Лекция 5: Теория исключения

5.1 Теорема об исключении и продолжении

Определение 5.1: Пусть $I < f_1, \dots, f_s > \subset k[x_1, \dots, x_n]$ — некоторый идеал. Тогда *ℓ-пм идеалом исключения* для I называется

$$I_\ell := I \cap k[x_{\ell+1}, \dots, x_n].$$

(I_ℓ является идеалом в кольце $k[x_{\ell+1}, \dots, x_n]$).

Теорема 5.1: (об исключении) Пусть $I < f_1, \dots, f_s > \subset k[x_1, \dots, x_n]$ — идеал, набор G — его базис Грёбнера относительно $lex: x_1 > x_2 > \dots > x_n$. Тогда для всех $\ell \in \{0, \dots, n-1\}$ пересечение

$$G_\ell := G \cap k[x_{\ell+1}, \dots, x_n]$$

является базисом Грёбнера ℓ-го идеала исключения I_ℓ.

Доказательство: Пусть $l \in \{0, \dots, n-1\}$, по определению набор G_l состоит из многочленов из идеала I, лежащих в $k[x_{l+1}, \dots, x_n]$, поэтому $G_l \subset I_l$. Тогда, если выполняется равенство

$$< lt(I_\ell) > = < lt(G_\ell) >,$$

то набор G_l является базисом Грёбнера идеала I_l. Включение $< lt(G_l) > \subset < lt(I_l) >$ очевидно. Нужно показать обратное: для этого достаточно, чтобы для многочлена $f \in I_\ell$ его старший член $lt f$ делился на некоторый $lt\, g$, где $g \in G_\ell$

Если $f \in I_\ell$, то он лежит и в I. По определению базиса Грёбнера найдётся $g \in G$, т.ч. $lt f$ делится на $lt g$. При этом многочлен $f \in k[x_{l+1}, \dots, x_n]$, а значит и $lt g \in k[x_{l+1}, \dots, x_n]$. Поскольку мы используем лексикографический мономиальный порядок с $x_1 > x_2 > \dots > x_n$, то все остальные мономы g тоже не зависят от $x_1, \dots, x_l$, иначе они были бы старше чем $lt(g)$. Заключаем, что $g \in k[x_{l+1}, \dots, x_n]$, а следовательно и $g \in G_\ell$. ◀

Пример 5.1: Рассмотрим идеал $I = < x^2 + y + z - 1, x + y^2 + z - 1, x + y + z^2 - 1 > \subset \mathbb{C}[x,y,z]$, его базис Грёбнера относительно $lex: x > y > z$ состоит

$$g_1 = x + y + z^2 - 1,\ g_2 = y^2 - y - z^2 + z,\ g_3 = 2yz^2 + z^4 - z^2,\ g_4 = z^6 - 4z^4 + 4z^3 - z^2$$

Согласно теореме 5.1

$$I_1 = I \cap \mathbb{C}[y,z] = < y^2 - y - z^2 + z,\ 2yz^2 + z^4 - z^2,\ z^6 - 4z^4 + 4z^3 - z^2 >,$$
$$I_2 = I \cap \mathbb{C}[z] = < z^6 - 4z^4 + 4z^3 - z^2 >.$$

Любой многочлен, получающийся исключением x и y, является кратным g_4. ◀

Напомним, что для идеала $I = \langle f_1, \dots, f_s \rangle$ его аффинное многообразие

$$\mathbb{V}(I) := \{ (a_1, \dots, a_n) \in k^n : f(a_1, \dots, a_n) = 0 \text{ для всех } f \in I \}$$

состоит из всевозможных решений системы $f_1 = \dots = f_s = 0$.
Пусть I_ℓ – ℓ-ый идеал исключения для I. Тогда точку $(a_{\ell+1}, \dots, a_n) \in \mathbb{V}(I_\ell)$ будем называть частичным решением указанной системы. Если мы хотим решить систему, то нужно уметь продолжать частичное решение до полного

Пример 5.2: Рассмотрим идеал $I = \langle xy-1, xz-1 \rangle \subset \mathbb{C}[x,y,z]$ и систему

$$\begin{cases} xy = 1 \\ xz = 1 \end{cases}$$

Нетрудно найти, что $I_1 = \langle y-z \rangle$. Следовательно, множество частичных решений состоит из точек (a,a), где $a \in \mathbb{C}$, они продолжаются до полных решений $(\frac{1}{a}, a, a)$, если $a \neq 0$.

Теорема 5.2 (об продолжении) Пусть $I = \langle f_1, \dots, f_s \rangle \subset \mathbb{C}[x_1, \dots, x_s]$, для всех $1 \le i \le s$ образующие идеала записываются в виде

$$f_i = g_i(x_2, \dots, x_n) x_1^{N_i} + \text{члены, в которых степень } x_1 < N_i,$$

где $N_i \ge 0$ и $g_i \in \mathbb{C}[x_2, \dots, x_n]$ ненулевой. Тогда, если частное решение $(a_2, \dots, a_n) \in \mathbb{V}(I_1)$, т.ч. $(a_2, \dots, a_n) \notin \mathbb{V}(g_1, \dots, g_s)$, то существует $a_1 \in \mathbb{C}$, для которого $(a_1, a_2, \dots, a_n) \in \mathbb{V}(I)$.

Следствие: Пусть $I = \langle f_1, \dots, f_s \rangle \subset \mathbb{C}[x_1, \dots, x_s]$, для некоторого $i \in \{1, \dots, s\}$

$$f_i = c\, x^N + \text{члены, в которых степень } x_1 < N_i,$$

где $c \in \mathbb{C} - \{0\}$ и $N > 0$. Тогда, если $(a_2, \dots, a_n) \in \mathbb{V}(I_1)$, то существует $a_1 \in \mathbb{C}$, т.ч. $(a_1, a_2, \dots, a_n) \in \mathbb{V}(I_1)$.

5.2 Геометрия исключения

Рассмотрим отображение проекции

$$\pi_\ell : \mathbb{C}^n \to \mathbb{C}^{n-\ell}, \quad \pi_\ell(a_1, \dots, a_n) = (a_{\ell+1}, \dots, a_n).$$

Лемма 5.1: Пусть $I_l = \langle f_1, \dots, f_s \rangle \cap \mathbb{C}[x_{l+1}, \dots, x_n]$ — l-ый идеал исключения идеала $I = \langle f_1, \dots, f_s \rangle$, а $V = \mathbb{V}(f_1, \dots, f_s)$. Тогда

$$\pi_l(V) \subset \mathbb{V}(I_l) \subset \mathbb{C}^{n-l}.$$

Доказательство: Выберем произвольный $f \in I_l$. В силу $I_l \subset I$ этот многочлен зануляется в $(a_1, \dots, a_n) \in V$. Более того, он зависит только от $x_{l+1}, \dots, x_n$, поэтому

$$f(a_1, \dots, a_n) = f(\pi(a_1, \dots, a_n)) = 0,$$

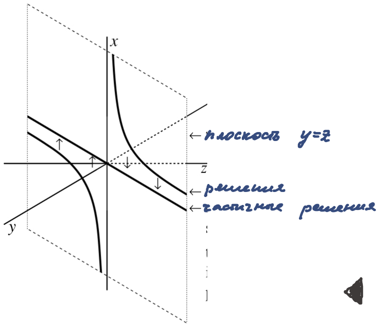
т.е. f зануляется во всех точках образа $\pi_l(V)$ ◀

Таким образом,

$$\pi_l(V) = \{(a_{l+1}, \dots, a_n) \in \mathbb{V}(I_l) : \exists a_1, \dots, a_l \in \mathbb{C} \text{ со свойством } (a_1, \dots, a_n) \in V\},$$

это множество всех частных решений, которые продолжаются до полных.

Пример 5.2 (продолжение) В этом случае $\mathbb{V}(I_1)$ — это прямая $y = z$ на плоскости $\mathbb{C}^2_{y,z}$. $\pi_1(V) = \{(a, a) \in \mathbb{C}^2 : a \neq 0\}$ не является алгебраическим многообразием (это полу-алгебраическое множество)



◀

Теорема 5.2': В условиях теоремы 5.2 имеется равенство

$$\mathbb{V}(I_1) = \pi_1(V) \cup (\mathbb{V}(g_1, \dots, g_s) \cap \mathbb{V}(I_1)).$$

Пример 5.3: Рассмотрим систему

$$\begin{cases} (y-z)x^2 + xy = 1 \\ (y-z)x^2 + xz = 1 \end{cases}$$

Можно показать, что $\langle xy - 1, xz - 1 \rangle = \langle (y-z)x^2 + x - 1, (y-z)x^2 + xz - 1 \rangle =: I$. Идеал исключения $I_1 = \langle y - z \rangle$ совпадает с $\langle g_1, g_2 \rangle = \langle y - z \rangle$, поэтому теорема о продолжении не даёт никакой информации о $\pi_1(V)$ в этом случае. ◀

Теорема 5.3: (о замыкании) Пусть $I = \langle f_1, \dots, f_s \rangle \subset \mathbb{C}[x_1, \dots, x_n]$, $V = \mathbb{V}(I) \subset \mathbb{C}^n$. Тогда

1) $\mathbb{V}(I_\ell)$ – это наименьшее аффинное многообразие, содержащее $\pi_\ell(V) \subset \mathbb{C}^{n-\ell}$.

2) Если $V \neq \varnothing$, то существует аффинное многообразие $W \subsetneqq \mathbb{V}(I_\ell)$, т.к. $\mathbb{V}(I_\ell) - W \subset \pi_\ell(V)$.

Доказательство: Пункт 1) будет доказан позднее, когда мы познакомимся с теоремой Гильберта о нулях

Пункт 2) докажем для случая $\ell = 1$. Рассмотрим разложение

$$\mathbb{V}(I_1) = \pi_1(V) \cup (\mathbb{V}(g_1, \dots, g_s) \cap \mathbb{V}(I_1))$$

из теоремы 5.2'. Обозначим через W аффинное многообразие $\mathbb{V}(g_1, \dots, g_s) \cap \mathbb{V}(I_1)$ (см. предложение 1.2) Из разложения следует, что $\mathbb{V}(I_1) - W \subset \pi_1(V)$. Если $W \neq \mathbb{V}(I_1)$, то утверждение доказано.

Если $W = \mathbb{V}(I_1)$, то можно показать, $V = \mathbb{V}(f_1, \dots, f_s, g_1, \dots, g_s)$. Включение $\mathbb{V}(f_1, \dots, f_s, g_1, \dots, g_s) \subset \mathbb{V}(f_1, \dots, f_s) = V$. Для доказательства обратного включения рассмотрим т. $(a_1, \dots, a_n) \in V$. Каждый f_i-ый зануляется в этой точке, а многочлены g_i-ые зануляются в $(a_2, \dots, a_n)$, т.к. $\pi_1(V) \subset \mathbb{V}(I_1) = W$. Следовательно, $\mathbb{V}(f_1, \dots, f_s) = \mathbb{V}(f_1, \dots, f_s, g_1, \dots, g_s)$.

Итак $\mathbb{V}(I) = \mathbb{V}(\tilde{I})$, где $\tilde{I} = \langle f_1, \dots, f_s, g_1, \dots, g_s \rangle$. Идеалы I и $\tilde{I}$ при этом могут не совпадать, соответствующие идеалы исключения I_1 и $\tilde{I}_1$ тоже могут не совпадать. Однако согласно пункту 1) $\mathbb{V}(I_1)$ и $\mathbb{V}(\tilde{I}_1)$ являются наименьшими многообразиями, содержащими $\pi_1(V)$. Поэтому $\mathbb{V}(I_1) = \mathbb{V}(\tilde{I}_1)$.

Запишем образующие идеала I в виде

$$f_i = g_i(x_2, \dots, x_n) x_1^{N_i} + \text{слагаемые со степенью } x_1 < N_i, \quad i = \overline{1, s}$$

где $N_i \geq 0$ и $g_i \in \mathbb{C}[x_2, \dots, x_n]$ ненулевые. Введём многочлены

$$\tilde{f}_i = f_i - g_i x_1^{N_i},$$

для $i \in \{1, s\}$ многочлен $\tilde{f}_i$ либо нулевой, либо имеет степень по x_1 строго меньше чем f_i. Заметим, что

$$\tilde{I} = \langle \tilde{f}_1, \dots, \tilde{f}_s, g_1, \dots, g_s \rangle.$$

Применим теорему 5.2' к многообразию $V = \mathbb{V}(\tilde{f}_1, \dots, \tilde{f}_s, g_1, \dots, g_s)$:

$$\mathbb{V}(I_1) = \mathbb{V}(\tilde{I}_1) = \pi_1(V) \cup \tilde{W},$$

где $\tilde{W}$ состоит всех частичных решений, зануляющих старшие коэффициенты многочлен $\tilde{f}_1, \dots, \tilde{f}_s, g_1, \dots, g_s$.

В общем случае может оказаться, что $\tilde{W} = \mathbb{V}(I_1)$. Тогда мы снова должны повторить описанное выше рассуждение. Если на какой-то шаге мы получим аффинное многообразие меньшее чем $\mathbb{V}(I_1)$, то теорема доказана.

Пусть на каждом шаге мы всегда получаем $\mathbb{V}(I_1)$. Заметим, что на каждой итерации степени образующих по x_1 уменьшаются (или остаются нулевыми). Поэтому в какой-то момент все образующие будут иметь степень 0 по x_1. Это означает, что V задаётся нулями многочленов из $\mathbb{C}[x_2, \dots, x_n]$. Тогда для частного решения $(a_2, \dots, a_n)$ точка $(a_1, a_2, \dots, a_n)$ будет лежать в V для всех $a_1 \in \mathbb{C}$. Таким образом каждое частное решение продолжаемо, т.е. $\pi_1(V) = \mathbb{V}(I_1)$. Это означает, что $\tilde{W} = \emptyset$, т.к. $V \neq \emptyset$. ◀

Пример 5.3: (продолжение) Напомним, что для идеала

$$I = \langle (y-z)x^2 + xy - 1,\ (y-z)x^2 + xz - 1 \rangle$$

идеал $I_1 = \langle y - z \rangle$ и $g_1 = g_2 = y - z$. Значит $W = \mathbb{V}(I_1)$ в этом случае. Тогда $\tilde{I} = \langle (y-z)x^2 + xy - 1,\ (y-z)x^2 + xz - 1,\ y - z \rangle = \langle xy - 1,\ xz - 1,\ y - z \rangle$. По теореме о продолжении $\tilde{W}$ состоит из точек зануляющих одновременно y и z, т.е. $\tilde{W} = \{(0,0)\} \subsetneq W$. ◀

Итак, теорема о замыкании утверждает, что $\pi_l(V)$ заполняет $\mathbb{V}(I_l)$ за исключением точек, лежащих в некотором многообразии меньшем чем $\mathbb{V}(I_l)$. К сожалению, эти точки могут не заполнять указанное многообразие.

Точное описание $\pi_l(V)$ таково: существуют аффинные многообразия $Z_i \subset W_i \subset \mathbb{C}^{n-l}$, где $i = 1, \dots, m$, т.ч.

$$\pi_l(V) = \bigcup_{i=1}^{m} (W_i - Z_i).$$

Следствие: Пусть $V = \mathbb{V}(f_1,\dots,f_s) \subset \mathbb{C}^n$, для некоторого $i \in \{1,\dots,s\}$

$$f_i = c x_1^N + \begin{matrix}\text{слагаемое с } x_1\\ \text{в степени} < N\end{matrix},$$

где $c \in \mathbb{C} - \{0\}$ и $N > 0$. Тогда $\pi_1(V) = \mathbb{V}(I_1)$.

5.3 Переход от параметризации к явному заданию

Рассмотрим полиномиальное отображение

$$(5.1) \qquad F: k^m \to k^n, \quad F(t_1,\dots,t_m) = (f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)),$$

где $f_i \in k[t_1,\dots,t_m]$, $i = 1,\dots,n$. Образ $F(k^m)$ может и не быть аффинным многообразием. Наша задача состоит в том, чтобы найти наименьшее аффинное многообразие, содержащее $F(k^m)$.

Пусть $V = \mathbb{V}(x_1 - f_1, \dots, x_n - f_n) \subset k^{n+m}$, его точки могут быть записаны в виде

$$(t_1,\dots,t_m, f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)),$$

т.е. V — это график отображения F. Рассмотрим два отображения

$$i: k^m \to k^{n+m},$$
$$i(t_1,\dots,t_m) = (t_1,\dots,t_m, f_1(t_1,\dots,t_m),\dots,f_n(t_1,\dots,t_m)),$$

и

$$\pi_m: k^{n+m} \to k^n,$$
$$\pi_m(t_1,\dots,t_m, x_1,\dots,x_n) = (x_1,\dots,x_n).$$

Тогда у нас есть следующая коммутативная диаграмма

$$\begin{tikzcd} & k^{n+m} \arrow[dr, "\pi_m"] & \\ k^m \arrow[ur, "i"] \arrow[rr, "F"] & & k^n \end{tikzcd}$$

Отображение $F = \pi_m \circ i$. Как мы отметили выше $i(k^m) = V$, поэтому

$$F(k^m) = \pi_m(i(k^m)) = \pi_m(V).$$

Теорема 5.4 Пусть k - бесконечное поле, отображение $F: k^m \to k^n$ имеет вид (5.1). Тогда, если $I = \langle x_1 - f_1, \dots, x_n - f_n\rangle \subset k[t_1,\dots,t_m, x_1,\dots,x_n]$ и $I_m := I \cap k[x_1,\dots,x_n]$ — его m-ый идеал исключения, то многообразие $\mathbb{V}(I_m)$ — наименьшее аффинное многообразие в k^n, содержащее образ $F(k^m)$.

Доказательство: Пусть $V = \mathbb{V}(I) \subset k^{n+m}$, как мы отметили $F(k^m) = \pi_m(V)$. Если $k = \mathbb{C}$, то теореме 5.3 о замыкании $\mathbb{V}(I_m)$ — это наименьшее аффинное многообразие, содержащее $\pi_m(V) = F(\mathbb{C}^m)$.

Предположим, что k - подполе поля $\mathbb{C}$. Оно содержит $\mathbb{Z}$ (и даже $\mathbb{Q}$), поэтому бесконечно. Будем использовать обозначение $\mathbb{V}_k(I_m)$ для многообразия в k^n, аналогично для $\mathbb{V}_{\mathbb{C}}(I_m) \subset \mathbb{C}^n$. Заметим, что переход к большему полю не изменяет идеал I_m. Итак, требуется доказать, что многообразие $\mathbb{V}_k(I_m)$ наименьшее в k^n содержащее $F(k^m)$.

Мы знаем, что $F(k^m) = \pi_m(V_k)$ лежит в $\mathbb{V}_k(I_m)$ по лемме 5.1. Рассмотрим произвольное многообразие $Z_k := \mathbb{V}_k(g_1, \dots, g_s) \subset k^n$, т.ч. $F(k^m) \subset Z_k$. Нужно показать включение $\mathbb{V}_k(I_m) \subset Z_k$. Поскольку $g_i = 0$ на Z_k, то $g_i = 0$ и на $F(k^m)$. Иными словами, композиция $g_i \circ F$ тождественно равна нулю на k^m. Очевидно, что $g_i \circ F \in k[t_1, \dots, t_m]$, поэтому в силу бесконечности поля k по предложению 1.1 $g_i \circ F$ является нулевым полиномом (для всех $i = 1, \dots, s$).

Таким образом, все $g_i \circ F$ зануляются на $\mathbb{C}^m$, а значит g_i-ые зануляются на $F(\mathbb{C}^m)$. Это означает, что $F(\mathbb{C}^m) \subset Z_{\mathbb{C}} := \mathbb{V}_{\mathbb{C}}(g_1, \dots, g_s)$. Поскольку теорема верна для поля $\mathbb{C}$, то $\mathbb{V}_{\mathbb{C}}(I_m) \subset Z_{\mathbb{C}} \subset \mathbb{C}^n$. Откуда сразу следует, что и $\mathbb{V}_k(I_m) \subset Z_k$.

В случае, когда поле k не содержится в $\mathbb{C}$, мы можем рассмотреть алгебраически замкнутое поле K, т.ч. $k \subset K$. Поскольку теорема 5.3 остаётся справедливой для любого алгебраически замкнутого поля, указанные выше рассуждения с заменой поля $\mathbb{C}$ на K доказывают теорему для такого k. ◀

Пример 5.4: Рассмотрим в $\mathbb{R}^3$ скрученную кубику, она задаётся параметризацией

$$x = t, \quad y = t^2, \quad z = t^3.$$

Очевидно, что касательная поверхность в $\mathbb{R}^3$ к скрученной кубике задаётся параметризацией

$$x = t + u, \quad y = t^2 + 2tu, \quad z = t^3 + 3t^2u.$$

Рассмотрим идеал $I = \langle x-t-u,\ y-t^2-2tu,\ z-t^3-3t^2u \rangle \subset \mathbb{R}[t,u,x,y,z]$. Его базис Грёбнера относительно lex: $t>u>x>y>z$ (см. пример кода для SINGULAR на сайте)

$$g_1 = t+u-x,$$
$$g_2 = u^2-x^2+y,$$
$$g_3 = 2ux^2-2uy-2x^3+3xy-z,$$
$$g_4 = uxy-uz-x^2y-xz+2y^2,$$
$$g_5 = 2uxz-2uy^2+2x^2z-xy^2-yz,$$
$$g_6 = 2uy^3-2uz^2-4x^2yz+xy^3-2xz^2+5y^2z,$$
$$g_7 = 4x^3z-3x^2y^2-6xyz+4y^3+z^2.$$

Следовательно, $I_2 = I \cap \mathbb{R}[x,y,z] = \langle 4x^3z-3x^2y^2-6xyz+4y^3+z^2 \rangle$. Многообразие $\mathbb{V}(g_7)$ является наименьшим содержащим касательную поверхность к скрученной кубике.

Если хотим понять заполняет ли эта поверхность всё многообразие $\mathbb{V}(g_7)$, то нужно выяснить, всякое ли частное решение $(x,y,z) \in \mathbb{V}(g_7) = \mathbb{V}(I_2)$ поднимается до $(t,u,x,y,z) \in \mathbb{V}(I)$.

Пусть $(x,y,z) \in \mathbb{V}(I_2)$. Идеал $I_2 \subset I_1$, где первый идеал исключения имеет вид

$$I_1 = \langle g_2, \dots, g_7 \rangle.$$

Поскольку g_2 имеет постоянный ненулевой коэффициент при u^2, то по следствию из теоремы 5.2 решение $(x,y,z) \in \mathbb{V}(I_2)$ продолжается до $(u,x,y,z) \in \mathbb{V}(I_1) \subset \mathbb{C}^4$. Аналогично, в силу того, что g_1 имеет постоянный ненулевой коэффициент при старшей степени по t, это решение может быть продолжено до т. $(t,u,x,y,z) \in \mathbb{V}(I) \subset \mathbb{C}^5$. Таким образом, мы показали, что $\mathbb{V}(g_7)$ совпадает с касательной поверхностью в $\mathbb{C}^3$.

Пусть точка $(x,y,z) \in \mathbb{R}^3$ зануляет многочлен g_7. Как видно из системы

$$g_1 = \dots = g_6 = g_7 = 0$$

параметр u зависит от x,y,z рационально над $\mathbb{Q}$, следовательно, $u \in \mathbb{R}$. В свою очередь параметр $t = x-u$, поэтому он тоже принадлежит $\mathbb{R}$. Мы показали, что касательная поверхность к скрученной кубике в $\mathbb{R}^3$ есть аффинное многообразие, определённое уравнением

$$4x^3z-3x^2y^2-6xyz+4y^3+z^2 = 0.$$

Рассмотрим теперь случай рациональной параметризации.

Теорема 5.5: Пусть k – бесконечное поле, отображение $F: k^m - W \to k^n$, т.ч.

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right),$$

где все $f_i, g_i \in k[t_1, \ldots, t_m]$, а $W = \mathbb{V}(g_1 \cdot g_2 \cdot \ldots \cdot g_n) \subset k^m$. Тогда, если идеал $J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - g_1 \cdot \ldots \cdot g_n \cdot y \rangle \subset k[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$, а $J_{m+1} = J \cap k[x_1, \ldots, x_n]$ его $(m+1)$-ый идеал исключения, то $\mathbb{V}(J_{m+1})$ – наименьшее аффинное многообразие, содержащее $F(k^m - W)$.