that the permutation $g_\infty \subset G_P$ coincides with the cycle $(1\,2\,\ldots\,n)$. The proposition below describes the position of branches appearing in Proposition 2.4 with respect to this numeration. More precisely, we describe the mutual position on the unit circle of the sets

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

where $\varepsilon_n = \exp(2\pi\sqrt{-1}/n)$.

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 one of two connected components of $S^1 \setminus \{s_1, s_2\}$ contains all points from X while the other connected component of $S^1 \setminus \{s_1, s_2\}$ contains all points from Y. 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 one of the two connected components of $S^1 \setminus \{s_1, s_2\}$ contains all points from $X \setminus s_1$ while the other connected component of $S^1 \setminus \{s_1, s_2\}$ contains all points from $Y \setminus s_1$.

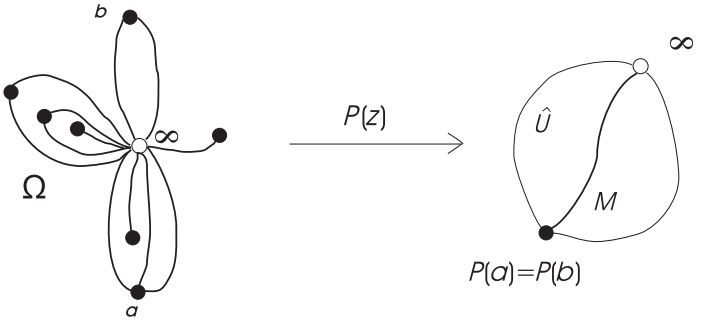

FIGURE 3.

PROPOSITION 2.6 [22]. *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.*

Proof. Consider first the case when $P(a) = P(b) = c_1$. Let $\hat{U}$ be a simply connected domain, containing no critical values of $P(z)$, such that $U \subset \hat{U}$ and $\infty \in \partial\hat{U}$. Any branch of $P^{-1}(z)$ in U can be extended analytically to $\hat{U}$, and we will assume that the numeration of branches of $P^{-1}(z)$ in $\hat{U}$ is induced by the numeration of branches of $P^{-1}(z)$ in U. Furthermore, let $M \subset \hat{U}$ be a simple curve connecting points c_1 and ∞ and let $\Omega = P^{-1}\{M\}$ be the preimage of M under the map $P(z) : \mathbb{CP}^1 \to \mathbb{CP}^1$. It is convenient to consider Ω as a bicolored graph embedded into the Riemann sphere. Namely, we define black vertices of Ω as preimages of c_1, a unique white vertex of Ω as the preimage of ∞, and edges of Ω as preimages of M (see Figure 3). The edges of Ω may be identified with branches of $P^{-1}(z)$ in $\hat{U}$ as follows: to the branch $P_i^{-1}(z)$, $1 \leqslant i \leqslant n$, corresponds the edge e_i such that $P_i^{-1}(z)$ maps bijectively the interior of M to the interior of e_i. In particular, the ordering of branches of $P^{-1}(z)$ in $\hat{U}$ induces the ordering of edges of Ω. Since the multiplicity of the vertex ∞ equals n and Ω has n edges, it follows that Ω is connected.

Let E_a (respectively E_b) be a union of edges of Ω that are adjacent to the vertex a (respectively b). It follows from the bijectivity of branches of $P^{-1}(z)$ on the interior of M that if D is a domain from the collection of domains $\mathbb{CP}^1 \setminus E_a$ such that $b \in D$, then D contains the whole set $E_b \setminus \infty$. Now the proposition follows from the observation that the cyclic ordering of edges of Ω, induced by the cyclic ordering of branches of $P^{-1}(z)$ in $\hat{U}$, coincides with the cyclic ordering of edges of Ω, induced by the orientation of $\mathbb{CP}^1$ in a neighborhood of infinity.

In the case where $P(a) \neq P(b)$ the proof is modified as follows. Take two simple curves M_1, $M_2 \subset \hat{U}$ connecting the point ∞ with the points $P(a)$ and $P(b)$ correspondingly, and consider the preimage $P^{-1}\{M_1 \cup M_2\}$ as a graph Ω embedded into the Riemann sphere. The vertices of Ω fall into three sets: the first set consists of a unique vertex which is the preimage of ∞, the second set consists of vertices which are preimages of $P(a)$, and the third set consists of vertices which are preimages of $P(b)$. Similarly, the edges of Ω fall into two sets: the first set consists of edges which are preimages of M_1 and the second set consists of edges which are preimages of M_2 (see Figure 4).

Each of two sets of edges of Ω may be identified with branches of $P^{-1}(z)$ in $\hat{U}$ as follows: to the branch $P_i^{-1}(z)$, $1 \leqslant i \leqslant n$, corresponds the edge e_i^1 from the first set (respectively the edge e_i^2 from the second set) such that $P_i^{-1}(z)$ maps bijectively the interior of M_1 (respectively of M_2) to the interior of e_i^1 (respectively of e_i^2). The ordering of branches of $P^{-1}(z)$ in $\hat{U}$ induces the ordering of edges of Ω in each of two sets. Clearly, this ordering coincides with the natural ordering induced by the orientation of $\mathbb{CP}^1$. Furthermore, it is easy to see that when

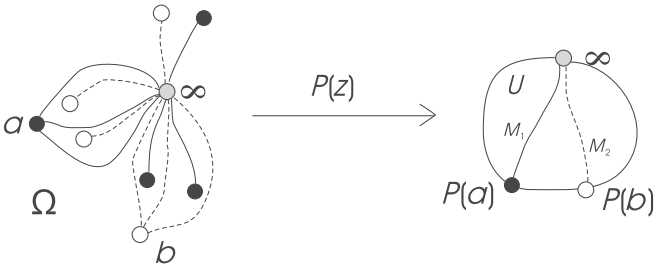

FIGURE 4.

going around infinity in the counterclockwise direction the edge e_i^1, $1 \leqslant i \leqslant n$, is followed by the edge e_i^2.

Let E_a^1 (respectively E_b^2) be a union of edges from the first (respectively the second) set Ω which are adjacent to the vertex a (respectively b). The bijectivity of branches of $P^{-1}(z)$ in the interior of M_1 and M_2 implies that if D is a domain from the collection of domains $\mathbb{CP}^1 \setminus E_a^1$ such that $b \in D$, then D contains the whole set $E_b^2 \setminus \infty$. Taking into account that for any k, $1 \leqslant i \leqslant n$, the edge e_i^1 is followed by e_i^2, this implies that $V(a)$ and $V(b)$ are disjointed or almost disjointed. □

REMARK. Since $Q(P_i^{-1}(z))$, $1 \leqslant i \leqslant n$, are branches of an algebraic function, relations (19) are examples of linear relations between roots of an algebraic equation over the field $\mathbb{C}(z)$. A general algebraic approach to such relations, over an arbitrary field, was developed in the papers [**12**, **13**]. In particular, it follows from [**13**, Theorem 1] that a necessary and sufficient condition for the existence of at least one solution $Q(z)$ of (19), such that the functions $Q(P_i^{-1}(z))$, $1 \leqslant i \leqslant n$, are distinct between themselves, is that the subspace $M_{P,a,b}$ does not contain elements of the form (20). 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. Note, however, that the method of [**13**] does not provide any information about the description or the actual finding of these solutions.

3. *Permutation matrix 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 matrix representation* of the group G_P on $\mathbb{Q}^n$. By definition, the permutation matrix representation of a transitive permutation group $H \subseteq S_n$ on $\mathbb{Q}^n$ is a homomorphism $R_H : H \to \mathrm{GL}_n(\mathbb{Q})$ which associates to $h \in H$ a permutation matrix $R_H(h) \in \mathrm{GL}_n(\mathbb{Q})$ the elements $r_{i,j}$, $1 \leqslant i, j \leqslant n$, of which satisfy $r_{i,j} = 1$ if $i = j^h$, and $r_{i,j} = 0$ otherwise. In other words,

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

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

The aim of this section is to provide a full description of the subspaces of $\mathbb{Q}^n$ invariant with respect to the permutation matrix representation of G_P. More generally, we classify all

subspaces of $\mathbb{Q}^n$ invariant with respect to the permutation matrix representation of an arbitrary group $G \subseteq S_n$ containing the cycle $(1\,2\,\ldots\,n)$. 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* of a transitive permutation group $H \subseteq S_n$ if for each $h \in H$ the set B^h is either disjoint or is equal to B (see, for example, [27]). For a block B the set $\mathcal{B} := \{B^h \,|\, h \in H\}$ 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 singletons 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 $(1, \ldots, n)$ implies easily the following 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.*

Denote by $D(G)$ the set of all divisors of n for which V_d is G-invariant. Clearly $1, n \in D(G)$. Note that $D(G)$ is a lattice with respect to the operations $\wedge, \vee$, where $d \wedge f := \gcd(d, f)$ and $d \vee f := \mathrm{lcm}(d, f)$. 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 that 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 $V_{d \wedge f}$.

We 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*

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

where $d \in D(G)$ and $f_1, \ldots, f_\ell$ is a complete set of elements of $D(G)$ covered by d. The subspaces U_d are mutually orthogonal and every R_G-invariant subspace of $\mathbb{Q}^n$ is a direct sum of some U_d as above.

The proof of this theorem splits into several steps and is given below. We start with recalling some basic facts of the representations theory that we will use later (see, for example, [14]).

First, any representation $T_H : H \to \mathrm{GL}_n(k)$ of a finite group H over a field k of characteristic not dividing $|H|$ is completely reducible; that is, k^n is a direct sum of T_H-invariant irreducible subspaces (Maschke's theorem). Furthermore, irreducible subspaces of a completely reducible representation $T_H : H \to \mathrm{GL}_n(k)$ are in one-to-one correspondence with minimal idempotents of the *centralizer ring* $V_k(T_H)$. Recall that $V_k(T_H)$ consists of all matrices $A \in M_n(k)$ that commute with every $T_H(h), h \in H$. Furthermore, a matrix E is called an idempotent if $E \neq 0$ and $E^2 = E$. Two idempotents E, F are called *orthogonal* if $EF = FE = 0$. Finally, an idempotent $E \in V_k(T_H)$ is called *minimal* if it cannot be presented as a sum of two orthogonal idempotents from $V_k(T_H)$. Under this notation the correspondence above is obtained as follows: to a minimal idempotent $E \in V_k(T_H)$ corresponds an irreducible subspace $V = \mathsf{Im}\{E\}$.

In general, the decomposition of k^n into a sum of T_H-invariant irreducible subspaces is not uniquely defined. Nevertheless, if

$$k^n = V_1^{\oplus a_1} \oplus \ldots \oplus V_r^{\oplus a_r} \tag{26}$$

is a decomposition such that V_i, $1 \leqslant i \leqslant r$, are pairwise non-isomorphic T_H-invariant irreducible subspaces of k^n, then the subspaces $V_i^{\oplus a_i}$, $1 \leqslant i \leqslant r$, are defined uniquely. They correspond to the minimal idempotents of the *center* $C(V_k(T_H))$ of the centralizer ring $V_k(T_H)$. Furthermore, $V_k(T_H)$ is commutative if and only if $a_i = 1$ for all i, $1 \leqslant i \leqslant r$. Note that if $V_k(T_H)$ is commutative and the space k^n admits a T_H-invariant scalar product, then all T_H-invariant irreducible subspaces of k^n are mutually orthogonal. Indeed, for any representation $T_H : H \to \mathrm{GL}_n(k)$, which admits an invariant scalar product, k^n can be decomposed into a sum of T_H-invariant irreducible subspaces

$$k^n = V_1 \oplus \ldots \oplus V_r \tag{27}$$

with mutually orthogonal V_i. On the other hand, if $V_k(T_H)$ is commutative then a decomposition of T_H into a sum of T_H-invariant irreducible subspaces is uniquely defined and therefore coincides with (27).

For the permutation matrix representation $R_H : H \to \mathrm{GL}_n(k)$ of a transitive permutation group $H \subseteq S_n$ instead of the notation $V_k(R_H)$ we will use simply the symbol $V_k(H)$. Below we will show (Proposition 3.5) that 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 and hence is commutative. Therefore, the above remarks imply the following statement.

PROPOSITION 3.2. *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 $\mathsf{Im}\{E\} = W$. The R_G-invariant irreducible subspaces of $\mathbb{Q}^n$ are mutually orthogonal and every R_G-invariant subspace is a direct sum of some W as above.*

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 A^{Δ}, where $A^{\Delta}_{i,j} = 1$ if there exist $h \in H$, $\delta \in \Delta$ such that $1^h = j$, $\delta^h = i$, and $A^{\Delta}_{i,j} = 0$ otherwise. In particular, for the first column of A^{Δ} the equality $A^{\Delta}_{i,1} = 1$ holds if and only if $i \in \Delta$. It turns out that the matrices A^{Δ} form a basis of $V_{\mathbb{C}}(H)$ (see, [27, Theorem 28.4]). Furthermore, since by construction the matrices A^{Δ} are contained in $M_n(\mathbb{Q})$, they form a basis of $V_{\mathbb{Q}}(H)$. We summarize the properties of A^{Δ} in the proposition below (see [27, § 28]).

PROPOSITION 3.3. *The matrices A^{Δ} satisfy the following conditions:*

(1) *A^{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 A^{Δ_1} and A^{Δ_2} do not occur in the same place; on the other hand, $\sum_{\Delta} A^{\Delta}$ is a matrix all the entries of which are 1s;*
(3) *For each orbit Δ there exists an orbit Γ such that $(A^{\Delta})^T = A^{\Gamma}$.*

Property (3) implies that for the first row of A^{Δ} the equality $A^{\Delta}_{1,j} = 1$ 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 H_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 the so-called *Schur rings* introduced by Schur in his classical paper [26] for the investigation of permutation groups containing a regular subgroup C. Since in this paper C will always be a cyclic group, in the following we will restrict our attention to this case alone (see [27] for the account of the Schur method in the general case).

The idea of the Schur approach can be described as follows. If $G \subseteq S_n$ contains the cycle $c := (1\,2\,\ldots\,n)$, 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 that transforms 1 to i. Therefore, we can consider G as a permutation group acting on its subgroup C. After such an identification we can 'multiply' elements of the set $\{1, 2, \ldots, n\}$, and this multiplication agrees with the action of G in the following sense: if $h, g \in C$ 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 elements 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* (see [27]).

Definition 3.4. 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 an $i' \in \{0, 1, \ldots, d\}$ such that $T_{i'} = T_i^{(-1)}$.

It is easy to see that the basis $\underline{T_0}, \ldots, \underline{T_d}$ satisfying (S1) and (S2) is unique. Such a basis is called the *standard basis* of $\mathcal{A}$. The number $d + 1$ is called the *rank* of $\mathcal{A}$. The sets T_i, $0 \leqslant i \leqslant d$, are called the *basic sets* of $\mathcal{A}$. Finally, the notation $\mathcal{A} = \langle \underline{T_0}, \ldots, \underline{T_d} \rangle$ is 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 $\{T_0, \ldots, T_d\}$. Note 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 3.5. *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.*

Proposition 3.5 is a particular case of [27, Theorem 28.8]. It implies in particular that in order to describe the minimal idempotents of $V_{\mathbb{Q}}(G)$ it is enough to describe those of $S_{\mathbb{Q}}(G)$. Since, however, for this purpose an explicit construction of the isomorphism between $S_{\mathbb{Q}}(G)$ and $V_{\mathbb{Q}}(G)$ is needed, we give below a short proof of Proposition 3.5 which is based on Proposition 3.3.

Proof of Proposition 3.5. 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 cyclically shifted for 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

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

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) and (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 3.3 that $\Delta^{(-1)} = \Gamma$. □

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 consisting of all divisors of n for which $\underline{C_d} \in \mathcal{A}$.

LEMMA 3.6. *The inclusion $d \in D(G)$ holds if and only if the inclusion $n/d \in D(S_{\mathbb{Q}}(G))$ holds.*

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. This implies that $C_{n/d}$ is a union of some G_1-orbits, say $T_0, \ldots, T_\ell$. Hence $\underline{C_{n/d}} = \underline{T_0} + \underline{T_1} + \ldots + \underline{T_\ell}$ 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. □

3.2.2. *Rational S-rings* The automorphism group of C is isomorphic to the multiplicative group $\mathbb{Z}_n^*$. Namely, 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 $\mathbb{Q}[C]$:

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

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 automorphisms of any S-ring $\mathcal{A}$ over C (see [**27**, 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 $T \subset C$, the set of mth powers of elements of T is denoted by $T^{(m)}$.

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

$$\chi_\ell(c^j) := e^{2\pi\sqrt{-1}\ell j/n}, \quad 0 \leqslant j, \ell \leqslant n-1.$$

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

LEMMA 3.7. *An element $\alpha \in \mathbb{Q}[C]$ is rational if and only if $\chi_l(\alpha) \in \mathbb{Q}$ for all l, $0 \leqslant l \leqslant n-1$.*

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

$$\sigma_m(\chi_\ell(\alpha)) = \sigma_m\left(\chi_\ell\left(\sum_{j=1}^{n} h_j c^j\right)\right) = \sigma_m\left(\sum_{j=1}^{n} h_j e^{2\pi\sqrt{-1}\ell j/n}\right)$$
$$= \sum_{j=1}^{n} h_j e^{2\pi\sqrt{-1}m\ell j/n} = \chi_\ell\left(\sum_{j=1}^{n} h_j c^{mj}\right) = \chi_\ell(\alpha^{(m)}).$$

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

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 (see [**26**]). 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 3.8 ([**17**]). *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 $\mathcal{A}$.*

Note that the basis $\underline{C_d}$, $d \in D$, is not a standard basis of $\mathcal{A}$ in the sense of Definition 3.4.

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 an $m \in \mathbb{Z}_n^*$ such that $S = T^{(m)}$. For $T \in \mathsf{Basic}(\mathcal{A})$ set

$$\mathring{T} := \bigcup \{T^{(m)} \mid m \in \mathbb{Z}_n^*\},$$

and denote by $\mathring{\mathcal{A}}$ a $\mathbb{Q}$-module spanned by $\underline{\mathring{T}}$, $T \in \mathsf{Basic}(\mathcal{A})$.

PROPOSITION 3.9 ([**26**]). *A Q-module $\mathring{\mathcal{A}}$ is an S-ring consisting of all rational elements of $\mathcal{A}$.*

Proposition 3.8 allows us to describe a rational closure of an arbitrary S-ring.

PROPOSITION 3.10. *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 3.8, we see that $\mathring{\mathcal{A}}$ 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

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

Conversely, choose 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 $\underline{C_f} = \underline{C_d}$ for suitable $d \in D$, it is enough to show that the simple quantities $\underline{C_d}$, $d \in D_n$, are linearly independent.

In order to prove the last statement assume that

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

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

3.3. *Proof of Theorem* 3.1

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

Set

$$\sigma_d := \frac{1}{d}\underline{C_d}, \quad d \in D(\mathcal{A}).$$

It follows from

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

that $\sigma_d, d \in D(\mathcal{A})$, are idempotents of the algebra $\mathcal{A}$. Nevertheless, they are not pairwise orthogonal.

PROPOSITION 3.11. *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*

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

where $d \in D(\mathcal{A})$ and $f_1, \ldots, f_\ell$ 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 idempotents. Since each σ_d, $d \in D_n$, is an idempotent, we have

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

Therefore, in order to show that ϵ_d is an idempotent, we must only 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 $f_1, \dots, f_\ell$ and $n_1, \dots, n_k$ be complete sets of elements of $D(\mathcal{A})$ that cover d and m, respectively. By (30) we have

$$\begin{aligned}\epsilon_d \epsilon_m &= \sigma_d \prod_{i=1}^{\ell}(1-\sigma_{f_i}) \cdot \sigma_m \prod_{j=1}^{k}(1-\sigma_{n_j}) = \sigma_d \sigma_m \prod_{i=1,j=1}^{i=\ell,j=k}(1-\sigma_{f_i})(1-\sigma_{n_j}) \\ &= \sigma_{d\vee m} \prod_{i=1,j=1}^{i=\ell,j=k}(1-\sigma_{f_i})(1-\sigma_{n_j}). \end{aligned} \tag{32}$$

Since $d \,|\, d \vee m$ and $d < d \vee m$, there exists an element $f_i \in D(\mathcal{A})$ that 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 Proposition 3.10 implies that $\epsilon_d \in \mathring{\mathcal{A}}$ for any $d \in D(\mathcal{A})$ and

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

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 $\epsilon = \sum_{d\in D(\mathcal{A})} a_d \epsilon_d$. Furthermore, 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 $\chi_i(\epsilon) \in \{0, 1\}$ for all i, $0 \leqslant i \leqslant n-1$. Therefore, by Proposition 3.9, we have $\epsilon \in \mathring{\mathcal{A}}$. Furthermore, if 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 $\mathring{\mathcal{A}}$. □

Proof of Theorem 3.1. By Proposition 3.2 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 $S_{\mathbb{Q}}(G)$, the element $\psi(E)$ is a minimal idempotent of $S_{\mathbb{Q}}(G)$ and therefore, by Proposition 3.11, $\psi(E) = \epsilon_d$ for some $d \in D(S_{\mathbb{Q}}(G))$. Thus W is R_G-irreducible invariant subspace of $\mathbb{Q}^n$ if and only if there exist $d \in D(S_{\mathbb{Q}}(G))$ such that

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

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 Lemma 3.5 implies that $V_{\mathbb{Q}}(G)$ is commutative, it follows now from (34) that

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

It was observed in the proof of Lemma 3.6 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

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

Finally, Lemma 3.6 implies that $n/d \in D(G)$ and $n/f_1, \ldots, n/f_\ell$ 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. A simple example is provided by the group S_5 acting on two element subsets of $\{1, 2, 3, 4, 5\}$. One can verify that in this way we obtain a primitive permutation group G on 10 points that yields a permutation matrix representation ρ_G of dimension 10. However, the collection of ρ_G-invariant irreducible subspaces of $\mathbb{Q}^{10}$ is distinct from the collection U_1, U_{10} since U_{10} is a direct sum of two irreducible ρ_G-invariant subspaces of dimensions 4 and 5.

Notice also that Theorem 3.1 is not true for representations over $\mathbb{C}$. In order to see this, it is enough to take as G any cyclic group.

4. *Description of $Q(z)$ satisfying $\varphi_s(t) = 0$*

4.1. *Geometry of $M_{P,a,b}$*

In notation of Section 3 set

$$W = V_{f_1}^{\perp} \cap \ldots \cap V_{f_\ell}^{\perp},$$

where $f_1, \ldots, f_\ell$ is the set of all elements of $D(G_P)$ distinct from n. Notice that since $n \in D(G_P)$ covers any other element of $D(G_P)$, the subspace W coincides with the subspace U_n from Theorem 3.1, and therefore is G_P-invariant irreducible subspace of $\mathbb{Q}^n$.

Theorem 3.1 together with Proposition 2.6 imply the following important geometric property of $M_{P,a,b}$.

Proposition 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 $\mathbb{Q}^n$, it follows from Theorem 3.1 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 $(\vec{v}, \vec{w}) \neq 0$.

In order to find such $\vec{w}$ observe that the vectors

$$\vec{w}_i = (1, \varepsilon_n^j, \varepsilon_n^{2j}, \ldots, \varepsilon_n^{(n-1)j}),$$

$1 \leqslant j \leqslant n$, where $\varepsilon_n = \exp(2\pi\sqrt{-1}/n)$, form an orthogonal basis of $\mathbb{C}^n$. Furthermore, for $d \mid n$ vectors $\vec{w}_j$ for which $(n/d) \mid j$ form a basis of $V_d^{\mathbb{C}}$. Therefore, the vector $\vec{w}_1$ is orthogonal to $V_f^{\mathbb{C}}$ for any $f \in D(G_P)$, $f \neq n$, and hence $\vec{w}_1 \in W^{\mathbb{C}}$. Set $\vec{w} = \vec{w}_1$.

Consider two cases now. Suppose first that $P(a)=P(b)$ and show that in this case, for the vector $\vec{v}\in M_{P,a,b}$ corresponding to equation (24), the inequality $(\vec{v},\vec{w})\neq 0$ holds. 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 'centers of mass' of the sets $V(a)$ and $V(b)$ coincide. However, this contradicts Proposition 2.6 since the center of mass of a system of points in $\mathbb{C}$ is inside of the convex envelope of this system and therefore the centers of mass of disjointed sets must be distinct.

Similarly, if $P(a)\neq P(b)$, then $(\vec{v},\vec{w})\neq 0$ for at least one of two vectors corresponding to equations (25). Indeed, otherwise

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

that contradicts again Proposition 2.6 since the fact that the sets $V(a)$ and $V(b)$ are almost disjointed implies that at least one of these sets is contained in an open half plane bounded by a line passing through the origin and therefore has the center of mass distinct from zero. □

4.2. *Puiseux expansions of* $Q(P^{-1}(z))$

Let $\hat{U}\subset\mathbb{C}$ be a domain as in the proof of Proposition 2.6. Then, taking into account our convention about the numeration of branches of $P^{-1}(z)$, at points of $\hat{U}$ close enough to infinity, the function $Q(P_i^{-1}(z))$, $1\leqslant i\leqslant n$, is represented by the converging series

$$Q(P_i^{-1}(z))=\sum_{k=-m}^{\infty}s_k\varepsilon_n^{(i-1)k}z^{-k/n},\tag{36}$$

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

$$\sum_{i=1}^{n}f_iQ(P_i^{-1}(z))=0,\quad f_i\in\mathbb{C},\tag{37}$$

is equivalent to the system

$$\sum_{i=1}^{n}f_is_k\varepsilon_n^{k(i-1)}=0,\quad k\geqslant -m.\tag{38}$$

In particular, in view of Theorem 2.2, the equality $\hat{H}(t)\equiv 0$ implies that for any $k\geqslant -m$ such that the coefficient s_k of series (36) is distinct from zero, the vector $\vec{w}_k$ is orthogonal to $M_{P,a,b}$. This fact together with Proposition 4.1 imply the following statement (cf. [**22**, Theorem 4.1]).

PROPOSITION 4.2. *Let $Q(z)$ be a polynomial such that $\hat{H}(t)\equiv 0$. Then for any $k\geqslant -m$ such that the coefficient s_k of series (36) is distinct from zero, there exists an $f\in D(G_P)$, $f\neq n$, such that $(n/f)\mid k$.*

Proof. Indeed, if $s_k\neq 0$, then it follows from (38) that the vector $\vec{w}_k$ is orthogonal to $M^{\mathbb{C}}_{P,a,b}$, and therefore by Proposition 4.1 is orthogonal to $W^{\mathbb{C}}$. Since the subspace $(W^{\mathbb{C}})^{\perp}$ is generated by the vectors $\vec{w}_j$, $(n/f)\mid j$, $f\in D(G_P)$, $f\neq n$, this implies that $\vec{w}_k$ is a linear combination of these vectors and hence coincides with one of them since the vectors $\vec{w}_i$, $1\leqslant i\leqslant n$, are linearly independent. Therefore, $(n/f)\mid k$ for some $f\in D(G_P)$, $f\neq n$. □

For $f \in D(G_P)$, $f \neq n$, set

$$\psi_f(z) = \sum_{\substack{k \geqslant -m \\ k \equiv 0 \bmod n/f}} s_k z^{-k/n},$$

where s_k, $k \geqslant -m$, are coefficients of series (36). Clearly, $\psi_f(z)$ is an analytic function in $\hat{U}$.

LEMMA 4.3. *For any $f \in D(G_P)$, $f \neq n$, there exists an $S_f(z) \in \mathbb{C}[z]$ such that*

$$\psi_f(z) = S_f(P_1^{-1}(z)). \tag{39}$$

Furthermore, we have

$$P(z) = A_1(B_1(z)), \quad S_f(z) = R_1(B_1(z)) \tag{40}$$

for some $A_1(z), B_1(z), R_1(z) \in \mathbb{C}[z]$ with $deg B_1(z) > 1$.

Proof. First, observe that since

$$1 + (\varepsilon_n^k)^f + (\varepsilon_n^k)^{2f} + \ldots + (\varepsilon_n^k)^{n-f}$$

equals n/f if $n \mid (fk)$, and zero otherwise, it follows from (36) that the equality

$$\left(\frac{n}{f}\right) \psi_f(z) = Q(P_1^{-1}(z)) + Q(P_{f+1}^{-1}(z)) + Q(P_{2f+1}^{-1}(z)) + \ldots + Q(P_{n-f+1}^{-1}(z)) \tag{41}$$

holds.

Let now Ω_P be a field generated by all branches of $P^{-1}(z)$ considered as elements of some fixed algebraic closure of $\mathbb{C}(z)$. Recall that the Galois group of the extension $[\Omega_P : \mathbb{C}(z)]$ is permutation equivalent to the group G_P, and, under the Galois correspondence, to the stabilizer of $P_1^{-1}(z)$ in G_P corresponds the invariant subfield $\mathbb{C}(P_1^{-1}(z))$ of Ω_P. Since $f \in D(G_P)$, the collection of branches appearing in the right part of equality (41) is a block of an imprimitivity system of G_P containing $P_1^{-1}(z)$. Therefore, equality (41) implies that the function $\psi_f(z) \in \Omega_P$ is invariant with respect to the action of the stabilizer of $P_1^{-1}(z)$ in G_P and hence is contained in the field $\mathbb{C}(P_1^{-1}(z))$. Hence, there exists a rational function $S_f(z)$ such that equality (39) holds. Furthermore, since the analytic continuation of the right side of (41) has no poles in $\mathbb{C}$ the function $S_f(z)$ is a polynomial. Finally, since branches appearing in the right part of equality (41) form a block, it is easy to see that

$$S_f(P_1^{-1}(z)) = S_f(P_{lf+1}^{-1}(z)), \quad 1 \leqslant l \leqslant n/f - 1,$$

and hence the last part of the lemma follows from Lemma 2.3. □

4.3. *Proof of Theorem 1.1*

In view of Theorem 2.2 we must essentially show that the conclusion of the theorem holds for any non zero polynomial $Q(z)$ such that $\hat{H}(t) \equiv 0$. Therefore, abusing the notation, below we will mean by a solution of the polynomial moment problem, such a polynomial $Q(z)$. The proof is by induction on the number $i(P)$ of imprimitivity systems of the group G_P. If $i(P) = 2$, that is, if G_P has only trivial imprimitivity systems, then Proposition 4.2 implies that for any non-zero coefficient s_j, $j \geqslant m$, of (36) the number k is a multiple of n. Therefore, all the functions $Q(P_i^{-1}(z))$, $1 \leqslant i \leqslant n$, are equal between themselves and hence $Q(z) = R(P(z))$ for some polynomial $R(z)$ by Lemma 2.3. Furthermore, necessarily $P(a) = P(b)$. Indeed otherwise, after the change of variable $z = P(z)$ we would obtain that the polynomial $R(z)$ is orthogonal to all powers of z on the segment $[P(a), P(b)]$. However, for

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

any of relations (25) reduces to the equality $R(z)\equiv 0$ in contradiction with the condition $Q(z)\not\equiv 0$ (of coarse instead of Proposition 2.1 we could also use the Weierstrass theorem). Therefore, if $i(P)=2$ then all solutions of the polynomial moment problem for $P(z)$ are reducible (cf. [**19**, Theorem 1; **22**, Theorem 5.3]).

Suppose now that the theorem is proved for all $P(z)$ with $i(P)<l$, and let $Q(z)$ be a non-zero solution of the polynomial moment problem for a polynomial $P(z)$ of degree n with $i(P)=l$. If $Q(z)=R(P(z))$ for some polynomial $R(z)$ then one can show as above that $P(a)=P(b)$ and $Q(z)$ is reducible. Otherwise there exists a non-zero coefficient s_{j_1}, $j_1\geqslant m$, of expansion (36) such that j_1 is not a multiple of n. By Proposition 4.2 this implies that there exists an $f_1\in D(G_P)$, $f_1\neq n$, such that $(n/f_1)\,|\,j_1$. Furthermore, by Lemma 4.3 there exists a polynomial $S_1(z)$ such that $\psi_{f_1}(z)=S_1(P_1^{-1}(z))$ and equalities

$$P(z)=A_1(B_1(z)),\quad S_1(z)=R_1(B_1(z))$$

hold for some $A_1(z),B_1(z),R_1(z)\in\mathbb{C}[z]$ with $\deg B_1(z)>1$.

Define a polynomial $T_1(z)$ by the equality $T_1(z)=Q(z)-S_1(z)$. Then for any i, $1\leqslant i\leqslant n$, we have

$$Q(P_i^{-1}(z))=S_1(P_i^{-1}(z))+T_1(P_i^{-1}(z)).$$

Since by construction the intersection of the supports of the series $S_1(P^{-1}(z))$ and $T_1(P^{-1}(z))$ is empty, if the series $Q(P_i^{-1}(z))$, $1\leqslant i\leqslant n$, satisfies some linear relation over $\mathbb{C}$ then the series $S_1(P_i^{-1}(z))$, $1\leqslant i\leqslant n$, and $T_1(P_i^{-1}(z))$, $1\leqslant i\leqslant n$, also satisfy this relation. It follows now from Theorem 2.2 that each of germs defined in a neighborhood of infinity by the integrals

$$\hat{H}_1(t)=\int_{\Gamma_{a,b}}\frac{S_1(z)P'(z)\,dz}{P(z)-t},\quad \hat{F}_1(t)=\int_{\Gamma_{a,b}}\frac{T_1(z)P'(z)\,dz}{P(z)-t},$$

vanishes or, in other words, the polynomials $S_1(z)$ and $R_1(z)$ are solutions of the polynomial moment problem for $P(z)$. Moreover, by construction the Puiseux series of $T_1(P^{-1}(z))$ contains no non-zero coefficients with indices that are multiple of n/f_1. In particular, this implies that all coefficients of $T_1(P^{-1}(z))$ whose indices are multiples of n vanish and hence $T_1(z)$ may not have the form $T_1(z)=R(P(z))$ for some $R(z)\in\mathbb{C}[z]$ unless $T_1(z)\equiv 0$.

If $T_1(t)\neq 0$, then arguing as above, we conclude that there exist $f_2\in D(G_P)$, $f_2\neq f_1$, $f_2\neq n$, and polynomials $S_2(z),T_2(z),R_2(z),A_2(z),B_2(z)\in\mathbb{C}[z]$ with $\deg B_2(z)>1$ such that the following conditions hold:

$$T_1(P^{-1}(z))=S_2(P^{-1}(z))+T_2(P^{-1}(z)),$$
$$P(z)=A_2(B_2(z)),\quad S_2(z)=R_2(B_2(z)),$$

the germs

$$\hat{H}_2(t)=\int_{\Gamma_{a,b}}\frac{S_2(z)P'(z)\,dz}{P(z)-t},\quad \hat{F}_2(t)=\int_{\Gamma_{a,b}}\frac{T_2(z)P'(z)\,dz}{P(z)-t}$$

vanish, and the Puiseux expansion of $T_2(P^{-1}(z))$ contains no non-zero coefficients whose indices are multiple of n/f_1 or n/f_2.

Since the number of divisors of n is finite, continuing in this way, after a finite number of steps we will arrive at a decomposition of the function $Q(z)$ into a sum of polynomials $S_s(z)$, $1\leqslant s\leqslant r$,

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

such that the germs

$$\hat{H}_s(t)=\int_{\Gamma_{a,b}}\frac{S_s(z)P'(z)\,dz}{P(z)-t},\quad 1\leqslant s\leqslant r,$$

vanish and

$$P(z) = A_s(B_s(z)), \quad S_s(z) = R_s(B_s(z)), \quad 1 \leqslant s \leqslant r,$$

for some $R_s(z), A_s(z), B_s(z) \in \mathbb{C}[z]$ with $\deg B_s(z) > 1$.

In order to conclude the proof it is enough to show any polynomial $S(z)$ from the collection $S_s(z)$, $1 \leqslant s \leqslant r$, is a sum of reducible solutions of the polynomial moment problem for $P(z)$. Thus, take some $S(z)$ and let $R(z), A(z), B(z)$, where $\deg B(z) > 1$, be polynomials such that

$$P(z) = A(B(z)), \quad S(z) = R(B(z)).$$

If $B(a) = B(b)$, then $S(z)$ itself is a reducible solution. Otherwise, since

$$\int_{\Gamma_{a,b}} \frac{S(z)P'(z)\,dz}{P(z) - t} = \int_{B(\Gamma_{a,b})} \frac{R(z)A'(z)\,dz}{A(z) - t},$$

we conclude that the polynomial $R(z)$ is a solution of the polynomial moment problem for the polynomial $A(z)$ (and the points $B(a)$, $B(b)$). Since the condition $\deg B(z) > 1$ implies that $i(A) < i(P)$, it follows from the induction assumption that there exist polynomials $V_1(z)$, $V_2(z), \ldots, V_j(z)$ such that

$$R(z) = V_1(z) + V_2(z) + \ldots + V_j(z)$$

and

$$V_e(z) = \tilde{V}_e(U_e(z)), \quad A(z) = \tilde{A}_e(U_e(z)), \quad U_e(B(a)) = U_e(B(b)),$$

for some $\tilde{V}_e(z), \tilde{A}_e(z), U_e(z) \in \mathbb{C}[z]$, $1 \leqslant e \leqslant j$.

Set now

$$E_e(x) = V_e(B(x)), \quad W_e(z) = U_e(B(z)), \quad 1 \leqslant e \leqslant j.$$

Then

$$S(z) = E_1(z) + E_2(z) + \ldots + E_j(z),$$

where for each e, $1 \leqslant e \leqslant j$, we have:

$$E_e(z) = \tilde{V}_e(W_e(z)), \quad P(z) = \tilde{A}_e(W_e(z)), \quad W_e(a) = W_e(b).$$

Therefore, $S(z)$ is a sum of reducible solutions.

Remark. Theorem 1.1 implies that if for a given polynomial $P(z)$ the corresponding polynomial moment problem has non-reducible solutions, then $P(z)$ has at least one 'double decomposition'

$$P = A \circ B = C \circ D$$

such that

$$B(z) \notin \mathbb{C}(D(z)), \quad D(z) \notin \mathbb{C}(B(z)).$$

Notice that this condition is quite restrictive. Namely, the results of Engstrom [10] and Ritt [24] imply that if polynomials A, B, C, D satisfy the equation

$$A \circ B = C \circ D,$$

then there exist polynomials $\hat{A}, \hat{B}, \hat{C}, \hat{D}, U, V$ such that

$$A = U \circ \hat{A}, \quad C = U \circ \hat{C}, \quad B = \hat{B} \circ V, \quad D = \hat{D} \circ V, \quad \hat{A} \circ \hat{B} = \hat{C} \circ \hat{D},$$

and up to a possible replacement of $\hat{A}$ by $\hat{C}$ and $\hat{B}$ by $\hat{D}$ either

$$\hat{A} \circ \hat{B} \sim z^n \circ z^r R(z^n), \quad \hat{C} \circ \hat{D} \sim z^r R^n(z) \circ z^n,$$

where $R(z)$ is a polynomial, $r \geqslant 0$, $n \geqslant 1$, and $\mathrm{GCD}(n, r) = 1$, or

$$\hat{A} \circ \hat{B} \sim T_n \circ T_m, \quad \hat{C} \circ \hat{D} \sim T_m \circ T_n,$$

where $T_n(z), T_m(z)$ are the corresponding Chebyshev polynomials, $n, m \geqslant 1$, and $\mathrm{GCD}(n, m) = 1$.

Notice however that a polynomial $P(z)$ may have more than *one* double decomposition satisfying the condition above. Indeed, for example, for any distinct prime divisors p_1, p_2 of a number n we have

$$T_n(z) = T_{n/p_1}(T_{p_1}(z)) = T_{n/p_2}(T_{p_2}(z))$$

and

$$T_{p_1}(z) \notin \mathbb{C}(T_{p_2}(z)), \quad T_{p_2}(z) \notin \mathbb{C}(T_{p_1}(z)).$$

It would be interesting to investigate what conditions should be imposed on the collection $P(z), a, b$ in order to conclude that any solution of the polynomial moment problem for $P(z)$ can be represented as a sum of *at most* r reducible solutions, where $r \geqslant 1$ is a fixed number.

Acknowledgements. The authors would like to thank C. Christopher, J. P. Françoise, L. Gavrilov, G. Jones, M. Klin, Y. Yomdin, and W. Zhao for discussions of different questions related to the subject of this paper. The authors are also grateful to the anonymous referee for valuable comments and suggestions.

References

1. M. Blinov, M. Briskin and Y. Yomdin, 'Local center conditions for a polynomial Abel equation and cyclicity of its zero solution', *Complex analysis and dynamical systems II*, Contemporary Mathematics 382 (American Mathematical Society, Providence, RI, 2005) 65–82.
2. M. Briskin and Y. Yomdin, 'Tangential version of Hilbert 16th problem for the Abel equation', *Mosc. Math. J.* 5 (2005) 23–53.
3. M. Briskin, J.-P. Françoise and Y. Yomdin, 'Une approche au probleme du centre-foyer de Poincaré', *C. R. Math. Acad. Sci. Paris Ser. I* 326 (1998) 1295–1298.
4. M. Briskin, J.-P. Françoise and Y. Yomdin, 'Center conditions, compositions of polynomials and moments on algebraic curve', *Ergodic Theory Dynam. Systems.* 19 (1999) 1201–1220.
5. M. Briskin, J.-P. Françoise and Y. Yomdin, 'Center condition II: parametric and model center problems', *Israel J. Math.* 118 (2000) 61–82.
6. M. Briskin, J.-P. Françoise and Y. Yomdin, 'Center condition III: parametric and model center problems', *Israel J. Math.* 118 (2000) 83–108.
7. M. Briskin, J.-P. Françoise and Y. Yomdin, 'Generalized moments, center-focus conditions and compositions of polynomials', *Operator theory, system theory and related topics*, Operator Theory: Advances and Applications 123 (Birkhäuser, Basel, 2001) 161–185.
8. M. Briskin, N. Roytvarf and Y. Yomdin, 'Center conditions at infinity for Abel differential equation', *Ann. of Math.*, to appear.
9. C. Christopher, 'Abel equations: composition conjectures and the model problem', *Bull. London Math. Soc.* 32 (2000) 332–338.
10. H. Engstrom, 'Polynomial substitutions', *Amer. J. Math.* 63 (1941) 249–255.
11. O. Forster, *Lectures on Riemann surfaces*, Graduate Texts in Mathematics 81 (Springer, New York, 1991).
12. K. Girstmair, 'Linear dependence of zeros of polynomials and construction of primitive elements', *Manuscripta Math.* 39 (1982) 81–97.
13. K. Girstmair, 'Linear relations between roots of polynomials', *Acta Arith.* 89 (1999) 53–96.
14. A. Kirillov, *Elements of the theory of representations*, Grundlehren der Mathematischen Wissenschaften 220 (Springer, Berlin, 1976).
15. S. Lando and A. Zvonkin, *Graphs on surfaces and their applications*, Low-Dimensional Topology II, Encyclopaedia of Mathematical Sciences 141 (Springer, Berlin, 2004).
16. N. Muskhelishvili, *Singular Integral Equations*, (Noordhoff, Groningen, 1953).
17. M. E. Muzychuk, 'The structure of rational Schur rings over cyclic groups', *European J. Combin.* 14 (1993) 479–490.

18. F. Pakovich, 'A counterexample to the "Composition Conjecture"', *Proc. Amer. Math. Soc.* 130 (2002) 3747–3749.
19. F. Pakovich, 'On the polynomial moment problem', *Math. Res. Lett.* 10 (2003) 401–410.
20. 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) 1167–1195.
21. F. Pakovich, 'On polynomials orthogonal to all powers of a Chebyshev polynomial on a segment', *Israel J. Math.* 142 (2004) 273–283.
22. F. Pakovich, 'On polynomials orthogonal to all powers of a given polynomial on a segment', *Bull. Sci. Math.* 129 (2005) 749–774.
23. F. Pakovich, N. Roytvarf and Y. Yomdin, 'Cauchy type integrals of Algebraic functions', *Israel J. Math.* 144 (2004) 221–291.
24. J. Ritt, 'Prime and composite polynomials', *Trans. Amer. Math. Soc.* 23 (1922) 51–66.
25. N. Roytvarf, 'Generalized moments, composition of polynomials and Bernstein classes', *Entire functions in modern analysis. B.Ya. Levin memorial volume*, Israel Mathematical Conference Proceedings 15 (Bar-Ilan Univ., Ramat Gan, 2001) 339–355.
26. I. Schur, 'Zur Theorie der einfach transitiven Permutationsgruppen', *Sitzungsber. Preuß. Akad. Wiss., Phys.-Math. Kl.* 1933 (1933) 598–623.
27. H. Wielandt, *Finite permutation groups* Academic Press, New York, 1964).
28. Y. Yomdin, 'Center problem for Abel equation, compositions of functions, and moment conditions,, *Mosc. Math. J.* 3 (2003) 1167–1195.

F. Pakovich
Department of Mathematics
Ben Gurion University
POB 653
Beer Sheva 84105
Israel

pakovich@math.bgu.ac.il

M. Muzychuk
Department of Mathematics
Netanya Academic College
Kibbutz Galuyot St. 16
Netanya 42365
Israel

muzy@netanya.ac.il