

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ
«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»
ФАКУЛЬТЕТ МАТЕМАТИКИ

Воробьев Иван Евгеньевич

Проблема Шпехта и гипотеза Гельфанда

Выпускная квалификационная работа — бакалаврская работа
по направлению подготовки 01.03.01 — Математика,
образовательная программа «Математика»

Рецензент:

доктор физико-математических
наук,
профессор
Горчинский Сергей Олегович

Научный руководитель:

доктор физико-математических
наук,
профессор
Канель-Белов Алексей Яковлевич

Москва 2024

Аннотация

Пусть F свободная некоммутативная про- p группа, и пусть Δ коммутативное нетерово полное локальное кольцо с максимальным идеалом I , такое что Δ/I конечное поле характеристики p . Определим группу

$$GL_d^1(\Delta) = \ker \left(GL_d(\Delta) \xrightarrow{\Delta \rightarrow \Delta/I} GL_d(\Delta/I) \right)$$

А.Н. Зубков доказал, что F не может быть непрерывно вложена в $GL_2^1(\Delta)$ для $p \neq 2$.

Д. Бен-Эзра и Е. Зельманов, показали, что и для $p = 2$, $\text{char}(\Delta) = 2$ имеет место такой же результат.

Цель данной статьи обобщить подход для $p = 2$ и $\text{char}(\Delta) = 4$.

Кроме того, Зельманов показал в [11], что гипотеза о нелинейности про- p групп тесно связана с PI-теорией.

Во второй части данной статьи мы изучаем связь между PI-теорией и гипотезой Гельфанда о конечномерности гомологий алгебр Ли векторных полей.

Таким образом, можно видеть, что работа в основном посвящена изучению комбинаторики подстановок.

Содержание

1	Введение	3
1.1	О нелинейности свободных про- p -групп	3
1.2	Гипотеза Гельфанда	5
2	Подход Зубкова, $p \neq 2$	5
2.1	Универсальное представление	5
2.2	Неточность универсального представления	8
3	Подход Бена-Эзры—Зельманова, $p = 2$, $\text{char}(\Delta) = 2$	11
3.1	Универсальное представление	11
3.2	Набросок доказательства	11
4	Случай $p = 2$, $\text{char}(\Delta) = 4$	11
5	Конечная базлируемость T-пространств в кольце многочленов над полем характеристики 0	11
5.1	Постановка задачи и основные леммы	11
5.2	Ключевая подстановка	13

5.3	Глобальная конечная базисуемость из конечной базисуемости по каждой координате	15
5.4	Конечная базисуемость по каждой координате	15
5.4.1	Доказательство в случае двух переменных.	16
5.4.2	Доказательство в общем случае	18
6	Связь методов Гришина с гипотезой Гельфанда	21

1 Введение

Мы рассмотрим применения теории полиномиальных тождеств (PI-теории для краткости) в двух, казалось бы, несвязанных с ней областях:

- В 2005, Е. Зельманов представил набросок доказательства нелинейности некоторых свободных про- r групп. Доказательство во многом опирается на стандартные подходы PI-теории (см. [11]).
- Дополнительно мы рассмотрим неожиданную связь между гипотезой Гельфанда и PI-теорией, а именно с методами Гришина ([7]).

Приведем краткую историческую справку и формулировку основных проблем. Отметим, что параграфы 2, 3 и параграфы 4, 5 независимы.

1.1 О нелинейности свободных про- r -групп

Проблема линейности топологических групп изучалась много лет. Одной из естественных топологий, наряду с \mathbb{R}^n и дискретной, является про- r топология.

Сформулируем центральную гипотезу данной теории, а далее приведем все необходимые определения:

Гипотеза 1.1. *Некоммутативная свободная про- r группа не может быть вложена в $GL_d(\Delta)$ ни для какого про- r кольца Δ .*

Определение 1.1. *Обратный (проективный) предел конечных r -групп называется про- r группой.*

Топология индуцируется с топологии тихоновского произведения.

Определение 1.2. *Коммутативное нетерово полное локальное кольцо Δ с максимальным идеалом I называется про- r кольцом, если Δ/I конечное поле характеристики r .*

Таким образом:

$$\Delta \cong \varprojlim \Delta/I^n$$

Рассмотрим конгруенц-подгруппу:

$$GL_d^1(\Delta) = \ker \left(GL_d(\Delta) \xrightarrow{\Delta \rightarrow \Delta/I} GL_d(\Delta/I) \right)$$

Можно видеть, что это про- p группа.

Основной вопрос состоит в том, может ли свободная про- p группа быть непрерывна вложена в $GL_d^1(\Delta)$.

Свободную про- p группу можно определить классическим способом через универсальное свойство или конструктивно:

Определение 1.3. *Свободная про- p группа $F_p(X)$ является пополнением дискретной свободной группы $F(X)$ относительно топологии всех нормальных подгрупп индекса степени p .*

Существует множество частичных результатов:

- В 1987, А.Н. Зубков ([12]) доказал гипотезу для $d = 2, p \neq 2$.
- В 1999, используя глубокие результаты Пинка ([9]), Й. Барнеа, М. Ларсен ([1]) подтвердили гипотезу для $\Delta = (\mathbb{Z}/p\mathbb{Z})[[t]]$
- В 1991, Д. Диксон, А. Манн, М.П.Ф. Ду Сатой, Д. Сигал ([4]) доказали гипотезу для всех размеров матриц для целых p -адических чисел $\Delta = \mathbb{Z}_p$, $GL_d^1(\mathbb{Z}_p) = \ker \left(GL_2(\mathbb{Z}_p) \xrightarrow{\mathbb{Z}_p \rightarrow \mathbb{F}_p} GL_2(\mathbb{F}_p) \right)$
- В 2005, Е. Зельманов ([11], [10]) анонсировал доказательство гипотезы для $p \gg d$, однако до сих пор существует только набросок доказательства.
- В 2020, Д. Бен-Эзра, Е. Зельманов ([2]) обобщили результат Зубкова для $d = 2, p = 2$ и $\text{char}(\Delta) = 2$.

Мы сконцентрируемся на случае 2×2 матриц, то есть на результатах Зубкова и Бена-Эзры—Зельманова.

Сейчас опишем общий план доказательства, он отчасти реализован для произвольных размеров матриц в [11], [10]:

Для начала сузим множество рассматриваемых колец. Можно построить, так называемое, универсальное представление в общие матрицы. Оказывается, что классическими алгебраическими рассуждениями можно показать, что если какое-то представление точно, то и это универсальное представление точно.

Таким образом, остается исследовать это универсальное представление. Это делается путем изучения алгебры Ли общих матриц, которая множество раз возникала в PI-теории. В завершение строится связь между этой алгеброй Ли и образом нашего представления — подобно связи между группой Ли и алгеброй Ли.

1.2 Гипотеза Гельфанда

В 2022 была обнаружена замечательная связь между PI-теорией (точнее методами Гришина) и гипотезой Гельфанда сформулированной на ISM'70 (см [6]).

Гипотеза 1.2 (Гельфанд, 1970). *Гомологии подалгебры Ли конечной ко-размерности алгебры Ли алгебраических векторных полей на аффинном алгебраическом многообразии конечномерны.*

Эта интересная связь была найдена в результате совместной работы А.С. Хорошкина, А.Я. Канель-Белова с некоторым участием автора. Можно найти набросок доказательства Хорошкина в [5], [3].

Дополнительно, мы заметим, что именно результат, которого касалась последняя курсовая работа автора (частный случай методов Гришина [7], описанный элементарными методами) помогает в доказательстве гипотезы Гельфанда.

2 Подход Зубкова, $p \neq 2$

Теорема 2.1 (Зубков, 1989). *Некоммутативная свободная про- p группа не может быть непрерывно вложена в $GL_2^1(\Delta)$ для $p \neq 2$.*

2.1 Универсальное представление

Определим алгебру общих матриц над p -адическими числами.

Мы будем работать с матрицами 2×2 , однако все результаты и конструкции этого параграфа дословно переносятся на матрицы произвольного размера.

Рассмотрим формальные степенные ряды от свободных коммутирующих переменных $x_{i,j}, y_{i,j}$ для $i, j \in \{1, 2\}$:

$$S = \mathbb{Z}_p \langle x_{1,1}, y_{1,1}, \dots, x_{2,2}, y_{2,2} \rangle$$

Введем стандартную градуировку \deg : любой элемент S записывается в виде $\sum f_i$ где $\deg(f_i) = i$.

Рассмотрим идеалы вида

$$S_k = \left\{ \sum_k^{\infty} f_i \right\}$$

Предложение 2.1. *Следующие идеалы*

$$B_{k,n} = S \cdot p^n + S_k$$

являются идеалами конечного индекса

Доказательство. Достаточно доказать, что $\mathbb{Z}_p/p^n\mathbb{Z}_p$ — конечное кольцо.

$$\ker(\mathbb{Z}_p \rightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p) = \mathbb{Z}_p p^n = (0, \dots, 0, a_{k+1}, a_{k+2}, \dots)$$

Ясно, что множество целых p -адических чисел отличающихся на элементы такого вида конечно и $\mathbb{Z}_p/\mathbb{Z}_p p^n \cong \mathbb{Z}/p^n\mathbb{Z}$ \square

Снабдим S топологией с базой окрестностей нуля состоящей из идеалов $B_{k,n}$. S является про- p кольцом:

$$S/B_{1,1} \cong \mathbb{Z}/p\mathbb{Z}$$

Наконец, рассмотрим матричное кольцо $M_2(S)$. Наделив его топологией с базой окрестностей нуля конгруэнц-идеалов

$$\ker(M_2(S) \rightarrow M_2(S/B_{k,n}))$$

получим, что $M_2(S)$ — про- p кольцо.

Предложение 2.2. *Множество*

$$1 + \ker(M_2(S) \rightarrow M_2(S/S_1))$$

является про- p группой.

Доказательство. Заметим, что $\ker(S \rightarrow S/S_1)$ состоит из рядов без свободного члена. Получается, что $1 + \ker(M_2(S) \rightarrow M_2(S/S_1))$ является группой, так как ряд обратим тогда и только тогда, когда его свободный член обратим.

Также можно заметить, что эта группа полна относительно определенной выше топологии, то есть является про- p группой. \square

Рассмотрим общие матрицы $X, Y \in \ker (M_2(S) \rightarrow M_2(S/S_1))$:

$$X = \begin{pmatrix} x_{1,1} & x_{1,2} \\ x_{2,1} & x_{2,2} \end{pmatrix}, \quad Y = \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{2,1} & y_{2,2} \end{pmatrix}$$

Пусть F — свободная про- p группа порожденная x, y .
Наконец определим универсальное представление:

$$\pi : \begin{cases} x \mapsto 1 + X \\ y \mapsto 1 + Y \end{cases}$$

Продолжим его на дискретную подгруппу, порожденную x, y :

$$\pi : \langle x, y \rangle \rightarrow \langle 1 + X, 1 + Y \rangle \subseteq 1 + \ker (M_2(S) \rightarrow M_2(S/S_1))$$

А затем можно непрерывно доопределить π на всей F , построив замыкание $\langle 1 + X, 1 + Y \rangle$ в топологии $1 + \ker (M_2(S) \rightarrow M_2(S/S_1))$:

$$\pi : F \rightarrow G \subseteq 1 + \ker (M_2(S) \rightarrow M_2(S/S_1))$$

Итак, следующая теорема позволяет нам изучать только универсальное представление, не задумываясь о других про- p кольцах.

Теорема 2.2 (Зубков, 1987). *Пусть F — свободная про- p группа порожденная x, y . Если существует инъективный непрерывный гомоморфизм $\varphi : F \rightarrow GL_2^1(\Delta)$, то и универсальное представление π инъективно.*

Доказательство. Напомним

$$GL_2^1(\Delta) = \ker (GL(\Delta \rightarrow \Delta/I))$$

Рассмотрим образы x, y :

$$\varphi(x) = 1 + A, \quad \varphi(y) = 1 + B$$

Заметим, что

$$A, B \in \ker (M_2(\Delta) \rightarrow M_2(\Delta/I))$$

так как $1 + A, 1 + B \in \ker (GL(\Delta \rightarrow \Delta/I))$. Пусть

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}, \quad B = \begin{pmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{pmatrix}$$

Ясно, что $\lim a_{i,j}^n = \lim b_{i,j}^n = 0$. Тогда можно построить гомоморфизм $\zeta : x_{i,j} \mapsto a_{i,j}, y_{i,j} \mapsto b_{i,j}$, он индуцирует эпиморфизм $\hat{\zeta} : G \rightarrow \text{Im } \varphi$.
Наконец, получаем коммутативную диаграмму

$$\begin{array}{ccc}
& F & \\
\pi \swarrow & & \searrow \varphi \\
G & \xrightarrow{\hat{\zeta}} & GL_2^1(\Delta)
\end{array}$$

Следовательно:

$$\ker \pi \subseteq \ker \varphi$$

□

2.2 Неточность универсального представления

Введем обозначения:

- \mathbf{S} — кольцо степенных рядов от общих матриц X, Y над \mathbb{Z}_p
- $\mathcal{L}_{\mathbb{Q}_p}$ — алгебра Ли порожденная общими матрицами X, Y над \mathbb{Q}_p
- $\mathcal{L}_{\mathbb{Z}_p}$ — алгебра Ли порожденная общими матрицами X, Y над \mathbb{Z}_p
- $\mathcal{L}_{\mathbb{Q}_p}^{(n)}$ — векторное пространство над \mathbb{Q}_p однородных элементов степени n в алгебре $\mathcal{L}_{\mathbb{Q}_p}$.
- $\mathcal{L}_{\mathbb{Z}_p}^{(n)}$ — \mathbb{Z}_p -модуль однородных элементов степени n в алгебре $\mathcal{L}_{\mathbb{Z}_p}$.
- Для $g \in G$: $\min g$ — однородная компонента наименьшей ненулевой степени (можно записать $g = 1 + a_n + a_{n+1} + \dots$)
- Будем записывать коммутатор веса n следующим образом $[l_1, \dots, l_n] = [[l_1, l_2, \dots, l_{n-1}], l_n]$

Приведем сначала план доказательства, чтобы была понятна мотивация каждой леммы:

1. Определим $G \supseteq G^{(n)}$, вложенную последовательность нормальных подгрупп попадающую в любую окрестность единицы, такую что для любого $g \in G^{(n)}$

$$\min g \in \mathcal{L}_{\mathbb{Q}_p}^{(n)} \cap \mathbf{S} = \mathcal{L}_{\mathbb{Z}_p}^{(n)}$$

2. Таким образом, можно изучать $G^{(n)}/G^{(n+1)}$ как \mathbb{Z}_p -модуль $\mathcal{L}_{\mathbb{Z}_p}^{(n)}$. Докажем, что $\text{rank}_{\mathbb{Z}_p} \mathcal{L}_{\mathbb{Z}_p}^{(n)} = f(n)$ для некоторой f .
3. Доказав, что $G^{(n)}$ — нижний центральный ряд G получим противоречие с формулой Э. Витта (см. [8]):

Предложение 2.3 (Витт, [8]). Пусть F — свободная про- p группа порожденная t образующими, тогда n -ый фактор нижнего центрального ряда имеет ранг (как \mathbb{Z}_p -модуль)

$$\frac{1}{n} \sum_{d|n} \mu(d) t^{n/d}$$

где μ — функция Мебиуса.

Итак, докажем следующее техническое утверждение:

Предложение 2.4. При $p \neq 2$:

$$\mathcal{L}_{\mathbb{Q}_p}^{(n)} \cap \mathbf{S} = \mathcal{L}_{\mathbb{Z}_p}^{(n)}$$

Замечание 2.1. Данное предложение не верно для $p = 2$, что влечет существенные сложности, возникающие для $p = 2$.

Доказательство. Пусть

$$\begin{aligned} a &= 4x_{1,2}x_{2,1} + (x_{1,1} - x_{2,2})^2 \\ b &= 2(y_{1,2}x_{2,1} + x_{1,2}y_{2,1}) + (x_{1,1} - x_{2,2})(y_{1,1} - y_{2,2}) \\ c &= 4y_{1,2}y_{2,1} + (y_{1,1} - y_{2,2})^2 \end{aligned}$$

Легко проверить, что

$$\begin{aligned} [x, y, x, x] &= a[x, y] \\ [x, y, y, x] &= b[x, y] \\ [x, y, y, y] &= c[x, y] \\ [x, y, x, y] &= [x, y, y, x] \end{aligned}$$

Получаем, что любой $l \in \mathcal{L}_{\mathbb{Q}_p}^{(n)}$ имеет вид

$$l = \begin{cases} \sum_{i_a+i_b+i_c=(n-2)/2} \lambda_{i_a, i_b, i_c} a^{i_a} b^{i_b} c^{i_c} [x, y], & \text{если } n \text{ четно} \\ \sum_{i_a+i_b+i_c=(n-3)/2} \alpha_{i_a, i_b, i_c} a^{i_a} b^{i_b} c^{i_c} [x, y, x] + \beta_{i_a, i_b, i_c} a^{i_a} b^{i_b} c^{i_c} [x, y, y], & \text{если } n \text{ нечетно} \end{cases} \quad (1)$$

где $\lambda_{i_a, i_b, i_c}, \alpha_{i_a, i_b, i_c}, \beta_{i_a, i_b, i_c} \in \mathbb{Q}_p$

Разберем случай нечетного n . Рассмотрим какое-то $l \in \mathcal{L}_{\mathbb{Q}_p}^{(n)} \cap \mathbf{S}$ с нецелыми p -адическими $\alpha_{i_a, i_b, i_c}, \beta_{i_a, i_b, i_c}$.

Далее рассуждение аналогично классическому доказательству теоремы Гильберта о базисе. Введем лексикографический порядок на мономах порожденный отношением

$$x_{1,2} > x_{1,1} > y_{1,2} > y_{1,1} > x_{2,1} > x_{2,2} > y_{2,1} > y_{2,2}$$

Старшие члены у a, b, c : $4x_{1,2}x_{2,1}, 2x_{1,2}y_{2,1}, 4y_{1,2}y_{2,1}$ соответственно. Тогда старший член элемента, стоящего в левом верхнем углу l равен старшему члену выражения

$$\sum_{i_a+i_b+i_c=(n-3)/2} 2^{2i_a+2i_c+i_b} (\alpha_{i_a,i_b,i_c} x_{1,1}^{i_c} x_{2,1}^{i_a} y_{2,1}^{i_b+i_c+1} + \beta_{i_a,i_b,i_c} y_{1,2}^{i_c} y_{1,1} x_{2,1}^{i_a} y_{2,1}^{i_b+i_c+1})$$

Старшие члены различны и 2^k обратим в кольце \mathbb{Z}_p (при $p \neq 2$). Следовательно, так как $\alpha_{i_a,i_b,i_c}, \beta_{i_a,i_b,i_c} \in \mathbb{Q}_p \setminus \mathbb{Z}_p$, а значит старший член левого верхнего угла l не лежит в \mathbb{Z}_p . Получаем противоречие с тем, что $l \in S$.

Случай четного n разбирается аналогично.

Замечание 2.2. Попутно мы доказали, что суммы в формуле (1) на самом деле прямые.

□

Сразу же получаем следствие

Следствие 2.1.

$$\text{rank}_{\mathbb{Z}_p} \mathcal{L}_{\mathbb{Z}_p}^{(n)} = \dim_{\mathbb{Q}_p} \mathcal{L}_{\mathbb{Q}_p}^{(n)} = \begin{cases} \frac{n(n+2)}{8}, & \text{при четном } n \\ \frac{(n-1)(n+1)}{4}, & \text{при нечетном } n \end{cases}$$

Итак, пусть

$$G^{(n)} = G \cap \ker (GL(S) \rightarrow GL(S/S_n))$$

Следующая лемма является ключевой.

Лемма 2.1. Пусть $g \in G^{(n)}$, тогда

$$\min g \in \mathcal{L}_{\mathbb{Z}_p}^{(n)}$$

Доказательство. В силу предложения 2.4 достаточно доказать, что $\min g \in \mathcal{L}_{\mathbb{Q}_p}^{(n)}$.

□

Пусть $G = G_1, \dots, G_n, \dots$ — нижний центральный ряд.

Следующее предложение завершает доказательство теоремы 2.1

Предложение 2.5. *Нижний центральный ряд совпадает с пересечениями группы G с конгруэнц-подгруппами по идеалу S_n , то есть*

$$G_n = G^{(n)}$$

Доказательство. Ясно, что $G_n \subseteq G^{(n)}$, так как коммутаторы веса n лежат в $\ker (GL(S) \rightarrow GL(S/S_n))$ по определению S_n .

С другой стороны, пусть $g \in G^{(n)}$:

$$g = 1 + v_n(X, Y) + \text{старшие члены}$$

где $v_n(X, Y)$ — линейная комбинация коммутаторов веса n над \mathbb{Z}_p . □

3 Подход Бена-Эзры—Зельманова, $p = 2$, $\text{char}(\Delta) = 2$

3.1 Универсальное представление

3.2 набросок доказательства

4 Случай $p = 2$, $\text{char}(\Delta) = 4$

5 Конечная базированность T -пространств в кольце многочленов над полем характеристики 0

Следующая теорема (а вернее, метод ее доказательства) очень полезна при изучении гипотезы Гельфанда:

5.1 Постановка задачи и основные леммы

Теорема 5.1. *Пусть есть множество M многочленов от n переменных над полем характеристики 0. Тогда существует его конечное подмножество, такое что любой многочлен из M можно добавить в это подмножество, конечное число раз применив следующие операции:*

- Если в множестве есть несколько многочленов, то можно добавить их линейную комбинацию.

- Если в множестве был многочлен $F(x_1, \dots, x_n)$, то можно добавить $F(t(x_1), \dots, t(x_n))$, где t – любой многочлен одной переменной.

Вторую операцию будем называть подстановкой. Для начала докажем три основных леммы.

Лемма 5.1. *Достаточно доказать теорему 5.1 для случая, когда M замкнуто относительно приведенных операций.*

Доказательство. Рассмотрим \overline{M} – множество, получаемое из M применением конечного количества последовательных операций.

Ясно, что \overline{M} замкнуто относительно них. Действительно, если взять любую линейную комбинацию многочленов из \overline{M} , то она получается из M последовательным применением конечного числа операций и следовательно лежит в \overline{M} . То же самое верно и про подстановку. Осталось доказать, что если \overline{M} конечно базируемо, то и M – тоже. Пусть \overline{M}_0 – конечная база \overline{M} . Тогда M_0 – это множество многочленов, из которых мы получили \overline{M}_0 . По построению M_0 конечно и является базой M . \square

Следующая лемма также сужает класс множеств для которых мы будем доказывать теорему: можно считать, что M содержит исключительно однородные многочлены.

Лемма 5.2. *Из многочлена F разрешенными операциями можно получить его однородные компоненты.*

Доказательство. Пусть t – степень F .

Сделаем подстановку: $F(\alpha x_1, \alpha x_2, \dots, \alpha x_n)$. Заметим, что при такой подстановке однородная компонента k -ой степени умножается на α^k . Тогда пусть v_0, \dots, v_n – однородные компоненты F .

Заметим, что все подстановки указанного вида лежат в линейной оболочке $\langle v_0, v_1, \dots, v_n \rangle$. Тогда заметим, что у многочлена $F(\alpha x_1, \alpha x_2, \dots, \alpha x_n)$ в нашем базисе это $(\alpha^0, \alpha^1, \dots, \alpha^n)$. Если вспомнить, что определитель матрицы Вандермонда не 0, то получаем, что если подставить любые $t + 1$ различных α , то сможем выразить любое v_i . \square

Теперь можно считать, что множество M состоит только из однородных многочленов, однако возникает проблема: нам было бы удобно считать и то, что множество замкнуто относительно операций, и то, что оно состоит из однородных многочленов. Однако сейчас эти условия, конечно, несовместимы.

Эта проблема решается следующим образом: разрешим применять только такую последовательность операций, которая из однородного многочлена получает однородный. Такие последовательности операций будем

называть однородной подстановкой.

Когда решается задача про конечную базисуемость множества многочленов (например, можно провести аналогию с базисом Грёбнера из теоремы Гильберта о базисе) полезной является лемма про светильники – она помогает следующим образом: если ввести порядок на старших членах многочленов и научиться выражать большие старшие члены из маленьких, то из этого получим конечную базисуемость.

Следующая лемма очевидным образом следует из теоремы Гильберта о базисе, но так как в курсе алгебры часто выводится следствие в обратную сторону, то приведем все-таки независимое доказательство этой леммы.

Лемма 5.3. Пусть в \mathbb{Z}_+^n дано некоторое множество светильников – точка с координатами (x_1, \dots, x_n) освещает все $(y_1, \dots, y_n), y_i \geq x_i \forall i$. Тогда можно выбрать конечное количество светильников, которые освещают все остальные.

Доказательство. Докажем индукцией по размерности пространства.

При $n = 1$ утверждение леммы тривиально.

Пусть лемма верна для $n - 1$, докажем для n .

Спроецируем все светильники на гиперплоскость $x_n = 0$. Выберем конечный набор проекций m'_1, \dots, m'_k , который освещает все остальные проекции (такой есть в силу индукционного предположения). Теперь найдем m_i – светильник с наименьшей координатой по x_n из тех, что спроецировались в m'_i .

Пусть l – наибольшая координата по x_n среди m_i . Заметим, что для все светильники с координатой по x_n , не меньшей l освещены множеством m_1, \dots, m_k . Осталось для каждой гиперплоскости $x_n = c$, где $c = 0, \dots, l - 1$ выбрать конечные наборы светильников, которые освещают все остальные, лежащие в соответствующей гиперплоскости. \square

5.2 Ключевая подстановка

Следующая подстановка является ключевой:

$$P(x_1, \dots, x_n) \mapsto P_{(t,1)}(x_1 + t(x_1)x_1, \dots, x_n + t(x_n)x_n) \quad (2)$$

где индекс $(t, 1)$ обозначает, что мы линеаризуем по t после того, как, сделаем приведенную подстановку.

Докажем, что мы можем отлинеаризовать по t . Будем рассматривать многочлен $P(x_1 + t(x_1)x_1, \dots, x_n + t(x_n)x_n)$ как многочлен от $2n$ переменных – от x_i и $t(x_i)$. При этом понятно, что переменные $t(x_i)$ можно умножать на константу все сразу – в подстановке (2) надо взять

$x_i \mapsto x_i + c \cdot t(x_i)x_i$. Далее все аналогично доказательству леммы 5.2. Итак, разберемся, что получилось после отлинеаризованной подстановки (2). Для этого поймем, что произойдет с мономом $x_1^{\alpha_1} \dots x_n^{\alpha_n}$:

$$x_1^{\alpha_1} \dots x_n^{\alpha_n} \mapsto ((x_1 + t(x_1)x_1)^{\alpha_1} \dots (x_n + t(x_n)x_n)^{\alpha_n})_{(t,1)}$$

Ясно, что после линеаризации по t останутся только те члены, в которых ровно из одной скобки произведения взяли $t(x_i)$. То есть при $t(x_i)$ будет $\alpha_i \cdot x_1^{\alpha_1} \dots x_n^{\alpha_n}$. Итак:

$$x_1^{\alpha_1} \dots x_n^{\alpha_n} \mapsto \sum_{i=1}^n t(x_i)(\alpha_i \cdot x_1^{\alpha_1} \dots x_n^{\alpha_n}) \quad (3)$$

Следовательно, однородный многочлен P степени m перейдет в:

$$\sum_{i=1}^n t(x_i)P_i(x_1, \dots, x_n) \quad (4)$$

Причем, если вместо t подставить $\frac{1}{m}$, то из последней формулы (4) получится ровно многочлен P .

Далее, нам потребуются лишь $t(x) = x^k$. Каждому многочлену из множества M мы сопоставили некоторое семейство многочленов:

$$\sum_{i=1}^n x_i^k P_i(x_1, \dots, x_n) \quad (5)$$

где k пробегает все целые неотрицательные числа.

Обозначим сумму (5) как (P_1, \dots, P_n) и назовем ее координатным представлением многочлена.

Пока не очень понятно, чего мы хотим добиться и зачем мы рассмотрели это семейство. На самом деле мы будем делать однородные подстановки специального вида уже к семействам. Причем будем делать их так, чтобы они инвариантно действовали на каждую координату. Таким образом, мы сможем доказать конечную базисуемость по каждой координате, а потом уже выведем из этого глобальную конечную базисуемость. Ключевая идея заключается в том, что для каждой отдельной координаты доказывать конечную базисуемость куда проще, чем для бескоординатного представления, так как наличие i -ой координаты разрешает нам умножать многочлены внутри нее на x_i , что существенно упрощает задачу.

Мы будем доказывать конечную базисуемость по каждой координате, но для начала докажем, что из этого будет следовать теорема 5.1.

5.3 Глобальная конечная базлируемость из конечной базлируемости по каждой координате

Мы рассматриваем вместо каждого многочлена $P(x_1, \dots, x_n)$ соответствующее ему семейство:

$$\sum_{i=1}^n x_i^k P_i(x_1, \dots, x_n)$$

Пусть N — множество координатных представлений многочленов из M . Аналогично лемме 5.1, рассмотрим вместо N , его замыкание \bar{N} . То есть будем рассматривать некоторое множество систем многочленов, уже возможно слабо связанное с изначальными многочленами, но содержащее в себе координатное представление каждого многочлена.

Теперь осталось явно описать конечный базис \bar{N} : возьмем конечное количество семейств многочленов, у которых первая координата является конечным базисом первых координат из \bar{N} . Далее, возьмем $\bar{N}_1 \subset \bar{N}$ состоящее только из семейств с нулевой первой координатой (ясно, что это подмножество тоже замкнуто относительно подстановок и линейных комбинаций). Теперь возьмем те семейства из \bar{N}_1 , у которых вторая координата является конечным базисом вторых координат. В итоге на i -ом шаге мы берем семейства с нулевыми первыми $i - 1$ -ой координатами и берем конечное множество систем, у которых i -ая координата является конечной базой i -ых координат соответствующего множества. Ясно, что в итоге мы действительно построим конечный базис всех систем. Действительно: чтобы получить какую-то систему из выбранных, мы можем последовательно занулить все ее координаты.

5.4 Конечная базлируемость по каждой координате

Ключевая подстановка решает задачу в случае двух переменных, однако в общем случае нужны тонкие индукционные рассуждения.

Докажем, что внутри каждой координаты можно опять сделать подстановку (2).

$$\begin{aligned} (p_1, \dots, p_n) &= \sum_{i=1}^n x_i^k p_i(x_1, \dots, x_n) \mapsto \\ &\mapsto \left[\sum_{i=1}^n (x_i + r(x_i)x_i)^k \cdot p_i(x_1 + r(x_1)x_1, \dots, x_n + r(x_n)x_n) \right]_{(r,1)} \end{aligned}$$

Здесь индекс $(r, 1)$ означает линеаризацию по r , как и раньше. Рассмотрим первую координату. Она, конечно, полностью получается из члена

$$[(x_1 + r(x_1)x_1)^k \cdot p_1(x_1 + r(x_1)x_1, \dots, x_n + r(x_n)x_n)]_{(r,1)}$$

Раскрыв первые скобки получаем

$$x_1^k \cdot (k \cdot r(x_1)p_1(x_1, \dots, x_n) + [p_1(x_1 + r(x_1)x_1, \dots, x_n + r(x_n)x_n)]_{(r,1)}) \quad (6)$$

Заметим, что первое слагаемое нам совсем не нужно, ведь оно преобразует только степень мономов p_1 по x_1 , а мы добиваемся увеличения других степеней. Так что вычтем из семейства, полученного при подстановке (6) изначальное семейство умноженное на $r(x_i)k$ по координатам. Получим, что по первой координате у нас:

$$[p_1(x_1 + r(x_1)x_1, \dots, x_n + r(x_n)x_n)]_{(r,1)}$$

Сравним это с подстановкой (2), специализуем $r(x) = x^m$ и сделаем вывод, что это равно

$$\sum_{i=1}^n x_i^m p_{1i}(x_1, \dots, x_n) \quad (7)$$

Итак, внутри каждой координаты можно опять делать ключевую подстановку. Назовем ее φ .

Докажем теперь теорему в следующем частном случае.

5.4.1 Доказательство в случае двух переменных.

Итак, пусть у нас есть многочлен

$$x_1^{m_1} p_1 + x_2^{m_1} p_2$$

Мы рассматриваем только случай, когда в p_1 все мономы делятся x_1 , ведь иначе первой координаты вообще не существовало бы, то есть она была бы нулевой (что видно из (3)). Мы хотим узнать, что из многочлена $x_1^{m_1} p_1 + x_2^{m_1} p_2$ можно получить по первой координате. Здесь потребуются лемма, которая сведет всю задачу к лемме о светильниках (5.3).

Лемма 5.4. *Если у p_1 старший член в лексикографическом порядке $x_2 \succ x_1$ это $x_1^{\alpha_1} x_2^{\alpha_2}$, причем $\alpha_2 > 0$, то для любого монома, делящегося на данный, мы можем получить многочлен, у которого по первой координате будет старшим этот моном.*

Доказательство. Пусть нам нужно получить моном $x_1^{\alpha_1+\beta_1}x_2^{\alpha_2+\beta_2}$. Рассмотрим случай, когда $\beta_2 = 0$. Тогда сдвинем $m_1 := m_1 + \beta_1$. Естественно, мы получим многочлен с нужным старшим членом. Пусть теперь $\beta_2 > 0$. Сделаем нашу подстановку еще раз, как мы описали в (7). Получится многочлен

$$x_1^{m_1}(x_1^{m_2}p_{11} + x_2^{m_2}p_{12})$$

Причем и в p_{11} , и в p_{22} старший член — это $x_1^{\alpha_1}x_2^{\alpha_2}$. Тогда возьмем $m_2 = \beta_2$ и, опять же, заменим m_1 на $m_1 + \beta_1$. Получается

$$x_1^{m_1}x_1^{\beta_1}(x_1^{\beta_2}p_{11} + x_2^{\beta_2}p_{12}) = x_1^{m_1}(x_1^{\beta_2}x_1^{\beta_1}p_{11} + x_2^{\beta_2}x_1^{\beta_1}p_{12})$$

Ясно, что старший моном содержится только во втором слагаемом (ведь $\beta_2 > 0$). Причем он имеет вид $x_1^{\alpha_1+\beta_1}x_2^{\alpha_2+\beta_2}$. \square

Замечание 5.1. *Полезно заметить, что если все же $\alpha_2 = 0$, то утверждение леммы верно для монома вида $x_1^{\alpha_1+\beta_1}x_2^{\alpha_2} = x_1^{\alpha_1+\beta_1}$.*

Итак, осталось свести к лемме о светильниках (5.3). Рассмотрим множество M и каждому многочлену из него сопоставим точку в \mathbb{Z}_+^2 — набор степеней в его старшем члене по первой координате. В этой точке расположим светильник: если ордината не равна 0, то он освещает все точки, которые не меньше его по абсциссе и ординате; если же ордината равна 0, то он освещает все точки, которые совпадают с ним по ординате и не меньше по абсциссе (см замечание 5.1).

Здесь видно, что нам не хватает леммы о светильниках и нужна ее расширенная версия:

Лемма 5.5. *Пусть, как и в лемме 5.3, дано множество светильников, только теперь каждый (x_1, \dots, x_n) освещает точки (y_1, \dots, y_n) , для которых выполнено два условия: $y_i \geq x_i$ и $y_i = 0$, если $x_i = 0$. Тогда, опять же, существует конечное подмножество светильников, которое освещает все остальные.*

Доказательство. Пусть K_i — множество точек, у которых ровно i координат ненулевые. Внутри K_i можно найти соответствующий ему конечный набор светильников по классической лемме. Остается заметить, что $\mathbb{Z}_+^n = \bigcup_{k=0}^n K_k$. \square

Теперь, в силу леммы, можно выбрать конечное подмножество светильников, которые мы сопоставили многочленам, освещающее все остальные.

Осталось доказать, что многочлены, которым соответствуют эти светильники являются конечной базой по первой координате (обозначим множество этих многочленов за M_0) множества M .

Предположим противное. Рассмотрим многочлен с наименьшим старшим членом по первой координате, первая координата которого не получается из M_0 .

Однако мы можем получить многочлен с таким же старшим членом по первой координате. Вычитая один из другого, получаем меньший многочлен, у которого первая координата не получается из M_0 . Противоречие.

5.4.2 Доказательство в общем случае

Как уже говорилось в этом параграфе, когда мы делаем подстановку φ внутри первой координаты, у нас возникает сумма

$$\sum_{i=1}^n x_i^m p_{1i}(x_1, \dots, x_n)$$

Видно, что первое слагаемое нам совсем не нужно, ведь оно разрешает умножать на x_1 , а это мы и так делать можем, в виду того, что работаем с первой координатой. Так что хотелось бы считать x_1 коэффициентом и воспользоваться конечной базируемостью уже для меньшего числа переменных.

Эта идея реализуется следующим образом. Во-первых, разрешим делать только φ подстановки, чтобы не потерять однородность. А во вторых, будем доказывать теорему 1 не над полем, а над произвольным нетеровым кольцом, содержащем подкольцо изоморфное \mathbb{Q} (последнее обобщение позволит нам в индукционном переходе считать x_1 коэффициентом, а не переменной).

Теорема 5.2. *Пусть M — множество многочленов от n переменных над нетеровым кольцом R , содержащем подкольцо изоморфное \mathbb{Q} . Тогда M конечно базируемо относительно линейных комбинаций и φ -подстановок.*

Ввиду того, что R содержит поле характеристики 0, леммы 5.1 и 5.2 дословно переносятся на этот обобщенный случай (ведь рассуждение с матрицей Вандермонда задействует только частный случай φ -подстановки). Значит, опять же можно доказывать теорему только для однородных многочленов.

Также мы все еще можем разбить многочлен на координаты 5 и доказать только конечную базируемость по каждой: параграф 4 нигде не использовал того, что множество коэффициентов — поле.

Итак, будем доказывать теорему 5.2 по индукции по числу переменных.

База индукции.

Пусть $n = 1$.

Заметим, что каждый многочлен с помощью φ -подстановки можно умножить на x , а с помощью линейной комбинации умножать на элемент кольца.

Следовательно из каждого многочлена из M можно получить идеал порожденный им в $R[x]$. Получается, что база индукции эквивалентна теореме Гильберта о базисе.

Переход индукции.

Пусть теорема верна для $n - 1$ переменной, докажем для n .

Рассмотрим координатные представления многочленов и, без ограничения общности, будем доказывать конечную базисуемость по первой.

Первая координата имеет вид $x_1^m P$. То есть, как и раньше, мы можем умножать многочлены внутри первой координаты на x_1 . Следовательно, достаточно доказать утверждение теоремы 5.2 с дополнительной операцией: теперь кроме линейных комбинаций и φ -подстановок также разрешим умножать на x_1 .

Как описывалось в начале параграфа, мы хотели бы на время забыть, что φ -подстановка действует на первую координату.

Введем ψ -подстановку:

$$\psi : P(x_1, \dots, x_n) \mapsto P_{(r,1)}(x_1, x_2 + r(x_2)x_2, \dots, x_n + r(x_n)x_n)$$

Лемма 5.6. *Множество многочленов от n переменных конечно базисуемо относительно ψ -подстановок, умножений на x_1 и линейных комбинаций.*

Доказательство. Заметим, что это множество можно рассматривать, как множество многочленов от $n - 1$ переменной (x_2, \dots, x_n) над кольцом $R[x_1]$. Причем все условия теоремы 2 в точности соблюдены. Так что по предположению индукции получаем требуемое. \square

Итак, осталось применить лемму. Назовем шириной монома его суммарную степень по переменным x_2, \dots, x_n .

Пусть нам нужно доказать конечную базисуемость множества M , причем опять же, как и раньше, будем считать, что оно замкнуто относительно φ -подстановок и линейных комбинаций. Тогда пусть N — множество получаемое из M , заменой каждого многочлена на него же, но с удаленными мономами не максимальной ширины.

Применив лемму 5.6 получаем, что N конечно базисуемо относительно ψ -подстановок. Пусть f'_1, \dots, f'_k конечный базис.

Рассмотрим f_1, \dots, f_k — какие-то многочлены, которые заменились на f'_1, \dots, f'_k при переходе от M к N . Предположим, что это не базис M . Тогда возьмем многочлен минимальной ширины $p \in M$, который нельзя получить с помощью φ -подстановок и линейных комбинаций (здесь мы пользуемся замкнутостью M). Пусть p' — соответствующий ему однородный по ширине многочлен из N .

Однако проделаем все те же операции, $\{f_i\}$, что делали с $\{f'_i\}$, чтобы получить p' , заменив подстановку вида ψ на соответствующую ей φ -подстановку. Заметим, что сначала мы можем применить операции подстановок, а потом уже один раз сделать линейную комбинацию, ведь φ и ψ -подстановки линейны.

Итак, сделаем все подстановки и заметим, что после линейной комбинации мономы старшей ширины совпадают с p' . Действительно, каждый раз делая φ -подстановку вместо ψ у нас возникают "лишние" члены не максимальной ширины (ведь отличие между ними в том, что одна бьет по x_1 — переменной не увеличивающей ширину, а другая нет). Также члены максимальной ширины не сократятся друг с другом или с какими-то другими, потому что они всегда совпадают с теми, что мы получали из $\{f'_i\}$.

Получается, что раз p не порождается базисом $\{f_i\}$, а какой-то многочлен с такими же мономами старшей ширины мы получить можем, то существует многочлен q меньшей ширины, чем p , который тоже не порождается базисом. Противоречие.

Замечание 5.2. В теореме 2 существенно, что мы доказываем конечную базисуемость относительно однородных подстановок. Иначе возникли бы эффекты, связанные с тем, что мономы старшей ширины, получаемые из f'_1, \dots, f'_k могли бы аннулировать, что не дало бы свести φ -подстановки к ψ -подстановкам.

Действительно, мы бы знали только то, что из f'_1, \dots, f'_k получаются все старшие по ширине компоненты. Однако они могли бы не совпасть со старшими компонентами после подстановок и линейной комбинации. Ведь последняя могла сократить старшие компоненты, полученные после подстановок (именно в этом месте мы существенно воспользовались однородностью подстановок), и разница между подстановками φ и ψ повлияла бы на итоговые старшие компоненты.

6 Связь методов Гришина с гипотезой Гельфанда

Список литературы

- [1] Y. Barnea и M. Larsen. “A non-abelian free pro-p group is not linear over a local field”. В: *Journal of Algebra* 214 (1999), с. 338—341.
- [2] D. Ben-Ezra и E. Zelmanov. “On Pro-2 Identities of 2×2 Linear Groups”. В: *arXiv:1910.05805v2* (2020).
- [3] L. Centrone и др. “Specht property for systems of commutative polynomials and Gelfand conjecture”. В: *researchgate net* (2022).
- [4] J. Dixon и др. “Analytic pro-p-groups”. В: *London Mathematical Society Lecture Note Series* (1991).
- [5] B. Feigin, A. Kanel-Belov и A. Khoroshkin. “On finite dimensionality of homology of subalgebras of vector fields”. В: *arXiv:2211.08510v1* (2022).
- [6] I.M. Gelfand. “The cohomology of infinite dimensional Lie algebras; Some questions of integral geometry”. В: *Proceedings of ICM T.1* (1970), с. 95—111.
- [7] A. Grishin. “On finitely based systems of generalized polynomials”. В: *Math. USSR-Izv.* 37.2 (1991), с. 243—272.
- [8] A. Lubotzky. “Combinatorial group theory for PRO-p groups”. В: *Pure and Applied Algebra* 25, (1982), с. 311—325.
- [9] R. Pink. “Compact subgroups of linear algebraic groups”. В: *Journal of Algebra* 206 (1998), с. 438—504.
- [10] E. Zelmanov. “Groups with identities”. В: *Note. Mat.* 36 (2016), с. 101—113.
- [11] E. Zelmanov. “Infinite algebras and pro-p groups”. В: *Infinite groups: geometric, combinatorial and dynamical aspects* 248 (2005), с. 403—413.
- [12] A. Zubkov. “Non-abelian free pro-p-groups cannot be represented by 2-by-2 matrices”. В: *Siberian Mathematical Journal* 28 (1987), с. 742—747.