Дважды экспоненциальная нижняя оценка на степень системы образующих полиномиального простого идеала

А. Л. Чистов

Санкт-Петербургское отделение
Математического института им. В.А. Стеклова
Российской академии наук,
191023 Санкт-Петербург, наб. р. Фонтанки 27
e-mail: alch@pdmi.ras.ru

2008

Аннотация

Рассмотрим полиномиальное кольцо A от $n+1$ переменных над произвольным бесконечным полем k. Мы доказываем, что для всех достаточно больших n и d существует однородный простой идеал $\mathfrak{p} \subset A$, удовлетворяющий следующим условиям. Идеал $\mathfrak{p}$ соответствует определённой над k и неприводимой над $\overline{k}$ компоненте проективного алгебраического многообразия, заданного системой однородных полиномиальных уравнений с многочленами из A степеней меньше чем d. Любая система образующих идеала $\mathfrak{p}$ содержит многочлен степени не меньше чем $d^{2^{cn}}$ для абсолютной константы $c > 0$, которая может быть вычислена эффективно. Это решает важную старую проблему в эффективной алгебраической геометрии. Для случая конечных полей мы получаем слегка менее сильный результат.

Введение

В классической статье [7] Д. Гильберт доказал, что произвольный полиномиальный идеал порождается конечным множеством многочленов. Следовательно, это справедливо для простого идеала $\mathfrak{p}$ неприводимой компоненты алгебраического многообразия, заданного системой полиномиальных уравнений от n неизвестных степеней меньше чем d. Возникла задача дать верхнюю и нижнюю оценки на степени образующих идеала $\mathfrak{p}$ как функцию от d и n. Отметим, что степень самого идеала $\mathfrak{p}$ (см. определение степени идеала ниже) ограничена сверху d^n согласно теореме Безу. Известно, что существует система образующих $\mathfrak{p}$ со степенями $d^{2^{O(n)}}$, см. замечание 2 ниже (случай неоднородного простого идеала легко сводится к случаю однородного простого идеала). Одной из самых важных открытых проблем эффективной алгебраической геометрии было получить аналогичную нижнюю оценку для степеней произвольной системы образующих некоторого идеала $\mathfrak{p}$. В настоящей статье мы решаем эту старую проблему над произвольным бесконечным полем, см. теорему 1 ниже. Отсюда вытекает та же самая нижняя оценка для стабилизации характеристической функции однородного идеала $\mathfrak{p}$, см. теорему 1 и замечание 1.

До сих пор дважды экспоненциальные нижние оценки были известны для биномиальных идеалов, подробности см. в разделе 1. Эти идеалы далеки от простых: они имеют много примарных компонент. Все попытки, свести случай простого идеала к известному случаю биномиальных идеалов, оканчивались неудачей. Наша конструкция – простая, однако весьма остроумная в этом смысле. Нам удалось осуществить требуемую редукцию! Ключ ко всему – лемма 2. Однако каким образом мы сделали это открытие? Не случайно. Мы исследовали проблему эффективной нормализации алгебраических многообразий. Оказывается, что построение нормализации алгебраического многообразия сводится к решению линейного уравнения $aX + bY + cZ = 0$ над кольцом многочленов. Одновременно как одно из следствий наших результатов мы получили лемму 2. Мы надеемся вернуться к нормализации алгебраического многообразия с алгоритмической точки зрения в одной из следующих статей. Заметим, что вопрос о решении уравнения $aX + bY + cZ = 0$ над кольцом многочленов близок к проблеме, сформулированной в конце введения.

Пусть k – поле с алгебраическим замыканием $\overline{k}$. Пусть $n \geqslant 0$ и $X_0, \ldots, X_n$ – переменные. Пусть $\mathfrak{a} \subset k[X_0, \ldots, X_n] = A$ – однородный идеал. Обозначим через $h(\mathfrak{a}, m) = \dim_k(A/\mathfrak{a})_m$ характеристическую функцию идеала $\mathfrak{a}$, где $(A/\mathfrak{a})_m$ – векторное пространство однородных элементов степени $m \geqslant 0$ кольца $A/\mathfrak{a}$. Напомним, что существует многочлен $P = \sum_{0 \leqslant i \leqslant n-s} p_i Z^i$, все $p_i \in \mathbb{Q}$, степени $\deg P = n - s$ такой, что $h(\mathfrak{a}, m) = P(m)$ для всех достаточно больших $m > 0$. По определению P – многочлен Гильберта кольца $A/\mathfrak{a}$. Степень идеала $\mathfrak{a}$ можно определить по формуле $\deg \mathfrak{a} = (n - s)! p_{n-s}$. Обозначим через $\mathcal{Z}(\mathfrak{a}) \subset \mathbb{P}^n(\overline{k})$ множество всех общих нулей многочленов из $\mathfrak{a}$ в $\mathbb{P}^n(\overline{k})$ (аналогичные обозначения будут использоваться ниже с другими идеалами или семействами многочленов и другими проективными или аффинными пространствами).

Ниже в формулировках теоремы, предложения, лемм и следствия утверждается существование констант c, n_0, d_0, c_0, c_1 и т. д. Все эти константы могут быть вычислены эффективно. Мы докажем следующий результат.

ТЕОРЕМА 1 *Существуют константы $c > 0$, $n_0 > 0$, $d_0 > 0$ такие, что для всякого бесконечного поля k для всех целых чисел $n > n_0$ и $d > d_0$ существуют однородные многочлены $f_1, \ldots, f_\nu \in A$, $\nu \leqslant n$, со всеми степенями $\deg f_i < d$, $1 \leqslant i \leqslant \nu$, и однородный простой идеал $\mathfrak{p} \subset A$, удовлетворяющие следующим условиям.*

(a) *Множество нулей $\mathcal{Z}(\mathfrak{p}) \subset \mathbb{P}^n(\overline{k})$ идеала $\mathfrak{p}$ совпадает с определённой над k и неприводимой над $\overline{k}$ компонентой проективного алгебраического многообразия $\mathcal{Z}(f_1, \ldots, f_\nu) \subset \mathbb{P}^n(\overline{k})$ всех общих нулей многочленов $f_1, \ldots, f_\nu$. Следовательно, идеал $\overline{k} \otimes_k \mathfrak{p} \subset \overline{k} \otimes_k A$ является простым. Более того, $\mathfrak{p}$ является примарной компонентой идеала $(f_1, \ldots, f_\nu) \subset A$, высота $\mathrm{ht}(\mathfrak{p}) = \nu$, и проективное алгебраическое многообразие $\mathcal{Z}(f_1, \ldots, f_\nu)$ имеет ровно две неприводимые над $\overline{k}$ компоненты: $\mathcal{Z}(\mathfrak{p})$ и некоторое линейное подпространство $\mathcal{L} \subset \mathbb{P}^n(\overline{k})$, определённое над k.*

(b) *Предположим, что характеристическая функция $h(\mathfrak{p}, m)$ стабильна для $m \geqslant m_0$, т.е., совпадает с многочленом Гильберта кольца $A/\mathfrak{p}$ для этих m. Тогда $m_0 \geqslant d^{2^{cn}}$.*

(c) *Пусть $a_1, \ldots, a_m$ – произвольная система образующих идеала $\mathfrak{p}$. Тогда максимальная степень $\max_{1 \leqslant i \leqslant m} \deg_{X_0, \ldots, X_n} a_i \geqslant d^{2^{cn}}$.*

Вполне вероятно, что можно удалить слово “бесконечного” в формулировке теоремы и получить результат для произвольного поля, см. замечание 5 в конце раздела 4. Также здесь может быть полезным замечание 4 в начале раздела 3. Однако в этой статье мы докажем только следующий результат.

ПРЕДЛОЖЕНИЕ 1 *Заменим в формулировке теоремы 1 слова “бесконечного поля” на “конечного поля” и $d^{2^{cn}}$ на $d^{2^{c\sqrt{n}}}$ в условиях (b) и (c). Тогда справедлива эта новая формулировка теоремы для случая конечных полей.*

ЗАМЕЧАНИЕ 1 *Известно, см. [5] разделы 6 и 7, что для любого однородного идеала $\mathfrak{a} \subset A$ выполняется следующее утверждение. Если характеристическая функция $h(\mathfrak{a}, m)$ стабильна для $m \geqslant m_0$, где $m_0 \geqslant 0$, то для всякого допустимого упорядочивания мономов редуцированный базис Грёбнера идеала $\mathfrak{a}$ относительно этого упорядочивания мономов состоит из однородных многочленов степеней самое большее $m_0 + 1$. Следовательно, существует система образующих идеала $\mathfrak{a}$ со степенями не больше чем $m_0 + 1$.*

Здесь вероятно надо привести некоторые подробности, относящиеся к последнему замечанию. Мы будем использовать обозначения из [5] (но заменим n на $n+1$). В [5] рассматриваются константы $b_0 \geqslant b_1 \geqslant \ldots \geqslant b_{n+2} = 0$, соответствующие идеалу $I = \mathfrak{a}$. Пусть целое число $m_0 \geqslant 0$ – минимально возможное такое, что характеристическая функция $h(\mathfrak{a}, m)$ стабильна для $m \geqslant m_0$. Тогда либо $m_0 = b_0$, или $m_0 = b_1 - 1$. Более точно, если $m_0 = b_1 - 1$, то $b_0 = b_1$ и не существует пары $\langle h, u \rangle$ в 0-стандартном точном коническом разложении N_I с $|u| = 0$ и $\deg h = b_1 - 1$. С другой стороны, по лемме 7.2 [5] степени многочленов рассматриваемого редуцированного базиса Грёбнера ограничены сверху b_0. Отсюда и вытекает утверждение замечания 1.

Заметим также, что перед леммой 7.2 [5] имеется следующая формула: $b_0 = \min\{d \geqslant b_1 : \forall_{z \geqslant d}\, \overline{\varphi}(z) = \varphi(z)\}$. Здесь мы исправили опечатку (которая сейчас может ввести в заблуждение читателя) и заменили $z > d$ на $z \geqslant d$ Иначе, эта формула противоречит определению констант b_i на стр.765 из [5].

ЗАМЕЧАНИЕ 2 *Пусть $\mathfrak{P} \subset A$ – произвольный однородный простой идеал высоты $\mathrm{ht}(\mathfrak{P}) = s$, $0 \leqslant s \leqslant n$, и степени d. Мы будем предполагать дополнительно, что идеал $\overline{k} \otimes_k \mathfrak{P} \subset \overline{k} \otimes_k A$ является радикальным. Тогда согласно лемме 9 и следствию 1 характеристическая функция $h(\mathfrak{P}, m)$ этого идеала стабильна для $m \geqslant \min\{(sd)^{O(n-s+1)^{n-s}}, d^{2^{O(n)}}\}$ и, следовательно, $\mathfrak{P}$ имеет систему образующих со степенями самое большее $\min\{(sd)^{O(n-s+1)^{n-s}}, d^{2^{O(n)}}\}$.*

ПРОБЛЕМА *Существуют ли константы $c > 0$, $n_0 > 0$, $d_0 > 0$, удовлетворяющие следующему свойству? Для всех целых чисел $n > n_0$, $d > d_0$ для всякого поля k существует однородный простой идеал $\mathfrak{p} \subset k[X_0, \ldots, X_n]$ со степенью $\deg \mathfrak{p} = d$ и высотой $\mathrm{ht}(\mathfrak{p}) = 2$ такой, что для этого идеала $\mathfrak{p}$ выполняется утверждение (c) теоремы 1.*

1 Нижние оценки для стабилизации характеристической функции биномиального идеала в произвольной характеристике

Произведение степеней переменных кольца $k[X_1, \ldots, X_{n-1}]$ – это моном $X_1^{i_1} \cdot \ldots \cdot X_{n-1}^{i_{n-1}}$ для некоторых целых чисел $i_j \geqslant 0$. По определению бином из $k[X_1, \ldots, X_{n-1}]$ есть разность двух различных произведений степеней переменных. Полиномиальный идеал $\mathfrak{g} \subset k[X_1, \ldots, X_{n-1}]$ называется биномиальным в том и только в том случае, когда у него есть система образующих, состоящая из биномов. Аналогичным образом определяются биномы и биномиальные идеалы для кольца $A^{(0)} = k[X_0, \ldots, X_{n-1}]$ и других полиномиальных колец.

ЛЕММА 1 *Существуют константы $c_1 > 0$, $n_0 > 0$ и $d_0 > 0$ такие, что для всякого поля k (произвольной характеристики и необязательно бесконечного) для всяких целых чисел $n > n_0$, $d > d_0$ существует однородный идеал $\mathfrak{b} \subset k[X_0, \ldots, X_{n-1}] = A^{(0)}$, удовлетворяющий следующему условию. Идеал $\mathfrak{b}$ порождён системой однородных биномов $b_1, \ldots, b_\mu$ степеней $\deg b_i = m_i < d$ и $\mu = O(n)$. Предположим, что характеристическая функция $h(\mathfrak{b}, m)$ стабильна для $m \geqslant m_0$, т.е., совпадает с многочленом Гильберта кольца $A^{(0)}/\mathfrak{b}$ для этих m. Тогда $m_0 \geqslant d^{2^{c_1 n}}$.*

ДОКАЗАТЕЛЬСТВО Покажем, ср. [11], что редуцированный базис Грёбнера любого биномиального идеала относительно любого допустимого упорядочивания мономов состоит из биномов. Действительно, можно построить базис Грёбнера согласно алгоритму Бухбергера. Каждый новый полином в алгоритме Бухбергера получается либо при помощи (i) редукции бинома другим биномом, либо (ii) как S-полином двух биномов. В обоих случаях (i) и (ii) результатом снова будет бином. Это доказывает требуемое утверждение.

Кроме того, если $e_1, \ldots, e_\alpha$ – редуцированный базис Грёбнера биномиального идеала $(q_1, \ldots, q_v) \subset k[X_1, \ldots, X_{n-1}]$ относительно некоторого допустимого упорядочивания мономов для произвольного фиксированного поля k нулевой характеристики (скажем для поля рациональных чисел $k = \mathbb{Q}$), то по той же причине $e_1 \bmod p, \ldots, e_\alpha \bmod p$ является редуцированным базисом Грёбнера идеала $(q_1 \bmod p, \ldots, q_v \bmod p) \subset k_p[X_1, \ldots, X_{n-1}]$ относительно того же самого упорядочивания мономов для произвольного поля k_p характеристики p для всякого простого числа p. Следовательно, число элементов α и максимальная степень $\max_{1 \leqslant i \leqslant \alpha} e_i$ редуцированного базиса Грёбнера идеала $(q_1, \ldots, q_v) \subset k[X_1, \ldots, X_{n-1}]$ не зависит от выбора поля k, в частности, от характеристики поля k.

В [11] доказано следующее утверждение (фактически для $\mathbb{Q}[X_1, \ldots, X_n]$ вместо $\mathbb{Q}[X_1, \ldots, X_{n-1}]$, но для нас удобно сформулировать его для $\mathbb{Q}[X_1, \ldots, X_{n-1}]$). Существуют константы $c_0 > 0$, $n_0 > 0$ и $d_0 > 0$ такие, что для всех целых чисел $n > n_0$, $d > d_0$ существуют целое число $\mu = O(n)$ и биномы $g_1, \ldots, g_\mu \in \mathbb{Q}[X_1, \ldots, X_{n-1}]$ (они строятся явно) степеней $\deg g_i < d$, $1 \leqslant i \leqslant \mu$, удовлетворяющие следующему условию. Пусть идеал $\mathfrak{g} = (g_1, \ldots, g_\mu) \subset \mathbb{Q}[X_1, \ldots, X_{n-1}]$. Пусть $e_1, \ldots, e_\alpha$ – редуцированный базис Грёбнера идеала $\mathfrak{g}$ относительно некоторого допустимого упорядочивания $<$ мономов (это упорядочивание может быть выбрано произвольным). Тогда $\max_{1 \leqslant i \leqslant \alpha} \deg e_i \geqslant d^{2^{c_0 n}}$. Согласно предыдущим аргументам это же утверждение справедливо над произвольным полем k вместо $\mathbb{Q}$. В дальнейшем мы будем обозначать через $e_1, \ldots, e_\alpha$ редуцированный базис Грёбнера идеала $(g_1, \ldots, g_\mu) \subset k[X_1, \ldots, X_{n-1}]$ относительно упорядочивания мономов $<$.

Для всякого $1 \leqslant i \leqslant \mu$ положим $b_i = X_0^{\deg g_i} g_i(X_1/X_0, \ldots, X_{n-1}/X_0) \in A^{(0)}$ равным гомогенизации многочлена g_i. Следовательно, b_i является однородным биномом из $k[X_0, \ldots, X_{n-1}]$. По определению однородный идеал $\mathfrak{b} = (b_1, \ldots, b_\mu) \subset k[X_0, \ldots, X_{n-1}]$. Мы будем предполагать без ограничения общности, что упорядочивание мономов $<$ является согласованным со степенью, т.е., для всех мономов $v_1, v_2 \in A$ условие $\deg v_1 < \deg v_2$ влечёт $v_1 < v_2$. Далее, рассмотрим допустимое упорядочивание мономов из $A^{(0)}$, которое продолжает упорядочивание $<$ на $k[X_1, \ldots, X_{n-1}]$ и такое, что $X_0^i < X_j$ для всех $1 \leqslant j \leqslant n$ и $i \geqslant 0$. Пусть $e'_1, \ldots, e'_\lambda$ – редуцированный базис Грёбнера идеала $\mathfrak{b}$ относительно рассматриваемого упорядочивания мономов. Тогда из определения базиса Грёбнера мы получаем немедленно, что $e'_1(1, X_1, \ldots, X_{n-1}), \ldots, e'_\lambda(1, X_1, \ldots, X_{n-1})$ является базисом Грёбнера относительно упорядочивания $<$ идеала $(g_1, \ldots, g_\mu)$. Поскольку упорядочивание $<$ мономов из $k[X_1, \ldots, X_{n-1}]$ является согласованным со степенью, то мы имеем

$$\max_{1 \leqslant i \leqslant \lambda} \deg e'_i(1, X_1, \ldots, X_{n-1}) \geqslant \max \deg_{1 \leqslant i \leqslant \alpha} e_i \geqslant d^{2^{c_0 n}}.$$

Следовательно, $\max_{1 \leqslant i \leqslant \lambda} \deg e'_i \geqslant d^{2^{c_0 n}}$. Теперь по замечанию 1 справедливо утверждение леммы. Лемма доказана.

В [11] можно найти также обзор результатов на эту тему. Все работы здесь основываются на первоначальных идеях из [9], где рассматриваются поля характеристики нуль (или, более точно, поле рациональных чисел). Доказательство леммы 2 [9] обо всех возможных биномах из биномиального идеала приводится над полем нулевой характеристики. Д. Ю. Григорьев (сообщение при личном общении) заметил, что имеется другое простое доказательство этой леммы в произвольной характеристике. Кажется, что нет других препятствий для того, чтобы распространить эти результаты на случай ненулевой характеристики. Следовательно, все нижние оценки для биномиальных идеалов справедливы в произвольной характеристике. В нашем доказательстве леммы 1 мы даже не используем лемму 2 из [9] в ненулевой характеристике.

2 Доказательство теоремы 1: условия (a) и (b)

Кольцо многочленов $A = k[X_0, \ldots, X_n]$ является градуированным относительно степени по всем переменным $X_0, \ldots, X_n$. Для градуированного A-модуля M и целого числа ν обозначим через $M(\nu)$ градуированный A-модуль со сдвинутой градуировкой. Именно, можно отождествить однородные компоненты $M(\nu)_m = M_{\nu+m}$ для всякого m, и это отождествление индуцирует изоморфизм A-модулей $M(\nu) \simeq M$. Последний изоморфизм является изоморфизмом степени ν градуированных A-модулей $M(\nu)$ и M.

Пусть X_{n+1}, $Z_1, \ldots, Z_\mu$ – новые переменные. Пусть

$$\Phi = X_0 X_n X_{n+1} + X_n^3 + X_{n+1}^3.$$

Положим кольца $A^{(1)} = A[X_{n+1}]$. Положим кольцо $B_\Phi = A^{(1)}/(\Phi)$. Теперь A, $A^{(1)}$, $A^{(1)}[Z_1, \ldots, Z_\mu]$ являются градуированными кольцами относительно полной степени по всем переменным $X_0, \ldots, X_{n+1}$, $Z_1, \ldots, Z_\mu$, т.е., однородные элементы степени m этих колец являются однородными многочленами степени m относительно всех этих переменных. Многочлен Φ однороден. Следовательно, B_Φ и $B_\Phi[Z_1, \ldots, Z_\mu]$ являются также градуированными кольцами.

Обозначим через $K^{(1)}$ и K' поля частных колец $A^{(1)}$ и B_Φ соответственно. Для произвольной рациональной функции $P/Q \in K^{(1)}$ такой, что $P, Q \in A^{(1)}$ и Φ не делит Q, мы будем обозначать через $(P/Q) \bmod \Phi$ образ этой рациональной функции в K'.

ЛЕММА 2 *Пусть k – произвольное поле. Пусть $\mathfrak{a} \subset A$ – однородный идеал такой, что $X_n \in \mathfrak{a}$, или $\mathfrak{a} = A$. Положим*

$$B_{\mathfrak{a}} = \left\{ \left(z_0 + z_1 X_{n+1} + z_2 \frac{X_{n+1}^2}{X_n} \right) \bmod \Phi \,:\, z_0, z_1 \in A \,\&\, z_2 \in \mathfrak{a} \right\} \subset K'.$$

Тогда $B_{\mathfrak{a}}$ является градуированным кольцом и конечно порождённым A-модулем. Далее, A-модуль $B_{\mathfrak{a}} \simeq A \oplus A(-1) \oplus \mathfrak{a}(-1)$. Кольцо $\overline{k} \otimes_k B_{\mathfrak{a}}$ является целостным. Поле частных кольца $B_{\mathfrak{a}}$ есть K', тензорное произведение $\overline{k} \otimes_k K'$ является полем, и расширение полей $\overline{k} \otimes_k K' \supset \overline{k}(X_0, \ldots, X_n)$ является конечным сепарабельным.

ДОКАЗАТЕЛЬСТВО Элемент $X_{n+1}^2 \bmod \Phi \in B_{\mathfrak{a}}$, поскольку $X_n \in \mathfrak{a}$. Для всех $x_1, x_2 \in \mathfrak{a}$ мы имеем

$$x_1 X_{n+1}^3 / X_n \bmod \Phi = (-x_1 X_n^2 - x_1 X_0 X_{n+1}) \bmod \Phi \in B_{\mathfrak{a}},$$
$$x_1 x_2 X_{n+1}^4 / X_n^2 \bmod \Phi = (-x_1 x_2 X_n X_{n+1} - x_1 x_2 X_0 X_{n+1}^2 / X_n) \bmod \Phi \in B_{\mathfrak{a}}$$

и $B_{\mathfrak{a}}$ является A-модулем. Поэтому $B_{\mathfrak{a}}$ является кольцом. Другие утверждения также устанавливаются непосредственно. Лемма доказана.

Пусть $\mathfrak{b} \subset A^{(0)}$ – идеал из леммы 1. Мы будем предполагать без ограничения общности, что $n_0 > 1$ в лемме 1 и, следовательно, $n \geqslant 2$. Положим $\mathfrak{b}' = \mathfrak{b}A + (X_n)$ равным однородному идеалу кольца A. Положим $\mathfrak{a} = \mathfrak{b}'$ в лемме 2 и $B' = B_{\mathfrak{b}'}$. Мы имеем $A/\mathfrak{b}' = A^{(0)}/\mathfrak{b}$. Следовательно, если $\dim(B')_m$ стабильна для $m \geqslant m_0$ (т.е., совпадает с многочленом Гильберта кольца $A^{(0)}/\mathfrak{b}$ для этих m), то $m_0 \geqslant d^{2^{c_1 n}} + 1$ согласно лемме 1.

Мы построим рекурсивно градуированные кольца $B^{(0)} = B'$, $B^{(1)}, \ldots, B^{(\mu)}$, удовлетворяющие для всякого i следующим свойствам.

(i) Кольцо $\overline{k} \otimes_k B^{(i)}$ целостно.

(ii) Расширение колец $B^{(i)} \supset A$ – целое.

(iii) Обозначим через $K^{(i)}$ поле частных кольца $B^{(i)}$. Тогда расширение полей $\overline{k} \otimes_k K^{(i)} \supset \overline{k}(X_0, \ldots, X_n)$ конечно сепарабельно.

(iv) Для $i \geqslant 1$ существуют ненулевые $\lambda_{i,1}, \lambda_{i,2}, \lambda_{i,3}, \lambda_{i,4} \in k$ такие, что многочлен

$$\begin{gathered}\varphi_i = Z_i^{m_i+1} + \lambda_{i,1} X_0^{m_i} Z_i + \lambda_{i,2} X_0^{m_i} X_1 + \lambda_{i,3} X_0^{m_i} X_2 + \\ \lambda_{i,4}(b_i X_{n+1}^2 / X_n) \bmod \Phi \in B^{(i-1)}[Z_i]\end{gathered}$$

является неприводимым элементом кольца $\overline{k} \otimes_k K^{(i)}[Z_i]$. *Положим по определению кольцо*

$$B^{(i)} = B^{(i-1)}[Z_i]/(\varphi_i).$$

Для $i = 0$ эти свойства следуют из определения кольца B'. Пусть $1 \leqslant i \leqslant \mu$ и $B^{(i-1)}$ построено. Построим $B^{(i)}$. Очевидно (i)–(iii) следуют из (iv). Так что достаточно построить многочлен φ_i из (iv).

Обозначим через $E^{(i-1)}$ целое замыкание кольца $\overline{k} \otimes_k B^{(i-1)}$ в его поле частных $\overline{k} \otimes_k K^{(i-1)}$. Заметим, что $E^{(i-1)}[Z_i] \supset \overline{k} \otimes_k B^{(i-1)}[Z_i]$. Обозначим через $V^{(i-1)}$ нормальное аффинное алгебраическое многообразие с кольцом регулярных функций $E^{(i-1)}[Z_i]$.

Пусть $\alpha \in k$ – ненулевой элемент. Определим элементы кольца $\overline{k} \otimes_k B^{(i-1)}[Z_i]$

$$\begin{array}{ll}\psi_1 = X_0^{m_i} X_2, & \psi_2 = X_0^{m_i} Z_i, \quad \psi_3 = X_0^{m_i} X_1, \\ \widetilde{\psi}_1 = \alpha Z_i^{m_i+1} + X_0^{m_i} X_2, & \widetilde{\psi}_2 = X_0^{m_i} Z_i, \\ \widetilde{\psi}_3 = X_0^{m_i} X_1 + \alpha(b_i X_{n+1}^2 / X_n) \bmod \Phi. & \end{array}$$

Тогда

$$V^{(i-1)} \cap \mathcal{Z}(\widetilde{\psi}_1, \widetilde{\psi}_2, \widetilde{\psi}_3) \subset V^{(i-1)} \cap \mathcal{Z}(Z_i, X_0 X_2).$$

Следовательно, по (ii) для $i - 1$

$$\dim(V^{(i-1)} \cap \mathcal{Z}(\widetilde{\psi}_1, \widetilde{\psi}_2, \widetilde{\psi}_3)) \leqslant \dim(V^{(i-1)}) - 2. \tag{1}$$

Далее, по (iii) для $i-1$ семейство $X_0, X_0^{m_i}X_1, X_0^{m_i}X_2, X_3, X_4, \ldots, X_n, X_0^{m_i}Z_i$ является сепарабельным базисом трансцендентности поля $\overline{k} \otimes_k K^{(i-1)}(Z_i)$ над $\overline{k}$. Поэтому морфизм

$$V^{(i-1)} \to \mathbb{A}^3(\overline{k}), \quad z \mapsto (\psi_1(z), \psi_2(z), \psi_3(z)) \tag{2}$$

сепарабелен доминантен, или, что эквивалентно, дифференциал этого морфизма в некоторой гладкой точке ξ является эпиморфизмом.

Покажем, что существует непустое открытое в топологии Зарисского подмножество $\mathcal{U}'' \subset \overline{k}$ (очевидно число элементов $\#(\overline{k} \setminus \mathcal{U}'') < +\infty$) такое, что для всех $\alpha \in \mathcal{U}'' \cap k$ рациональный морфизм

$$V^{(i-1)} \to \mathbb{P}^2(\overline{k}), \quad z \mapsto (\widetilde{\psi}_1(z) : \widetilde{\psi}_2(z) : \widetilde{\psi}_3(z)) \tag{3}$$

сепарабелен доминантен. Действительно, рассмотрим морфизм

$$\widetilde{\psi} : V^{(i-1)} \to \mathbb{A}^3(\overline{k}), \quad z \mapsto (\widetilde{\psi}_1(z), \widetilde{\psi}_2(z), \widetilde{\psi}_3(z)).$$

Пусть $V^{(i-1)} \subset \mathbb{A}^{n_1+2}(\overline{k})$, $n_1 \geqslant n+1$, и $\mathbb{A}^{n_1+2}(\overline{k})$ имеет координатные функции $Z_i, X_0, \ldots, X_{n_1}$. Пусть $h_1, \ldots, h_s \in \overline{k}[Z_i, X_0, \ldots, X_{n_1}]$ – система локальных параметров алгебраического многообразия $V^{(i-1)}$ в точке ξ. Тогда дифференциал морфизма (2) в точке ξ является эпиморфизмом в том и только в том случае, если дифференциалы $d_\xi h_1, \ldots, d_\xi h_s, d_\xi \psi_1, d_\xi \psi_2, d_\xi \psi_3$ линейно независимы над $\overline{k}$. Следовательно, дифференциалы $d_\xi h_1, \ldots, d_\xi h_s$, $d_\xi \widetilde{\psi}_1, d_\xi \widetilde{\psi}_2, d_\xi \widetilde{\psi}_3$ являются линейно независимыми над $\overline{k}$ для всех α из непустого открытого в топологии Зарисского подмножества $\mathcal{U}'' \subset \overline{k}$. Поэтому морфизм $\widetilde{\psi}$ доминантен и сепарабелен для всех $\alpha \in \mathcal{U}''$. Естественный морфизм $\pi : \mathbb{A}^3(\overline{k}) \setminus \{0\} \to \mathbb{P}^2(\overline{k})$ является доминантным сепарабельным. Морфизм (3) равен $\pi \circ \widetilde{\psi}$. Поэтому последний морфизм также является доминантным сепарабельным для всех $\alpha \in \mathcal{U}''$. Этим требуемое утверждение доказано.

Пусть $V', V'' \subset \mathbb{A}^n(\overline{k})$ – произвольные аффинные алгебраические многообразия. Напомним, что по определению пересечение алгебраических многообразий V' и V'' трансверсально тогда и только тогда, когда для всякой неприводимой над $\overline{k}$ компоненты W пересечения $V' \cap V''$ существует гладкая точка $z \in W$ такая, что z является гладкой точкой V' и V'' одновременно, и пересечение касательных пространств алгебраических многообразий V' и V'' в точке z трансверсально, где касательные пространства рассматриваются как подпространства в $\mathbb{A}^n(\overline{k})$.

В дальнейшем, если не оговорено противное, мы будем предполагать, что поле k бесконечно. Выберем и зафиксируем $\alpha \in \mathcal{U}'' \cap k$ (оно зависит от i). Напомним, что $V^{(i-1)} \subset \mathbb{A}^{n_1+2}(\overline{k})$. Морфизм (3) является сепарабельным доминантным, справедливо (1) и $n \geqslant 2$. Поэтому можно применить первую теорему Бертини, см. [12], [1], ср. [4], к морфизму (3). Согласно этой теореме существует многочлен φ, который является линейной комбинацией $\widetilde{\psi}_1, \widetilde{\psi}_2, \widetilde{\psi}_3$ с коэффициентами из k в общем положении такой, что пересечение $V^{(i-1)}$ и $\mathcal{Z}(\varphi)$ трансверсально в $\mathbb{A}^{n_1+2}(\overline{k})$ и неприводимо над $\overline{k}$.

Поскольку $E^{(i-1)}[Z_i]$ целозамкнуто, то для любого ненулевого элемента $\varphi' \in E^{(i-1)}[Z_i]$ идеал $(\varphi') \subset E^{(i-1)}[Z]$ является несмешанным, т.е. все ассоциированные простые идеалы идеала (φ') имеют одну и ту же высоту 1.

В нашей ситуации отсюда следует, что идеал $(\varphi) \subset E^{(i-1)}[Z_i]$ является простым. Следовательно, многочлен $\varphi \in \overline{k} \otimes_k K^{(i-1)}[Z_i]$ неприводим, поскольку $E^{(i-1)}$ является целозамкнутым. Умножая φ на ненулевой множитель из k, мы будем предполагать без ограничения общности, что старший коэффициент относительно Z_i многочлена φ равен 1. Теперь положим $\varphi_i = \varphi$. Следовательно, выполняется условие (iv). Мы получаем также $\lambda_{i,3} = \alpha^{-1}$, $\lambda_{i,4} = \alpha\lambda_{i,2}$, и, поэтому $\lambda_{i,2} = \lambda_{i,3}\lambda_{i,4}$.

Положим $B = B^{(\mu)}$. Обозначим через K поле частных кольца B. Следовательно, $\overline{k} \otimes_k K$ является полем частных кольца $\overline{k} \otimes_k B$. Согласно (iii) расширение полей $\overline{k} \otimes_k K \supset \overline{k}(X_0, \ldots, X_n)$ конечно сепарабельно.

Согласно (iv) имеет место изоморфизм градуированных A-модулей $B \simeq \oplus_{i \in I} B'(-\alpha_i)$, где число элементов $\#I = (m_1+1) \cdot \ldots \cdot (m_\mu+1) \leqslant d^\mu = d^{O(n)}$ и $0 \leqslant \alpha_i \leqslant (m_1 + \ldots + m_\mu) \leqslant (d-1)\mu = O(nd)$.

Согласно (iv) кольцо B порождено над k своей однородной компонентой B_1 и $\dim_k B_1 \leqslant N+1$, где $N = n+1+\mu = O(n)$. Положим $X_{n+1+i} = Z_i$, $1 \leqslant i \leqslant \mu$. Пусть $\mathbb{P}^N(\overline{k})$ имеет однородные координатные функции $X_0, \ldots, X_N$. Тогда по нашей конструкции $\overline{k} \otimes_k B$ является однородным кольцом проективного алгебраического многообразия $V' \subset \mathbb{P}^N(\overline{k})$, определённого над k и неприводимого над $\overline{k}$. Положим $\mathfrak{P}'$ равным однородному идеалу проективного алгебраического многообразия V'. Положим $f_1 = \Phi$ и

$$f_{i+1} = X_n X_{n+1+i}^{m_i+1} + \lambda_{i,1} X_0^{m_i} X_n X_{n+1+i} + \lambda_{i,2} X_0^{m_i} X_1 X_n + \\ \lambda_{i,3} X_0^{m_i} X_2 X_n + \lambda_{i,4} b_i X_{n+1}^2 \in k[X_0, \ldots, X_N], \quad 1 \leqslant i \leqslant \mu,$$

ср. с формулами для φ_i выше. Теперь $B = k[X_0, \ldots, X_N]/\mathfrak{P}'$,

$$f_1, \ldots, f_{\mu+1} \in k[X_0, \ldots, X_N], \quad \deg f_i < d' = O(d),\ 1 \leqslant i \leqslant \mu+1, \quad N = O(n). \tag{4}$$

Далее, $\mathcal{Z}(\mathfrak{P}')$ является определённой над k и неприводимой над $\overline{k}$ компонентой многообразия $\mathcal{Z}(f_1, \ldots, f_{\mu+1})$. Более точно, мы имеем разложение в объединение неприводимых над $\overline{k}$ компонент $\mathcal{Z}(f_1, \ldots, f_{\mu+1}) = \mathcal{Z}(\mathfrak{P}') \cup \mathcal{Z}(X_n, X_{n+1})$. Наконец, согласно нашей конструкции $\mathfrak{P}'$ является примарной компонентой идеала $(f_1, \ldots, f_{\mu+1}) \subset k[X_0, \ldots, X_N]$, высота $\mathrm{ht}(\mathfrak{P}') = \mu+1$ и размерность $\dim \mathcal{Z}(\mathfrak{P}') = n$. Следовательно, утверждение (a) теоремы справедливо для N, $(f_1, \ldots, f_{\mu+1})$, $\mathfrak{P}'$ (вместо n, $(f_1, \ldots, f_\nu)$, $\mathfrak{p}$).

Пусть $\alpha = \max_{i \in I} \alpha_i$. Тогда $\dim_k B_m$ стабильна для $m \geqslant m_0$ в том и только в том случае, если $\dim_k B'(-\alpha)_m$ стабильна для $m \geqslant m_0$. Мы имеем $B' \simeq A \oplus A(-1) \oplus \mathfrak{b}'(-1)$ и $\mathfrak{b}' = A\mathfrak{b} + (X_n)$, где $\mathfrak{b}$ – идеал из леммы 1. Следовательно, если $\dim_k B_m$ стабильна для $m \geqslant m_0$, то $\dim_k((A^{(0)}/\mathfrak{b})(-\alpha-1))_m$ стабильна для $m \geqslant m_0$. Поэтому $m_0 \geqslant d^{2^{c_1 n}} + \alpha +$ по лемме 1.

ЗАМЕЧАНИЕ 3 *Пусть $\mathfrak{P} \subset A$ – однородный простой идеал. $A' = A[X_{n+1}, \ldots, X_{n'}]$ для $n' \geqslant n$. Рассмотрим однородный простой идеал $\mathfrak{P}' = \mathfrak{P}A' + (X_{n+1}, \ldots, X_{n'}) \subset A'$. Тогда функция Гильберта кольца $A/\mathfrak{P}$ стабильна для $m \geqslant m_0$ в том и только в том случае, если функция Гильберта кольца $A'/\mathfrak{P}'$ стабильна для $m \geqslant m_0$. Далее, идеал $\mathfrak{P}$ имеет систему образующих $b_1, \ldots, b_w$ со всеми степенями $\deg b_i \leqslant v$ тогда и только тогда, когда $\mathfrak{P}'$ имеет систему образующих $b'_1, \ldots, b'_{w'}$ со всеми степенями $\deg b'_i \leqslant v$.*

Теперь можно рассмотреть простой идеал $\mathfrak{P}'' = \mathfrak{P}A'$. Функция Гильберта кольца $A'/\mathfrak{P}''$ стабильна для $m \geqslant m_0$ тогда и только тогда, когда функция Гильберта кольца $A'/\mathfrak{P}'$ стабильна для $m \geqslant m_0 + n' - n$ (это доказывается при помощи индукции по $n' - n$; здесь m_0 или $m_0 + n' - n$ может быть отрицательным).

Целые числа n, d – произвольные достаточно большие. Следовательно, из нашей конструкции и (4), используя замечание 3 и изменяя обозначения (N, $\mathfrak{P}'$, d' на n, $\mathfrak{P}^{(0)}$, d соответственно; подробности оставляем читателю), мы получаем следующее утверждение.

(*) *существуют константы $c_2 > 0$, $n_0 > 0$, $d_0 > 0$ (они могут быть отличны от констант из условия леммы 1) такие, что для всех целых чисел $n > n_0$, $d > d_0$ для всякого бесконечного поля k существуют однородные многочлены $f_1, \ldots, f_{\mu+1} \in k[X_0, \ldots, X_n]$, $\mu < n$, со всеми степенями $\deg f_i < d$, и однородный простой идеал $\mathfrak{P}^{(0)} \subset k[X_0, \ldots, X_n]$, удовлетворяющие условиям (a) и (b) теоремы 1 (вместо $f_1, \ldots, f_\nu$ и простого идеала $\mathfrak{p}$) с c_2 вместо c. Кроме того, согласно нашей конструкции высота $\mathrm{ht}(\mathfrak{P}^{(0)}) = \mu + 1 \leqslant n - 1$. Многочлены $f_1, \ldots, f_{\mu+1}$ зависят от выбора семейства элементов $\lambda_{i,j}$, $1 \leqslant i \leqslant \mu$, $1 \leqslant j \leqslant 3$, см. выше. Наконец, $\mathfrak{P}^{(0)}$ является примарной компонентой идеала $(f_1, \ldots, f_{\mu+1}) \subset k[X_0, \ldots, X_n]$, и проективное алгебраическое многообразие $\mathcal{Z}(f_1, \ldots, f_{\mu+1})$ имеет ровно две неприводимые над $\overline{k}$ компоненты: $\mathcal{Z}(\mathfrak{P}^{(0)})$ и некоторое линейное подпространство $\mathcal{L}^{(0)} \subset \mathbb{P}^n(\overline{k})$, определённое над k.*

3 Доказательство теоремы 1: условие (c)

Теперь наша цель - рассмотреть (a), (b) и (c) вместе.

ЗАМЕЧАНИЕ 4 *Было бы интересно установить, что $\mathfrak{P}^{(0)}$ также удовлетворяет (c) с константой $c_3 > 0$ вместо c, и после этого взять $c = \min\{c_2, c_3\}$ (фактически $c_2 \geqslant c_3$). Поскольку $3\mu = O(n)$, отсюда можно было бы вывести аналогично доказательству предложения 1, см. ниже в конце раздела, что теорема 1 верна также для любого конечного поля k, т.е., без всяких ограничений на поле k.*

Однако мы получим другой результат достаточный для того, чтобы доказать теорему.

Отождествим множество всех $(n-s)$-наборов $(L_{s+1}, \ldots, L_n)$ линейных форм $L_j \in \overline{k}[X_0, \ldots, X_n]$, $s \leqslant j \leqslant n$, с $\mathbb{A}^{(n+1)(n-s)}(\overline{k})$.

Пусть $\mathfrak{P} \subset A$ – произвольный однородный простой идеал высоты $s = \mathrm{ht}(\mathfrak{P})$, $0 \leqslant s \leqslant n-1$, и степени $\deg \mathfrak{P} = d$. Пусть $V = \mathcal{Z}(\mathfrak{P}) \subset \mathbb{P}^n(\overline{k})$ – проективное алгебраическое многообразие всех общих нулей многочленов из $\mathfrak{P}$ в $\mathbb{P}^n(\overline{k})$. Следовательно, $\dim V = n - s$. Мы будем предполагать дополнительно, что идеал $\overline{k} \otimes_k \mathfrak{P} \subset \overline{k} \otimes_k A$ – радикальный или, что эквивалентно, многообразие $\mathcal{Z}(\mathfrak{P})$ определено над k. Обозначим через $\mathfrak{M} = (X_0, \ldots, X_n)$ максимальный однородный простой идеал кольца A. Следующая лемма известна в случае, когда алгебраическое многообразие $\mathcal{Z}(\mathfrak{P}) \subset \mathbb{P}^n(\overline{k})$ является неприводимым над $\overline{k}$ (и фактически этот случай достаточен для наших целей). Всё же мы хотели бы доказать её в общем случае.

ЛЕММА 3 *Существует непустое открытое в топологии Зарисского подмножество $\mathcal{U} \subset \mathbb{A}^{(n+1)(n-s)}(\overline{k})$, удовлетворяющее следующим свойствам. Пусть набор из $(n-s)$ линейных форм $(L_{s+1}, \ldots, L_n) \in \mathcal{U}$, и все $L_j \in A$. Тогда* *(i)* *для всякого целого числа $s \leqslant i \leqslant n$ пересечение V и $\mathcal{Z}(L_{s+1}, \dots, L_i)$ трансверсально или, что эквивалентно в рассматриваемом случае, размерность $\dim(V \cap \mathcal{Z}(L_{s+1}, \dots, L_i)) = n - i$, и степень $\deg V = \deg(V \cap \mathcal{Z}(L_{s+1}, \dots, L_i))$;*

(ii) *для всякого целого числа $s \leqslant i < n$ число неприводимых над $\overline{k}$ компонент многообразия $V_i = V \cap \mathcal{Z}(L_{s+1}, \dots, L_i)$ равно числу неприводимых над $\overline{k}$ компонент многообразия V;*

(iii) *для всякого целого числа $s \leqslant i \leqslant n$ алгебраическое многообразие V_i определено над k;*

(iv) *для всякого целого числа $s \leqslant i < n$ проективное алгебраическое многообразие V_i является неприводимым над k и соответствует однородному простому идеалу $\mathfrak{P}_{L_{s+1},\dots,L_i} \subset k[X_0, \dots, X_n]$ высоты i;*

(v) *для $i = n$ проективное алгебраическое многообразие V_n является определённым над k конечным множеством точек в $\mathbb{P}^n(\overline{k})$, соответствующим однородному радикальному идеалу $\mathfrak{P}_{L_{s+1},\dots,L_n} \subset k[X_0, \dots, X_n]$;*

(vi) *следовательно, идеал $\overline{k} \otimes_k \mathfrak{P}_{L_{s+1},\dots,L_i} \subset \overline{k} \otimes_k A$ радикален для всех $s + 1 \leqslant i \leqslant n$;*

(vii) *для всякого $s + 1 \leqslant i \leqslant n$*

$$\mathfrak{P} + (L_{s+1}, \dots, L_i) = \mathfrak{P}_{L_{s+1},\dots,L_i} \cap \mathfrak{Q}_{L_{s+1},\dots,L_i},$$

где $\mathfrak{Q}_{L_{s+1},\dots,L_i}$ является $\mathfrak{M}$-примарным идеалом или $\mathfrak{Q}_{L_{s+1},\dots,L_i} = A$;

(viii) *следовательно, $X_j^N \mathfrak{P}_{L_{s+1},\dots,L_i} \subset \mathfrak{P} + (L_{s+1}, \dots, L_i)$ для всех $0 \leqslant j \leqslant n$ и всех достаточно больших $N \geqslant 0$.*

ДОКАЗАТЕЛЬСТВО Существует непустое открытое в топологии Зарисского подмножество $\mathcal{U}^{(0)} \subset \mathbb{A}^{(n-s)(n+1)}(\overline{k})$ такое, что для всякого $(L_{s+1}, \dots, L_n) \in \mathcal{U}^{(0)}$ пересечение V и $\mathcal{Z}(L_{s+1}, \dots, L_n)$ является трансверсальным, т.е. выполнено (i) (здесь мы оставляем подробности читателю). Пусть $\overline{k} \otimes_k \mathfrak{P} = \bigcap_{j \in J} \mathfrak{p}_j$ – редуцированное примарное разложение идеала $\overline{k} \otimes_k \mathfrak{P}$, где все $\mathfrak{p}_j \subset \overline{k} \otimes_k A$, $j \in J$, являются простыми идеалами. Тогда известно (это является следствием первой теоремы Бертини) см., например, приложение из [4], что, если заменить $\mathcal{U}$, k, A, $\mathfrak{P}$ на $\mathcal{U}_j$, $\overline{k}$, $\overline{k}[X_0, \dots, X_n]$, $\mathfrak{p}_j$ (для произвольного но фиксированного $j \in J$) соответственно, то справедливы утверждения (i)–(v), (vii), (viii). Положим $\mathcal{U} = \mathcal{U}^{(0)} \cap \bigcap_{j \in J} \mathcal{U}_j$.

Пусть $(L_{s+1}, \dots, L_n) \in \mathcal{U}$. Теперь выполняются (i) и (ii). Однородный идеал алгебраического многообразия V_i равен $\bigcap_{j \in J} \mathfrak{p}_{j,L_{s+1},\dots,L_i}$. Мы имеем $\overline{k} \otimes_k \mathfrak{P} + (L_{s+1}, \dots, L_n)\overline{k} \otimes_k A \subset \bigcap_{j \in J}(\mathfrak{p}_j + (L_{s+1}, \dots, L_n)\overline{k} \otimes_k A)$. Следовательно, по (vii) для $\mathfrak{p}_j$ справедливо равенство

$$\overline{k} \otimes_k \mathfrak{P} + (L_{s+1}, \dots, L_n)\overline{k} \otimes_k A = \bigcap_{j \in J} \mathfrak{p}_j \cap \mathfrak{Q}', \tag{5}$$

где $\mathfrak{Q}'$ является $\overline{k} \otimes_k \mathfrak{M}$-примарным идеалом или $\mathfrak{Q}' = \overline{k} \otimes_k A$.

Докажем (iii). Существует ненулевая линейная форма $L_0 \in A$ такая, что $V_i \setminus \mathcal{Z}(L_0)$ является плотным в топологии Зарисского подмножеством многообразия V_i. Согласно (5) кольцо определённых над $\overline{k}$ регулярных функций на $V_i \setminus \mathcal{Z}(L_0)$ равно $\overline{k}[V \setminus \mathcal{Z}(L_0)]/(L_{s+1}/L_0, \ldots, L_i/L_0)$. Поэтому $V_i \setminus \mathcal{Z}(L_0)$ определено над k. Обозначим через k_s сепарабельное замыкание поля k. Следовательно, множество точек $(V_i \setminus \mathcal{Z}(L_0))(k_s)$ является плотным в топологии Зарисского и инвариантным относительно действия группы Галуа $\mathrm{Gal}(\overline{k}/k)$ подмножеством многообразия V_i. Следовательно, по известному критерию V_i определено над k. Утверждение (iii) доказано. Теперь также выполняется (v).

Докажем (iv). Группа Галуа $\mathrm{Gal}(\overline{k}/k)$ действует транзитивно на неприводимых над $\overline{k}$ компонентах $\mathcal{Z}(\mathfrak{p}_{j,L_{s+1},\ldots,L_i})$ алгебраического многообразия V_i. Поэтому V_i неприводимо над k и (iv) доказано. Теперь также доказано (vi).

Докажем (viii). По (5) мы имеем

$$X_j^N \mathfrak{P}_{L_{s+1},\ldots,L_i} \subset (\overline{k} \otimes_k \mathfrak{P} + (L_{s+1}, \ldots, L_i)\overline{k} \otimes_k A) \cap A = \mathfrak{P} + (L_{s+1}, \ldots, L_i)$$

и (viii) доказано. Очевидно (viii) влечёт (vii). Лемма доказана.

Пусть $u = \{u_{i,j}\}$, $i \in \{0, s+1, s+2, \ldots, n+1\}$, $0 \leqslant j \leqslant n$, – семейство алгебраически независимых элементов над полем k, т.е., степень трансцендентности этого семейства над k равна $(n-s+2)(n+1)$. Обозначим через $k_u = k(u)$ расширение поля k элементами семейства u. Пусть $U_i = \sum_{0 \leqslant j \leqslant n} u_{i,j} X_j \in k_u[X_0, \ldots, X_n]$, $s+1 \leqslant i \leqslant n$, – семейство общих линейных форм над k. Тогда $(n-s)$-набор $(U_{s+1}, \ldots, U_n)$ является общей точкой многообразия $\mathcal{U}$, см. лемма 3, и $(U_{n+1}, \ldots, U_n) \in \mathcal{U}(\overline{k_u})$. Расширим основное поле k до k_u. Мы будем обозначать снова через $\mathfrak{P}$ идеал кольца $k_u \otimes_k \mathfrak{P} \subset k_u \otimes_k A$ (это не приведёт в двусмысленности). Теперь идеалы $\mathfrak{P}_{U_{s+1},\ldots,U_i}$ определены для всех $s \leqslant i \leqslant n$.

Обозначим через $k[u]$ полиномиальное кольцо с коэффициентами из k и переменными из семейства u. Обозначим через $k[u, X_0, \ldots, X_n]$ полиномиальное кольцо с коэффициентами из k и переменными из семейств u и $X_0, \ldots, X_n$ (аналогичные обозначения будут использоваться с другими переменными). Пусть $s+1 \leqslant i \leqslant n$ – целое число. Обозначим для краткости $\mathfrak{P}_{i-1} = \mathfrak{P}_{U_{s+1},\ldots,U_{i-1}}$, $\mathfrak{P}_i = \mathfrak{P}_{U_{s+1},\ldots,U_i}$. Положим

$$k_u'' = \left\{ P/Q \in k_u \,:\, P, Q \in k[u] \,\&\, \deg_{u_{i,n}} P \leqslant 0, \deg_{u_{i,n}} Q = 0 \right\},$$

т.е., k_u'' является подполем в k_u всех элементов, которые не зависят от $u_{i,n}$. Заметим, что идеал $\mathfrak{P}_{i-1}$ имеет систему образующих $p_1, \ldots, p_\gamma \in k_u''[X_0, \ldots, X_n]$ (фактически можно выбрать все $p_j \in k[u, X_0, \ldots, X_n]$ со степенями $\deg_{u_{i_1,j_1}} p_j = 0$ для всех $i_1 \in \{0, i, \ldots, n+1\}$, $0 \leqslant j_1 \leqslant n$). Определим мультипликативно замкнутые множества

$$\begin{aligned}
&S_{\mathfrak{P}_{i-1}} = k_u''[X_0, \ldots, X_n] \setminus (p_1, \ldots, p_\gamma) \subset k_u''[X_0, \ldots, X_n],\\
&S_{i,n} = k[u, X_0, \ldots, X_n] \setminus U_i k[u, X_0, \ldots, X_n] \subset k[u, X_0, \ldots, X_n],\\
&S = \{X_n^i \,:\, 0 \leqslant i \in \mathbb{Z}\} \subset k[X_0, \ldots, X_n].
\end{aligned}$$

Локализация $S_{i,n}^{-1} k[u, X_0, \ldots, X_n] \supset k_u[X_0, \ldots, X_n]$. Если $z \in S_{i,n}^{-1} k[u, X_0, \ldots, X_n]$, то можно подставить $u_{i,n} = (-\sum_{0 \leqslant i \leqslant n-1} u_{i,j} X_j)/X_n$ в z. Обозначим через $\pi(z)$ результат этой подстановки. Тогда очевидно $\pi(z) \in k_u''(X_0,$

$\ldots, X_n)$, и отображение $z \mapsto \pi(z)$ является гомоморфизмом k''_u-алгебр $\pi : S_{i,n}^{-1} k[u, X_0, \ldots, X_n] \to k''_u(X_0, \ldots, X_n)$. Если $z \in k''_u(X_0, \ldots, X_n)$, то $\pi(z) = z$. Очевидно ядро $\mathrm{Ker}(\pi) = U_i S_{i,n}^{-1} k[X_0, \ldots, X_n]$.

ЛЕММА 4 *В предыдущих обозначениях предположим, что $X_n \notin \mathfrak{P}$. Тогда для всякого $z \in k_u[X_0, \ldots, X_n]$ элемент $\pi(z) \in S_{\mathfrak{P}_{i-1}}^{-1} k''_u[X_0, \ldots, X_n]$. Далее, если $z \in \mathfrak{P}_i$, то $\pi(z) \in S_{\mathfrak{P}_{i-1}}^{-1}(k''_u[X_0, \ldots, X_n] \cap \mathfrak{P}_{i-1})$. Наконец, если $z \in k[u, X_0, \ldots, X_n] \cap \mathfrak{P}_i$, то $\pi(z) \in S^{-1}(k[u, X_0, \ldots, X_n] \cap \mathfrak{P}_{i-1})$.*

ДОКАЗАТЕЛЬСТВО Пусть $z \in k_u[X_0, \ldots, X_n]$. Тогда $z = P/Q$, где $0 \neq Q \in k[u]$, $P \in k[u, X_0, \ldots, X_n]$. Мы имеем $\pi(P) \in S^{-1} k''_u[X_0, \ldots, X_n] \subset S_{\mathfrak{P}_{i-1}}^{-1} k''_u[X_0, \ldots, X_n]$. Пусть $\deg_{u_{i,n}} Q = r$. Тогда $X_n^r \pi(Q) \in k''_u[X_0, \ldots, X_n]$. Следовательно, достаточно доказать, что $X_n^r \pi(Q) \in S_{\mathfrak{P}_{i-1}}$. Определение гомоморфизма π влечёт $\pi(Q) = q((-\sum_{0 \leqslant j \leqslant n-1} X_j u_{i,j})/X_n)$ для некоторого многочлена $0 \neq q \in k''_u[Z]$. Обозначим через $k_u(\mathcal{Z}(\mathfrak{P}_{i-1}))$ поле определённых над k_u рациональных функций на алгебраическом многообразии $\mathcal{Z}(\mathfrak{P}_{i-1}) \subset \mathbb{P}^n(\overline{k_u})$. Мы имеем $X_n \notin \mathfrak{P}$ и $U_{s+1}, \ldots, U_{i-1}$ – являются общими линейными формами. Следовательно, X_n не обращается в нуль в общей точке алгебраического многообразия $\mathcal{Z}(\mathfrak{P}) \cap \mathcal{Z}(U_{s+1}, \ldots, U_{i-1}) \subset \mathbb{P}^n(\overline{k_u})$. Поэтому $X_n \notin \mathfrak{P}_{i-1}$ и очевидно $i - 1 < n$. Пусть

$$k'''_u = \left\{ P/Q \in k_u \,:\, P, Q \in k[u] \,\&\, \deg_{u_{i,j}} P \leqslant 0,\, \deg_{u_{i,j}} Q = 0,\, 0 \leqslant j \leqslant n \right\},$$

т.е., k'''_u является подполем поля k_u, состоящим из всех элементов, которые не зависят от всех $u_{i,j}$, $0 \leqslant j \leqslant n$. Алгебраическое многообразие $\mathcal{Z}(\mathfrak{P}_{i-1})$ определено над k'''_u согласно лемме 3 с основным полем k'''_u вместо k. Следовательно,

$$-\sum_{0 \leqslant j \leqslant n-1} u_{i,j}(X_j/X_n) \in k_u(\mathcal{Z}(\mathfrak{P}_{i-1}))$$

является трансцендентным элементом над полем k_u. Поэтому $X_n^r \pi(Q) \notin \mathfrak{P}_{i-1}$. Требуемое утверждение доказано.

Пусть $z \in \mathfrak{P}_i$. Тогда $z \in S^{-1}(\mathfrak{P}_{i-1} + (U_i))$ по лемме 3 (viii) с основным полем k_u вместо k. Следовательно, можно представить $z = \sum_{1 \leqslant j \leqslant \gamma} p_j q_j + U_i q$, где p_j были введены выше, все $q_j, q \in S^{-1} k_u[X_0, \ldots, X_n]$. Поэтому

$$\pi(z) = \sum_{1 \leqslant j \leqslant \gamma} p_j \pi(q_j) \in S_{\mathfrak{P}_{i-1}}^{-1}(k''_u[X_0, \ldots, X_n] \cap \mathfrak{P}_{i-1}).$$

Пусть $z \in k[u, X_0, \ldots, X_n] \cap \mathfrak{P}_{i-1}$. Тогда по доказанному

$$\pi(z) \in S^{-1} k[u, X_0, \ldots, X_n] \cap S_{\mathfrak{P}_{i-1}}^{-1} \mathfrak{P}_{i-1} = S^{-1}(k[u, X_0, \ldots, X_n] \cap \mathfrak{P}_{i-1}).$$

Последнее утверждение и вся лемма доказаны.

ЛЕММА 5 *В предыдущих обозначениях предположим, что для некоторого $s + 1 \leqslant i \leqslant n - 1$ идеал $\mathfrak{P}_{U_{s+1}, \ldots, U_i}$ имеет систему образующих со степенями относительно $X_0, \ldots, X_n$ самое большее D, где $D \geqslant 2$. Тогда*

(i) Существует система образующих $q_1, \ldots, q_\beta \in k[u, X_0, \ldots, X_n]$ идеала $\mathfrak{P}_{U_{s+1}, \ldots, U_i}$ такая, что $\deg_{X_0, \ldots, X_n} q_j \leqslant D$ и $\deg_{u_{v,w}} q_j = (Dd)^{O(n-i)}$ для всех v, w (здесь и ниже $\deg_{u_{w,v}}$ – степень относительно переменной $u_{w,v}$) с универсальной константой в $O(n - i)$.

(ii) *Существует непустое открытое в топологии Зарисского подмножество $\mathcal{U}'_i \subset \mathcal{U}$, удовлетворяющее следующим свойствам. Существует абсолютная константа $c'_4 > 0$ такая, что для всякого $(L_{s+1}, \dots, L_n) \in \mathcal{U}'_i$ для всех $0 \leqslant j \leqslant n$ идеал*

$$X_j^N \mathfrak{P}_{L_{s+1},\dots,L_i} \subset \mathfrak{P}_{L_{s+1},\dots,L_{i-1}} + (L_i) \tag{6}$$

для некоторого целого числа $N \leqslant (Dd)^{c'_4(n-i)}$. Следовательно, существует абсолютная константа $c_4 > 0$ такая, что для всякого $(L_{s+1}, \dots, L_n) \in \mathcal{U}'_i$ для всех $m \geqslant (Dd)^{c_4(n-i)}$ однородные компоненты $(\mathfrak{P}_{L_{s+1},\dots,L_i})_m$ и $(\mathfrak{P}_{L_{s+1},\dots,L_{i-1}} + (L_i))_m$ (идеалов $\mathfrak{P}_{L_{s+1},\dots,L_i}$ и $\mathfrak{P}_{L_{s+1},\dots,L_{i-1}} + (L_i)$) совпадают.

ДОКАЗАТЕЛЬСТВО Докажем (i). Рассмотрим морфизм $\pi_U : \mathcal{Z}(\mathfrak{P}) \to \mathbb{P}^{n-s+1}(\overline{k_u})$, $(X_0 : \ldots : X_n) \mapsto (U_0 : U_{s+1} : \ldots : U_{n+1})$ проективных алгебраических многообразий. Тогда, ср. [3], образ $\pi_U(\mathcal{Z}(\mathfrak{P}))$ замкнут в $\mathbb{P}^{n-s+1}(\overline{k_u})$ и определён над k_u, $\deg \pi_U(\mathcal{Z}(\mathfrak{P})) = d$. Далее, $\pi_U(\mathcal{Z}(\mathfrak{P})) = \mathcal{Z}(F_{\mathfrak{P}})$, где $F_{\mathfrak{P}} \in k[u, Z_0, Z_{s+1}, \ldots, Z_n]$ – однородный многочлен относительно $Z_0, Z_{s+1}, \ldots, Z_n$ такой, что $F_{\mathfrak{P}}(U_0, U_{s+1}, \ldots, U_{n+1})$ обращается в нуль тождественно на $\mathcal{Z}(\mathfrak{P})$ в $\mathbb{P}^n(\overline{k_u})$, степень $\deg F_{\mathfrak{P}} = d$ и старший коэффициент $0 \neq \mathrm{lc}_{Z_{n+1}} F_{\mathfrak{P}} \in k[u]$ (здесь мы обозначаем через $\mathrm{lc}_{Z_n} F_{\mathfrak{P}}$ старший коэффициент многочлена $F_{\mathfrak{P}}$ относительно Z_{n+1}). Поскольку $\pi_U(\mathcal{Z}(\mathfrak{P}))$ определено над k_u и неприводимо над k_u, то многочлен $F_{\mathfrak{P}}$ не имеет кратных множителей над $\overline{k_u}$ и неприводим над k_u. Так как $0 \neq \mathrm{lc}_{Z_{n+1}} F_{\mathfrak{P}} \in k[u]$, то полином $F_{\mathfrak{P}}$ сепарабелен относительно Z_{n+1}, т.е., $\partial F_{\mathfrak{P}} / \partial Z_{n+1} \neq 0$. Кроме того, ср. [3], морфизм $\mathcal{Z}(\mathfrak{P}) \to \pi_U(\mathcal{Z}(\mathfrak{P}))$, индуцированный π_U, является конечным сепарабельным и бирациональным изоморфизмом определённых над k_u проективных алгебраических многообразий.

Многочлен $F_{\mathfrak{P}}$ однозначно определён с точностью до множителя из $k[u]$. В дальнейшем мы будем предполагать, не умаляя общности, что GCD всех коэффициентов из $k[u]$ при мономах от $X_0, \ldots, X_n$ многочлена $F_{\mathfrak{P}}$ равен 1. Так что мы фиксируем $F_{\mathfrak{P}}$ с точностью до ненулевого множителя из k. Мы имеем $\deg_{u_{i,0},\ldots,u_{i,n}} F_{\mathfrak{P}} = d$ для всякого $i \in \{0, s+1, s+2, \ldots, n+1\}$, см. [3] лемма 9.

Пусть $L_0, L_{s+1}, \ldots, L_{n+1} \in k[u, X_0, \ldots, X_n]$ – линейные формы относительно $X_0, \ldots, X_n$ в общем положении. Обозначим $L = (L_0, L_{s+1}, \ldots, L_{n+1})$. Пусть $L_i = \sum_{0 \leqslant j \leqslant n} l_{i,j} X_j$, где коэффициенты $l_{i,j} \in k_u$ для всех i, j. Подставим $u_{i,j} = l_{i,j}$ для всех i, j в $F_{\mathfrak{P}}$. Обозначим полученный многочлен через $F_{\mathfrak{P},L} \in k[u, X_0, \ldots, X_n]$. Поскольку $L_0, L_{s+1}, \ldots, L_{n+1}$ находятся в общем положении многочлен $F_{\mathfrak{P},L}$ сепарабелен относительно Z_{n+1}, $\deg F_{\mathfrak{P},L} = \deg_{Z_{n+1}} F_{\mathfrak{P},L} = d$, $0 \neq \mathrm{lc}_{Z_{n+1}} F_{\mathfrak{P},L} \in k[u]$, и многочлен $F_{\mathfrak{P},L}(L_0, L_{s+1}, \ldots, L_{n+1})$ обращается в нуль тождественно на $\mathcal{Z}(\mathfrak{P})$. Далее, обозначим через $\pi_L : \mathcal{Z}(\mathfrak{P}) \to \mathbb{P}^{n-s+1}(\overline{k_u})$, $(X_0 : \ldots : X_n) \mapsto (L_0 : L_{s+1} : \ldots : L_{n+1})$ морфизм проективных алгебраических многообразий. Тогда образ $\pi_L(\mathcal{Z}(\mathfrak{P}))$ замкнут в $\mathbb{P}^{n-s+1}(\overline{k_u})$ и определён над k_u, $\deg \pi(\mathcal{Z}(\mathfrak{P})) = d$ и $\pi_L(\mathcal{Z}(\mathfrak{P})) = \mathcal{Z}(F_{\mathfrak{P},L})$. Кроме того, морфизм $\mathcal{Z}(\mathfrak{P}) \to \pi_L(\mathcal{Z}(\mathfrak{P}))$, индуцированный π_L, является конечным сепарабельным и бирациональным изоморфизмом определённых над k_u проективных алгебраических многообразий. В частности, многочлен $F_{\mathfrak{P},L}$ неприводим над полем k_u.

Пусть $s \leqslant i \leqslant n-1$. Положим $L' = (L_0, U_{s+1}, \ldots, U_i, L_{i+1}, \ldots, L_{n+1})$, где все $L_i \in k[X_0, \ldots, X_n]$ являются линейными формами в общем положении. Напомним обозначение $\mathfrak{P}_i = \mathfrak{P}_{U_{s+1},\ldots,U_i}$. Так как L_0 – линейная форма в общем положении, то мы будем предполагать в дальнейшем без ограничения общности, что L_0 не обращается в нуль тождественно ни на какой определённой над $\overline{k}$ компоненте многообразия $\mathcal{Z}(\mathfrak{P}_i)$. Многочлен $F' = F_{\mathfrak{P},L'}(Z_0, 0, \ldots, 0,\ Z_{i+1}, \ldots, Z_{n+1}) \in k_u[Z_0, Z_{i+1}, \ldots, Z_{n+1}]$ (здесь мы подставляем 0 вместо U_j, $s+1 \leqslant j \leqslant i$) – ненулевой степени d, поскольку старший коэффициент многочлена F' относительно Z_{n+1} является ненулевым полиномом из $k[u]$. Очевидно многочлен F' обращается в нуль тождественно на $\mathcal{Z}(\mathfrak{P}_i)$. Поскольку линейные формы L_i находятся в общем положении, то многочлен $F_{\mathfrak{P}_i,(L_0,L_{i+1},\ldots,L_{n+1})}$ определён и удовлетворяет свойствам, аналогичным тем, которым удовлетворяет полином $F_{\mathfrak{P},L}$, см. выше. Теперь $F_{\mathfrak{P}_i,(L_0,L_{i+1},\ldots,L_{n+1})}$ совпадает с F' с точностью до множителя $f' \in k[u]$. В частности, полином F' неприводим над полем k_u.

Заменим F' на F'/f'. Обозначим через k'_u подполе поля k_u, порождённое над k элементами семейства $u' = \{u_{v,j}\}$, $s+1 \leqslant v \leqslant i$, $0 \leqslant j \leqslant n$. Теперь все коэффициенты многочлена F' принадлежат полю k'_u

Положим $t_j = L_j/L_0$, $i+1 \leqslant j \leqslant n$, и $\Psi = F'(1, t_{i+1}, \ldots, t_n, Z) \in k[u, t_{i+1}, \ldots,\ t_n, Z]$. Многочлен $\Psi \in k_u(t_{i+1}, \ldots, t_n)[Z]$ неприводим и сепарабелен относительно Z, $\deg_Z \Psi = d$, $0 \neq \mathrm{lc}_Z \Psi \in k[u]$. Следовательно, поле определённых над k_u рациональных функций $k_u(\mathcal{Z}(\mathfrak{P}_i)) \simeq k_u(t_{i+1}, \ldots, t_n)[Z]/(\Psi)$ согласно описанной конструкции. Положим

$$\theta = Z \bmod \Psi \in k_u(t_{i+1}, \ldots, t_n)[Z]/(\Psi) \simeq k_u(\mathcal{Z}(\mathfrak{P}_i)). \tag{7}$$

Очевидно коэффициенты полинома Ψ принадлежат полю k'_u.

Положим $L'' = (L_0, U_{s+1}, \ldots, U_i, L_{i+1}, \ldots, L_n, U_{n+1})$, где линейные формы $L_{i+1},\ \ldots, L_n$ – такие же, как и выше. Положим $F'' = F_{\mathfrak{P},L''}(Z_0, 0, \ldots, 0, Z_{i+1}, \ldots, Z_{n+1}) \in k_u[Z_0,\ Z_{i+1}, \ldots, L_n]$ (здесь мы подставляем 0 вместо U_j, $s+1 \leqslant j \leqslant i$). Рациональная функция $F''(1, t_{i+1}, \ldots, t_n, U_{n+1}/L_0)$ обращается в нуль тождественно на $\mathcal{Z}(\mathfrak{P}_i) \setminus \mathcal{Z}(L_0)$. Поэтому существует корень $Z = \xi_U$ многочлена $F''(1, t_{i+1}, \ldots, t_n, Z)$ в поле $k_u(t_{i+1}, \ldots, t_n)[\theta]$ вида

$$\xi_U = \frac{1}{\xi^{(0)}} \sum_{0 \leqslant v \leqslant n} \left(\sum_{0 \leqslant j < \deg_Z \Psi} \xi_{v,j} \theta^j \right) u_{n+1,v},$$

где все $\xi^{(0)}, \xi_{v,j} \in k[u', t_{i+1}, \ldots, t_n]$, $0 \leqslant j \leqslant n$, $\xi^{(0)} \neq 0$, и наибольший общий делитель $\mathrm{GCD}_{v,j}\{\xi^{(0)}, \xi_{v,j}\} = 1$ в кольце $k[u', t_{i+1}, \ldots, t_n]$.

Таким образом, существует общая точка алгебраического многообразия $\mathcal{Z}(\mathfrak{P}_{U_{s+1},\ldots,U_i}) \subset \mathbb{P}^n(\overline{k_u})$ вида

$$\frac{X_v}{L_0} = \xi_v = \frac{1}{\xi^{(0)}} \sum_{0 \leqslant j < \deg_Z \Psi} \xi_{v,j} \theta^j \in k'_u(t_{i+1}, \ldots, t_n)[\theta], \quad 0 \leqslant v \leqslant n, \tag{8}$$

Согласно алгоритму для факторизации полиномов, см. [2]: $\deg_Z \Psi = d$, все степени

$$\deg_{t_j} \Psi,\ \deg_{u_{v,w}} \Psi,\ \deg_{t_j} \xi^{(0)},\ \deg_{t_j} \xi_{v,j},\ \deg_{u_{v,w}} \xi^{(0)},\ \deg_{u_{v,w}} \xi_{v,j}$$

ограничены сверху $(d+1)^{O(1)}$ с абсолютной константой в $O(1)$ для всех j v, w.

Обозначим через I_δ множество всех $(i_0, \ldots, i_n)$ таких, что все $i_w \geqslant 0$ – целые числа и $i_0 + \ldots + i_n = \delta$. Теперь пусть

$$F = \sum_{(i_0,\ldots,i_n)\in I_\delta} F_{i_0,\ldots,i_n} X_0^{i_0} \cdot \ldots \cdot X_n^{i_n}$$

– однородный многочлен степени $\delta \leqslant D$ с произвольными коэффициентами $F_{i_0,\ldots,i_n}$ из поля k_u. Тогда соотношение

$$F(\xi_0, \ldots, \xi_n) = 0 \tag{9}$$

справедливо в том и только в том случае, если F обращается в нуль тождественно на $\mathcal{Z}(\mathfrak{P}_{U_{s+1},\ldots,U_i})$. Обозначим через J_0 множество всех $j = (j_{i+1}, \ldots, j_n, j_0)$ таких, что все $j_w \geqslant 0$ являются целыми числами и $0 \leqslant j_0 < \deg \Psi$. Тогда согласно (8), (7) равенство (9) эквивалентно

$$\sum_{j\in J_0} \left(\sum_{(i_0,\ldots,i_n)\in I_\delta} a_{j,i_0,\ldots,i_n} F_{i_0,\ldots,i_n} \right) t_{i+1}^{j_{i+1}} \cdot \ldots \cdot t_n^{j_n} \theta^{j_0} = 0, \tag{10}$$

где все $a_{j,i_0,\ldots,i_n} \in k[u]$ и наибольший общий делитель $\mathrm{G\,C\,D}_{j,i_0,\ldots,i_n}\{a_{j,i_0,\ldots,i_n}\}$ $= 1$ в $k[u]$. Далее, из установленных оценок на степени ξ_v и Ψ вытекает, что для всякого ненулевого $a_{j,i_0,\ldots,i_n} \in k[u]$ любой индекс $j_\alpha = (Dd)^{O(1)}$, $i+1 \leqslant \alpha \leqslant n$, и степени $\deg_{u_{v,w}} a_{j,i_0,\ldots,i_n} = (Dd)^{O(1)}$ для всех v, w. Поэтому существует подмножество $J_1 \subset J_0$ такое, что число элементов $\#J_1 = (Dd)^{O(n-i)}$ и, если $a_{j,i_0,\ldots,i_n} \neq 0$, то $j \in J_1$. Следовательно, рассматривая коэффициенты $F_{i_0,\ldots,i_n}$ как неизвестные, мы получаем из (10) линейную систему $\sum_{(i_0,\ldots,i_n)\in I_\delta} a_{j,i_0,\ldots,i_n} F_{i_0,\ldots,i_n} = 0$, $j \in J_1$, относительно $F_{i_0,\ldots,i_n}$ с коэффициентами $a_{j,i_0,\ldots,i_n} \in k_u$. Решая эту линейную систему, мы находим базис $y_1, \ldots, y_\gamma \in k[u, X_0, \ldots, X_n]$ над полем k_u однородной компоненты $(\mathfrak{P}_{U_{s+1},\ldots,U_i})_\delta$ степени δ идеала $\mathfrak{P}_{U_{s+1},\ldots,U_i}$. Согласно алгоритму для решения линейных систем мы получаем $\deg_{u_{v,w}} y_j = (Dd)^{O(n-i)}$ для всех v, w и $1 \leqslant j \leqslant \gamma$. Утверждение (i) доказано.

Докажем (ii). Пусть $y = y_j$ для некоторых $1 \leqslant j \leqslant \gamma$, $\delta \leqslant D$. Мы будем предполагать без ограничения общности, осуществляя при необходимости невырожденное линейное преобразование координатных функций $X_0, \ldots, X_n$ над k, что $X_i \notin \mathfrak{P}$ для всех $0 \leqslant i \leqslant n$ (после этой замены целое число N для старых координатных функций будет $(n+1)N - n$). Тогда, см. лемму 4, $\pi(y) \in S^{-1}(\mathfrak{P}_{i-1} \cap k[u, X_0, \ldots, X_n])$ и, следовательно, $y - \pi(y) \in U_i S^{-1} k[u, X_0, \ldots, X_n]$. Мы доказали, что $\deg_{u_{i,n}} y = (Dd)^{O(n-i)}$ с абсолютной константой в $O(n-i)$. Отсюда вытекает, что $X_n^N \pi(y) \in \mathfrak{P}_{U_{s+1},\ldots,U_{i-1}} \cap k[u, X_0, \ldots, X_n]$ для целого числа $N = (Dd)^{O(n-i)}$. Поэтому $X_n^N (y - \pi(y)) \in U_i k[u, X_0, \ldots, X_n]$. Таким образом, $X_n^N \mathfrak{P}_{U_{s+1},\ldots,U_i} \subset \mathfrak{P}_{U_{s+1},\ldots,U_{i-1}} + (U_i)$. Аналогично $X_j^N \mathfrak{P}_{U_{s+1},\ldots,U_i} \subset \mathfrak{P}_{U_{s+1},\ldots,U_{i-1}} + (U_i)$ для всякого $0 \leqslant j \leqslant n$.

Пусть $\delta_1 = \delta + N$. Мы построили базис $y_1, \ldots, y_\gamma$ однородной компоненты $(\mathfrak{P}_{U_{s+1},\ldots,U_i})_\delta$ над полем k_u. Аналогичным образом мы можем построить базис $y'_1, \ldots, y'_\sigma \in k[u, X_0, \ldots, X_n]$ однородной компоненты $(\mathfrak{P}_{U_{s+1},\ldots,U_{i-1}})_{\delta_1}$. Теперь для всех ρ, j можно представить

$$X_\rho^N y_j = \sum_{1\leqslant\alpha\leqslant\sigma} b_{\rho,j,\alpha} y'_\alpha, \quad b_{\rho,j,\alpha} \in k_u. \tag{11}$$

Для завершения доказательства мы используем "специализацию параметров" $u_{v,j}$. Мы оставляем читателю проверить, что описанная явная конструкция допускает "специализацию параметров", т.е., если $(l_{v,j})$ принадлежат непустому открытому в топологией Зарисского подмножеству из $\mathbb{A}^{(n-s+2)(n+1)}(\overline{k})$, то можно подставить $u_{v,j} = l_{v,j} \in k$ в (7), (8) и получить общую точку многообразия $\mathcal{Z}(\mathfrak{P}_{L_{s+1},\ldots,L_i})$ со всеми $L_v = \sum_{0\leqslant j\leqslant n} l_{v,j}X_j$. Здесь также используется лемма 3. Далее, снова для непустого открытого в топологии Зарисского подмножества можно подставить $u_{v,j} = l_{v,j}$ в $y_1, \ldots, y_\gamma$ и получить базис над полем k однородной компоненты $(\mathfrak{P}_{L_{s+1},\ldots,L_i})_\delta$ степени δ идеала $\mathfrak{P}_{L_{s+1},\ldots,L_i}$. Это следует из алгоритма для решения линейных систем. Аналогичное утверждение выполняется для базиса $y'_1, \ldots, y'_\sigma$ однородной компоненты $(\mathfrak{P}_{L_{s+1},\ldots,L_{i-1}})_{\delta_1}$ идеала $\mathfrak{P}_{L_{s+1},\ldots,L_{i-1}}$. Для всех $0 \leqslant \delta \leqslant D$ формулы (11), относящиеся к общей точке $(u_{v,i})$, также допускают "специализацию параметров". Наконец, заметим, что мы имеем естественную линейную проекцию

$$\varepsilon : \mathbb{A}^{(n-s+2)(n+1)}(\overline{k}) \to \mathbb{A}^{(n-s)(n+1)}(\overline{k}),$$
$$(L_0, L_{s+1}, \ldots, L_{n+1}) \mapsto (L_{s+1}, \ldots, L_n),$$

и для всякого открытого в топологии Зарисского подмножества $\mathcal{W}$ аффинного пространства $\mathbb{A}^{(n-s+2)(n+1)}(\overline{k})$ его образ $\varepsilon(\mathcal{W})$ является открытым относительно топологии Зарисского в $\mathbb{A}^{(n-s)(n+1)}(\overline{k})$. Так что теперь при помощи проекции ε мы получаем требуемое подмножество $\mathcal{U}'_i$. Таким образом, утверждение (ii) и вся лемма доказаны.

ЛЕММА 6 *В предыдущих обозначениях пусть* $s = \mathrm{ht}(\mathfrak{P}) = n - 1$. *Пусть* $\mathcal{U} \subset \mathbb{A}^n(\overline{k})$ *– открытое в топологии Зарисского подмножество линейных форм, соответствующее простому идеалу* $\mathfrak{P}$, *см. выше. Тогда для всякого* $L_n \in \mathcal{U}$ *характеристическая функция* $h(\mathfrak{P}_{L_n}, m) = \dim_k(A/\mathfrak{P}_{L_n})_m$ *стабильна для* $m \geqslant (n-1)d - n + 2$. *Далее, для всех* $m \geqslant (n-1)d - n + 2$ *мы имеем равенство*

$$(\mathfrak{P}_{L_n})_m = (\mathfrak{P} + (L_n))_m \tag{12}$$

однородных компонент степени m *идеалов* $\mathfrak{P}_{L_n}$ *и* $\mathfrak{P} + (L_n)$.

ДОКАЗАТЕЛЬСТВО Существуют однородные многочлены $F_1, \ldots, F_m \in k[X_0, \ldots, X_n]$ одной и той же степени d такие, что $\mathcal{Z}(\mathfrak{P}) = \mathcal{Z}(F_1, \ldots, F_m)$ в $\mathbb{P}^n(\overline{k})$ и $\mathfrak{P}$ является $\mathfrak{P}$-примарной компонентой идеала $(F_1, \ldots, F_m) \subset k[X_0, \ldots, X_n]$, ср. [2], [3]. Тогда для линейной формы $L_n \in \mathcal{U}$ идеал $\mathfrak{P} + (L_n) \supset (F_1, \ldots, F_m, L_n) = \mathfrak{P}_{L_n} \cap \mathfrak{Q}$, где $\mathfrak{Q}$ является $\mathfrak{M}$-примарным идеалом или $\mathfrak{Q} = k[X_0, \ldots, X_n]$. Поэтому, см. [8], однородные компоненты $(F_1, \ldots, F_m, L_n)_m = (\mathfrak{P}_{L_n})_m$ идеалов $(F_1, \ldots, F_m, L_n)$ и $\mathfrak{P}_{L_n}$ совпадают для $m \geqslant (n-1)d - n + 2$, и выполняется (12). Следовательно, см. [8], характеристическая функция $h(\mathfrak{P}_{L_n}, m)$ стабильна для $m \geqslant (n-1)d - n + 2$, ср. также лемма 8 ниже. Лемма доказана.

ЛЕММА 7 *Предположим, что условия леммы 5 выполняются для всех* $s + 1 \leqslant i \leqslant n - 1$ *с одним и тем же* D. *Положим* $\mathcal{U}' = \bigcap_{s+1\leqslant i\leqslant n-1} \mathcal{U}'_i$, *см. лемма 5 (ii) и*

$$D_1 = \max\{(Dd)^{c_4(n-s-1)}, sd - s\}.$$

Тогда для всякого $(L_{s+1}, \ldots, L_n) \in \mathcal{U}'$ *для всякого* $s \leqslant i \leqslant n - 1$ *характеристическая функция*

$$h(\mathfrak{P}_{L_{s+1},\ldots,L_i}, m) = \dim_k(A/\mathfrak{P}_{L_{s+1},\ldots,L_i})_m \tag{13}$$

стабильна для $m \geqslant D_1$.

ДОКАЗАТЕЛЬСТВО Пусть $(L_{s+1}, \ldots, L_n) \in \mathcal{U}'$. Заметим, что $k[X_0, \ldots, X_n]/(L_{s+1}, \ldots, L_{n-1})$ изоморфно кольцу многочленов над k от $s+2$ переменных, и $\mathcal{U}' \subset \mathcal{U}$, где $\mathcal{U}$ открытое множество из леммы 3. Применим лемму 6 к идеалу

$$\mathfrak{P}_{L_{s+1},\ldots,L_{n-1}}/(L_{s+1}, \ldots, L_{n-1}) \subset k[X_0, \ldots, X_n]/(L_{s+1}, \ldots, L_{n-1})$$

вместо $\mathfrak{P} \subset k[X_0, \ldots, X_n]$. Мы получаем, что при $i = n$ характеристическая функция (13) стабильна для $m \geqslant sd - s + 1$. Теперь (12) и точная последовательность (14) с $i = n$, см. ниже, влекут, что при $i = n - 1$ характеристическая функция (13) стабильна для $m \geqslant sd - s$. Это доказывает требуемое утверждение при $i = n - 1$.

Мы используем убывающую индукцию по i. Предположим, что эта характеристическая функция стабильна для $m \geqslant D_1$ для некоторого $s + 1 \leqslant i \leqslant n - 1$. Докажем, что она стабильна для $m \geqslant D_1$ также для $i - 1$ (вместо i). Мы имеем точную последовательность

$$\begin{aligned} &0 \to (A/\mathfrak{P}_{L_{s+1},\ldots,L_{i-1}})_{m-1} \to (A/\mathfrak{P}_{L_{s+1},\ldots,L_{i-1}})_m \to \\ &(A/(\mathfrak{P}_{L_{s+1},\ldots,L_{i-1}} + (L_i)))_m \to 0 \end{aligned} \tag{14}$$

векторных пространств, и $(A/(\mathfrak{P}_{L_{s+1},\ldots,L_{i-1}}+(L_i)))_m = (A/\mathfrak{P}_{L_{s+1},\ldots,L_i})_m$ для $m \geqslant (Dd)^{c_4(n-s-1)}$ по лемме 5. Следовательно, (13) стабильна для $m \geqslant D_1$ по индукционному предположению. Лемма доказана.

ЗАВЕРШЕНИЕ ДОКАЗАТЕЛЬСТВА ТЕОРЕМЫ 1 Положим $\mathfrak{P} = \mathfrak{P}_0$, см. (*). Следовательно, сейчас согласно (*) высота $\mathrm{ht}(\mathfrak{P}) = s = \mu + 1$, и по теореме Безу $\deg \mathfrak{P} = \deg \mathfrak{P}_0 = d_1 \leqslant d^s$ вместо $\deg \mathfrak{P} = d$. Мы имеем $s \leqslant n - 1$, поскольку $\mathrm{ht}(\mathfrak{P}^{(0)}) \leqslant n - 1$. Пусть D – наименьшее целое число такое, что условия леммы 5 выполняются для всех $s + 1 \leqslant i \leqslant n - 1$ для $\mathfrak{P} = \mathfrak{P}_0$ с d_1 вместо d. Пусть $\mathcal{U}'_i$, $s + 1 \leqslant i \leqslant n - 1$, – множества из леммы 5 (ii), и $\mathcal{U}' = \bigcap_{s+1 \leqslant i \leqslant n-1} \mathcal{U}'_i$. Применим лемму 7 с d_1 вместо d. Так что сейчас $D_1 = \max\{(Dd_1)^{c_4(n-s-1)}, sd_1 - s\}$. Для $i = s$ согласно (*) мы получаем $D_1 \geqslant d^{2^{c_2 n}}$. Поэтому для всех достаточно больших n и d число $D \geqslant d^{2^{c'n}} + 1$ для абсолютной константы $c' > 0$. Следовательно, для любого $(L_{s+1}, \ldots, L_n) \in \mathcal{U}'$ существует $s + 1 \leqslant i_0 \leqslant n - 1$ такое, что всякая система образующих простого идеала $\mathfrak{P}_{L_{s+1},\ldots,L_{i_0}}$ содержит многочлен степени по крайней мере $d^{2^{c'n}} + 1$ (целое число i_0 может зависеть от $(L_{s+1}, \ldots, L_n)$). Выберем и зафиксируем $(L_{s+1}, \ldots, L_n) \in \mathcal{U}'$. Теперь положим $\mathfrak{p} = \mathfrak{P}_{L_{s+1},\ldots,L_{i_0}}$ и $c = c'$. Следовательно, $\mathcal{Z}(\mathfrak{p})$ является определённой над k и неприводимой над $\overline{k}$ компонентой алгебраического многообразия $\mathcal{Z}(f_1, \ldots, f_{\mu+1}, L_{s+1}, \ldots, L_{i_0})$ по лемме 3. Положим $f_j = L_j$ для всех $\mu + 2 \leqslant j \leqslant i_0$, и $\nu = i_0$. Теперь определены все многочлены $f_1, \ldots, f_\nu$, и выполняется утверждение (a) теоремы. Очевидно (c) выполнено. По замечанию 1 также справедливо утверждение (b). Теорема 1 доказана.

ДОКАЗАТЕЛЬСТВО ПРЕДЛОЖЕНИЯ 1 Пусть $\mathfrak{p}$ – идеал, построенный в доказательстве теоремы 1. Напомним, что мы используем первую теорему Бертини несколько раз и получаем элементы из поля k вместо трансцендентных элементов. Теперь мы хотим избежать применения первой теоремы Бертини. Именно, заменим семейство элементов $\lambda_{v,w}$, $1 \leqslant v \leqslant \mu$, $1 \leqslant w \leqslant 3$ (напомним, что $\lambda_{v,4} = \lambda_{v,2}\lambda_{v,3}^{-1}$) семейством λ трансцендентных над k элементов. Мы будем обозначать их снова через $\lambda_{v,w}$. Обозначим через k_λ расширение поля k при помощи всех элементов из семейства λ. Так что теперь степень трансцендентности поля k_λ над k равна 3μ. Далее, заменим семейство коэффициентов $l_{i,j} \in k$, $i \in \{0, s+1, \dots, n+1\}$, $0 \leqslant j \leqslant n$ линейных форм $L_{s+1}, \dots, L_{n+1}$ семейством u трансцендентных над k_λ элементов $u_{i,j}$ со степенью трансцендентности $(n-s+2)(n+1)$ над k_λ. Обозначим через $k_{\lambda,u}$ расширение поля k_λ всеми элементами из семейства $u_{i,j}$. Так что степень трансцендентности поля $k_{\lambda,u}$ над k равна $3\mu + (n-s+2)(n+1) = O(n^2)$. Пусть k – конечное поле. После этой замены согласно конструкции из доказательства теоремы 1 мы получаем семейство многочленов $f_1, \dots, f_\nu \in k_{\lambda,u}[X_0, \dots, X_n]$ (мы используем для них те же самые обозначения) и простой идеал $\mathfrak{p}' \subset k_{\lambda,u}[X_0, \dots, X_n]$ вместо $\mathfrak{p} \subset k[X_0, \dots, X_n]$.

Обозначим через $k[\lambda, u, X_0, \dots, X_n]$ полиномиальное кольцо над k с переменными из семейств λ, u, $X_0, \dots, X_n$. Положим $\mathfrak{p}'' = \mathfrak{p}' \cap k[\lambda, u, X_0, \dots, X_n]$. Согласно описанной конструкции все $f_1, \dots, f_\nu \in k[\lambda, u, X_0, \dots, X_n]$ и все степени $\deg_{\lambda,u,X_0,\dots,X_n} f_i < d+1$.

Идеал $\mathfrak{p}''$ не является обязательно однородным относительно всех переменных. Для упрощения обозначений обозначим все переменные из семейств λ, u, $X_0, \dots, X_n$ через $Y_1, \dots, Y_m$. Обозначим через $\mathbb{A}^m(\overline{k})$ аффинное пространство с координатными функциями $Y_1, \dots, Y_m$. Поле k является совершенным, поскольку оно конечно. Поэтому $\mathcal{Z}(\mathfrak{p}'') \subset \mathbb{A}^m(\overline{k})$ является определённой над k компонентой алгебраического многообразия $\mathcal{Z}(f_1, \dots, f_\nu) \subset \mathbb{A}^m(\overline{k})$. Многообразие $\mathcal{Z}(\mathfrak{p}'') \subset \mathbb{A}^m(\overline{k})$ неприводимо над $\overline{k}$, так как многообразие $\mathcal{Z}(\mathfrak{p}') \subset \mathbb{P}^n(\overline{k_{\lambda,v}})$ является неприводимым над $\overline{k_{\lambda,v}}$ согласно условию (a) теоремы.

Пусть Y_0 – новая переменная. Гомогенизация многочлена $a \in k[Y_1, \dots, Y_m]$ есть многочлен $\overline{a} = Y_0^{\deg a} a(Y_1/Y_0, \dots, Y_m/Y_0) \in k[Y_0, \dots, Y_m]$. Пусть $\mathfrak{p}''' \subset k[Y_0, \dots, Y_m]$ – однородный простой идеал, порождённый всеми элементами $\overline{a}$, $a \in \mathfrak{p}''$. Пусть $\mathbb{P}^m(\overline{k})$ – проективное пространство с однородными координатными функциями $Y_0, \dots, Y_m$. Проективные алгебраические многообразия $\mathcal{Z}(\mathfrak{p}''') \subset \mathbb{P}^m(\overline{k})$ и $\mathcal{Z}(\overline{f_1}, \dots, \overline{f_\nu}) \subset \mathbb{P}^m(\overline{k})$ являются замыканиями относительно топологии Зарисского аффинных алгебраических многообразий $\mathcal{Z}(\mathfrak{p}'')$ и $\mathcal{Z}(f_1, \dots, f_\nu)$ соответственно. Следовательно, $\mathcal{Z}(\mathfrak{p}''')$ является определённой над k и неприводимой над $\overline{k}$ компонентой алгебраического многообразия $\mathcal{Z}(\overline{f_1}, \dots, \overline{f_\nu})$. Согласно (*) $\mathfrak{p}$ является примарной компонентой идеала $f_1, \dots, f_\nu$, и высота $\mathrm{ht}(\mathfrak{p}) = \nu$. Поэтому $\mathfrak{p}'''$ является примарной компонентой идеала $(\overline{f_1}, \dots, \overline{f_\nu})$, и высота $\mathrm{ht}(\mathfrak{p}''') = \nu$. Таким образом, над конечным полем k выполняется утверждение (a) теоремы 1 для m, $\overline{f_1}, \dots, \overline{f_\nu}$ и $\mathfrak{p}'''$ вместо n, $f_1, \dots, f_\nu$ и $\mathfrak{p}$ соответственно. Очевидно все степени $\deg_{Y_0,\dots,Y_m} \overline{f_i} < d+1$. Для доказательства новых версий утверждений (b) и (c), см. формулировку предложения, мы будем также рассматривать $\overline{f_1}, \dots, \overline{f_\nu}$ и $\mathfrak{p}'''$.

Утверждение (c) теоремы 1 выполняется для $\mathfrak{p}'$ над полем $k_{\lambda,u}$ (вместо $\mathfrak{p}$ над k). Любая система образующих идеала $\mathfrak{p}''$ является системой образующих идеала $\mathfrak{p}'$. Следовательно, для любой системы образующих $a_1, \dots, a_m$

идеала $\mathfrak{p}''$ максимальная степень

$$\max_{1\leqslant i\leqslant m} \deg_{Y_1,\dots,Y_m} a_i \geqslant \max_{1\leqslant i\leqslant m} \deg_{X_0,\dots,X_n} a_i \geqslant \deg d^{2^{cn}}$$

Поэтому для всякой системы образующих $a'_1,\dots,a'_{m'}$ идеала $\mathfrak{p}'''$

$$\max_{1\leqslant i\leqslant m'} \deg_{Y_0,\dots,Y_m} a'_i \geqslant d^{2^{cn}}.$$

Отсюда вытекает утверждение (c) новой версии теоремы, см. формулировку предложения, поскольку $n > n_0$, $d > d_0$ – произвольные, $m = O(n^2)$, все $\deg \overline{f_i} < d+1$, см. замечание 3. Более того, очевидно здесь в (c) можно заменить $d^{2^{c\sqrt{n}}}$ на $d^{2^{c\sqrt{n}}}+1$ (и получить слегка более сильное утверждение). Тогда новая версия утверждения (b) следует из замечания 1. Предложение доказано.

ЗАМЕЧАНИЕ 5 *Пусть k – конечное поле и t – трансцендентный элемент над полем k. Пусть $\mathfrak{p} \subset k(t)[X_0,\dots,X_n]$ – идеал, построенный в доказательстве теоремы 1 над бесконечным полем $k(t)$. Согласно доказательству предложения 1, чтобы доказать теорему 1 для конечного поля k, достаточно установить следующее. Применяя первую теорему Бертини, можно выбрать все коэффициенты $\lambda_{v,w} \in k[t]$ многочленов f_{v+1}, и коэффициенты $l_{i,j} \in k[t]$ линейных форм L_i со степенями $\deg_t \lambda_{v,w}$, $\deg_t l_{i,j}$, ограниченными сверху $d^{n^{O(1)}}$.*

ЗАМЕЧАНИЕ 6 *Аналогичная проблема имеется также для бесконечного поля k. Пусть $\lambda_{v,w} \in k$ и $l_{i,j} \in k$, см. доказательство теоремы 1, соответствуют идеалу $\mathfrak{p}$. Требуется доказать, что длины записи элементов $\lambda_{v,w} \in k$ и $l_{i,j} \in k$ ограничены сверху $d^{n^{O(1)}}$.*

Одной из трудностей, относящихся к утверждениям из замечания 5 и замечания 6, является оценка размера нормализации алгебраического многообразия. Я не смог найти явную оценку нормализации в литературе. Однако мы видим, что её можно дать. Мы надеемся вернуться к этому вопросу в одной из следующих статей. Кажется, что других принципиальных трудностей нет, ср. приложение из [4].

4 Верхние оценки

Мы можем дать также верхние оценки для стабилизации характеристической функции однородного простого идеала и для системы образующих этого идеала. Пусть $\mathfrak{P}$ – простой идеал из раздела 3, но сейчас мы предполагаем, что высота $\mathrm{ht}(\mathfrak{P}) = s$, $0 \leqslant s \leqslant n$. Так что степень $\deg \mathfrak{P} = d$, и идеал $\overline{k} \otimes_k \mathfrak{P} \subset \overline{k} \otimes_k A$ является радикальным.

ЛЕММА 8 *Пусть $\mathfrak{Q} \subset A$ – однородный идеал такой, что идеал $\overline{k} \otimes_k \mathfrak{Q} \subset \overline{k} \otimes_k A$ радикален, размерность многообразия нулей $\dim \mathcal{Z}(\mathfrak{q}) = 0$ в $\mathbb{P}^n(\overline{k})$ и степень $\deg \mathfrak{Q} = d$. Тогда характеристическая функция $h(\mathfrak{Q}, m)$ стабильна для всех $m \geqslant d-1$. В частности, это верно для однородного простого идеала $\mathfrak{P} \subset A$ (вместо $\mathfrak{Q}$) с $s = \mathrm{ht}(\mathfrak{P}) = n$ такого, что $\mathcal{Z}(\mathfrak{P}) \subset \mathbb{P}^n(\overline{k})$ определено над k.*

ДОКАЗАТЕЛЬСТВО Обозначим для краткости $\overline{A} = \overline{k} \otimes_k A$. Мы имеем $h(\mathfrak{Q}, m) = h(\overline{k} \otimes_k \mathfrak{Q}, m)$. Пусть $\overline{k} \otimes_k \mathfrak{Q} = \cap_{1 \leqslant j \leqslant d} \mathfrak{m}_j$ – редуцированное примарное разложение идеала $\overline{k} \otimes_k \mathfrak{Q}$. Следовательно, все $\mathfrak{m}_j \subset \overline{A}$, $1 \leqslant j \leqslant d$, являются однородными простыми идеалами степени один и высоты n. Поэтому достаточно доказать, что характеристическая функция $h(\cap_{1 \leqslant j \leqslant \delta} \mathfrak{m}_j, m)$ стабильна для $m \geqslant \delta - 1$. Мы используем индукцию по δ. База $\delta = 1$ очевидна. Имеем точную последовательность однородных компонент степени m, индуцированную точной последовательностью гомоморфизмов градуированных $\overline{A}$-модулей,

$$\begin{aligned} &0 \to (\overline{A}/(\cap_{1 \leqslant j \leqslant \delta} \mathfrak{m}_j))_m \to (\overline{A}/(\cap_{1 \leqslant j \leqslant \delta-1} \mathfrak{m}_j))_m \times (\overline{A}/(\mathfrak{m}_\delta))_m \to \\ &(\overline{A}/(\mathfrak{m}_\delta + \cap_{1 \leqslant j \leqslant \delta-1} \mathfrak{m}_j))_m \to 0. \end{aligned} \qquad (15)$$

Существует однородный многочлен $\varphi \in \cap_{1 \leqslant j \leqslant \delta-1} \mathfrak{m}_j \setminus \mathfrak{m}_\delta$ такой, что $\deg \varphi = \delta - 1$. Следовательно, $(\overline{A}/(\mathfrak{m}_\delta + \cap_{1 \leqslant j \leqslant \delta-1} \mathfrak{m}_j))_m = \{0\}$ для $m \geqslant \delta - 1$. Поэтому согласно индукционному предположению и (15) характеристическая функция $h(\cap_{1 \leqslant j \leqslant \delta} \mathfrak{m}_j, m)$ стабильна для $m \geqslant \delta - 1$. Лемма доказана.

ЛЕММА 9 *В обозначениях из начала раздела предположим, что* $1 \leqslant s \leqslant n - 1$. *Тогда характеристическая функция* $h(\mathfrak{P}, m) = \dim_k (A/\mathfrak{P})_m$ *стабильна для всех целых чисел* $m \geqslant (sd)^{(c_5(n-s))^{n-s-1}}$ *для абсолютной константы* $c_5 > 0$. *Следовательно, по замечанию 1 идеал* $\mathfrak{P}$ *имеет систему образующих, состоящую из однородных многочленов степеней самое большее* $1 + (sd)^{(c_5(n-s))^{n-s-1}}$. *Наконец, лемма 8 теперь влечёт, что для всех* $0 \leqslant s \leqslant n$ *характеристическая функция* $h(\mathfrak{P}, m)$ *стабильна для* $m \geqslant (sd)^{(c_5(n-s+1))^{n-s}}$, *и идеал* $\mathfrak{P}$ *имеет систему образующих, состоящую из однородных многочленов степени самое большее* $1 + (sd)^{(c_5(n-s+1))^{n-s}}$.

ДОКАЗАТЕЛЬСТВО Мы будем предполагать без ограничения общности, что $1 < s < n$. Следовательно, $sd \geqslant 2$. Покажем, что для всех $(L_{s+1}, \ldots, L_n)$ из непустого открытого в топологии Зарисского подмножества в $\mathbb{A}^{(n-s)(n+1)}(\overline{k})$ для всякого $s \leqslant i \leqslant n-1$ характеристическая функция (13) стабильна для $m \geqslant (sd)^{(c_5(n-s))^{n-i-1}}$, и, следовательно, по замечанию 1 идеал $\mathfrak{P}_{L_{s+1}, \ldots, L_i}$ имеет систему однородных образующих степеней самое большее $1 + (sd)^{(c_5(n-s))^{n-i-1}}$ для абсолютной константы $c_5 > 0$. Действительно, это верно для $i = n - 1$ согласно лемме 6. Мы используем убывающую индукцию по i. Предположим, что наше утверждение доказано для некоторого $s + 1 \leqslant i \leqslant n - 1$. Докажем, что оно справедливо также для $i - 1$ (вместо i). Мы имеем точную последовательность (14) векторных пространств. Поэтому по индукционному предположению и лемме 5 с $D = (sd)^{(c_5(n-s))^{n-i-1}}$ для всех $(L_{s+1}, \ldots, L_n) \in \bigcap_{i \leqslant j \leqslant n-1} \mathcal{U}'_j$ (множество $\mathcal{U}'_i$ определено на этом индукционном шаге в лемме 5 (ii), и аналогично множества $\mathcal{U}'_j$, $i + 1 \leqslant j \leqslant n - 1$, определены на предыдущих шагах индукции) справедливо равенство $(A/(\mathfrak{P}_{L_{s+1}, \ldots, L_{i-1}} + (L_i)))_m = (A/\mathfrak{P}_{L_{s+1}, \ldots, L_i})_m$ для

$$m \geqslant (sd)^{(c_5(n-s))^{n-i}} \geqslant ((sd)^{(c_5(n-s))^{n-i-1}} d)^{c_4(n-i)}$$

для подходящей константы c_5. Следовательно, характеристическая функция (13) с $i-1$ вместо i стабильна для $m \geqslant (sd)^{(c_5(n-s))^{n-i}}$ по индукционному предположению. Требуемое утверждение доказано. Лемма доказана.

ЛЕММА 10 *В обозначениях из начала раздела существует абсолютная константа* $c_6 > 0$ *такая, что простой идеал* $\mathfrak{P}$ *имеет систему образующих* $q_1, \ldots, q_w \in k[X_0, \ldots, X_n]$ *со степенями* $\deg q_i \leqslant d^{2^{c_6 n}}$ *для всех* $1 \leqslant i \leqslant w$.

ДОКАЗАТЕЛЬСТВО Мы можем предполагать без ограничения общности, что $1 < s < n$, см. лемму 8, и $d > 1$. Существуют однородные многочлены $F_1, \ldots, F_m \in k[X_0, \ldots, X_n]$ одной и той же степени d такие, что $\mathcal{Z}(\mathfrak{P}) = \mathcal{Z}(F_1, \ldots, F_m)$ в $\mathbb{P}^n(\overline{k})$ и $\mathfrak{P}$ является $\mathfrak{P}$-примарной компонентой идеала $(F_1, \ldots, F_m) \subset k[X_0, \ldots, X_n]$, ср. [2], [3]. Пусть $\widetilde{F}_1, \ldots, \widetilde{F}_s$ – линейные комбинации многочленов $F_1, \ldots, F_m$ с коэффициентами из $\overline{k}$ в общем положении. Тогда по первой теореме Бертини, см. [12], [1], ср. [4], идеал кольца $\overline{k}[X_0, \ldots, X_n]$

$$(\widetilde{F}_1, \ldots, \widetilde{F}_s) = (\overline{k} \otimes_k \mathfrak{P}) \cap \widetilde{\mathfrak{P}},$$

где $\widetilde{\mathfrak{P}}$ является однородным простым идеалом кольца $\overline{k}[X_0, \ldots, X_n]$ с высотой $\mathrm{ht}(\widetilde{\mathfrak{P}}) = s$, степенью $\deg(\widetilde{\mathfrak{P}}) = d^s - d > 0$ и такой, что $\widetilde{\mathfrak{P}}$ не является примарной компонентой идеала $\overline{k} \otimes_k \mathfrak{P}$. Пусть $\overline{k} \otimes_k \mathfrak{P} = \bigcap_{j \in J} \mathfrak{p}_j$ – редуцированное примарное разложение радикального идеала $\overline{k} \otimes_k \mathfrak{P}$. Существует многочлен $F \in \widetilde{\mathfrak{P}} \setminus \bigcup_{j \in J} \mathfrak{p}_j$ такой, что $\deg F \leqslant d^s - d$. Теперь $\overline{k} \otimes_k \mathfrak{P} = \{z \in \overline{k}[X_0, \ldots, X_n] \,:\, zF \in (F_1, \ldots, F_m)\}$. Рассмотрим линейное уравнение

$$ZF = \sum_{1 \leqslant i \leqslant s} Z_i F_i \tag{16}$$

над кольцом полиномов $\overline{k}[X_0, \ldots, X_n]$. Согласно [6], [10] подмодуль в $(\overline{k} \otimes_k A)^{s+1}$ решений $(Z, Z_1, \ldots, Z_s)$ уравнения (16) имеет систему образующих $z_i, z_{i,1}, \ldots, z_{i,s}$, $i \in I$, состоящую из многочленов из $\overline{k} \otimes_k A$ степеней $\deg z_i$, $\deg z_{i,j}$, ограниченных сверху $d^{2^{c_6 n}}$ для подходящей универсальной константы $c_6 > 0$. Теперь $z_i \in \overline{k} \otimes_k A$, $i \in I$, является системой образующих идеала $\overline{k} \otimes_k \mathfrak{P}$ требуемых степеней. Поскольку многообразие $\mathcal{Z}(\mathfrak{P})$ определено над k, существует также система образующих $q_1, \ldots, q_w \in k[X_0, \ldots, X_n]$ идеала $\mathfrak{P}$ со степенями $\deg q_i \leqslant d^{2^{c_6 n}}$ для всех $1 \leqslant i \leqslant w$. Лемма доказана.

СЛЕДСТВИЕ 1 *В обозначениях из начала раздела существует абсолютная константа* $c_7 > 0$ *такая, что характеристическая функция* $h(\mathfrak{P}, m)$ *простого идеала* $\mathfrak{P}$ *стабильна для* $m \geqslant d^{2^{c_7 n}}$.

ДОКАЗАТЕЛЬСТВО Действительно, согласно лемме 8 и [8] мы можем предполагать без ограничения общности, что $\mathrm{ht}(\mathfrak{P}) = s \leqslant n - 1$. Условия леммы 5 с основным полем k_u (вместо k) выполнены для всех $s + 1 \leqslant i \leqslant n - 1$ для $D = d^{2^{c_6 n}} + 1$. Пусть $(L_{s+1}, \ldots, L_n) \in \mathcal{U}' = \bigcap_{s+1 \leqslant i \leqslant n-1} \mathcal{U}'_i$, см. лемма 5 (ii). Теперь требуемое утверждение вытекает из леммы 7. Следствие доказано.

Список литературы

[1] **Бальдассарри М.:** *"Алгебраические многообразия"*, Издательство иностранной литературы, М., 1961.

[2] **Чистов А. Л.:** *"Алгоритм полиномиальной сложности для разложения многочленов на неприводимые множители и нахождение компонент многообразия в субэкспоненциальное время"*, Зап. научн. семинаров ЛОМИ АН, т. 137 (1984), с. 124–188.

[3] **Чистов А. Л.:** *"Эффективная конструкция локальных параметров неприводимых компонент алгебраического многообразия"*, Труды Санкт–Петербургского математического общества, т. 7 (1999), с. 230–266.

[4] **Chistov A. L.:** *"A deterministic polynomial–time algorithm for the first Bertini theorem"*, Preprint of St.Petersburg Mathematical Society (2004), http://www.mathsoc.spb.ru/preprint/

[5] **Dubé T. W.:** *"The structure of polynomial ideals and Gröbner bases"*, SIAM J. Comput. 19 (1990), 750–775.

[6] **Hermann G.:** *Die Frage der endlich vielen Schritte in der Theorie der Polynomideale*, Math. Ann. **95**, (1926), 736-788.

[7] **Hilbert D.:** *"Über die Teorie der algebraischen Formen"*, Math. Ann. 36 (1890), 473–534.

[8] **Lazard D.:** *"Algèbre linéaire sur* $k[x_1, \ldots, x_n]$ *et élimination"*, Bull. Soc. Math. France 105 (1977) p. 165–190.

[9] **Mayr E.W., Meyer A.R.:** *"The complexity of the word problems for commutative semigroups and polynomial ideals"*, Adv. Math. 46 (1982), 305-329.

[10] **Seidenberg A.:** *"Constructions in algebra"*, Trans. Amer. Math. Soc. 97 (1974), 273–313.

[11] **Yap Chee K.:** *"A new lower bound construction for commutative Thue systems, with applications"*, J. Symb. Comput., 12 (1991), 1–28.

[12] **Zariski O.:** *"Pencils on an algebraic variety and a new proof of a theorem of Bertini"*, Trans. Amer. Math. Soc., v. 50 (1941) p. 48–70.