Math-Net.Ru

Общероссийский математический портал

Л. М. Самойлов, О радикале относительно свободной ассоциативной алгебры над полями положительной характеристики, *Матем. сб.*, 2008, том 199, номер 5, 81–126

DOI: <https://doi.org/10.4213/sm3890>

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: 54.198.67.100

26 апреля 2023 г., 11:11:23

УДК 512.552.4

Л. М. Самойлов

О радикале относительно свободной ассоциативной алгебры над полями положительной характеристики

В работе решена проблема А. Р. Кемера о нильиндексе радикала: показано, что над бесконечным полем положительной характеристики радикал Джекобсона относительно свободной ассоциативной алгебры является нильидеалом ограниченного индекса. Описан базис тождеств с формами матричных алгебр над бесконечными полями положительной характеристики.

Библиография: 10 названий.

§ 1. Введение

Все рассматриваемые алгебры будем предполагать ассоциативными, в общем случае без единицы. В работе [1] А. Р. Кемером сформулирована следующая

ПРОБЛЕМА. Является ли радикал Джекобсона относительно свободной алгебры счетного ранга над бесконечным полем характеристики $p > 0$ нильидеалом ограниченного индекса?

В настоящей работе будет получено положительное решение этой проблемы.

ОСНОВНАЯ ТЕОРЕМА. *Радикал Джекобсона относительно свободной алгебры счетного ранга над бесконечным полем характеристики $p > 0$ есть нильидеал ограниченного индекса.*

Зафиксируем бесконечное поле F характеристики $p > 0$ и рассмотрим свободную ассоциативную алгебру $F\langle X \rangle$, порожденную счетным множеством X . Пусть Γ – собственный T -идеал (т.е. $\Gamma \neq (0)$ и $\Gamma \neq F\langle X \rangle$), $F\langle X \rangle/\Gamma$ – относительно свободная алгебра счетного ранга. Через n обозначим наибольший порядок матричной алгебры M_n , содержащейся в $\text{Var}(F\langle X \rangle/\Gamma)$. Число n называется *сложностью* T -идеала Γ , а также сложностью соответствующего многообразия $\text{Var}(F\langle X \rangle/\Gamma)$. Сложность нетривиального многообразия всегда конечна по теореме Амицура–Левицкого. Хорошо известно, что радикалом Джекобсона алгебры $F\langle X \rangle/\Gamma$ является идеал $T[M_n]/\Gamma$, где через $T[A]$ будем обозначать идеал тождеств алгебры A . В случаях $\Gamma = (0)$ или $\Gamma = F\langle X \rangle$ основная теорема очевидна, поэтому исключим их из дальнейшего рассмотрения.

Несложно показать, что над произвольным бесконечным полем $\text{Rad}(F\langle X \rangle/\Gamma)$ является нильидеалом (теорема Амицура). Над полем нулевой характеристики также можно рассмотреть вопрос о нильиндексе радикала. Как показала

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 04-01-00739).

И. Ю. Свиридова (см. [2]), над полем характеристики нуль радикал алгебры $F\langle X \rangle / \Gamma$ будет иметь ограниченный нильиндекс тогда и только тогда, когда Γ является идеалом тождеств некоторой конечномерной алгебры или когда $\Gamma = (0)$. При этом радикал будет являться нильпотентным идеалом. Тем самым, в нулевой и положительной характеристиках радикалы относительно свободных алгебр имеют разные нильсвойства.

В работе [1] А. Р. Кемер получил следующее утверждение, которое существенным образом будет использоваться при доказательстве основной теоремы.

ТЕОРЕМА 1 (см. [1]). *Любой конечно базлируемый T -идеал из радикала относительно свободной алгебры счетного ранга над бесконечным полем характеристики $p > 0$ является нильидеалом ограниченного индекса.*

В частности, для нематричных многообразий (т.е. многообразий сложности 1) проблема решается положительно. Для многообразий сложности $< p$ проблема была решена автором в [3]. В настоящей работе методы из [3] переносятся на случай многообразий произвольной сложности.

Теорема 1 показывает, что решение проблемы в той или иной форме должно опираться на некоторые ослабленные варианты открытой проблемы конечной базлируемости идеала $T[M_n]$. При доказательстве основной теоремы конечная базлируемость будет использоваться в форме теоремы 2, которая является основным техническим утверждением работы.

ТЕОРЕМА 2. *Для произвольных n и p существуют полином $K(z_1, \dots, z_k) \notin T[M_n]$ и конечно базлируемый T -идеал $\Gamma \subset T[M_n]$, удовлетворяющие свойству:*

$$\text{если } f(x_1, \dots, x_m) \in T[M_n], \quad \text{то } f(x_1, \dots, x_m)K(z_1, \dots, z_k) \in \Gamma.$$

Прежде всего покажем, как из теоремы 2 вытекает решение проблемы.

ДОКАЗАТЕЛЬСТВО ОСНОВНОЙ ТЕОРЕМЫ. Будем вести индукцию по сложности многообразия. Для многообразия сложности 0 теорема очевидна, так как такое многообразие удовлетворяет тождеству $x^N = 0$ для некоторого N . Базой индукции является случай нематричных многообразий; справедливость базы вытекает из теоремы 1.

Зафиксируем n и рассмотрим T -идеал K_n , порожденный полиномом $K(z_1, \dots, z_k)$. Так как $K(z_1, \dots, z_k) \notin T[M_n]$, то сложность идеала K_n (обозначим ее r) не превосходит $n - 1$. Поэтому из соображений индукции можно считать, что $\text{Rad}(F\langle X \rangle / K_n)$ является нильидеалом ограниченного индекса s . Это означает, что для каждого $f = f(x_1, \dots, x_m) \in T[M_r]$ полином f^s содержится в K_n . В частности, если $f \in T[M_n]$, то $f^s \in K_n$. Тогда из включения $f \cdot K(z_1, \dots, z_k) \in \Gamma$ вытекает, что $f^{s+1} \in \Gamma$.

Пусть теперь U – произвольный T -идеал сложности n . Тогда радикал алгебры $F\langle X \rangle / U$ совпадает с $T[M_n] / U$. Так как T -идеал Γ конечно базлируем, то по теореме 1 T -идеал $\Gamma + U / U$ относительно свободной алгебры $F\langle X \rangle / U$ является нильидеалом ограниченного индекса t , где число t зависит от U . Следовательно, для каждого $f \in T[M_n]$ полином $f^{(s+1)t}$ содержится в U . Итак, радикал относительно свободной алгебры $F\langle X \rangle / U$ является нильидеалом индекса $(s + 1)t$. Теорема доказана.

Оставшаяся часть работы посвящена доказательству теоремы 2. Важную роль при этом будут играть тождества с формами матричных алгебр. Имеются в виду тождества M_n , которые являются выражениями от $d_1(\cdot), \dots, d_n(\cdot)$, где $d_i(x)$ – канонические формы на M_n . Например,

$$x^3 d_1(y) d_1(y^2) - d_3(xy)$$

– полиоднородный полином с формами d_1 и d_3 , в который можно подставлять матрицы порядка ≥ 3 . Строгое определение тождеств с формами содержится в § 2 и § 4. Через $\tilde{F}\langle X \rangle$ обозначим относительно свободную алгебру с формами, на которую наложены некоторые тривиальные тождества, выполняющиеся во всех алгебрах M_n . А именно, тождества

$$d_{p^i}(ab) = d_{p^i}(ba), \quad p^i \leq n, \quad d_{p^i}(x^p) = (d_{p^i}(x))^p, \quad p^i \leq n,$$

и тождества, позволяющие выражать формы $d_1, \dots, d_n$ и все их частичные линейаризации через формы d_{p^i} , $p^i \leq n$. Если это конечное число тождеств на $\tilde{F}\langle X \rangle$ не накладывать, то их необходимо добавить в базис тождеств с формами алгебры M_n . Важно подчеркнуть, что алгебра $\tilde{F}\langle X \rangle$ зависит от n . Опираясь на результаты А. Н. Зубкова об инвариантах полной линейной группы над бесконечными полями положительной характеристики, в работе автором получена следующая теорема (определения полиномов с формами $\chi_n(x)$, $d_N^+(x)$, $d_{N,(s,N-s)}^+(x, y)$ и $d_{p^s}(L_\rho(\chi_n(x)))$ содержатся в § 2 и § 4).

ТЕОРЕМА 3. *Над бесконечным полем характеристики $p > 0$ базис тождеств с формами алгебры M_n в алгебре $\tilde{F}\langle X \rangle$ образуют:*

- (i) *тождества нулевой степени $d_{p^s}(1) = C_n^{p^s}$, $p^s \leq n$ ($C_n^{p^s}$ – биномиальный коэффициент);*
- (ii) *тождество Кэли–Гамильтона $\chi_n(x) = 0$;*
- (iii) *тождества от одной переменной $d_N^+(x) = 0$, $N > n$;*
- (iv) *тождества от двух переменных $d_{N,(s,N-s)}^+(x, y) = 0$, $N > n$, $0 < s < N$;*
- (v) *тождества от $\leq n$ переменных $d_{p^s}(L_\rho(\chi_n(x)))$, $p^s \leq n$.*

Отметим, что указанная в теореме система тождеств является бесконечной. Вопрос о ее конечной базируемости остается открытым (в случае конечной базируемости можно несколько упростить рассуждения из § 6). При $n < p$ конечная базируемость идеала тождеств с формами алгебры M_n фактически была доказана в работе автора [3]. В этой работе рассматривались тождества со следом, однако при $n < p$ все формы $d_1, \dots, d_n$ выражаются через следы.

Теорема 3 показывает, что базис тождеств с формами алгебры M_n образуют полиномы, зависящие не более чем от n переменных.

Материал работы расположен следующим образом. В §§ 2–4 доказывается теорема 3. В § 5 собраны технические леммы о тождествах матричных алгебр. В § 6 содержатся основные рассуждения работы. Центральное место занимает конструкция полиномов $R(f) \in F\langle X \rangle / \Gamma$ и доказательство свойств этих полиномов.

§ 2. Канонические формы на матричных алгебрах

Напомним некоторые определения из работы [4].

Пусть R – ассоциативно-коммутативная F -алгебра с единицей, V – левый R -модуль; $\eta_{i,j} \in \text{Hom}_R(V, R)$, где $i = 1, \dots, m$, $j = 1, 2, \dots$; $\rho_1, \dots, \rho_m$ – натуральные числа. Отображение $d: \underbrace{V \times \dots \times V}_m \rightarrow R$, определенное по формуле

$$d(x_1, \dots, x_m) = \sum_{(j)} r_{(j)} \eta_{1,j_1}(x_1) \cdots \eta_{1,j_{\gamma_1}}(x_1) \cdots \eta_{m,j_{\gamma_{m-1}+1}}(x_m) \cdots \eta_{m,j_{\gamma_m}}(x_m),$$

где $r_{(j)} \in R$, $(j) = (j_1, \dots, j_{\gamma_m})$, $\gamma_k = \sum_{i=1}^k \rho_i$, называется *однородной формой степени* $(\rho) = (\rho_1, \dots, \rho_m)$ по $(x_1, \dots, x_m)$, определенной на V со значениями в R . Если $m = 1$, $\rho_1 = n$, то форму d будем называть *формой степени n* .

Разбиением числа n будем называть произвольный упорядоченный набор натуральных чисел $(\rho) = (\rho_1, \dots, \rho_m)$, где $\sum_{i=1}^m \rho_i = n$.

Рассмотрим однородную форму $d_n: V \rightarrow R$ степени n . Так как поле F бесконечно, то по форме d_n однозначно определяются ее *частичные линейаризации* – однородные формы $d_{n,(\rho)}(x_1, \dots, x_m)$ степени $(\rho) = (\rho_1, \dots, \rho_m)$ по $(x_1, \dots, x_m)$, где (ρ) – произвольное разбиение числа n . При этом выполняются условия:

1) для любой перестановки $\sigma \in S_m$

$$d_{n,(\rho)}(x_1, \dots, x_m) = d_{n,(\sigma\rho)}(x_{\sigma(1)}, \dots, x_{\sigma(m)}), \quad (1)$$

где $\sigma\rho = (\rho_{\sigma(1)}, \dots, \rho_{\sigma(m)})$;

2) для любого разбиения $(\rho) = (\rho_1, \dots, \rho_m)$ числа n и любого $i = 1, \dots, m$, для любых $s, r \in R$ и $x, x', x_1, \dots, x_m, x'_1, \dots, x'_m \in V$ выполняются равенства

$$d_n(sx + rx') = s^n d_n(x) + r^n d_n(x') + \sum_{j=1}^{n-1} s^j r^{n-j} d_{n,(j,n-j)}(x, x'), \quad (2)$$

$$\begin{aligned} d_{n,(\rho)}(x_1, \dots, x_{i-1}, sx_i + rx'_i, x_{i+1}, \dots, x_m) \\ = s^{\rho_i} d_{n,(\rho)}(x_1, \dots, x_m) + r^{\rho_i} d_{n,(\rho)}(x_1, \dots, x_{i-1}, x'_i, x_{i+1}, \dots, x_m) \\ + \sum_{j=1}^{\rho_i-1} s^j r^{\rho_i-j} d_{n,(\rho^j)}(x_1, \dots, x_{i-1}, x_i, x'_i, x_{i+1}, \dots, x_m), \end{aligned} \quad (3)$$

где $\rho^{(j)} = (\rho_1, \dots, \rho_{i-1}, j, \rho_i - j, \rho_{i+1}, \dots, \rho_m)$.

По определению $d_{n,(n)} = d_n$. Формы $d_{n,(\rho)}$ называются *частичными линейаризациями* формы d_n . Если разбиение (ρ) состоит более чем из одного числа, то частичная линейаризация $d_{n,(\rho)}$ называется *собственной*.

Пусть

$$\lambda^n - d_1(x)\lambda^{n-1} + \dots + (-1)^n d_n(x) = \det(\lambda E - x)$$

– характеристический многочлен матрицы $x \in M_n$. Ясно, что отображение $d_i: x \rightarrow d_i(x)$, $i = 1, 2, \dots, n$, является однородной формой степени i , определенной на M_n , со значениями в F . Положим также $d_i(x) = 0$ при $i > n$. Определенные таким образом формы $d_1, d_2, \dots$ будем называть *каноническими*. Для

формы d_1 будем использовать также более традиционное обозначение Tr . По теореме Кэли–Гамильтона в алгебре M_n выполнено тождество $\chi_n(x) = 0$, где

$$\chi_n(x) = x^n - d_1(x)x^{n-1} + \dots + (-1)^n d_n(x).$$

Формы $d_1, d_2, \dots$ и их частичные линеаризации связаны между собой рядом соотношений, причем некоторые из этих соотношений имеют один и тот же вид для матричных алгебр всех порядков. Например, $d_{2,(1,1)}(x, y) = \text{Tr}(x) \text{Tr}(y) - \text{Tr}(xy)$, т.е. собственная линеаризация формы d_2 выражается через форму d_1 , при этом n произвольно.

Как доказано в работе [5], аналогичная ситуация имеет место и для собственных линеаризаций форм d_m . Зафиксируем разбиение $(\rho) = (\rho_1, \dots, \rho_s)$ числа m . Последовательность $(a_1, \dots, a_q)$, $a_i \in \{x_1, \dots, x_s\}$, назовем *циклом*; циклы, отличающиеся циклической перестановкой символов, будем отождествлять. Цикл называется *примитивным*, если его нельзя представить в виде $(b \dots b)$, где b – цикл длины $< q$. *Содержанием* цикла c назовем вектор $[c] = (n_{x_1}, \dots, n_{x_s})$, где n_{x_i} – число букв x_i в цикле c . По формуле Амицура (см. [5]) получаем

$$d_{m,(\rho)}(x_1, \dots, x_s) = \sum (-1)^{m-(j_1+\dots+j_k)} d_{j_1}(c_1) d_{j_2}(c_2) \dots d_{j_k}(c_k), \quad (4)$$

причем это равенство имеет место для всех n . Здесь суммирование ведется по всем попарно различным примитивным циклам $c_1, \dots, c_k$ и всем натуральным числам $j_1, \dots, j_k$, удовлетворяющим соотношению $j_1[c_1] + \dots + j_k[c_k] = (\rho)$. В частности,

$$\begin{aligned} d_{m,(m-1,1)} &= (-1)^{m-1} \text{Tr}(\chi_{m-1}(x)y) \\ &= (-1)^{m-1} \sum_{i=0}^{m-1} (-1)^{m-1-i} d_{m-1-i}(x) \text{Tr}(x^i y). \end{aligned}$$

Далее, каждая из алгебр M_n удовлетворяет тождествам

$$d_{p^s}(x^p) = (d_{p^s}(x))^p, \quad s = 0, 1, 2, \dots \quad (5)$$

Действительно, достаточно доказать равенства (5) для произвольной диагональной матрицы x , а в этом случае они очевидны.

ЗАМЕЧАНИЕ 1. Везде в дальнейшем под канонической формой $d_{m,(\rho)}$, где (ρ) – собственное разбиение, будем понимать ее представление в виде (4).

Формы $d_m(x)$ иногда представляются в виде линейных комбинаций произведений форм $d_i(x^j)$, $i < m$. Например, над полями характеристики, не равной 2, $d_2(x) = \frac{1}{2}(\text{Tr}(x)^2 - \text{Tr}(x^2))$, причем это равенство имеет место для алгебры матриц произвольного порядка. Над бесконечными полями характеристики 2 форма $d_2(x)$ через следы не выражается. Над полями характеристики $p > 0$ верны аналогичные равенства.

ЛЕММА 1. При $m \neq p^t$ форма d_m выражается через формы d_{p^s} , где $s = 0, 1, 2, \dots, p^s < m$. Более подробно, $d_m(x)$ представляется в виде линейной комбинации произведений $d_{p^{s_1}}(x^{\alpha_1}) \dots d_{p^{s_k}}(x^{\alpha_k})$, где $p^{s_i} < m$, $\alpha_i > 0$. Коэффициенты этой линейной комбинации можно выбрать не зависящими от n .

ДОКАЗАТЕЛЬСТВО. Представим m в p -ичной системе счисления:

$$m = \sum_{j=1}^k \rho_{l_j} p^{l_j}, \quad 0 < \rho_{l_j} < p, \quad k > 0.$$

Рассмотрим частичную линейризацию формы d_m типа

$$(\rho) = \left(\underbrace{p^{l_1}, \dots, p^{l_1}}_{\rho_{l_1}}, \dots, \underbrace{p^{l_k}, \dots, p^{l_k}}_{\rho_{l_k}} \right).$$

По замечанию 1 $d_{m,(\rho)}$ представляется в виде линейной комбинации произведений вида $d_{i_1}(u_1) \cdots d_{i_t}(u_t)$, u_i – мономы, $i_j < m$. Подставим в это равенство вместо всех переменных x . Получим, что форма $\gamma d_m(x)$ является линейной комбинацией произведений $d_{i_1}(x^{\alpha_1}) \cdots d_{i_t}(x^{\alpha_t})$, где $i_j < m$, $\alpha_i > 0$, коэффициенты этой линейной комбинации лежат в простом подполе поля F и не зависят от n ; $\gamma = \frac{m!}{(p^{l_1}!)^{\rho_{l_1}} \cdots (p^{l_k}!)^{\rho_{l_k}}}$ – целое число, не кратное p . Так как $\gamma \neq 0$ в F , то на γ можно поделить. Следовательно, форма $d_m(x)$ есть линейная комбинация произведений $d_{i_1}(x^{\alpha_1}) \cdots d_{i_t}(x^{\alpha_t})$, где $i_j < m$. Если некоторое $i_j < m$ не является степенью числа p , то к форме d_{i_j} можно применить предыдущие рассуждения и т.д. В итоге форма d_m представима в требуемом виде. Лемма 1 доказана.

ЗАМЕЧАНИЕ 2. Далее везде под канонической формой $d_m(x)$ при $m \neq p^t$ будем понимать фиксированное выражение $d_m(x)$ через произведения форм $d_{p^i}(x^j)$, $p^i < m$, полученное в лемме 1, с коэффициентами, не зависящими от n . Отметим, что такое представление, вообще говоря, не единственно. Так как M_n удовлетворяет тождеству (5), то будем считать, что во всех сомножителях $d_{p^i}(x^j)$ степень j не кратна p .

ЗАМЕЧАНИЕ 3. Из замечаний 1, 2 и формулы (4) вытекает, что любая форма $d_{m,(\rho)}$ является линейной комбинацией произведений форм $d_{p^i}(u_j)$ с коэффициентами, не зависящими от n . При этом u_j не являются p -словами (т.е. не равны p -м степеням своих подслов).

Определим теперь свободную алгебру с формами счетного ранга. Наша конструкция отличается от изложенной в работе [4] наличием выражений типа $d_n(1)$.

Пусть $\langle X \rangle$ и $\langle X \rangle^\sharp$ – свободные полугруппы без единицы и с единицей соответственно, порожденные счетным множеством X , $F^\sharp \langle X \rangle$ – свободная ассоциативная алгебра с единицей. Обозначим через Q множество всех символов $d_n(u)$, $d_{n,(\rho)}(u_1, \dots, u_m)$, $n = 1, 2, \dots$; $(\rho) = (\rho_1, \dots, \rho_m)$ – разбиение числа n ; $u, u_i \in \langle X \rangle^\sharp$. Обозначим через (Q) свободную коммутативную полугруппу, порожденную множеством Q , и рассмотрим полугрупповую алгебру $F(Q)$. Профакторизуем $F(Q)$ по определяющим соотношениям

$$d_{n,(\rho)}(u_1, \dots, u_m) = d_{n,(\sigma\rho)}(u_{\sigma(1)}, \dots, u_{\sigma(m)}),$$

где $\sigma\rho = (\rho_{\sigma(1)}, \dots, \rho_{\sigma(m)})$; $u_i \in \langle X \rangle^\sharp$ (ср. с (1)). Полученную алгебру обозначим S .

Положим $\check{F}\langle X \rangle = F^\sharp\langle X \rangle \otimes_F S$ и назовем $\check{F}\langle X \rangle$ *абсолютно свободной ассоциативной алгеброй с формами*, порожденной множеством X . Элементы этой алгебры будем называть *полиномами с формами*. Алгебра $F^\sharp\langle X \rangle$ естественным образом вложена в $\check{F}\langle X \rangle$. При помощи формул (2), (3) на S -алгебре $\check{F}\langle X \rangle$ определяются формы $d_n(x)$ со значениями в S , а также все их частичные линейаризации $d_{n,(\rho)}$.

Пусть R – коммутативная F -алгебра с единицей, A – R -алгебра. Предположим, что на A определены однородные формы $d_n: A \rightarrow R$ степени n . Тогда для каждого полинома $\check{f}(x_1, \dots, x_m) \in \check{F}\langle X \rangle$ и произвольных $a_1, \dots, a_m \in A$ естественным образом (подробности см. в [4]) определяется элемент $\check{f}(a_1, \dots, a_m) \in A$ как результат подстановки $x_1 = a_1, \dots, x_m = a_m$. После этого можно определить понятие тождества с формами алгебры A .

Для полиномов с формами из $\check{F}\langle X \rangle$ так же, как и для обычных полиномов из $F^\sharp\langle X \rangle$, определяются понятия степени, полиоднородности, полилинейности, частичных линейаризаций, следствий, вербальных идеалов и т.п.

В дальнейшем мы будем рассматривать только тождества с формами матричных алгебр. Поэтому удобно будет работать не в алгебре $\check{F}\langle X \rangle$, а в некоторой другой алгебре $\widehat{F}\langle X \rangle$, которая определяется следующим образом. По замечанию 3 любая каноническая форма $d_{m,(\rho)}(x_1, \dots, x_s)$ на алгебре M_n является линейной комбинацией форм $d_{p^{k_1}}(u_1) \cdots d_{p^{k_t}}(u_t)$, где u_i – мономы от переменных $x_1, \dots, x_s$, причем коэффициенты этой линейной комбинации не зависят от n :

$$d_{m,(\rho)}(x_1, \dots, x_s) = \sum_{(k),(u)} \alpha_{(k),(u)}^{(\rho)} d_{p^{k_1}}(u_1) \cdots d_{p^{k_t}}(u_t), \quad (6)$$

$\alpha_{(k),(u)}^{(\rho)} \in F$, $u_i \in \langle x_1, \dots, x_s \rangle$, u_i не являются p -словами, равенство (6) полиоднородно. Профакторизуем $\check{F}\langle X \rangle$ по $\check{T}$ -идеалу, порожденному тождествами (5), (6) и

$$d_{p^i}(xy) = d_{p^i}(yx). \quad (7)$$

Получившуюся алгебру обозначим $\widehat{F}\langle X \rangle$. Элементы этой алгебры также будем называть полиномами с формами.

Ясно, что $\widehat{F}\langle X \rangle$ является относительно свободной алгеброй в классе всех алгебр с формами, удовлетворяющих тождествам (5)–(7). Любой элемент из $\widehat{F}\langle X \rangle$ можно представить в виде линейной комбинации мономов $u_0 d_{p^{k_1}}(u_1) \cdots d_{p^{k_t}}(u_t)$, $u_i \in \langle X \rangle^\sharp$; такое представление, вообще говоря, не единственно.

В алгебре $\widehat{F}\langle X \rangle$ рассмотрим коммутативную F -подалгебру без единицы, порожденную элементами $d_{p^s}(u)$, $u \in \langle X \rangle$; эту алгебру обозначим $\widehat{F}\{X\}$. Элементы из $\widehat{F}\{X\}$ будем называть *чистыми полиномами с формами*. Естественным образом определяется понятие чистого тождества с формами и понятие чистого $\widehat{T}$ -идеала. Полином $\widehat{f}$ лежит в чистом $\widehat{T}$ -идеале, порожденном полиоднородными полиномами $\widehat{g}_i \in \widehat{F}\{X\}$, $i \in I$, тогда и только тогда, когда $\widehat{f}$ можно представить в виде линейной комбинации слагаемых

$$\widehat{h}_j(u_1, \dots, u_{m_j}) d_{p^{k_1}}(v_1) \cdots d_{p^{k_s}}(v_s), \quad (8)$$

где $s \geq 0$, $u_i, v_l \in \langle X \rangle$, $\hat{h}_j$ – некоторая частичная линейаризация полинома $\hat{g}_i$. Из бесконечности основного поля и полиоднородности соотношений (1)–(3), (5)–(7) вытекает, что если полином $\hat{f}$ полиоднородный степени (ρ) , то все слагаемые (8) также можно считать полиоднородными степени (ρ) .

В работе [4] было показано, что для алгебры M_n существуют *киллеры* всех форм d_k . Без доказательства приведем конструкцию этих киллеров, изложенную в [4] в более общей ситуации. Рассмотрим полином

$$q(x_1, \dots, x_n, y_1, \dots, y_{n-1}) = \sum_{\sigma \in S_n} (-1)^\sigma x_{\sigma(1)} y_1 x_{\sigma(2)} y_2 \cdots y_{n-1} x_{\sigma(n)}.$$

Тогда для каждого $k = 1, \dots, n$ найдется такое натуральное число r_k , что алгебра M_n удовлетворяет некоторому полиоднородному тождеству

$$d_k(z) \cdot (q(x, x^2, \dots, x^n, y_1, \dots, y_{n-1}))^{r_k} = q_k(x, y_1, \dots, y_{n-1}, z),$$

где $q_k \in F\langle X \rangle$ (см. [4; тождество 40]). При $k > n$ M_n удовлетворяет тождеству

$$d_k(z) \cdot q(x, x^2, \dots, x^n, y_1, \dots, y_{n-1}) = 0.$$

Легко понять (см. рассуждение перед леммой 3), что полиномы

$$(q(x, x^2, \dots, x^n, y_1, \dots, y_{n-1}))^{r_k}$$

не являются тождествами M_n .

§ 3. Чистые тождества с формами, выполняющиеся во всех алгебрах M_n

Обозначим через $\hat{U}$ множество чистых полиномов с формами из $\hat{F}\{X\}$, которые являются тождествами алгебр M_n при всех n . В $\hat{U}$ содержатся все полиномы (5)–(7), однако они равны нулю в $\hat{F}\{X\}$.

ПРЕДЛОЖЕНИЕ 1. *Идеал $\hat{U}$ является нулевым.*

Перед доказательством предложения 1 докажем несколько вспомогательных утверждений.

Будем называть $\hat{T}$ -идеал $\hat{\Gamma}$ алгебры $\hat{F}\langle X \rangle$ *вербально первичным* (или *$\hat{T}$ -первичным*), если из включения $\hat{\Gamma}_1 \cdot \hat{\Gamma}_2 \subseteq \hat{\Gamma}$ следует, что $\hat{\Gamma}_1 \subseteq \hat{\Gamma}$ или $\hat{\Gamma}_2 \subseteq \hat{\Gamma}$.

ЛЕММА 2. *Идеал $\hat{T}[M_n]$ является вербально первичным.*

ДОКАЗАТЕЛЬСТВО. Предположим, что $\hat{f}(x_1, \dots, x_s) \cdot \hat{g}(y_1, \dots, y_t) \in \hat{T}[M_n]$, но $\hat{f} \notin \hat{T}[M_n]$ и $\hat{g} \notin \hat{T}[M_n]$. В силу бесконечности основного поля существуют полиоднородные полиномы $\hat{f}$ и $\hat{g}$ с таким свойством. Подставим вместо переменных такие матрицы порядка n , что значения полиномов $\hat{f}$ и $\hat{g}$ равны ненулевым матрицам X и Y соответственно. Для произвольной невырожденной матрицы C и произвольных матриц $X_1, \dots, X_s, Y_1, \dots, Y_t$ имеет место равенство

$$\hat{f}(C^{-1}X_1C, \dots, C^{-1}X_sC) \cdot \hat{g}(Y_1, \dots, Y_t) = C^{-1}XC \cdot Y.$$

Для доказательства леммы осталось показать, что для произвольных ненулевых матриц X и Y найдется невырожденная матрица C , для которой $C^{-1}XCY \neq 0$, что равносильно $XCY \neq 0$. Ясно, что существует матрица A со свойством $XAY \neq 0$. Так как пространство M_n имеет базис, состоящий из невырожденных матриц, то для некоторой невырожденной матрицы C из этого базиса будет выполнено $XCY \neq 0$.

Аналогично показывается, что если $\hat{f}(x_1, \dots, x_s) \cdot z \cdot \hat{g}(y_1, \dots, y_t) \in \hat{T}[M_n]$, то или $\hat{f}(x_1, \dots, x_s) \in \hat{T}[M_n]$, или $\hat{g}(y_1, \dots, y_t) \in \hat{T}[M_n]$. Лемма 2 доказана.

Хорошо известно, что над произвольным бесконечным полем относительно свободная алгебра счетного ранга в многообразии $\text{Var}(M_n)$ удовлетворяет более сильному свойству, чем доказанное в лемме 2. А именно, эта алгебра не имеет делителей нуля (см., например, [6]). Иначе говоря, если

$$f(x_1, \dots, x_s) \cdot g(y_1, \dots, y_t) \in T[M_n],$$

то тождеством M_n будет являться или $f(x_1, \dots, x_s) = 0$, или $g(y_1, \dots, y_t) = 0$; здесь множества переменных $\{x_1, \dots, x_s\}$ и $\{y_1, \dots, y_t\}$ могут иметь непустое пересечение.

Докажем аналогичное утверждение для тождеств с формами.

ЛЕММА 3. Пусть поле F бесконечно и алгебра M_n удовлетворяет тождеству с формами $\hat{f}(x_1, \dots, x_s) \cdot \hat{g}(y_1, \dots, y_t) = 0$ (полиномы $\hat{f}$ и $\hat{g}$ могут зависеть от общих переменных). Тогда или $\hat{f}(x_1, \dots, x_s) = 0$, или $\hat{g}(y_1, \dots, y_t) = 0$ будет тождеством M_n .

ДОКАЗАТЕЛЬСТВО. Как отмечалось выше, для алгебры матриц M_n существуют киллеры всех форм d_k , $k = 1, 2, \dots$. Пусть $h_k, g_k \in F\langle X \rangle$, $k = 1, 2, \dots$, и

$$h_k(x_1, \dots, x_{i_k}) \notin T[M_n], \quad h_k(x_1, \dots, x_{i_k})d_k(z) - g_k(x_1, \dots, x_{i_k}, z) \in \hat{T}[M_n].$$

Положим $h_{k,j} = h_k(x_1^{(k,j)}, \dots, x_{i_k}^{(k,j)})$, $k, j = 1, 2, \dots$, причем полиномы $h_{k,j}$ попарно не зависят от общих переменных и от переменных $x_1, \dots, x_s, y_1, \dots, y_t$. Тогда найдутся полиномы $l_1 l_2 \dots l_u$ и $l_{u+1} l_{u+2} \dots l_v$, где $l_1, \dots, l_v \in \{h_{k,j} \mid k, j = 1, 2, \dots\}$ и все $l_1, \dots, l_v$ попарно различны, для которых выполнены сравнения

$$l_1 \dots l_u \hat{f} \equiv f_1 \pmod{\hat{T}[M_n]}, \quad \hat{g} l_{u+1} \dots l_v \equiv g_1 \pmod{\hat{T}[M_n]}, \quad (9)$$

где $f_1, g_1 \in F\langle X \rangle$. Умножим тождество с формами $\hat{f}\hat{g} = 0$ слева на полином $l_1 \dots l_u$ и справа на полином $l_{u+1} \dots l_v$. Тогда из (9) получаем, что обычный полином $f_1 g_1$ будет тождеством M_n . Так как в относительно свободной алгебре $F\langle X \rangle / T[M_n]$ нет делителей нуля, то или $f_1 \in T[M_n]$, или $g_1 \in T[M_n]$. Пусть для определенности $f_1 \in T[M_n]$.

В этом случае из (9) следует, что полином с формами $l_1 \dots l_u \hat{f}$ является тождеством M_n . Полиномы $l_1, \dots, l_u, \hat{f}$ зависят от попарно непересекающихся наборов переменных, а по лемме 2 идеал $\hat{T}[M_n]$ является вербально первичным. Так как $l_j \notin \hat{T}[M_n]$ при $j = 1, 2, \dots, u$, то $\hat{f} \in \hat{T}[M_n]$. Лемма 3 доказана.

Легко видеть, что чистый полином с формами $\hat{f}(x_1, \dots, x_m)$ можно представить в алгебре $\hat{F}\{X\}$ в виде F -линейной комбинации мономов вида

$$d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1} d_{p^{k_2}}(u_2^{\alpha_2})^{\beta_2} \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s}, \quad (10)$$

причем для каждого такого монома выполнены следующие условия:

- 1) каждое слово $u_i \in \langle X \rangle$ определено с точностью до циклического сдвига и не представляется в виде $u_i = v_i^\gamma$ при $\gamma > 1$;
- 2) сгруппируем сомножители $d_{p^{k_i}}(u_i^{\alpha_i})^{\beta_i}$, соответствующие одинаковым значениям k_i ; тогда в каждой такой группе все слова $u_j^{\alpha_j}$, рассматриваемые с точностью до циклического сдвига, являются попарно различными;
- 3) моном (10) определен с точностью до порядка сомножителей $d_{p^{k_i}}(u_i^{\alpha_i})^{\beta_i}$;
- 4) все $\alpha_1, \dots, \alpha_s$ не кратны p .

Про моном в форме (10) будем говорить, что он имеет *канонический вид*. Представление чистого полинома $\hat{f}(x_1, \dots, x_m)$ в виде линейной комбинации попарно различных мономов канонического вида будем называть *канонической записью* полинома. Ниже мы покажем, что различные мономы вида (10) образуют линейный базис алгебры $\hat{F}\{X\}$. Каноническую запись будем называть *нулевой*, если все входящие в нее мономы имеют нулевые коэффициенты.

Пусть S – множество тех переменных, по которым моном (10) имеет степень 1. Назовем моном (10) *отмеченным*, если выполнены два условия:

- 1) если $k_i \neq 0$, то $\beta_i : p$;
- 2) если $k_i = 0$, то или $\beta_i : p$, или $\beta_i = 1$. При этом $\beta_i = 1$ тогда и только тогда, когда слово $u_i^{\alpha_i}$ зависит только от переменных из множества S ; в частности, в этом случае $\alpha_i = 1$.

ЗАМЕЧАНИЕ 4. Пусть слово u не представляется в виде $u = v^k$, $k > 1$. Допустим, что степень u по переменной x равна l и u не зависит от переменной y . Образует из u l слов $u_1, \dots, u_l$ следующим образом: u_i получается из u заменой i -й слева буквы x на букву y . Тогда для $\alpha \geq 0$ все слова $u^\alpha u_1, \dots, u^\alpha u_l$ попарно циклически не эквивалентны, т.е. $\text{Tr}(u^\alpha u_i) \neq \text{Tr}(u^\alpha u_j)$ при $i \neq j$.

ДОКАЗАТЕЛЬСТВО. Докажем вспомогательное утверждение: если A и B – такие слова, что $AxBx = BxAx$, то $Ax = v^a$ и $Bx = v^b$ для некоторого слова v . В самом деле, если $|A| = |B|$, то можно положить $v = Ax$. Если $|A| \neq |B|$, то без ограничения общности пусть $|A| < |B|$. Тогда $B = AxB'$, откуда $AxAxB'x = Ax B'x Ax$, т.е. $AxB'x = B'x Ax$. В силу индукционных соображений по $|A| + |B|$ можно считать, что $Ax = v^a$, $B'x = v^b$, откуда $Bx = Ax B'x = v^a v^b = v^{a+b}$, что доказывает шаг индукции.

Пусть слова $u^\alpha u_i$ и $u^\alpha u_j$ циклически эквивалентны. Представим u в виде $u = axbxc$, причем $u_i = aybxc$, $u_j = axbyc$. В силу циклической эквивалентности выполнено

$$bxcu^\alpha ay = cu^\alpha axby,$$

откуда

$$bxc(axbxc) \dots (axbxc)ax = c(axbxc) \dots (axbxc)axbx.$$

Выделяя в равных словах общее начало, получаем $bxcax = caxbx$. По вспомогательному утверждению $bx = v^a$, $cax = v^b$, поэтому $bxcax = v^{a+b}$, $a + b > 1$.

Слова $u = axbxc$ и $bxcax$ циклически эквивалентны, поэтому $u = (v')^{a+b}$ для некоторого слова v' , циклически эквивалентного слову v . Полученное противоречие с условием $u \neq (v')^k$, $k > 1$, доказывает замечание.

При доказательстве следующих двух лемм мы предполагаем, что чистый полином априори может иметь несколько различных канонических записей. Каждый раз из контекста будет ясно, какая именно каноническая запись имеется в виду.

ЛЕММА 4. Пусть в некоторую каноническую запись полиоднородного неполилинейного полинома $\hat{f}(x_1, \dots, x_m)$ входит с ненулевым коэффициентом некоторый неотмеченный моном. Тогда $\hat{f}(x_1, \dots, x_m)$ имеет собственную частичную линеаризацию, которая обладает ненулевой канонической записью.

ДОКАЗАТЕЛЬСТВО. Пусть в каноническую запись полинома $\hat{f}$ с ненулевыми коэффициентами входят несколько неотмеченных мономов вида (10). Зафиксируем эту каноническую запись и рассмотрим два случая.

Случай 1. Среди этих мономов есть хотя бы один такой моном, что для некоторого l выполнено $k_l \neq 0$ и β_l не кратно p . Среди всех таких мономов выберем неотмеченный моном $\hat{m}$ канонического вида (10) с максимальным k_l , для которого β_l не кратно p . Без ограничения общности считаем $l = 1$.

Пусть слово u_1 зависит от переменной x_1 , а переменная y отлична от $x_1, \dots, x_m$. Для произвольного полиоднородного полинома $\hat{g}$ через $D(\hat{g})$ обозначим однородную компоненту степени 1 по y полинома $\hat{g}(x_1 + y, x_2, \dots)$. Если $\hat{g}$ не зависит от x_1 , то положим $D(\hat{g}) = 0$. Легко видеть, что линейный оператор D обладает свойством

$$D(\hat{g} \cdot \hat{h}) = D(\hat{g}) \cdot \hat{h} + \hat{g} \cdot D(\hat{h}). \quad (11)$$

В силу наложенных соотношений на алгебру $\hat{F}\langle X \rangle$

$$D(d_n(x_1)) = (-1)^{n-1} \text{Tr}(\chi_{n-1}(x_1)y).$$

При помощи этих равенств вычислим $D(d_{p^k}(u^\alpha)^\beta)$:

$$\begin{aligned} D(d_{p^k}(u^\alpha)^\beta) &= \beta d_{p^k}(u^\alpha)^{\beta-1} D(d_{p^k}(u^\alpha)) \\ &= (-1)^{p^k-1} \beta d_{p^k}(u^\alpha)^{\beta-1} \text{Tr}(\chi_{p^k-1}(u^\alpha) D(u^\alpha)) \\ &= (-1)^{p^k-1} \beta d_{p^k}(u^\alpha)^{\beta-1} \text{Tr}\left(\chi_{p^k-1}(u^\alpha) \sum_{i=0}^{\alpha-1} u^i D(u) u^{\alpha-1-i}\right). \end{aligned} \quad (12)$$

Очевидно, что для произвольных n , α , β выполняется равенство

$$\chi_n(u^\alpha) u^\beta = u^\beta \chi_n(u^\alpha),$$

откуда

$$\begin{aligned} \text{Tr}\left(\chi_{p^k-1}(u^\alpha) \sum_{i=0}^{\alpha-1} u^i D(u) u^{\alpha-1-i}\right) &= \text{Tr}\left(\sum_{i=0}^{\alpha-1} u^{\alpha-1-i} \chi_{p^k-1}(u^\alpha) u^i D(u)\right) \\ &= \text{Tr}\left(\sum_{i=0}^{\alpha-1} \chi_{p^k-1}(u^\alpha) u^{\alpha-1-i} u^i D(u)\right) = \alpha \text{Tr}(\chi_{p^k-1}(u^\alpha) u^{\alpha-1} D(u)). \end{aligned} \quad (13)$$

Из (12) и (13) окончательно получаем

$$D(d_{p^k}(u^\alpha)^\beta) = (-1)^{p^k-1} \alpha \beta d_{p^k}(u^\alpha)^{\beta-1} \text{Tr}(\chi_{p^k-1}(u^\alpha) u^{\alpha-1} D(u)). \quad (14)$$

При помощи (11) и (14) можно вычислить значение оператора D на мономе $d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1} \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s}$:

$$\begin{aligned} & D(d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1} \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s}) \\ &= \sum_{i=1}^s d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1} \dots (-1)^{p^{k_i}-1} \alpha_i \beta_i d_{p^{k_i}}(u_i^{\alpha_i})^{\beta_i-1} \\ & \quad \times \text{Tr}(\chi_{p^{k_i}-1}(u_i^{\alpha_i}) u_i^{\alpha_i-1} D(u_i)) \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s}. \end{aligned} \quad (15)$$

Из формулы (15) немедленно вытекает, что значение оператора D на любом отмеченном мономе степени > 1 по x_1 равно нулю, так как $\beta_i \vdots p$. Следовательно, при вычислении $D(\hat{f})$ отмеченные мономы можно не рассматривать, так как в случае 1 степень полинома $\hat{f}$ по x_1 больше 1.

Заметим, что

$$\begin{aligned} & \text{Tr}(\chi_{p^{k_1}-1}(u_1^{\alpha_1}) u_1^{\alpha_1-1} D(u_1)) = \text{Tr}(u_1^{\alpha_1 \cdot p^{k_1}-1} D(u_1)) \\ & \quad + \sum_{j=0}^{p^{k_1}-2} (-1)^{p^{k_1}-1-j} \text{Tr}(u_1^{\alpha_1(j+1)-1} d_{p^{k_1}-1-j}(u_1^{\alpha_1}) D(u_1)). \end{aligned} \quad (16)$$

Так как $(-1)^{p^{k_1}-1} \alpha_1 \beta_1 \neq 0$, то в сумму (15) с ненулевым коэффициентом входит слагаемое

$$d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1-1} \text{Tr}(u_1^{\alpha_1 \cdot p^{k_1}-1} D(u_1)) d_{p^{k_2}}(u_2^{\alpha_2})^{\beta_2} \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s}.$$

По замечанию 4 все мономы в канонической записи $\text{Tr}(u_1^{\alpha_1 \cdot p^{k_1}-1} D(u_1))$ попарно различны, а число этих мономов в точности равно степени u_1 по переменной x_1 . Обозначим через v произвольный моном в записи $D(u_1)$. Тогда в каноническую запись полинома $D(\hat{f})$ входит моном канонического вида

$$\hat{w} = d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1-1} \text{Tr}(u_1^{\alpha_1 \cdot p^{k_1}-1} v) d_{p^{k_2}}(u_2^{\alpha_2})^{\beta_2} \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s}.$$

Покажем, что этот моном встречается в канонической записи суммы (15) с коэффициентом $(-1)^{p^{k_1}-1} \alpha_1 \beta_1 \neq 0$. В самом деле, в каноническую запись части суммы (15), соответствующей значению $i = 1$, моном $\hat{w}$ входит, очевидно, с коэффициентом $(-1)^{p^{k_1}-1} \alpha_1 \beta_1$. В канонические записи слагаемых суммы (15), соответствующих значениям $i > 1$, моном $\hat{w}$ не входит.

Действительно, из (16) с заменой k_1 на k_i вытекает, что каноническая запись i -го слагаемого суммы (15) является линейной комбинацией с ненулевыми коэффициентами некоторых полиномов

$$d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1} \dots d_{p^{k_i}}(u_i^{\alpha_i})^{\beta_i-1} d_{p^{k_i}-j}(u_i^{\alpha_i}) \text{Tr}(u_i^{\alpha_i(j+1)-1} u_i') \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s}, \quad (17)$$

где $j \leq p^{k_i} - 1$, а слово u_i' (оно разное в разных слагаемых) обладает свойством $u_i'|_{y \rightarrow x_1} = u_i$. Ясно, что $k_i \leq k_1$. В самом деле, если $k_i > k_1$, то $\beta_i \vdots p$, и так

как в i -м слагаемом суммы (15) присутствует коэффициент β_i , то полином (17) имеет нулевой коэффициент.

Запись (17) за счет сомножителя $d_{p^{k_i-1-j}}(u_i^{\alpha_i})$ не является канонической. Поэтому, используя тождество (6), представим $d_{p^{k_i-1-j}}(u_i^{\alpha_i})$ в виде линейной комбинации произведений форм $d_{p^\beta}(u_i^{\alpha_i})$ и преобразуем (17) к канонической записи при помощи равенства $d_{p^\alpha}(v)^\beta \cdot d_{p^\alpha}(v)^\gamma = d_{p^\alpha}(v)^{\beta+\gamma}$. Тогда если какой-либо моном в полученной канонической записи полинома (17) совпадает с $\hat{w}$, то должно выполняться равенство

$$\mathrm{Tr}(u_i^{\alpha_i(j+1)-1} u_i') = \mathrm{Tr}(u_1^{\alpha_1 \cdot p^{k_1}-1} v),$$

так как $\hat{w}$ имеет степень 1 по y , а слова u_i' и v содержат y .

Подставляя вместо y переменную x_1 , получаем

$$\mathrm{Tr}(u_i^{\alpha_i(j+1)}) = \mathrm{Tr}(u_1^{\alpha_1 \cdot p^{k_1}}).$$

Поскольку слова u_1 и u_i не являются степенями собственных подслов, то u_1 и u_i получаются друг из друга циклическим сдвигом и $\alpha_i(j+1) = \alpha_1 p^{k_1}$. Так как α_i не кратно p , то $j+1 : p^{k_1}$. С учетом $j \leq p^{k_i} - 1$ и $k_i \leq k_1$ это означает, что $j = p^{k_1} - 1$, $k_i = k_1$, $\alpha_i = \alpha_1$. По определению канонической записи равенство слов u_i и u_1 с точностью до циклической перестановки и равенства $k_i = k_1$, $\alpha_i = \alpha_1$ при $i > 1$ одновременно выполняться не могут.

Покажем теперь, что $\hat{w}$ не встречается в некоторой канонической записи линеаризации мономов, отличных от $\hat{m}$. Действительно, пусть моном $\hat{m}'$ отличен от $\hat{m}$ и имеет канонический вид

$$\hat{m}' = d_{p^{l_1}}(v_1^{\gamma_1})^{\delta_1} \dots d_{p^{l_t}}(v_t^{\gamma_t})^{\delta_t}.$$

Меняя обозначения в формуле (17), получаем, что каноническая запись полинома $D(\hat{m}')$ является линейной комбинацией с ненулевыми коэффициентами некоторых полиномов

$$d_{p^{l_1}}(u_1^{\gamma_1})^{\delta_1} \dots d_{p^{l_i}}(u_i^{\gamma_i})^{\delta_i-1} d_{p^{l_i-1-j}}(v_i^{\gamma_i}) \mathrm{Tr}(v_i^{\gamma_i(j+1)-1} v_i') \dots d_{p^{l_t}}(v_t^{\gamma_t})^{\delta_t}, \quad (18)$$

где $j \leq p^{l_i} - 1$, $v_i'|_{y \rightarrow x_1} = v_i$. Кроме того, ясно, что $l_i \leq k_1$. Рассмотрим каноническую запись полинома (18), аналогичную той, которая рассматривалась для полинома (17).

Если некоторый моном в этой канонической записи полинома (18) совпадает с $\hat{w}$, то аналогично изложенному выше заключаем, что $l_i = k_1$, $\gamma_i = \alpha_1$, $j = p^{k_1} - 1 = p^{l_i} - 1$ и слова u_1 , v_i равны с точностью до циклического сдвига. Далее получаем равенство

$$\begin{aligned} & d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1-1} d_{p^{k_2}}(u_2^{\alpha_2})^{\beta_2} \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s} \\ &= d_{p^{l_1}}(u_1^{\gamma_1})^{\delta_1} \dots d_{p^{l_i}}(u_i^{\gamma_i})^{\delta_i-1} \dots d_{p^{l_t}}(v_t^{\gamma_t})^{\delta_t}, \end{aligned}$$

откуда с учетом $d_{p^{k_1}}(u_1^{\alpha_1}) = d_{p^{l_i}}(u_i^{\gamma_i})$ имеем $\beta_1 = \delta_i$ и

$$\begin{aligned} & d_{p^{k_2}}(u_2^{\alpha_2})^{\beta_2} \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s} \\ &= d_{p^{l_1}}(u_1^{\gamma_1})^{\delta_1} \dots d_{p^{l_{i-1}}}(u_{i-1}^{\gamma_{i-1}})^{\delta_{i-1}} d_{p^{l_{i+1}}}(u_{i+1}^{\gamma_{i+1}})^{\delta_{i+1}} \dots d_{p^{l_t}}(v_t^{\gamma_t})^{\delta_t}. \end{aligned}$$

Тем самым, мономы $\hat{m}$ и $\hat{m}'$ равны.

Итак, в случае 1 моном $\hat{w}$ входит с ненулевым коэффициентом в некоторую каноническую запись частичной линеаризации $D(\hat{f})$ полинома $\hat{f}$.

Случай 2. Пусть теперь все неотмеченные мономы вида (10), входящие в каноническую запись $\hat{f}$, удовлетворяют следующему свойству: если $k_i \neq 0$, то $\beta_i \vdots p$.

Тогда в каноническую запись $\hat{f}$ входит некоторый моном вида (10), для которого $k_i = 0$, но β_i не кратно p . По определению отмеченного монома или $\beta_i > 1$, или $\beta_i = 1$, но при этом слово $u_i^{\alpha_i}$ зависит от некоторой переменной x_1 , по которой моном (10) имеет степень > 1 . Если $\beta_i > 1$, то степень монома (10) по любой переменной x_1 , входящей в слово $u_i^{\alpha_i}$, больше 1. Без ограничения общности можно считать $i = 1$.

Из (15) и замечания 4 вытекает, что некоторая каноническая запись $D(\hat{m})$ содержит с ненулевым коэффициентом $\alpha_1 \beta_1$ моном канонического вида

$$\alpha_1 \beta_1 \operatorname{Tr}(u_1^{\alpha_1})^{\beta_1 - 1} \operatorname{Tr}(u_1^{\alpha_1 - 1} u'_1) d_{p k_2} (u_2^{\alpha_2})^{\beta_2} \dots d_{p k_s} (u_s^{\alpha_s})^{\beta_s}, \quad (19)$$

где u'_1 зависит от y и $u'_1|_{y \rightarrow x_1} = u_1$.

Совершенно аналогично случаю 1 (но проще за счет импликации $(k_i \neq 0) \Rightarrow (\beta_i \vdots p)$) показывается, что в некоторую каноническую запись частичной линеаризации $D(\hat{f})$ полинома $\hat{f}$ моном (19) входит с коэффициентом $\alpha_1 \beta_1 \neq 0$. Лемма 4 доказана.

ЗАМЕЧАНИЕ 5. При доказательстве основной теоремы в работе [7] был доказан следующий факт. Рассмотрим произвольный набор различных чистых полилинейных мономов со следом $\hat{m}_1, \dots, \hat{m}_s$ канонического вида от переменных $x_1, \dots, x_l$. Тогда вместо переменных x_i можно так подставить матричные единицы из любой алгебры M_N , $N \geq l$, что значение монома $\hat{m}_1$ будет равно единице, а значения всех мономов $\hat{m}_2, \dots, \hat{m}_s$ будут равны нулю.

ЛЕММА 5. Пусть полиоднородный чистый полином $\hat{f}(x_1, \dots, x_m)$ имеет ненулевую каноническую запись. Тогда $\hat{f}$ не является тождеством алгебры матриц некоторого порядка.

ДОКАЗАТЕЛЬСТВО. Для каждого полиоднородного полинома $\hat{g}(x_1, \dots, x_k)$ рассмотрим величину $d(\hat{g}) = \deg \hat{g} - k$.

Будем вести индукцию по паре $(\deg \hat{f}, d(\hat{f}))$. Множество таких пар упорядочим сначала по первой координате, затем по второй. Для полиномов степени 1 лемма очевидна. Если $d(\hat{f}) = 0$, т.е. если полином $\hat{f}$ является полилинейным, утверждение леммы вытекает из замечания 5. Для всех остальных полиномов рассмотрим два случая.

Случай 1. В рассматриваемой канонической записи $\hat{f}$ содержатся только отмеченные мономы. Предположим сначала, что $\hat{f}$ имеет степень 1 хотя бы по одной из переменных. Через S обозначим множество переменных, по которым степень $\hat{f}$ равна единице. Не ограничивая общности, будем считать, что $S = \{x_1, \dots, x_l\}$.

Слагаемые в ненулевой канонической записи полинома $\hat{f}$ можно сгруппировать в виде

$$\hat{f} = \sum_i \hat{m}_i(x_1, \dots, x_l) \hat{f}_i(x_{l+1}, \dots, x_m), \quad (20)$$

где $\hat{m}_i$ – различные чистые мономы со следом канонического вида, $\hat{f}_i$ – некоторые чистые полиномы с формами, $l < m$. Так как каноническая запись $\hat{f}$ не равна нулю, то найдется некоторый полином $\hat{f}_j$, имеющий ненулевую каноническую запись. По замечанию 5 можно так подставить вместо $x_1, \dots, x_l$ матричные единички из алгебры матриц любого порядка $\geq l$, чтобы значение монома $\hat{m}_j$ равнялось 1, а значения мономов $\hat{m}_i$ при $i \neq j$ равнялись нулю. Тогда из (20) следует, что полином $\hat{f}_j$ должен являться чистым тождеством с формами всех алгебр M_n при $n \geq l$. Но $\hat{f}_j$ имеет ненулевую каноническую запись и $\deg \hat{f}_j < \deg \hat{f}$, поэтому по предположению индукции это невозможно.

Пусть теперь $\hat{f}$ имеет по всем переменным степень, строго большую 1. В этом случае все β_i во всех мономах вида (10), входящих в каноническую запись $\hat{f}$, кратны p . Поэтому $\hat{f}$ можно представить в виде

$$\hat{f} = (\hat{f}_0)^p,$$

где $\hat{f}_0$ – некоторый чистый полином с формами. Здесь мы воспользовались алгебраической замкнутостью поля F , извлекая из каждого коэффициента полинома $\hat{f}$ корень степени p . Полином $(\hat{f}_0)^p$ является тождеством с формами всех алгебр M_n , поэтому по лемме 3 $\hat{f}_0$ будет являться тождеством всех алгебр M_n . Полином $\hat{f}_0$ имеет ненулевую каноническую запись. Так как $\deg \hat{f}_0 < \deg \hat{f}$, то по предположению индукции это невозможно.

Случай 2. В канонической записи $\hat{f}$ содержится хотя бы один неотмеченный моном. Так как $\hat{f}$ неполилинеен, то по лемме 4 $\hat{f}$ имеет некоторую собственную частичную линейаризацию $\hat{g}$, обладающую ненулевой канонической формой. При этом $\deg \hat{g} = \deg \hat{f}$ и $d(\hat{g}) < d(\hat{f})$. Поэтому по предположению индукции $\hat{g}$ не является тождеством алгебры матриц некоторого порядка n , следовательно, полином $\hat{f}$ также не является тождеством M_n .

Пусть теперь поле F не является алгебраически замкнутым. В этом случае по доказанному выше $\hat{f}$ не является тождеством алгебры матриц некоторого порядка n над алгебраическим замыканием поля F . Это равносильно тому, что при некоторой подстановке в некоторую частичную линейаризацию полинома $\hat{f}$ вместо переменных матричных единичек получается ненулевая матрица. В свою очередь, это означает, что $\hat{f}$ не является тождеством алгебры M_n над полем F . Лемма 5 доказана.

ЗАМЕЧАНИЕ 6. При рассмотрении случая 1 можно было бы обойтись без использования леммы 3. Достаточно было заметить, что если $\hat{f}_0$ принимает ненулевое значение, то это будет ненулевая диагональная матрица, которая при возведении в произвольную степень снова будет ненулевой. Мы сослались на лемму 3 по той причине, что она имеет самостоятельный интерес.

СЛЕДСТВИЕ 1. *Каноническая запись чистого полинома с формами единственна.*

ДОКАЗАТЕЛЬСТВО. Достаточно отметить, что по построению алгебры $\hat{F}\{X\}$ все чистые тождества, выполняющиеся в ней, выполняются и во всех алгебрах M_n . Если нулевой полином из $\hat{F}\{X\}$ имеет ненулевую каноническую форму, то по лемме 5 он не является тождеством некоторой алгебры M_n ; с другой

стороны, нулевой полином является тождеством во всех алгебрах. Следствие доказано.

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 1. Используя тождества (5)–(7), приведем любой полиоднородный чистый полином $\hat{f} \in \hat{U}$ к канонической записи. Если она ненулевая, то по лемме 5 полином $\hat{f}$ не является тождеством алгебры матриц некоторого порядка, откуда $\hat{f} \notin \hat{U}$ – противоречие. Предложение доказано.

§ 4. Базис тождеств с формами алгебры матриц

Чистые тождества с формами алгебры матриц порядка n тесно связаны с описанием соотношений алгебры инвариантов полной линейной группы. Ниже приведены основные определения и результаты, касающиеся этого вопроса. При этом мы следуем статье А. Н. Зубкова [8], для удобства изменяя обозначения.

Пусть M_n – пространство квадратных матриц порядка n над бесконечным полем F . На пространстве

$$X_{n,m} = \underbrace{M_n \times \cdots \times M_n}_m$$

действует сопряжениями полная линейная группа $\mathrm{GL}(n)$ по правилу

$$g \circ (A_1, \dots, A_m) = (gA_1g^{-1}, \dots, gA_mg^{-1}), \quad g \in \mathrm{GL}(n), \quad A_i \in M_n.$$

Это действие на многообразии $X_{n,m}$ индуцирует действие на его координатном кольце

$$F[X_{n,m}] = F[x_{ij}^{(t)} \mid i, j = 1, 2, \dots, n; t = 1, 2, \dots, m].$$

Через $J_{n,m} = F[X_{n,m}]^{\mathrm{GL}(n)}$ обозначим F -алгебру инвариантов при рассматриваемом действии.

Гипотеза Прочези, доказанная С. Донкиным (см. [9]), описывает порождающие элементы $J_{n,m}$ над бесконечным полем положительной характеристики. Обозначим через X_t , $t = 1, 2, \dots, m$, общую матрицу порядка n , в которой в i -й строке и j -м столбце стоит переменная $x_{ij}^{(t)}$. Тогда в качестве порождающих элементов F -алгебры $J_{n,m}$ можно взять элементы $d_s(X_{i_1} \cdots X_{i_k})$, $s = 1, 2, \dots, n$, где $d_s(X)$ с точностью до знака есть s -й коэффициент характеристического многочлена матрицы X , т.е. это значение канонической формы на общей матрице X . Как уже отмечалось выше, над полем характеристики p можно рассматривать только элементы $d_s(X_{i_1} \cdots X_{i_k})$ при $s = p^0, p^1, p^2, \dots$. Если же $\mathrm{char} F = 0$, то коэффициенты характеристического многочлена выражаются через следы, и кольцо $J_{n,m}$ порождается следами произведений общих матриц. Случай нулевой характеристики был рассмотрен Прочези в работе [10].

Для $N \geq n$ имеет место естественный эпиморфизм $\alpha_{N,n}: J_{N,m} \rightarrow J_{n,m}$. Он индуцирован отображением на общих $N \times N$ -матрицах, при котором переменные $x_{ij}^{(t)}$ отображаются в нуль при $i > n$ или при $j > n$. Таким образом, можно определить свободную алгебру инвариантов J_m как $J_m = \mathrm{projlim}_n J_{n,m}$, где $\mathrm{projlim}$ – проективный предел.

Охарактеризуем свободную алгебру инвариантов J_m в терминах чистых тождеств с формами. Для этого рассмотрим алгебру чистых полиномов с формами $\hat{A}_m = \hat{F}\{x_1, \dots, x_m\}$ от переменных $x_1, \dots, x_m$, где $\hat{A}_m$ – подалгебра в $\hat{F}\{X\}$. Имеется естественный морфизм $\beta_{n,m}: \hat{A}_m \rightarrow J_{n,m}$, при котором элемент $d_{p^s}(x_{i_1} \cdots x_{i_k})$ при $p^s > n$ отображается в нуль, а при $p^s \leq n$ отображается в порождающий элемент $d_{p^s}(X_{i_1} \cdots X_{i_k})$ алгебры $J_{n,m}$. На остальные элементы из $\hat{A}_m$ отображение $\beta_{n,m}$ продолжается по мультипликативности и линейности. Так как все соотношения, наложенные на алгебру $\hat{A}_m$, выполнены в алгебре $J_{n,m}$, то отображение определено корректно.

По построению $\beta_{n,m}$ является эпиморфизмом, его ядро обозначим $\hat{\Gamma}_{n,m}$. Ясно, что $\hat{\Gamma}_{n,m}$ – это в точности множество чистых тождеств с формами алгебры матриц M_n от переменных $x_1, \dots, x_m$. По определению проективного предела существует отображение $\beta_m: \hat{A}_m \rightarrow J_m$, для которого $\theta_{n,m} \circ \beta_m = \beta_{n,m}$ при всех $n = 1, 2, \dots$, где через $\theta_{n,m}$ обозначена естественная проекция $\theta_{n,m}: J_m \rightarrow J_{n,m}$. Легко видеть, что β_m является эпиморфизмом и что его ядро $\hat{U}_m$ совпадает с $\bigcap_{n=1}^{+\infty} \hat{\Gamma}_{n,m}$.

Сделаем отступление о нулевой характеристике. Если $\text{char } F = 0$, то по упоминавшейся выше теореме Прочези алгебра J_m порождается следами общих матриц. Если обозначить через $\tilde{T}_m$ алгебру чистых полиномов со следом от переменных $x_1, \dots, x_m$, то аналогично вышеизложенному определен эпиморфизм $\tilde{T}_m \rightarrow J_m$. Ядро этого эпиморфизма совпадает с $\bigcap_{n=1}^{+\infty} \tilde{T}_{n,m}$, где $\tilde{T}_{n,m}$ – идеал чистых тождеств со следом от переменных $x_1, \dots, x_m$ алгебры M_n . Из замечания 5 легко следует, что $\bigcap_{n=1}^{+\infty} \tilde{T}_{n,m} = (0)$, и, тем самым, алгебры J_m и $\tilde{T}_m$ изоморфны.

В случае положительной характеристики поля F ситуация аналогична.

ЛЕММА 6. *Идеал $\hat{U}_m$ алгебры $\hat{A}_m$ нулевой.*

ДОКАЗАТЕЛЬСТВО. Пусть $\hat{f} \in \hat{U}_m = \bigcap_{n=1}^{+\infty} \hat{\Gamma}_{n,m}$. Тогда $\hat{f} \in \hat{U}$, и по предложению 1 $\hat{f} = 0$. Лемма доказана.

Пусть $J = \text{dirlim}_m J_m$, где dirlim – прямой предел, а также $J_n = \text{dirlim}_m J_{n,m}$. Имеется естественная проекция $\theta_n: J \rightarrow J_n$, индуцированная проекциями $\theta_{n,m}: J_m \rightarrow J_{n,m}$. Обозначим ядро проекции θ_n через $\hat{T}_n$. Идеал $\hat{T}_n$ является $\hat{T}$ -идеалом алгебры J , т.е. он инвариантен при подстановках $X_i \rightarrow F_i$, где F_i есть линейная комбинация выражений $u_0 d_{i_1}(u_1) \cdots d_{i_s}(u_s)$, u_j – непустое произведение общих матриц. Отметим, что результаты подстановок

$$X_i \rightarrow d_{i_1}(u_1) \cdots d_{i_s}(u_s)$$

в алгебре J определены не всегда.

Основная теорема в работе А. Н. Зубкова [8] утверждает, что $\hat{T}_n$ порождается как $\hat{T}$ -идеал элементами $d_{n+1}(x), d_{n+2}(x), \dots$.

По лемме 6 $J_m \cong \hat{A}_m$. Отсюда немедленно следует, что $J \cong \hat{F}\{X\}$. Тем самым, из результатов А. Н. Зубкова вытекает следующее предложение.

ПРЕДЛОЖЕНИЕ 2. *Идеал чистых тождеств с формами алгебры M_n порождается как чистый $\hat{T}$ -идеал тождествами $d_{n+1}(x) = 0, d_{n+2}(x) = 0, \dots$.*

Из предложения 2 легко можно вывести описание базиса тождеств с формами алгебры M_n .

ПРЕДЛОЖЕНИЕ 3. *Идеал $\widehat{T}[M_n]$ порождается как $\widehat{T}$ -идеал тождествами $d_N(x) = 0$ при $N > n$, $d_{p^s}(1) = C_n^{p^s}$ при $p^s \leq n$ и тождеством Кэли–Гамильтона $\chi_n(x) = 0$.*

Доказательство предложения аналогично изложенному в [8] и здесь не приводится.

При изучении тождеств алгебры M_n неудобно работать в алгебре $\widehat{F}\langle X \rangle$, где имеются формы $d_{p^i}(x)$ при $p^i > n$, тождественно равные нулю на M_n , но при этом некоторые линейаризации форм $d_{p^i}(x)$, $p^i > n$, являются нетривиальными соотношениями между формами $d_{p^i}(x)$, $p^i \leq n$. Поэтому рассмотрим в $\widehat{F}\langle X \rangle$ подалгебру с единицей $\widetilde{F}\langle X \rangle$, порожденную множеством $\langle X \rangle^\sharp$ и символами $d_{p^i}(u)$, $u \in \langle X \rangle^\sharp$, при $p^i \leq n$. В силу замечания 1 и замечания 2 $\widetilde{F}\langle X \rangle$ содержит формы $d_i(x)$, $i \leq n$, а также все их частичные линейаризации. Элементы $\widetilde{F}\langle X \rangle$, как и элементы $\widehat{F}\langle X \rangle$, будем называть *полиномами с формами*. Естественным образом можно определить понятие $\widetilde{T}$ -идеала и т.п. Через $\widehat{K}_n$ обозначим $\widetilde{T}$ -идеал алгебры $\widetilde{F}\langle X \rangle$, порожденный тождествами нулевой степени $d_{p^i}(1) = C_n^{p^i}$, $p^i \leq n$, а через $\widehat{K}_n$ обозначим $\widehat{T}$ -идеал, порожденный тождествами $d_{p^i}(1) = C_n^{p^i}$, $p^i \leq n$, и $d_{p^i}(1) = 0$, $p^i > n$.

Опишем базис тождеств с формами алгебры M_n в алгебре $\widetilde{F}\langle X \rangle$. Для этого докажем несколько вспомогательных утверждений.

Рассмотрим мономы с формами из $\widehat{F}\langle X \rangle / \widehat{K}_n$

$$\widehat{m} = u_0 d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1} d_{p^{k_2}}(u_2^{\alpha_2})^{\beta_2} \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s}, \quad (21)$$

где $s \geq 0$, $u_i \in \langle X \rangle$, $i = 1, \dots, s$, $u_0 \in \langle X \rangle^\sharp$, а чистые мономы

$$d_{p^{k_1}}(u_1^{\alpha_1})^{\beta_1} d_{p^{k_2}}(u_2^{\alpha_2})^{\beta_2} \dots d_{p^{k_s}}(u_s^{\alpha_s})^{\beta_s}$$

удовлетворяют условиям 1)–4) для (10). Несложно показать, что все такие мономы образуют линейный базис алгебры $\widehat{F}\langle X \rangle / \widehat{K}_n$.

В дальнейшем все элементы из $\widehat{F}\langle X \rangle / \widehat{K}_n$ будем записывать как однозначно определенные линейные комбинации элементов вида (21).

Представим произвольный полином с формами $\widehat{f} \in \widehat{F}\langle X \rangle / \widehat{K}_n$ в виде линейной комбинации мономов вида (21). Если положить все d_{p^i} при $p^i > n$ равными нулю, то получится некоторый полином с формами, принадлежащий алгебре $\widetilde{F}\langle X \rangle / \widehat{K}_n$. Обозначим его $\widehat{f}^+$ и положим $\widehat{f}^- = \widehat{f} - \widehat{f}^+$. Ясно, что отображения $\widehat{f} \rightarrow \widehat{f}^+$ и $\widehat{f} \rightarrow \widehat{f}^-$ являются линейными. Кроме того, отображение $\widehat{f} \rightarrow \widehat{f}^+$ является гомоморфизмом F -алгебр $\widehat{F}\langle X \rangle / \widehat{K}_n \rightarrow \widetilde{F}\langle X \rangle / \widehat{K}_n$. Очевидно также, что рассматриваемые отображения коммутируют с операторами подстановок $x_i \rightarrow u_i$, $u_i \in \langle X \rangle$.

ЛЕММА 7. *Для каждого $N > n$ и произвольных $u_1, \dots, u_m \in \langle X \rangle$ полином $[d_N(u_1 + \dots + u_m)]^+$ можно представить в виде линейной комбинации полиномов*

$$L_\rho(d_k^+(x))|_{x_i \rightarrow w_i} \cdot \widetilde{u}, \quad (22)$$

$$L_\rho(d_{k,(s,k-s)}^+(x, y))|_{x_i \rightarrow w_i} \cdot \widetilde{u}, \quad (23)$$

где $n < k \leq N$, $w_i \in \langle X \rangle$, $1 \leq s < k$; $\tilde{u}$ – чистый моном с формами в каноническом виде из алгебры $\tilde{F}\langle X \rangle$ или формальная единица; L_ρ – оператор некоторой частичной линеаризации.

ДОКАЗАТЕЛЬСТВО. Будем вести индукцию по N . Если $N = n + 1$, то $[d_N(u_1 + \dots + u_m)]^+$ есть линейная комбинация полиномов

$$[d_N(u_i)]^+, \quad (24)$$

$$[d_{N,(\rho)}(x_1, \dots, x_s)|_{x_i \rightarrow w_i}]^+, \quad w_i \in \{u_1, \dots, u_m\}, \quad (25)$$

где $d_{N,(\rho)}$ – собственная линеаризация формы d_N . Ясно, что полином (24) равен $(d_N^+(x))|_{x \rightarrow u_i}$, т.е. имеет вид (22). Если в (25) $(\rho) = (\rho_1, \dots, \rho_s)$, то $d_{N,(\rho_1, N-\rho_1)}(x, y) = d_{N,(\rho_1, N-\rho_1)}^+(x, y)$ и полином (25) равен

$$L_\tau(d_{N,(\rho_1, N-\rho_1)}^+(x, y))|_{x_i \rightarrow w_i}$$

для некоторой линеаризации L_τ , т.е. имеет вид (23). Предположим, что лемма справедлива при $N = n + 1, \dots, l - 1$, и докажем ее для $N = l$.

Будем вести доказательство индукцией по m . Случай $m = 1$ очевиден, базой индукции является случай $m = 2$:

$$\begin{aligned} [d_l(u_1 + u_2)]^+ &= \left[d_l(u_1) + d_l(u_2) + \sum_{s=1}^{l-1} (d_{l,(l-l-s)}(x, y))|_{x \rightarrow u_1, y \rightarrow u_2} \right]^+ \\ &= (d_l^+(x))|_{x \rightarrow u_1} + (d_l^+(x))|_{x \rightarrow u_2} + \sum_{s=1}^{l-1} (d_{l,(l-l-s)}^+(x, y))|_{x \rightarrow u_1, y \rightarrow u_2}. \end{aligned}$$

В этой сумме все слагаемые имеют вид (22) или (23). Предположим, что $[d_l(u_1 + \dots + u_m)]^+$ есть линейная комбинация полиномов вида (22) и (23) при любых $u_1, \dots, u_m$, и докажем, что полином $[d_l(u_1 + \dots + u_m + u_{m+1})]^+$ представим в таком же виде для любых $u_1, \dots, u_m, u_{m+1}$. Имеем

$$\begin{aligned} [d_l((u_1 + \dots + u_m) + u_{m+1})]^+ &= [d_l(u_1 + \dots + u_m)]^+ + [d_l(u_m)]^+ \\ &\quad + \sum_{s=1}^{l-1} [(d_{l,(s,l-s)}(x, y))|_{x \rightarrow u_1 + \dots + u_m, y \rightarrow u_{m+1}}]^+. \end{aligned} \quad (26)$$

Первое слагаемое в правой части (26) представимо в нужном виде по предположению индукции; второе равно $(d_l^+(x))|_{x \rightarrow u_m}$. Рассмотрим s -е слагаемое в сумме из (26):

$$\begin{aligned} [(d_{l,(s,l-s)}(x, y))|_{x \rightarrow u_1 + \dots + u_m, y \rightarrow u_{m+1}}]^+ &= [(d_{l,(s,l-s)}^+(x, y))|_{x \rightarrow u_1 + \dots + u_m, y \rightarrow u_{m+1}}]^+ \\ &\quad + [(d_{l,(s,l-s)}^-(x, y))|_{x \rightarrow u_1 + \dots + u_m, y \rightarrow u_{m+1}}]^+. \end{aligned} \quad (27)$$

Первое слагаемое в правой части (27) является в силу определения частичных линеаризаций линейной комбинацией полиномов

$$L_\rho(d_{l,(s,l-s)}^+(x, y))|_{x_i \rightarrow w_i}, \quad w_i \in \langle u_1, \dots, u_{m+1} \rangle.$$

По замечанию 1, замечанию 2 и формуле (4) второе слагаемое в правой части (14) является линейной комбинацией выражений

$$\left[(d_{p^{\alpha_1}}(m_1) \cdots d_{p^{\alpha_t}}(m_t)) \Big|_{x \rightarrow u_1 + \cdots + u_m, y \rightarrow u_{m+1}} \right]^+, \quad (28)$$

где m_i – мономы от переменных x и y (зависящие, возможно, только от x или только от y); при этом для некоторого i выполнено неравенство $n < p^{\alpha_i} < l$. Без ограничения общности будем считать, что $i = 1$.

Воспользовавшись равенством $[\widehat{f}\widehat{g}]^+ = [\widehat{f}]^+[\widehat{g}]^+$ при

$$\begin{aligned} \widehat{f} &= (d_{p^{\alpha_1}}(m_1)) \Big|_{x \rightarrow u_1 + \cdots + u_m, y \rightarrow u_{m+1}}, \\ \widehat{g} &= (d_{p^{\alpha_2}}(m_2) \cdots d_{p^{\alpha_t}}(m_t)) \Big|_{x \rightarrow u_1 + \cdots + u_m, y \rightarrow u_{m+1}} \end{aligned}$$

и записав $\widehat{g}$ в виде линейной комбинации чистых мономов с формами в каноническом виде, представим полином (28) в виде линейной комбинации полиномов

$$\left[(d_{p^{\alpha_1}}(m_1)) \Big|_{x \rightarrow u_1 + \cdots + u_m, y \rightarrow u_{m+1}} \right]^+ \cdot [\widehat{u}]^+, \quad (29)$$

где $\widehat{u}$ – чистый моном в канонической форме из $\widehat{F}\langle X \rangle$ или формальная единица при $t = 1$. Ясно, что или $[\widehat{u}]^+ = 0$, или $[\widehat{u}]^+ = \widehat{u} = \widetilde{u} \in \widetilde{F}\langle X \rangle$. Так как $n < p^{\alpha_1} < l$, то по предположению индукции

$$\left[(d_{p^{\alpha_1}}(m_1)) \Big|_{x \rightarrow u_1 + \cdots + u_m, y \rightarrow u_{m+1}} \right]^+ = \left[d_{p^{\alpha_1}} \left(\sum w_j \right) \right]^+$$

есть линейная комбинация полиномов вида (22) и (23), поэтому полином (29) также представим в таком же виде. Лемма 7 доказана.

СЛЕДСТВИЕ 2. В обозначениях леммы 7 $[d_{N,(\tau)}(x_1, \dots, x_m)]^+$ есть линейная комбинация полиномов вида (22) и (23).

ДОКАЗАТЕЛЬСТВО. По лемме 7 $[d_N(x_1 + \cdots + x_m)]^+$ есть линейная комбинация полиномов вида (22) и (23). Полином $[d_{N,(\tau)}(x_1, \dots, x_m)]^+$ является полиоднородной компонентой типа (τ) полинома $[d_N(x_1 + \cdots + x_m)]^+$. Осталось заметить, что полиномы вида (22) и (23) полиоднородны, поэтому каждый из них или целиком входит в $[d_{N,(\tau)}(x_1, \dots, x_m)]^+$ в качестве слагаемого, или целиком не входит. Следствие доказано.

СЛЕДСТВИЕ 3. В обозначениях леммы 7 $[d_{N,(\tau)}(u_1, \dots, u_m)]^+$, $u_i \in \langle X \rangle$, есть линейная комбинация полиномов вида (22) и (23).

ДОКАЗАТЕЛЬСТВО. Достаточно воспользоваться коммутированием операторов подстановки $x_i \rightarrow u_i$ с оператором $\widehat{f} \rightarrow \widehat{f}^+$ и применить следствие 1. Следствие доказано.

ЗАМЕЧАНИЕ 7. Отметим, что если $\widehat{f}$ – ненулевой полиоднородный полином из $\widehat{F}\langle X \rangle$ степени $\leq n$, то $\widehat{f}$ не является тождеством M_n .

Это утверждение очевидно, если $\widehat{f}$ полилинеен. Доказательство в общем случае аналогично доказательству леммы 5, поэтому мы его опускаем.

В следующей лемме собраны свойства, относящиеся к взятию форм и к подстановке единицы в частичные линейаризации полиномов $\chi_n(x)$ и $d_N(x)$.

ЛЕММА 8. (i) Пусть $\hat{g}(x_1, \dots, x_s)$ – некоторая частичная линейаризация полинома $d_N(x)$, $N > n$. Тогда в алгебре $\hat{F}\langle X \rangle$ выполнено $\hat{g}|_{x_i=1} \equiv \gamma d_{M,(\tau)} \pmod{\hat{K}_n}$, $i = 1, \dots, s$, $\gamma \in F$ (γ зависит от i). При этом если $M \leq n$, то $\gamma = 0$.

(ii) Пусть $\hat{g}(x_1, \dots, x_s)$ – некоторая частичная линейаризация полинома Кэли–Гамильтона $\chi_n(x)$. Тогда в алгебре $\hat{F}\langle X \rangle$ выполнено $\hat{g}|_{x_i=1} \equiv 0 \pmod{\hat{K}_n}$, $i = 1, \dots, s$.

(iii) Пусть $\hat{g}(x_1, \dots, x_s)$ – некоторая частичная линейаризация полинома Кэли–Гамильтона $\chi_n(x)$. Тогда при $p^l > n$ в алгебре $\hat{F}\langle X \rangle / \hat{K}_n$ полином $d_{p^l}(\hat{g})$ является линейной комбинацией полиномов

$$d_{M,(\tau)}(x_1, \dots, x_t)|_{x_i \rightarrow u_i} \cdot \hat{w}, \quad M > n, \quad u_i \in \langle x_1, \dots, x_s \rangle,$$

где $\hat{w}$ – чистый моном с формами или единица.

ДОКАЗАТЕЛЬСТВО. Для обоснования утверждения (i) леммы воспользуемся формулой Амицура (4). Без ограничения общности будем рассматривать случай, когда в частичную линейаризацию $d_{N,(\rho)} = d_{N,(\rho_1, \dots, \rho_s)}$ осуществляется подстановка $x_s = 1$. Положим для краткости $r = \rho_s$ и $M = N - r$. Тогда по формуле Амицура

$$d_{N,(\rho_1, \dots, \rho_s)}(x_1, \dots, x_s) = \sum_{i=0}^r d_i(x_s) h_{N-i}(x_1, \dots, x_s),$$

где полином $h_{N-i}(x_1, \dots, x_s)$ представляет собой сумму всех произведений

$$(-1)^{N-i-(j_1+\dots+j_k)} d_{j_1}(c_1) \cdots d_{j_k}(c_k);$$

суммирование ведется по всем попарно различным примитивным циклам $c_1, \dots, c_k$ и всем числам $j_1, \dots, j_k$, для которых

$$j_1[c_1] + \dots + j_k[c_k] = (\rho_1, \dots, \rho_{s-1}, r - i).$$

Заметим, что все циклы c_j содержат переменные, отличные от x_s . Кроме того, $d_0(1) = 1$ и $h_{N-r} = \pm d_{M,(\rho_1, \dots, \rho_{s-1})}$, это следует из формулы Амицура для $d_{M,(\rho_1, \dots, \rho_{s-1})}$.

Если полином $h_{N-i}(x_1, \dots, x_s)|_{x_s=1}$ имеет каноническую запись

$$h_{N-i}(x_1, \dots, x_s)|_{x_s=1} = \sum_j \alpha_{i,j} \hat{m}_j,$$

то

$$d_{N,(\rho)}(x_1, \dots, x_s)|_{x_s=1} = \sum_j \left(\sum_{i=0}^r \alpha_{i,j} d_i(1) \right) \hat{m}_j. \quad (30)$$

Очевидно, что если $d_{p^s}(1) = C_m^{p^s}$ при $p^s \leq m$ и $d_{p^s}(1) = 0$ при $p^s > m$ (для краткости назовем это m -подстановкой), то $d_i(1) = C_m^i$ при $i \leq m$ и $d_i(1) = 0$

при $i > m$. Ясно, что при m -подстановках, где $m = M, M+1, \dots, N-1$, (30) превращается в чистое тождество M_m степени M . По замечанию 7 при $m = M, \dots, N-1$ получится тождественно нулевой полином, т.е. в поле F для каждого j выполнены равенства

$$\alpha_{0,j}C_m^0 + \alpha_{1,j}C_m^1 + \dots + \alpha_{r-1,j}C_m^{r-1} = -\alpha_{r,j}C_m^r, \quad m = M, \dots, N-1. \quad (31)$$

Рассмотрим (31) как систему из r линейных уравнений относительно неизвестных $\alpha_{i,j}$, $i = 0, \dots, r-1$. Докажем, что у нее единственное решение (при любых $\alpha_{r,j}$). Действительно, определитель системы равен

$$\begin{vmatrix} C_M^0 & C_M^1 & \dots & C_M^{r-1} \\ C_{M+1}^0 & C_{M+1}^1 & \dots & C_{M+1}^{r-1} \\ \dots & \dots & \dots & \dots \\ C_{M+r-1}^0 & C_{M+r-1}^1 & \dots & C_{M+r-1}^{r-1} \end{vmatrix} = \begin{vmatrix} C_M^0 & C_M^1 & \dots & C_M^{r-1} \\ 0 & C_M^0 & \dots & C_M^{r-2} \\ \dots & \dots & \dots & \dots \\ 0 & C_{M+r-2}^0 & \dots & C_{M+r-2}^{r-2} \end{vmatrix} \quad (32)$$

Второй определитель был получен из первого вычитанием из последней строки предпоследней, из предпоследней строки второй снизу строки, $\dots$, из второй строки первой строки. Индукцией из (32) получаем, что определитель системы (31) равен 1, следовательно, у нее единственное решение.

Обозначим через a_i , $i = 0, \dots, r-1$, решение системы (31) при $\alpha_{r,j} = 1$. Тогда решение системы (31) имеет вид $\alpha_{i,j} = a_i \alpha_{r,j}$, $i = 0, \dots, r-1$.

Следовательно, из (30) при n -подстановке имеем

$$\begin{aligned} d_{N,(\rho_1, \dots, \rho_s)}(x_1, \dots, x_s) \Big|_{x_s=1} &\equiv \sum_j \left(\sum_{i=0}^r \alpha_{i,j} C_n^i \right) \hat{m}_j \\ &= \sum_j \left(\alpha_{r,j} C_n^r + \sum_{i=0}^{r-1} a_i \alpha_{r,j} C_n^i \right) \hat{m}_j \\ &= \sum_j \theta \alpha_{r,j} \hat{m}_j = \pm \theta d_{M,(\rho_1, \dots, \rho_{s-1})}(x_1, \dots, x_{s-1}) \pmod{\hat{K}_n}. \end{aligned}$$

Далее, заметим, что полином $\pm \theta d_{M,(\rho_1, \dots, \rho_{s-1})}(x_1, \dots, x_{s-1})$ является тождеством M_n , поэтому по замечанию 7 при $M \leq n$ коэффициент $\pm \theta$ должен равняться нулю. Таким образом, часть (i) леммы доказана.

Докажем часть (ii) леммы. Равенство $\hat{g}|_{x_i=1} \equiv 0 \pmod{\hat{K}_n}$, $i = 1, \dots, s$, вытекает из замечания 7. Действительно, пусть $\hat{g}|_{x_i=1} \equiv \hat{h} \pmod{\hat{K}_n}$, где полином $\hat{h}$ записан как линейная комбинация мономов (21). Тогда $\hat{h} \in \hat{T}[M_n]$, откуда $\text{Tr}(y\hat{h}) \in \hat{T}[M_n]$, $\hat{h}$ не зависит от y . Чистый полином $\text{Tr}(y\hat{h})$ имеет степень $\leq n$ и является тождеством M_n . Поэтому по замечанию 7 $\text{Tr}(y\hat{h})$ является нулевым полиномом, следовательно, $\hat{h}$ тоже является нулевым полиномом.

Докажем часть (iii) леммы. Для этого рассмотрим полином $d_{p^l}(y\hat{g})$. Этот полином является линейной комбинацией слагаемых

$$d_{p^l,(\rho)}(x_1, \dots, x_s) \Big|_{x_i \rightarrow v_i} \cdot \hat{w}, \quad (33)$$

где $v_i \in \langle x_1, \dots, x_s, y \rangle$, $\hat{w}$ — чистый моном с формами, не зависящий от y , или единица. Подставим в (33) $y = 1$. По части (i) леммы (33) перейдет в полином $\gamma d_{M,(\rho)}(x_1, \dots, x_t) \Big|_{x_i \rightarrow u_i} \cdot \hat{w}$, причем $\gamma = 0$ при $M \leq n$. Лемма 8 доказана.

ЗАМЕЧАНИЕ 8. Из доказательства леммы вытекает, что в части (iii) леммы полином $\widehat{g}$ можно считать произвольным.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3. Рассмотрим полином $d_M(x)$ при $M > n$. Из леммы 8, (i) вытекает, что любое следствие полинома $d_M(x)$ (в $\widehat{F}\langle X \rangle / \widehat{K}_n$) является линейной комбинацией слагаемых

$$d_{N,(\tau)}(u_1, \dots, u_m) \cdot \widehat{w}, \quad N > n, \quad u_i \in \langle X \rangle, \quad \widehat{w} \in \widehat{F}\langle X \rangle / \widehat{K}_n. \quad (34)$$

Для полинома Кэли–Гамильтона $\chi_n(x)$ по лемме 8, (ii) выполнено свойство, что при подстановке единиц вместо некоторых переменных в любую частичную линейаризацию $L_\rho(\chi_n(x))$ получается 0 по модулю $\widehat{K}_n$. По той же лемме $d_{p^l}(L_\rho(\chi_n(x)))$ по модулю $\widehat{K}_n$ при $p^l > n$ является линейной комбинацией слагаемых вида (34). Поэтому с учетом формулы Амицура любое следствие полинома $\chi_n(x)$ (в $\widehat{F}\langle X \rangle / \widehat{K}_n$) является линейной комбинацией слагаемых вида (34) и слагаемых вида

$$\widehat{w} \cdot L_\rho(\chi_n(x))|_{x_i \rightarrow u_i} \cdot \widehat{w}', \quad u_i \in \langle X \rangle, \quad \widehat{w}, \widehat{w}' \in \widehat{F}\langle X \rangle / \widehat{K}_n, \quad (35)$$

$$d_{p^s}(L_\rho(\chi_n(x))z)|_{x_i \rightarrow u_i, z \rightarrow u} \cdot \widehat{w}, \quad p^s \leq n, \quad u, u_i \in \langle X \rangle, \quad \widehat{w} \in \widehat{F}\langle X \rangle / \widehat{K}_n, \quad (36)$$

$$d_{p^s}(L_\rho(\chi_n(x)))|_{x_i \rightarrow u_i} \cdot \widehat{w}, \quad p^s \leq n, \quad u_i \in \langle X \rangle, \quad \widehat{w} \in \widehat{F}\langle X \rangle / \widehat{K}_n. \quad (37)$$

Пусть теперь $\widetilde{f} \in \widetilde{T}[M_n]$. Так как $\widetilde{T}[M_n] \subset \widehat{T}[M_n]$, то по предложению 3 полином $\widetilde{f}$ равен в алгебре $\widehat{F}\langle X \rangle / \widehat{K}_n$ линейной комбинации полиномов вида (34)–(37). Применив к этой линейной комбинации гомоморфизм $\widehat{g} \rightarrow \widehat{g}^+$, получаем, что полином $\widetilde{f} = [\widetilde{f}]^+$ является (уже в алгебре $\widehat{F}\langle X \rangle / \widehat{K}_n$) линейной комбинацией значений гомоморфизма $\widehat{g} \rightarrow \widehat{g}^+$ на полиномах (34)–(37). Очевидно, что это значение:

- 1) на полиноме (34) является по следствию 3 линейной комбинацией полиномов (22) и (23); каждый из полиномов (22) и (23) является следствием (в $\widehat{F}\langle X \rangle$) тождеств $d_N^+(x) = 0$, $N > n$, и $d_{N,(s,N-s)}^+(x, y) = 0$, $N > n$, $0 < s < N$;
- 2) на полиноме (35) является (в $\widehat{F}\langle X \rangle$) следствием тождества $\chi_n(x) = 0$;
- 3) на полиноме (36) при $p^s \leq n$ является следствием (в $\widehat{F}\langle X \rangle$) тождества $\chi_n(x) = 0$, а при $p^s > n$ является по лемме 7 линейной комбинацией полиномов (22) и (23);
- 4) на полиноме (37) является следствием (в $\widehat{F}\langle X \rangle$) тождества

$$d_{p^s}(L_\rho(\chi_n(x))) = 0, \quad p^s \leq n.$$

В каждом из этих четырех случаев значения гомоморфизма $\widehat{g} \rightarrow \widehat{g}^+$ на полиномах (34)–(37) являются линейной комбинацией следствий полиномов (ii)–(v) из формулировки теоремы. Теорема 3 доказана.

§ 5. Некоторые тождества алгебры M_n

Рассмотрим полином $f(x_1, \dots, x_l, y_1, \dots, y_q) \in F\langle X \rangle$, имеющий степень d по переменным $x_1, \dots, x_l$. Обозначим

$$S_f^d(x_1, \dots, x_l, y_1, \dots, y_q) = \sum_{\sigma \in \text{Sym}\{1, \dots, l\}} f(x_{\sigma(1)}, \dots, x_{\sigma(l)}, y_1, \dots, y_q).$$

ЛЕММА 9. (i) При $d \leq n$ и $l = 2^n \cdot n^{2n} \cdot p$ полином $S_f^d(x_1, \dots, x_l, y_1, \dots, y_q)$ является тождеством M_n .

(ii) T -идеал U , порожденный всеми полиномами $S_f^d(x_1, \dots, x_l, y_1, \dots, y_q)$, $d = 1, 2, \dots, n$, $l = 2^n \cdot n^{2n} \cdot p$, $q \in \mathbb{N} \cup \{0\}$, является конечно базлируемым. Базис тождеств образуют полиномы, зависящие от $l(n+1) - 1$ переменных.

ДОКАЗАТЕЛЬСТВО. Пусть $(\rho_i) = (\rho_1^{(i)}, \dots, \rho_{m_i}^{(i)})$, $i = 1, \dots, l$, — разбиения числа d . Через $L_{\rho_1, \dots, \rho_l} S_f^d$ обозначим полиоднородную компоненту степени $\rho_j^{(i)}$ по переменной $x_{i,j}$ полинома

$$S_f^d \left(\sum_{j=1}^{m_1} x_{1,j}, \dots, \sum_{j=1}^{m_l} x_{l,j}, y_1, \dots, y_q \right),$$

т.е. некоторую частичную линейаризацию. Для доказательства части (i) леммы достаточно показать, что для любых разбиений $(\rho_1), \dots, (\rho_l)$ полином $L_{\rho_1, \dots, \rho_l} S_f^d$ обращается в нуль при подстановке вместо переменных $x_{i,j}$ матричных единичек $e_{\alpha, \beta}$, $\alpha, \beta = 1, \dots, n$, а вместо переменных $y_1, \dots, y_q$ — произвольных матриц. Зафиксируем подстановку матриц P такого вида.

Всего имеется не более $2^{d-1} < 2^n$ различных разбиений числа d . Так как $l = 2^n \cdot n^{2n} \cdot p$, то среди разбиений $(\rho_1), \dots, (\rho_l)$ найдется по крайней мере $l' = n^{2n} \cdot p$ одинаковых; не ограничивая общности, будем считать, что

$$(\rho_1) = \dots = (\rho_{l'}) = (d_1, \dots, d_k).$$

При фиксированном i в переменные $x_{i,1}, \dots, x_{i,k}$ можно подставить матричные единички $e_{\alpha, \beta}$ не более чем $(n^2)^k \leq n^{2n}$ способами. Так как $l' = n^{2n} \cdot p$, то среди значений индекса i найдется p значений (обозначим их $i_1, \dots, i_p$), для которых выполнено свойство: при подстановке P вместо переменных $x_{i_1,1}, \dots, x_{i_p,1}$ подставлена одна и та же матричная единичка $e_{\alpha_1, \beta_1}, \dots$, вместо переменных $x_{i_1,k}, \dots, x_{i_p,k}$ подставлена одна и та же матричная единичка e_{α_k, β_k} .

В силу инвариантности полинома $L_{\rho_1, \dots, \rho_l} S_f^d$ относительно перестановки переменных

$$x_{i,j} \rightarrow x_{\tau(i),j}, \quad \tau \in \text{Sym}\{i_1, \dots, i_p\}, \quad j = 1, \dots, k,$$

получаем, что значение полинома $L_{\rho_1, \dots, \rho_l} S_f^d$ при подстановке P является суммой $p!$ одинаковых матриц, т.е. равно нулю.

Для доказательства части (ii) леммы рассмотрим для $d = 1, \dots, n$ все мономы $m_1^{(d)}, \dots, m_{R_d}^{(d)}$ от переменных $x_1, \dots, x_l, y_1, \dots, y_q$, удовлетворяющие следующим свойствам:

- 1) степень монома $m_i^{(d)}$ по каждой из переменных $x_1, \dots, x_l$ равна d ;
- 2) $0 \leq q \leq ld - 1 \leq ln - 1$;
- 3) степень монома $m_i^{(d)}$ по каждой из переменных $y_1, \dots, y_q$ равна 1;
- 4) переменные $y_1, \dots, y_q$ идут в мономе $m_i^{(d)}$ в порядке возрастания, причем никакие две переменные y_s, y_t не стоят рядом.

Очевидно, что T -идеал U порождается всеми полиномами $S_{m_i^{(d)}}^d$, $d = 1, \dots, n$, $i = 1, \dots, R_d$, причем каждый из них зависит от $\leq l + ln - 1$ переменных. Лемма 9 доказана.

Для монома канонического вида $\tilde{m} = d_{p^{k_1}}(u_1) \cdots d_{p^{k_s}}(u_s)$, $u_i \in \langle X \rangle$ (u_i может равняться u_j), положим $\nu(\tilde{m}) = \sum_{i=1}^s p^{k_i}$. По определению будем считать $\nu(1) = 0$. В силу единственности канонической записи такое определение корректно. Отметим, что $\nu(\tilde{m}_1 \cdot \tilde{m}_2) = \nu(\tilde{m}_1) + \nu(\tilde{m}_2)$.

Определим на чистых мономах с формами бинарное отношение $\prec$. Для этого рассмотрим два чистых монома, записанных в каноническом виде:

$$\tilde{m}_1 = d_{p^{l_1}}(v_1) \cdots d_{p^{l_t}}(v_t), \quad \tilde{m}_2 = d_{p^{k_1}}(u_1) \cdots d_{p^{k_s}}(u_s), \quad u_i, v_j \in \langle X \rangle.$$

Если $\nu(\tilde{m}_1) < \nu(\tilde{m}_2)$, то положим $\tilde{m}_1 \prec \tilde{m}_2$. Если же $\nu(\tilde{m}_1) = \nu(\tilde{m}_2)$, то положим $\tilde{m}_1 \prec \tilde{m}_2$, если от мультимножества $\{p^{k_1}, p^{k_2}, \dots, p^{k_s}\}$ можно перейти к мультимножеству $\{p^{l_1}, p^{l_2}, \dots, p^{l_t}\}$ при помощи нескольких *операций подразбиения*. Операция подразбиения заменяет число p^a на несколько чисел $p^{b_1}, \dots, p^{b_q}$ так, что $p^a = p^{b_1} + \dots + p^{b_q}$. Легко видеть, что построенное отношение $\prec$ на чистых мономах транзитивно и удовлетворяет двум свойствам:

- 1) если $\tilde{m}_1 \prec \tilde{m}_2$, то $\tilde{m}_1 \cdot \tilde{m} \prec \tilde{m}_2 \cdot \tilde{m}$;
- 2) если $\tilde{m}_1 \prec \tilde{m}_2$ и $\tilde{m}'_1 \prec \tilde{m}'_2$, то $\tilde{m}_1 \cdot \tilde{m}'_1 \prec \tilde{m}_2 \cdot \tilde{m}'_2$.

Докажем, что для мономов $d_{p^{l_1}}(u_1) \cdots d_{p^{l_t}}(u_t) \neq d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$ степени $(\rho) = (p^{k_1}, \dots, p^{k_s})$ выполнено $d_{p^{l_1}}(u_1) \cdots d_{p^{l_t}}(u_t) \prec d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$. В самом деле, если некоторое слово u_i имеет длину > 1 , то из равенства

$$\sum_{i=1}^t |u_i| \cdot p^{l_i} = \sum_{j=1}^s p^{k_j},$$

где $|u_i|$ — длина слова u_i , получаем, что

$$\nu(d_{p^{l_1}}(u_1) \cdots d_{p^{l_t}}(u_t)) < \nu(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)).$$

Если же длина каждого из слов u_i равна 1, то из сравнения степеней по переменным $x_1, \dots, x_s$ заключаем, что от мультимножества $\{p^{k_1}, p^{k_2}, \dots, p^{k_s}\}$ можно перейти к мультимножеству $\{p^{l_1}, p^{l_2}, \dots, p^{l_t}\}$ при помощи нескольких операций подразбиения.

Зафиксируем разбиение $(\rho) = (p^{k_1}, \dots, p^{k_s})$ числа $N > n$ с условием $p^{k_i} \leq n$, $i = 1, \dots, s$. Ясно, что при таком ограничении на (ρ) выполнено $d_{N,(\rho)}^+ = d_{N,(\rho)}$.

По (6) форма $d_{N,(\rho)}(x_1, \dots, x_s)$ является линейной комбинацией произведений $d_{p^{l_i}}(u_i)$, $u_i \in \langle x_1, \dots, x_s \rangle$, где u_i не p -слова. Установим полезное свойство коэффициентов этой линейной комбинации.

ЛЕММА 10. Форма $d_{N,(\rho)}$ представима в виде

$$\pm d_{N,(\rho)}(x_1, \dots, x_s) = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s) + \sum_i \alpha_i \tilde{m}_i, \quad \alpha_i \in F,$$

где для каждого монома $\tilde{m}_i$ выполнено $\tilde{m}_i \prec d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$.

ДОКАЗАТЕЛЬСТВО. Необходимо показать, что моном $d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$ входит в форму $d_{N,(\rho)}$ с коэффициентом ± 1 . Для этого рассмотрим полную линеаризацию полинома $d_{N,(\rho)}$, при которой переменные x_i “расклеиваются”

в переменные $x_{i,1}, \dots, x_{i,p^{k_i}}$, $i = 1, \dots, s$. В эту линейаризацию любой полилинейный моном со следом от переменных $x_{i,j}$ входит с коэффициентом ± 1 ; в частности, это относится к моному

$$\mathrm{Tr}(x_{1,1} \cdots x_{1,p^{k_1}}) \cdots \mathrm{Tr}(x_{s,1} \cdots x_{s,p^{k_s}}). \quad (38)$$

Ясно, что в полную линейаризацию монома $d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$ моном (38) входит с коэффициентом ± 1 . Докажем, что в полную линейаризацию любого другого монома $\tilde{m}$ степени (ρ) моном (38) не входит; отсюда немедленно будет следовать, что моном $d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$ входит в полином $d_{N,(\rho)}$ с коэффициентом ± 1 .

Действительно, пусть $\tilde{m} = d_{p^{l_1}}(u_1) \cdots d_{p^{l_t}}(u_t)$. Если некоторое слово u_i зависит хотя бы от двух различных переменных, скажем, от x_α и x_β , то в полной линейаризации монома $\tilde{m}$ все слагаемые будут иметь вид

$$\mathrm{Tr}(\cdots) \cdots \mathrm{Tr}(\cdots x_{\alpha,r} \cdots x_{\beta,q} \cdots) \cdots \mathrm{Tr}(\cdots),$$

поэтому ни одно из них не совпадет с (38).

Пусть теперь моном $\tilde{m}$ имеет каноническую запись

$$\tilde{m} = d_{p^{l_1}}(x_{i_1}^{n_1}) \cdots d_{p^{l_t}}(x_{i_t}^{n_t}),$$

где все $n_1, \dots, n_t$ не кратны p (возможно, $x_{i_\alpha} = x_{i_\beta}$ при $\alpha \neq \beta$). Полная линейаризация монома $\tilde{m}$ является линейной комбинацией полилинейных мономов со следом $\mathrm{Tr}(v_1) \cdots \mathrm{Tr}(v_q)$, причем для каждого $j = 1, \dots, t$ длина некоторого слова v_{α_j} кратна n_j . Такой моном может совпасть с (38) только при условии $n_1 = \cdots = n_t = 1$. Очевидно, что в этом случае полная линейаризация монома $\tilde{m}$ содержит моном (38) только тогда, когда $\tilde{m} = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$. Лемма 10 доказана.

Рассмотрим более подробно равенство (4). Разделим в каждом слагаемом циклы $c_1, \dots, c_r$ на две группы: пусть циклы $\nu_1, \dots, \nu_q$ содержат x_1 , а циклы $\omega_1, \dots, \omega_t$ не содержат. Тогда (4) можно переписать в виде

$$\begin{aligned} d_{m,(\rho)}(x_1, \dots, x_s) &= \sum (-1)^{m - (\sum j_\alpha |\nu_\alpha|) - (j_1 + \cdots + j_q)} d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q) \\ &\quad \times \sum (-1)^{(\sum j_\alpha |\nu_\alpha|) - (i_1 + \cdots + i_t)} d_{i_1}(\omega_1) \cdots d_{i_t}(\omega_t) \\ &= \sum (-1)^{m - (\sum j_\alpha |\nu_\alpha|) - (j_1 + \cdots + j_q)} d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q) \cdot d_{l,(\tau)}(x_2, \dots, x_s) \\ &= \sum d_{l,(\tau)}(x_2, \dots, x_s) \cdot \left(\sum (-1)^{m-l - (j_1 + \cdots + j_q)} d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q) \right). \end{aligned} \quad (39)$$

В последнем равенстве в первой сумме суммирование ведется по всем таким наборам (τ) , для которых все координаты вектора $(\rho_2, \dots, \rho_s) - (\tau)$ неотрицательны, $l = \sum \tau_i$. Во второй сумме суммирование ведется по всем попарно различным примитивным циклам $\nu_1, \dots, \nu_q$, содержащим x_1 , и всем натуральным числам $j_1, \dots, j_q$, для которых $j_1[\nu_1] + \cdots + j_q[\nu_q] = (\rho_2, \dots, \rho_s) - (\tau)$.

Леммы 9, 10 и равенство (39) мы будем использовать вместе со следующим теоретико-групповым утверждением.

ЛЕММА 11. Для произвольных чисел n и l положим $r = ln^2$. Тогда для числа r выполнено следующее свойство. Если G – подгруппа симметрической группы $S_r = \text{Sym}\{1, 2, \dots, r\}$ и $|G| \leq n$, то для некоторого $m \geq l$ найдется симметрическая подгруппа $H = \text{Sym}\{j_1, \dots, j_m\} \subset S_r$ такая, что $H \cap G = \{e\}$ и $gH = Hg$ для всех $g \in G$.

ДОКАЗАТЕЛЬСТВО. Для каждого $j \in \{1, \dots, r\}$ рассмотрим множество

$$L(j) = \{k \mid \exists g \in G : g(j) = k\} \subset \{1, \dots, r\}.$$

Ясно, что множество $\{1, \dots, r\}$ является дизъюнктивным объединением некоторых подмножеств $L(j_1), \dots, L(j_s)$, которые для краткости обозначим $L_1, \dots, L_s$. Так как $|G| \leq n$, то $|L_j| \leq n$, откуда $s \geq r/n = ln$. Положим

$$M_i = L_{(i-1)l+1} \cup L_{(i-1)l+2} \cup \dots \cup L_{(i-1)l+l}, \quad i = 1, 2, \dots, n.$$

Рассмотрим непересекающиеся симметрические подгруппы $H_i = \text{Sym}\{M_i\}$, $i = 1, \dots, n$. Так как $|G| \leq n$, то группа G имеет единичное пересечение с некоторой подгруппой H_{i_0} , которую обозначим через H . Покажем, что H является искомой группой.

Во-первых, $|M_{i_0}| = |L_{(i_0-1)l+1}| + \dots + |L_{(i_0-1)l+l}| \geq l$. Во-вторых, по построению $H \cap G = \{e\}$. Осталось проверить, что для каждого $g \in G$ выполнено $gH = Hg$. Для этого достаточно показать, что если $h \in H$ и $j \notin M_{i_0}$, то $g^{-1}hg(j) = j$. Так как $j \notin M_{i_0}$ и $g(j) \in L(j)$, то с учетом $L(j) \cap M_{i_0} = \emptyset$ получаем, что $h(g(j)) = g(j)$, откуда $g^{-1}hg(j) = g^{-1}(g(j)) = j$. Лемма 11 доказана.

§ 6. Доказательство теоремы 2

На протяжении этого параграфа все рассматриваемые полиномы с формами лежат в алгебре $\tilde{F}\langle X \rangle$. Будем считать единицу алгебры $\tilde{F}\langle X \rangle$ чистым мономом с формами; степень этого монома равна нулю.

Разобьем доказательство теоремы 2 на несколько шагов.

1) Определим полином $K(z_1, \dots, z_k)$, фигурирующий в формулировке теоремы 2. Сразу отметим, что в нашей конструкции k будет равно n .

ЛЕММА 12. Для каждого n существует полиоднородный полином

$$K_0(z_1, \dots, z_n) \in F\langle X \rangle,$$

удовлетворяющий свойствам:

- (i) $K_0(z_1, \dots, z_n) \notin T[M_n]$;
- (ii) для любого чистого монома с формами $\tilde{m} \in \tilde{F}\langle X \rangle$ вида

$$\tilde{m} = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), \quad \deg(\tilde{m}) \leq n,$$

алгебра M_n удовлетворяет полиоднородному тождеству

$$\tilde{m}(x_1, \dots, x_s)K_0(z_1, \dots, z_n) = Q_{\tilde{m}}(x_1, \dots, x_s, z_1, \dots, z_n),$$

где $Q_{\tilde{m}}(x_1, \dots, x_s, z_1, \dots, z_n) \in F\langle X \rangle$.

ДОКАЗАТЕЛЬСТВО. Рассмотрим полином $q(x_1, \dots, x_n, y_1, \dots, y_{n-1})$ и положим $L(x, y_1, \dots, y_{n-1}) = q(x, x^2, \dots, x^n, y_1, \dots, y_{n-1})^r$, где $r = \max\{r_1, \dots, r_n\}$ (полином q и числа r_i определены в конце § 2). Тогда L является киллером всех форм $d_{p^k}(z)$, где $p^k \leq n$. Поэтому полином

$$K_0(z_1, \dots, z_n) = L(z_1, z_2, \dots, z_n)^n$$

является киллером всех форм $d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$ при $s \leq n$. Кроме того, в силу отсутствия делителей нуля в алгебре $F\langle X \rangle / T[M_n]$ выполнено $K_0 \notin T[M_n]$. Лемма 12 доказана.

Положим $X = X_0 \cup \{z_1, \dots, z_n\}$, $X_0 \cap \{z_1, \dots, z_n\} = \emptyset$, где X_0 – счетное множество.

В записи полиномов $Q_{\tilde{m}}(x_1, \dots, x_s, z_1, \dots, z_n)$ будем опускать переменные $z_1, \dots, z_n$. Ниже для произвольных чистых мономов с формами

$$\tilde{m}_1 = \tilde{m}_1(x_1, \dots, x_s), \quad \tilde{m}_2 = \tilde{m}_2(x_1, \dots, x_s), \quad \tilde{m}_1, \tilde{m}_2 \in \tilde{F}\langle X_0 \rangle,$$

и произвольного полинома с формами

$$\tilde{f} = \tilde{f}(x_1, \dots, x_s) \in \tilde{F}\langle X_0 \rangle / \tilde{K}_n$$

будут построены полиномы

$$R(\tilde{m}_1, \tilde{m}_2)(x_1, \dots, x_s, z_1, \dots, z_n) \in F\langle X \rangle / \Gamma, \\ R(\tilde{f})(x_1, \dots, x_s, z_1, \dots, z_n) \in F\langle X \rangle / \Gamma.$$

Для сокращения записи всюду в дальнейшем в полиномах $R(\tilde{m}_1, \tilde{m}_2)$ и $R(\tilde{f})$ также будем опускать переменные $z_1, \dots, z_n$.

Положим $K(z_1, \dots, z_n) = K_0(z_1, \dots, z_n)^2$. Ясно, что $K(z_1, \dots, z_n) \notin T[M_n]$.

2) В качестве T -идеала $\Gamma \subset T[M_n]$ возьмем T -идеал, порожденный всеми тождествами M_n , зависящими не более чем от $L = 2n(n!)^2l + n + 2$ переменных, где число l определено в лемме 9. При таком условии на L выполнено включение $U \subseteq \Gamma$, где U – T -идеал из леммы 9.

В силу теоремы А. Р. Кемера о положительном решении локальной проблемы Шпехта (см. [4]) Γ является конечно базлируемым T -идеалом. Неформально говоря, в T -идеал Γ мы включаем все тождества M_n , зависящие от не слишком большого числа переменных.

Несложно проверить, что Γ является унитарно замкнутым T -идеалом: если $f(x_1, \dots, x_s) \in \Gamma$, то $f(x_1, \dots, x_s)_{x_{i_1}, \dots, x_{i_r} \rightarrow 1} \in \Gamma$, $r \leq s$.

3) Теперь приступим к определению для произвольных чистых мономов с формами $\tilde{m}_1, \tilde{m}_2 \in \tilde{F}\langle X_0 \rangle$ полинома $R(\tilde{m}_1, \tilde{m}_2) \in F\langle X \rangle / \Gamma$. При этом будем допускать, что мономы $\tilde{m}_1, \tilde{m}_2$ могут равняться единице. Будем строить полиномы $R(\tilde{m}_1, \tilde{m}_2)$ индуктивно, считая, что все полиномы $R(\tilde{m}'_1, \tilde{m}'_2)$ с условием $\tilde{m}'_1 \cdot \tilde{m}'_2 \prec \tilde{m}_1 \cdot \tilde{m}_2$ уже построены.

При этом если уже построен полином

$$R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), d_{p^{l_1}}(x_{s+1}) \cdots d_{p^{l_t}}(x_{s+t})),$$

то для любых $u_i \in \langle X_0 \rangle$, $i = 1, 2, \dots, s + t$, где u_i не p -слова, положим

$$\begin{aligned} R(d_{p^{k_1}}(u_1) \cdots d_{p^{k_s}}(u_s), d_{p^{l_1}}(u_{s+1}) \cdots d_{p^{l_t}}(u_{s+t})) \\ = R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), d_{p^{l_1}}(x_{s+1}) \cdots d_{p^{l_t}}(x_{s+t}))|_{x_i \rightarrow u_i}. \end{aligned} \quad (40)$$

Тем самым, полиномы $R(\tilde{m}_1, \tilde{m}_2)$ определяются для всех чистых мономов с формами, вообще говоря, не единственным образом. Однако ниже будет показано, что по модулю Γ единственность имеет место, т.е. наша конструкция корректна. Более подробно вопрос о корректности обсуждается в пункте 5).

Далее, пусть полиномы $R(\tilde{m}_{1,i}, \tilde{m}_{2,j})$ уже построены и $\tilde{f}_1 = \sum_i \alpha_i \tilde{m}_{1,i}$, $\tilde{f}_2 = \sum_j \beta_j \tilde{m}_{2,j}$. Тогда положим $R(\tilde{f}_1, \tilde{f}_2) = \sum_{i,j} \alpha_i \beta_j R(\tilde{m}_{1,i}, \tilde{m}_{2,j})$.

4) Будем требовать, чтобы полиномы $R(\tilde{m}_1, \tilde{m}_2)$ обладали следующими пятью свойствами.

Свойство 1. Алгебра M_n должна удовлетворять тождеству с формами

$$\tilde{m}_1 \tilde{m}_2 K = R(\tilde{m}_1, \tilde{m}_2). \quad (41)$$

Свойство 2. Пусть $\tilde{m}_1 = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$ и $\tilde{m}_2 = d_{p^{l_1}}(x_{s+1}) \cdots d_{p^{l_t}}(x_{s+t})$. Если $k_i = k_j$, $i, j \in \{1, 2, \dots, s\}$, или $l_i = l_j$, $i, j \in \{1, 2, \dots, t\}$, то по свойству 1 алгебра M_n удовлетворяет обычному тождеству

$$R(\tilde{m}_1, \tilde{m}_2)(\dots, x_i, \dots, x_j, \dots) = R(\tilde{m}_1, \tilde{m}_2)(\dots, x_j, \dots, x_i, \dots). \quad (42)$$

Параллельно с определением $R(\tilde{m}_1, \tilde{m}_2)$ будем доказывать, что тождество (42) принадлежит T -идеалу Γ . Это тождество индуцировано свойством канонических форм $d_{p^m}(x)d_{p^m}(y) = d_{p^m}(y)d_{p^m}(x)$.

Свойство 3. Пусть $\tilde{m}_1 = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$ и $\tilde{m}_2 = d_{p^{l_1}}(x_{s+1}) \cdots d_{p^{l_t}}(x_{s+t})$. Тогда по свойству 1 для каждого $i = 1, 2, \dots, t$ алгебра M_n удовлетворяет обычному тождеству

$$R(\tilde{m}_1, \tilde{m}_2)|_{x_i=ab} = R(\tilde{m}_1, \tilde{m}_2)|_{x_i=ba}. \quad (43)$$

Параллельно с определением $R(\tilde{m}_1, \tilde{m}_2)$ будем доказывать, что тождество (43) принадлежит T -идеалу Γ . Это тождество индуцировано свойством канонических форм $d_{p^m}(ab) = d_{p^m}(ba)$.

Свойство 4. Пусть $\tilde{m}_1, \tilde{m}_2, \tilde{m}'_1, \tilde{m}'_2$ – произвольные чистые мономы с формами. Если $\tilde{m}_1 \cdot \tilde{m}_2 = \tilde{m}'_1 \cdot \tilde{m}'_2$, то по свойству 1 в алгебре M_n выполнено обычное тождество

$$R(\tilde{m}_1, \tilde{m}_2) = R(\tilde{m}'_1, \tilde{m}'_2). \quad (44)$$

Параллельно с определением $R(\tilde{m}_1, \tilde{m}_2)$ будем доказывать, что тождество (44) принадлежит T -идеалу Γ . Будем называть это свойство “перекресткой”.

Свойство 5. Пусть $N > n$ и $(\rho) = (p^{k_1}, \dots, p^{k_s})$ – некоторое разбиение числа N с условием $p^{k_i} \leq n$, $i = 1, 2, \dots, s$. Параллельно с определением $R(\tilde{m}_1, \tilde{m}_2)$ будем доказывать, что для каждого чистого монома $\tilde{m}$ тождества

$$R(d_{N,(\rho)}^+, \tilde{m}) = 0, \quad R(\tilde{m}, d_{N,(\rho)}^+) = 0 \quad (45)$$

принадлежат Γ . Ясно, что по свойству 1 эти тождества лежат в $T[M_n]$. Очевидно так же, что при рассматриваемом ограничении на (ρ) выполнено равенство $d_{N,(\rho)}^+ = d_{N,(\rho)}$.

5) Сделаем важное замечание. Определение полиномов $R(\tilde{m}_1, \tilde{m}_2)$ будет являться некорректным в том смысле, что полиномы $R(\tilde{m}_1, \tilde{m}_2)$ будут изначально определены не для мономов $\tilde{m}_1$ и $\tilde{m}_2$, а для неоднозначных *записей* мономов. Например, $R(\text{Tr}(xy), 1) \neq R(\text{Tr}(yx), 1)$ и $R(\text{Tr}(x) \text{Tr}(y), 1) \neq R(\text{Tr}(y) \text{Tr}(x), 1)$ в $F\langle X \rangle$. Для преодоления этой ситуации в T -идеал Γ включаются тождества (42) и (43). Тождества (43) вместе с определением (40) позволяют циклически переставлять слова внутри форм, если это не p -слова. Тождества (42) вместе с определением (40) позволяют менять местами произведения форм $d_{p^s}(u)$ и $d_{p^s}(v)$, если u и v не p -слова. Накладывать тождества, позволяющие менять местами $d_{p^s}(u)$ и $d_{p^t}(v)$ при $s \neq t$, нет необходимости, так как конструкция полиномов $R(\tilde{m}_1, \tilde{m}_2)$ автоматически предусматривает эту возможность даже в алгебре $F\langle X \rangle$.

Поскольку каждый чистый моном имеет единственную каноническую запись, а две равные канонические записи получаются друг из друга вышеописанными операциями, то после доказательства свойств 2 и 3 определение полиномов $R(\tilde{m}_1, \tilde{m}_2)$ становится корректным, но уже по модулю Γ . Это является основным соображением в конструкции T -идеала Γ . Тождества (44) и (45) нужны, в частности, для обоснования выполнения тождеств (42) и (43) при индукционном переходе. Кроме того, мы будем использовать их для доказательства других свойств полиномов $R(\tilde{m}_1, \tilde{m}_2)$.

Отметим в качестве примера, что полиномы $R(\text{Tr}(x_1) \cdots \text{Tr}(x_p), 1)|_{x_i \rightarrow x}$ и $R(\text{Tr}(x_1), 1)|_{x_1 \rightarrow x^p}$, вообще говоря, различны, хотя соответствуют одному и тому же моному $\text{Tr}(x)^p = \text{Tr}(x^p)$. Чтобы подобных эффектов не возникало, в формулу (40) при обосновании свойств 1–5 подставляются только мономы u_i , не являющиеся p -словами. Однако в дальнейшем (пункт 9)) будет показано, что в (40) можно подставлять p -слова с сохранением корректности конструкции. В пунктах 6)–8) подстановки p -слов использоваться не будут.

6) Определим в качестве базы индукции полиномы $R(\tilde{m}_1, \tilde{m}_2)$ с условием

$$\nu(\tilde{m}_1) \leq n, \quad \nu(\tilde{m}_2) \leq n. \quad (46)$$

Прежде всего, положим

$$\begin{aligned} & R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), d_{p^{k_{s+1}}}(x_{s+1}) \cdots d_{p^{k_t}}(x_{s+t})) \\ &= Q_{d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)}(x_1, \dots, x_s) \cdot Q_{d_{p^{k_{s+1}}}(x_{s+1}) \cdots d_{p^{k_t}}(x_{s+t})}(x_{s+1}, \dots, x_{s+t}), \end{aligned}$$

где полиномы $Q_{\tilde{m}}(\cdot)$ определены в лемме 12. При этом считаем, что

$$Q_1(z_1, \dots, z_n) = K_0(z_1, \dots, z_n).$$

Далее по формуле (40) определим $R(\tilde{m}_1, \tilde{m}_2)$ для произвольных мономов $\tilde{m}_1, \tilde{m}_2$ с условием (46). Полиномы $Q_{\tilde{m}}(\cdot)$ из леммы 12 определены, разумеется, неоднозначно, поэтому мы каким-либо образом фиксируем способ их выбора.

Если в лемме 12 выполнено $k_i = k_j$, $i, j \in \{1, 2, \dots, s\}$, то алгебра M_n удовлетворяет обычному тождеству

$$Q_{\tilde{m}}(\dots, x_i, \dots, x_j, \dots) = Q_{\tilde{m}}(\dots, x_j, \dots, x_i, \dots). \quad (47)$$

Так как число L больше, чем число переменных в каждом из тождеств (47), то все такие тождества лежат в T -идеале Γ . Очевидно, что все тождества (42) при условии (46) являются следствиями системы тождеств (47).

Далее, если моном $\tilde{m}$ имеет вид $\tilde{m} = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$, то для каждого $i = 1, 2, \dots, s$ алгебра M_n удовлетворяет обычному тождеству

$$Q_{\tilde{m}}(x_1, \dots, x_s)|_{x_i=ab} = Q_{\tilde{m}}(x_1, \dots, x_s)|_{x_i=ba}, \quad (48)$$

в котором менее L переменных. Следовательно, все тождества (48) лежат в T -идеале Γ . Поэтому Γ будет содержать все тождества (43) при условии (46), так как они являются следствиями системы тождеств (48).

Наконец, если

$$\tilde{m}_1 \cdot \tilde{m}_2 = \tilde{m}'_1 \cdot \tilde{m}'_2,$$

где

$$\begin{aligned} \nu(\tilde{m}_i) &\leq n, & \nu(\tilde{m}'_i) &\leq n, \\ \tilde{m}_1 &= d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), & \tilde{m}_2 &= d_{p^{l_1}}(x_{s+1}) \cdots d_{p^{l_t}}(x_{s+t}), \end{aligned}$$

то число L больше, чем число переменных в каждом тождестве (44) с этими ограничениями. Поэтому Γ будет содержать все тождества (44) с условиями $\nu(\tilde{m}_i) \leq n$, $\nu(\tilde{m}'_i) \leq n$.

Теперь определим все полиномы $R(\tilde{m}_1, \tilde{m}_2)$ с условием $\nu(\tilde{m}_1 \tilde{m}_2) \leq 2n$, которые не были определены ранее. Для этого рассмотрим чистые мономы

$$\tilde{m}_1 = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), \quad \tilde{m}_2 = d_{p^{l_1}}(x_{s+1}) \cdots d_{p^{l_t}}(x_{s+t})$$

с условием $\nu(\tilde{m}_1) > n$, $\nu(\tilde{m}_2) < n$ или $\nu(\tilde{m}_2) > n$, $\nu(\tilde{m}_1) < n$. Допустим, что уже определены все полиномы $R(\tilde{m}'_1, \tilde{m}'_2)$ с условием $\tilde{m}'_1 \cdot \tilde{m}'_2 \prec \tilde{m}_1 \cdot \tilde{m}_2$.

Пусть $N_1 = \nu(\tilde{m}_1) = \deg \tilde{m}_1$, $N_2 = \nu(\tilde{m}_2) = \deg \tilde{m}_2$. Если $N_1 > n$, то рассмотрим полином $d_{N_1, (p^{k_1}, \dots, p^{k_s})}^+(x_1, \dots, x_s) = d_{N_1, (p^{k_1}, \dots, p^{k_s})}(x_1, \dots, x_s)$, который по лемме 10 имеет вид

$$\pm d_{N_1, (p^{k_1}, \dots, p^{k_s})}^+(x_1, \dots, x_s) = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s) + \sum_i \alpha_i \tilde{m}_{1,i}, \quad (49)$$

где $\alpha_i \in F$, и для каждого i выполнено $\tilde{m}_{1,i} \prec \tilde{m}_1$.

Аналогично, если $N_2 > n$, то полином $d_{N_2, (p^{l_1}, \dots, p^{l_t})}^+(x_{s+1}, \dots, x_{s+t})$ имеет вид

$$\pm d_{N_2, (p^{l_1}, \dots, p^{l_t})}^+(x_{s+1}, \dots, x_{s+t}) = d_{p^{l_1}}(x_{s+1}) \cdots d_{p^{l_t}}(x_{s+t}) + \sum_j \beta_j \tilde{m}_{2,j}, \quad (50)$$

где $\beta_j \in F$, и для каждого j выполнено $\tilde{m}_{2,j} \prec \tilde{m}_2$.

Если $N_1 > n$ и $N_2 \leq n$, то положим

$$R(\tilde{m}_1, \tilde{m}_2) = - \sum_i \alpha_i R(\tilde{m}_{1,i}, \tilde{m}_2). \quad (51)$$

Если $N_1 \leq n$ и $N_2 > n$, то положим

$$R(\tilde{m}_1, \tilde{m}_2) = - \sum_j \beta_j R(\tilde{m}_1, \tilde{m}_{2,j}). \quad (52)$$

Так как L достаточно велико, то выполняются свойства 1–4 (соответствующие тождества зависят не более чем от $3n < L$ переменных). Свойство 5 при этом тоже выполнено. В самом деле, формула (51) равносильна тому, что

$$R(d_{N_1, (p^{k_1}, \dots, p^{k_s})}, \tilde{m}_2) = 0,$$

а формула (52) равносильна равенству

$$R(\tilde{m}_1, d_{N_2, (p^{l_1}, \dots, p^{l_t})}) = 0.$$

Итак, в качестве базы индукции определены все полиномы $R(\tilde{m}_1, \tilde{m}_2)$ с условием $\nu(\tilde{m}_1 \tilde{m}_2) \leq 2n$, удовлетворяющие свойствам 1–4. При этом тождества (45) выполнены для всех $d_{N, (\rho)}$ и $\tilde{m}$ с условием $\nu(d_{N, (\rho)} \cdot \tilde{m}) \leq 2n$. Под значением функции $\nu(\tilde{f})$ на чистом полиноме $\tilde{f}$ мы понимаем максимум значений ν на мономах, которые входят в каноническую запись $\tilde{f}$ с ненулевыми коэффициентами.

7) Рассмотрим чистые мономы

$$\tilde{m}_1 = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), \quad \tilde{m}_2 = d_{p^{l_1}}(x_{s+1}) \cdots d_{p^{l_t}}(x_{s+t})$$

с условием $\nu(\tilde{m}_1) > n$ или $\nu(\tilde{m}_2) > n$. Пусть для всех мономов $\tilde{m}'_1, \tilde{m}'_2$ с условием $\tilde{m}'_1 \cdot \tilde{m}'_2 \prec \tilde{m}_1 \cdot \tilde{m}_2$ уже определены полиномы $R(\tilde{m}'_1, \tilde{m}'_2)$, удовлетворяющие свойствам 1–4. Кроме того, пусть выполнено свойство 5 для всех $d_{N, (p^{\alpha_1}, \dots, p^{\alpha_r})}$ и $\tilde{m}$ с условием $\tilde{u} \tilde{m} \prec \tilde{m}_1 \tilde{m}_2$, где $\tilde{u} = d_{p^{\alpha_1}}(x_1) \cdots d_{p^{\alpha_r}}(x_r)$ – старший относительно порядка $\prec$ моном в $d_{N, (p^{\alpha_1}, \dots, p^{\alpha_r})}$. Определим полиномы $R(\tilde{m}_1, \tilde{m}_2)$, также удовлетворяющие свойствам 1–4 и свойству 5 для $d_{N, (p^{\alpha_1}, \dots, p^{\alpha_r})}$ и $\tilde{m}$ с условием $\tilde{u} \tilde{m} = \tilde{m}_1 \tilde{m}_2$. Затем по формуле (40) определим

$$R(d_{p^{k_1}}(u_1) \cdots d_{p^{k_s}}(u_s), d_{p^{l_1}}(u_{s+1}) \cdots d_{p^{l_t}}(u_{s+t})),$$

где u_i не p -слова.

Пусть $N_1 = \nu(\tilde{m}_1) = \deg \tilde{m}_1$, $N_2 = \nu(\tilde{m}_2) = \deg \tilde{m}_2$. Аналогично вышеизложенному при $N_1 > n$ рассматриваем полином $d_{N_1, (p^{k_1}, \dots, p^{k_s})}(x_1, \dots, x_s)$ вида (49), а при $N_2 > n$ рассматриваем полином $d_{N_2, (p^{l_1}, \dots, p^{l_t})}(x_{s+1}, \dots, x_{s+t})$ вида (50).

Если $N_1 > n$ и $N_2 > n$, то положим

$$R(\tilde{m}_1, \tilde{m}_2) = \sum_{i,j} \alpha_i \beta_j R(\tilde{m}_{1,i}, \tilde{m}_{2,j}). \quad (53)$$

Если $N_1 > n$ и $N_2 \leq n$, то определяем $R(\tilde{m}_1, \tilde{m}_2)$ по формуле (51).

Если $N_1 \leq n$ и $N_2 > n$, то определяем $R(\tilde{m}_1, \tilde{m}_2)$ по формуле (52).

8) Покажем, что для полинома $R(\tilde{m}_1, \tilde{m}_2)$ выполняется свойство 1. В самом деле, если полином $R(\tilde{m}_1, \tilde{m}_2)$ определен по формуле (53), то по предположению индукции

$$\begin{aligned} \tilde{m}_1 \tilde{m}_2 \cdot K &= \left(\pm d_{N_1, (p^{k_1}, \dots, p^{k_s})}^+ - \sum_i \alpha_i \tilde{m}_{1,i} \right) \left(\pm d_{N_2, (p^{l_1}, \dots, p^{l_t})}^+ - \sum_j \beta_j \tilde{m}_{2,j} \right) K \\ &\equiv \sum_{i,j} \alpha_i \beta_j \tilde{m}_{1,i} \tilde{m}_{2,j} K \equiv \sum_{i,j} \alpha_i \beta_j R(\tilde{m}_{1,i}, \tilde{m}_{2,j}) = R(\tilde{m}_1, \tilde{m}_2) \pmod{\tilde{T}[M_n]}. \end{aligned}$$

Аналогично доказывается свойство 1 в случаях, когда полином $R(\tilde{m}_1, \tilde{m}_2)$ определен по формулам (51) или (52).

Докажем, что для полинома $R(\tilde{m}_1, \tilde{m}_2)$ выполнено свойство 2. Пусть сначала $k_i = k_j$, $i, j \in \{1, \dots, s\}$. Если полином $R(\tilde{m}_1, \tilde{m}_2)$ определен по формуле (52), то для этих i, j тождество (42) является следствием тождеств (47). Если же полином $R(\tilde{m}_1, \tilde{m}_2)$ определен по формулам (51) или (52), то правая часть равенства (49) симметрична по переменным x_i и x_j . Поэтому правая часть равенств (51) или (53) симметрична по переменным x_i и x_j по модулю Γ . Действительно, достаточно воспользоваться свойствами 2 и 3 для полиномов $R(\tilde{m}_{1,i}, \tilde{m}_{2,j})$ и $R(\tilde{m}_{1,i}, \tilde{m}_2)$ по модулю Γ . Аналогично доказывается тождество (42) в случае $l_i = l_j$, $i, j \in \{1, \dots, t\}$.

Покажем, что для полинома $R(\tilde{m}_1, \tilde{m}_2)$ выполнено свойство 3. Это наиболее сложный технический шаг в конструкции полиномов $R(\tilde{m}_1, \tilde{m}_2)$. Если полином $R(\tilde{m}_1, \tilde{m}_2)$ определен по формуле (51), то тождество (43) для $i = s+1, \dots, t$ является следствием системы тождеств (48), т.е. принадлежит Γ . Если полином $R(\tilde{m}_1, \tilde{m}_2)$ определен по формуле (52), то тождество (43) для $i = 1, \dots, s$ является следствием системы тождеств (48), поэтому лежит в Γ . Рассмотрим более подробно остальные случаи. Покажем сначала выполнимость свойства 3, если полином $R(\tilde{m}_1, \tilde{m}_2)$ определен по формуле (51), $i = 1, \dots, s$; совершенно аналогично рассматривается случай, когда полином $R(\tilde{m}_1, \tilde{m}_2)$ определяется по формуле (52), $i = s+1, \dots, s+t$.

Если $N_1 \leq n(n!)^2 l$, где число l определено в лемме 9, то T -идеал Γ содержит тождество (43), так как (43) является тождеством M_n и зависит менее чем от L переменных.

Если же $N_1 > n(n!)^2 l$, то положим

$$\tilde{g}(x_2, \dots, x_s) = d_{N_1 - p^{k_1}, (p^{k_2}, \dots, p^{k_s})}(x_2, \dots, x_s) \pm d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s).$$

Знак плюс или минус выбирается в соответствии с леммой 10 так, чтобы полином $\tilde{g}(x_2, \dots, x_s)$ не содержал монома $d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s)$.

ЛЕММА 13. Если $N_1 > n(n!)^2 l$ и $\tilde{m} \preceq \tilde{m}_2$, то

$$\sum \alpha_i R(\tilde{m}_{1,i}, \tilde{m}) \equiv \pm R(d_{p^{k_1}}(x_1) \tilde{g}(x_2, \dots, x_s), \tilde{m}) \pmod{\Gamma}, \quad (54)$$

где знак плюс или минус не зависит от $\tilde{m}$.

ДОКАЗАТЕЛЬСТВО. Воспользуемся равенством (39) для формы

$$d_{N_1, (p^{k_1}, \dots, p^{k_s})}(x_1, \dots, x_s).$$

Имеем

$$\begin{aligned} \sum \alpha_i R(\tilde{m}_{1,i}, \tilde{m}) &\equiv \pm \sum R\left(d_{k_i(\tau)}(x_2, \dots, x_s) \right. \\ &\quad \times \left(\sum (-1)^{m-k-(j_1+\dots+j_q)} d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q) \right), \tilde{m} \Big) \\ &\quad \pm R(d_{p^{k_1}}(x_1) \tilde{g}(x_2, \dots, x_s), \tilde{m}), \end{aligned}$$

где первое суммирование ведется по всем наборам, указанным в формуле (39), за исключением $k = N_1 - p^{k_1}$. Докажем, что

$$\sum R\left(d_{k,(\tau)}(x_2, \dots, x_s) \times \left(\sum (-1)^{m-k-(j_1+\dots+j_q)} d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q)\right), \tilde{m}\right) \equiv 0 \pmod{\Gamma}, \quad (55)$$

откуда будет следовать утверждение леммы. Для этого рассмотрим два случая: в (55) $k > n$ и $k \leq n$.

Если $k > n$, то запишем каждое слагаемое $d_{k,(\tau)}(x_2, \dots, x_s) \cdot d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q)$ в виде линейной комбинации мономов канонического вида. Каждый из этих мономов $\prec \tilde{m}_1$, поэтому к каждому из них применимо по предположению индукции свойство 4. Отсюда по модулю Γ

$$\begin{aligned} & R\left(d_{k,(\tau)}(x_2, \dots, x_s) \cdot \left(\sum (-1)^{m-l-(j_1+\dots+j_q)} d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q)\right), \tilde{m}\right) \\ & \equiv R\left(d_{k,(\tau)}(x_2, \dots, x_s), \left(\sum (-1)^{m-l-(j_1+\dots+j_q)} d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q)\right) \cdot \tilde{m}\right). \end{aligned}$$

Осталось заметить, что последний полином по свойству 5 равен нулю по модулю Γ в силу индукционных предположений.

Случай $k \leq n$ рассматривается более сложным образом. Прежде всего, по свойству 4 (которое справедливо по предположению индукции) (55) является линейной комбинацией полиномов вида

$$\sum R(d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q), \tilde{w}_i), \quad (56)$$

где суммирование ведется по всем таким наборам попарно различных примитивных циклов $\nu_1, \dots, \nu_q$, для которых

$$j_1[\nu_1] + \dots + j_q[\nu_q] = (p^{k_1}, p^{k_2}, \dots, p^{k_s}) - (0, \tau) = (p^{k_1}, \mu) = \text{const.}$$

Докажем, что каждая сумма (56) равна нулю по модулю Γ .

Общая степень (μ) больше, чем $N_1 - n = n((n!)^2 l - 1)$, а степень (μ) по каждой из переменных $x_2, \dots, x_s$ не превосходит n . Поэтому найдется $r = (n!)^2 l$ таких переменных $x_{i_1}, \dots, x_{i_r}$, $i_j > 1$, что степень (μ) по этим переменным одинакова и равна $d \leq n$. Для краткости обозначим эти переменные $y_1, \dots, y_r$.

На множестве $\overline{E}$ всех мономов $d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q)$, по которым ведется суммирование в (56), действует симметрическая группа S_r :

$$\sigma \cdot \tilde{m}(y_1, \dots, y_r, \dots) = \tilde{m}(y_{\sigma(1)}, \dots, y_{\sigma(r)}, \dots), \quad \sigma \in S_r.$$

Ясно, что такое переименование переменных не выводит за пределы множества $\overline{E}$. Представим $\overline{E}$ в виде дизъюнктивного объединения орбит относительно рассматриваемого действия, и пусть E – произвольная из этих орбит. Для доказательства (56) покажем, что следующий полином равен нулю по модулю Γ :

$$\sum_{d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q) \in E} R(d_{j_1}(\nu_1) \cdots d_{j_q}(\nu_q), \tilde{w}_i) \equiv 0 \pmod{\Gamma}. \quad (57)$$

Для этого рассмотрим любой моном $\tilde{w} \in E$ и стабилизатор $G = \{\sigma \in S_r \mid \sigma \cdot \tilde{w} = \tilde{w}\}$. Заметим, что $|G| \leq n!$. В самом деле, если записать моном $\tilde{w}$ в виде

$$\tilde{w} = d_{j_1}(x_1^{a_1} A_1 x_1^{a_2} A_2 \cdots) d_{j_2}(x_1^{b_1} B_1 x_1^{b_2} B_2 \cdots) \cdots,$$

где все слова $A_i, B_j, \dots$ не зависят от переменной x_1 , то под действием $\sigma \in G$ на моном $\tilde{w}$ слова $A_i, B_j, \dots$ должны каким-то образом поменяться друг с другом местами. Число таких слов не превосходит степени $\tilde{w}$ по переменной x_1 , т.е. не превосходит n . Тем самым, получаем (теоретико-множественное) отображение $G \rightarrow S_n$, и нетрудно понять, что это отображение инъективно.

Выберем симметрическую подгруппу $H \subset S_r$ в соответствии с леммой 11, в которой вместо числа n рассматривается $n!$. Множество $HG = \{hg \mid h \in H, g \in G\}$ является подгруппой, поэтому множество $E = \{S_r \cdot \tilde{w}\}$ можно представить в виде дизъюнктивного объединения некоторых множеств $\{\tau HG \cdot \tilde{w}\} = \{\tau H \cdot \tilde{w}\} = \{\tau H \tau^{-1} \cdot \tau \tilde{w}\}$. При этом в множестве $\{\tau H \cdot \tilde{w}\}$ ровно $|H|$ элементов. В самом деле, если $\tau h_1 \tilde{w} = \tau h_2 \tilde{w}$, то $\tau h_1 = \tau h_2 g$ для некоторого $g \in G$, откуда $h_2^{-1} h_1 = g \in H \cap G$, следовательно, $h_1 = h_2$.

Таким образом, полином (57) является линейной комбинацией полиномов

$$\sum_{\sigma \in \tau H \tau^{-1}} R(\sigma \cdot \tau \tilde{w}, \tilde{w}_i). \quad (58)$$

Легко понять, что любой полином (58) лежит в T -идеале U из формулировки леммы 9, при этом не важно, зависит ли $\tilde{w}_i$ от переменных $y_1, \dots, y_r$. Так как $U \subset \Gamma$, то лемма 13 доказана.

Запишем полином $d_{p^{k_1}}(x_1) \tilde{g}(x_2, \dots, x_s)$ как линейную комбинацию мономов $\tilde{w}_i$ канонического вида. Тогда каждый такой моном имеет вид

$$d_{p^{k_1}}(x_1) d_{p^{f_2}}(u_2) \cdots d_{p^{f_r}}(u_r),$$

где слова $u_2, \dots, u_r$ не зависят от x_1 и $d_{p^{k_1}}(x_1) d_{p^{f_2}}(u_2) \cdots d_{p^{f_r}}(u_r) \prec \tilde{m}_1$. По предположению индукции по модулю Γ выполнено

$$\begin{aligned} R(d_{p^{k_1}}(x_1) d_{p^{f_2}}(x_2) \cdots d_{p^{f_r}}(x_r), \tilde{m}_2) \Big|_{x_1=ab} \\ \equiv R(d_{p^{k_1}}(x_1) d_{p^{f_2}}(x_2) \cdots d_{p^{f_r}}(x_r), \tilde{m}_2) \Big|_{x_1=ba}. \end{aligned}$$

Поэтому с учетом определения (40) по модулю Γ имеем

$$R(d_{p^{k_1}}(x_1) \tilde{g}(x_2, \dots, x_s), \tilde{m}_2) \Big|_{x_1=ab} \equiv R(d_{p^{k_1}}(x_1) \tilde{g}(x_2, \dots, x_s), \tilde{m}_2) \Big|_{x_1=ba}.$$

Из этого равенства и леммы 13 (в которой нужно положить $\tilde{m} = \tilde{m}_2$) вытекает тождество (43) в рассматриваемом случае.

Далее, заметим, что по модулю Γ (53) можно записать в виде

$$R(\tilde{m}_1, \tilde{m}_2) \equiv - \sum \beta_j R(\tilde{m}_1, \tilde{m}_{2,j}) \equiv - \sum \alpha_i R(\tilde{m}_{1,i}, \tilde{m}_2). \quad (59)$$

В самом деле, разность между (53) и первой суммой в (59) равна

$$\sum \beta_j \left(R(\tilde{m}_1, \tilde{m}_{2,j}) + \sum \alpha_i R(\tilde{m}_{1,i}, \tilde{m}_{2,j}) \right) \equiv \sum \pm \beta_j R(d_{N_1, (p^{k_1} \dots p^{k_s})}, \tilde{m}_{2,j}).$$

В последней сумме каждый полином $R(d_{N_1, (p^{k_1} \dots p^{k_s})}, \tilde{m}_{2,j})$ равен нулю по модулю Γ по свойству 5, которое выполнено по предположению индукции, так как $\tilde{m}_{2,j} \prec \tilde{m}_2$. Аналогично доказывается второе равенство (59).

Рассмотрим теперь последний случай в обосновании свойства 3, когда полином $R(\tilde{m}_1, \tilde{m}_2)$ определен по формуле (53). Без ограничения общности считаем в тождестве (43) $i = 1$. Сведем этот случай к уже рассмотренному случаю, когда полином $R(\tilde{m}_1, \tilde{m}_2)$ определяется по формуле (51). Многократно применяя (59), получаем, что $R(\tilde{m}_1, \tilde{m}_2)$ является по модулю Γ линейной комбинацией полиномов $R(\tilde{m}_1, \tilde{m}'_{2,j})$, где для каждого j выполнено $\nu(\tilde{m}'_{2,j}) \leq n$. По доказанному выше для каждого j имеет место равенство

$$R(\tilde{m}_1, \tilde{m}'_{2,j})|_{x_1=ab} \equiv R(\tilde{m}_1, \tilde{m}'_{2,j})|_{x_1=ba} \pmod{\Gamma},$$

что завершает доказательство свойства 3.

Докажем свойство 4. Если $\nu(\tilde{m}_1 \cdot \tilde{m}_2) \leq 2n(n!)^2l + 2$, то все тождества (44) с этим условием лежат в T -идеале Γ . Рассмотрим основной случай, когда

$$\nu(\tilde{m}_1 \cdot \tilde{m}_2) > 2n(n!)^2l + 2.$$

Покажем сначала, что если $\nu(\tilde{m}_1) > n(n!)^2l$, то любой сомножитель $d_{p^{k_i}}(x_i)$ можно “перебросить” из $\tilde{m}_1$ в $\tilde{m}_2$ по модулю Γ (назовем это *операцией 1*). Без ограничения общности достаточно доказать это утверждение для случая $i = 1$. Имеем по модулю Γ

$$\begin{aligned} R(\tilde{m}_1, \tilde{m}_2) &\equiv \pm R(d_{p^{k_1}}(x_1)\tilde{g}(x_2, \dots, x_s), \tilde{m}_2) \\ &\equiv \pm R(\tilde{g}(x_2, \dots, x_s), d_{p^{k_1}}(x_1)\tilde{m}_2) \\ &\equiv \pm R(d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s), d_{p^{k_1}}(x_1)\tilde{m}_2). \end{aligned} \quad (60)$$

Приведем обоснование равенств формулы (60). Если полином $R(\tilde{m}_1, \tilde{m}_2)$ определен по формуле (51), то первое сравнение в (60) следует из (51) и леммы 13; если же $R(\tilde{m}_1, \tilde{m}_2)$ определен по формуле (53), то оно следует из второй формулы (59) и леммы 13. Второе сравнение в (60) следует из свойства 4, которое в этом случае справедливо по предположению индукции. Третье сравнение в (60) вытекает из свойства 5, которое справедливо по предположению индукции.

Итак, из (60) получаем, что

$$R(\tilde{m}_1, \tilde{m}_2) \equiv \pm R(d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s), d_{p^{k_1}}(x_1)\tilde{m}_2).$$

Покажем, что в этой формуле на самом деле стоит знак $+$. Действительно, если $\text{char } F = 2$, то это очевидно. Если же $\text{char } F > 2$ и стоит знак $-$, то с учетом свойства 1 получаем, что $2\tilde{m}_1\tilde{m}_2 \cdot K \in \tilde{T}[M_n]$, чего быть не может в силу $\tilde{T}$ -первичности идеала $\tilde{T}[M_n]$.

Совершенно аналогично доказывается, что если $\nu(\tilde{m}_2) > n(n!)^2l$, то любой сомножитель $d_{p^{k_j}}(x_{s+j})$ можно “перебросить” из $\tilde{m}_2$ в $\tilde{m}_1$ по модулю Γ (назовем это *операцией 2*).

Легко понять, что при помощи операций 1 и 2 можно получить любое тождество (44) с условием $\nu(\tilde{m}_1 \cdot \tilde{m}_2) > 2n(n!)^2l + 2$. Свойство 4 доказано.

Для завершения индуктивной конструкции полиномов $R(\tilde{m}_1, \tilde{m}_2)$ осталось доказать свойство 5. Прежде всего, очевидно, что если $R(\tilde{m}_1, \tilde{m}_2)$ определяется по формуле (51), то $R(d_{N_1, (p^{k_1}, \dots, p^{k_s})}, \tilde{m}_2) = 0$, а если по формуле (52), то $R(\tilde{m}_1, d_{N_2, (p^{l_1}, \dots, p^{l_t})}) = 0$. Осталось рассмотреть случай, когда $R(\tilde{m}_1, \tilde{m}_2)$ определяется по формуле (53). Но тогда формулы (59) в точности означают, что

$$R(d_{N_1, (p^{k_1}, \dots, p^{k_s})}, \tilde{m}_2) \equiv 0 \pmod{\Gamma}, \quad R(\tilde{m}_1, d_{N_2, (p^{l_1}, \dots, p^{l_t})}) \equiv 0 \pmod{\Gamma}.$$

Отметим, что множество доказанных в предыдущем абзаце тождеств и тождеств из базы индукции в точности совпадает с множеством тождеств (45).

8) Следующая простая лемма многократно будет использоваться при обосновании свойств полиномов $R(\tilde{m}_1, \tilde{m}_2)$ и $R(\tilde{f})$. Ее смысл состоит в том, что “длинные” мономы $\tilde{m}_2$ могут быть выражены через “короткие” мономы $\tilde{m}_{2,j}$, тем самым, эти свойства достаточно доказывать только для “коротких” мономов $\tilde{m}_{2,j}$.

ЛЕММА 14. Полином $R(\tilde{m}_1, \tilde{m}_2)$ представляется по модулю Γ в виде

$$R(\tilde{m}_1, \tilde{m}_2) \equiv \sum_j \gamma_j R(\tilde{m}_1, \tilde{m}_{2,j}) \pmod{\Gamma},$$

где $\gamma_j \in F$, $\nu(\tilde{m}_{2,j}) \leq n$, причем коэффициенты γ_j не зависят от $\tilde{m}_1$, а зависят только от $\tilde{m}_2$.

ДОКАЗАТЕЛЬСТВО. Достаточно многократно воспользоваться равенствами (59). Лемма 14 доказана.

9) Докажем, что если моном $u_1 \cdots u_{s+t}$ зависит от переменных $y_1, \dots, y_r$, то

$$\begin{aligned} & R(d_{p^{k_1}}(u_1) \cdots d_{p^{k_s}}(u_s), d_{p^{l_1}}(u_{s+1}) \cdots d_{p^{l_t}}(u_{s+t})) \Big|_{y_i \rightarrow v_i} \\ & \equiv R((d_{p^{k_1}}(u_1) \cdots d_{p^{k_s}}(u_s)) \Big|_{y_i \rightarrow v_i}, (d_{p^{l_1}}(u_{s+1}) \cdots d_{p^{l_t}}(u_{s+t})) \Big|_{y_i \rightarrow v_i}) \pmod{\Gamma}, \end{aligned} \quad (61)$$

где $v_1, \dots, v_r \in \langle X_0 \rangle$. Это равенство означает, что оператор подстановки $y_1 \rightarrow v_1, \dots, y_r \rightarrow v_r$ “коммутирует” с билинейным отображением $R: \tilde{A} \times \tilde{A} \rightarrow F\langle X \rangle/\Gamma$, где $\tilde{A}$ – пространство, порожденное чистыми полиномами с формами от переменных из множества X_0 и единицей. Пусть при подстановке $y_i \rightarrow v_i$ слова u_j переходят в слова A_j . Нетривиальность равенства (61) состоит в том, что некоторые из A_j могут быть p -словами; тогда для вычисления правой части (61) надо сначала привести чистые мономы к каноническому виду. Во всех остальных случаях равенство (61) есть прямое следствие определения (40).

Представим A_j в виде $A_j = (B_j)^{p^{q_j}}$, где B_j не p -слова. Тогда (61) можно переписать в виде

$$\begin{aligned} & R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), d_{p^{l_1}}(x_{s+1}) \cdots d_{p^{l_t}}(x_{s+t})) \Big|_{x_j \rightarrow B_j^{p^{q_j}}} \\ & \equiv R\left(\prod_{r=1}^{p^{q_1}} d_{p^{k_1}}(x_{1,r}) \cdots, \prod_{r=1}^{p^{q_{s+1}}} d_{p^{l_1}}(x_{s+1,r}) \cdots\right) \Big|_{x_{j,r} \rightarrow B_j} \pmod{\Gamma}. \end{aligned} \quad (62)$$

Ясно, что равенство (62) достаточно доказать только для случая $B_1 = y_1, \dots, B_{s+t} = y_{s+t}$. Кроме того, по свойству 4 можно “перебросить” все множители $d_{p^\alpha}(x_\beta)$ из второго аргумента $R(\dots)$ в первый аргумент. Таким образом, после последовательных переобозначений $l_j \rightarrow k_{s+j}$ и $s+t \rightarrow s$ в формуле (62) достаточно доказать равенство

$$\begin{aligned} & R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), 1) \Big|_{x_j \rightarrow y_j^{p^{q_j}}} \\ & \equiv R\left(\prod_{r=1}^{p^{q_1}} d_{p^{k_1}}(x_{1,r}) \cdots \prod_{r=1}^{p^{q_s}} d_{p^{k_s}}(x_{s,r}), 1\right) \Big|_{x_{j,r} \rightarrow y_j} \pmod{\Gamma}. \end{aligned} \quad (63)$$

Докажем сначала, что

$$\begin{aligned} & R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), 1) \Big|_{x_1 \rightarrow y^{p^q}} \\ & \equiv R\left(\prod_{r=1}^{p^q} d_{p^{k_1}}(x_{1,r}) \cdots d_{p^{k_s}}(x_s), 1\right) \Big|_{x_{1,r} \rightarrow y} \pmod{\Gamma}, \end{aligned} \quad (64)$$

где $s \geq 1$, $q \geq 0$. Снова воспользовавшись свойством 4, получаем, что (64) равносильно равенству

$$\begin{aligned} & R(d_{p^{k_1}}(x_1), d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s)) \Big|_{x_1 \rightarrow y^{p^q}} \\ & \equiv R\left(\prod_{r=1}^{p^q} d_{p^{k_1}}(x_{1,r}), d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s)\right) \Big|_{x_{1,r} \rightarrow y} \pmod{\Gamma}. \end{aligned} \quad (65)$$

Если в (65) выполнено $\nu(d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s)) \leq n$, то тождество алгебры M_n (65) зависит от $1 + (s-1) + n \leq 2n < L$ переменных. Поэтому сравнение (65) выполнено не только по модулю $T[M_n]$, но и по модулю Γ .

Если же в (65) $\nu(d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s)) > n$, то в обозначениях леммы 14

$$\begin{aligned} & R(d_{p^{k_1}}(x_1), d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s)) \Big|_{x_1 \rightarrow y^{p^q}} \\ & \equiv \sum \gamma_j R(d_{p^{k_1}}(x_1), \tilde{m}_{2,j}) \Big|_{x_1 \rightarrow y^{p^q}} \pmod{\Gamma}, \\ & R\left(\prod_{r=1}^{p^q} d_{p^{k_1}}(x_{1,r}), d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s)\right) \Big|_{x_{1,r} \rightarrow y} \\ & \equiv \sum \gamma_j R\left(\prod_{r=1}^{p^q} d_{p^{k_1}}(x_{1,r}), \tilde{m}_{2,j}\right) \Big|_{x_{1,r} \rightarrow y} \pmod{\Gamma}, \end{aligned}$$

где $\nu(m_{2,j}) \leq n$. Осталось воспользоваться для каждого j уже доказанными равенствами

$$R(d_{p^{k_1}}(x_1), \tilde{m}_{2,j}) \Big|_{x_1 \rightarrow y^{p^q}} \equiv R\left(\prod_{r=1}^{p^q} d_{p^{k_1}}(x_{1,r}), \tilde{m}_{2,j}\right) \Big|_{x_{1,r} \rightarrow y} \pmod{\Gamma}.$$

Таким образом, равенство (64) доказано.

Далее, индукцией по $1 \leq m \leq s$ докажем, что

$$\begin{aligned} & R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_m}}(x_m) d_{p^{k_{m+1}}}(x_{m+1}) \cdots d_{p^{k_s}}(x_s), 1) \Big|_{x_j \rightarrow y_j^{p^{q_j}}, j=1, \dots, m} \\ & \equiv R\left(\prod_{r=1}^{p^{q_1}} d_{p^{k_1}}(x_{1,r}) \cdots \prod_{r=1}^{p^{q_m}} d_{p^{k_m}}(x_{m,r}) \right. \\ & \quad \left. \times d_{p^{k_{m+1}}}(x_{m+1}) \cdots d_{p^{k_s}}(x_s), 1\right) \Big|_{x_{j,r} \rightarrow y_j, j=1, \dots, m} \pmod{\Gamma}. \end{aligned} \quad (66)$$

База индукции $m = 1$ совпадает с (64), а при $m = s$ получится доказываемое равенство (63). Предположим, что тождество (66) доказано для m , и докажем его для $m + 1$. Имеем

$$\begin{aligned} & R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), 1) \Big|_{\substack{x_j \rightarrow y_j^{p^{q_j}} \\ j=1, \dots, m+1}} \\ & = \left[R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), 1) \Big|_{\substack{x_j \rightarrow y_j^{p^{q_j}} \\ j=1, \dots, m}} \right] \Big|_{x_{m+1} \rightarrow y_{m+1}^{p^{q_{m+1}}}} \\ & \equiv \left[R\left(\prod_{r=1}^{p^{q_1}} d_{p^{k_1}}(x_{1,r}) \right. \right. \\ & \quad \left. \left. \cdots \prod_{r=1}^{p^{q_m}} d_{p^{k_m}}(x_{m,r}) d_{p^{k_{m+1}}}(x_{m+1}) \cdots d_{p^{k_s}}(x_s), 1\right) \Big|_{\substack{x_{j,r} \rightarrow y_j \\ j=1, \dots, m}} \right] \Big|_{x_{m+1} \rightarrow y_{m+1}^{p^{q_{m+1}}}} \\ & = \left[R\left(\prod_{r=1}^{p^{q_1}} d_{p^{k_1}}(x_{1,r}) \right. \right. \\ & \quad \left. \left. \cdots \prod_{r=1}^{p^{q_m}} d_{p^{k_m}}(x_{m,r}) d_{p^{k_{m+1}}}(x_{m+1}) \cdots d_{p^{k_s}}(x_s), 1\right) \Big|_{x_{m+1} \rightarrow y_{m+1}^{p^{q_{m+1}}}} \right] \Big|_{\substack{x_{j,r} \rightarrow y_j \\ j=1, \dots, m}} \\ & \stackrel{(60)}{=} \left[R\left(\prod_{r=1}^{p^{q_1}} d_{p^{k_1}}(x_{1,r}) \right. \right. \\ & \quad \left. \left. \cdots \prod_{r=1}^{p^{q_{m+1}}} d_{p^{k_{m+1}}}(x_{m+1,r}) \cdots d_{p^{k_s}}(x_s), 1\right) \Big|_{x_{m+1,r} \rightarrow y_{m+1}} \right] \Big|_{\substack{x_{j,r} \rightarrow y_j \\ j=1, \dots, m}} \\ & = R\left(\prod_{r=1}^{p^{q_1}} d_{p^{k_1}}(x_{1,r}) \right. \\ & \quad \left. \cdots \prod_{r=1}^{p^{q_{m+1}}} d_{p^{k_{m+1}}}(x_{m+1,r}) \cdots d_{p^{k_s}}(x_s), 1\right) \Big|_{\substack{x_{j,r} \rightarrow y_j \\ j=1, \dots, m+1}} \pmod{\Gamma}. \end{aligned}$$

Таким образом, индукционный переход доказан, а вместе с ним доказаны тождества (63) и (61).

10) Для каждого монома с формами $\tilde{u} = u_0 \cdot \tilde{m} \in \tilde{F}\langle X_0 \rangle / \tilde{K}_n$, где $u_0 \in \langle X_0 \rangle^\sharp$, $\tilde{m}$ – чистый моном с формами или единица, положим $R(\tilde{u}) = u_0 R(\tilde{m}, 1)$. Далее, по линейности определим $R(\tilde{f})$ для произвольного полинома $\tilde{f} \in \tilde{F}\langle X_0 \rangle / \tilde{K}_n$.

Отметим, что если $\tilde{f} \in F\langle X_0 \rangle \subset \tilde{F}\langle X_0 \rangle / \tilde{K}_n$, то $R(\tilde{f}) = f \cdot K$. По свойству 1 выполнено $R(\tilde{f}) \equiv \tilde{f} \cdot K \pmod{\tilde{T}[M_n]}$.

Из доказанного в пункте 9) утверждения вытекает, что если $v_1, \dots, v_s \in \langle X_0 \rangle$, то

$$R(\tilde{f}(x_1, \dots, x_s)|_{x_i \rightarrow v_i}) \equiv R(\tilde{f})|_{x_i \rightarrow v_i} \pmod{\Gamma}. \quad (67)$$

Таким образом, линейное отображение $R: \tilde{F}\langle X_0 \rangle / \tilde{K}_n \rightarrow F\langle X \rangle / \Gamma$ “коммутирует” с оператором подстановки $x_1 \rightarrow v_1, \dots, x_s \rightarrow v_s$.

11) Докажем, что отображение R “коммутирует” с операторами частных линеаризаций. Более подробно, пусть L_ρ – некоторый оператор частичной линеаризации по переменным $x_1, \dots, x_t$. Тогда имеет место равенство

$$R(L_\rho[\tilde{f}]) \equiv L_\rho[R(\tilde{f})] \pmod{\Gamma}, \quad (68)$$

где полином с формами $\tilde{f} \in \tilde{F}\langle X_0 \rangle / \tilde{K}_n$ зависит от переменных $x_1, \dots, x_t$ и, возможно, от других переменных. Разобьем доказательство формулы (68) на несколько шагов.

а) Прежде всего, заметим, что формулу (68) достаточно доказать только для случая, когда $\tilde{f}$ является мономом с формами. Пусть $\tilde{f} = u\tilde{m}$, где $u \in \langle X_0 \rangle^\#$, $\tilde{m}$ – чистый моном с формами или единица. Тогда

$$L_\rho[u\tilde{m}] = \sum_{(\rho_1, \rho_2)} L_{\rho_1}[u] L_{\rho_2}[\tilde{m}],$$

откуда по определению полиномов $R(\tilde{g})$ получаем

$$R(L_\rho[u\tilde{m}]) = \sum_{(\rho_1, \rho_2)} L_{\rho_1}[u] R(L_{\rho_2}[\tilde{m}]). \quad (69)$$

С другой стороны,

$$L_\rho[R(u\tilde{m})] = L_\rho[u(R(\tilde{m}))] = \sum_{(\rho_1, \rho_2)} L_{\rho_1}[u] L_{\rho_2}[R(\tilde{m})]. \quad (70)$$

В (69) и (70) суммирование ведется по одному и тому же множеству пар частных линеаризаций. Сравнивая (69) и (70), заключаем, что формулу (68) достаточно доказать только для случая, когда $\tilde{f} = \tilde{m}$, где $\tilde{m}$ – чистый моном с формами.

б) Докажем, что если формула (68) верна для всех мономов

$$\tilde{m} = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s),$$

то она верна и для всех мономов $\tilde{m} = d_{p^{k_1}}(u_1) \cdots d_{p^{k_s}}(u_s)$, где $u_i \in \langle X_0 \rangle$ не p -слова.

Понятно, что достаточно рассмотреть случай линеаризации только по одной переменной, скажем, по y . Общий случай будет получаться из этого индукцией. Доказательство шага индукции мы опускаем, так как оно аналогично доказательству формулы (66).

Пусть степени мономов u_i по переменной y равны β_i , $\tilde{f}(x_1, \dots, x_s)$ – произвольный полиоднородный полином с формами степени α_i по переменной x_i , зависящий, возможно, и от других переменных, отличных от y и x_i , $i \geq 1$. Положим $r = \alpha_1\beta_1 + \dots + \alpha_s\beta_s$ и подставим вместо y сумму $y_1 + \dots + y_r$. При такой подстановке моном u_i перейдет в сумму мономов $\sum_{j=1}^{\beta_i} u_i^j$. Отметим, что u_i^j не p -слова. Для краткости обозначим $\gamma_i = \beta_i^r$. При подстановке $y \rightarrow y_1 + \dots + y_r$ полином $\tilde{f}(x_1, \dots, x_s)|_{x_i \rightarrow u_i}$ перейдет в полином $\tilde{f}(\sum_{j=1}^{\gamma_1} u_1^j, \dots, \sum_{j=1}^{\gamma_s} u_s^j)$, равный полиному

$$\sum_{\rho_1 \vdash \alpha_1} \dots \sum_{\rho_s \vdash \alpha_s} \sum_{j_{1,1} < \dots < j_{1,t_1}} \dots \sum_{j_{s,1} < \dots < j_{s,t_s}} L_{\rho_1, \dots, \rho_s}(\tilde{f})(x_{1,1}, \dots, x_{1,t_1}, \dots, x_{s,1}, \dots, x_{s,t_s})|_{x_{i,k} \rightarrow u_i^{j_{i,k}}} \quad (71)$$

В первой группе сумм суммирование ведется по всем неупорядоченным разбиениям ρ_i чисел α_i ; если такие разбиения имеют t_i слагаемых, то во второй группе сумм суммирование ведется по всем t_i -элементным подмножествам множества $\{u_i^1, \dots, u_i^{\gamma_i}\}$; через $L_{\rho_1, \dots, \rho_s}(\tilde{f})$ обозначена частичная линейаризация полинома $\tilde{f}$ типа ρ_i по переменной x_i .

Любая частичная линейаризация полинома $\tilde{f}(x_1, \dots, x_s)|_{x_i \rightarrow u_i}$ по переменной y представляет собой некоторую полиоднородную компоненту полинома (71). Возьмем в качестве полинома $\tilde{f}$ сначала моном $d_{p^{k_1}}(x_1) \dots d_{p^{k_s}}(x_s)$ и применим к (71) линейное отображение R , а затем возьмем в качестве $\tilde{f}$ полином $R(d_{p^{k_1}}(x_1) \dots d_{p^{k_s}}(x_s))$. Получим, что если для всех $\rho_1, \dots, \rho_s$ выполнено

$$R(L_{\rho_1, \dots, \rho_s}[d_{p^{k_1}}(x_1) \dots d_{p^{k_s}}(x_s)]) \equiv L_{\rho_1, \dots, \rho_s}[R(d_{p^{k_1}}(x_1) \dots d_{p^{k_s}}(x_s))] \pmod{\Gamma}, \quad (72)$$

то с учетом инвариантности Γ относительно подстановок $x_{i,k} \rightarrow u_i^{j_{i,k}}$ и (67) выполнено и равенство (68) для $\tilde{f} = d_{p^{k_1}}(u_1) \dots d_{p^{k_s}}(u_s)$, что и требовалось доказать.

в) Из пунктов а) и б) вытекает, что достаточно доказать все равенства (72). Сначала докажем (72) для случая, когда $L_{\rho_1, \dots, \rho_s}$ представляет собой некоторую частичную линейаризацию по одной переменной. Не ограничивая общности, можно считать, что это переменная x_1 , т.е. что $L_{\rho_1, \dots, \rho_s} = L_{\rho_1}$. Прежде всего, заметим, что по свойству 1 левая и правая части (72) равны по модулю $T[M_n]$. Поэтому если $\nu(d_{p^{k_2}}(x_2) \dots d_{p^{k_s}}(x_s)) \leq n$, то, так как (72) зависит от $s + n \leq 2n + 1 < L$ переменных, левая и правая части (72) равны по модулю Γ .

Если $\nu(d_{p^{k_2}}(x_2) \dots d_{p^{k_s}}(x_s)) > n$, то воспользуемся “переброской” переменных, которую мы уже применяли ранее. Из доказанного в начале пункта в) вытекает, что для произвольных мономов $\tilde{m}_j$ (с условиями: $\nu(\tilde{m}_j) \leq n$ и $\tilde{m}_j$ не имеет общих переменных с $L_{\rho_1}[d_{p^{k_1}}(x_1)]$) выполнено равенство

$$R(L_{\rho_1}[d_{p^{k_1}}(x_1)], \tilde{m}_j) \equiv L_{\rho_1}[R(d_{p^{k_1}}(x_1), \tilde{m}_j)] \pmod{\Gamma}. \quad (73)$$

Последовательно применяя “переброску”, лемму 14, равенство (73), еще раз лемму 14 и снова “переброску”, получаем

$$\begin{aligned}
 R(L_{\rho_1}[d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)]) &\equiv R(L_{\rho_1}[d_{p^{k_1}}(x_1), d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s)]) \\
 &\equiv \sum_j \gamma_j R(L_{\rho_1}[d_{p^{k_1}}(x_1), \tilde{m}_{2,j}]) \equiv \sum_j \gamma_j L_{\rho_1}[R(d_{p^{k_1}}(x_1), \tilde{m}_{2,j})] \\
 &\equiv L_{\rho_1}[R(d_{p^{k_1}}(x_1), d_{p^{k_2}}(x_2) \cdots d_{p^{k_s}}(x_s))] \\
 &\equiv L_{\rho_1}[R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s))] \pmod{\Gamma}.
 \end{aligned}$$

г) Далее индукцией по m показывается, что равенство (72) справедливо для линеаризаций по любым m переменным. Рассмотренный в пункте в) случай является базой индукции. Доказательство шага индукции мы снова опускаем, так как оно аналогично доказательству формулы (66).

12) В связи с доказанными свойствами (67) и (68) естественным образом возникает предположение, что отображение R по модулю Γ “коммутирует с операциями получения следствий” (в этом состоит весь смысл конструкции полиномов $R(\tilde{f})$). Иначе говоря, если $\tilde{g} \in \{\tilde{f}\}^T$, то $R(\tilde{g}) \in \{R(\tilde{f})\}^T$ в алгебре $F\langle X \rangle/\Gamma$; при этом на полином $\tilde{g}$ могут быть наложены несущественные ограничения. Однако это по всей видимости неверно. А именно, полином $R(f \cdot d_{p^k}(y))$ не обязательно лежит в T -идеале $\{R(\tilde{f})\}^T$ алгебры $F\langle X \rangle/\Gamma$. Дело в том, что для определенных в конце § 2 киллеров $q(x, y_1, \dots, y_n)^{r_k}$ не обязательно выполняется свойство, что $q_k(x, y_1, \dots, y_n, z) \in \{q(x, y_1, \dots, y_n)^{r_k}\}^T$. Точнее говоря, это свойство напрямую не вытекает из явной конструкции киллеров.

Вместе с тем имеет место ослабленное свойство “коммутирования отображения R с операциями получения следствий” (лемма 16 ниже), которого будет достаточно для доказательства теоремы 2. Ослабление состоит в том, что вместе с каждым полиномом с формами $\tilde{f}$ нужно рассматривать конечное множество полиномов $\{\tilde{f}\tilde{m}_j\}$, где для чистого монома $\tilde{m}_j = d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s)$ выполнено $\nu(\tilde{m}_j) \leq n$.

ЛЕММА 15. Для каждого полинома $R(\tilde{f}(y_1, \dots, y_s)\tilde{m})$, где $\tilde{m}$ – произвольный чистый моном с формами, в алгебре $F\langle X \rangle/\Gamma$ выполнено включение

$$R(\tilde{f}\tilde{m}) \in \{R(\tilde{f}\tilde{m}_j)\}^T,$$

где $\{\tilde{m}_j\}$ – конечное множество всех чистых мономов вида

$$d_{p^{k_1}}(x_1) \cdots d_{p^{k_s}}(x_s), \quad \nu(\tilde{m}_j) \leq n.$$

ДОКАЗАТЕЛЬСТВО. Если полином $\tilde{f}$ имеет вид $\tilde{f} = \sum u_i \tilde{m}_i$, $u_i \in \langle y_1, \dots, y_s \rangle^\sharp$, $\tilde{m}_i$ – чистые мономы с формами или единицы, то по свойству “переброски” в обозначениях леммы 14

$$\begin{aligned}
 R(\tilde{f}\tilde{m}) &= \sum_i u_i R(\tilde{m}_i \tilde{m}) \equiv \sum_i u_i R(\tilde{m}_i, \tilde{m}) \equiv \sum_i \sum_j \gamma_j u_i R(\tilde{m}_i, \tilde{m}_{2,j}) \\
 &\equiv \sum_j \gamma_j \left(\sum_i u_i R(\tilde{m}_i \tilde{m}_{2,j}) \right) = \sum_j \gamma_j R(\tilde{f}\tilde{m}_{2,j}) \pmod{\Gamma},
 \end{aligned}$$

где $\nu(\tilde{m}_{2,j}) \leq n$. Ясно, что каждый полином $R(\tilde{f}\tilde{m}_{2,j})$ лежит в T -идеале $\{R(\tilde{f}\tilde{m}_j)\}^T$ алгебры $F\langle X \rangle/\Gamma$. Лемма 15 доказана.

13) Докажем, что отображение R “коммутирует” с операциями подстановки единицы, т.е.

$$R(\tilde{f}(y_1, \dots, y_k)|_{y_{j_1}, \dots, y_{j_r} \rightarrow 1}) \equiv R(\tilde{f})(y_1, \dots, y_k)|_{y_{j_1}, \dots, y_{j_r} \rightarrow 1} \pmod{\Gamma}. \quad (74)$$

Разумеется, в $\tilde{f}$ единицы подставляются только по модулю $\tilde{K}_n$. Аналогично доказательству (66) индукцией по r показывается, что достаточно доказать (69) только для $r = 1$; при этом используется замкнутость T -идеала Γ относительно подстановки единицы. Очевидно также, что (69) достаточно доказать только для случая, когда $\tilde{f}$ – чистый моном с формами.

Итак, пусть $\tilde{f} = d_{p^{k_1}}(u_1) \cdots d_{p^{k_s}}(u_s)$, где u_i не p -слова. Допустим, что при подстановке $y_1 = 1$ некоторые из слов u_i переходят в единицу, а остальные слова u_i переходят в непустые слова v_i ; v_i уже могут быть p -словами. Без ограничения общности можно считать, что $u_1, \dots, u_t$ перешли в непустые слова $v_1, \dots, v_t$, а слова $u_{t+1}, \dots, u_s$ перешли в единицы. Необходимо показать, что

$$\begin{aligned} & R(d_{p^{k_1}}(v_1) \cdots d_{p^{k_t}}(v_t) d_{p^{k_{t+1}}}(1) \cdots d_{p^{k_s}}(1)) \\ & \equiv R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_t}}(x_t) \\ & \quad \times d_{p^{k_{t+1}}}(x_{t+1}) \cdots d_{p^{k_s}}(x_s))|_{x_1=v_1, \dots, x_t=v_t, x_{t+1}=1, \dots, x_s=1} \pmod{\Gamma}. \end{aligned} \quad (75)$$

Здесь под $d_{p^i}(1)$ мы понимаем элемент $C_n^{p^i}$ поля F . По (67) левая часть (75) равна

$$d_{p^{k_{t+1}}}(1) \cdots d_{p^{k_s}}(1) R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_t}}(x_t))|_{x_1=v_1, \dots, x_t=v_t} \pmod{\Gamma}.$$

Поэтому достаточно доказать, что

$$\begin{aligned} & d_{p^{k_{t+1}}}(1) \cdots d_{p^{k_s}}(1) R(1, d_{p^{k_1}}(x_1) \cdots d_{p^{k_t}}(x_t)) \\ & \equiv R(1, d_{p^{k_1}}(x_1) \cdots d_{p^{k_t}}(x_t) d_{p^{k_{t+1}}}(x_{t+1}) \cdots d_{p^{k_s}}(x_s))|_{x_{t+1}=1, \dots, x_s=1} \pmod{\Gamma}. \end{aligned} \quad (76)$$

Так как (76) является тождеством M_n , то равенство (76) справедливо, если $\nu(d_{p^{k_1}}(x_1) \cdots d_{p^{k_t}}(x_t)) \leq n$. Остальные случаи сводятся к этому при помощи леммы 14 и “переброски” аналогично тому, как это делалось выше. В обозначениях леммы 14 с учетом унитарной замкнутости Γ имеем

$$\begin{aligned} & d_{p^{k_{t+1}}}(1) \cdots d_{p^{k_s}}(1) R(1, d_{p^{k_1}}(x_1) \cdots d_{p^{k_t}}(x_t)) \\ & \equiv \sum_j \gamma_j d_{p^{k_{t+1}}}(1) \cdots d_{p^{k_s}}(1) R(1, \tilde{m}_{2,j}) \\ & \equiv \sum_j \gamma_j R(d_{p^{k_{t+1}}}(x_{t+1}) \cdots d_{p^{k_s}}(x_s), \tilde{m}_{2,j})|_{x_{t+1}=1, \dots, x_s=1} \\ & \equiv R(d_{p^{k_{t+1}}}(x_{t+1}) \cdots d_{p^{k_s}}(x_s), d_{p^{k_1}}(x_1) \cdots d_{p^{k_t}}(x_t))|_{x_{t+1}=1, \dots, x_s=1} \\ & \equiv R(d_{p^{k_1}}(x_1) \cdots d_{p^{k_t}}(x_t) d_{p^{k_{t+1}}}(x_{t+1}) \cdots d_{p^{k_s}}(x_s))|_{x_{t+1}=1, \dots, x_s=1} \pmod{\Gamma}, \end{aligned}$$

что и требовалось доказать.

14) Объединим доказанные свойства отображения R в следующей лемме.

ЛЕММА 16. Пусть $\tilde{g}(x_1, \dots, x_k) \in \tilde{F}\langle X_0 \rangle / \tilde{K}_n$ – полиоднородный полином с формами и для всех мономов $d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})$ с условием

$$\nu(d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \leq n$$

выполнено

$$R(\tilde{g}(x_1, \dots, x_k) d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \in \Gamma.$$

Тогда все полиномы

$$R(L_\rho[\tilde{g}]|_{x_i \rightarrow u_i} d_{p^{k_1}}(v_1) \cdots d_{p^{k_l}}(v_l)), \quad u_i \in \langle X_0 \rangle^\sharp, \quad v_j \in \langle X_0 \rangle,$$

тоже лежат в Γ .

ДОКАЗАТЕЛЬСТВО. В лемме под T -идеалами всюду будем понимать T -идеалы алгебры $F\langle X_0 \rangle / \Gamma$. По лемме 15 и определению (40) полином

$$h = R(L_\rho[\tilde{g}]|_{x_i \rightarrow u_i} d_{p^{k_1}}(v_1) \cdots d_{p^{k_l}}(v_l))$$

лежит в T -идеале

$$\left\{ R(L_\rho[\tilde{g}]|_{x_i \rightarrow u_i} d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \right\}^T, \\ \nu(d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \leq n.$$

Из (67) следует, что этот T -идеал содержится в T -идеале

$$\left\{ R(L_\rho[\tilde{g}]|_{x_{i_1} \rightarrow 1, \dots, x_{i_r} \rightarrow 1} d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \right\}^T, \\ \nu(d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \leq n.$$

В свою очередь, этот T -идеал по (74) лежит в T -идеале

$$\left\{ R(L_\rho[\tilde{g}] d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s}))|_{x_{i_1} \rightarrow 1, \dots, x_{i_r} \rightarrow 1} \right\}^T, \quad (77) \\ \nu(d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \leq n.$$

Далее, по (68) полином $R(L_\rho[\tilde{g}] d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s}))$ лежит в T -идеале

$$\left\{ R(\tilde{g} d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \right\}^T \subset \Gamma, \quad \nu(d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \leq n. \quad (78)$$

Из (77), (78) и унитарной замкнутости T -идеала Γ получаем, что $h \in \Gamma$. Лемма 16 доказана.

Теперь можно завершить доказательство теоремы 2. По теореме 3 $\tilde{T}$ -идеал $\tilde{T}[M_n]$ имеет базис $\{\tilde{f}_i\}$, состоящий из полиномов, зависящих не более чем от n переменных. С каждым полиномом $\tilde{f}_i = \tilde{f}_i(x_1, \dots, x_k)$, $1 \leq k \leq n$, ассоциируем полиномы

$$y\tilde{f}_i z, \quad y d_{p^s}(\tilde{f}_i z), \quad p^s \leq n,$$

где переменные y и z отличны от $x_1, \dots, x_n$. Все полученные полиномы образуют некоторое множество $\{\tilde{g}_j\}$, а все полиномы $\tilde{g}_j$ зависят не более чем от $n+2$

переменных. Из построения системы $\{\tilde{g}_j\}$ вытекает, что любое следствие системы $\{\tilde{g}_j\}$ в алгебре $\tilde{F}\langle X_0 \rangle / \tilde{K}_n$ можно записать в виде линейной комбинации полиномов

$$L_\rho(\tilde{g}_j)|_{x_i \rightarrow u_i} d_{p^{k_1}}(v_1) \cdots d_{p^{k_s}}(v_s), \quad p^{k_1}, \dots, p^{k_s} \leq n, \quad (79)$$

где $L_\rho(\tilde{g}_j)(x_1, \dots, x_t)$ – некоторая частичная линейаризация полинома $\tilde{g}_j$, $u_i \in \langle X_0 \rangle^\sharp$, $v_l \in \langle X_0 \rangle$, $s \geq 0$.

Пусть теперь $f \in T[M_n] \subset \tilde{T}[M_n] \subseteq \tilde{F}\langle X_0 \rangle$. Тогда f является следствием системы полиномов $\{\tilde{g}_j\}$, стало быть,

$$f = \sum_{\alpha} \gamma_{\alpha} \tilde{h}_{\alpha}, \quad \gamma_{\alpha} \in F,$$

где каждый из полиномов с формами $\tilde{h}_{\alpha}$ имеет вид (79). По построению полиномов $R(\tilde{g})$ в алгебре $F\langle X \rangle / \Gamma$ выполнено равенство

$$R(f) \equiv \sum_{\alpha} \gamma_{\alpha} R(\tilde{h}_{\alpha}).$$

Из определения $R(f)$ немедленно вытекает, что $R(f) = f \cdot K$, поэтому в $F\langle X \rangle / \Gamma$ имеет место равенство

$$f \cdot K \equiv \sum_{\alpha} \gamma_{\alpha} R(\tilde{h}_{\alpha}).$$

Рассмотрим более подробно произвольное слагаемое $R(\tilde{h}_{\alpha})$, где полином $\tilde{h}_{\alpha}$ имеет вид (79). Все полиномы $R(\tilde{g}_j(x_1, \dots, x_k) d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s}))$ с условием $\nu(d_{p^{k_1}}(x_{k+1}) \cdots d_{p^{k_s}}(x_{k+s})) \leq n$ лежат в Γ . Действительно, они являются тождествами M_n и зависят от $\leq 3n + 2 < L$ переменных. Поэтому по лемме 16 Γ содержит все полиномы $R(\tilde{h}_{\alpha})$, а $\tilde{h}_{\alpha}$ имеет вид (79). Но тогда $f \cdot K \in \Gamma$. Таким образом, теорема 2 доказана для случая, когда f не зависит от $z_1, \dots, z_n$. Из инвариантности T -идеала Γ относительно подстановок следует, что теорема 2 верна и для произвольных полиномов f .

Автор выражает благодарность А. Р. Кемеру за внимание к работе и ценные замечания.

Список литературы

- [1] A. Kemer, “PI-algebras and nil algebras of bounded index”, *Trends in ring theory* (Miskolc, Hungary, 1996), CMS Conf. Proc., **22**, Amer. Math. Soc., Providence, RI, 1998, 59–69.
- [2] I. Sviridova, “Varieties and algebraic algebras of bounded degree”, *J. Pure Appl. Algebra*, **133**:1–2 (1998), 233–240.
- [3] Л. М. Самойлов, “О нильиндексе радикала относительно свободной ассоциативной алгебры”, *Матем. заметки*, **82**:4 (2007), 583–592; англ. пер.: L. M. Samoilov, “On the nilindex of the radical of a relatively free associative algebra”, *Math. Notes*, **82**:3–4 (2007), 522–530.
- [4] А. Р. Кемер, “Тождества конечнопорожденных алгебр над бесконечным полем”, *Изв. АН СССР. Сер. матем.*, **54**:4 (1990), 726–753; англ. пер.: A. R. Kemer, “Identities of finitely generated algebras over an infinite field”, *Math. USSR-Izv.*, **37**:1 (1991), 69–96.

- [5] S. A. Amitsur, “On the characteristic polynomial of a sum of matrices”, *Linear and Multilinear Algebra*, **8**:3 (1980), 177–182.
- [6] C. Procesi, *Rings with polynomial identities*, Pure Appl. Math. (N.Y.), **17**, Dekker, New York, 1973.
- [7] A. Kemer, “Multilinear identities of the algebras over a field of characteristic p ”, *Internat. J. Algebra Comput.*, **5**:2 (1995), 189–197.
- [8] А. Н. Зубков, “Об обобщении теоремы Размыслова–Прочези”, *Алгебра и логика*, **35**:4 (1996), 433–457; англ. пер.: A. N. Zubkov, “A generalization of the Razmyslov–Procesi theorem”, *Algebra and Logic*, **35**:4 (1996), 241–254.
- [9] S. Donkin, “Invariants of several matrices”, *Invent. Math.*, **110**:1 (1992), 389–401.
- [10] C. Procesi, “The invariant theory of $n \times n$ -matrices”, *Advances in Math.*, **19**:3 (1976), 306–381.

Л. М. Самойлов (L. M. Samoilov)

Ульяновский государственный университет

E-mail: samoilov_l@rambler.ru

Поступила в редакцию

31.05.2007