Math-Net.Ru

Общероссийский математический портал

С. А. Степанов, О структуре L -функций Артина, *Изв. РАН. Сер. матем.*, 2014, том 78, выпуск 1, 167–180

DOI: <https://doi.org/10.4213/im7988>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.209.158.208

26 апреля 2023 г., 12:14:19

УДК 512.754

С. А. Степанов

О структуре L -функций Артина

Рассматривается производящая L -функция Артина $L(z) = L(z, f) = \exp(\sum_{\nu=1}^{\infty} \frac{T_{\nu}}{\nu} z^{\nu})$ для сумм характеров $T_{\nu} = \sum_{x_1, \dots, x_n \in \mathbb{F}_{q^{\nu}}} \psi_{\nu}(f(x_1, \dots, x_n))$, где $\mathbb{F}_q$ – конечное поле, $\mathbb{F}_{q^{\nu}}$ – его конечное расширение, $\psi_{\nu}(\alpha)$ – нетривиальный аддитивный характер поля $\mathbb{F}_{q^{\nu}}$, $f \in \mathbb{F}_q[x_1, \dots, x_n]$ – многочлен степени $d \geq 2$, и дается элементарное доказательство гипотезы Е. Бомбьери об алгебраической структуре функции $L(z)$ в случае $n = 2$.

Библиография: 16 наименований.

Ключевые слова: конечные поля, суммы характеров с многочленами от многих переменных, L -функция Артина, гипотеза Бомбьери, поляризованные симметрические многочлены от многих переменных, теорема Варинга о симметрических многочленах.

DOI: 10.4213/im7988

Введение

Пусть p – простое число, r, ν – положительные целые числа, $\mathbb{F}_p$ – простое конечное поле, состоящее из p элементов, $\mathbb{F}_q$ – конечное расширение поля $\mathbb{F}_p$ степени r и $\mathbb{F}_{q^{\nu}}$ – конечное расширение поля $\mathbb{F}_q$ степени ν , так что

$$\mathbb{F}_p \subset \mathbb{F}_q \subset \mathbb{F}_{q^{\nu}}.$$

Группа Галуа G_{ν} поля $\mathbb{F}_{q^{\nu}}$ над $\mathbb{F}_q$ является циклической группой порядка ν . Если σ_{ν} – порождающий элемент группы G_{ν} , то его действие на элемент $\alpha \in \mathbb{F}_{q^{\nu}}$ задается следующим образом: $\sigma_{\nu}(\alpha) = \alpha^q$. Отображение $\text{tr}_{\nu}: \mathbb{F}_{q^{\nu}} \rightarrow \mathbb{F}_q$, определяемое соотношением

$$\text{tr}_{\nu}(\alpha) = \alpha + \sigma_{\nu}(\alpha) + \dots + \sigma_{\nu}^{\nu-1}(\alpha) = \alpha + \alpha^q + \dots + \alpha^{q^{\nu-1}},$$

называется *относительным следом* элемента $\alpha \in \mathbb{F}_{q^{\nu}}$, и если $\text{tr}: \mathbb{F}_q \rightarrow \mathbb{F}_p$ – след из $\mathbb{F}_q$ в $\mathbb{F}_p$, то отображение $\text{tr}(\text{tr}_{\nu}): \mathbb{F}_{q^{\nu}} \rightarrow \mathbb{F}_p$, задаваемое соотношением

$$\text{tr}(\text{tr}_{\nu}(\alpha)) = \alpha + \alpha^p + \dots + \alpha^{p^{r\nu-1}},$$

называется *абсолютным следом* элемента α . Пусть теперь

$$\psi(a) = \exp\left(2\pi i \frac{\text{tr}(ca)}{p}\right), \quad c \in F_q^*,$$

– нетривиальный аддитивный характер поля F_q . Тогда

$$\psi_{\nu}(\alpha) = \psi(\text{tr}_{\nu}(\alpha))$$

является нетривиальным характером поля $\mathbb{F}_{q^{\nu}}$, называемым *аддитивным характером, индуцированным характером ψ* .

Для произвольного многочлена $f(x_1, \dots, x_n) \in \mathbb{F}_q[x_1, \dots, x_n]$ степени $d \geq 1$ и любого нетривиального аддитивного характера ψ_ν поля $\mathbb{F}_{q^\nu}$ определим *сумму характеров* $T_\nu = T_\nu(f)$ соотношением

$$T_\nu = \sum_{x_1, \dots, x_n \in \mathbb{F}_{q^\nu}} \psi_\nu(f(x_1, \dots, x_n))$$

и рассмотрим соответствующую производящую *L-функцию Артина* [1] комплексного переменного z , определяемую следующим образом:

$$L(z) = L(z, f) = \exp\left(\sum_{\nu=1}^{\infty} \frac{T_\nu}{\nu} z^\nu\right).$$

При $n = 1$ из классического результата А. Вейля [2] следует, что функция $L(z)$ является многочленом из кольца $\mathbb{C}[z]$ степени $d - 1$ с алгебраическими коэффициентами. Позже вполне элементарное доказательство этого результата было дано автором [3, п. 1.3]. А. Гротендик [4] при произвольном $n \geq 1$ доказал с использованием весьма глубоких топологических методов l -адических когомологий, что $L(z)$ является рациональной функцией. Затем Е. Бомбьери [5] предположил, что $L(z)$ имеет весьма специальный вид:

$$L(z) = P(z)^{(-1)^{n-1}}$$

с многочленом $P(z)$, при условии, что $f(x_1, \dots, x_n)$ удовлетворяет некоторым условиям невырожденности.

Пусть X – неособое проективное алгебраическое многообразие, определенное над конечным полем $\mathbb{F}_{q^\nu}$, и пусть N_ν – число его $\mathbb{F}_{q^\nu}$ -рациональных точек. Определим, следуя [6], дзета-функцию $Z(X, t)$ многообразия X равенством

$$Z(X, t) = \exp\left(\sum_{\nu=1}^{\infty} \frac{N_\nu}{\nu} t^\nu\right)$$

и отметим наличие определенной взаимосвязи между данным определением и указанным выше определением L -функции Артина. В 1949 г. Вейль высказал ряд гипотез относительно структуры функции $Z(X, t)$:

1) если $r = \dim X$, то степенной ряд, определяющий функцию $Z(X, t)$, абсолютно сходится в круге $|t| < q^{-r}$ комплексной плоскости $\mathbb{C}$;

2) $Z(X, t)$ является рациональной функцией комплексного переменного t вида

$$Z(X, t) = \frac{P_1(t)P_3(t) \cdots P_{2r-1}(t)}{P_0(t)P_2(t) \cdots P_{2r}(t)},$$

где

$$P_i(t) = \prod_{j=1}^{B_i} (1 - \omega_{ij}t), \quad 0 \leq i \leq 2r, \quad P_0(z) = 1 - t, \quad P_{2r}(z) = 1 - q^r t;$$

3) $Z(X, t)$ удовлетворяет функциональному уравнению

$$Z\left(X, \frac{1}{q^r t}\right) = \pm q^{rx/2} t^x Z(X, t),$$

где

$$\chi = \sum_{i=0}^{2r} (-1)^i B_i;$$

4) для функции $Z(X, z)$ справедлива “гипотеза Римана”

$$|\omega_{ij}| = q^{i/2}, \quad 0 \leq i \leq 2r, \quad 1 \leq j \leq B_i;$$

5) если $\mathfrak{p}$ – простой идеал конечного расширения F поля рациональных чисел $\mathbb{Q}$ и X – редукция по модулю $\mathfrak{p}$ неособого комплексного проективного многообразия $X_{\mathbb{C}}$, определенного над F , то степень B_i многочлена $P_i(t)$, $0 \leq i \leq 2r$, совпадает с i -мерным числом Бетти многообразия $X_{\mathbb{C}}$, а число χ – с характеристикой Эйлера–Пуанкаре этого многообразия.

Позже Дойринг предположил, что коэффициенты многочленов P_i , $0 \leq i \leq 2r$, являются целыми рациональными числами. Затем все указанные выше гипотезы А. Вейля были в общей полноте доказаны П. Делинем [7].

Пусть $\mathbb{F}_q$ – конечное поле характеристики $p > 2$ и χ_ν – квадратичный мультипликативный характер поля $\mathbb{F}_{q^\nu}$. Далее, пусть $f(x_0, x_1, \dots, x_n)$ – однородный многочлен четной степени $d = 2s$ с коэффициентами из поля $\mathbb{F}_q$,

$$T_\nu^*(f) = \sum_{x_0, x_1, \dots, x_n \in \mathbb{F}_{q^\nu}} \chi_\nu(f(x_0, x_1, \dots, x_n))$$

– ассоциированная с этим многочленом сумма характеров и

$$L^*(z) = \exp\left(\sum_{\nu=1}^{\infty} \frac{T_\nu^*}{\nu} z^\nu\right)$$

– ассоциированная с рассматриваемой суммой L -функция. Г.И. Перельмутер [8] в 1975 г. определил в явном виде многообразие, соответствующее сумме $T_\nu^*(f)$, и, основываясь на результатах П. Делиня, установил, что

$$L^*(z) = P_n^*(z)^{(-1)^n},$$

где $P_n^*(z)$ – многочлен степени B_n .

В настоящей работе рассматривается случай многочленов $f(x_1, x_2)$ над полем $\mathbb{F}_q[x_1, x_2]$ от двух переменных x_1, x_2 и дается элементарное доказательство гипотезы Бомбьери для L -функции Артина с аддитивным характером в наиболее интересном случае, когда характеристика p поля $\mathbb{F}_q$ достаточно велика.

ТЕОРЕМА 1. Пусть $\mathbb{F}_q$ – конечное поле характеристики p и

$$f(x_1, x_2) = \sum_{0 \leq d_1 + d_2 \leq d} a_{d_1, d_2} x_1^{d_1} x_2^{d_2} \in \mathbb{F}_q[x_1, x_2]$$

– многочлен степени $d \geq 2$. Если $p > d$ и ведущая однородная часть

$$f_d(x_1, x_2) = \sum_{d_1 + d_2 = d} a_{d_1, d_2} x_1^{d_1} x_2^{d_2}$$

многочлена $f(x_1, x_2)$ неособа в стандартном смысле (т.е. не существует ни одной ненулевой точки над $\overline{\mathbb{F}}_q$, в которой f , $\frac{\partial f}{\partial x_1}$, $\frac{\partial f}{\partial x_2}$ обращаются в нуль одновременно), то L -функция Артина $L(z)$ является рациональной функцией вида

$$L(z) = P(z)^{-1},$$

где $P(z) \in \mathbb{C}[z]$ – многочлен степени $(d-1)^2$.

В заключение заметим, что представленное в настоящей работе доказательство теоремы 1 может быть обобщено на случай многочленов $f(x_1, \dots, x_n)$, зависящих от произвольного числа $n \geq 1$ переменных $x_1, \dots, x_n$.

§ 1. Поляризованные элементарные симметрические многочлены

Пусть m, n – положительные целые числа, $\mathbb{F}$ – произвольное поле и

$$A_{mn} = \mathbb{F}[x_{11}, \dots, x_{m1}; \dots; x_{1n}, \dots, x_{mn}]$$

– алгебра многочленов от mn переменных x_{ij} над полем $\mathbb{F}$. Симметрическая группа $G = S_n$ действует на алгебре A_{mn} как группа $\mathbb{F}$ -автоморфизмов по правилу

$$g(x_{ij}) = x_{i,g(j)}, \quad g \in G.$$

Обозначим через A_{mn}^G подалгебру инвариантов алгебры A_{mn} относительно действия группы G . Далее, определим *поляризованные элементарные симметрические многочлены* $u_{r_1, \dots, r_m} \in A_{mn}^G$ от n векторных переменных

$$(x_{11}, \dots, x_{m1}), \dots, (x_{1n}, \dots, x_{mn})$$

при помощи следующего формального равенства:

$$\prod_{j=1}^n (1 + x_{1j}z_1 + \dots + x_{mj}z_m) = \sum_{1 \leq r_1 + \dots + r_m \leq n} u_{r_1, \dots, r_m} z_1^{r_1} \dots z_m^{r_m}. \quad (1)$$

Если $\mathbb{F}$ – поле нулевой характеристики, то из теоремы Гильберта–Нётер (см. [9], [10]) следует, что A_{mn}^G является конечно порожденной коммутативной $\mathbb{F}$ -алгеброй, алгебра A_{mn} конечно порождена как модуль над A_{mn}^G и поляризованные элементарные симметрические многочлены $u_{r_1, \dots, r_m}$, $1 \leq r_1 + \dots + r_m \leq n$, образуют полную систему порождающих элементов алгебры A_{mn}^G над $\mathbb{F}$ (см. [11, гл. II]). Позже этот результат был расширен Э. Нётер [12] на случай полей $\mathbb{F}$ простой характеристики $p > n!$. В 1996 г. результат Э. Нётер был существенно усилен Д. Ричманом [13], который доказал, что алгебра A_{mn}^G порождается многочленами $u_{r_1, \dots, r_m}$, $1 \leq r_1 + \dots + r_m \leq n$, при значительно более слабом условии $p > n$. Несколько позднее автором [14] было дано элементарное доказательство этого результата Ричмана.

В настоящей работе мы ограничимся рассмотрением инвариантных многочленов $f \in A_{mn}^G$ вида

$$f = \sum_{0 \leq d_1 + \dots + d_m \leq d} a_{d_1, \dots, d_m} \sum_{j=1}^m x_{1j}^{d_1} \dots x_{mj}^{d_m}$$

и найдем явные формулы, выражающие суммы

$$f_{d_1, \dots, d_m} = \sum_{j=1}^n x_{1j}^{d_1} \dots x_{mj}^{d_m}, \quad 0 \leq d_1 + \dots + d_m \leq d,$$

в виде многочленов от $u_{r_1, \dots, r_m}$, $1 \leq r_1 + \dots + r_m \leq n$. Этот результат может быть рассмотрен как соответствующее обобщение в многомерном случае (см. также [14]) хорошо известной формулы Варинга [15, с. 13]

$$f_d = \sum_{j=1}^n x_j^d = \sum_{s_1 + 2s_2 + \dots + ns_n = d} c(s_1, \dots, s_n) u_1^{s_1} \dots u_n^{s_n}, \quad (2)$$

где $c(s_1, \dots, s_n)$ – целые рациональные числа вида

$$c(s_1, \dots, s_n) = (-1)^{s_2+2s_3+\dots+(n-1)s_n} \frac{d(s_1 + \dots + s_n - 1)!}{s_1! \dots s_n!}. \quad (3)$$

ПРЕДЛОЖЕНИЕ 2. Пусть $d_1, \dots, d_m$ – неотрицательные целые числа,

$$f_{d_1, \dots, d_m} = \sum_{j=1}^n x_{1j}^{d_1} \dots x_{mj}^{d_m}$$

– многочлен из A_{mn}^G степени $d = d_1 + \dots + d_m$ над полем $\mathbb{F}$ характеристики $p > d$, и пусть $u_{r_1, \dots, r_m}$, $1 \leq r_1 + \dots + r_m \leq n$, – поляризованные элементарные симметрические многочлены от векторных переменных $(x_{1j}, \dots, x_{mj})$, $1 \leq j \leq n$. Далее, пусть $s_1, \dots, s_n$ и $s_{1\nu}, \dots, s_{m\nu}$ – неотрицательные целые числа такие, что $s_1 + 2s_2 + \dots + ns_n = d$ и $s_{1\nu} + \dots + s_{m\nu} = \nu s_\nu$ при $1 \leq \nu \leq n$. Наконец, пусть

$$v_{s_{1\nu}, \dots, s_{m\nu}} = \sum \frac{s_\nu!}{\sigma_{\nu 1}! \dots \sigma_{\nu s_\nu}!} \prod_{\tau=1}^{s_\nu} u_{r_{1\tau}, \dots, r_{m\tau}}^{\sigma_{\nu\tau}},$$

где суммирование проводится по всем неотрицательным целым $\sigma_{\nu 1}, \dots, \sigma_{\nu s_\nu}$, $1 \leq \nu \leq n$, и $r_{1\tau}, \dots, r_{m\tau}$, $1 \leq \tau \leq s_\nu$, таким, что

$$r_{\mu 1} \sigma_{\nu 1} + \dots + r_{\mu s_\nu} \sigma_{\nu s_\nu} = s_{\mu\nu}, \quad \sigma_{\nu 1} + \dots + \sigma_{\nu s_\nu} = s_\nu, \quad r_{1\tau} + \dots + r_{m\tau} = \nu$$

для $1 \leq \mu \leq m$, $1 \leq \nu \leq n$ и $1 \leq \tau \leq s_\nu$. Тогда

$$f_{d_1, \dots, d_m} = \frac{d_1! \dots d_m!}{d!} \sum_{s_1+2s_2+\dots+ns_n=d} c(s_1, \dots, s_n) \sum_{i=1}^n \prod_{i=1}^n v_{s_{1\nu_i}, \dots, s_{m\nu_i}}, \quad (4)$$

где внутренняя сумма берется по всем неотрицательным целым $s_{\mu\nu_1}, \dots, s_{\mu\nu_n}$ таким, что

$$s_{\mu\nu_1} + \dots + s_{\mu\nu_n} = d_\mu, \quad s_{1\nu_i} + \dots + s_{m\nu_i} = i s_i$$

для $1 \leq \mu \leq m$ и $1 \leq i \leq n$.

ДОКАЗАТЕЛЬСТВО. Положим в соотношении (2)

$$x_j = x_{1j} z_1 + \dots + x_{mj} z_m, \quad 1 \leq j \leq n,$$

и заметим, что соотношение

$$(x_{1j} z_1 + \dots + x_{mj} z_m)^d = \sum_{d_1+\dots+d_m=d} \frac{d!}{d_1! \dots d_m!} x_{1j}^{d_1} \dots x_{mj}^{d_m} z_1^{d_1} \dots z_m^{d_m}$$

влечет

$$\sum_{j=1}^n (x_{1j} z_1 + \dots + x_{mj} z_m)^d = \sum_{d_1+\dots+d_m=d} \frac{d!}{d_1! \dots d_m!} \left(\sum_{j=1}^n x_{1j}^{d_1} \dots x_{mj}^{d_m} \right) z_1^{d_1} \dots z_m^{d_m}.$$

С другой стороны, имеем

$$\sum_{1 \leq j_1 < \dots < j_\nu \leq n} \prod_{s=1}^{\nu} (x_{1j_s} z_1 + \dots + x_{mj_s} z_m) = \sum_{r_1+\dots+r_m=\nu} u_{r_1, \dots, r_m} z_1^{r_1} \dots z_m^{r_m},$$

и тогда, учитывая соотношения (2), (3), получаем

$$\sum_{j=1}^n (x_{1j}z_1 + \dots + x_{mj}z_m)^d = \sum_{s_1+2s_2+\dots+ns_n=d} c(s_1, \dots, s_n) \times \prod_{\nu=1}^n \left(\sum_{r_1+\dots+r_m=\nu} u_{r_1, \dots, r_m} z_1^{r_1} \dots z_m^{r_m} \right)^{s_\nu}.$$

В результате приходим к соотношению

$$\begin{aligned} & \sum_{d_1+\dots+d_m=d} \frac{d!}{d_1! \dots d_m!} \left(\sum_{j=1}^n x_{1j}^{d_1} \dots x_{mj}^{d_m} \right) z_1^{d_1} \dots z_m^{d_m} \\ &= \sum_{s_1+2s_2+\dots+ns_n=d} c(s_1, \dots, s_n) \prod_{\nu=1}^n \left(\sum_{r_1+\dots+r_m=\nu} u_{r_1, \dots, r_m} z_1^{r_1} \dots z_m^{r_m} \right)^{s_\nu}. \end{aligned}$$

Кроме того, имеем

$$\left(\sum_{r_1+\dots+r_m=\nu} u_{r_1, \dots, r_m} z_1^{r_1} \dots z_m^{r_m} \right)^{s_\nu} = \sum_{s_{1\nu}+\dots+s_{m\nu}=\nu s_\nu} v_{s_{1\nu}, \dots, s_{m\nu}} z_1^{s_{1\nu}} \dots z_m^{s_{m\nu}},$$

где

$$v_{s_{1\nu}, \dots, s_{m\nu}} = \sum \frac{s_\nu!}{\sigma_{\nu 1}! \dots \sigma_{\nu s_\nu}!} \prod_{\tau=1}^{s_\nu} u_{r_{1\tau}, \dots, r_{m\tau}};$$

здесь сумма берется по всем неотрицательным целым $\sigma_{\nu 1}, \dots, \sigma_{\nu s_\nu}$, $1 \leq \nu \leq n$, и $r_{1\tau}, \dots, r_{m\tau}$, $1 \leq \tau \leq s_\nu$, таким, что

$$r_{\mu 1}\sigma_{\nu 1} + \dots + r_{\mu s_\nu}\sigma_{\nu s_\nu} = s_{\mu\nu}, \quad r_{1\tau} + \dots + r_{m\tau} = \nu, \quad \sigma_{\nu 1} + \dots + \sigma_{\nu s_\nu} = s_\nu.$$

Отсюда следует, что

$$\begin{aligned} & \sum_{d_1+\dots+d_m=d} \frac{d!}{d_1! \dots d_m!} \left(\sum_{j=1}^n x_{1j}^{d_1} \dots x_{mj}^{d_m} \right) z_1^{d_1} \dots z_m^{d_m} \\ &= \sum_{d_1+\dots+d_m=d} \left(\sum_{s_1+2s_2+\dots+ns_n=d} c(s_1, \dots, s_n) \sum_S \prod_{i=1}^n v_{s_{1\nu_i}, \dots, s_{m\nu_i}} \right) z_1^{d_1} \dots z_m^{d_m}, \end{aligned}$$

где вторая внутренняя сумма берется по множеству S неотрицательных целых чисел $s_{\mu\nu_1}, \dots, s_{\mu\nu_n}$ таких, что

$$s_{\mu\nu_1} + \dots + s_{\mu\nu_n} = d_\mu, \quad s_{1\nu_i} + \dots + s_{m\nu_i} = i s_i$$

для $1 \leq \mu \leq m$ и $1 \leq i \leq n$. Отсюда мы находим, что

$$\sum_{j=1}^n x_{1j}^{d_1} \dots x_{mj}^{d_m} = \frac{d_1! \dots d_m!}{d!} \sum_{s_1+2s_2+\dots+ns_n=d} c(s_1, \dots, s_n) \sum_S \prod_{i=1}^n v_{s_{1\nu_i}, \dots, s_{m\nu_i}}, \quad (5)$$

и результат следует теперь из того факта, что коэффициенты многочлена, расположенного в правой части равенства (5), являются рациональными числами, знаменатели которых не делятся ни на одно простое $p > d$.

Пусть $\mathbb{F}_q[x]$ – кольцо многочленов от одной переменной x над полем $\mathbb{F}_q$. Теперь мы напомним следующий широко известный факт: если для каждого $\tau = 1, 2, \dots, \nu$ многочлен

$$g(x) = x^\nu + u_1 x^{\nu-1} + \dots + u_\nu \in \mathbb{F}_q[x]$$

имеет в кольце $\mathbb{F}_q[x]$ в точности i_τ неприводимых множителей степени τ , то набор $(i_1, i_2, \dots, i_\nu)$ называется *типом разложения* многочлена $g(x)$. Положим

$$g(x) = \prod_{\tau=1}^{\nu} \prod_{i=1}^{i_\tau} \prod_{k=0}^{\tau-1} (x + \sigma_\tau^k(x_i^{(\tau)})),$$

где σ_τ – порождающий элемент группы Галуа G_τ поля $\mathbb{F}_{q^\tau}$, и заметим, что коэффициенты $u_1, u_2, \dots, u_\nu$ многочлена $g(x)$ инвариантны относительно всевозможных перестановок элементов

$$x_1^{(\tau)}, x_2^{(\tau)}, \dots, x_{i_\tau}^{(\tau)} \in \mathbb{F}_{q^\tau}, \quad 1 \leq \tau \leq \nu,$$

а также относительно всевозможных замен этих элементов на их сопряженные над полем $\mathbb{F}_q$. Отсюда следует, что если неотрицательные целые числа $i_1, i_2, \dots, i_\nu$ пробегает все целочисленные решения уравнения

$$i_1 + 2i_2 + \dots + \nu i_\nu = \nu,$$

а переменные $x_1^{(\tau)}, x_2^{(\tau)}, \dots, x_{i_\tau}^{(\tau)}$ независимо друг от друга пробегает все элементы полей $\mathbb{F}_{q^\tau}$ для $\tau = 1, 2, \dots, \nu$, то элементарные симметрические многочлены $u_1, u_2, \dots, u_\nu$ от этих переменных независимо друг от друга пробегает все элементы поля $\mathbb{F}_q$ с кратностями $i_1! i_2! \dots i_\nu! 1^{i_1} 2^{i_2} \dots \nu^{i_\nu}$ соответственно. Далее, если

$$f(x) = \sum_{i=0}^d a_i x^i \in \mathbb{F}_q[x]$$

– многочлен положительной степени $d \leq \nu$, из формулы Варинга следует, что

$$\sum_{k=1}^{\nu} f(x_k) = \sum_{i=0}^d a_i \sum_{k=1}^{\nu} x_k^i$$

является многочленом от $u_1, u_2, \dots, u_d$ над полем $\mathbb{F}_q$ и, более того, этот многочлен линеен относительно переменной u_d .

Пусть теперь

$$f(x_1, x_2) = \sum_{0 \leq i_1 + i_2 \leq d} a_{i_1, i_2} x_1^{i_1} x_2^{i_2} \in \mathbb{F}_q[x_1, x_2]$$

– многочлен степени $d \geq 1$ от двух переменных x_1, x_2 , и пусть $\nu \geq d$ – произвольное целое число. Если $i_1, i_2, \dots, i_\nu$ – неотрицательные целые числа, удовлетворяющие соотношению $i_1 + 2i_2 + \dots + \nu i_\nu = \nu$, рассмотрим множество пар

$$(x_{1,1}^{(\tau)}, x_{2,1}^{(\tau)}), (x_{1,2}^{(\tau)}, x_{2,2}^{(\tau)}), \dots, (x_{1,i_\tau}^{(\tau)}, x_{2,i_\tau}^{(\tau)}) \in \mathbb{F}_{q^\tau} \times \mathbb{F}_{q^\tau}, \quad 1 \leq \tau \leq \nu,$$

и определим элементарные симметрические многочлены u_{r_1, r_2} от этих пар соотношением

$$\prod_{\tau=1}^{\nu} \prod_{i=1}^{i_\tau} \prod_{k=0}^{\tau-1} (1 + \sigma_\tau^k(x_{1,i}^{(\tau)})z_1 + \sigma_\tau^k(x_{2,i}^{(\tau)})z_2) = 1 + \sum_{\substack{1 \leq r_1 + r_2 \leq \nu \\ r_1 \geq 0, r_2 \geq 0}} u_{r_1, r_2} z_1^{r_1} z_2^{r_2}.$$

Используя указанные выше аргументы, мы находим, что если для любых двух произвольно выбранных неотрицательных целых $i_1, i_2, \dots, i_\nu$, удовлетворяющих условию $i_1 + 2i_2 + \dots + \nu i_\nu = \nu$, переменные $x_{1,1}^{(\tau)}, x_{1,2}^{(\tau)}, \dots, x_{1,i_\tau}^{(\tau)}$ (соответственно, $x_{2,1}^{(\tau)}, x_{2,2}^{(\tau)}, \dots, x_{2,i_\tau}^{(\tau)}$) независимо друг от друга пробегают все элементы полей $\mathbb{F}_{q^\tau}$ для $1 \leq \tau \leq \nu$, то многочлены $u_{1,0}, u_{2,0}, \dots, u_{\nu,0}$ (соответственно, $u_{0,1}, u_{0,2}, \dots, u_{0,\nu}$) от этих переменных независимо друг от друга пробегают все элементы соответствующих подмножеств

$$U_{i_1, i_2, \dots, i_\nu}^{(1)}, U_{i_1, i_2, \dots, i_\nu}^{(2)}, \dots, U_{i_1, i_2, \dots, i_\nu}^{(\nu)}$$

поля $\mathbb{F}_q$ с кратностями $i_1! i_2! \dots i_\nu! 1^{i_1} 2^{i_2} \dots \nu^{i_\nu}$ соответственно. Более того, если неотрицательные целые $i_1, i_2, \dots, i_\nu$ пробегают при этом все решения уравнения $i_1 + 2i_2 + \dots + \nu i_\nu = \nu$, то многочлены $u_{1,0}, u_{2,0}, \dots, u_{\nu,0}$ (соответственно, $u_{0,1}, u_{0,2}, \dots, u_{0,\nu}$) независимо друг от друга пробегают все элементы поля $\mathbb{F}_q$ с теми же самыми кратностями.

Теперь мы предположим, что

$$\nu \geq d + 2 \frac{(d-2)(d-1)}{2} = (d-1)^2 + 1.$$

Для произвольных целых $i_1, i_2, \dots, i_\nu$, удовлетворяющих условию $i_1 + 2i_2 + \dots + \nu i_\nu = \nu$, и любых заданных $\alpha_{r_1, r_2} \in \mathbb{F}_q$, $2 \leq r_1 + r_2 \leq d-1$, $r_1, r_2 \geq 1$, рассмотрим следующую систему полиномиальных уравнений:

$$u_{r_1, r_2} = \alpha_{r_1, r_2}, \quad 2 \leq r_1 + r_2 \leq d-1, \quad 1 \leq r_1, r_2 \leq d-2, \quad (6)$$

относительно определенных выше многочленов u_{r_1, r_2} . Поскольку каждый элемент u_{r_1, r_2} этой системы является однородным симметрическим многочленом от переменных $\sigma_\tau^k(x_{1,i}^{(\tau)})$, $\sigma_\tau^k(x_{2,i}^{(\tau)})$, $1 \leq i \leq i_\tau$, $1 \leq k \leq \tau$, $1 \leq \tau \leq \nu$, степени $r = r_1 + r_2$, то система (6) может быть рассмотрена как система из

$$1 + 2 + \dots + (d-2) = \frac{(d-2)(d-1)}{2}$$

полилинейных уравнений относительно $\nu \geq (d-1)^2 + 1$ неизвестных $\sigma_\tau^k(x_{1,i}^{(\tau)})$ и $\sigma_\tau^k(x_{2,i}^{(\tau)})$, $1 \leq i \leq i_\tau$, $1 \leq k \leq \tau$, $1 \leq \tau \leq \nu$. Далее, если $\omega_1^{(\tau)}, \dots, \omega_\tau^{(\tau)}$ – некоторый базис поля $\mathbb{F}_{q^\tau}$, то, представляя элементы $\sigma_\tau^k(x_{1,i}^{(\tau)})$, $\sigma_\tau^k(x_{2,i}^{(\tau)})$ в виде

$$\begin{aligned} \sigma_\tau^k(x_{1,i}^{(\tau)}) &= x_{1,i}^{(k,1)} \omega_1^{(\tau)} + \dots + x_{1,i}^{(k,\tau)} \omega_\tau^{(\tau)}, \\ \sigma_\tau^k(x_{2,i}^{(\tau)}) &= x_{2,i}^{(k,1)} \omega_1^{(\tau)} + \dots + x_{2,i}^{(k,\tau)} \omega_\tau^{(\tau)}, \end{aligned}$$

где $x_{1,i}^{(k,l)}, x_{2,i}^{(k,l)} \in \mathbb{F}_q$, $1 \leq i \leq i_\tau$, $1 \leq k \leq \tau$, $1 \leq l \leq \tau$, $1 \leq \tau \leq \nu$, мы находим, что система (6) теперь может быть рассмотрена как система из $(d-2)(d-1)/2$ полилинейных уравнений относительно $\nu \geq (d-1)^2 + 1$ переменных $x_{1,i}^{(k,l)}, x_{2,i}^{(k,l)}$.

Используя индукцию по $d \geq 2$, мы находим, что для любых $\nu \geq (d-1)^2 + 1$, α_{r_1, r_2} и любых фиксированных $u_{1,0}, u_{2,0}, \dots, u_{d,0}$; $u_{0,1}, u_{0,2}, \dots, u_{0,d} \in \mathbb{F}_q$ вышеуказанная система полилинейных уравнений разрешима в элементах $\sigma_\tau^k(x_{1,i}^{(\tau)})$, $\sigma_\tau^k(x_{2,i}^{(\tau)})$, $1 \leq i \leq i_\tau$, $1 \leq k \leq \tau$, $1 \leq \tau \leq \nu$. Это означает, что поляризованные элементарные симметрические многочлены $u_{1,0}, u_{2,0}, \dots, u_{d,0}$; $u_{0,1}, u_{0,2}, \dots, u_{0,d}$

и u_{r_1, r_2} , $2 \leq r_1 + r_2 \leq d - 1$, от переменных $\sigma_\tau^k(x_{1,i}^{(\tau)}), \sigma_\tau^k(x_{2,i}^{(\tau)}) \in \mathbb{F}_{q^\tau}$, $1 \leq i \leq i_\tau$, $1 \leq k \leq \tau$, $1 \leq \tau \leq \nu$, могут теперь быть рассмотрены как некоторые новые независимые переменные, принимающие значения в поле $\mathbb{F}_q$ с одними и теми же кратностями $i_1! i_2! \dots i_\nu! 1^{i_1} 2^{i_2} \dots \nu^{i_\nu}$.

Более того, из изложенного выше следует также, что если неотрицательные целые $i_1, i_2, \dots, i_\nu$ пробегают все решения уравнения

$$i_1 + 2i_2 + \dots + \nu i_\nu = \nu \quad \text{при} \quad \nu \geq (d-1)^2 + 1,$$

а переменные $x_{1,1}^{(\tau)}, x_{1,2}^{(\tau)}, \dots, x_{1,i_\tau}^{(\tau)}, x_{2,1}^{(\tau)}, x_{2,2}^{(\tau)}, \dots, x_{2,i_\tau}^{(\tau)}$ независимо друг от друга пробегают элементы полей $\mathbb{F}_{q^\tau}$, $1 \leq \tau \leq \nu$, то значения многочленов $u_{1,0}, u_{2,0}, \dots, u_{d,0}$ (соответственно, $u_{0,1}, u_{0,2}, \dots, u_{0,d}$) независимо друг от друга и от значений многочленов u_{r_1, r_2} , $2 \leq r_1 + r_2 \leq d - 1$, $1 \leq r_1, r_2 \leq d - 2$, пробегают все элементы поля $\mathbb{F}_q$ с кратностями $i_1! i_2! \dots i_\nu! 1^{i_1} 2^{i_2} \dots \nu^{i_\nu}$ соответственно. Таким образом, мы приходим к следующему результату.

ПРЕДЛОЖЕНИЕ 3. Пусть $d \geq 3$, $\nu \geq (d-1)^2 + 1$ – положительные целые и $i_1, i_2, \dots, i_\nu$ – неотрицательные целые числа, удовлетворяющие соотношению

$$i_1 + 2i_2 + \dots + \nu i_\nu = \nu. \quad (7)$$

Если переменные $x_{1,1}^{(\tau)}, x_{1,2}^{(\tau)}, \dots, x_{1,i_\tau}^{(\tau)}, x_{2,1}^{(\tau)}, x_{2,2}^{(\tau)}, \dots, x_{2,i_\tau}^{(\tau)}$ независимо друг от друга пробегают все элементы полей $\mathbb{F}_{q^\tau}$ для $1 \leq \tau \leq \nu$, то поляризованные элементарные симметрические многочлены $u_{1,0}, u_{2,0}, \dots, u_{d,0}$ (соответственно, $u_{0,1}, u_{0,2}, \dots, u_{0,d}$) от этих переменных независимо друг от друга пробегают элементы связанных с ними подмножеств $U_{i_1, i_2, \dots, i_\nu}^{(1)}, U_{i_1, i_2, \dots, i_\nu}^{(2)}, \dots, U_{i_1, i_2, \dots, i_\nu}^{(d)}$ поля $\mathbb{F}_q$ с кратностями $i_1! i_2! \dots i_\nu! 1^{i_1} 2^{i_2} \dots \nu^{i_\nu}$ соответственно. Аналогично, поляризованные элементарные симметрические многочлены u_{r_1, r_2} для $2 \leq r_1 + r_2 \leq d - 2$, $1 \leq r_1, r_2 \leq d - 2$, от указанных переменных независимо друг от друга и от $u_{1,0}, u_{2,0}, \dots, u_{d,0}, u_{0,1}, u_{0,2}, \dots, u_{0,d}$ пробегают все элементы соответствующих подмножеств $U_{i_1, \dots, i_\nu}^{(r_1, r_2)}$ поля $\mathbb{F}_q$ с теми же самыми кратностями $i_1! i_2! \dots i_\nu! 1^{i_1} 2^{i_2} \dots \nu^{i_\nu}$. Более того, если целые числа $i_1, i_2, \dots, i_\nu$ пробегают все решения уравнения (7), то многочлены $u_{1,0}, u_{2,0}, \dots, u_{d,0}$ (соответственно, $u_{0,1}, u_{0,2}, \dots, u_{0,d}$) независимо друг от друга и от u_{r_1, r_2} для $2 \leq r_1 + r_2 \leq d - 1$, $1 \leq r_1, r_2 \leq d - 2$, пробегают все элементы поля $\mathbb{F}_q$ также с кратностями $i_1! i_2! \dots i_\nu! 1^{i_1} 2^{i_2} \dots \nu^{i_\nu}$.

§ 2. Доказательство теоремы 1

Пусть

$$f(x_1, x_2) = \sum_{0 \leq d_1 + d_2 \leq d} a_{d_1, d_2} x_1^{d_1} x_2^{d_2}$$

– многочлен степени $d \geq 2$ с коэффициентами из $\mathbb{F}_q$, и пусть

$$T_\nu = T_\nu(f) = \sum_{x_1, x_2 \in \mathbb{F}_{q^\nu}} \psi_\nu(f(x_1, x_2)), \quad (8)$$

$$L(z) = L(z, f) = \exp\left(\sum_{\nu=1}^{\infty} \frac{T_\nu}{\nu} z^\nu\right). \quad (9)$$

В соответствии с хорошо известным комбинаторным тождеством (см., например, [16, гл. 4.2]) имеем

$$L^{-1}(z) = \exp\left(-\sum_{\nu=1}^{\infty} \frac{T_{\nu}}{\nu} z^{\nu}\right) = 1 + \sum_{\nu=1}^{\infty} \beta_{\nu} z^{\nu}, \quad (10)$$

где

$$\beta_{\nu} = \sum_{\substack{i_1+2i_2+\dots+\nu i_{\nu}=\nu \\ 0 \leq i_1, i_2, \dots, i_{\nu} \leq \nu}} \frac{(-1)^{i_1+i_2+\dots+i_{\nu}} T_1^{i_1} T_2^{i_2} \dots T_{\nu}^{i_{\nu}}}{i_1! i_2! \dots i_{\nu}! 1^{i_1} 2^{i_2} \dots \nu^{i_{\nu}}} \quad (11)$$

являются элементами кругового поля $\mathbb{Q}(e^{2\pi i/p})$.

Для заданных неотрицательных целых $i_1, i_2, \dots, i_{\nu}$, удовлетворяющих соотношению $i_1 + 2i_2 + \dots + \nu i_{\nu} = \nu$, пусть u_{r_1, r_2} , $1 \leq r_1 + r_2 \leq \nu$, $r_1, r_2 \geq 0$, — поляризованные элементарные симметрические многочлены пар точек

$$(x_{1,1}^{(\tau)}, x_{2,1}^{(\tau)}), (x_{1,2}^{(\tau)}, x_{2,2}^{(\tau)}), \dots, (x_{1,i_{\tau}}^{(\tau)}, x_{2,i_{\tau}}^{(\tau)}) \in \mathbb{F}_{q^{\tau}} \times \mathbb{F}_{q^{\tau}}, \quad 1 \leq \tau \leq \nu, \quad (12)$$

определенные соотношением

$$\prod_{\tau=1}^{\nu} \prod_{i=1}^{i_{\tau}} \prod_{k=0}^{\tau-1} \left(1 + \sigma_{\tau}^k(x_{1,i}^{(\tau)}) z_1 + \sigma_{\tau}^k(x_{2,i}^{(\tau)}) z_2\right) = 1 + \sum_{\substack{1 \leq r_1+r_2 \leq \nu \\ r_1 \geq 0, r_2 \geq 0}} u_{r_1, r_2} z_1^{r_1} z_2^{r_2}.$$

Легко видеть, что многочлены u_{r_1, r_2} инвариантны относительно всех перестановок пар (12), а также относительно замены этих пар на их сопряженные над полем $\mathbb{F}_q$. Затем, полагая

$$\begin{aligned} f^*((u_{r_1, r_2})_{1 \leq r_1+r_2 \leq d}) &= \sum_{\tau=1}^{\nu} \sum_{i=1}^{i_{\tau}} \sum_{k=0}^{\tau-1} \sigma_{\tau}^k(f(x_{1,i}^{(\tau)}, x_{2,i}^{(\tau)})) \\ &= \sum_{0 \leq d_1+d_2 \leq d} a_{d_1, d_2} \sum_{\tau=1}^{\nu} \sum_{i=1}^{i_{\tau}} \sum_{k=0}^{\tau-1} (\sigma_{\tau}^k(x_{1,i}^{(\tau)}))^{d_1} (\sigma_{\tau}^k(x_{2,i}^{(\tau)}))^{d_2}, \end{aligned} \quad (13)$$

мы получаем из предложения 2, что $f^*((u_{r_1, r_2})_{1 \leq r_1+r_2 \leq d})$ является многочленом над $\mathbb{F}_q$ от переменных u_{r_1, r_2} , $1 \leq r_1 + r_2 \leq d$, $r_1, r_2 \geq 0$, степени не выше d . Более того, из предложения 3 следует, что если неотрицательные целые $i_1, i_2, \dots, i_{\nu}$ пробегает все решения уравнения $i_1 + 2i_2 + \dots + \nu i_{\nu} = \nu$, а переменные $x_{1,1}^{(\tau)}, x_{1,2}^{(\tau)}, \dots, x_{1,i_{\tau}}^{(\tau)}, x_{2,1}^{(\tau)}, x_{2,2}^{(\tau)}, \dots, x_{2,i_{\tau}}^{(\tau)}$ независимо друг от друга пробегает все элементы полей $\mathbb{F}_{q^{\tau}}$ для $\tau = 1, 2, \dots, \nu$, то поляризованные элементарные симметрические многочлены u_{r_1, r_2} , $r_1, r_2 \geq 0$, $1 \leq r_1 + r_2 \leq \nu$, этих переменных пробегает все элементы соответствующих подмножеств $U_{i_1, \dots, i_{\nu}}^{(r_1, r_2)}$ поля $\mathbb{F}_q$ с кратностями $i_1! i_2! \dots i_{\nu}! 1^{i_1} 2^{i_2} \dots \nu^{i_{\nu}}$ соответственно. Следовательно, если мы ассоциируем каждый набор $(u_{r_1, r_2})_{1 \leq r_1+r_2 \leq \nu}$ элементарных симметрических многочленов u_{r_1, r_2} с $i_1! i_2! \dots i_{\nu}! 1^{i_1} 2^{i_2} \dots \nu^{i_{\nu}}$ (возможно, повторяющихся) наборами точек (12), то из (8), (9), (11) и (13) мы получаем

$$\beta_{\nu} = \sum_{i_1+2i_2+\dots+\nu i_{\nu}=\nu} (-1)^{i_1+i_2+\dots+i_{\nu}} \sum_{\substack{u_{r_1, r_2} \in U_{i_1, \dots, i_{\nu}}^{(r_1, r_2)} \\ 1 \leq r_1+r_2 \leq d}} \psi(f^*((u_{r_1, r_2})_{1 \leq r_1+r_2 \leq d})). \quad (14)$$

Далее используем специальную структуру многочленов $f^*((u_{r_1, r_2})_{1 \leq r_1 + r_2 \leq \nu})$. Поскольку ведущая однородная часть

$$f_d(x_1, x_2) = \sum_{d_1 + d_2 = d} a_{d_1, d_2} x_1^{d_1} x_2^{d_2}$$

многочлена $f(x_1, x_2)$ является неособой, то по меньшей мере один из двух её коэффициентов $a_{d, 0}$ и $a_{d-1, 1}$ (соответственно, $a_{0, d}$ и $a_{1, d-1}$) отличен от нуля. Далее, из предложения 2 следует, что многочлен

$$f^*((u_{r_1, r_2})_{1 \leq r_1 + r_2 \leq d}) = \sum_{\tau=1}^{\nu} \sum_{i=1}^{i_{\tau}} \sum_{k=0}^{\tau-1} \sigma_{\tau}^k(f(x_{1,i}^{(\tau)}, x_{2,i}^{(\tau)})) \in \mathbb{F}_q[(u_{r_1, r_2})_{1 \leq r_1 + r_2 \leq d}]$$

имеет вид

$$f^*((u_{r_1, r_2})_{1 \leq r_1 + r_2 \leq d}) = g^*((u_{r_1, r_2})_{1 \leq r_1 + r_2 \leq d-1}) + \sum_{\substack{r_1 + r_2 = d \\ r_1 \geq 0, r_2 \geq 0}} a_{r_1, r_2}^* u_{r_1, r_2},$$

где многочлен g^* зависит лишь от u_{r_1, r_2} , $1 \leq r_1 + r_2 \leq d-1$, $r_1, r_2 \geq 0$. Более того, если ведущая однородная часть $f_d(x_1, x_2)$ многочлена $f(x_1, x_2)$ содержит моном $x_1^{d_1} x_2^{d_2}$ с ненулевым коэффициентом a_{d_1, d_2} , то из предложения 2 следует, что линейная часть

$$l^*((u_{r_1, r_2})_{r_1 + r_2 = d}) = \sum_{\substack{r_1 + r_2 = d \\ r_1 \geq 0, r_2 \geq 0}} a_{r_1, r_2}^* u_{r_1, r_2}$$

многочлена $f^*((u_{r_1, r_2})_{1 \leq r_1 + r_2 \leq d})$ включает в себя соответствующий поляризованный элементарный симметрический многочлен u_{d_1, d_2} с ненулевым коэффициентом a_{r_1, r_2}^* . В результате мы получаем, что по меньшей мере один из двух коэффициентов $a_{d, 0}$ и $a_{d-1, 1}$ (соответственно, $a_{0, d}$ и $a_{1, d-1}$) линейного многочлена $l^*((u_{r_1, r_2})_{r_1 + r_2 = d})$ отличен от нуля. Для дальнейшего изложения удобно предположить, без уменьшения общности, что $a_{d, 0} \neq 0$ и $a_{0, d} \neq 0$. При таком предположении линейная часть $l^*((u_{r_1, r_2})_{r_1 + r_2 = d})$ многочлена $f^*((u_{r_1, r_2})_{1 \leq r_1 + r_2 \leq d})$ имеет вид

$$l^*((u_{r_1, r_2})_{r_1 + r_2 = d}) = a_{d, 0}^* u_{d, 0} + \sum_{\substack{r_1 + r_2 = d \\ 0 \leq r_1 < d, 0 \leq r_2 < d}} a_{r_1, r_2}^* u_{r_1, r_2} + a_{0, d}^* u_{0, d}.$$

Поскольку каждый элемент u_{r_1, r_2} системы (6) является однородным полилинейным многочленом от переменных $\sigma_{\tau}^k(x_{i, 1}^{(\tau)}), \sigma_{\tau}^k(x_{i, 2}^{(\tau)})$, для любого $\nu \geq (d-1)^2 + 1$ и любых заданных $\alpha_{r_1, r_2} \in \mathbb{F}_q$ при $2 \leq r_1 + r_2 \leq d-1$, $1 \leq r_1, r_2 \leq d-2$, эта система разрешима в элементах $\sigma_{\tau}^k(x_{i, 1}^{(\tau)}), \sigma_{\tau}^k(x_{i, 2}^{(\tau)}) \in \mathbb{F}_{q^{\tau}}$, $1 \leq \tau \leq \nu$. Более того, если неотрицательные целые $i_1, i_2, \dots, i_{\nu}$ пробегает все решения уравнения $i_1 + 2i_2 + \dots + \nu i_{\nu} = \nu$, а переменные $x_{1, 1}^{(\tau)}, x_{1, 2}^{(\tau)}, \dots, x_{1, i_{\tau}}^{(\tau)}, x_{2, 1}^{(\tau)}, x_{2, 2}^{(\tau)}, \dots, x_{2, i_{\tau}}^{(\tau)}$ независимо друг от друга пробегает все элементы полей $\mathbb{F}_{q^{\tau}}$ для $\tau = 1, 2, \dots, \nu$, то при любом $\nu \geq (d-1)^2 + 1$, любых фиксированных $u_{r_1, r_2} = \alpha_{r_1, r_2} \in \mathbb{F}_q$, $2 \leq r_1 + r_2 \leq d-1$, $r_1, r_2 \geq 1$, и любом фиксированном значении $\bar{l}_0^*$ линейного многочлена

$$\bar{l}^*((u_{r_1, r_2})_{r_1 + r_2 = d}) = \sum_{\substack{r_1 + r_2 = d \\ (r_1, r_2) \neq (d, 0), (0, d)}} a_{r_1, r_2}^* u_{r_1, r_2}$$

переменные $u_{1,0}, u_{2,0}, \dots, u_{d,0}; u_{0,1}, u_{0,2}, \dots, u_{0,d}$ независимо друг от друга пробегают все элементы поля $\mathbb{F}_q$. Теперь мы запишем многочлен

$$f(x_1, x_2) = \sum_{0 \leq d_1 + d_2 \leq d} a_{d_1, d_2} x_1^{d_1} x_2^{d_2}$$

в виде

$$f(x_1, x_2) = f_1(x_1) + f_2(x_2) + \sum_{\substack{2 \leq d_1 + d_2 \leq d \\ d_1 \geq 1, d_2 \geq 1}} a_{d_1, d_2} x_1^{d_1} x_2^{d_2},$$

где

$$f_1(x_1) = \sum_{d_1=0}^d a_{d_1, 0} x_1^{d_1}, \quad f_2(x_2) = \sum_{d_2=1}^d a_{0, d_2} x_2^{d_2},$$

а затем положим

$$T_{1,\mu} = \sum_{x_1 \in \mathbb{F}_q^\mu} \psi_\mu(f_1(x_1)), \quad T_{2,\mu} = \sum_{x_2 \in \mathbb{F}_q^\mu} \psi_\mu(f_2(x_2)), \quad 1 \leq \mu \leq \nu. \quad (15)$$

В результате указанной выше специализации переменных u_{r_1, r_2} , $2 \leq r_1 + r_2 \leq d - 1$, $r_1 \geq 1$, $r_2 \geq 1$, и линейного многочлена $\bar{l}^*((u_{r_1, r_2})_{r_1 + r_2 = d})$ мы получаем, что сумма в правой части соотношения (11) преобразуются в сумму вида

$$\begin{aligned} \bar{\beta}_\nu = c_\nu \sum_{i_1 + 2i_2 + \dots + \nu i_\nu = \nu} \frac{(-1)^{i_1 + i_2 + \dots + i_\nu}}{i_1! i_2! \dots i_\nu! 1^{i_1} 2^{i_2} \dots \nu^{i_\nu}} \\ \times (T_{1,1} T_{2,1})^{i_1} (T_{1,2} T_{2,2})^{i_2} \dots (T_{1,\nu} T_{2,\nu})^{i_\nu} \end{aligned} \quad (16)$$

с некоторой константой $c_\nu \in \mathbb{C}$.

Теперь мы покажем, что сумма в (16) равна нулю при каждом $\nu \geq (d-1)^2 + 1$. Для доказательства этого результата рассмотрим тригонометрические суммы (15) и соответствующие им порождающие функции

$$\begin{aligned} L_1(z) &= \exp\left(\sum_{\mu=1}^{\infty} \frac{T_{1,\mu}}{\mu} z^\mu\right) = 1 + \sum_{\mu=1}^{\infty} \beta_{1,\mu} z^\mu, \\ L_2(z) &= \exp\left(\sum_{\mu=1}^{\infty} \frac{T_{2,\mu}}{\mu} z^\mu\right) = 1 + \sum_{\mu=1}^{\infty} \beta_{2,\mu} z^\mu, \end{aligned} \quad (17)$$

где

$$\begin{aligned} \beta_{1,\mu} &= \sum_{i_1 + 2i_2 + \dots + \mu i_\mu = \mu} \frac{T_{1,1}^{i_1} T_{1,2}^{i_2} \dots T_{1,\mu}^{i_\mu}}{i_1! i_2! \dots i_\mu! 1^{i_1} 2^{i_2} \dots \mu^{i_\mu}} \\ &= \sum_{u_{1,0}, u_{2,0}, \dots, u_{\mu,0} \in \mathbb{F}_q} \psi(f_1^*(u_{1,0}, u_{2,0}, \dots, u_{\mu,0})), \end{aligned} \quad (18)$$

$$\begin{aligned} \beta_{2,\mu} &= \sum_{i_1 + 2i_2 + \dots + \mu i_\mu = \mu} \frac{T_{2,1}^{i_1} T_{2,2}^{i_2} \dots T_{2,\mu}^{i_\mu}}{i_1! i_2! \dots i_\mu! 1^{i_1} 2^{i_2} \dots \mu^{i_\mu}} \\ &= \sum_{u_{0,1}, u_{0,2}, \dots, u_{0,\mu} \in \mathbb{F}_q} \psi(f_2^*(u_{0,1}, u_{0,2}, \dots, u_{0,\mu})). \end{aligned} \quad (19)$$

Используя результаты автора (см. [3, гл. I, § 3]), касающиеся структуры функций $L_1(z)$, $L_2(z)$, мы получаем

$$\beta_{1,\mu} = 0, \quad \beta_{2,\mu} = 0 \quad \forall \mu > d-1 \quad (20)$$

и, как следствие, приходим к соотношениям

$$\begin{aligned} L_1(z) &= 1 + \beta_{1,1}z + \dots + \beta_{1,d-1}z^{d-1} = \prod_{k=1}^{d-1} (1 - \omega_{1,k}z), \quad \omega_{1,k} \in \mathbb{C}, \\ L_2(z) &= 1 + \beta_{2,1}z + \dots + \beta_{2,d-1}z^{d-1} = \prod_{l=1}^{d-1} (1 - \omega_{2,l}z), \quad \omega_{2,l} \in \mathbb{C}. \end{aligned} \quad (21)$$

Далее, из (17) и (21) имеем

$$\begin{aligned} \sum_{\mu=1}^{\infty} \frac{T_{1,\mu}}{\mu} z^{\mu} &= \sum_{k=1}^{d-1} \log(1 - \omega_{1,k}z) = - \sum_{\mu=1}^{\infty} \left(\sum_{k=1}^{d-1} \omega_{1,k}^{\mu} \right) \frac{z^{\mu}}{\mu}, \\ \sum_{\mu=1}^{\infty} \frac{T_{2,\mu}}{\mu} z^{\mu} &= \sum_{l=1}^{d-1} \log(1 - \omega_{2,l}z) = - \sum_{\mu=1}^{\infty} \left(\sum_{l=1}^{d-1} \omega_{2,l}^{\mu} \right) \frac{z^{\mu}}{\mu} \end{aligned}$$

и, следовательно,

$$T_{1,\mu} = - \sum_{i=1}^{d-1} \omega_{1,i}^{\mu}, \quad T_{2,\mu} = - \sum_{k=1}^{d-1} \omega_{2,k}^{\mu}. \quad (22)$$

В результате мы можем переписать (16) в виде

$$\bar{\beta}_{\nu} = c_{\nu} \sum_{i_1+2i_2+\dots+\nu i_{\nu}=\nu} \frac{(-1)^{i_1+i_2+\dots+i_{\nu}}}{i_1! i_2! \dots i_{\nu}! 1^{i_1} 2^{i_2} \dots \nu^{i_{\nu}}} \prod_{\mu=1}^{\nu} \left(\sum_{k=1}^{d-1} \omega_{1,k}^{\mu} \right)^{i_{\mu}} \left(\sum_{l=1}^{d-1} \omega_{2,l}^{\mu} \right)^{i_{\mu}}.$$

Наконец, учитывая (18)–(20) и (22), приходим к соотношениям

$$\bar{\beta}_{\nu} = 0 \quad \forall \nu \geq (d-1)^2 + 1,$$

которые означают, что

$$\beta_{\nu} = \sum_{i_1+2i_2+\dots+\nu i_{\nu}=\nu} (-1)^{i_1+i_2+\dots+i_{\nu}} \sum_{u_{r_1}, r_2 \in U_{i_1, i_2, \dots, i_{\nu}}^{(r_1, r_2)}} \psi(f^*((u_{r_1}, r_2)_{1 \leq r_1+r_2 \leq d})) = 0$$

для всех $\nu \geq (d-1)^2 + 1$. Этот результат доказывает теорему 1.

В заключение автор выражает свою искреннюю признательность рецензенту за ряд ценных замечаний и советов.

Список литературы

1. E. Artin, “Quadratische Körper im Gebiete der höheren Kongruenzen. I, II”, *Math. Zeitschr.*, **19**:1 (1924), 153–246.
2. A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris, 1948.

3. С. А. Степанов, *Арифметика алгебраических кривых*, Мир, М., 1991; англ. пер.: S. A. Stepanov, *Arithmetic of algebraic curves*, Monogr. Contemp. Math., Consultants Bureau, New York, 1994.
4. A. Grothendieck, “Formule de Lefschetz et rationalité des fonctions L ”, *Séminaire Bourbaki*, v. 9, Exp. No. 279, Soc. Math. France, Paris, 1966, 41–55.
5. Е. Бомбьери, “Об экспоненциальных суммах в конечных полях”, *Математика: Сб. пер.*, **12**:2, Мир, М., 1968, 58–87; пер. с англ.: Е. Bombieri, “On exponential sums in finite fields”, *Amer. J. Math.*, **88** (1966), 71–105.
6. A. Weil, “Number of solutions of equations in finite fields”, *Bull. Amer. Math. Soc.*, **55** (1949), 497–508.
7. П. Делинь, “Гипотеза Вейля. I”, *УМН*, **30**:5 (1975), 159–190; пер. с фр.: P. Deligne, “La conjecture de Weil. I”, *Inst. Hautes Etudes Sci. Publ. Math.*, **43**:1 (1974), 273–307.
8. Г. И. Перельмутер, “Оценка многократной суммы с символом Лежандра”, *Матем. заметки*, **18**:3 (1975), 421–427; англ. пер.: G. I. Perel'muter, “Estimate of a multiple sum involving the legendre symbol”, *Math. Notes*, **18**:3 (1975), 840–844.
9. D. Hilbert, “Ueber die vollen Invariantensysteme”, *Math. Ann.*, **42**:3 (1893), 313–373.
10. E. Noether, “Der Endlichkeitssatz der Invarianten endlicher Gruppen”, *Math. Ann.*, **77**:1 (1916), 89–92.
11. H. Weyl, *The classical groups, their invariants and representations*, Princeton Univ. Press, Princeton, NJ, 1946.
12. E. Noether, “Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p ”, *Nachr. Ges. Wiss. Göttingen*, 1926, 28–35.
13. D. R. Richman, “Explicit generators of the invariants of finite groups”, *Adv. Math.*, **124**:1 (1996), 49–76.
14. С. А. Степанов, “Полиномиальные инварианты конечных групп над полями простой характеристики”, *Дискрет. матем.*, **11**:3 (1999), 3–14; англ. пер.: S. A. Stepanov, “Polynomial invariants of finite groups over fields of prime characteristics”, *Discr. Math. Appl.*, **9**:4 (1999), 343–354.
15. E. Waring, *Mediationes algebraicae*, Cambridge Univ. Press, Cambridge, 1782.
16. Дж. Риордан, *Введение в комбинаторный анализ*, ИЛ, М., 1969; пер. с англ.: J. Riordan, *An introduction to combinatorial analysis*, Wiley, New York, 1958.

СЕРГЕЙ АЛЕКСАНДРОВИЧ СТЕПАНОВ

(SERGEI A. STEPANOV)

Институт проблем передачи информации

им. А. А. Харкевича РАН, г. Москва

E-mail: sa-stepanov@iitp.ru

Поступило в редакцию

05.04.2012

07.12.2012