Math-Net.Ru

Общероссийский математический портал

С. А. Степанов, Метод орбитальных сумм в теории модулярных векторных инвариантов, *Матем. сб.*, 2006, том 197, номер 11, 79–114

DOI: <https://doi.org/10.4213/sm3787>

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: 54.205.225.156

26 апреля 2023 г., 11:23:21

УДК 511

С. А. Степанов

Метод орбитальных сумм в теории модулярных векторных инвариантов

Пусть F – произвольное поле, V – конечномерное векторное пространство над полем F , $G \leq \mathrm{GL}_F(V)$ – конечная группа и $V^m = V \oplus \dots \oplus V$ – прямая сумма m копий пространства V с диагональным действием на ней группы G . Группа G естественным образом действует на градуированной симметрической алгебре $A_m = F[V^m]$ как группа невырожденных линейных преобразований переменных. Пусть A_m^G – подалгебра инвариантов полиномиальной алгебры A_m относительно действия группы G . Классический результат Нётер [1] гласит, что если $\mathrm{char} F = 0$, то F -алгебра A_m^G порождается однородными многочленами степени не выше $|G|$ независимо от того, как велико m . С другой стороны, из работ Ричмана [2], [3] следует, что указанный результат неверен в случае, когда характеристика поля F положительна и делит порядок $|G|$ группы G . Пусть $p > 2$ – простое число, $F = F_p$ – конечное поле из p элементов, V – линейное пространство размерности n над полем F_p и $H \leq \mathrm{GL}_{F_p}(V)$ – циклическая группа порядка p , порожденная матрицей γ некоторого специального вида. В настоящей работе дается явная конструкция (теорема 1) одной из полных систем порождающих элементов алгебры A_m^H . Затем для произвольной полной системы порождающих элементов этой алгебры указывается нижняя граница для наибольшей степени входящих в эту систему многочленов. Это приводит к существенному обобщению соответствующего результата Кэмпбелла и Хагеса [4], полученного авторами в весьма частном случае, когда $n = 2$. В качестве следствия доказывается (теорема 3), что если $m > n$ и $G \geq H$ – произвольная конечная группа, то каждая полная система порождающих элементов алгебры A_m^G содержит по меньшей мере один многочлен степени не ниже чем $2(m - n + 2r)(p - 1)/r$, где $r = r(H)$ – некоторое положительное целое число, зависящее от структуры порождающей матрицы γ группы H . Этот результат существенно улучшает нижнюю границу, полученную ранее Ричманом [3].

Библиография: 13 названий.

Введение

Пусть m, n – положительные целые числа, R – коммутативное кольцо с единицей и

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

– алгебра многочленов от mn переменных x_{ij} над кольцом R . Симметрическая группа S_n действует на A_{mn} как группа R -автоморфизмов по правилу $\sigma(x_{ij}) = x_{i, \sigma(j)}$, $\sigma \in S_n$. Обозначим через $A_{mn}^{S_n}$ подалгебру инвариантов алгебры A_{mn} по отношению к действию группы S_n и определим поляризованные

элементарные симметрические многочлены $u_{r_1, \dots, r_m} \in A_{mn}^{S_n}$ от n векторных переменных $(x_{11}, \dots, x_{m1}), \dots, (x_{1n}, \dots, x_{mn})$ с помощью следующего формального тождества:

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

Обычно элементы алгебры $A_{mn}^{S_n}$ называются *векторными инвариантами* группы S_n . Если R – нётерово кольцо, то из теоремы конечности Гильберта–Нётер [1], [5], [6] следует, что $A_{mn}^{S_n}$ является конечно порожденной коммутативной R -алгеброй, а исходная алгебра A_{mn} является конечно порожденным модулем над $A_{mn}^{S_n}$. Кроме того, если каждое отличное от нуля целое число обратимо в кольце R , теорема Вейля [7] утверждает, что инварианты $u_{r_1, \dots, r_m}$ образуют полную систему порождающих элементов алгебры $A_{mn}^{S_n}$ над кольцом R . Другими словами, каждый инвариант $u \in A_{mn}^{S_n}$ может быть записан в виде многочлена от $u_{r_1, \dots, r_m}$, $1 \leq r_1 + \dots + r_m \leq n$, с коэффициентами из кольца R . Последний результат был недавно усилен Ричманом [3] и автором [8] следующим образом: *если порядок $|S_n| = n!$ группы S_n обратим в кольце R , то $A_{mn}^{S_n}$ порождается как R -алгебра поляризованными элементарными симметрическими многочленами $u_{r_1, \dots, r_m}$, $1 \leq r_1 + \dots + r_m \leq n$, степени не выше чем n .*

Пусть $A = R[x_1, \dots, x_N]$ – конечно порожденная коммутативная R -алгебра, G – конечная группа автоморфизмов алгебры A над R и A^G – подалгебра инвариантов алгебры A относительно действия группы G . Если $z_1, \dots, z_N$ – коммутирующие переменные, положим

$$P(z_1, \dots, z_N) = \prod_{\sigma \in G} (1 + \sigma(x_1)z_1 + \sigma(x_2)z_2 + \dots + \sigma(x_N)z_N)$$

и определим $\beta(A^G)$ как наименьшее целое положительное число β такое, что A^G порождается над кольцом R многочленами степени не выше чем β . Если каждое ненулевое целое число обратимо в кольце R , то классический результат Нётер [1] утверждает, что алгебра A^G порождается над R коэффициентами многочлена $P(z_1, \dots, z_N)$. Отсюда следует неравенство $\beta(A^G) \leq |G|$, известное в литературе как *верхняя граница Нётер*. Приведенный выше результат Ричмана и автора, а также некоторые дополнительные соображения, основанные на использовании оператора Рейнольдса и отображения Нётер [9], обеспечивают выполнение неравенства $\beta(A^G) \leq |G|$ при условии, что целое число $|G|!$ обратимо в R . Недавний результат Флейшмана [10] показывает, что на самом деле последнее неравенство справедливо и при более слабом условии, что порядок $|G|$ группы G обратим в кольце R .

Пусть $R = F$ – произвольное поле и G – конечная группа, действующая линейно на векторном пространстве V размерности n над полем F . Если характеристика поля F положительна и делит порядок $|G|$ группы G , то мы говорим о *модулярном случае*. При выполнении противоположных условий мы имеем

немодулярный случай, включающий в себя классический случай полиномиальных инвариантов над алгебраически замкнутым полем характеристики нуль. Заметим, что практически весь арсенал идей и методов, используемых в немодулярном случае, перестает работать в модулярном случае, а именно, в модулярном случае, вообще говоря, не выполняется свойство Коэна–Маколея, мы не имеем операторов Рейнольдса (усреднений по группе G), а также не имеем формулы Молина для производящих рядов Пуанкаре. Тем не менее, если F – поле простой характеристики p и H – некоторая p -подгруппа группы G , в модулярном случае возможно интенсивное использование *обобщенных орбитальных классов Черна* для группы H , в частности орбитальных следов (*орбитальных сумм мономов*) и норменных орбитальных классов Черна (*орбитальных норм мономов*). Пусть $F = F_p$ – простое конечное поле и $H \leq \mathrm{GL}(n, F_p)$ – циклическая группа простого порядка p , действующая линейно на пространстве V . Положим $A_{mn} = F_p[V^m]$ и обозначим через A_{mn}^H подалгебру векторных инвариантов алгебры A_{mn} относительно действия группы H . В настоящей работе показывается (теоремы 5, 8 и 16), что существуют линейное пространство $\tilde{V}$ над F_p , содержащее V в качестве собственного подпространства, а также циклическая группа $\tilde{H}$ порядка p , действующая линейно на $\tilde{V}$, которые обладают тем свойством, что каждый инвариант $u \in A_{mn}^H$ может быть представлен в виде некоторой F_p -линейной комбинации орбитальных сумм $S_{\tilde{H}}(f)$ и орбитальных норм $N_{\tilde{H}}(f)$ для различных мономов $f \in A_{mn}$. Указанный факт дает совершенно новую точку зрения в теории модулярных инвариантов, выявляющую основополагающую роль p -подгрупп H группы G и соответствующих им орбитальных классов Черна. Следует отметить, что если H – циклическая группа простого порядка p и $F = F_p$ – простое конечное поле из p элементов, то $S_{\tilde{H}}(f)$ и $N_{\tilde{H}}(f)$ легко могут быть вычислены в явном виде, что приводит к явному построению полной системы порождающих элементов алгебры A_{mn}^H . Заметим также, что из соотношения $A_{mn}^G \subseteq A_{mn}^H$ вытекает, что структура алгебры A_{mn}^G во многих аспектах определяется структурой алгебры A_{mn}^H .

Наиболее значительным различием между модулярным и немодулярным случаями является то, что в модулярном случае граница Нётер перестает быть верной. В частности, если $l \leq n$ и α – положительные целые числа, F – поле простой характеристики p и $G = S_n$ – симметрическая группа степени n , то справедлив следующий результат (Кемпер [11], С. А. Степанов [8]): *если p^α делит l , то каждая полная система порождающих элементов F -алгебры $A_{mn}^{S_n}$ содержит многочлен степени не ниже чем $\max\{n, m(p^\alpha - 1)\}$* . Отсюда следует, в частности, что если $R = \mathbb{Z}$ – кольцо целых рациональных чисел, то каждая полная система порождающих элементов R -алгебры $A_{mn}^{S_n}$ содержит многочлен, степень которого не меньше чем $\max\{n, m(n-1)/2\}$. Приведенные результаты показывают, что наличие верхней границы Нётер для степеней многочленов, образующих полную систему порождающих элементов R -алгебры $A_{mn}^{S_n}$, существенно зависит от арифметической структуры кольца R . Как недавно было показано Флейшманом [12], указанная выше нижняя граница $\max\{n, m(p^\alpha - 1)\}$ для наибольшей из степеней многочленов, образующих полную систему порож-

дающих элементов алгебры $A_{mn}^{S_n}$, является точной. Именно, для любого целого $m > 1$ и любого целого $n > 1$, являющегося степенью $n = p^\alpha$ простого числа p , было установлено, что $\beta(A_{mn}^{S_n}) \leq \max\{n, m(n-1)\}$. Заметим, что последнее неравенство может быть рассмотрено как некоторое уточнение в весьма специальной ситуации верхней границы $\beta(A_{mn}^{S_n}) \leq \max\{n, mn(n-1)/2\}$, полученной Кемпбеллом, Хагесом и Поллаком [13] для общего случая полиномиальной алгебры A_{mn} над произвольным коммутативным кольцом R .

Пусть m, n – положительные целые числа, $p > 2$ – простое число, $F = F_p$ – конечное поле из p элементов и $V = F_p x_1 + \dots + F_p x_n$ – векторное пространство над F_p размерности $n \geq 2$. Пусть $G \leq \text{GL}(n, F_p)$ – конечная группа, порядок которой делится на p , и $H = \langle \gamma \rangle$ – ее циклическая подгруппа порядка p . Будем считать, что порождающая матрица γ группы H представлена в канонической жордановой форме

$$\gamma = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_s \end{pmatrix}.$$

В рассматриваемой нами ситуации размеры $n_1, \dots, n_s$ базовых жордановых блоков $J_1, \dots, J_s$ матрицы γ удовлетворяют условиям $1 \leq n_i \leq p$ для всех $1 \leq i \leq n$, а также условиям

$$n_1 + n_2 + \dots + n_s = n \quad \text{и} \quad n_1 \cdot \dots \cdot n_s \geq 2.$$

Без уменьшения общности будем считать, что

$$p \geq n_1 \geq n_2 \geq \dots \geq n_r \geq 2 \quad \text{и} \quad n_{r+1} = \dots = n_s = 1.$$

Пусть A_{mn}^G – алгебра векторных инвариантов полиномиальной алгебры

$$A_{mn} = F_p[V^m] = F_p[x_{11}, \dots, x_{m1}; \dots; x_{1n}, \dots, x_{mn}]$$

относительно действия на ней группы G . Если $n_1 = \dots = n_r = 2$ и $n_{r+1} = \dots = n_s = 1$, положим

$$N_H^{(0)}(x_{i,2\tau-1}) = \prod_{\alpha \in F_p} \left(x_{i,2\tau-1} + \binom{\alpha}{1} x_{i,2\tau} \right) = x_{i,2\tau-1}^p - x_{i,2\tau-1} x_{i,2\tau}^{p-1},$$

где $1 \leq i \leq m$, $1 \leq \tau \leq r$, и

$$S_H^{(0)}(f) = \sum_{\alpha \in F_p} \prod_{i=1}^m \prod_{\tau=1}^r \left(x_{i,2\tau-1} + \binom{\alpha}{1} x_{i,2\tau} \right)^{s_{i,\tau p-1}},$$

где

$$f = \prod_{i=1}^m \prod_{\tau=1}^r x_{i,2\tau-1}^{s_{i,2\tau-1}}$$

– некоторый моном от переменных $x_{i,2\tau-1}$, $1 \leq i \leq m$, $1 \leq \tau \leq r$. Далее, если (i_1, j_1) и (i_2, j_2) – две различные пары положительных целых чисел, мы запишем

$$(i_1, j_1) \prec (i_2, j_2) \quad \Leftrightarrow \quad i_1 < i_2 \quad \text{или} \quad i_1 = i_2 \text{ и } j_1 < j_2.$$

В настоящей работе дается дальнейшее развитие идей работы автора [8] и доказывается следующий результат.

ТЕОРЕМА 1. Пусть $H \leq \text{GL}(n, F_p)$ – циклическая группа простого порядка p , порожденная матрицей γ . Если $n \geq 2$ и размеры $n_1, \dots, n_s$ базовых жордановых блоков $J_1, \dots, J_s$ матрицы γ удовлетворяют условиям

$$n_1 = \dots = n_r = 2 \quad \text{и} \quad n_{r+1} = \dots = n_s = 1,$$

то

$$A_{mn}^H = F_p[x_{i,2\tau}, x_{ij}, N_H^{(0)}(x_{i,2\tau-1}), (x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1}), S_H^{(0)}(f')],$$

где $1 \leq i \leq m$, $1 \leq \tau \leq r$, $2r+1 \leq j \leq s$, $1 \leq i_1, i_2 \leq m$, $1 \leq \tau_1, \tau_2 \leq r$, $(i_1, \tau_1) \prec (i_2, \tau_2)$, а f' пробегает множество всех мономов f указанного выше вида таких, что $0 \leq s_{i,2\tau-1} \leq p-1$.

В качестве легкого следствия теоремы 1 мы получаем следующий результат, дающий нижнюю границу для максимальной степени многочленов, образующих произвольную полную систему порождающих элементов алгебры A_{mn}^H .

СЛЕДСТВИЕ 2. Если в дополнение к сказанному выполняется условие $mr > 2$, то каждая полная система порождающих элементов алгебры A_{mn}^H содержит многочлен степени не ниже чем $mr(p-1)$.

Если G – произвольная конечная группа, содержащая H в качестве подгруппы, то для каждой полной системы порождающих элементов соответствующей полиномиальной алгебры A_{mn}^G мы также в состоянии указать нижнюю границу для максимальной степени входящих в нее многочленов.

ТЕОРЕМА 3. Пусть $G \leq \text{GL}(n, F_p)$ – конечная группа, порядок которой делится на характеристику $p > 2$ поля F_p , и $H = \langle \gamma \rangle$ – циклическая подгруппа группы G простого порядка p . Если $m > n \geq 2$ и размеры $n_1, \dots, n_s$ базовых жордановых блоков $J_1, \dots, J_s$ матрицы γ удовлетворяют условиям

$$n_1 = \dots = n_r = 2 \quad \text{и} \quad n_{r+1} = \dots = n_s = 1,$$

то каждая полная система порождающих элементов F_p -алгебры $A_{mn}^G = F_p[V^m]^G$ содержит многочлен степени не ниже чем $(m-n+2r)(p-1)/r$.

Теорема 1 дает явное описание системы порождающих элементов алгебры A_{mn}^H в терминах орбитальных сумм и орбитальных норм мономов. Весьма

правдоподобно, что нижняя граница, указанная в следствии 2, является точной. Теорема 3 значительно усиливает нижнюю оценку

$$\max \left\{ 2, \frac{m}{n-1}, \frac{m}{|G|-1}, \frac{mp}{n(p-1)} \right\},$$

полученную ранее Ричманом [3]. Случай $r = 1$ изучался Ричманом [2] (в случае $p = 2$), в также Кэмпбеллом и Хагесом [4] (в случае $p > 2$). Аргументы, используемые в настоящей работе, существенно отличаются от аргументов, использованных в работах указанных выше авторов. В частности, все рассмотренные в работе конструкции основаны лишь на изучении орбитальных классов Черна, без привлечения каких-либо глубоких фактов из теории представлений конечных групп или комбинаторного анализа. Случай

$$p \geq n_1 \geq \dots \geq n_\sigma \geq 3,$$

где $1 \leq \sigma \leq s$, требует значительно более сложных вычислений и будет рассмотрен позже. Следует также заметить, что полученные в работе результаты могут быть легко перенесены на случай произвольного поля простой характеристики p .

Наконец, разъясним кратко основные идеи, лежащие в основе доказательств теорем 1 и 3. Использование орбитальных сумм

$$S_G(f) = \sum_{w \in \{\sigma(f) | \sigma \in G\}} w,$$

где $f \in A_{mn}$ – некоторый моном, наиболее эффективно в том случае, когда группа G действует на элементы R -алгебры A_{mn} как группа перестановок векторных переменных $x_j = (x_{1j}, x_{2j}, \dots, x_{mj})$ для $j = 1, 2, \dots, n$. В этом случае каждый инвариант $u \in A_{mn}^G$ является R -линейной комбинацией указанных выше орбитальных сумм для всевозможных мономов f . Этот важный результат является следствием того факта, что если некоторый моном f входит в инвариант u с ненулевым коэффициентом a , то для каждого $\sigma \in G$ соответствующий моном $\sigma(f)$ также входит в u с тем же самым коэффициентом a . К сожалению, указанное свойство орбитальных сумм перестает быть верным для конечных групп более общего вида. В частности, это свойство отсутствует в случае циклических групп H , порожденных матрицами вида

$$\gamma = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_s \end{pmatrix},$$

где размеры $n_1, n_2, \dots, n_s$ базовых жордановых блоков $J_1, J_2, \dots, J_s$ таковы, что $2 < n_i < p$ хотя бы для одного $i = 1, 2, \dots, s$. С другой стороны, если рассматриваемые размеры удовлетворяют условиям $n_1 = n_2 = \dots = n_r = p$ и

$n_{r+1} = \dots n_s = 1$, то с помощью некоторого невырожденного линейного преобразования мы можем перейти к некоторой новой системе векторных переменных $\tilde{x}_j = (\tilde{x}_{1j}, \tilde{x}_{2j}, \dots, \tilde{x}_{mj})$, $1 \leq j \leq n$, на которой группа H действует в виде циклических перестановок.

Пусть H – циклическая группа простого порядка $p > 2$, порожденная невырожденной квадратной матрицей γ с жордановыми блоками $J_1, J_2, \dots, J_s$ размеров $n_1, n_2, \dots, n_s$ соответственно. Предположим, что $n_1 = n_2 = \dots = n_r = 2$, $n_{r+1} = \dots = n_s = 1$, и напомним, что группа H действует линейно на векторном пространстве V^m размерности $m(r+s)$. Доказательство теоремы 1 состоит из следующих двух этапов.

(i) На первом этапе каждый блок J_i , $1 \leq i \leq r$, размера $n_i = 2$ матрицы γ расширяется до жорданова блока максимально возможного размера p . При этом порождающая матрица γ группы H преобразуется в соответствующую квадратную матрицу $\tilde{\gamma}$ размера $\nu = (p-1)r + s$, а группа H – в соответствующую циклическую группу $\tilde{H}$, порожденную матрицей $\tilde{\gamma}$ и действующую на векторном пространстве $\tilde{V}^m$ размерности $m\nu$. Из сказанного выше следует, что в этом случае возможно найти такие новые векторные переменные $\tilde{x}_j = (\tilde{x}_{1j}, \tilde{x}_{2j}, \dots, \tilde{x}_{mj})$, $1 \leq j \leq \nu$, получающиеся из исходных переменных $x_j = (x_{1j}, x_{2j}, \dots, x_{mj})$ при помощи некоторого невырожденного линейного преобразования, на которые группа $\tilde{H}$ действует в виде их циклических перестановок. Это свойство группы $\tilde{H}$ дает возможность установить (теорема 5), что каждый инвариант v алгебры $A_{m\nu}^{\tilde{H}}$ является F_p -линейной комбинацией орбитальных норм $N_{\tilde{H}}(f)$ и орбитальных сумм $S_{\tilde{H}}(f)$ для всевозможных мономов $f \in A_{m\nu}$.

(ii) На втором этапе показывается, что надлежащее вложение алгебры A_{mn} в алгебру $A_{\nu\nu}$ приводит к весьма простому критерию (теорема 8), позволяющему выяснять, какие из многочленов $v \in A_{m\nu}^{\tilde{H}}$, инвариантных относительно действия группы $\tilde{H}$, являются в то же время полиномиальными инвариантами по отношению к действию группы H . Использование этого критерия открывает возможность для явной конструкции инвариантов $u \in A_{mn}^H$ в виде F_p -линейных комбинаций орбитальных норм $N_{\tilde{H}}(f)$ и орбитальных сумм $S_{\tilde{H}}(f)$ специального вида.

Идея доказательства теоремы 3 состоит в следующем. Так как $A_{mn}^G \subseteq A_{mn}^H$, то система порождающих элементов алгебры A_{mn}^H , указанная в теореме 1, содержит соответствующую систему порождающих элементов алгебры A_{mn}^G . Для доказательства того, что последняя система содержит хотя бы один многочлен достаточно высокой степени, мы показываем, что некоторый многочлен $f_0 \in A_{mn}$ весьма специального вида, инвариантный относительно действия любой подгруппы полной линейной группы $\text{GL}(F_p, n)$ (см. §4), не может быть представлен не только в виде многочлена над полем F_p от элементов упомянутой выше системы порождающих полиномов алгебры A_{mn}^G , имеющих не слишком высокую степень, но даже в виде многочлена над F_p от аналогичных элементов более широкой системы порождающих полиномов алгебры A_{mn}^H .

§ 1. Орбитальные суммы

Пусть m, n – положительные целые числа, $p \geq 3$ – простое число, F_p – простое конечное поле из p элементов, $\text{GL}(n, F_p)$ – группа обратимых $(n \times n)$ -матриц с элементами из поля F_p и

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

– алгебра многочленов от коммутирующих переменных $x_{11}, \dots, x_{m1}; \dots; x_{1n}, \dots, x_{mn}$ с коэффициентами из F_p . Всюду в дальнейшем элементы поля F_p идентифицируются с элементами множества $\{0, 1, \dots, p-1\}$. Если $g \in A_{mn}$ и

$$\sigma = \begin{pmatrix} \sigma_{11} & \sigma_{12} & \dots & \sigma_{1n} \\ \sigma_{21} & \sigma_{22} & \dots & \sigma_{2n} \\ \dots & \dots & \dots & \dots \\ \sigma_{n1} & \sigma_{n2} & \dots & \sigma_{nn} \end{pmatrix}$$

– элемент группы $\text{GL}(n, F_p)$, обозначим через $\sigma(g)$ образ многочлена g относительно эндоморфизма σ , действующего на базисные элементы $x_{i1}, \dots, x_{in}$ векторных пространств $V_i = F_p x_{i1} + F_p x_{i2} + \dots + F_p x_{in}$, $1 \leq i \leq m$, по правилу

$$\begin{pmatrix} \sigma(x_{i1}) \\ \sigma(x_{i2}) \\ \dots \\ \sigma(x_{in}) \end{pmatrix} = \sigma \begin{pmatrix} x_{i1} \\ x_{i2} \\ \dots \\ x_{in} \end{pmatrix} = \begin{pmatrix} \sigma_{11}x_{i1} + \dots + \sigma_{1n}x_{in} \\ \sigma_{21}x_{i1} + \dots + \sigma_{2n}x_{in} \\ \dots \\ \sigma_{n1}x_{i1} + \dots + \sigma_{nn}x_{in} \end{pmatrix}.$$

Пусть G – подгруппа группы $\text{GL}(n, F_p)$ и A_{mn}^G – множество многочленов $u \in A_{mn}$ таких, что $\sigma(u) = u$ для каждого $\sigma \in G$. Множество A_{mn}^G образует подалгебру алгебры A_{mn} , которая называется *алгеброй векторных инвариантов* группы G .

Пусть p – простой делитель числа $|G|$ и $H = \langle \gamma \rangle$ – циклическая подгруппа группы G порядка p . Матрица γ может быть представлена в канонической жордановой форме

$$\gamma = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_s \end{pmatrix},$$

где базовые жордановы блоки

$$J_\rho = \begin{pmatrix} 1 & 1 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

суть квадратные матрицы размеров $n_1, n_2, \dots, n_s$ с условиями

$$n_1 + n_2 + \dots + n_s = n \quad \text{и} \quad 1 \leq n_\rho \leq p$$

для всех $\rho = 1, 2, \dots, s$. Без уменьшения общности можем предположить, что

$$n_1 \geq n_2 \geq \dots \geq n_r \geq 2 \quad \text{и} \quad n_{r+1} = \dots = n_s = 1.$$

Пусть A_{mn}^H – подалгебра многочленов $u \in A_{mn}$, инвариантных относительно действия циклической группы $H = \langle \gamma \rangle$. Нашей целью является явное описание всех элементов алгебры A_{mn}^H . Пусть

$$A_{m,2r} = F_p[x_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq 2r],$$

и пусть $A_{m,2r}^H$ – подалгебра инвариантов алгебры $A_{m,2r}$ относительно действия группы H . Так как переменные x_{ij} , $1 \leq i \leq m$, $2r+1 \leq j \leq n$, инвариантны относительно действия группы H , то каждый инвариант $u \in A_{mn}^H$ является многочленом вида

$$u = u_1 f_1 + u_2 f_2 + \dots + u_l f_l,$$

где $u_k \in A_{m,2r}^H$, а f_k , $1 \leq k \leq l$, суть мономы от переменных x_{ij} , $1 \leq i \leq m$, $2r+1 \leq j \leq n$. Отсюда следует, что изучение инвариантов u алгебры A_{mn}^H сводится к изучению инвариантов $u_k \in A_{m,2r}^H$. Стало быть, без уменьшения общности мы можем предположить, что $n = 2r$, $u \in A_{m,2r}$ и

$$\gamma = \begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_r \end{pmatrix},$$

где $J_1, J_2, \dots, J_r$ – базовые жордановы блоки размеров $n_1, n_2, \dots, n_r$ соответственно, причем

$$n = n_1 + n_2 + \dots + n_r \quad \text{и} \quad p \geq n_1 \geq n_2 \geq \dots \geq n_r \geq 2. \quad (1)$$

Положим $\nu = rp$ и расширим каждый из жордановых блоков $J_l, \dots, J_r$ матрицы γ до жорданова блока

$$\tilde{J} = \begin{pmatrix} 1 & 1 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$$

размера p . В результате матрица γ преобразуется в квадратную $(\nu \times \nu)$ -матрицу

$$\tilde{\gamma} = \begin{pmatrix} \tilde{J} & & & \\ & \tilde{J} & & \\ & & \ddots & \\ & & & \tilde{J} \end{pmatrix},$$

действующую одним и тем же образом на каждом из векторных пространств

$$\tilde{V}_i = F_p z_{i1} + F_p z_{i2} + \dots + F_p z_{i\nu}, \quad i = 1, 2, \dots, m,$$

в виде невырожденных линейных преобразований. Обозначим через $\tilde{H}$ циклическую группу порядка p , порожденную матрицей $\tilde{\gamma}$, и заметим, что действие группы $\tilde{H}$ на векторных пространствах $\tilde{V}_i$, $i = 1, 2, \dots, m$, может быть рассмотрено как некоторое расширение действия группы H на соответствующих векторных подпространствах V_i пространств $\tilde{V}_i$, $i = 1, 2, \dots, m$, до ее действия на $\tilde{V}_i$. Если

$$A_{m\nu} = F_p[z_{11}, \dots, z_{m1}; \dots; z_{1\nu}, \dots, z_{m\nu}]$$

– алгебра многочленов над F_p от коммутирующих переменных $z_{11}, \dots, z_{1n}; \dots; z_{1\nu}, \dots, z_{m\nu}$, то каждый элемент $\tilde{\sigma}$ группы $\tilde{H}$ задает соответствующий эндоморфизм алгебры $A_{m\nu}$ над F_p . Пусть $A_{m\nu}^{\tilde{H}}$ означает подалгебру инвариантов полиномиальной алгебры $A_{m\nu}$ относительно действия группы $\tilde{H}$. Если $f \in A_{m\nu}$ – некоторый моном, обозначим через

$$\text{Orb}_{\tilde{H}}(f) = \{\tilde{\sigma}(f) \mid \tilde{\sigma} \in \tilde{H}\}$$

его орбиту относительно действия группы $\tilde{H}$. Положим $q = |\text{Orb}_{\tilde{H}}(f)|$ и заметим, что либо $q = 1$, либо $q = p$. Далее, выражения

$$N_{\tilde{H}}(f) = \prod_{g \in \text{Orb}_{\tilde{H}}(f)} g \quad \text{и} \quad S_{\tilde{H}}(f) = \sum_{g \in \text{Orb}_{\tilde{H}}(f)} g$$

назовем *орбитальной нормой* и *орбитальной суммой* монома f относительно группы $\tilde{H}$. Ясно, что $N_{\tilde{H}}(f)$ и $S_{\tilde{H}}(f)$ являются инвариантами группы $\tilde{H}$. Заметим также, что $N_{\tilde{H}}(f)$ и $S_{\tilde{H}}(f)$ являются однородными многочленами алгебры $A_{m\nu}$. Опишем теперь все элементы алгебры $A_{m\nu}$, которые инвариантны относительно действия циклической группы $\tilde{H}$. Сначала мы докажем следующий арифметический результат.

ЛЕММА 4. Пусть $p \geq 3$ – простое число, $l_1, l_2, \dots, l_p$ – целые числа такие, что

$$0 \leq l_\rho \leq p-1 \quad \text{для всех} \quad \rho = 1, 2, \dots, p,$$

и

$$l = \sum_{\rho=1}^p l_\rho.$$

Тогда

$$\sum_{\alpha \in F_p} \prod_{\rho=1}^p \binom{\alpha}{l_\rho} = \begin{cases} 0, & \text{если } l \leq p-2, \\ \frac{p-1}{l_1! \dots l_p!}, & \text{если } l = p-1. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Как обычно, мы считаем, что

$$\binom{\alpha}{l_\rho} = \begin{cases} 1, & \text{если } l_\rho = 0, \\ 0, & \text{если } \alpha < l_\rho. \end{cases}$$

Рассмотрим произведение

$$\prod_{\rho=1}^p \binom{\alpha}{l_{\rho}}$$

как многочлен из кольца $F_p[\alpha]$ степени l , скажем,

$$\prod_{\rho=1}^p \binom{\alpha}{l_{\rho}} = c_0 \alpha^l + c_1 \alpha^{l-1} + \dots + c_l.$$

Результат следует теперь из соотношений

$$\sum_{\alpha \in F_p} \alpha^k = \begin{cases} p-1, & \text{если } (p-1) \mid k, \\ 0 & \text{в противном случае.} \end{cases}$$

Тем самым лемма доказана.

Пусть

$$f = \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} z_{ij}^{s_{ij}\tau}$$

– некоторый моном из кольца

$$A_{m\nu} = F_p[z_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq \nu].$$

Предположим, что f не инвариантен относительно действия группы $\tilde{H}$, и рассмотрим соответствующую орбитальную сумму

$$S_{\tilde{H}}(f) = \sum_{\alpha \in F_p} \tilde{\gamma}^{\alpha}(f).$$

Поскольку

$$\tilde{\gamma}^{\alpha}(z_{ij}) = \sum_{l=j}^{\tau p} \binom{\alpha}{l-j} z_{il}$$

для $1 \leq i \leq m$, $(\tau-1)p+1 \leq j \leq \tau p$, $1 \leq \tau \leq r$, мы находим, что

$$S_{\tilde{H}}(f) = \sum_{\alpha \in F_p} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l} \right)^{s_{ij}\tau}. \quad (2)$$

Пусть $\{\tilde{z}_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq \nu\}$ – новые переменные, определенные соотношениями

$$\tilde{z}_{i,(\tau-1)p+\alpha+1} = \sum_{l=0}^{\alpha} \binom{\alpha}{l} z_{i,(\tau-1)p+l+1} \quad (3)$$

для всех $1 \leq i \leq m$, $0 \leq \alpha \leq p-1$ и $1 \leq \tau \leq r$. Для каждого фиксированного i приведенные выше соотношения задают невырожденное линейное преобразование переменных, так что каждая переменная z_{ij} может быть представлена

в виде F_p -линейной комбинации переменных $\tilde{z}_{ij}$. Отсюда следует, что каждая орбитальная сумма $S_{\tilde{H}}(f)$ является F_p -линейной комбинацией орбитальных сумм

$$S_{\tilde{H}}(\tilde{f}) = \sum_{\tilde{g} \in \text{Orb}(\tilde{f})} \tilde{g},$$

где $\tilde{f}$ – мономы вида

$$\tilde{f} = \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \tilde{z}_{ij}^{s_{ij\tau}}$$

из кольца $F_p[\tilde{z}_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq \nu]$. Заметим теперь, что элементы $\{\tilde{z}_{ij} \mid 1 \leq j \leq \nu\}$, определенные соотношениями (3), образуют некоторый новый базис пространства

$$\tilde{V}_i = F_p z_{i1} + \cdots + F_p z_{i\nu}, \quad 1 \leq i \leq m.$$

Кроме того, для каждого $\tau = 1, 2, \dots, r$ группа $\tilde{H}$ действует на указанные базисные элементы $\tilde{z}_{ij}$, $(\tau - 1)p + 1 \leq j \leq \tau p$, при помощи их циклических перестановок. Пусть $v \in A_{m\nu}^{\tilde{H}}$ – какой-либо инвариант относительно действия группы $\tilde{H}$ и $\tilde{f}$ – некоторый моном из кольца $F_p[\tilde{z}_{ij} \mid 1 \leq i \leq m, 1 \leq j \leq \nu]$, входящий в этот инвариант с ненулевым коэффициентом. Поскольку $\tilde{\gamma}^\alpha(v) = v$ для любого элемента $\tilde{\gamma}^\alpha \in \tilde{H}$, то мономы $\tilde{f}$ и $\tilde{\gamma}^\alpha(\tilde{f})$ входят в инвариант v с одним и тем же коэффициентом и, значит, каждый инвариант $v \in A_{m\nu}^{\tilde{H}}$ является F_p -линейной комбинацией орбитальных норм $N_{\tilde{H}}(\tilde{f})$ и орбитальных сумм $S_{\tilde{H}}(\tilde{f})$ для различных мономов $\tilde{f}$ указанного выше вида. С другой стороны, каждая орбитальная сумма $S_{\tilde{H}}(\tilde{f})$ является в свою очередь F_p -линейной комбинацией орбитальных сумм вида $S_{\tilde{H}}(f)$, откуда следует, что каждый инвариант $v \in A_{m\nu}^{\tilde{H}}$ является F_p -линейной комбинацией орбитальных норм $N_{\tilde{H}}(f)$ и орбитальных сумм $S_{\tilde{H}}(f)$. Таким образом, мы получаем следующий результат.

ТЕОРЕМА 5. *Каждый инвариант алгебры $A_{m\nu}^{\tilde{H}}$ является F_p -линейной комбинацией орбитальных норм $N_{\tilde{H}}(f)$ и орбитальных сумм $S_{\tilde{H}}(f)$ для всевозможных мономов $f \in A_{m\nu}$ вида*

$$f = \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} z_{ij}^{s_{ij\tau}}.$$

Если $0 \leq \lambda < p - 1$ – целое число, то среди множества всех орбитальных сумм $S_{\tilde{H}}(f) \in A_{m\nu}$ рассмотрим лишь те суммы, которые не содержат ни одной из переменных z_{ij} для всех $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1 - \lambda$, $1 \leq \tau \leq r$. Нашей ближайшей целью является точное описание таких орбитальных сумм $S_{\tilde{H}}(f)$ для различных мономов f . Положим

$$s_{ij\tau} = \sum_{e=0}^{\eta} s_{ij\tau}^{(e)} p^e, \quad 0 \leq s_{ij\tau}^{(e)} \leq p - 1,$$

для всех $0 \leq e \leq \eta$, $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j \leq \tau p$, $1 \leq \tau \leq r$, и запишем f в виде

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}. \quad (4)$$

Затем определим *вес* монома f и связанной с ним орбитальной суммы $S_{\tilde{H}}(f)$ как

$$w(f) = w(S_{\tilde{H}}(f)) = \sum_{e=0}^{\eta} \sum_{i=1}^m \sum_{\tau=1}^r \sum_{j=(\tau-1)p+1}^{\tau p} (\tau p - j) s_{ij\tau}^{(e)}.$$

Если некоторый моном f инвариантен относительно действия группы $\tilde{H}$, то он имеет вид

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r z_{i,\tau p}^{s_{i,\tau p}^{(e)}}.$$

Предположим теперь, что f не инвариантен относительно действия $\tilde{H}$. Если $w(f) < p - 1$, то из (2), (4) и леммы 4 следует, что $S_{\tilde{H}}(f) = 0$. С другой стороны, если $w(f) > p + \lambda$ и $s_{ij\tau} \geq 1$ по меньшей мере для одного набора (i, j, τ) с условиями $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1 - \lambda$, $1 \leq \tau \leq r$, то инвариант $S_{\tilde{H}}(f)$ содержит хотя бы одну переменную z_{ij} для $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1 - \lambda$, $1 \leq \tau \leq r$. Тем самым доказан следующий результат.

ПРЕДЛОЖЕНИЕ 6. Пусть $0 \leq \lambda < p - 1$, $\mu \geq 1$ – целые числа и

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}$$

– некоторый моном из кольца $A_{m\nu}$, который не инвариантен относительно действия группы $\tilde{H}$. Каждая орбитальная норма $N_{\tilde{H}}(f) \in A_{m\nu}$, не содержащая ни одну из переменных z_{ij} , $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1 - \lambda$, $1 \leq \tau \leq r$, имеет вид

$$N_{\tilde{H}}^{(\lambda)}(f) = \prod_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=\tau p-1-\lambda}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e)}},$$

а каждая орбитальная сумма $S_{\tilde{H}}(f) \in A_{m\nu}$, не содержащая ни одну из переменных z_{ij} , $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1 - \lambda$, $1 \leq \tau \leq r$, имеет либо вид

$$S_{\tilde{H}}^{(\lambda)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=\tau p-1-\lambda}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e)}},$$

либо вид

$$S_{\tilde{H}}^{(\mu,\lambda)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e)}},$$

где $w(f) = p - 1 + \mu \geq p + \lambda$ и $s_{ij\tau}^{(e)} \geq 1$ по меньшей мере для одного набора (e, i, j, τ) такого, что $0 \leq e \leq \eta$, $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1 - \lambda$, $1 \leq \tau \leq r$.

В дальнейшем предполагаем, что

$$n_1 = \dots = n_r = 2. \quad (5)$$

При этом предположении следующий результат является легким следствием предложения 6 в частном случае, когда $\lambda = 0$.

СЛЕДСТВИЕ 7. Пусть μ – положительное целое число и

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}$$

– некоторый моном из кольца $A_{m\nu}$, который не инвариантен относительно действия группы $\tilde{H}$. Каждая орбитальная норма $N_{\tilde{H}}(f) \in A_{m\nu}$, не содержащая ни одну из переменных z_{ij} , $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1$, $1 \leq \tau \leq r$, имеет вид

$$N_{\tilde{H}}^{(0)}(f) = \prod_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \left(z_{i,\tau p-1}^{p^e} + \binom{\alpha}{1} z_{i,\tau p}^{p^e} \right)^{s_{i,\tau p-1}^{(e)}} (z_{i,\tau p}^{p^e})^{s_{i,\tau p}^{(e)}},$$

а каждая орбитальная сумма $S_{\tilde{H}}(f) \in A_{\nu\nu}$, не содержащая ни одну из переменных z_{ij} , $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1$, $1 \leq \tau \leq r$, имеет либо

$$S_{\tilde{H}}^{(0)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \left(z_{i,\tau p-1}^{p^e} + \binom{\alpha}{1} z_{i,\tau p}^{p^e} \right)^{s_{i,\tau p-1}^{(e)}} (z_{i,\tau p}^{p^e})^{s_{i,\tau p}^{(e)}},$$

либо вид

$$S_{\tilde{H}}^{(1)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e)}},$$

где $w(f) = p$ и $s_{ij\tau} \geq 1$ по меньшей мере для одного набора (e, i, j, τ) такого, что $0 \leq e \leq \eta$, $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1$, $1 \leq \tau \leq r$.

С другой стороны, если $S_{\tilde{H}}(f)$ содержит по крайней мере одну из переменных $z_{i,j}$, $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1$, $1 \leq \tau \leq r$, орбитальная сумма $S_{\tilde{H}}(f)$ имеет вид

$$S_{\tilde{H}}^{(\mu)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e)}},$$

где $w(f) = p - 1 + \mu \geq p + 1$ и $s_{ij\tau} \geq 1$ по меньшей мере для одного набора (e, i, j, τ) такого, что $0 \leq e \leq \eta$, $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j < \tau p - 1$, $1 \leq \tau \leq r$.

Для каждого $i = 1, 2, \dots, m$ рассмотрим вложение

$$\vartheta: V_i \hookrightarrow \tilde{V}_i \quad (6)$$

пространства V_i в пространство $\tilde{V}_i$, заданное соотношениями

$$\vartheta(x_{ij}) = \begin{cases} z_{i,\tau p-1}, & \text{если } j = 2\tau - 1, \ 1 \leq \tau \leq r, \\ z_{i,\tau p}, & \text{если } j = 2\tau, \ 1 \leq \tau \leq r, \end{cases}$$

и зададим действие циклической группы H на пространстве $\tilde{V}_i$ следующим образом. Если γ – порождающий элемент группы H , то его действие на элементы $(x_{i1}, \dots, x_{in})$ пространства V_i определим правилом

$$\gamma(x_{ij}) = \begin{cases} x_{ij} + x_{i,j+1}, & \text{если } j = 2\tau - 1, \ 1 \leq \tau \leq r, \\ x_{ij}, & \text{если } j \neq 2\tau - 1, \ 1 \leq \tau \leq r. \end{cases}$$

В таком случае отображение $\vartheta: V_i \hookrightarrow \tilde{V}_i$ индуцирует соответствующее действие элемента γ на пространстве $\tilde{V}_i$, определенное по правилу

$$\gamma(z_{ij}) = \begin{cases} z_{ij} + z_{i,j+1}, & \text{если } j = \tau p - 1, \ 1 \leq \tau \leq r, \\ z_{ij}, & \text{если } j \neq \tau p - 1, \ 1 \leq \tau \leq r. \end{cases} \quad (7)$$

Указанное правило расширяет действие группы H , определенное на подпространстве $V_i \subseteq \tilde{V}_i$, до ее действия на всем пространстве $\tilde{V}_i$ и тем самым расширяет действие группы H , определенное на элементах алгебры A_{mn} , до ее действия на элементы большей алгебры $A_{m\nu}$. С другой стороны, если $\tilde{\gamma}$ – порождающий элемент группы $\tilde{H}$, его действие на элементы $(z_{i1}, \dots, z_{i\nu})$ пространства $\tilde{V}_i$ задается следующим правилом

$$\tilde{\gamma}(z_{ij}) = \begin{cases} z_{ij} + z_{i,j+1}, & \text{если } (\tau - 1)p + 1 \leq j \leq \tau p - 1, \ 1 \leq \tau \leq r, \\ z_{ij}, & \text{если } j = \tau p, \ 1 \leq \tau \leq r. \end{cases}$$

Рассмотрим теперь те инварианты $u \in A_{m\nu}^{\tilde{H}}$, которые инвариантны также относительно действия группы H .

ТЕОРЕМА 8. Пусть $v \in A_{m\nu}^{\tilde{H}}$ – многочлен положительной степени. Тогда v инвариантен относительно действия группы H в том и только том случае, если v не содержит ни одной из переменных z_{ij} , $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j \leq \tau p - 2$, $1 \leq \tau \leq r$.

ДОКАЗАТЕЛЬСТВО. Каждый инвариант $v \in A_{m\nu}^{\tilde{H}}$ степени $s \geq 1$ является суммой его однородных компонент $v_k \in A_{m\nu}^{\tilde{H}}$ степени k для $0 \leq k \leq s$. Это редуцирует задачу к случаю, когда v есть однородный многочлен, инвариантный относительно действия группы $\tilde{H}$.

Предположим, что $v \in A_{m\nu}^{\tilde{H}}$ содержит по меньшей мере одну переменную z_{ij} , где $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j \leq \tau p - 2$, $1 \leq \tau \leq r$, и запишем v в виде

$$v = \sum_{(s_{ij})} v_{(s_{ij})} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{(\tau-1)p+1 \leq j \leq \tau p-2} z_{ij}^{s_{ij}},$$

где $v_{(s_{ij})}$ – однородные многочлены из кольца

$$F_p[z_{i,\tau p-1}, z_{i,\tau p} \mid 1 \leq i \leq m, 1 \leq \tau \leq r],$$

а суммирование ведется по всем наборам

$$(s_{ij}) = (s_{ij} \mid 1 \leq i \leq m, (\tau-1)p+1 \leq j \leq \tau p-2, 1 \leq \tau \leq r)$$

неотрицательных целых чисел s_{ij} таких, что

$$\sum_{i=1}^m \sum_{\tau=1}^r \sum_{(\tau-1)p+1 \leq j \leq \tau p-2} s_{ij} \leq s.$$

Пусть $j_0 \geq 1$ – наибольшее целое положительное число такое, что $j_0 \neq \tau p-1, \tau p$ для $1 \leq \tau \leq r$, а многочлен v не содержит ни одного из мономов

$$\prod_{i=1}^m \prod_{j=1}^{\tau p} z_{ij}^{s_{ij}}$$

с условием $s_{ij} \geq 1$ для всех $1 \leq i \leq m, j > j_0$ и содержит по крайней мере один ненулевой член

$$v_{(s_{ij})} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{\substack{(\tau-1)p+1 \leq j \leq \tau p-2 \\ 1 \leq j \leq j_0}} z_{ij}^{s_{ij}},$$

включающий переменную z_{ij_0} для некоторого $i = 1, 2, \dots, m$.

Запишем

$$v = v_{(0)} + \sum_{(s_{ij}) \neq (0)} v_{(s_{ij})} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{\substack{(\tau-1)p+1 \leq j \leq \tau p-2 \\ 1 \leq j \leq j_0}} z_{ij}^{s_{ij}}$$

и предположим, что многочлен v инвариантен относительно действия группы H . Так как переменные z_{ij} , $1 \leq i \leq m$, $(\tau-1)p+1 \leq j \leq \tau p-2$, $1 \leq \tau \leq r$, неподвижны под воздействием элемента $\gamma \in H$, мы имеем

$$\gamma(v) = \gamma(v_{(0)}) + \sum_{(s_{ij}) \neq (0)} \gamma(v_{(s_{ij})}) \prod_{i=1}^m \prod_{\tau=1}^r \prod_{\substack{(\tau-1)p+1 \leq j \leq \tau p-2 \\ 1 \leq j \leq j_0}} z_{ij}^{s_{ij}}.$$

Отсюда следует, что коэффициенты $v_{(s_{ij})}$ многочлена v инвариантны относительно действия группы H и, значит,

$$\gamma(v) = v_{(0)} + \sum_{(s_{ij}) \neq (0)} v_{(s_{ij})} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{\substack{(\tau-1)p+1 \leq j \leq \tau p-2 \\ 1 \leq j \leq j_0}} z_{ij}^{s_{ij}}.$$

С другой стороны, так как $\tilde{\gamma}(z_{ij}) = \gamma(z_{ij})$ для всех $1 \leq i \leq m, j = \tau p-1, \tau p$, $1 \leq \tau \leq r$, и $\tilde{\gamma}(z_{ij}) = z_{ij} + z_{i,j+1}$ для всех $1 \leq i \leq m, (\tau-1)p+1 \leq j \leq \tau p-2$, $1 \leq \tau \leq r$, то

$$\tilde{\gamma}(v) = v_{(0)} + \sum_{(s_{ij}) \neq (0)} v_{(s_{ij})} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{\substack{(\tau-1)p+1 \leq j \leq \tau p-2 \\ 1 \leq j \leq j_0}} (z_{ij} + z_{i,j+1})^{s_{ij}},$$

так что многочлен $\tilde{\gamma}(v)$ содержит по меньшей мере один ненулевой член

$$v(s_{ij}) \prod_{i=1}^m \prod_{\tau=1}^r \prod_{\substack{(\tau-1)p+1 \leq j \leq \tau p-2 \\ 1 \leq j \leq j_0}} z_{i,j+1}^{s_{ij}},$$

включающий переменную z_{i,j_0+1} , который отсутствует в многочлене $\gamma(v) = v$. Это означает, что многочлен v не может быть инвариантным относительно действия группы H . Обратно, если многочлен $v \in A_{m\nu}^{\tilde{H}}$ не содержит ни одной из переменных z_{ij} для $1 \leq i \leq m$, $(\tau-1)p+1 \leq j \leq \tau p-2$, $1 \leq \tau \leq r$, то v инвариантен относительно действия группы H , что доказывает теорему 8.

Пусть $v \in A_{m\nu}^{\tilde{H}}$ – многочлен, инвариантный относительно действия группы $\tilde{H}$. Теорема 5 показывает, что v является F_p -линейной комбинацией инвариантов $N_{\tilde{H}}^{(0)}(f)$, $S_{\tilde{H}}^{(0)}(f)$ и $S_{\tilde{H}}^{(\mu)}(f)$ для различных целых $\mu \geq 1$ и всевозможных мономов $f \in A_{m\nu}$. Так как многочлены $N_{\tilde{H}}^{(0)}(f)$, $S_{\tilde{H}}^{(0)}(f)$ и $S_{\tilde{H}}^{(1)}(f)$ не содержат ни одной из переменных z_{ij} , $1 \leq i \leq m$, $(\tau-1)p+1 \leq j \leq \tau p-2$, $1 \leq \tau \leq r$, из теоремы 8 следует, что $N_{\tilde{H}}^{(0)}(f)$, $S_{\tilde{H}}^{(0)}(f)$ и $S_{\tilde{H}}^{(1)}(f)$ являются в то же время и H -инвариантами. Теперь мы докажем следующий результат.

ПРЕДЛОЖЕНИЕ 9. Пусть

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij}^{(e)}}$$

– моном из кольца $A_{m\nu}$. Тогда орбитальная сумма $S_{\tilde{H}}^{(1)}(f)$ является F_p -линейной комбинацией H -инвариантов вида

$$(z_{i_1, \tau_1 p-1}^{p^{e_1}} z_{i_2, \tau_2 p}^{p^{e_2}} - z_{i_1, \tau_1 p}^{p^{e_1}} z_{i_2, \tau_2 p-1}^{p^{e_2}}) \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i, \tau p}^{p^e})^{\omega_{i, \tau p}^{(e)}},$$

где $0 \leq e_1, e_2 \leq \eta$, $1 \leq i_1, i_2 \leq m$, $1 \leq \tau_1, \tau_2 \leq r$, $(i_1, \tau_1) \prec (i_2, \tau_2)$, а также H -инвариантов вида

$$\prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i, \tau p}^{p^e})^{v_{i, \tau p}^{(e)}}.$$

ДОКАЗАТЕЛЬСТВО. Пусть

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij}^{(e)}}$$

и

$$S_{\tilde{H}}^{(1)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i, j+l}^{p^e} \right)^{s_{ij}^{(e)}},$$

где $w(f) = p$ и $s_{ij}^{(e)} \geq 1$ по крайней мере для одного набора (e, i, j, τ) такого, что $0 \leq e \leq \eta$, $1 \leq i \leq m$, $(\tau-1)p+1 \leq j \leq \tau p-2$, $1 \leq \tau \leq r$. Положим

$$v_{i, \tau p}^{(e)} = \sum_{j=(\tau-1)p+1}^{\tau p} s_{ij}^{(e)}.$$

Так как многочлен $S_{\tilde{H}}^{(1)}(f)$ не содержит ни одной из переменных z_{ij} , $1 \leq i \leq m$, $(\tau - 1)p + 1 \leq j \leq \tau p - 2$, $1 \leq \tau \leq r$, то

$$S_{\tilde{H}}^{(1)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \left(\binom{\alpha}{\tau p - j - 1} z_{i,\tau p-1}^{p^e} + \binom{\alpha}{\tau p - j} z_{i,\tau p}^{p^e} \right)^{s_{ij\tau}^{(e)}}.$$

Отсюда следует, что

$$\begin{aligned} S_{\tilde{H}}^{(1)}(f) = & \sum_{(e_1, e_2, i_1, i_2, \tau_1, \tau_2)} \left(a_{i_1 i_2 \tau_1 \tau_2}^{(e_1, e_2)} z_{i_1, \tau_1 p-1}^{p^{e_1}} z_{i_2, \tau_2 p}^{p^{e_2}} + b_{i_1 i_2 \tau_1 \tau_2}^{(e_1, e_2)} z_{i_1, \tau_1 p}^{p^{e_1}} z_{i_2, \tau_2 p-1}^{p^{e_2}} \right) \\ & \times \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i,\tau p}^{p^e})^{\omega_{i,\tau p}^{(e)}} + a \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i,\tau p}^{p^e})^{v_{i,\tau p}^{(e)}}, \end{aligned}$$

где

$$\omega_{i,\tau p}^{(e)} = \begin{cases} v_{i,\tau p}^{(e)} - 1, & \text{если } (e, i, \tau) = (e_1, i_1, \tau_1), (e_2, i_2, \tau_2), \\ v_{i,\tau p}^{(e)}, & \text{если } (e, i, \tau) \neq (e_1, i_1, \tau_1), (e_2, i_2, \tau_2). \end{cases}$$

Учитывая теперь, что многочлен $S_{\tilde{H}}^{(1)}$ инвариантен относительно действия группы H , а также тот факт, что

$$\gamma(z_{ij}) = \begin{cases} z_{ij} + z_{i,j+1}, & \text{если } j = \tau p - 1, 1 \leq \tau \leq r, \\ z_{ij}, & \text{если } j = \tau p, 1 \leq \tau \leq r, \end{cases}$$

мы приходим к соотношениям $a_{i_1 i_2 \tau_1 \tau_2}^{(e_1, e_2)} + b_{i_1 i_2 \tau_1 \tau_2}^{(e_1, e_2)} = 0$ для всех $(e_1, e_2, i_1, i_2, \tau_1, \tau_2)$, которые показывают, что

$$\begin{aligned} S_{\tilde{H}}^{(1)}(f) = & \sum_{(e_1, e_2, i_1, i_2, \tau_1, \tau_2)} a_{i_1 i_2 \tau_1 \tau_2}^{(e_1, e_2)} (z_{i_1, \tau_1 p-1}^{p^{e_1}} z_{i_2, \tau_2 p}^{p^{e_2}} - z_{i_1, \tau_1 p}^{p^{e_1}} z_{i_2, \tau_2 p-1}^{p^{e_2}}) \\ & \times \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i,\tau p}^{p^e})^{\omega_{i,\tau p}^{(e)}} + a \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i,\tau p}^{p^e})^{v_{i,\tau p}^{(e)}}. \end{aligned}$$

Предложение 9 доказано.

Рассмотрим инварианты $v \in A_{m\nu}^{\tilde{H}}$, которые являются F_p -линейными комбинациями орбитальных сумм вида $S_{\tilde{H}}^{(\mu)}(f)$, где $\mu \geq 2$ и f – моном из кольца $A_{m\nu}$. Наша дальнейшая цель состоит в явном описании тех многочленов $v \in A_{m\nu}$, которые одновременно инвариантны относительно действия групп H и $\tilde{H}$.

ПРЕДЛОЖЕНИЕ 10. Пусть $v \in A_{m\nu}^{\tilde{H}}$ – многочлен, являющийся F_p -линейной комбинацией

$$v = \sum_{k=1}^K a_k S_{\tilde{H}}^{(\mu_k)}(f_k), \quad a_k \neq 0,$$

орбитальных сумм $S_{\tilde{H}}^{(\mu_k)}(f_k)$ для различных

$$f_k = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e,k)}}$$

и положительных целых $\mu_1 \geq \mu_2 \geq \dots \geq \mu_K \geq 2$. Если v инвариантен относительно действия группы H , то $\mu_{k'} = \mu_k$ по крайней мере для одной целочисленной пары (k', k) с условием $k' > k$ и при этом

$$\sum_{j=(\tau-1)p+1}^{\tau p} s_{ij\tau}^{(e,k')} = \sum_{j=(\tau-1)p+1}^{\tau p} s_{ij\tau}^{(e,k)}.$$

ДОКАЗАТЕЛЬСТВО. Так как $\mu_k \geq 2$, то орбитальная сумма $S_{\tilde{H}}^{(\mu_k)}$ содержит ввиду следствия 7 по меньшей мере одну из переменных z_{ij} , $1 \leq i \leq m$, $(\tau-1)p+1 \leq j \leq \tau p-2$, $1 \leq \tau \leq r$, скажем $z_{\iota k}$. С другой стороны, так как многочлен v инвариантен относительно действия группы H , то ввиду теоремы 8 многочлен v не может содержать ни одной из указанных выше переменных z_{ij} . Отсюда мы заключаем, что переменная $z_{\iota k}$ должна элиминироваться в многочлене v за счет некоторой другой орбитальной суммы, входящей в рассматриваемую линейную комбинацию с ненулевым коэффициентом. Это означает, что наряду с $S_{\tilde{H}}^{(\mu_k)}$ рассматриваемая линейная комбинация

$$v = \sum_{k=1}^K a_k S_{\tilde{H}}^{(\mu_k)}(f_k)$$

должна содержать по меньшей мере еще одну орбитальную сумму $S_{\tilde{H}}^{(\mu_{k'})}(f_{k'})$ для некоторого

$$f_{k'} = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e,k')}}.$$

с условиями $k' > k$ и $\mu_{k'} = \mu_k$. Рассмотрим орбитальные суммы

$$S_{\tilde{H}}^{(\mu_k)}(f_k) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e,k)}},$$

$$S_{\tilde{H}}^{(\mu_k)}(f_{k'}) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \left(\sum_{l=0}^{\tau p-j} \binom{\alpha}{l} z_{i,j+l}^{p^e} \right)^{s_{ij\tau}^{(e,k')}}.$$

и предположим, в противоположность с нашим утверждением, что

$$\sum_{j=(\tau-1)p+1}^{\tau p} s_{ij\tau}^{(e,k')} \neq \sum_{j=(\tau-1)p+1}^{\tau p} s_{ij\tau}^{(e,k)}$$

для некоторой тройки (e, i, τ) . Многочлены $S_{\tilde{H}}^{(\mu_k)}(f_k)$ и $S_{\tilde{H}}^{(\mu_k)}$ являются F_p -линейными комбинациями мономов

$$\left(\sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \prod_{l=0}^{\tau p-j} \binom{\alpha}{l} \right)^{\sigma_{i,j+l,\tau}^{(e,k)}} \\ \times \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \prod_{l=0}^{\tau p-j} (z_{i,j+l}^{p^e})^{\sigma_{i,j+l,\tau}^{(e,k)'}}$$

и

$$\left(\sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \prod_{l=0}^{\tau p-j} \binom{\alpha}{l}^{\sigma_{i,j+l,\tau}^{(e,k')}} \right) \\ \times \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} \prod_{l=0}^{\tau p-j} (z_{i,j+l}^e)^{s_{i,j+l,\tau}^{(e,k')}}.$$

соответственно, где

$$\sum_{l=0}^{\tau p-j} \sigma_{i,j+l,\tau}^{(e,k)} = s_{ij\tau}^{(e,k)} \quad \text{и} \quad \sum_{l=0}^{\tau p-j} \sigma_{i,j+l,\tau}^{(e,k')} = s_{ij\tau}^{(e,k')}.$$

Согласно предположению всякий моном, входящий в многочлен $S_{\tilde{H}}^{(\mu_k)}(f_k)$ и включающий в себя переменную $z_{\ell k}$, отличен от любого монома, входящего в многочлен $S_{\tilde{H}}^{(\mu_{k'})}(f_{k'})$. Отсюда следует, что ни один моном, входящий в многочлен $S_{\tilde{H}}^{(\mu_k)}$ и включающий в себя переменную $z_{\ell k}$, не может быть элиминирован. Полученное противоречие доказывает предложение 10.

Положим $z_{ij}^{(e)} = z_{ij}^{p^e}$ и рассмотрим произведение

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e)}}$$

как моном относительно $z_{ij}^{(e)}$. Аналогичным образом рассмотрим соответствующую орбитальную сумму $S_{\tilde{H}}^{(\mu)}(f)$ как многочлен относительно $z_{ij}^{(e)}$. Заметим также, что вес каждого монома, входящего в многочлен $S_{\tilde{H}}^{(\mu)}(f)$ с ненулевым коэффициентом, не превышает μ . Исходный моном f и связанная с ним орбитальная сумма $S_{\tilde{H}}^{(\mu)}(f)$ называются *гладкими*, если $s_{ij\tau}^{(e)} = 0$ или $s_{ij\tau}^{(e)} = 1$ для всех $0 \leq e \leq \eta$, $1 \leq i \leq m$, $(\tau-1)p+1 \leq j \leq \tau p$, $1 \leq \tau \leq r$. Заметим сразу же, что произвольная орбитальная сумма $S_{\tilde{H}}^{(\mu)}(f)$ может быть получена из некоторой гладкой орбитальной суммы путем идентификации соответствующих степеней $z_{i,(\tau-1)p+l}^{p^e}$ для всевозможных (e, i, τ) . Из этого замечания следует, что изучение свойств произвольных орбитальных сумм $S_{\tilde{H}}^{(\mu)}(f)$ сводится к изучению аналогичных свойств соответствующих гладких орбитальных сумм. Следующий результат непосредственно вытекает из предложения 10.

СЛЕДСТВИЕ 11. Пусть $v \in A_{m\nu}^{\tilde{H}}$ – многочлен положительной степени, являющийся F_p -линейной комбинацией

$$v = \sum_{k=1}^K a_k S_{\tilde{H}}^{(\mu_k)}(f_k), \quad a_k \neq 0,$$

гладких орбитальных сумм $S_{\tilde{H}}^{(\mu_k)}(f_k)$ для различных

$$f_k = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e,k)}}.$$

Предположим, что $\mu_1 \geq \mu_2 \geq \dots \geq \mu_K \geq 2$ и что многочлен v инвариантен относительно действия группы H . Если две орбитальные суммы $S_{\tilde{H}}^{(\mu_k)}$ и $S_{\tilde{H}}^{(\mu_{k'})}$ такие, что $\mu_{k'} = \mu_k$ при $k' > k$, входят в рассматриваемую линейную комбинацию v с ненулевыми коэффициентами, то мономы $f_{k'}$ и f_k преобразуются друг в друга путем подстановок вида

$$z_{ij}^{p^e} \mapsto z_{i,j+l}^{p^e} \quad \text{и} \quad z_{i'j'}^{p^e} \mapsto z_{i',j'-l}^{p^e},$$

где $(\tau - 1)p + 1 \leq j + l, j' - l \leq \tau p$, $0 \leq e \leq \eta$, $1 \leq i, i' \leq m$, $1 \leq \tau \leq r$, сохраняющих веса и степени мономов f_k и $f_{k'}$.

Теперь мы в состоянии дать полное описание тех H -инвариантных многочленов $v \in A_{m\nu}^{\tilde{H}}$, которые являются F_p -линейными комбинациями гладких орбитальных сумм $S_{\tilde{H}}^{(\mu)}(f)$ для всевозможных $\mu \geq 2$ и f . Следующий результат играет ключевую роль в построении полной системы порождающих элементов алгебры $A_{m\nu}^H$.

ПРЕДЛОЖЕНИЕ 12. Пусть $v \in A_{m\nu}^{\tilde{H}}$ — многочлен положительной степени, являющийся F_p -линейной комбинацией

$$v = \sum_{k=1}^K a_k S_{\tilde{H}}^{(\mu_k)}(f_k), \quad a_k \neq 0,$$

гладких орбитальных сумм $S_{\tilde{H}}^{(\mu_k)}(f_k)$ для различных $\mu_k \geq 2$ и

$$f_k = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)p+1}^{\tau p} (z_{ij}^{p^e})^{s_{ij\tau}^{(e,k)}}.$$

Если многочлен v инвариантен относительно действия группы H , то он является F_p -линейной комбинацией многочленов вида

$$\prod_{\kappa=1}^{\sigma} (z_{i_{2\kappa-1}, \tau_{2\kappa-1}p-1}^{p^{e_{2\kappa-1}}} z_{i_{2\kappa}, \tau_{2\kappa}p}^{p^{e_{2\kappa}}} - z_{i_{2\kappa-1}, \tau_{2\kappa-1}p}^{p^{e_{2\kappa-1}}} z_{i_{2\kappa}, \tau_{2\kappa}p-1}^{p^{e_{2\kappa}}}) \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i, \tau p}^{p^e})^{\omega_{i, \tau p}^{(e)}},$$

где $0 \leq \sigma \leq [s/2]$, $(i_{2\kappa-1}, \tau_{2\kappa-1}) \prec (i_{2\kappa}, \tau_{2\kappa})$ и $0 \leq \omega_{i, \tau p}^{(e)} \leq 1$.

ДОКАЗАТЕЛЬСТВО. Так как многочлен v инвариантен относительно действия группы H , из теоремы 8 следует, что v содержит лишь мономы вида

$$z_{i_1, \tau_1 p - \varepsilon_1}^{p^{e_1}} \cdots z_{i_s, \tau_s p - \varepsilon_s}^{p^{e_s}},$$

где $1 \leq s \leq \deg v$, $1 \leq e_1, \dots, e_s \leq \eta$, $1 \leq i_1 \leq \dots \leq i_s \leq m$, $1 \leq \tau_1, \dots, \tau_s \leq r$ и $\varepsilon_1, \dots, \varepsilon_s \in \{0, 1\}$. Кроме того, так как v является F_p -линейной комбинацией гладких орбитальных сумм, то $(e_k, i_k, \tau_k) \neq (e_l, i_l, \tau_l)$ для всех k и l таких, что $k \neq l$.

Пусть

$$g = z_{i_1, \tau_1 p - \varepsilon_1}^{p^{e_1}} \cdots z_{i_s, \tau_s p - \varepsilon_s}^{p^{e_s}}$$

обозначает моном максимального возможного веса $\sigma \leq s$, входящий в многочлен v с ненулевым коэффициентом $a \in F_p$. Без уменьшения общности мы можем считать, что

$$g = z_{i_1, \tau_1 p - 1}^{p^{e_1}} \cdots z_{i_{\sigma-1}, \tau_{\sigma-1} p - 1}^{p^{e_{\sigma-1}}} z_{i_\sigma, \tau_\sigma p - 1}^{p^{e_\sigma}} z_{i_{\sigma+1}, \tau_{\sigma+1} p}^{p^{e_{\sigma+1}}} z_{i_{\sigma+2}, \tau_{\sigma+2} p}^{p^{e_{\sigma+2}}} \cdots z_{i_s, \tau_s p}^{p^{e_s}}.$$

Поскольку $\gamma(v) = v$, то наряду с многочленом ag инвариант v содержит также и многочлен

$$\gamma(ag) = ag + \sum_{\kappa=1}^{\sigma} \frac{a}{\kappa!} \left(z_{i_1, \tau_1 p}^{p^{e_1}} \frac{\partial}{\partial z_{i_1, \tau_1 p - 1}^{(e_1)}} + \cdots + z_{i_s, \tau_s p}^{p^{e_s}} \frac{\partial}{\partial z_{i_s, \tau_s p - 1}^{(e_s)}} \right)^{\kappa} g,$$

включающий в себя несколько дополнительных членов

$$ag_{\kappa} = \frac{a}{\kappa!} \left(z_{i_1, \tau_1 p}^{p^{e_1}} \frac{\partial}{\partial z_{i_1, \tau_1 p - 1}^{(e_1)}} + \cdots + z_{i_s, \tau_s p}^{p^{e_s}} \frac{\partial}{\partial z_{i_s, \tau_s p - 1}^{(e_s)}} \right)^{\kappa} g,$$

каждый из которых является линейной комбинацией мономов $g_{l\kappa}$ одного и того же веса $\sigma - \kappa$. С другой стороны, поскольку многочлен v инвариантен относительно действия группы H , он не может содержать указанных выше дополнительных членов, так что многочлен v должен включать в себя по меньшей мере еще один моном g' того же самого веса σ , который обеспечивает возможность для элиминации указанных выше лишних мономов $g_{l\kappa}$. Указанный процесс элиминации лишних мономов $g_{l\kappa}$ может быть описан индуктивно следующим образом.

Прибавляя и вычитая в случае необходимости члены вида ag' для всевозможных различных мономов g' одного и того же веса σ , мы можем считать без уменьшения общности, что

$$g' = z_{i_1, \tau_1 p - 1}^{p^{e_1}} \cdots z_{i_{\sigma-1}, \tau_{\sigma-1} p - 1}^{p^{e_{\sigma-1}}} z_{i_\sigma, \tau_\sigma p}^{p^{e_\sigma}} z_{i_{\sigma+1}, \tau_{\sigma+1} p - 1}^{p^{e_{\sigma+1}}} z_{i_{\sigma+2}, \tau_{\sigma+2} p}^{p^{e_{\sigma+2}}} \cdots z_{i_s, \tau_s p}^{p^{e_s}}.$$

Так как

$$\begin{aligned} a(g - g') &= a(z_{i_\sigma, \tau_\sigma p - 1}^{p^{e_\sigma}} z_{i_{\sigma+1}, \tau_{\sigma+1} p}^{p^{e_{\sigma+1}}} - z_{i_\sigma, \tau_\sigma p}^{p^{e_\sigma}} z_{i_{\sigma+1}, \tau_{\sigma+1} p - 1}^{p^{e_{\sigma+1}}}) \\ &\quad \times z_{i_1, \tau_1 p - 1}^{p^{e_1}} \cdots z_{i_{\sigma-1}, \tau_{\sigma-1} p - 1}^{p^{e_{\sigma-1}}} z_{i_{\sigma+2}, \tau_{\sigma+2} p}^{p^{e_{\sigma+2}}} \cdots z_{i_s, \tau_s p}^{p^{e_s}}, \end{aligned}$$

то

$$a(g - g') = a' z_{i_1, \tau_1 p - 1}^{p^{e_1}} \cdots z_{i_{\sigma-1}, \tau_{\sigma-1} p - 1}^{p^{e_{\sigma-1}}} z_{i_{\sigma+1}, \tau_{\sigma+1} p}^{p^{e_{\sigma+1}}} \cdots z_{i_s, \tau_s p}^{p^{e_s}},$$

где многочлен

$$a' = a(z_{i_\sigma, \tau_\sigma p - 1}^{p^{e_\sigma}} z_{i_{\sigma+1}, \tau_{\sigma+1} p}^{p^{e_{\sigma+1}}} - z_{i_\sigma, \tau_\sigma p}^{p^{e_\sigma}} z_{i_{\sigma+1}, \tau_{\sigma+1} p - 1}^{p^{e_{\sigma+1}}})$$

инвариантен относительно действия группы H . Итерируя этот процесс, через конечное число шагов мы элиминируем все дополнительные члены ag_{κ} в указанном выше представлении многочлена $\gamma(g)$ и заключаем, что $\sigma \leq [s/2]$ и что

многочлен v является F_p -линейной комбинацией инвариантов

$$\prod_{\kappa=1}^{\sigma} (z_{i_{\kappa}, \tau_{\kappa} p-1}^{p^{e_{\kappa}}} z_{i_{\kappa+1}, \tau_{\kappa+1} p}^{p^{e_{\kappa+1}}} - z_{i_{\kappa}, \tau_{\kappa} p}^{p^{e_{\kappa}}} z_{i_{\kappa+1}, \tau_{\kappa+1} p-1}^{p^{e_{\kappa+1}}}) \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r z_{i, \tau p}^{\omega_{i, \tau p}^{(e)}}.$$

Предложение 12 доказано.

Используя те же самые аргументы в случае повторяющихся $z_{i, \tau p-1}^{p^e}$ и $z_{i, \tau p}^{p^e}$, мы получаем следующий результат.

СЛЕДСТВИЕ 13. Пусть $v \in A_{m\nu}^{\tilde{H}}$ – многочлен положительной степени, являющийся F_p -линейной комбинацией

$$v = \sum_{k=1}^K a_k S_{\tilde{H}}^{(\mu_k)}(f_k), \quad a_k \neq 0,$$

орбитальных сумм $S_{\tilde{H}}^{(\mu_k)}(f_k)$ для различных $\mu_k \geq 2$ и

$$f_k = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \prod_{j=(\tau-1)+1}^{\tau p} (z_{ij}^{(e)})^{s_{ij\tau}^{(e)}}.$$

Если v инвариантен относительно действия группы H , то он является F_p -линейной комбинацией H -инвариантов

$$\begin{aligned} & \prod_{\kappa=1}^{\sigma} (z_{i_{2\kappa-1}, \tau_{2\kappa-1} p-1}^{p^{e_{2\kappa-1}}} z_{i_{2\kappa}, \tau_{2\kappa} p}^{p^{e_{2\kappa}}} - z_{i_{2\kappa-1}, \tau_{2\kappa-1} p}^{p^{e_{2\kappa-1}}} z_{i_{2\kappa}, \tau_{2\kappa} p-1}^{p^{e_{2\kappa}}})^{s_{i_{2\kappa-1} i_{2\kappa} \tau_{2\kappa-1} \tau_{2\kappa}}^{(e_{2\kappa-1}, e_{2\kappa})}} \\ & \times \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i, \tau p}^{p^e})^{\omega_{i, \tau p}^{(e)}}, \end{aligned}$$

где $0 \leq \sigma \leq [s/2]$, $(i_{2\kappa-1}, \tau_{2\kappa-1}) \prec (i_{2\kappa}, \tau_{2\kappa})$ и $0 \leq s_{i_{2\kappa-1} i_{2\kappa} \tau_{2\kappa-1} \tau_{2\kappa}}^{(e_{2\kappa-1}, e_{2\kappa})}, \omega_{i, \tau p}^{(e)} \leq p-1$.

Теперь мы изучим структуру инвариантов $N_{\tilde{H}}^{(0)}(f)$ и $S_{\tilde{H}}^{(0)}(f)$ для всевозможных мономов $f \in F_p[z_{i, \tau p-1}, z_{i, \tau p} \mid 1 \leq i \leq m, 1 \leq \tau \leq r]$. Сначала мы заметим, что

$$N_{\tilde{H}}^{(0)}(z_{i, \tau p-1}) = z_{i, \tau p-1}^p - z_{i, \tau p-1} z_{i, \tau p}^{p-1} \quad \text{и} \quad N_{\tilde{H}}^{(0)}(z_{i, \tau p}) = z_{i, \tau p}^p.$$

Отсюда следует, что если

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i, \tau p-1}^{p^e})^{s_{i, \tau p-1}^{(e)}} (z_{i, \tau p}^{p^e})^{s_{i, \tau p}^{(e)}},$$

то

$$N_{\tilde{H}}^{(0)}(f) = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i, \tau p-1}^{p^{e+1}} - z_{i, \tau p-1}^{p^e} z_{i, \tau p}^{p^{e-1}})^{s_{i, \tau p-1}^{(e)}} (z_{i, \tau p}^{p^{e+1}})^{s_{i, \tau p}^{(e)}}.$$

Заметим также, что

$$\begin{aligned} & z_{i_1, \tau_1 p-1}^{p^{e_1}} z_{i_2, \tau_2 p}^{p^{e_2}} - z_{i_1, \tau_1 p}^{p^{e_1}} z_{i_2, \tau_2 p-1}^{p^{e_2}} = (z_{i_1, \tau_1 p-1}^{p^{e_1}} - z_{i_1, \tau_1 p-1}^{p^{e_1-1}} z_{i_1, \tau_1 p}^{p^{e_1-1}(p-1)}) z_{i_2, \tau_2 p}^{p^{e_2}} \\ & - (z_{i_1, \tau_1 p}^{p^{e_1-1}} z_{i_2, \tau_2 p}^{p^{e_2}} - z_{i_1, \tau_1 p-1}^{p^{e_1-1}} z_{i_2, \tau_2 p}^{p^{e_2}}) z_{i_1, \tau_1 p}^{p^{e_1-1}(p-1)} \\ & = N_{\tilde{H}}^{(0)}(z_{i_1, \tau_1 p-1})^{p^{e_1-1}} z_{i_2, \tau_2 p}^{p^{e_2}} - (z_{i_1, \tau_1 p}^{p^{e_1-1}} z_{i_2, \tau_2 p-1}^{p^{e_2}} - z_{i_1, \tau_1 p-1}^{p^{e_1-1}} z_{i_2, \tau_2 p}^{p^{e_2}}) z_{i_1, \tau_1 p}^{p^{e_1-1}(p-1)}. \end{aligned}$$

Итерируя последнее соотношение, мы получаем

$$\begin{aligned} z_{i_1, \tau_1 p-1}^{p^{\varepsilon_1}} z_{i_2, \tau_2 p}^{p^{\varepsilon_2}} - z_{i_1, \tau_1 p}^{p^{\varepsilon_1}} z_{i_2, \tau_2 p-1}^{p^{\varepsilon_2}} &= (z_{i_1, \tau_1 p-1} z_{i_2, \tau_2 p} - z_{i_1, \tau_1 p} z_{i_2, \tau_2 p-1}) z_{i_1, \tau_1 p}^{p^{\varepsilon_1}-1} z_{i_2, \tau_2 p}^{p^{\varepsilon_2}-1} \\ &+ \left(\sum_{\varepsilon_1=1}^{e_1} N_{\tilde{H}}^{(0)}(z_{i_1, \tau_1 p-1})^{p^{\varepsilon_1}-\varepsilon_1} z_{i_1, \tau_1 p}^{p^{\varepsilon_1}-\varepsilon_1+1} (p^{\varepsilon_1-1}-1) \right) z_{i_2, \tau_2 p}^{p^{\varepsilon_2}} \\ &- \left(\sum_{\varepsilon_2=1}^{e_2} N_{\tilde{H}}^{(0)}(z_{i_2, \tau_2 p-1})^{p^{\varepsilon_2}-\varepsilon_2} z_{i_2, \tau_2 p}^{p^{\varepsilon_2}-\varepsilon_2+1} (p^{\varepsilon_2-1}-1) \right) z_{i_1, \tau_1 p}^{p^{\varepsilon_1}-1}. \end{aligned}$$

Учитывая теперь предложение 9 и следствие 13, мы приходим к следующему результату.

ПРЕДЛОЖЕНИЕ 14. Пусть $v \in A_{m\nu}^{\tilde{H}}$ — многочлен положительной степени, являющийся F_p -линейной комбинацией орбитальных сумм $S_{\tilde{H}}^{(\mu_k)}(f_k)$ для различных $\mu_k \geq 1$ и $f_k \in A_{m\nu}$. Если многочлен v инвариантен относительно действия группы H , то v является многочленом над полем F_p от H -инвариантов $N_{\tilde{H}}^{(0)}(z_{i, \tau p-1})$, $z_{i, \tau p}$ для всех $1 \leq i \leq m$, $1 \leq r \leq r$ и H -инвариантов $(z_{i_1, \tau_1 p-1} z_{i_2, \tau_2 p} - z_{i_1, \tau_1 p} z_{i_2, \tau_2 p-1})$ для всех $1 \leq i_1, i_2 \leq m$, $1 \leq \tau_1, \tau_2 \leq r$.

Пусть снова

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i, \tau p-1}^{p^e})^{s_{i, \tau p-1}^{(e)}} (z_{i, \tau p}^{p^e})^{s_{i, \tau p}^{(e)}}.$$

Положим

$$\sum_{e=0}^{\eta} s_{i, \tau p-1}^{(e)} = s_{i, \tau p-1}^{(0)} + t_{i, \tau p-1}^{(0)} p,$$

где $0 \leq s_{i, \tau p-1}^{(0)} \leq p-1$, и запишем f в виде

$$f = \prod_{i=1}^m \prod_{\tau=1}^r z_{i, \tau p-1}^{s_{i, \tau p-1}^{(0)}} (z_{i, \tau p-1}^{p^e})^{t_{i, \tau p-1}^{(0)}} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r z_{i, \tau p}^{s_{i, \tau p}^{(e)}}.$$

Поскольку

$$z_{i, \tau p-1}^p = N_{\tilde{H}}^{(0)}(z_{i, \tau p-1}) + z_{i, \tau p-1} z_{i, \tau p}^{p-1},$$

то мы имеем

$$f = \prod_{i=1}^m \prod_{\tau=1}^r z_{i, \tau p-1}^{s_{i, \tau p-1}^{(0)}} (N_{\tilde{H}}^{(0)}(z_{i, \tau p-1}) + z_{i, \tau p-1} z_{i, \tau p}^{p-1})^{t_{i, \tau p-1}^{(0)}} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r z_{i, \tau p}^{s_{i, \tau p}^{(e)}}.$$

Итерируя теперь последнее соотношение, мы находим, что f является F_p -линейной комбинацией многочленов

$$\prod_{i=1}^m \prod_{\tau=1}^r z_{i, \tau p-1}^{s_{i, \tau p-1}^{(0)}} z_{i, \tau p}^{t_{i, \tau p}^{(0)}} N_{\tilde{H}}^{(0)}(z_{i, \tau p-1})^{\omega_{i, \tau p-1}^{(1)}},$$

где $0 \leq s_{i, \tau p-1}^{(0)} \leq p-1$. Следовательно, сумма $S_{\tilde{H}}^{(0)}(f)$ является F_p -линейной комбинацией H -инвариантов

$$S_{\tilde{H}}^{(0)}(f') \prod_{i=1}^m \prod_{\tau=1}^r z_{i, \tau p}^{t_{i, \tau p}^{(0)}} N_{\tilde{H}}^{(0)}(z_{i, \tau p-1})^{\omega_{i, \tau p-1}^{(1)}},$$

где

$$f' = \prod_{i=1}^m \prod_{\tau=1}^r z_{i,\tau p-1}^{s_{i,\tau p-1}}$$

и $0 \leq s_{i,\tau p-1} \leq p-1$ для всех $1 \leq i \leq m$, $1 \leq \tau \leq r$. Таким образом, мы имеем следующий результат.

ПРЕДЛОЖЕНИЕ 15. Пусть

$$f = \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r (z_{i,\tau p-1}^{p^e})^{s_{i,\tau p-1}^{(e)}} (z_{i,\tau p}^{p^e})^{s_{i,\tau p}^{(e)}}$$

– моном из кольца $F_p[z_{i,\tau p-1}, z_{i,\tau p} \mid 1 \leq i \leq m, 1 \leq \tau \leq r]$ и

$$S_{\tilde{H}}^{(0)}(f) = \sum_{\alpha \in F_p} \prod_{e=0}^{\eta} \prod_{i=1}^m \prod_{\tau=1}^r \left(z_{i,\tau p-1}^{p^e} + \binom{\alpha}{1} z_{i,\tau p}^{p^e} \right)^{s_{i,\tau p-1}^{(e)}} (z_{i,\tau p}^{p^e})^{s_{i,\tau p}^{(e)}}$$

– соответствующая орбитальная сумма. Тогда $S_{\tilde{H}}^{(0)}(f)$ является многочленом над полем F_p от H -инвариантов $N_{\tilde{H}}^{(0)}(z_{i,\tau p-1})$, $z_{i,\tau p}$ для всех $1 \leq i \leq m$, $1 \leq \tau \leq r$ и от H -инвариантов $S_{\tilde{H}}^{(0)}(f')$ для различных мономов

$$f' = \prod_{i=1}^m \prod_{\tau=1}^r z_{i,\tau p-1}^{s_{i,\tau p-1}}$$

таких, что $0 \leq s_{i,\tau p-1} \leq p-1$ для всех $1 \leq i \leq m$, $1 \leq \tau \leq r$.

Принимая во внимание теоремы 5, 8 и предложения 14, 15, мы приходим к следующему результату.

ТЕОРЕМА 16. Пусть $v \in A_{m\nu}^{\tilde{H}}$ – многочлен положительной степени, инвариантный относительно действия группы H . Тогда v является многочленом над полем F_p от H -инвариантов $N_{\tilde{H}}^{(0)}(z_{i,\tau p-1})$, $z_{i,\tau p}$, $1 \leq i \leq m$, $1 \leq \tau \leq r$, H -инвариантов $(z_{i_1,\tau_1 p-1} z_{i_2,\tau_2 p} - z_{i_1,\tau_1 p} z_{i_2,\tau_2 p-1})$, $1 \leq i_1, i_2 \leq m$, $1 \leq \tau_1, \tau_2 \leq r$, $(i_1, \tau_1) \prec (i_2, \tau_2)$, и H -инвариантов $S_{\tilde{H}}^{(0)}(f')$ для различных мономов

$$f' = \prod_{i=1}^m \prod_{\tau=1}^r z_{i,\tau p-1}^{s_{i,\tau p-1}}$$

таких, что $0 \leq s_{i,\tau p-1} \leq p-1$.

Наконец, дадим явное описание инвариантов $S_{\tilde{H}}^{(0)}(f')$ для мономов f' указанного выше вида.

ПРЕДЛОЖЕНИЕ 17. Пусть

$$f' = \prod_{i=1}^m \prod_{\tau=1}^r z_{i,\tau p-1}^{s_{i,\tau p-1}}$$

– моном положительной степени $s \geq 1$ такой, что $0 \leq s_{i,\tau p-1} \leq p-1$ для всех $1 \leq i \leq m$, $1 \leq \tau \leq r$. Тогда

$$S_H^{(0)}(f') = - \sum_{l=1}^{[s/(p-1)]} \sum_{(\sigma_{i,\tau p-1})} \prod_{i=1}^m \prod_{\tau=1}^r a_{i,\tau p-1} z_{i,\tau p-1}^{s_{i,\tau p-1} - \sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p-1}},$$

где внутренняя сумма берется по всем целочисленным наборам $(\sigma_{i,\tau p-1})$ таким, что $0 \leq \sigma_{i,\tau p-1} \leq s_{i,\tau p-1}$, $1 \leq i \leq m$, $1 \leq \tau \leq r$, и

$$\sum_{i=1}^m \sum_{\tau=1}^r \sigma_{i,\tau p-1} = l(p-1) \leq s.$$

ДОКАЗАТЕЛЬСТВО. Положим

$$s_i = \sum_{\tau=1}^r s_{i,\tau p-1} \quad \text{и} \quad s = \sum_{i=1}^m s_i.$$

Так как

$$\left(z_{i,\tau p-1} + \binom{\alpha}{1} z_{i,\tau p} \right)^{s_{i,\tau p-1}} = \sum_{\alpha \in F_p} a_{\sigma_{i,\tau p-1}} \alpha^{\sigma_{i,\tau p-1}} z_{i,\tau p-1}^{s_{i,\tau p-1} - \sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p-1}},$$

где

$$a_{\sigma_{i,\tau p-1}} = \binom{s_{i,\tau p-1}}{\sigma_{i,\tau p-1}},$$

то

$$\begin{aligned} & \prod_{\tau=1}^r \left(z_{i,\tau p-1} + \binom{\alpha}{1} z_{i,\tau p} \right)^{s_{i,\tau p-1}} \\ &= \sum_{\sigma_i=0}^{s_i} \alpha^{\sigma_i} \sum_{\sigma_{i,p-1} + \dots + \sigma_{i,\tau p-1} = \sigma_i} \prod_{\tau=1}^r a_{i,\tau p-1} z_{i,\tau p-1}^{s_{i,\tau p-1} - \sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p-1}}. \end{aligned}$$

В таком случае

$$\begin{aligned} & \prod_{i=1}^m \prod_{\tau=1}^r \left(z_{i,\tau p-1} + \binom{\alpha}{1} z_{i,\tau p} \right)^{s_{i,\tau p-1}} \\ &= \sum_{\sigma=0}^s \alpha^{\sigma} \sum_{(\sigma_{i,\tau p-1})} \prod_{i=1}^m \prod_{\tau=1}^r a_{i,\tau p-1} z_{i,\tau p-1}^{s_{i,\tau p-1} - \sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p-1}} \end{aligned}$$

и, значит,

$$\begin{aligned} S_H^{(0)}(f') &= \sum_{\alpha \in F_p} \prod_{i=1}^m \prod_{\tau=1}^r \left(z_{i,\tau p-1} + \binom{\alpha}{1} z_{i,\tau p} \right)^{s_{i,\tau p-1}} \\ &= \sum_{\sigma=0}^s \sum_{\alpha \in F_p} \alpha^{\sigma} \sum_{(\sigma_{i,\tau p-1})} \prod_{i=1}^m \prod_{\tau=1}^r a_{i,\tau p-1} z_{i,\tau p-1}^{s_{i,\tau p-1} - \sigma_{i,\tau p-1}} z_{i,\tau p}^{\sigma_{i,\tau p-1}}, \end{aligned}$$

где внутренняя сумма берется по всем наборам $(\sigma_{i,\tau p-1})$ таким, что $0 \leq \sigma_{i,\tau p-1} \leq s_{i,\tau p-1}$, $1 \leq i \leq m$, $1 \leq \tau \leq r$, и

$$\sum_{i=1}^m \sum_{\tau=1}^r \sigma_{i,\tau p-1} = \sigma.$$

Результат следует теперь из того факта, что

$$\sum_{\alpha \in F_p} \alpha^\sigma = \begin{cases} p-1, & \text{если } \sigma = l(p-1), \\ 0 & \text{в противном случае.} \end{cases}$$

§ 2. Доказательство теоремы 1 и следствия 2

Так как переменные x_{ij} , $1 \leq i \leq m$, $2r+1 \leq j \leq n$, инвариантны относительно действия группы H , каждый инвариант $u \in A_{mn}^H$ является многочленом вида

$$u = u_1 f_1 + \cdots + u_l f_l,$$

где $u_i \in A_{m,2r}^H$, а f_k , $1 \leq k \leq l$, – некоторые мономы из кольца

$$F_p[x_{i,j} \mid 1 \leq i \leq m, 2r+1 \leq j \leq n].$$

В таком случае без потери общности можно считать, что $u \in A_{m,2r}^H$. Следовательно, достаточно показать, что

$$A_{m,2r}^H = F_p[x_{i,2\tau}, N_H^{(0)}(x_{i,2\tau-1}), (x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1}), S_H^{(0)}(f')],$$

где $1 \leq i \leq m$, $1 \leq \tau \leq r$, $1 \leq i_1, i_2 \leq m$, $1 \leq \tau_1, \tau_2 \leq r$, $(i_1, \tau_1) \prec (i_2, \tau_2)$, а f' пробегает множество мономов вида

$$f' = \prod_{i=1}^m \prod_{\tau=1}^r x_{i,2\tau-1}^{s_{i,2\tau-1}}, \quad 0 \leq s_{i,2\tau-1} \leq p-1.$$

Если $\vartheta: V_i \hookrightarrow \tilde{V}_i$ – вложение, заданное отображением (6), то ϑ индуцирует соответствующий мономорфизм

$$\vartheta: A_{m,2r} \rightarrow A_{m\nu}$$

F_p -алгебры $A_{m,2r}$ в F_p -алгебру $A_{m\nu}$. Пусть u – некоторый элемент алгебры $A_{m,2r}^H$ и $v = \vartheta(u) \in A_{m\nu}$ – его образ в алгебре $A_{m\nu}$. Тогда многочлен v инвариантен относительно действия группы H на элементы алгебры $A_{m\nu}$, определенного соотношением (7), а также инвариантен относительно действия группы $\tilde{H}$.

Из теоремы 16 следует, что в этом случае v является многочленом от H -инвариантов $N_{\tilde{H}}^{(0)}(z_{i,\tau p-1})$, $z_{i,\tau p}$, $1 \leq i \leq m$, $1 \leq \tau \leq r$, H -инвариантов $(z_{i_1,\tau_1 p-1}z_{i_2,\tau_2 p} - z_{i_1,\tau_1 p}z_{i_2,\tau_2 p-1})$, $1 \leq i_2, i_2 \leq m$, $1 \leq \tau_1, \tau_2 \leq r$, $(i_1, \tau_1) \prec (i_2, \tau_2)$, и H -инвариантов $S_H^{(0)}(f')$ для всевозможных мономов

$$f' = \prod_{i=1}^m \prod_{\tau=1}^r z_{i,\tau p-1}^{s_{i,\tau p-1}}$$

с условием, что $0 \leq s_{i,\tau p-1} \leq p-1$. Принимая теперь во внимание изоморфизм ϑ , отождествим переменные $z_{i,\tau p-1}$, $z_{i,\tau p}$ с переменными $x_{i,2\tau-1}$, $x_{i,2\tau}$ соответственно. При таком отождествлении мы получаем

$$\vartheta(N_H^{(0)}(x_{i,2\tau-1})) = N_H^{(0)}(z_{i,2\tau p-1}), \quad \vartheta(S_H^{(0)}(f')) = S_H^{(0)}(f')$$

и находим, что

$$A_{mn}^H = F_p[x_{i,2\tau}, x_{ij}, N_H^{(0)}(x_{i,2\tau-1}), (x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1}), S_H^{(0)}(f')].$$

Полученное соотношение доказывает теорему 1.

Для доказательства следствия 2 рассмотрим орбитальную сумму

$$S_H^{(0)}(g') = \sum_{\alpha \in F_p} \prod_{i=1}^m \prod_{\tau=1}^r \left(x_{i,2\tau-1} + \binom{\alpha}{1} x_{i,2\tau} \right)^{p-1}$$

и докажем, что сумма $S_H^{(0)}(g')$ не может быть представлена в виде многочлена над полем F_p от H -инвариантов $x_{i,2\tau}$, $N_H^{(0)}(x_{i,2\tau-1})$, $(x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1})$ и $S_H^{(0)}(f')$, где

$$f' = \prod_{i=1}^m \prod_{\tau=1}^r x_{i,2\tau-1}^{s_{i,2\tau-1}}$$

– некоторый моном с условием, что $s_{i,2\tau-1} < p-1$ по крайней мере для одной целочисленной пары (i, τ) . Сначала мы заметим, что многочлен $S_H^{(0)}(g')$ содержит моном

$$h' = x_{12}^{p-1} \prod_{\substack{i=1 \\ (i,\tau) \neq (1,1)}}^m \prod_{\tau=1}^r x_{i,2\tau-1}^{p-1}$$

полной степени $mr(p-1)$, входящий в $S_H^{(0)}(g')$ с ненулевым коэффициентом -1 . Кроме того, если

$$f' = \prod_{i=1}^m \prod_{\tau=1}^r x_{i,2\tau-1}^{s_{i,2\tau-1}} \quad \text{и} \quad S_H^{(0)}(f') \neq 0,$$

то, принимая во внимание предложение 17, мы заключаем, что многочлен $S_H^{(0)}(f')$ содержит моном вида

$$\prod_{i=1}^m \prod_{\tau=1}^r x_{i,2\tau-1}^{s_{i,2\tau-1} - \sigma_{i,2\tau-1}} x_{i,2\tau}^{\sigma_{i,2\tau-1}},$$

где $0 \leq \sigma_{i,2\tau-1} \leq s_{i,2\tau-1}$ и

$$\sum_{i=1}^m \sum_{\tau=1}^r \sigma_{i,2\tau-1} = p-1.$$

Предположим, что орбитальная сумма $S_H^{(0)}(g')$ представима в виде многочлена над полем F_p относительно H -инвариантов $x_{i,2\tau}$, $(x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau}x_{i_2,2\tau-1})$, $N_H^{(0)}(x_{i,2\tau-1})$ и $S_H^{(0)}(f')$, где $\deg f' < mr(p-1)$, и покажем, что любой моном M относительно приведенных выше инвариантов, который входит в многочлен $S_H^{(0)}(g')$ с ненулевым коэффициентом, после его разложения по степеням переменных $x_{i,2\tau-1}$, $x_{i,2\tau}$, $1 \leq i \leq m$, $1 \leq \tau \leq r$, не может содержать указанный выше моном h' . Заметим, что в силу однородности многочлена $S_H^{(0)}(f')$ каждый из рассматриваемых нами мономов M имеет одну и ту же степень $mr(p-1)$ относительно переменных $x_{i,2\tau-1}$ и $x_{i,2\tau}$.

Если M содержит в качестве множителя некоторую степень многочлена

$$N_H^{(0)}(x_{i,2\tau-1}) = x_{i,2\tau-1}^p - x_{i,2\tau-1}x_{i,2\tau}^{p-1},$$

то из весьма специального вида многочленов $N_H^{(0)}(x_{i,2\tau-1})$, $(x_{i_1,2\tau_1-1}x_{i_2,2\tau_2} - x_{i_1,2\tau}x_{i_2,2\tau-1})$ и $S_H^{(0)}(f')$ следует, что разложение монома M по степеням переменных $x_{i,2\tau-1}$ и $x_{i,2\tau}$ представляет собой F_p -линейную комбинацию мономов, каждый из которых либо включает в себя по крайней мере одну из степеней $x_{i,2\tau-1}^p$, либо имеет полную степень по переменным $x_{i,2\tau}$, не меньшую чем p .

Предположим теперь, что M содержит в качестве множителя многочлен $S_H^{(0)}(f')$, где $\deg f' < mr(p-1)$. Используя аргументы, аналогичные вышеуказанным, мы видим, что любой входящий в M с ненулевым коэффициентом моном имеет по переменным $x_{i,2\tau}$ полную степень, не меньшую чем p .

Наконец, так как $mr > 2$, то каждый моном M относительно выражений $x_{i,2\tau}$, $1 \leq i \leq m$, $1 \leq \tau \leq r$, и $(x_{i_2,2\tau_1}x_{i_2,2\tau_2} - x_{i_1,2\tau_1}x_{i_2,2\tau_2-1})$, $1 \leq i_1, i_2 \leq m$, $1 \leq \tau_1, \tau_2 \leq r$, $(i_1, \tau_1) \prec (i_2, \tau_2)$, полная степень которого по переменным $x_{i,2\tau-1}$ и $x_{i,2\tau}$ равна $mr(p-1)$, имеет по переменным $x_{i,2\tau}$ полную степень, не меньшую чем $mr(p-1)/2 > p-1$.

В любом из рассмотренных выше трех случаев случаев моном h' не может появиться в многочлене M с ненулевым коэффициентом, что доказывает следствие 2.

§ 3. Универсальный инвариант

Предположим, что $m \geq n$, и рассмотрим многочлен

$$f_0 = \sum_{\alpha_1, \dots, \alpha_n \in F_p} (\alpha_1 x_{11} + \dots + \alpha_n x_{1n})^{p-1} \dots (\alpha_1 x_{m1} + \dots + \alpha_n x_{mn})^{p-1}. \quad (8)$$

Вначале мы покажем, что f_0 инвариантен относительно действия общей линейной группы $\mathrm{GL}(n, F_p)$. Отсюда следует, в частности, что многочлен f_0 инвариантен также относительно действия любой подгруппы G группы $\mathrm{GL}(n, F_p)$. Достаточно установить, что многочлен f_0 инвариантен относительно действия произвольного элемента группы $\mathrm{GL}(n, F_p)$.

ПРЕДЛОЖЕНИЕ 18. Если σ – произвольный элемент группы $\mathrm{GL}(n, F_p)$, то $\sigma(f_0) = f_0$.

ДОКАЗАТЕЛЬСТВО. Так как

$$\begin{aligned} & \sigma((\alpha_1 x_{11} + \dots + \alpha_n x_{1n})^{p-1} \dots (\alpha_1 x_{m1} + \dots + \alpha_n x_{mn})^{p-1}) \\ &= (\alpha_1 \sigma(x_{11}) + \dots + \sigma(x_{1n}))^{p-1} \dots (\alpha_1 \sigma(x_{m1}) + \dots + \alpha_n \sigma(x_{mn}))^{p-1} \end{aligned}$$

и действие элемента σ одинаково на каждом из пространств $V_i = F_p x_{i1} + \dots + F_p x_{in}$, $1 \leq i \leq m$, мы находим, что

$$\begin{aligned} \sigma(f_0) &= \sum_{\alpha_1, \dots, \alpha_n \in F_p} (\alpha_1 \sigma(x_{11}) + \dots + \alpha_n \sigma(x_{1n}))^{p-1} \dots (\alpha_1 \sigma(x_{m1}) + \dots + \alpha_n \sigma(x_{mn}))^{p-1} \\ &= \sum_{\alpha'_1, \dots, \alpha'_n \in F_p} (\alpha'_1 x_{11} + \dots + \alpha'_n x_{1n})^{p-1} \dots (\alpha'_1 x_{m1} + \dots + \alpha'_n x_{mn})^{p-1} = f_0. \end{aligned}$$

Предложение доказано.

Если F — многочлен из кольца A_{mn} , обозначим через $\pi(F)$ его образ при проекции

$$\pi(x_{11}, \dots, x_{1n}; \dots; x_{m1}, \dots, x_{mn}) = (\pi_1(x_{11}, \dots, x_{1n}); \dots; \pi_m(x_{m1}, \dots, x_{mn})), \quad (9)$$

где

$$\pi_i(x_{i1}, \dots, x_{in}) = \begin{cases} (0, \dots, 0, x_{ii}, 0, \dots, 0), & i = 1, 2, \dots, n, \\ (x_{i1}, 0, \dots, 0, 0, \dots, 0), & i = n+1, \dots, m. \end{cases}$$

Ясно, что отображение

$$\pi(f(x_{11}, \dots, x_{1n}; \dots; x_{m1}, \dots, x_{mn})) = f(\pi_1(x_{11}, \dots, x_{1n}); \dots; \pi_m(x_{m1}, \dots, x_{mn}))$$

определяет гомоморфизм соответствующих F_p -алгебр.

Обозначим через $\pi(f_0)$ образ многочлена f_0 при проекции π и найдем явный вид многочлена $\pi(f_0)$.

ПРЕДЛОЖЕНИЕ 19. Если $m \geq n$, то многочлен $\pi(f_0)$ имеет вид

$$\pi(f_0) = (-1)^n \prod_{i=1}^n x_{ii}^{p-1} \prod_{i=n+1}^m x_{i1}^{p-1}.$$

ДОКАЗАТЕЛЬСТВО. Заметим сначала, что

$$\pi(f_0) = \sum_{\alpha_1, \dots, \alpha_n \in F_p} \prod_{i=1}^n (\alpha_i x_{ii})^{p-1} \prod_{i=n+1}^m (\alpha_1 x_{i1})^{p-1}.$$

В таком случае

$$\pi(f_0) = \prod_{i=1}^n x_{ii}^{p-1} \prod_{i=n+1}^m x_{i1}^{p-1} \left(\sum_{\alpha_1, \dots, \alpha_n \in F_p} \alpha_1^{(m-n+1)(p-1)} \prod_{j=2}^n \alpha_j^{p-1} \right),$$

и так как

$$\sum_{\alpha \in F_p} \alpha^{l(p-1)} = -1$$

для каждого целого числа l , то

$$\pi(f_0) = (-1)^n \prod_{i=1}^n x_{ii}^{p-1} \prod_{i=n+1}^m x_{i1}^{p-1}.$$

Тем самым, предложение доказано.

§ 4. Доказательство теоремы 3

Пусть $G \leq \mathrm{GL}(n, F_p)$ – конечная группа, порядок $|G|$ которой делится на простое число $p \geq 3$, а $H = \langle \gamma \rangle$ – циклическая подгруппа группы G порядка p . Так как $H \leq G \leq \mathrm{GL}(n, F_p)$, то мы имеем

$$A_{mn}^{\mathrm{GL}(n, F_p)} \subseteq A_{mn}^G \subseteq A_{mn}^H.$$

Предположим, что $m > n$ и что размеры $n_1, \dots, n_s$ базисных жордановых блоков матрицы γ удовлетворяют условиям

$$n_1 = \dots = n_r = 1 \quad \text{и} \quad n_{r+1} = \dots = n_s = 1,$$

так что $n = 2r + s - r = r + s$.

Чтобы доказать теорему 3, достаточно показать, что каждая полная система порождающих элементов F_p -алгебры A_{mn}^G содержит по крайней мере один многочлен степени не ниже чем $(m - n + 2r)(p - 1)/r$. Положим

$$u_{(i_1, \tau_1), (i_2, \tau_2)} = (x_{i_1, 2\tau_1-1} x_{i_2, 2\tau_2} - x_{i_1, 2\tau_1} x_{i_2, 2\tau_2-1})$$

и рассмотрим систему порождающих элементов

$$B_{mn}^H = \{x_{i, 2\tau}, x_{ij}, N_H^{(0)}(x_{i_1, 2\tau_1-1}), u_{(i_1, \tau_1), (i_2, \tau_2)}, S_H^{(0)}(f')\}$$

алгебры A_{mn}^H , указанную в теореме 1. Следствие 2 показывает, что рассматриваемая система B_{mn}^H состоит из порождающих элементов F_p -алгебры A_{mn} минимальной возможной степени. Пусть B_{mn}^G – некоторая система порождающих элементов F_p -алгебры A_{mn}^G . Так как $A_{mn}^G \subseteq A_{mn}^H$, без уменьшения общности мы можем предположить, что $B_{mn}^G \subseteq B_{mn}^H$. Пусть $f_0 \in A_{mn}$ – многочлен, определенный соотношением (8). Предложения 18 и 19 показывают, что f_0 является однородным многочленом степени $m(p - 1)$, который инвариантен относительно действия группы $\mathrm{GL}(n, F_p)$. В таком случае многочлен f_0 инвариантен также относительно действия как группы G , так и ее подгруппы H . Решающим моментом наших рассуждений является тот факт, что многочлен $f_0 \in A_{mn}^G$ неразложим в алгебре A_{mn}^H относительно системы B_{mn}^H , т.е. f_0 не может быть записан как многочлен над полем F_p от векторных инвариантов $u \in B_{mn}^H$. Отсюда следует, что f_0 неразложим также и в алгебре A_{mn}^G относительно системы B_{mn}^G , т.е. f_0 не может быть представлен в виде многочлена от полиномиальных инвариантов $u \in B_{mn}^G$.

Обозначим через η число элементов множества B_{mn}^H и занумеруем элементы u множества B_{mn}^H числами $1, 2, \dots, \eta$. Допустим, что f_0 является многочленом над полем F_p относительно инвариантов $u_1, \dots, u_\eta \in B_{mn}^H$, и запишем

$$f_0 = \sum_{\substack{1 \leq \delta_1 + \dots + \delta_\eta \leq m(p-1) \\ \delta_1 \deg u_1 + \dots + \delta_\eta \deg u_\eta = m(p-1)}} a_{\delta_1, \dots, \delta_\eta} u_1^{\delta_1} \dots u_\eta^{\delta_\eta}. \quad (10)$$

Сравнивая степени входящих в обе части последнего тождества мономов относительно каждой из переменных $x_{11}, \dots, x_{m1}; \dots; x_{1n}, \dots, x_{mn}$ и принимая во внимание, что f_0 и $u_1, \dots, u_\eta$ являются однородными многочленами от переменных $x_{11}, \dots, x_{m1}; \dots; x_{1n}, \dots, x_{mn}$, а также что $\deg f_0 = m(p-1)$, $\deg_{x_{ij}} f_0 = p-1$ для $1 \leq i \leq m$, $1 \leq j \leq n$, мы получаем $0 \leq \delta_\rho \leq p-1$, $1 \leq \rho \leq \eta$, и $\delta_1 + \dots + \delta_\eta > 1$. Более того, мы видим, что

$$\deg_{x_{ij}} u_\rho \leq p-1$$

для всех $1 \leq i \leq m$, $1 \leq j \leq n$ и $1 \leq \rho \leq \eta$. Предположим теперь, что

$$\{1, 2, \dots, \eta\} = I_1 \cup I_2 \cup I_3 \cup I_4 \cup I_5$$

и что $u_\epsilon = S_H^{(0)}(f'_\epsilon)$ для $\epsilon \in I_1$; $u_\kappa = N_H^{(0)}(x_{i, 2\tau-1})$ для $\kappa \in I_2$, $1 \leq i = i(\kappa) \leq m$ и $1 \leq \tau = \tau(\kappa) \leq r$; $u_\lambda = u_{(i_1, \tau_1), (i_2, \tau_2)}$ для $\lambda \in I_3$, $1 \leq i_1 = i_1(\lambda)$, $i_2 = i_2(\lambda) \leq m$, $1 \leq \tau_1 = \tau_1(\lambda)$, $\tau_2 = \tau_2(\lambda) \leq r$ и $(i_1, \tau_1) \prec (i_2, \tau_2)$; $u_\mu = x_{i, 2\tau}$ для $\mu \in I_4$, $1 \leq i = i(\mu) \leq m$ и $1 \leq \tau = \tau(\mu) \leq r$; $u_\nu = x_{ij}$ для $\nu \in I_5$, $1 \leq i = i(\nu) \leq m$ и $2r+1 \leq j = j(\nu) \leq n$. Тогда соотношение (10) принимает вид

$$f_0 = \sum a_{\delta_1, \dots, \delta_\eta} \prod_{\epsilon \in I_1} (S_H^{(0)}(f'_\epsilon))^{\delta_\epsilon} \prod_{\kappa \in I_2} (N_H^{(0)}(x_{i(\kappa), 2\tau(\kappa)-1}))^{\delta_\kappa} \\ \times \prod_{\lambda \in I_3} (u_{(i_1(\lambda), \tau_1(\lambda)), (i_2(\lambda), \tau_2(\lambda))})^{\delta_\lambda} \prod_{\mu \in I_4} x_{i(\mu), 2\tau(\mu)}^{\delta_\mu} \prod_{\nu \in I_5} x_{i(\nu), j(\nu)}^{\delta_\nu}, \quad (11)$$

где суммирование в правой части ведется по всем неотрицательным целым числам $\delta_1, \dots, \delta_\eta$, удовлетворяющим условию

$$\sum_{\epsilon \in I_1} \delta_\epsilon \deg S_H^{(0)}(f'_\epsilon) + \sum_{\kappa \in I_2} \delta_\kappa \deg N_H^{(0)}(x_{i(\kappa), 2\tau(\kappa)-1}) \\ + \sum_{\lambda \in I_3} 2\delta_\lambda + \sum_{\mu \in I_4} \delta_\mu + \sum_{\nu \in I_5} \delta_\nu = m(p-1).$$

Докажем теперь, что равенство (11) невозможно. Для этого мы покажем, что моном

$$\prod_{i=1}^n x_{ii}^{p-1} \prod_{i=n+1}^m x_{i1}^{p-1}$$

входит в левую часть равенства (11), но не может входить в его правую часть. Пусть π – гомоморфизм F_p -алгебр, определенный соотношениями (9). Тогда предложение 19 показывает, что

$$\pi(f_0) = (-1)^n \prod_{i=1}^n x_{ii}^{p-1} \prod_{i=n+1}^m x_{i1}^{p-1}.$$

С другой стороны, мы имеем

$$\pi(N_H^{(0)}(x_{i,2\tau-1})) = \begin{cases} x_{2\tau-1,2\tau-1}^p, & \text{если } i = 2\tau - 1, \ 1 \leq \tau \leq r, \\ x_{i1}^p, & \text{если } n+1 \leq i \leq m, \\ 0 & \text{в остальных случаях,} \end{cases}$$

$$\pi(u_{(i,\sigma),(k,\tau)}) = \begin{cases} x_{2\sigma-1,2\sigma-1}x_{2\tau,2\tau}, & \text{если } i = 2\sigma - 1, \ k = 2\tau, \ 1 \leq \sigma \leq \tau \leq r, \\ -x_{2\sigma,2\sigma}x_{2\tau-1,2\tau-1}, & \text{если } i_1 = 2\sigma, \ k = 2\tau - 1, \ 1 \leq \sigma < \tau \leq r, \\ -x_{k1}x_{2\sigma,2\sigma}, & \text{если } n+1 \leq k \leq m, \ \tau = 1, \ 1 \leq \sigma \leq r, \\ 0 & \text{в остальных случаях,} \end{cases}$$

и если

$$f' = \prod_{i=1}^m \prod_{\tau=1}^r x_{i,2\tau-1}^{s_{i,2\tau-1}},$$

то в соответствии с предложением 17 мы получаем

$$\pi(S_H^{(0)}(f')) = - \prod_{\tau=1}^r x_{2\tau-1,2\tau-1}^{s_{2\tau-1,2\tau-1}} x_{2\tau,2\tau}^{s_{2\tau,2\tau}},$$

где

$$\sum_{\tau=1}^r s_{2\tau,2\tau-1} = l(p-1)$$

для некоторого положительного целого $l \leq m$.

Применяя гомоморфизм π к обеим частям равенства (11), мы получаем соотношение

$$\begin{aligned} \prod_{i=1}^{2r} x_{ii}^{p-1} \prod_{i=n+1}^m x_{i1}^{p-1} &= \prod_{\epsilon \in I_1} \left(\prod_{\tau=1}^r x_{2\tau-1,2\tau-1}^{s_{2\tau-1,2\tau-1}^{(\epsilon)}} x_{2\tau,2\tau}^{s_{2\tau,2\tau}^{(\epsilon)}} \prod_{i=n+1}^m x_{i1}^{s_{i1}^{(\epsilon)}} \right)^{\delta_\epsilon} \\ &\times \prod_{\kappa \in I_2} \left(\prod_{\tau=1}^r (x_{2\tau-1,2\tau-1}^p)^{s_{2\tau-1,2\tau-1}^{(\kappa)}} \prod_{i=n+1}^m (x_{i1}^p)^{s_{i1}^{(\kappa)}} \right)^{\delta_\kappa} \\ &\times \prod_{\lambda \in J_3} \left(\prod_{\rho=1}^r \prod_{\sigma=1}^r (x_{2\rho-1,2\rho-1} x_{2\sigma,2\sigma})^{s_{2\rho-1,2\sigma}^{(\lambda)}} \prod_{i=n+1}^m \prod_{\tau=1}^r (x_{i1} x_{2\tau,2\tau})^{s_{i,2\tau}^{(\lambda)}} \right)^{\delta_\lambda} \\ &\times \prod_{\mu \in I_4} \left(\prod_{\tau=1}^r x_{2\tau,2\tau}^{s_{2\tau,2\tau}^{(\mu)}} \right)^{\delta_\mu}, \end{aligned} \quad (12)$$

где

$$\begin{aligned} \sum_{\tau=1}^r s_{2\tau-1,2\tau}^{(\epsilon)} &= l(p-1), & \sum_{\tau=1}^r s_{2\tau-1,2\tau-1}^{(\kappa)} &= 1, & \sum_{i=n+1}^m s_{ii}^{(\kappa)} &= 1, \\ \sum_{\rho=1}^r \sum_{\sigma=1}^r s_{2\rho-1,2\sigma}^{(\lambda)} &= 1, & \sum_{i=n+1}^m \sum_{\tau=1}^r s_{i,2\tau}^{(\lambda)} &= 1, \\ \sum_{\tau=1}^r s_{2\tau,2\tau}^{(\mu)} &= 1, & \sum_{i=1}^m \sum_{j=2r+1}^n s_{ij}^{(\nu)} &= 1 \end{aligned}$$

и

$$s_{2\tau-1,2\tau-1}^{(\kappa)} + s_{ii}^{(\kappa)} \leq 1, \quad s_{2\rho-1,2\sigma}^{(\lambda)} + s_{i,2\tau}^{(\lambda)} \leq 1.$$

Если $s_{2\tau-1,2\tau-1}^{(\kappa)} \delta_\kappa \geq 1$ или $s_{i1}^{(\kappa)} \delta_\kappa \geq 1$ для некоторых (τ, κ) , (i, κ) , то степень правой части равенства (12) относительно переменных $x_{2\tau,2\tau}$ или x_{i1} не меньше чем p , что невозможно. Отсюда следует, что $\delta_\kappa = 0$ для всех $\kappa \in I_2$.

Положим

$$\begin{aligned} L_1 &= \sum_{\epsilon \in I_1} \sum_{i=n+1}^m \delta_\epsilon s_{i,1}^{(\epsilon)}, & L_3 &= \sum_{\lambda \in I_3} \sum_{i=n+1}^m \delta_\lambda s_{i,2\tau}^{(\lambda)}, \\ M_1 &= \sum_{\epsilon \in I_1} \sum_{\tau=1}^r \delta_\epsilon s_{2\tau-1,2\tau-1}^{(\epsilon)}, & M_3 &= \sum_{\lambda \in I_3} \sum_{\rho=1}^r \sum_{\sigma=1}^r \delta_\lambda s_{2\rho-1,2\sigma}^{(\lambda)} \end{aligned}$$

и

$$N_1 = \sum_{\epsilon \in I_1} \sum_{\tau=1}^r \delta_\epsilon s_{2\tau,2\tau-1}^{(\epsilon)}, \quad N_4 = \sum_{\mu \in I_4} \sum_{\tau=1}^r \delta_\mu s_{2\tau,2\tau}^{(\mu)}.$$

Сравнивая полные степени мономов в левой и правой частях равенства (12) относительно переменных x_{i1} , $x_{2\tau-1,2\tau-1}$ и $x_{2\tau,2\tau}$ соответственно, мы получаем

$$L_1 + L_3 = (m - n)(p - 1), \quad M_1 + M_3 = r(p - 1)$$

и

$$N_1 + L_3 + M_3 + N_4 = r(p - 1).$$

Заметим также, что условие

$$\sum_{\tau=1}^r s_{2\tau,2\tau-1}^{(\epsilon)} \geq l(p - 1) \geq p - 1$$

влечет неравенство

$$N_1 \geq (p - 1) \sum_{\epsilon \in I_1} \delta_\epsilon.$$

Положим

$$\theta = \sum_{\epsilon \in I_1} \delta_\epsilon$$

и заметим, что $\theta \leq r$. Теперь мы рассмотрим следующие два случая.

Случай 1. Если $\vartheta = r$, то $L_3 = M_3 = N_4 = 0$ и, следовательно,

$$\prod_{i=1}^{2r} x_{ii}^{p-1} \prod_{i=n+1}^m x_{i1}^{p-1} = \prod_{\epsilon \in I_1} \left(\prod_{i=n+1}^m x_{i1}^{s_{i1}^{(\epsilon)}} \prod_{\tau=1}^r x_{2\tau-1,2\tau-1}^{s_{2\tau-1,2\tau-1}^{(\epsilon)}} x_{2\tau,2\tau}^{s_{2\tau,2\tau}^{(\epsilon)}} \right)^{\tau_\mu}.$$

Сравнивая полные степени мономов в обеих частях последнего равенства и принимая во внимание, что

$$\deg S_H^{(0)}(f'_\epsilon) < \frac{(m - n + 2r)(p - 1)}{r},$$

мы получаем неравенство

$$(m - n + 2r)(p - 1) < (m - n + 2r)(p - 1)$$

и приходим к противоречию.

Случай 2. Пусть $\vartheta < r$. Так как

$$\begin{aligned} L_1 + L_3 + M_1 + M_3 + N_1 &= (m - n + r)(p - 1) + N_1, \\ L_3 + M_3 &\leq r(p - 1) - N_1, \quad N_1 \geq \theta(p - 1), \end{aligned}$$

и так как по условию

$$L_1 + M_1 + N_1 < \theta \frac{(m - n + 2r)(p - 1)}{r},$$

то

$$(m - n + r)(p - 1) + N_1 < \theta \frac{(m - n + 2r)(p - 1)}{r} + M_1 + M_3.$$

В таком случае

$$(m - n + r)(p - 1) < \theta \frac{(m - n + r)(p - 1)}{r} + (r - \theta)(p - 1)$$

и, следовательно,

$$(r - \theta)(m - n + r)(p - 1) < (r - \theta)r(p - 1).$$

Принимая во внимание условие $m > n$, мы снова приходим к противоречию, что доказывает теорему 3.

Список литературы

- [1] E. Noether, “Der Endlichkeitssatz der Invarianten endlicher Gruppen”, *Math. Ann.*, **77**:1 (1915), 89–92.
- [2] D. Richman, “On vector invariants over finite fields”, *Adv. Math.*, **81**:1 (1990), 30–65.
- [3] D. Richman, “Invariants of finite groups over fields of characteristic p ”, *Adv. Math.*, **124**:1 (1996), 25–48.
- [4] H. E. A. Campbell, I. Hughes, “Vector invariants of $U_2(F_p)$: a proof of a conjecture of Richman”, *Adv. Math.*, **126**:1 (1997), 1–20.
- [5] D. Hilbert, “Über die vollen Invariantensystem”, *Math. Ann.*, **42**:3 (1893), 313–373.
- [6] E. Noether, “Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p ”, *Nachr. Gesellsch. Wiss. Göttingen*, 1926, 28–35.
- [7] H. Weyl, *The classical groups*, Princeton Univ. Press, Princeton, NJ, 1953.
- [8] S. A. Stepanov, “Vector invariants of symmetric groups in prime characteristic”, *Discrete Math. Appl.*, **10**:5 (2000), 455–468.
- [9] L. Smith, *Polynomial invariants of finite groups*, Res. Notes Math., **6**, A. K. Peters, Wellesley, MA, 1995.

- [10] P. Fleischmann, “The Noether bound in invariant theory of finite groups”, *Adv. Math.*, **156**:1 (2000), 23–32.
- [11] G. Kemper, “Lower degree bounds for modular invariants and a question of I. Hughes”, *Transform. Groups*, **3**:2 (1998), 135–144.
- [12] P. Fleischmann, “A new degree bound for the vector invariants of symmetric groups”, *Trans. Amer. Math. Soc.*, **350** (1998), 1703–1712.
- [13] H. E. A. Campbell, I. Hughes, R. D. Pollack, “Vector invariants of symmetric groups”, *Canad. Math. Bull.*, **33**:4 (1990), 391–397.

С. А. Степанов (S. A. Stepanov)

Институт проблем передачи информации РАН,
г. Москва

Поступила в редакцию

29.01.2004 и 15.02.2006