Записки научных
семинаров ПОМИ
Том 272, 2000 г.

Nikolai Gordeev

THE HILBERT-POINCARE SERIES FOR SOME ALGEBRAS OF INVARIANTS OF CYCLIC GROUPS

Abstract. Let ρ be a linear representation of a finite group over a field of characteristic 0. Further, let R_ρ be the corresponding algebra of invariants and let $P_\rho(t)$ be its Hilbert-Poincare series. Then the series $P_\rho(t)$ presents a rational function $\Psi(t)/\Theta(t)$. If R_ρ is a complete intersection then $\Psi(t)$ is a product of cyclotomic polynomials. Here we prove the inverse statement for the case when ρ is "almost regular" (in particular, regular) representation of a cyclic group. It gives the answer to a question of R. Stanley in this very particular case.

1. Introduction.

Let G be a finite group and let $\rho : G \to GL(V)$ be its linear representation in a finite dimensional vector space V over an algebraically closed field K of characteristic zero. Then the group $\rho(G)$ acts naturally on the symmetric algebra $S = S(V)$. Let $R_\rho = S^{\rho(G)}$ be the corresponding algebra of invariants:

$$R_\rho = \{s \in S \mid \rho(\sigma)s = s \text{ for every } \sigma \in G\}.$$

Then R_ρ is a graded algebra $= \sum_{n=0}^{\infty} R_{\rho,n}$ where $R_{\rho,n}$ is the homogeneous component of the degree n. The Hilbert–Poincare series of R_ρ (see, [2, 3])

$$P_\rho(t) = \sum_{n=0}^{\infty} (\dim R_{\rho,n}) t^n$$

defines a rational function $\Psi(t)/\Theta(t)$ and in the sequel we identify $P_\rho(t)$ and the function $\Psi(t)/\Theta(t)$. We can take different presentations of the function $P_\rho(t)$ in the form $\Psi(t)/\Theta(t)$. In particular, we can take Ψ and Θ such that $\Psi(t) \in \mathbb{Z}[t]$, $\Theta(t) = \prod_j (1 - t^{m_j})$ (see, [2, 3]). In the cases when R_ρ is a **complete intersection** the numerator $\Psi(t)$ of $P_\rho(t)$ can also be written in the form $\prod_i (1 - t^{e_i})$. Note, this statement is true for

The author is supported by SFB 343 "Diskrete Strukturen in der Mathematik" and INTAS-93-2618-Ext.

every graded complete intersection but not necessary for an algebra of invariants. R. Stanley formulated a question in [2]: under what additional conditions the inverse statement holds, i.e., if the numerator of a Cohen–Macaulay graded algebra is of the form $\prod_i (1-t^{e_i})/\prod_j (1-t^{m_j})$ for some $\{e_i\}$, $\{m_j\} \subset N$ then this algebra is a complete intersection. He pointed out two special cases when it is true and gave an example when it is false. It seems it would be reasonable to look at a naturally defined class of graded algebras, say, for algebras of invariants from the point of view of the Stanley's question. However, it is a difficult problem even for the case when G is a cyclic group. Here we give an affirmative answer to Stanley's question in the cases when G is a cyclic group and ρ is close to the regular representation.

Let $\rho : G = \langle \sigma \rangle \to GL(V)$ be a representation of a cyclic group of the order n. Further, let $d \mid n$ and let ε_d be a fixed primitive d-th root of unity. For $g \in G$ we put

$$m_d(g) = \text{multiplicity of the eigenvalue } \varepsilon_d \text{ of the operator } \rho(g).$$

By m_d we denote $\max\{m_d(g) \mid g \in G\}$.

Definition. *We say that a representation ρ is* **almost regular** *if:*

(1) $m_n(\sigma) \geq 1$;

(2) *ρ is $\operatorname{Aut} G$-invariant (i.e., $\rho(f(\sigma)) = \rho(\sigma)$ for every $f \in \operatorname{Aut} G$);*

(3) *for every divisor d of n the equality $m_d(g) = m_d$ holds if and only if the order of g is equal to d.*

Example 1. Let ρ be the regular representation. Then ρ is almost regular. Indeed, conditions (1) and (2) obviously hold. Further, let $g = \sigma^\ell$ where $\ell \mid n$. Then the restriction of ρ on the group $\langle g \rangle$ is the sum of ℓ copies of regular representation of $\langle g \rangle$. Hence $m_d(g) = 0$ if d is not a divisor of n/ℓ and $m_d(g) = \ell$ if $d \mid (n/\ell)$. Thus the maximum of the function $m_d(g)$ is equal to n/d and it is reached only on elements of the order d.

Example 2. Let ρ be a representation satisfying conditions (1) and (2). Further,

$$V = \sum_{d \mid n} V_d$$

where V_d is a vector space generated by eigenvectors of $\rho(\sigma)$ with eigenvalues which are primitive d-th roots of unity. Suppose the following condition holds:

(3′) $\dim V_{d_1} < \dim V_{d_2}$ for every divisors $d_1 \neq d_2$ of n

such that $1 \neq d_1 \mid d_2$.

We show that ρ is almost regular. Let $n = dk\ell$ for some $d, k, \ell,\ d \neq 1,\ k \neq 1$;and let $g = \sigma^\ell$.

Put

$$D_{d,\ell} = \{\, a \mid n \ \mid\ \varepsilon_a^\ell \text{ is a primitive } d-\text{th root of unity}\}$$

(here ε_a is a primitive a-th root of unity). Since ρ is Aut G-invariant we get

$$m_d(g) = \sum_{a \in D_{d,\ell}} (\dim V_a)/\varphi(d).$$

If $a \in D_{d,\ell}$ then $\varepsilon_{ak}^{\ell k}$ is a primitive d-th root unity. Using $(3')$ we obtain

$$m_d(g^k) \geq \sum_{a \in D_{d,\ell}} (\dim V_{ak})/\varphi(d) \ >\ m_d(g).$$

Thus the function $m_d(g)$ reaches its maximum only on elements of order d.

Example 3. Let ρ be a representation satisfying condition (1) and (2) and let

$$V = V_n + V_1,$$

i.e., V is the sum of $V_1 = V^{\rho(G)}$ and the vector space V_n generated by eigenvectors of $\rho(\sigma)$ with eigenvalues which are primitive n-th roots of unity. Then $m_d(g) \neq 0$ if and only if the element g has the order d. Thus ρ is almost regular.

The main result of this paper is the following theorem.

Theorem 1. *Let ρ be an almost regular representation of a cyclic group of the order n. Let $P_\rho(t) = \Psi(t)/\Theta(t)$ be the corresponding Hilbert–Poincare series. Assume $\Psi(t)$ is a product of cyclotomic polynomials. Then either $n = 2$, $\dim V/V^{\rho(G)} = 1$ and R_ρ is a polynomial algebra or $n = 2, 3, 4, 6$, $\dim V/V^{\rho(G)} = 2$ and R_ρ is a hypersurface.*

Remark 1. If the numerator of $P_\rho(t)$ (in some presentation) is a product of cyclotomic polynomials then multiplying $\Psi(t)$ and $\Theta(t)$ for some appropriate cyclotomic polynomials we can obtain the form

$$P_\rho(t) = \prod_i (1 - t^{e_i}) / \prod_j (1 - t^{m_j})$$

for some e_i, m_j. Thus, we obtain the affirmative answer for the Stanley's question in this very particular case.

In the case when $n = p$ is a prime we obtain a stronger assertion.

Theorem 2. *Let $\rho : G = \langle\sigma\rangle \to GL(V)$ be a faithful representation of a cyclic group of a prime order p. Assume $\rho(f(\sigma)) = \rho(\sigma)$ for some $f \in \operatorname{Aut} G$, $f \neq 1$, and the numerator $\Psi(t)$ of the Hilbert–Poincare series $P_\rho(t)$ is a product of cyclotomic polynomials. Then $f(\sigma) = \sigma^{-1}$, $\dim V/V^{\rho(G)} = 2$ and the algebra R_ρ is a hypersurface.*

We prove both results using the approach developed in [1] for the classification of finite groups whose algebra of invariants is a complete intersection. This method is based on arithmetical properties of algebraic numbers $\Psi(\varepsilon)$ where ε is a root of Θ.

2. Arithmetical characteristics of cyclotomic polynomials.

2.1. Let p be a prime and let α be an algebraic integer (i.e., α is a root of a polynomial $x^n + a_1x^{n-1} + \cdots + a_n$ where $a_i \in Z$). Further, let $(\alpha), (p)$ be the principal divisor of the field $Q(\alpha)$ corresponding to α. Put

$$v_p(\alpha) = \max\{r \in Q^+ \mid (p)^r \mid (\alpha)\}.$$

Assume $Q(\alpha)/Q$ is a normal extension. Then

$$(p) = P_1^e P_2^e \dots P_s^e, \quad (\alpha) = P_1^{m_1} P_2^{m_2} \dots P_s^{m_s} D$$

for some prime divisors $P_1, \dots, P_s$ of $Q(\alpha)$ and some divisor D of $Q(\alpha)$ such that $(P_i, D) = 1$ for every i (here $e, m_i \in Z$, $e > 0$, $m_i \geqslant 0$). In this case $v_p(\alpha) = m_{i_0}/e$ where $m_{i_0} = \min\{m_i\}$. Note, that if L/Q is any normal extension which contains the normal extension $Q(\alpha)/Q$ then $v_p(\alpha) = v_{p,L}(\alpha)$ where

$$v_{p,L}(\alpha) = \max\{r \in Q^+ \mid (p)_L^r \mid (\alpha)_L\}$$

and $(p)_L$, $(\alpha)_L$ are the corresponding principal divisors of L. Thus, if $Q(\alpha) \subset L$ and L/Q, $Q(\alpha)/Q$ are normal we can replace $v_{p,L}(\alpha)$ for $v_p(\alpha)$. Below we consider values $v_p(\Psi_m(\varepsilon_n))$ where Ψ_m is the m-cyclotomic polynomial and ε_n is a primitive n-th root of unity (for some m, n). We can calculate such values considering $\Psi_m(\varepsilon_n)$ as an element of $L = Q(\varepsilon_n, \varepsilon_m)$.

2.2. Let $n = p^r n_1 \neq m = p^s m_1$, where $(n_1, p) = (m_1, p) = 1$. Using the identity $n = \prod_{1 \leqslant k \leqslant n-1}(1 - \varepsilon_n^k)$ it is easy to get the following equalities:

$$v_p(\Psi_m(\varepsilon_n)) = \begin{cases} 0 & \text{if } n_1 \neq m_1, \\ 1 & \text{if } n_1 = m_1,\ s > r \\ \dfrac{\varphi(p^s)}{\varphi(p^r)} & \text{if } n_1 = m_1,\ s < r. \end{cases} \tag{1}$$

where φ is the Euler function (see [1], Lemma 5.)

2.3. Assume

$$\Psi(t) = \prod_{m_i \in M} \Psi_{m_i}(t), \tag{2}$$

where $\Psi_{m_i}(t)$ is the m_i-cyclotomic polynomial and $M = \{m_1, \dots, m_k\}$ is a finite sequence of natural numbers (possibly $m_i = m_j$ for $i \neq j$).

Let p be a prime and let $d = p^a d_1$ where $(p, d_1) = 1$ (possibly $a = 0$). Put

$$M_{p,d} = \{m_i \in M \mid m_i = p^s d_1,\ s \geq 0\},\ \ \Psi_{p,d} = \prod_{m_i \in M_{p,d}} \Psi_{m_i}. \tag{3}$$

The following statement is a variation of Lemmas 6 and 7 of [1].

Proposition 1. *Suppose* $\Psi(\varepsilon_n) \neq 0$ *for every* $n = p^b d_1,\ 0 \leq b \leqslant a + a_0$ *where* $a_0 \in Z,\ a_0 \geqslant 0$. *Then for every such* n

$$v_p(\Psi(\varepsilon_n)) = v_p(\Psi(\varepsilon_d))$$

and

$$\deg \Psi_{p,d} \geqslant v_p(\Psi(\varepsilon_d)) \cdot \varphi(d) \frac{\varphi(p^{a+a_0+1})}{\varphi(p^a)}.$$

Moreover, if $e = v_p(\Psi(\varepsilon_d))$ *and* P *is a prime divisor of* p *in* $Q(\varepsilon_d)$. *Then*

$$0 \not\equiv \Psi(\varepsilon_n)/p^e \equiv \Psi(\varepsilon_d)/p^e \ (mod\, P).$$

Remark 2. We do not use the last congruence below. However, this congruence could be useful if we consider Hilbert–Poincare series for different types of linear groups; (see [1]).

Proof. Let $m_i \in M_{p,d}$. Then $m_i = p^s d_1$ for some $s \geq 0$. Since $\Psi(\varepsilon_n) \neq 0$ for every $n = p^b d_1,\ b \leqslant a + a_0$, we have $\Psi_{m_i}(\varepsilon_n) \neq 0$ for every $n = p^b d_1,\ b \leqslant a + a_0$, and, therefore, $s > a + a_0$. We obtain from (1)

$$v_p(\Psi_{m_i}(\varepsilon_n)) = v_p(\Psi_{m_i}(\varepsilon_d)) = 1 \tag{4}$$

for every $n = p^b d_1,\ b \leqslant a + a_0$. If $m_i \notin M_{p,d}$ then we get again from (1)

$$v_p(\Psi_{m_i}(\varepsilon_n)) = v_p(\Psi_{m_i}(\varepsilon_d)) = 0. \tag{5}$$

The equality of the proposition follows now from (2), (4), and (5).

From (1), (3), and (4) we obtain

$$\deg \Psi_{p,d} = \sum_{m_i \in M_{p,d}} \varphi(m_i) \geqslant |M_{p,d}| \min\{\varphi(m_i) | \, m_i \in M_{p,d}\} =$$

$$= v_p(\Psi(\varepsilon_d)) \cdot \min\{\varphi(m_i) |\, m_i \in M_{p,d}\} \geqslant$$

$$\geqslant v_p(\Psi(\varepsilon_d))\varphi(p^{a+a_0+1}d_1) = v_p(\Psi(\varepsilon_d))\varphi(d)\frac{\varphi(p^{a+a_0+1})}{\varphi(p^a)}.$$

Now we prove the congruence. If $m_i = p^s d_1,\ s > a$ then

$$\Psi_{m_i}(\varepsilon_n) = \Psi_{m_i}(\varepsilon_d)) = \Psi_{m_i}(\varepsilon_{d_1}).$$

Equality (4) implies that $\Psi_{m_i}(\varepsilon_n)/p = \Psi_{m_i}(\varepsilon_d)/p$ is an algebraic integer of the field $Q(\varepsilon_d)$ and

$$0 \not\equiv \Psi_{m_i}(\varepsilon_n)/p \equiv \Psi_{m_i}(\varepsilon_d)/p \pmod P \tag{6}$$

if $m_i \in M_{p,d}$. Further, $\varepsilon_{p^b} \equiv 1 \pmod P$ and, therefore,

$$\Psi_{m_i}(\varepsilon_n) \equiv \Psi_{m_i}(\varepsilon_d) \pmod P \tag{7}$$

for every m_i. Moreover, (5) implies

$$\Psi_{m_i}(\varepsilon_n) \not\equiv 0 \pmod P \tag{8}$$

for $m_i \notin M_{p,d}$. From (4)–(8) we get

$$\frac{\Psi(\varepsilon_n)}{p^e} = \left(\prod_{m_i \in M_{p,d}} \left(\frac{\Psi_{m_i}(\varepsilon_n)}{p}\right)\right)\left(\prod_{m_i \notin M_{p,d}} \Psi_{m_i}(\varepsilon_n)\right) \equiv$$

$$\equiv \left(\prod_{m_i \in M_{p,d}} \left(\frac{\Psi_{m_i}(\varepsilon_d)}{p}\right)\right)\left(\prod_{m_i \notin M_{p,d}} \Psi_{m_i}(\varepsilon_d)\right) =$$

$$= \frac{\Psi(\varepsilon_d)}{p^e} \not\equiv 0 \pmod P.$$

3. The Hilbert–Poincare series of an algebra of invariants.

Let $\rho : G \to GL(V)$ be a linear representation of a finite group G over a field K (below we assume K is an algebraically closed field of characteristic zero). The linear group $\rho(G)$ acts naturally on symmetric algebra $S(V)$. Let $R_\rho = S(V)^{\rho(G)}$ be the corresponding algebra of invariants. According to Maschke's theorem the Hilbert–Poincare series $P_\rho(t)$ of R_ρ can be expressed by the following formula

$$P_\rho(t) = \frac{1}{|G|}\left(\sum_{g \in G} \frac{1}{\det(1 - \rho(g)t)}\right)$$

(see [2, 3]). Thus

$$P_\rho(t) = \frac{\Psi(t)}{\Theta(t)}$$

where

$$\Theta(t) = LCM\{\Theta_g(t) = \det(1-\rho(g)t) \,|\, g \in G\}$$

and

$$\Psi = \frac{1}{|G|}\sum_{g\in G}\Theta(t)\Theta_g^{-1}(t).$$

On the other hand, R_ρ is a Cohen–Macaulay algebra (see [2, 3]), and therefore

$$P_\rho(t) = \frac{\widetilde{\Psi}(t)}{\prod_{j=1}^m (1-t^{e_j})}$$

where

$$\widetilde{\Psi}(t) = a_0 t^n + a_1 t^{n-1} + \cdots + a_n$$

for some $n, a_0, \ldots\ a_n \in N \cup \{0\}$, $m = \dim V$ and $e_1, \ldots, e_m$ are the degrees of a homogeneous R_ρ-sequence (see [2, 3]). Moreover, the algebra R_ρ is Gorenstein if and only if the polynomial $\widetilde{\Psi}(t)$ is symmetric, i.e., $a_i = a_{n-i}$ for every i (see [2]). Obviously, every cyclotomic polynomial is symmetric. Further, if $f = g\,h$ where $f,\ g,\ h \in F[t]$ for some field F and if f, h are symmetric polynomials then g is also symmetric. Thus, if the numerator of $P_\rho(t)$ in some presentation $P_\rho(t) = \Psi'(t)/\Theta' t)$ is a product of cyclotomic polynomials then algebra R_ρ is Gorenstein. Further, if the group $\rho(G)$ does not contain a reflection then the algebra R_ρ is Gorenstein if and only if $\rho(G) \leqslant SL(V)$ (see [2, 3]). Thus we have the following fact.

Lemma 1. *Let the numerator of $P_\rho(t)$ (in some presentation) be a product of cyclotomic polynomials. If the group $\rho(G)$ has no reflections then $\rho(G) \leqslant SL(V)$.*

4. Cyclic groups of primary orders.

We get the statement of Theorem 2 from a more general assertion.

Theorem 3. *Let $\rho : G = \langle\sigma\rangle \to GL(V)$ be a faithful linear representation of a cyclic group of a primary order p^s, $p \neq 2$, and let $P_\rho(t) = \Psi(t)/\Theta(t)$ be the corresponding Hilbert–Poincare series. Assume:*

(a) *$\rho(f(\sigma)) = \rho(\sigma)$ for an automorphism $f \in \operatorname{Aut} G$ such that the subgroup of automorphisms $\langle f\rangle$ acts without fixed points on $G\setminus\{1\}$ (i.e., $f^a(\sigma^b) \neq \sigma^b$ if $f^a \neq 1$ and $\sigma^b \neq 1$;*

(b) $\Psi(t)$ *is a product of cyclotomic polynomials;*

(c) $(\Psi(t), \Theta(t)) = 1$ *and* $\Theta(\varepsilon_{p^e}) = 0$ *for every* $1 \leqslant e \leqslant s$.

Then $\dim V/V^{\rho(G)} = 2$, *the matrix* $\rho(\sigma)$ *is similar to a matrix* $\mathrm{diag}(\varepsilon_{p^s}, \varepsilon_{p^s}^{-1}, 1, 1, \ldots, 1)$ *and the algebra* R_ρ *is a hypersurface generated by monomials* $x_1^{p^s}, x_2^{p^s}, x_1x_2, x_3, \ldots, x_m$ *for some basis* $x_1, x_2, \ldots, x_m$ *of* V.

Proof. We have

$$P_\rho(t) = \frac{1}{|G|}\left(\sum_{g\in G}\frac{1}{\Theta_g(t)}\right) = \frac{1}{p^s}\left(\frac{1}{(1-t)^m} + \sum_{g\neq 1}\frac{1}{\Theta_g(t)}\right) =$$

$$= \frac{1}{p^s}\left(\frac{1}{(1-t)^m} + \frac{h(t)}{\widetilde{\Theta}(t)},\right) \tag{9}$$

where $\widetilde{\Theta}(t) = LCM\{\Theta_g \mid g \neq 1\}$ and

$$h(t) = \sum_{g\neq 1}\frac{\widetilde{\Theta}(t)}{\Theta_g(t)}. \tag{10}$$

Since $|\langle\sigma\rangle| = p^s$ then

$$\Theta_g(t) = (1-\varepsilon_{1g}t)(1-\varepsilon_{2g}t)\ldots(1-\varepsilon_{mg}t),$$

where $\{\varepsilon_{ig}\}$ are p^s-th roots of unity (not necessarily primitive). The Galois group $\mathrm{Gal}\,(Q(\varepsilon_{p^s}/Q)$ acts on the set $\{\Theta_g \mid g \neq 1\}$ by permutations. Thus $\widetilde{\Theta}(t) \in Z[t]$ and from (10), $h(t) \in Z[t]$. Since all roots of $\widetilde{\Theta}(t)$ are p^s-th roots of unity we have

$$\widetilde{\Theta}(t) = \Psi_{p^s}^{a_0}\Psi_{p^{s-1}}^{a_1}\ldots\Psi_p^{a_{s-1}}(1-t)^{a_s}. \tag{11}$$

Let

$$d(t) = (h(t), \widetilde{\Theta}(t)),\ \ h(t) = d(t)h_0(t),\ \ \widetilde{\Theta}(t) = d(t)\widetilde{\Theta}_0(t).$$

From (11) we obtain

$$\widetilde{\Theta}_0(t) = \Psi_{p^s}^{b_0}\Psi_{p^{s-1}}^{b_1}\ldots\Psi_p^{b_{s-1}}(1-t)^{b_s}. \tag{12}$$

Now (9), (12), $(\widetilde{\Theta}_0(t), h_0(t)) = 1$ and the condition (c) of the theorem imply

$$b_0, b_1, \ldots, b_{s-1} \geqslant 1,\ \ b_s < m. \tag{13}$$

Moreover,

$$\Theta(t) = (1-t)^{m-b_s}\widetilde{\Theta}_0(t),$$

$$\Psi(t) = \frac{1}{p^s}\left(\Psi_{p^s}^{b_0}\cdots\Psi_p^{b_{s-1}} + (1-t)^{m-b_s}h_0(t)\right). \tag{14}$$

Let us show

$$b_0 = b_1 = \cdots = b_{s-1} = 1. \tag{15}$$

Assume $b_i > 1$ for some i. Then from (13), (14)

$$\ell = v_p(\Psi(1)) = b_0 + \cdots + b_{s-1} - s > 0. \tag{16}$$

Applying Proposition 1 with $d = p^s,\ d_1 = 1$ we obtain from (16)

$$\deg\Psi(t) \geqslant \deg\Psi_{p,p^s} \geqslant \ell\cdot(p-1)p^s. \tag{17}$$

On the other hand, (9) and (14) imply

$$\begin{aligned}\deg\Psi(t) &\leq b_0\cdot(p-1)p^{s-1} + b_1(p-1)p^{s-2} + \ldots + b_{s-1}(p-1) = \\ &= (p-1)[b_0p^{s-1} + b_1p^{s-2} + \ldots + b_{s-1}].\end{aligned} \tag{18}$$

If we fix the number $b = b_0 + \ldots + b_{s-1}$ then the sum (18) is maximal if $b_1 = 1, \ldots, b_{s-1} = 1$ and $b_0 = b-(s-1) = (\ell+s)-(s-1) = \ell+1$. Thus

$$\begin{aligned}\deg\Psi(t) &\leqslant (p-1)[(\ell+1)p^{s-1} + p^{s-2} + \ldots + 1] = \\ &= (p-1)\left[\ell p^{s-1} + \frac{p^s-1}{p-1}\right].\end{aligned} \tag{19}$$

From (17) and (19) we obtain

$$\ell p^{s-1} + \frac{p^s-1}{p-1} \geqslant \ell p^s \tag{20}$$

for an integer $\ell > 0$. Thus $p^s - 1 \geqslant \ell p^{s-1}(p-1)^2$. If $p > 2$ then $(p-1)^2 > p$ and we have the contradiction: $p^s - 1 > \ell p^s$. Thus, (20) and, therefore, (16) was false. Hence we have (15).

From (14) and (15) we get

$$\Psi(t) = \frac{1}{p^s}\left(\frac{1-t^{p^s}}{1-t} + (1-t)^{m-b_s}h_0(t)\right). \tag{21}$$

All coefficients of the polynomial $h_0(t)$ are divisible by $c = |\langle f\rangle|$. Indeed, the condition (a) of the theorem implies that the set $G\setminus\{1\}$ decomposes into the union $\cup_{\alpha\in A}O_\alpha$ of $\langle f\rangle$-orbits with $|O_\alpha| = |\langle f\rangle| = c$ (here

A is a set of representatives of orbits). Moreover, $\Theta_{g_1} = \Theta_{g_2}$ for every $g_1, g_2 \in O_\alpha$. Thus from (7) we obtain

$$h(t) = c\left(\sum_{\alpha\in A} \frac{\widetilde{\Theta}(t)}{\Theta_g(t)}\right)$$

where $g_\alpha \in O_\alpha$. Hence all coefficients of h are divisible by c. Since $h_0 = h/d$ and d is a product of cyclotomic polynomials we obtain our assertion.

Thus for every n the divisor $(h_0(\varepsilon_n))$ of the field $Q(\varepsilon_n)$ is divisible by the divisor (c).

Let q be a prime which divides c and let $n = qp^a$, $1 \leqslant a \leqslant s$. Note, $(c,p) = 1$ and therefore $(q,p) = 1$ (because $c \mid |G \setminus \{1\}|$; it follows from the condition (a)) Assume $q \neq 2$. Since $(c) \mid (h_0(\varepsilon_m))$ and $v_q\left((1-\varepsilon_n^{p^s})/(1-\varepsilon_n)\right) = 1/q - 1$ the formula (21) implies $\Psi(\varepsilon_n) \neq 0$ and

$$v_q(\Psi(\varepsilon_n)) = 1/q - 1. \tag{22}$$

Comparing (22) with (1) we obtain $\Psi_{p^a} \mid \Psi$. This is a contradiction with (14). Thus $q = 2$. For every $n = 2 \cdot p^a$, $1 \leqslant a \leqslant s$, we have $2 \mid (\Psi(\varepsilon_n))$ (possibly, $\Psi(\varepsilon_n) = 0$). Thus, for every $1 \leqslant a \leqslant s$ we have $\Psi_{2^{e_a}p^a} \mid \Psi$ for some $e_a \geqslant 1$ (it follows from (1)). Since $\deg\Psi \leqslant p^s - 1$ we get $e_a = 1$ for every $1 \leqslant a \leqslant s$ and, therefore, $\Psi = \Psi_{2p^s} \cdot \Psi_{2p^{s-1}} \cdots \Psi_{2p}$. Now, from (9), (12), (14), (15), and (21) we get

$$\begin{aligned} P_\rho(t) &= \frac{\Psi_{2p^s}\Psi_{2p^{s-1}}\cdots\Psi_{2p}}{\Psi_{p^s}\Psi_{p^{s-1}}\cdots\Psi_p(1-t)^m} = \\ &= \frac{1-t^{2p^s}}{(1-t^{p^s})^2(1-t^2)(1-t)^{m-2}}. \end{aligned} \tag{23}$$

Consider the representation $\widetilde{\rho} : G = \langle\sigma\rangle \to GL(V)$ defined by the formula

$$\widetilde{\rho}(\sigma) = \operatorname{diag}(\varepsilon_{p^s}, \varepsilon_{p^s}^{-1}, 1, \ldots, 1).$$

One can easily check that the algebra of invariants $R_{\tilde{\rho}}$ is a hypersurface and its Hilbert–Poincare series has the form (23), i.e., $P_{\tilde{\rho}}(t) = P_\rho(t)$. We show now that the representation ρ is equivalent to $\widetilde{\rho}$ (with some choice of ε_{p^s}). We have $\dim V^{\rho(G)} = P'_\rho(0) = P'_{\tilde{\rho}}(0) = m-2$. Since $\operatorname{char} K = 0$ we have $V = V_1 \oplus V^{\rho(G)}$ where V_1 is a 2-dimensional $\rho(G)$-module. Let $\rho_1 : G = \langle\sigma\rangle \to GL(V_1)$ be the restriction of ρ. Then

$$P_\rho(t) = \frac{1}{(1-t)^{m-2}} P_{\rho_1}(t).$$

The condition (a) implies that the group $\rho(G)$ has no reflections. Thus the group $\rho_1(G)$ has no reflections too. Since the numerator of $P_{\rho_1}(t)$ is a product of cyclotomic polynomials we may apply Lemma 1. Therefore $\rho_1(G) \subset SL(V_1)$ and $\rho_1(\sigma) \sim \operatorname{diag}(\varepsilon_{p^s}, \varepsilon_{p^s}^{-1})$.

Now we show how Theorem 3 implies Theorem 2. Since $f \neq 1$ in the condition of Theorem 2 we have $p \neq 2$. In the case $s = 1$ conditions (a) and (b) of Theorem 3 follows from the condition of Theorem 2. Consider condition (c) of Theorem 3. If $s = 1$ we obtain from (9)

$$P_\rho(t) = \frac{f(t)}{(1-t)^m \Psi_p^k}$$

for some $k \geqslant 0$. We may assume

$$(f, \Psi_p) = 1), \ \deg f \leqslant \deg \Psi_p^k.$$

If $k = 0$ then $P_\rho(t) = 1/(1-t)^m$. But it means that $\dim V^{\rho(G)} = P'_\rho(0) = m$. Thus $k > 0$ and we have condition (c).

This proves Theorem 2.

5. Proof of Theorem 1.

Let $\rho : G = \langle \sigma \rangle \to GL(V)$ be an almost regular representation and let $m = \dim V$. Further, let $g \in G$ and let $\varepsilon_{\rho(g)1}, \dots, \varepsilon_{\rho(g)m}$ be the eigenvalues of the operator $\rho(g)$. Then

$$\det(1 - \rho(g)t) = \prod_{i=1}^{m} (1 - \varepsilon_{\rho(g)i} t).$$

Put

$$\Theta_g(t) = \prod_{i=1}^{m} (1 - \varepsilon_{\rho(g)i} t), \ \ \Theta(t) = LCM\{\Theta_g(t)\}.$$

From the Mashke formula we have

$$P_\rho(t) = \frac{1}{n} \sum_{g \in G} \frac{\Theta(t)\Theta_g^{-1}(t)}{\Theta(t)}. \tag{24}$$

Further, from the definition of almost regular representation we have

$$\Theta(t) = (1-t)^m \prod_{d|n, d \neq 1} \Psi_d^{m_d}. \tag{25}$$

(Here Ψ_d is the d-cyclotomic polynomial). Let $d \mid n$. Since ρ is $\operatorname{Aut} G$-invariant all polynomials $\Theta_g(t)$ for elements of the same order d has the form

$$\Theta_d(t) = \Psi_d^{m_d} \prod_{k \mid d, k \neq 1, d} \Psi_k^{m_{k,d}} (1-t)^{m_{1,d}}. \tag{26}$$

Note that m_d in (26) is the same as in (3). of the definition of almost regular representation. Also, this definition implies

$$m_{k,d} < m_k \tag{27}$$

for every $k \mid d,\ k \neq 1$. Put

$$\widetilde{\Theta}_d(t) = \Theta(t)\Theta_d(t)^{-1}.$$

Then from (24) we get

$$P_\rho(t) = \frac{1}{n} \sum_{d \mid n} \frac{\varphi(d)\widetilde{\Theta}_d(t)}{\Theta(t)} = \frac{\Psi(t)}{\Theta(t)}. \tag{28}$$

From(25), (26), (27), and (28), we obtain $(\Psi(t), \Theta(t)) = 1$ and

$$0 \neq \Psi(\varepsilon_d) = \frac{1}{n}\varphi(d)\widetilde{\Theta}_d(\varepsilon_d) =$$

$$= \frac{1}{n}\varphi(d)(1-\varepsilon_d)^{m-m_{1,d}} \prod_{k \mid d, k \neq 1} \Psi^{m_k - m_{k,d}}(\varepsilon_d) \prod_{\ell \nmid d} \Psi_\ell^{m_\ell}(\varepsilon_d). \tag{29}$$

Lemma 2. *Let $p^2 \mid n$ for some prime p. Then $p = 2$, $n = 4$, the matrix $\rho(\sigma)$ is similar to* $\operatorname{diag}(i, -i, 1, \dots, 1)$ *and R_ρ is a hypersurface.*

Proof. Let $n = p^a \ell,\ a > 1,\ (\ell, n) = 1$. Further, let $g = \sigma^\ell$. From (3) of the definition we have $m_{p^a}(g) = m_{p^a}$. Obviously,

$$m_{p^{a-b}} = m_{p^{a-b}}(g^{p^b}) = p^b m_{p^a}$$

for every $b < a$. Put

$$s_0 = m_{p^a},\ s_1 = m_{p^{a-1}}, \cdots, s_{a-1} = m_p.$$

Thus,

$$s_i = p^i s_0. \tag{30}$$

From (1), (29), and (30) we have

$$v_p(\Psi(1)) = v_p\left(\Psi_{p^a}^{s_0}(1)\Psi_{p^{a-1}}^{s_1}(1)\dots\Psi_p^{s_{a-1}}(1)\right) - v_p(n) =$$

$$= s_0 + \cdots + s_{a-1} - a = s_0(1 + p + \cdots + p^{a-1}) - a = s_0 \frac{p^a - 1}{p - 1} - a. \quad (31)$$

From (1), (26), and (29), we have

$$v_p(\Psi(\varepsilon_{p^a})) = v_p(\Psi_{p^{a-1}}^{s_1 - e_1}(\varepsilon_{p^a})\Psi_{p^{a-2}}^{s_2 - e_2}(\varepsilon_{p^a}) \cdots \Psi_p^{s_{a-1} - e_{a-1}}(\varepsilon_{p^a})) +$$
$$+ v_p((1 - \varepsilon_{p^a})^{m - e_0}) + v_p(\varphi(p^a)) - v_p(n), \quad (32)$$

where

$$e_1 = m_{p^{a-1}, p^a}, \;\; e_2 = m_{p^{a-2}, p^a}, \ldots, e_{a-1} = m_{p, p^a}, \;\; e_0 = m_{1, p^a}.$$

From (30) and (32) we obtain

$$v_p(\Psi(\varepsilon_{p^a})) =$$
$$= \frac{s_1 - e_1}{p} + \frac{s_2 - e_2}{p^2} + \cdots \frac{s_{a-1} - e_{a-1}}{p^{a-1}} + \frac{m - e_0}{(p-1)p^{a-1}} - 1 = \quad (33)$$
$$= s_0(a-1) - \sum_{i=1}^{a-1} \frac{e_i}{p^i} + \frac{m - e_0}{(p-1)p^{a-1}} - 1.$$

From (26) we have

$$m = \deg \Theta_{p^a} = m_{p^a}\varphi(p^a) + \sum_{i=1}^{a-1} m_{p^{a-i}, p^a}\varphi(p^{a-i}) + m_{1, p^a} =$$
$$= s_0\varphi(p^a) + e_1\varphi(p^{a-1}) + e_2\varphi(p^{a-2}) + \ldots e_{a-1}\varphi(p) + e_0 =$$
$$= s_0(p-1)p^{a-1} + (p-1)(e_1p^{a-2} + e_2p^{a-3} + \cdots e_{a-1}) + e_0.$$

Hence,

$$m - e_0 = s_0(p-1)p^{a-1} + (p-1)(e_1p^{a-2} + \cdots + e_{a-1}). \quad (34)$$

From (33) and (34) we get

$$v_p(\Psi(\varepsilon_{p^a})) = s_0a - 1. \quad (35)$$

Proposition 1, (31) and (35) imply

$$s_0\frac{p^a - 1}{p - 1} - a = s_0a - 1$$

and, therefore,

$$\frac{p^a - 1}{p - 1} = a + \frac{a - 1}{s_0}. \quad (36)$$

We have $(p^a-1)/(p-1) \geqslant 2^a-1$. On the other hand, $a+(a-1)/s_0 \leqslant 2a-1$. Thus (36) implies $a=2$ and therefore $p+1=2+1/s_0$. Then $p=2$, $s_0=1$. Now $n=4\cdot\ell$, $(2,\ell)=1$. Recall, that $s_0=m_{p^a}=m_4$ is the multiplicity of the eigenvalue ε_4 of the operator $\rho(\sigma^\ell)$. Since $s_0=1$ we have $\ell=1$. Further,

$$V=V_4+V_2+V_1,$$

where V_d is the vector space generated by eigenvectors with eigenvalues which are primitive d-th roots of unity. From (3) of the definition of almost regular representation we obtain $\dim V_2<\dim V_4$. But $\dim V_4=2$ because $s_0=1$ and ρ is $\operatorname{Aut} G$-invariant. Since $\dim V_2\neq 1$ (because $\rho(G)\leqslant SL(V)$; see Lemma 1) we have $\dim V_2=0$. Thus $V=V_4+V_1$. If x_1,x_2 are eigenvectors corresponding to $i,-i$ and $x_3,\dots,x_m$ are linearly independent $\rho(G)$-invariants then in the basis $x_1,x_2,x_3\dots x_m$ the matrix $\rho(\sigma)$ has the form $\operatorname{diag}(i,-i,1,\dots,1)$ and the algebra of invariants R_ρ is generated by the monomials $x_1^4, x_1x_2, x_2^4, x_3,\dots,x_m$.

We assume now

$$n=p_1p_2\cdots p_k.$$

Lemma 3. *Let $k>1$. Then $n=6$, the matrix $\rho(\sigma)$ is similar to* $\operatorname{diag}(\varepsilon_6,\varepsilon_6^{-1},1,\dots,1)$ *and R_ρ is a hypersurface.*

Proof. If $k>1$ then $n>2$. Then the operator $\rho(\sigma)$ has $\varphi(n)>1$ different eigenvalues which are primitive n-th roots of unity. Thus $\rho(\sigma^e)$ is not a reflection for every e. By Lemma 1, $\rho(G)\leqslant SL(V)$. Therefore all coefficients with t^m in the polynomials $\Theta_g(t)$ are equal to $(-1)^m$. Now, from (24) and (28) we obtain

$$\deg\Psi(t)=\deg\Theta(t)-m. \tag{37}$$

From (25) and (37) we get

$$\deg\Psi(t)=\sum_{d|n,d\neq 1}\varphi(d)m_d. \tag{38}$$

Now let $1\neq d\,|\,n$ and let $p\,|\,d$ for some prime p. Put $d_1=d/p$. From (1), (25), and (26), we have

$$v_p(\Psi(\varepsilon_{d_1}))\geqslant v_p(\Psi_d^{m_d}(\varepsilon_{d_1}))-v_p(n)=m_d-1. \tag{39}$$

Let $\Psi_{p,d}(t)$ be the product of polynomials of the form $\Psi_{d_1p^s}(t)$, $s>0$, which divides the polynomial Ψ. Then $s>1$ and by Proposition 1 and (39) we get

$$\deg \Psi_{p,d} \geqslant (m_d-1)p\varphi(d). \tag{40}$$

(Here $a=1$, $a_0=0$ in the condition of Proposition 1). Note, if $d_1\neq d_2$ are two divisors of n and if $p_1\,|\,d_1$, $p_2\,|\,d_2$ are primes (possibly $p_1=p_2$) then $(\Psi_{p_1,d_1},\Psi_{p_2,d_2})=1$ (recall, $s>1$). Thus, if for every divisor $1\neq d\,|\,n$ we fix any prime $p_d\,|\,d$ we obtain from (40)

$$\deg \Psi \geqslant \sum_{d|n,d\neq 1}(m_d-1)p_d\varphi(d). \tag{41}$$

If $m_d>1$ then

$$(m_d-1)p_d \geq m_d. \tag{42}$$

and moreover,

$$(m_d-1)p_d > m_d \ \text{ if } p_d \neq 2. \tag{43}$$

Thus, if $m_d>1$ for every $d\,|\,n$ then (41)–(43) contradict to (38). Note, $m_d>1$ for every $d\,|\,n$, $d\neq n$, $n/2$ because $m_d\geqslant\varphi(n/d)m_n$. Therefore we may assume $m_n=1$.

Suppose $p\,|\,n$ for some prime $p>2$ and $n\neq 2p$. Then $m_p>1$ and

$$\begin{aligned}(m_p-1)p\varphi(p) &= (m_p-1)2\varphi(p)+(m_p-1)(p-2)\varphi(p)\geq\\ &\geq m_p\varphi(p)+(\varphi(n/p)-1)(p-2)\varphi(p)=\\ &= m_p\varphi(p)+(1-\varphi(p)/\varphi(n))(p-2)\varphi(n)\geqslant\\ &\geqslant m_p\varphi(p)+\frac{(p-2)}{2}\varphi(n)\end{aligned} \tag{44}$$

($\varphi(p)/\varphi(n)\leqslant\frac{1}{2}$ because $n\neq 2p$). If we compare (41)–(44) with (38) we obtain $p\leqslant 3$ in the cases of odd n or $m_{n/2}>1$ and $p\leqslant 5$ in the case $m_{n/2}=1$. Thus, we have the single possibility $n=2\cdot 3\cdot 5$ and $m_{n/2}=1$. Now we put in (41) the last sum of (44) for $p=3$ and 5 instead of the corresponding members. The inequality obtained contradicts to (38). Hence $n=2p$ for some prime p. Recall, we may assume $m_n=1$. From (38) and (41) we obtain

$$\begin{aligned}\varphi(2p)+m_p\varphi(p)+m_2\varphi(2)=(m_p+1)\varphi(p)+m_2\geqslant\\ \geqslant (m_p-1)p\varphi(p)+(m_2-1)2\varphi(2)=(m_p-1)p\varphi(p)+2(m_2-1).\end{aligned}$$

Hence $m_p = 1$ or

$$p \leqslant \frac{m_p + 1}{m_p - 1}.$$

The latter inequality is possible only if $p = 3$, $m_p = 2$. Assume $m_p = 1$. Then

$$\deg \Psi = 2\varphi(p) + m_2.$$

Let $q \,|\, p-1$ and let $\ell_q = v_q(\Psi(\varepsilon_{2p}))$. From (1), (29) we obtain $\ell_q \geqslant 1$ for every $q \,|\, p-1$. By Proposition 1,

$$\deg \Psi_{q,2p} \geqslant \ell_q \varphi(2pq).$$

Moreover, $\deg \Psi_{2,1} \geqslant 2(m_2 - 1)$. Since cyclotomic polynomials $\Psi_{q,2p}$ are prime to each other and $\Psi_{2,1}$ we have the inequality

$$\deg \Psi = 2\varphi(p) + m_2 \geqslant \sum_{q \,|\, p-1} \ell_q \varphi(2pq) + 2(m_2 - 1)$$

(recall, that q in this sum are primes). Note, that $m_2 \geqslant \varphi(p)$. Therefore, this inequality is possible only when $m_2 = 2$ and when there exists only one prime q which divides $p-1$, moreover, $q = p-1$. Hence $m_2 = 2$, $p = 3$. Now we have $n = 6$ and ρ is $\operatorname{Aut} G$-invariant representation with $m_6 = m_3 = 1$ and $m_2 = 2$. Obviously,

$$\rho(\sigma) \sim \operatorname{diag}(\varepsilon_6, \varepsilon_6^{-1}, 1, \dots, 1),$$

where ε_6 is a primitive 6-th root of unity. In this case algebra R_ρ is hypersurface generated by monomials $x_1^6, x_1 x_2, x_2^6, x_3, \dots, x_m$. Assume now $n = 6$, $m_3 = 2$. Then

$$\deg \Psi = \varphi(6) + 2\varphi(3) + m_2\varphi(2) = 6 + m_2.$$

By Proposition 1,

$$\deg \Psi_{3,1} \geqslant 3\varphi(6) = 6,\ \deg \Psi_{2,1} \geqslant$$
$$\geqslant 2(m_2 - 1),\ \deg \Psi_{2,6} \geqslant 2 \cdot \varphi(6) = 4.$$

Hence $6 + m_2 \geqslant 6 + 4 + 2(m_2 - 1)$. It is a contradiction.

Consider the case $k = 1$, i.e., $n = p$ is a prime. If $p \geqslant 3$ the result follows from Theorem 2. Let $p = 2$. If $\dim V/V^{\rho(G)} = 1$ then $\rho(\sigma)$ is a reflection and R_ρ is a polynomial algebra. If $\dim V/V^{\rho(G)} = 2$ then R_ρ is a hypersurface which are generated by monomials $x_1^2, x_1 x_2, x_2^2, x_3, \dots, x_m$. Let $m_2 = \dim V/V^{\rho(G)} > 2$. Then $\deg \Psi = m_2$. On the other hand, by Proposition 1 $\deg \Psi_{2,1} \geqslant 2(m_2 - 1)$. Thus, $m_2 \geqslant 2(m_2 - 1)$. This is a contradiction.

Theorem 1 has now been proved.

References

1. N. Gordeev, *Finite linear groups whose algebra of invariants is a complete intersection.* — Izv. Akad. Nauk USSR, Ser. Mat. **50** (1986), 343–392.
2. R. P. Stanley, *Hilbert functions of graded algebras.* — Adv. Math. **28** (1978), 57–83.
3. R. P. Stanley, *Invariants of finite groups and their application to combinatorics.* — Bull. Am. Math. Soc. **1** (1979), 475–511.

Department of Mathematics
of Russian State
Pedagogical University
email gordeev@pdmi.ras.ru

Поступило 4 мая 2000