Белорусский государственный университет

Полиномиальные идеалы и многообразия

Садовский А.П.

Минск, 2004

Оглавление.

ВВЕДЕНИЕ.

Многие практические и научные задачи приводят к сложным полиномиальным вычислениям, которые в значительной степени удается осуществить благодаря появлению мощных компьютеров. Для решения различных вычислительных задач, связанных с полиномиальными выражениями, весьма удобны базисы Грёбнера. В книге для полиномиальных идеалов вводятся базисы Грёбнера и подробно описываются их свойства. Излагается алгоритм деления в кольце полиномов от многих переменных, являющийся главным инструментом при построении базисов Грёбнера. Доказываются знаменитые теоремы Гильберта о базисе и о нулях, приводится теория исключения и описываются различные применения базисов Грёбнера, в частности, для решения систем полиномиальных уравнений. Решение системы полиномиальных уравнений представляется в виде аффинного многообразия полиномиального идеала. Наряду с аффинными многообразиями рассматриваются и проективные многообразия.

Книга представляет собой курс лекций по алгебре полиномов, читаемый автором в течение ряда лет на механико-математическом факультете Белгосуниверситета.

При изложении материала лекций в основном использована книга Д. Кокса, Дж. Литтла, Д. О'Ши [1]. При написании п. 1.9 и п. 4.3 был использован материал книги [2]. В пп. 3.2 и 3.6 использовалась книга [3].

Для чтения этой книги почти никаких предварительных сведений не требуется. Все необходимые понятия из теории групп и колец можно найти в [5], [8] – [10]. Вопросы теории полиномиальных идеалов, которые рассматриваются в книге, излагаются в [5] – [6], [8] – [10]. Вопросы теории исключения рассматриваются в [7].

Автор весьма признателен Ю.Л. Бондарь за помощь при подготовке рукописи к печати.

ГЛАВА 1. БАЗИСЫ ГРЁБНЕРА

1.1. АФФИННЫЕ МНОГООБРАЗИЯ И ИДЕАЛЫ

Определение 1. *Мономом* от переменных $x_1, x_2,\ldots,x_n$ называется произведение вида $x_1^{\alpha_1}x_2^{\alpha_2}\ldots.x_n^{\alpha_n}$, где $\alpha_1, \alpha_2,\ldots,\alpha_n$ – неотрицательные целые числа.

Будем использовать следующие обозначения для мономов. Пусть $\alpha = (\alpha_1, \alpha_2,\ldots,\alpha_n)$ – набор неотрицательных целых чисел, $x = (x_1, x_2,\ldots,x_n)$. Положим $x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\ldots.x_n^{\alpha_n}$. Если $\alpha = (0, 0,\ldots,0)$, то $x^\alpha = 1$.

Определение 2. *Полной степенью монома* x^α называется число $|\alpha| = \sum_{k=1}^{n}\alpha_k$.

Определение 3. *Полиномом* f от переменных $x_1, x_2,\ldots,x_n$ с коэффициентами из поля k называется конечная линейная комбинация мономов (с коэффициентами из k), т.е. $f = \sum_{\alpha} a_\alpha x^\alpha$, $a_\alpha \in k$, где суммирование проводится по конечному множеству наборов $\alpha = (\alpha_1, \alpha_2,\ldots,\alpha_n)$. Множество всех полиномов с коэффициентами из поля k обозначается $k[x_1, x_2,\ldots,x_n]$.

Множество $k[x_1, x_2,\ldots,x_n]$ образует *кольцо полиномов* (*полиномиальное кольцо*).

Определение 4. Пусть $f = \sum_{\alpha} a_\alpha x^\alpha \in k[x_1, x_2,\ldots,x_n]$.

1) a_α называется *коэффициентом монома* x^α.

2) Если $a_\alpha \neq 0$, то $a_\alpha x^\alpha$ называется *членом полинома* f.

3) *Полной степенью полинома* f называется число $\deg(f) = \max(|\alpha|: a_\alpha \neq 0)$.

Мы говорим, что полином f делит полином g, если $\exists\ h \in k[x_1, x_2,\ldots,x_n]$ такой, что $g = fh$.

Определение 5. Пусть дано поле k и $n \in \mathbf{N}$. Тогда *n-мерным аффинным пространством* над k называется множество $k^n = \{(a_1,\ldots,a_n): a_1,\ldots,a_n \in k\}$.

Полином $f = \sum_{\alpha} a_\alpha x^\alpha \in k[x_1, x_2,\ldots,x_n]$ задает функцию $f : k^n \to k$, определенную следующим образом. Пусть $(a_1,\ldots,a_n) \in k^n$. В формуле, опреде-

ляющей f, заменим x_i на a_i. Так как $a_\alpha \in k$, то эта операция дает элемент $f(a_1,\ldots,a_n) \in k$.

Очевидно, что если $f = 0$, т.е. все коэффициенты $a_\alpha = 0$, то $f : k^n \to k$ является нулевой функцией, т.е. для $\forall\ (a_1,\ldots,a_n)\quad f(a_1,\ldots,a_n) = 0$.

В случае бесконечного поля k имеет место

Предложение 1. *Пусть k – бесконечное поле и $f \in k[x_1, x_2,\ldots,x_n]$. Тогда $f = 0$ тогда и только тогда, когда $f : k^n \to k$ является нулевой функцией.*

Доказательство. Если $f = 0$, то, очевидно, нулевой полином определяет нулевую функцию. Докажем обратное утверждение. Нам надо доказать, что если $\forall\ (a_1,\ldots,a_n)\quad f(a_1,\ldots,a_n) = 0$, то $f = 0$. Доказательство проведем методом математической индукции. Пусть $n = 1$. Если $f \in k[x]$ и $\forall\ a \in k\quad f(a) = 0$, то f имеет бесконечное множество корней, так как поле k является бесконечным. Следовательно, $f = 0$, ибо в противном случае ненулевой полином f степени m имел бы не более m различных корней.

Пусть обратное утверждение справедливо для $n - 1$ и пусть $f \in k[x_1, x_2,\ldots,x_n]$ – полином, равный нулю во всех точках из k^n. Объединяя члены полинома f по степеням переменной x_n, запишем f в виде

$$f = \sum_{i=1}^{N} g_i(x_1,\ldots,x_{n-1})x_n^i, \text{ где } g_i \in k[x_1,\ldots,x_{n-1}].$$

Докажем, что $g_i = 0$ в $k[x_1,\ldots,x_{n-1}]$, откуда уже будет следовать, что $f = 0$ в $k[x_1,\ldots,x_n]$.

Возьмем любой элемент $(a_1,\ldots,a_{n-1}) \in k^{n-1}$ и зафиксируем его. Тогда получаем полином $f(a_1,\ldots,a_{n-1}, x_n) \in k[x_n]$ от одной переменной. Для любого $a_n \in k\quad f(a_1,\ldots,a_{n-1}, a_n) = 0$. Следовательно, $f(a_1,\ldots,a_{n-1}, x_n) = 0 \in k[x_n]$, а значит, $g_i(a_1,\ldots,a_{n-1}) = 0$, $i = \overline{1,N}$. Так как выбиралось любое фиксированное $(a_1,\ldots,a_{n-1}) \in k^{n-1}$, то для каждого $(a_1,\ldots,a_{n-1})\quad g_i(a_1,\ldots,a_{n-1}) = 0$, $i = \overline{1,N}$. Согласно индуктивному предположению $g_i = 0 \in k[x_1,\ldots,x_{n-1}]$, где $i = \overline{1,N}$. Таким образом, $f = 0 \in k[x_1,\ldots,x_n]$. □

Следствие 1. *Пусть k – бесконечное поле и $f, g \in k[x_1,\ldots,x_n]$. Тогда $f = g$ в $k[x_1,\ldots,x_n]$ тогда и только тогда, когда функции $f : k^n \to k$, $g : k^n \to k$ равны.*

Доказательство. Если $f = g$, то тогда очевидно функции $f : k^n \to k$, $g : k^n \to k$ равны между собой.

Пусть $f, g \in k[x_1,\ldots,x_n]$ задают одну и ту же функцию на k^n. Тогда для любого $(a_1,\ldots,a_n) \in k^n\quad h = f - g$ обращается в нуль, а значит, на основа-

нии предположения 1 $f - g = 0$ в $k[x_1,\ldots,x_n]$, т.е. $f = g$. Следствие доказано.

Определение 6. Поле k называется *алгебраически замкнутым*, если любой непостоянный полином из $k[x]$ имеет корень в k.

Из основной теоремы алгебры вытекает, что поле **C** алгебраически замкнуто.

Определение 7. Пусть k – некоторое поле, а $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,s}$. Положим $\mathbf{V}(f_1,\ldots,f_s) = \{(a_1,\ldots,a_n) \in k^n : f_i(a_1,\ldots,a_n) = 0,\ i = \overline{1,s}\}$. Множество $V = \mathbf{V}(f_1,\ldots,f_s)$ называется *аффинным многообразием*, определенным полиномами f_i, $i = \overline{1,s}$.

Аффинное многообразие $\mathbf{V}(f_1,\ldots,f_s) \subset k^n$ – множество решений системы уравнений $f_1(x_1,\ldots,x_n) = 0,\ldots,f_s(x_1,\ldots,x_n) = 0$.

Решения линейной системы

$$\begin{gathered} a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m, \end{gathered}$$

образуют аффинное многообразие в k^n, которое называется *линейным многообразием*.

Отметим, что аффинное многообразие может быть пустым множеством.

Теорема 1. *Если V, $W \subset k^n$ – аффинные многообразия, то $V \cup W$, $V \cap W$ также являются аффинными многообразиями.*

Доказательство. Пусть $V = \mathbf{V}(f_1,\ldots,f_s)$, $W = \mathbf{V}(g_1,\ldots,g_t)$. Покажем, что

$$V \cap W = \mathbf{V}(f_1,\ldots,f_s, g_1,\ldots,g_t), \tag{1}$$

$$V \cup W = \mathbf{V}(f_i g_j,\ i = \overline{1,s},\ j = \overline{1,t}). \tag{2}$$

Пусть $(a_1,\ldots,a_n) \in V \cap W$. Тогда $(a_1,\ldots,a_n) \in V$, $(a_1,\ldots,a_n) \in W$, а значит, f_i, $i = \overline{1,s}$, g_j, $j = \overline{1,t}$, обращаются в ноль в этой точке, т.е. $(a_1,\ldots,a_n) \in \mathbf{V}(f_1,\ldots,f_s, g_1,\ldots,g_t)$. Следовательно, $V \cap W \subset \mathbf{V}(f_1,\ldots,f_s, g_1,\ldots,g_t)$. Наоборот, если $(a_1,\ldots,a_n) \in \mathbf{V}(f_1,\ldots,f_s, g_1,\ldots,g_t)$, то в точке $(a_1,\ldots,a_n)$ f_i, $i = \overline{1,s}$, g_j, $j = \overline{1,t}$, обращаются в нуль. Значит, $(a_1,\ldots,a_n) \in V$, $(a_1,\ldots,a_n) \in W$, т.е. $\mathbf{V}(f_1,\ldots,f_s, g_1,\ldots,g_t) \subset V \cap W$. Формула (1) доказана. Докажем формулу (2). Пусть $(a_1,\ldots,a_n) \in V$. Тогда все f_i равны нулю в этой точке, а значит, все функции $f_i g_j$ равны нулю в $(a_1,\ldots,a_n)$. Следовательно, $V \subset \mathbf{V}(f_i g_j)$.

Аналогично $W \subset \mathbf{V}(f_i g_j)$. Отсюда $V \cup W \subset \mathbf{V}(f_i g_j)$. Наоборот, пусть $(a_1,\ldots,a_n) \in \mathbf{V}(f_i g_j)$. Если $(a_1,\ldots,a_n) \in V$, то $\mathbf{V}(f_i g_j) \subset V$. Отсюда $\mathbf{V}(f_i g_j) \subset V \cup W$; в этом случае формула (2) доказана. Если $(a_1,\ldots,a_n) \notin V$, то $\exists\, i_0$ такое, что $f_{i_0}(a_1,\ldots,a_n) \neq 0$. Так как $(a_1,\ldots,a_n) \in \mathbf{V}(f_i g_j)$, то для любого j $f_{i_0} g_j$ обращаются в нуль в $(a_1,\ldots,a_n)$. Следовательно, все g_i равны нулю в этой точке. Значит, $(a_1,\ldots,a_n) \in W$, а потому $\mathbf{V}(f_i g_j) \subset W$. Отсюда $\mathbf{V}(f_i g_j) \subset V \cup W$. □

Из этой теоремы с использованием метода математической индукции вытекает, что конечные объединения и пересечения аффинных многообразий являются аффинными многообразиями.

Теорема 2. *Любое конечное подмножество в k^n является аффинным многообразием.*

Доказательство. Пусть рассматриваемое множество состоит из точки $(a_1,\ldots,a_n) \in k^n$. Тогда $(a_1,\ldots,a_n) = \mathbf{V}(x_1 - a_1,\ldots,x_n - a_n)$. Дальнейшее очевидно.

Рассмотрим теперь задачу описания точек аффинного многообразия $\mathbf{V}(f_1,\ldots,f_s)$, т.е. задачу описания всех решений системы полиномиальных уравнений $f_1 = 0,\ldots,f_s = 0$.

Определение 7. Пусть k – некоторое поле. *Рациональной функцией* от переменных $t_1,\ldots,t_m$ с коэффициентами из поля k называется отношение $\frac{f}{g}$ двух полиномов $f, g \in k[t_1,\ldots,t_m]$, где g не является нулевым полиномом. Две рациональные функции $\frac{f}{g}$ и $\frac{h}{k}$ называются *равными*, если $kf = gh$ в $k[t_1,\ldots,t_m]$. Множество всех рациональных функций от переменных $t_1,\ldots,t_m$ с коэффициентами из поля k обозначается $k(t_1,\ldots,t_m)$.

Множество $k(t_1,\ldots,t_m)$образует *поле рациональных функций* от переменных $t_1,\ldots,t_m$ с коэффициентами из поля k.

Определение 8. *Рациональной параметризацией* (или *рациональным параметрическим представлением*) многообразия $V = \mathbf{V}(f_1,\ldots,f_s) \subset k^n$ называется набор из n рациональных функций $r_i \in k(t_1,\ldots,t_m)$, $i = \overline{1,n}$ такой, что точки с координатами $x_1 = r_1(t_1,\ldots,t_m),\ldots,x_n = r_n(t_1,\ldots,t_m)$ принадлежат V. При этом предполагается, что V представляет наименьшее многообразие, содержащее эти точки. Если r_i, $i = \overline{1,n}$ – полиномы, то параметризация многообразия V называется *полиномиальной*.

Отметим, что первоначальный набор уравнений $f_1 = 0,\ldots,f_s = 0$, который определяет многообразие V, называется его *неявным представлением*.

Определение 9. Подмножество $I \subset k[x_1,\ldots,x_n]$ называется *идеалом*, если выполнены следующие условия:

1) $0 \in I$,
2) если $f, g \in I$, то $f + g \in I$,
3) если $f \in I$, и $h \in k[x_1,\ldots,x_n]$, то $f \cdot h \in I$.

Определение 10. Пусть $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,s}$. Положим $< f_1,\ldots,f_s > = \{\sum_{i=1}^{s} h_i f_i : h_i \in k[x_1,\ldots,x_n],\ i = \overline{1,s}\}$.

Теорема 3. *Пусть $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,s}$. Тогда множество $< f_1,\ldots,f_s >$ является идеалом в $k[x_1,\ldots,x_n]$. Это множество называется идеалом, порожденным полиномами f_i, $i = \overline{1,s}$, а полиномы f_i, $i = \overline{1,s}$, называются образующими этого идеала или его порождающими элементами.*

Доказательство. $0 \in < f_1,\ldots,f_s >$, ибо $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Пусть теперь $f = \sum_{i=1}^{s} p_i f_i$, $g = \sum_{i=1}^{s} q_i f_i$, где $p_i, q_i \in k[x_1,\ldots,x_n]$ и $h \in k[x_1,\ldots,x_n]$. Тогда $f + g = \sum_{i=1}^{s} (p_i + q_i) f_i \in I$, $hf = \sum_{i=1}^{s} (hp_i) f_i \in I$. □

Идеал $< f_1,\ldots,f_s >$ имеет замечательную интерпретацию на языке полиномиальных уравнений. Пусть $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,s}$. Рассмотрим систему уравнений $f_1 = 0,\ldots,f_s = 0$. Из этой системы уравнений можно вывести другие уравнения с помощью алгебраических преобразований. Например, $h_1f_1 + \ldots + h_sf_s = 0$. Это уравнение – следствие уравнений первоначальной системы. Левая часть этого уравнения принадлежит идеалу $< f_1,\ldots,f_s >$, т.е. идеал можно рассматривать как множество всех полиномиальных следствий системы $f_1 = 0,\ldots,f_s = 0$.

Определение 10. Идеал I называется *конечно порожденным*, если существуют полиномы $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,s}$ такие, что $I = < f_1,\ldots,f_s >$. При этом множество полиномов f_i, $i = \overline{1,s}$, называется *базисом идеала I*.

Теорема 4. *Пусть* f_i, $i = \overline{1,s}$, g_j, $j = \overline{1,t}$ *– базисы одного и того же идеала в* $k[x_1,\ldots,x_n]$, *т.е.* $< f_1,\ldots,f_s > = < g_1,\ldots,g_t >$. *Тогда* $\mathbf{V}(f_1,\ldots,f_s) = \mathbf{V}(g_1,\ldots,g_t)$.

Доказательство. Пусть $(a_1,\ldots,a_n) \in \mathbf{V}(f_1,\ldots,f_s)$. Тогда $g_j = \sum_{i=1}^{s} h_{ij} f_i$, $j = \overline{1,t}$, где $h_{ij} \in k[x_1,\ldots,x_n]$. Следовательно, $g_j(a_1,\ldots,a_n) = 0$, $j = \overline{1,t}$, т.е. $(a_1,\ldots,a_n) \in \mathbf{V}(g_1,\ldots,g_t)$. Аналогично, если $(a_1,\ldots,a_n) \in \mathbf{V}(g_1,\ldots,g_t)$, то $(a_1,\ldots,a_n) \in \mathbf{V}(f_1,\ldots,f_s)$. □

Определение 11. Пусть $V \subset k^n$ – аффинное многообразие. Положим $\mathbf{I}(V) = \{f \in k[x_1,\ldots,x_n] : \forall\ (a_1,\ldots,a_n) \in V \quad f(a_1,\ldots,a_n) = 0\}$.

Теорема 5. *Пусть* $V \subset k^n$ *– аффинное многообразие. Тогда* $\mathbf{I}(V)$ *– идеал. Идеал* $\mathbf{I}(V)$ *называется идеалом многообразия* V.

Доказательство. Ясно, что $0 \in \mathbf{I}(V)$, ибо нулевой полином равен нулю на k^n и в частности на V. Пусть $f, g \in \mathbf{I}(V)$, $h \in k[x_1,\ldots,x_n]$. Для любого $(a_1,\ldots,a_n) \in V$ имеем $f(a_1,\ldots,a_n) + g(a_1,\ldots,a_n) = 0 + 0 = 0$, $h(a_1,\ldots,a_n)f(a_1,\ldots,a_n) = h(a_1,\ldots,a_n)\cdot 0 = 0$, т.е. $f + g \in \mathbf{I}(V)$, $hf \in \mathbf{I}(V)$. □

Пусть $V = k^n$. Тогда $\mathbf{I}(k^n) = \{0\}$, если поле k бесконечно, ибо полином, равный нулю на k^n, является нулевым.

Теорема 6. *Пусть* $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,s}$. *Тогда* $< f_1,\ldots,f_s > \subset \mathbf{I}(\mathbf{V}(f_1,\ldots,f_s))$. *Эти два идеала не всегда совпадают.*

Доказательство. Пусть $f \in < f_1,\ldots,f_s >$. Имеем $f = \sum_{i=1}^{s} h_i f_i$, где $h_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,s}$. Так как f_i, $i = \overline{1,s}$ равны нулю на $\mathbf{V}(f_1,\ldots,f_s)$, то и f равен нулю на $\mathbf{V}(f_1,\ldots,f_s)$, т.е. $f \in \mathbf{I}(\mathbf{V}(f_1,\ldots,f_s))$. Покажем, что $< x^2, y^2 > \subset \mathbf{I}(\mathbf{V}(x^2, y^2))$ не является равенством. Действительно, $\mathbf{V}(x^2, y^2) = \{(0,0)\}$, $x \in \mathbf{I}(\mathbf{V}(x^2, y^2))$, но $x \notin < x^2, y^2 >$, так как равенство $x = h_1(x, y)x^2 + h_2(x, y)y^2$ невозможно.

Теорема 7. *Пусть* V, W *– аффинные многообразия в* k^n. *Тогда*

1) $V \subset W$ *тогда и только тогда, когда* $\mathbf{I}(V) \supset \mathbf{I}(W)$,

2) $V = W$ *тогда и только тогда, когда* $\mathbf{I}(V) = \mathbf{I}(W)$.

Доказательство. Докажем 1). Пусть $V \subset W$. Тогда любой полином, равный нулю на W, будет равен нулю и на V, т.е. $\mathbf{I}(W) \subset \mathbf{I}(V)$. Пусть теперь наоборот $\mathbf{I}(W) \subset \mathbf{I}(V)$. Допустим, что $W = \mathbf{V}(g_1,\ldots,g_t)$, где $g_j \in k[x_1,\ldots,x_n]$, $j = \overline{1,t}$. Тогда $g_j \in \mathbf{I}(W) \subset \mathbf{I}(V)$, а поэтому g_j равны нулю и на многообразии V. Так как W – множество всех общих нулей полиномов g_j, $j = \overline{1,t}$, а g_j равны нулю на V, то $V \subset W$.

Теперь докажем 2). Пусть $V = W$. Тогда на основании 1) $\mathbf{I}(V) \subset \mathbf{I}(W)$ и $\mathbf{I}(V) \supset \mathbf{I}(W)$, т.е. $\mathbf{I}(V) = \mathbf{I}(W)$. Аналогично и обратное. □

1.2. ПОЛИНОМЫ ОТ ОДНОЙ ПЕРЕМЕННОЙ

Определение 1. Пусть $f \in k[x]$ – ненулевой полином вида $f = a_0x^m + a_1x^{m-1} + \ldots + a_m$, где $a_i \in k$, $a_0 \neq 0$ (т.е. $\deg(f) = m$). Тогда a_0x^m называется *старшим членом полинома* f и обозначается $\mathrm{LT}(f) = a_0x^m$.

Заметим, что если $f, g \in k[x]$ – ненулевые полиномы, то $\deg(f) \leq \deg(g)$ тогда и только тогда, когда $\mathrm{LT}(f)$ делит $\mathrm{LT}(g)$.

Теорема 1 (алгоритм деления). *Пусть $g \in k[x]$ – ненулевой полином. Тогда любой полином $f \in k[x]$ может быть записан в виде $f = qg + r$, где $q, r \in k[x]$ и либо $r = 0$, либо $\deg(r) < \deg(g)$. При этом q, r определены однозначно, и имеется алгоритм для их вычисления.*

Доказательство. Возьмем любой полином $f \in k[x]$. Тогда $f = q_0g + r_0$, где $q_0 = 0$, $r_0 = f$. Если $\deg(r_0) < \deg(g)$ или $r_0 = 0$, то тогда требуемое представление для f получено. Пусть $\deg(r_0) = \deg(g)$. Тогда $f = q_1g + r_1$, где $q_1 = q_0 + \dfrac{\mathrm{LT}(r_0)}{\mathrm{LT}(g)}$, $r_1 = r_0 - \dfrac{\mathrm{LT}(r_0)}{\mathrm{LT}(g)}g$. Покажем, что $\deg(r_1) < \deg(r_0)$ или $r_1 = 0$. Действительно, пусть $r_0 = a_0x^m + \ldots + a_m$, $\mathrm{LT}(r_0) = a_0x^m$, $g = b_0x^k + \ldots + b_k$, $\mathrm{LT}(g) = b_0x^k$, где $m \geq k$. Тогда $r_1 = (a_0x^m + \ldots + a_m) - \dfrac{a_0}{b_0}x^{m-k}(b_0x^k + \ldots + b_k)$, т.е. $\deg(r_1) < \deg(r_0)$ или $r_1 = 0$. Если $\deg(r_1) < \deg(g)$ или $r_1 = 0$, то требуемое представление для f найдено. В случае же $\deg(r_1) \geq \deg(g)$ $f = q_2g + r_2$, где $q_2 = q_1 + \dfrac{\mathrm{LT}(r_1)}{\mathrm{LT}(g)}$, $r_2 = r_1 - \dfrac{\mathrm{LT}(r_1)}{\mathrm{LT}(g)}g$. Ясно, что $\deg(r_2) < \deg(r_1)$ или $r_2 = 0$. Если $\deg(r_2) < \deg(g)$ или $r_2 = 0$, то нужное представление для f найдено. В противном случае этот процесс будет продолжаться, и на n-м шаге $f = q_ng + r_n$, где $q_n = q_{n-1} + \dfrac{\mathrm{LT}(r_{n-1})}{\mathrm{LT}(g)}$, $r_n = r_{n-1} - \dfrac{\mathrm{LT}(r_{n-1})}{\mathrm{LT}(g)}g$, $\deg(r_n) < \deg(r_{n-1})$ или $r_n = 0$. Так как степень полинома f конечна, то существует n, для которого $\deg(r_n) < \deg(g)$ или $r_n = 0$. В этом случае $f = qg + r$, где $q = q_n$, $r = r_n$, $\deg(r) < \deg(g)$ или $r = 0$, т.е. требуемое представление для f найдено. Таким образом, доказано существование алгоритма для вычисления q, r, где q – частное, r – остаток, полученные от деления f на g. Указанный алгоритм называется *алгоритмом деления*.

Докажем, что q и r определяются единственным образом. Предположим, что $f = qg + r = q'g + r'$, где $\deg(r) < \deg(g)$, $\deg(r') < \deg(g)$ либо оба r, r' или один из них равен нулю. Если $r \neq r'$, то $\deg(r - r') < \deg(g)$. Имеем $(q - q')g = r' - r$, а значит, $q - q' \neq 0$. Следовательно, $\deg(r' - r) = \deg((q - q')g) = \deg(q - q') + \deg(g)$. Получили противоречие. Значит, $r = r'$, а тогда ввиду $g \neq 0$ $q = q'$. □

Следствие 1. *Пусть $f \in k[x]$ – ненулевой полином. Тогда он имеет в k не более чем $\deg(f)$ корней.*

Доказательство. Воспользуемся методом математической индукции относительно $m = \deg(f)$. Если $m = 0$, то $f = \text{const} \neq 0$, корней нет, утверждение доказано. Пусть теперь утверждение выполняется для всех полиномов степени $m - 1$ и пусть f имеет степень m. Если f не имеет корней в k, то утверждение доказано. Пусть теперь $a \in k$ – корень f. Поделим f на $x - a$. На основании теоремы 1 $f = q(x - a) + r$, где $r \in k$, так как $x - a$ имеет степень 1. Положим в этом равенстве $x = a$. Имеем $0 = f(a) = q(a)(a - a) + r = r$, т.е. $f = q(x - a)$. Отсюда следует, что степень полинома q равна $m - 1$. Покажем, что любой корень f, отличный от a, является корнем полинома q. Действительно, если $b \neq a$ – корень полинома f, то $0 = f(b) = q(b)(b - a)$. Отсюда следует, что $q(b) = 0$, так как k – поле. Согласно индуктивному предположению q имеет не более $m - 1$ корней, значит, f имеет не более m корней. Следствие доказано.

Теорема 2. *Пусть k – поле. Тогда каждый идеал в $k[x]$ может быть представлен в виде $< f >$, где $f \in k[x]$. При этом f определен однозначно с точностью до умножения на ненулевую константу из k.*

Доказательство. Пусть $I \subset k[x]$ – некоторый идеал. Если $I = \{0\}$, то $I = < 0 >$ и утверждение доказано. Пусть $I \neq \{0\}$ и пусть $f \in I$ – ненулевой полином минимальной степени в множестве полиномов, содержащихся в I. Докажем, что $I = < f >$. $< f > \subset I$, так как I – идеал. Возьмем любой полином $g \in I$. Тогда на основании теоремы 1 $g = qf + r$, где $\deg(r) < \deg(f)$ или $r = 0$. Так как I – идеал, то $qf \in I$; следовательно, $r = g - qf \in I$. Если $r \neq 0$, то $\deg(r) < \deg(f)$, что противоречит выбору f. Следовательно, $r = 0$, т.е. $g = qf \in < f >$. Значит, $I = < f >$.

Докажем единственность. Пусть $I = < f > = < g >$. Так как $f \in < g >$, то $f = hg$, где $h \in k[x]$. Значит, $\deg(f) = \deg(h) + \deg(g)$, т.е. $\deg(f) \geq \deg(g)$. Аналогично, имеем $\deg(g) \geq \deg(f)$. Отсюда $\deg(h) = \deg(f) - \deg(g) = 0$, т.е. h – ненулевая константа. □

Определение 2. Идеал $I \subset k[x_1,\ldots,x_n]$, порожденный одним элементом $f \in k[x_1,\ldots,x_n]$, т.е. $I = < f >$ называется *главным идеалом*.

Из теоремы 2 следует, что все идеалы в $k[x]$ являются главными, т.е. $k[x]$ является областью главных идеалов.

Определение 3. *Наибольшим общим делителем полиномов* $f, g \in k[x]$ называется полином $h \in k[x]$ такой, что

1) h делит и f, и g;

2) если ненулевой полином $p \in k[x]$ делит и f, и g, то p делит h.

Наибольший общий делитель полиномов f и g будем обозначать GCD(f, g).

Теорема 3. *Пусть* $f, g \in k[x]$. *Тогда*

1) $GCD(f, g)$ *существует и единственен с точностью до умножения на ненулевую константу из* k;

2) идеал $< f, g > = < GCD(f, g) >$;

3) *существует алгоритм для вычисления* $GCD(f, g)$.

Доказательство. Рассмотрим идеал $< f, g > \subset k[x]$. Так как идеал в $k[x]$ является главным, то существует $h \in k[x]$ такой, что $< f, g > = < h >$. Таким образом, первый пункт определения 3 выполнен. Возьмем теперь любой полином $p \in k[x]$, который делит и f, и g. Это означает, что $f = Cp$, $g = Dp$, где $C, D \in k[x]$. Так как $h \in < f, g >$, то существуют $A, B \in k[x]$, такие, что $h = Af + Bg$. Значит, $h = Acp + BDp = (AC + BD)p$, т.е. p делит h. Следовательно, h = GCD(f, g). Итак, доказано существование GCD(f, g) и пункт 2) теоремы. Докажем единственность. Пусть h' – другой наибольший общий делитель полиномов f, g. Тогда из определения 2 следует, что h и h' делят друг друга, т.е. h равен h' с точностью до умножения на ненулевую константу. Пункт 1) доказан.

Докажем существование алгоритма для вычисления GCD(f, g). Пусть $g \neq 0$. С помощью алгоритма деления f представляем в виде $f = qg + r$, где $q, r \in k[x]$, deg(r) < deg(g) или $r = 0$. Покажем, что GCD(f, g) = GCD(r, g).

В силу п. 2) для этого достаточно доказать, что $< f, g > = < r, g >$. Возьмем любой полином $p \in < f, g >$. Тогда существуют $A, B \in k[x]$ такие, что $p = Af + Bg$. Отсюда $p = A(qg + r) + Bg = Ar + (Aq + B)g$, т.е. $p \in < r, g >$, а значит, $< f, g > \subset < r, g >$. Выберем теперь любое $p \in < r, g >$. Тогда существуют $C, D \in k[x]$ такие, что $p = Cr + Dg$. Следовательно, $p = C(f – qg) + Dg = Cf + (D – Cq)g$, т.е. $p \in < f, g >$. Отсюда $< r, g > \subset < f, g >$. Следовательно, $< f, g > = < r, g >$. Таким образом, GCD(f, g) = GCD(r, g), где deg(g) > deg(r) или $r = 0$. Если $r \neq 0$, то, повторяя эту процедуру, g представляем в виде $g = q'r + r'$, где deg(r) > deg(r') или $r' = 0$. Тогда GCD(g, r) = GCD(r, r'). Если $r' \neq 0$, то $r = q''r' + r''$. Таким образом, имеем равенства

$$\text{GCD}(f, g) = \text{GCD}(g, r) = \text{GCD}(r, r') = \text{GCD}(r', r'') = \ldots,$$

где $\deg(g) > \deg(r) > \deg(r') > \deg(r'') > \ldots$

Так как степени полиномов уменьшаются, то через конечное число шагов одно из $r, r', r'', \ldots$ будет равно нулю. В этот момент имеем $\mathrm{GCD}(h, 0) = \mathrm{GCD}(f, g)$. Так как $< h, 0 > = < h >$, то $\mathrm{GCD}(h, 0) = h$. Таким образом, $h = \mathrm{GCD}(f, g)$, т.е. $\mathrm{GCD}(f, g)$ равен последнему ненулевому остатку. Работа алгоритма заканчивается, когда остаток равен нулю. Этот алгоритм нахождения наибольшего общего делителя полиномов f, g называется *алгоритмом Евклида*.

Определение 4. *Наибольшим общим делителем полиномов* $f_1,\ldots,f_s \in k[x]$ называется полином $h \in k[x]$ такой, что

1) h делит $f_1,\ldots,f_s$;
2) если некоторый полином $p \in k[x]$ делит $f_1,\ldots,f_s$, то p делит h.

Наибольший общий делитель h полиномов $f_1,\ldots,f_s$ обозначается через $\mathrm{GCD}(f_1,\ldots,f_s)$.

Теорема 4. *Пусть* $f_1,\ldots,f_s \in k[x], s \geq 2$. *Тогда*

1) $\mathrm{GCD}(f_1,\ldots,f_s)$ *существует и определен однозначно;*
2) Идеал $< f_1,\ldots,f_s > = < \mathrm{GCD}(f_1,\ldots,f_s) >$;
3) если $s \geq 3$, *то* $\mathrm{GCD}(f_1,\ldots,f_s) = \mathrm{GCD}(f_1, \mathrm{GCD}(f_2,\ldots,f_s))$;
4) существует алгоритм для вычисления $\mathrm{GCD}(f_1,\ldots,f_s)$.

Доказательство. Доказательство пп. 1) и 2) проводится аналогично доказательству тех же пунктов теоремы 3. Докажем п. 3).Пусть $h = \mathrm{GCD}(f_2,\ldots,f_s)$. Покажем, что $< f_1, h > = < f_1,\ldots,f_s >$. Пусть $g \in < f_1, h >$. Тогда существуют $A, B \in k[x]$ такие, что $g = Af_1 + Bh$. На основании п. 2 идеал $< f_2,\ldots,f_s > = < h >$. Значит, существуют $A_2,\ldots,A_s \in k[x]$ такие, что $h = \sum_{k=2}^{s} A_k f_k$. Отсюда $g = Af_1 + \sum_{k=2}^{s} (A_k B) f_k$, т.е. $< f_1, h > \subset < f_1,\ldots,f_s >$. Пусть теперь $g \in < f_1,\ldots,f_s >$. Тогда существуют $C_k \in k[x]$, $k = \overline{1,s}$ такие, что $g = \sum_{k=1}^{s} C_k f_k$. Так как $< f_2,\ldots,f_s > = < h >$, то существуют $D_k \in k[x]$, $k = \overline{2,s}$ такие, что $f_k = D_k h$. Следовательно, $g = C_1 f_1 + \left(\sum_{k=2}^{s} C_k D_k \right) h$, т.е. $< f_1,\ldots,f_s > = < f_1, h >$. На основании п. 2) $< \mathrm{GCD}(f_1, h) > = < \mathrm{GCD}(f_1,\ldots,f_s) >$. Из теоремы 2 следует, что $\mathrm{GCD}(f_1, h) = \mathrm{GCD}(f_1,\ldots,f_s)$, т.е. доказан п. 3).

Из п. 3) получаем цепочку равенств

$$\mathrm{GCD}(f_1,\ldots,f_s) = \mathrm{GCD}(f_1, \mathrm{GCD}(f_2,\ldots,f_s)) =$$

$$= \mathrm{GCD}(f_1, \mathrm{GCD}(f_2, \mathrm{GCD}(f_3,\ldots,f_s))) = \ldots =$$

$$= \mathrm{GCD}(f_1, \mathrm{GCD}(f_2, \mathrm{GCD}(f_3,\ldots, \mathrm{GCD}(f_{s-2}, \mathrm{GCD}(f_{s-1}, f_s))\ldots).$$

Отсюда с использованием алгоритма Евклида и вытекает существование алгоритма для вычисления $\mathrm{GCD}(f_1,\ldots,f_s)$. □

1.3. АЛГОРИТМ ДЕЛЕНИЯ В $k[x_1,\ldots,x_n]$

Введем множество $\mathbf{Z}_{\geq 0}^n = \{(\alpha_1,\ldots,\alpha_n)\colon \alpha_i \in \{0\} \cup \mathbf{N},\ i = \overline{1,n}\}$.

Существует взаимно однозначное соответствие между мономами $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$ и n-наборами показателей степеней $\alpha = (\alpha_1, \alpha_2,\ldots,\alpha_n) \in \mathbf{Z}_{\geq 0}^n$. Упорядочение на $\mathbf{Z}_{\geq 0}^n$ определяет и упорядочение на множестве мономов. Если $\alpha > \beta$ в $\mathbf{Z}_{\geq 0}^n$, то мы будем говорить, что $x^\alpha > x^\beta$. Так как полином представляет собой линейную комбинацию мономов, то мы должны уметь расположить его члены в порядке убывания или возрастания. Для этого нужно уметь сравнивать любую пару мономов и определять, какой из них больше, т.е. наше упорядочение должно быть линейным. Это означает, что для любой пары мономов x^α и x^β должно выполняться ровно одно из следующих соотношений: $x^\alpha > x^\beta$, $x^\alpha = x^\beta$, $x^\alpha < x^\beta$. Нужно учитывать связь упорядочения с операциями сложения и умножения полиномов. Нужно требовать, что если $x^\alpha > x^\beta$, а x^γ – произвольный моном, то должно быть $x^\alpha x^\gamma > x^\beta x^\gamma$. Это означает, что если $\alpha > \beta$ в $\mathbf{Z}_{\geq 0}^n$, то для любого $\gamma \in \mathbf{Z}_{\geq 0}^n$ $\alpha + \gamma > \beta + \gamma$.

Определение 1. *Мономиальным упорядочением* на $k[x_1,\ldots,x_n]$ называется любое бинарное отношение $>$ на $\mathbf{Z}_{\geq 0}^n$, обладающее следующими свойствами:

1) отношение $>$ является линейным упорядочением на $\mathbf{Z}_{\geq 0}^n$;

2) если $\alpha > \beta$, то для любого $\gamma \in \mathbf{Z}_{\geq 0}^n$ $\alpha + \gamma > \beta + \gamma$;

3) отношение $>$ вполне упорядочивает множество $\mathbf{Z}_{\geq 0}^n$, т.е. любое ненулевое подмножество в $\mathbf{Z}_{\geq 0}^n$ имеет минимальный (наименьший) элемент (по отношению к упорядочению $>$).

Лемма 1. *Упорядочение $>$ на $\mathbf{Z}_{\geq 0}^n$ вполне упорядочивает это множество тогда и только тогда, когда любая строго убывающая последовательность элементов из $\mathbf{Z}_{\geq 0}^n$ $\alpha(1) > \alpha(2) > \alpha(3) > \ldots$ обрывается.*

Доказательство. Очевидно, что лемма 1 эквивалентна следующему утверждению: отношение > не является вполне упорядочением тогда и только тогда, когда существует бесконечная строго убывающая последовательность элементов из $\mathbf{Z}_{\geq 0}^{n}$. Если отношение > не является вполне упорядочением, то существует непустое подмножество $S \subset \mathbf{Z}_{\geq 0}^{n}$, которое не имеет минимального элемента. В качестве α(1) возьмем произвольный элемент S. Так как этот элемент не является минимальным, то существует $\alpha(2) \in S$ такой, что α(2) < α(1). Так как α(2) не минимален, то существует α(3) < α(2). Продолжая этот процесс неограниченно, получим бесконечную строго убывающую последовательность α(1) > α(2) > α(3) > …. Наоборот, если существует бесконечная строго убывающая последовательность α(1) > α(2) > α(3) > …, то множество {α(1), α(2), α(3),…} является непустым подмножеством в $\mathbf{Z}_{\geq 0}^{n}$, которое не имеет минимального элемента, т.е. отношение > не является вполне упорядочением. □

Предложение 1. *Пусть отношение > – некоторое мономиальное упорядочение. Тогда*

1) для любого $\alpha \in \mathbf{Z}_{\geq 0}^{n}$ $\alpha \geq 0$;

2) если x^{α} *делит* x^{β}, *то* $\alpha \leq \beta$.

Доказательство. Докажем 1). Пусть α_0 – наименьший элемент в $\mathbf{Z}_{\geq 0}^{n}$. Допустим, что $\alpha_0 < 0$. На основании свойства 2) определения 1 имеем $\alpha_0 + \alpha_0 < \alpha_0$, т.е. $2\alpha_0 < \alpha_0$, а тогда α_0 не является наименьшим элементом в $\mathbf{Z}_{\geq 0}^{n}$. Получили противоречие. Докажем 2). Пусть x^{α} делит x^{β}. Тогда существует моном x^{γ} такой, что $x^{\beta} = x^{\alpha}x^{\gamma}$, т.е. $\beta = \alpha + \gamma$. Из п. 1) $\gamma \geq 0$, а значит, $\alpha + \gamma \geq \alpha$. Следовательно, $\beta \geq \alpha$. □

Доказательства корректности алгоритмов (т.е. получение требуемого результата через конечное число шагов) будут базироваться на том, что старший член выражения, с которым работает алгоритм, строго убывает относительно некоторого фиксированного мономиального упорядочения на каждом шаге работы алгоритма.

Определение 2 (*лексикографического упорядочения*, или *lex-упорядочения*). Пусть $\alpha = (\alpha_1,\ldots,\alpha_n)$, $\beta = (\beta_1,\ldots,\beta_n) \in \mathbf{Z}_{\geq 0}^{n}$. Будем говорить, что $\alpha >_{\text{lex}} \beta$, если самая левая ненулевая координата вектора $\alpha - \beta \in \mathbf{Z}_{\geq 0}^{n}$ положительна. Мы будем писать $x^{\alpha} >_{\text{lex}} x^{\beta}$, если $\alpha >_{\text{lex}} \beta$.

Порядок $x_1 > x_2 > \ldots > x_n$ является lex-упорядочением, так как $(1, 0, 0,\ldots,0) >_{\text{lex}} (0, 1, 0,\ldots,0) >_{\text{lex}} \ldots >_{\text{lex}} (0, 0,\ldots,0, 1)$.

Предложение 2. *Лексикографическое упорядочение на* $\mathbf{Z}_{\geq 0}^{n}$ *является мономиальным упорядочением.*

Доказательство. 1) Тот факт, что отношение $>_{\text{lex}}$ – линейное упорядочение, непосредственно следует из определения 2 и из того, что обычное упорядочение на множестве $\mathbf{Z}_{\geq 0}$ линейно.

2) Пусть $\alpha >_{\text{lex}} \beta$. Тогда самая левая ненулевая координата вектора $\alpha - \beta$ положительна. Пусть это будет $\alpha_k - \beta_k > 0$. Имеем $x^{\alpha}x^{\gamma} = x^{\alpha+\gamma}$, $x^{\beta}x^{\gamma} = x^{\beta+\gamma}$. Тогда $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$, и самой левой ненулевой координатой этой разности является $\alpha_k - \beta_k > 0$, т.е. $(\alpha + \gamma) >_{\text{lex}} (\beta + \gamma)$.

Докажем свойство 3). Предположим, что отношение $>_{\text{lex}}$ не является вполне упорядочением. Из леммы 1 следует существование строго убывающей последовательности $\alpha(1) >_{\text{lex}} \alpha(2) >_{\text{lex}} \alpha(3) >_{\text{lex}} \ldots$ элементов из $\mathbf{Z}_{\geq 0}^{n}$. Покажем, что это невозможно. Действительно, рассмотрим первые координаты векторов $\alpha(i) \in \mathbf{Z}_{\geq 0}^{n}$. По определению лексикографического упорядочения они образуют невозрастающую последовательность неотрицательных целых чисел. Так как $\mathbf{Z}_{\geq 0}$ вполне упорядочено, то эта последовательность стабилизируется, т.е. существует k такое, что первые координаты векторов $\alpha(i)$ одинаковы для $i \geq k$. Начиная с $\alpha(k)$ будем рассматривать вторые координаты, а затем третьи и т.д. Последовательность вторых координат векторов $\alpha(k)$, $\alpha(k + 1),\ldots$ не возрастает, поэтому она стабилизируется, т.е. существует $l \geq k$ такое, что первые и вторые координаты векторов $\alpha(i)$ одинаковы для $i \geq l$. Продолжая это рассуждение, мы находим такое m, что у векторов $\alpha(m)$, $\alpha(m + 1),\ldots$ равны все координаты. Следовательно, это одинаковые векторы, что противоречит строгому убыванию последовательности. □

Задав произвольный порядок переменных $x_1,\ldots,x_n$, получим соответствующее ему лексикографическое упорядочение. В случае n переменных имеется $n!$ лексикографических упорядочений. В случае лексикографического переменная больше любого монома, содержащего только меньшие переменные вне зависимости от его степени. Иногда необходимо учитывать также степени мономов и сравнивать сначала именно степени. Это можно сделать с помощью градуированного лексикографического упорядочения (grlex-упорядочения).

Определение 3 (*градуированного лексикографического упорядочения*, или *grlex-упорядочения*). Пусть $\alpha, \beta \in \mathbf{Z}_{\geq 0}^{n}$. Будем говорить, что $\alpha >_{\text{grlex}} \beta$, если $|\alpha| = \sum_{i=1}^{n} б_i > |\beta| = \sum_{i=1}^{n} \beta_i$ или $|\alpha| = |\beta|$ и $\alpha >_{\text{lex}} \beta$.

Предложение 3. *Градуированное лексикографическое упорядочение является мономиальным упорядочением.*

Доказательство. 1) То, что отношение $>_{\text{grlex}}$ – линейное упорядочение, следует из того, что обычное упорядочение на $\mathbf{Z}_{\geq 0}^{n}$ линейно.

2) Если $\alpha >_{\text{grlex}} \beta$, то для любого $\gamma \in \mathbf{Z}_{\geq 0}^{n}$ $(\alpha + \gamma) >_{\text{grlex}} (\beta + \gamma)$ ввиду того, что в случае $|\alpha|>|\beta|$ $|\alpha + \gamma| > |\beta + \gamma|$, а в случае $|\alpha| = |\beta|$ $|\alpha + \gamma| = |\beta + \gamma|$ и $(\alpha + \gamma) >_{\text{lex}} (\beta + \gamma)$.

3) Предположим, что отношение $>_{\text{grlex}}$ не является вполне упорядочением. Тогда существует строго убывающая бесконечная последовательность $\alpha(1) >_{\text{grlex}} \alpha(2) >_{\text{grlex}} \ldots$. Покажем, что это невозможно. Действительно, $|\alpha(i)|$ образует невозрастающую последовательность неотрицательных целых чисел. Так как $\mathbf{Z}_{\geq 0}^{n}$ вполне упорядочено, то существует k такое, что для $i \geq k$ $|\alpha(i)| = |\alpha(k)|$. Следовательно, $\alpha(k) >_{\text{lex}} \alpha(k + 1) >_{\text{lex}} \ldots$. Дальнейшее – повторение доказательства п. 3) предложения 2. □

Определение 4 (*градуированного обратного лексикографического упорядочения*, или *grevlex-упорядочения*). Пусть $\alpha, \beta \in \mathbf{Z}_{\geq 0}^{n}$. Будем говорить, что $\alpha >_{\text{grevlex}} \beta$, если $|\alpha| = \sum_{i=1}^{n} б_i > |\beta| = \sum_{i=1}^{n} \beta_i$ или $|\alpha| = |\beta|$ и самая правая ненулевая координата вектора $\alpha - \beta \in \mathbf{Z}^{n}$ отрицательна.

Предложение 4. *Градуированное обратное лексикографическое упорядочение является мономиальным упорядочением.*

Доказательство. 1) Линейность градуированного обратного лексикографического упорядочения следует из линейности обычного упорядочения на $\mathbf{Z}_{\geq 0}$. 2) Пусть $\alpha >_{\text{grevlex}} \beta$ и $|\alpha| > |\beta|$. Тогда для любого $\gamma \in \mathbf{Z}_{\geq 0}^{n}$ $|\alpha + \gamma| > |\beta + \gamma|$, а значит $(\alpha + \gamma) >_{\text{grevlex}} (\beta + \gamma)$. Пусть теперь $\alpha >_{\text{grevlex}} \beta$ и $|\alpha| = |\beta|$. Тогда для любого $\gamma \in \mathbf{Z}_{\geq 0}^{n}$ $(\alpha + \gamma) >_{\text{grevlex}} (\beta + \gamma)$, так как $(\alpha + \gamma) - (\beta + \gamma) = \alpha - \beta$. 3) Предположим, что отношение $>_{\text{grevlex}}$ не является вполне упорядочением. Тогда существует строго убывающая бесконечная последовательность $\alpha(1) >_{\text{grevlex}} \alpha(2) >_{\text{grevlex}} \ldots$. Так как $\mathbf{Z}_{\geq 0}$ вполне упорядочено, то существует k такое, что для любого $i \geq k$ $|\alpha(i)| = |\alpha(k)| = m$. Координаты векторов строго убывающей последовательности $\alpha(k) >_{\text{grevlex}} \alpha(k + 1) >_{\text{grevlex}} \ldots$ не превосходят m. Рассмотрим последние координаты векторов $\alpha(i) \in \mathbf{Z}_{\geq 0}^{n}$, где $i \geq k$. Они образуют неубывающую последовательность неотрицательных целых чисел, ограниченную сверху числом m. Отсюда следует, что существует l такое, что последние координаты

векторов $\alpha(i)$ при $i \geq l$ будут одинаковыми. Будем далее рассматривать предпоследние координаты векторов $\alpha(i)$ при $i \geq l$. Ввиду того, что они образуют ограниченную последовательность неотрицательных целых чисел, существует s такое, что при $i \geq s$ предпоследние и последние координаты векторов $\alpha(i)$ будут одинаковыми. Продолжая это рассуждение, мы найдем такое p, что у векторов $\alpha(p)$, $\alpha(p + 1)$,… равны все координаты, но это противоречит строгому убыванию последовательности $\alpha(i)$. □

Для n переменных имеется $n!$ grlex-упорядочений, зависящих от порядка переменных. Как и в lex- и grlex-случаях для n переменных существует $n!$ различных grevlex-упорядочений.

Определение 5. Пусть ненулевой полином $f = \sum_{б} a_б x^б \in k[x_1,\ldots,x_n]$ и пусть отношение $>$ – мономиальное упорядочение.

1) *Мультистепень полинома* f – это $\text{multideg}(f) = \max(\alpha \in \mathbf{Z}^n_{\geq 0} : a_\alpha \neq 0)$, где максимум берется по отношению $>$;

2) *Старший коэффициент полинома* f – это $\text{LC}(f) = a_{\text{multideg}(f)} \in k$;

3) *Старший моном полинома* f – это $\text{LM}(f) = x^{\text{multideg}(f)}$;

4) *Старший член полинома* f – это $\text{LT}(f) = \text{LC}(f)\text{LM}(f)$.

Предложение 5. *Пусть* $f, g \in k[x_1,\ldots,x_n]$ *– ненулевые полиномы. Тогда*

1) $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$;

2) *Если* $f + g \neq 0$, *то* $\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. *Если, кроме того,* $\text{multideg}(f) \neq \text{mulfideg}(g)$, *то указанное неравенство становится равенством.*

Доказательство. Пусть $\alpha_0 = \text{multideg}(f)$, $\beta_0 = \text{multideg}(g)$. Тогда $f = \text{LT}(f) + \sum_{\alpha<\alpha_0} a_\alpha x^\alpha$, $g = \text{LT}(g) + \sum_{\beta<\beta_0} b_\beta x^\beta$. Значит, $fg = \text{LT}(f)\text{LT}(g) + \text{LT}(g) \sum_{\alpha<\alpha_0} a_\alpha x^\alpha + \text{LT}(f) \sum_{\beta<\beta_0} b_\beta x^\beta + \sum_{\substack{\alpha<\alpha_0 \\ \beta<\beta_0}} a_\alpha b_\beta x^{\alpha+\beta}$. Отсюда $\text{LT}(fg) = \text{LT}(f)\text{LT}(g)$, т.е. $\text{LC}(fg)x^{\text{multideg}(fg)} = \text{LC}(f)\text{LC}(g)\, x^{\alpha_0+\beta_0}$. Значит, $\text{multideg}(fg) = \text{multideg}(f) + \text{multideg}(g)$. Свойство 1) доказано.

Докажем 2). Имеем $f + g = \text{LT}(f) + \text{LT}(g) + \sum_{\alpha<\alpha_0} a_\alpha x^\alpha + \sum_{\beta<\beta_0} b_\beta x^\beta$. Пусть $\text{LT}(f) + \text{LT}(g) \neq 0$. Тогда $\text{LT}(f + g) = \text{LT}(\text{LT}(f) + \text{LT}(g))$, т.е. $\text{multideg}(f + g) = \max(\text{multideg}(f), \text{multideg}(g))$. Очевидно, что это равенство выполняется

в случае $\alpha_0 \neq \beta_0$. Если $LT(f) + LT(g) = 0$, то $LT(f + g) = LT(\sum_{\alpha<\alpha_0} a_\alpha x^\alpha + \sum_{\beta<\beta_0} b_\beta x^\beta)$. Значит, $multideg(f + g) < \max(multideg(f), multideg(g))$. □

В дальнейшем будем считать, что выбрано некоторое мономиальное упорядочение и старшие члены, мультистепени и т.д. определяются относительно этого упорядочения.

Теорема 1 (алгоритм деления в $k[x_1,\ldots,x_n]$). *Зафиксируем некоторое мономиальное упорядочение $>$ на $\mathbf{Z}^n_{\geq 0}$ и пусть $F = (f_1,\ldots,f_s)$ – упорядоченный s-набор полиномов из $k[x_1,\ldots,x_n]$. Тогда любой полином $f \in k[x_1,\ldots,x_n]$ может быть записан в виде $f = \sum_{i=1}^{s} a_i f_i + r$, где $a_i, r \in k[x_1,\ldots,x_n]$ и или $r = 0$, или r есть линейная комбинация мономов с коэффициентами из k, ни один из которых не делится ни на один из старших членов $LT(f_i)$, $i = \overline{1,s}$. Мы называем r остатком от деления полинома f на F, а a_i, $i = \overline{1,s}$, – частными. Более того, если $a_i f_i \neq 0$, то $multideg(f) \geq multideg(a_i f_i)$. Существует алгоритм, вычисляющий a_i, r.*

Доказательство. Возьмем любой полином $f \in k[x_1,\ldots,x_n]$. Тогда

$$f = \sum_{i=1}^{s} a_{i0} f_i + p_0 + r_0, \qquad (1)$$

где $a_{i0} = 0$, $i = \overline{1,s}$, $p_0 = f$, $r_0 = 0$. Пусть никакой из $LT(f_i)$, $i = \overline{1, j-1}$, не делит $LT(p_0)$, но $LT(f_j)$ делит $LT(p_0)$. Тогда из (1) имеем

$$f = \sum_{i=1}^{s} a_{i1} f_i + p_1 + r_1, \qquad (2)$$

где $a_{i1} = a_{i0}$ для $i \neq j$, $a_{j1} = a_{j0} + \frac{LT(p_0)}{LT(f_j)}$, $p_1 = p_0 - \frac{LT(p_0)}{LT(f_j)} f_j$, $r_1 = r_0$. Из предложения 5 получаем

$$LT(\frac{LT(p_0)}{LT(f_j)} f_j) = \frac{LT(p_0)}{LT(f_j)} LT(f_j) = LT(p_0).$$

Отсюда в случае $p_1 \neq 0$ $multideg(p_1) < multideg(p_0)$. Здесь $LT(a_{j1} f_j) = LT(p_0)$, т.е. $multideg(a_{j1} f_j) = multideg(f)$. Аналогично, если, например, ни-

какой из LT(f_i), $i = \overline{1,k-1}$, не делит LT(p_1), но LT(f_k) делит LT(p_1), то из (2) находим

$$f = \sum_{i=1}^{s} a_{i2} f_i + p_2 + r_2, \qquad (3)$$

где $a_{i2} = a_{i1}$ для $i \neq k$, $a_{k2} = a_{k1} + \frac{\mathrm{LT}(p_1)}{\mathrm{LT}(f_k)}$, $p_2 = p_1 - \frac{\mathrm{LT}(p_1)}{\mathrm{LT}(f_k)} f_k$, $r_2 = r_1$. В случае $p_2 \neq 0$ multideg(p_2) < multideg(p_1). Здесь LT($a_{k2}f_k$) = LT($a_{k1}f_k + \frac{\mathrm{LT}(p_1)}{\mathrm{LT}(f_k)} f_k$). Поэтому в случае $k \neq j$ multideg($a_{k2}f_k$) = multideg(p_1) < multideg(f). В случае же $k = j$ multideg($a_{j2}f_j$) = multideg($a_{j1}f_j$) = multideg(f). Итак, в любом случае при $a_{i2}f_i \neq 0$ multideg($a_{i2}f_i$) ≤ multideg(f). Пусть далее, например, никакой из LT(f_i) не делит LT(p_2). Тогда из (3) имеем

$$f = \sum_{i=1}^{s} a_{i3} f_i + p_3 + r_3,$$

где $a_{i3} = a_{i2}$ для $i = \overline{1,s}$, $r_3 = r_2 + \mathrm{LT}(p_2)$, $p_3 = p_2 - \mathrm{LT}(p_2)$. Здесь при $p_3 \neq 0$ multideg(p_3) < multideg(p_2). Ясно, что при $a_{i3}f_i \neq 0$ multideg($a_{i3}f_i$) ≤ multideg(f). В рассмотренных случаях вычислений p_1, p_2 мы имеем шаги деления, т.е. шаги вычисления частных, в случае же вычисления p_3 имеем шаг вычисления остатка. Заметим, что multideg(p_3) < multideg(p_2) < multideg(p_1) < multideg(f). Далее могут снова возникать шаги вычисления частных и шаги вычисления остатков. Заметим, что алгоритм оканчивает свою работу через некоторое конечное число шагов m, когда $p_m = 0$, ибо в противном случае будем иметь бесконечную строго убывающую последовательность мультистепеней, что невозможно, так как отношение > является вполне упорядочением. Итак, на m-м шаге найдем $a_{im} = a_i$, $i = \overline{1,s}$, $p_m = 0$, $r_m = r$. Из приведенных выше рассуждений следует, что для f получим формулу (1), где или $r = 0$ или r есть линейная комбинация мономов с коэффициентами из k, ни один из которых не делится ни на один из старших членов LT(f_i), $i = \overline{1,s}$. При этом если $a_i f_i \neq 0$, то multideg(f) ≥ multideg($a_i f_i$). Из приведенных рассуждений следует, что алгоритм для вычисления a_i, r из (1) выглядит так:

Вход: $f_1,\ldots,f_s, f$
Выход: $a_1,\ldots,a_s, r$

$a_1 := 0; \ldots; a_s := 0; r := 0$
$p := f$
WHILE $p \neq 0$ DO
    IF существует i такое, что LT(f_i) делит LT(p)
        THEN выбираем наименьшее i такое, что LT(f_i) делит LT(p)
            $a_i := a_i + \mathrm{LT}(p)/\mathrm{LT}(f_i)$
            $p := p - (\mathrm{LT}(p)/\mathrm{LT}(f_i))f_i$
        ELSE
            $r := r + \mathrm{LT}(p)$
            $p := p - \mathrm{LT}(p)$

В приведенном алгоритме равенство

$$f = \sum_{i=1}^{s} a_i f_i + p + r \qquad (4)$$

выполняется на каждом шаге. Действительно, (4) выполнено для начальных значений a_i, $i = \overline{1,s}$, p и r. Пусть на некотором шаге (4) выполняется. Если следующим шагом является шаг деления, то некоторый LT(f_i) делит LT(p) и равенство

$$a_i f_i + p = (a_i + \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)})f_i + (p - \frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)} f_i)$$

показывает, что сумма $a_i f_i + p$ не изменилась. Равенство (4) выполняется и на этом шаге, так как все остальные переменные при этом не изменились. Если же следующим является шаг вычисления остатка, то меняются p и r, но их сумма не меняется, так как

$$p + r = (p - \mathrm{LT}(p)) + (r + \mathrm{LT}(p)).$$

Ясно, что и снова (4) выполняется на следующем шаге. Алгоритм прекращает работу, когда $p = 0$. В этом случае (4) имеет вид (2). Так как к r добавляются только такие члены, которые не делятся ни на один из LT(f_i), то это означает, что a_i и r удовлетворяют условиям теоремы в случае остановки работы алгоритма. Алгоритм остановится через конечное число шагов, так как на каждом шаге multideg(p) уменьшается. Каждый член полинома a_i равен $\frac{\mathrm{LT}(p)}{\mathrm{LT}(f_i)}$ для некоторого значения переменной p. Начальное значение p есть f, а так как multideg(p) строго убывает, то mul-

tideg(p) ≤ multideg(f). Следовательно, multideg($a_i f_i$) ≤ multideg(f), если $a_i f_i \neq 0$. □

Заметим, что упорядочение полиномов в s-наборе ($f_1,\ldots,f_s$) влияет на количество шагов алгоритма и на результат. Полиномы a_i и r могут измениться при изменении порядка делителей f_i. Они могут измениться и при переходе к другому мономиальному упорядочению.

1.4. МОНОМИАЛЬНЫЕ ИДЕАЛЫ

Определение 1. Идеал $I \subset k[x_1,\ldots,x_n]$ называется *мономиальным*, если существует подмножество $A \subset \mathbf{Z}^n_{\geq 0}$ (которое может быть бесконечным), такое, что I состоит из всех конечных сумм вида $\sum_{\alpha \in A} h_\alpha x^\alpha$, где $h_\alpha \in k[x_1,\ldots,x_n]$. Такой идеал I обозначается через $< x^\alpha : \alpha \in A >$.

Предложение 1. *Пусть $I = < x^\alpha : \alpha \in A >$ – мономиальный идеал. Тогда моном $x^\beta \in I$ тогда и только тогда, когда x^β делится на некоторый моном x^α, $\alpha \in A$.*

Доказательство. Если x^β делится на некоторый моном x^α, $\alpha \in A$, то из определения мономиального идеала $x^\beta \in I$. Пусть теперь $x^\beta \in I$. Тогда $x^\beta = \sum_{i=1}^{s} h_i x^{\delta(i)}$, где $h_i \in k[x_1,\ldots,x_n]$, $\alpha(i) \in A$. Рассматривая h_i как линейную комбинацию мономов, получим, что моном x^β содержится как член хотя бы в одном слагаемом из $h_i x^{\alpha(i)}$, т.е. $x^\beta = x^\gamma x^{\alpha(i)}$. □

Предложение 2. *Пусть I – некоторый мономиальный идеал, а $f \in k[x_1,\ldots,x_n]$. Тогда следующие условия эквивалентны:*

1) $f \in I$;

2) каждый член полинома f принадлежит I;

3) *f является k-линейной комбинацией мономов из I.*

Доказательство. Если f является k-линейной комбинацией мономов из I, то каждый член полинома f принадлежит I, т.е. имеет место импликация 3) ⇒ 2). Импликация 2) ⇒ 1) вытекает из определения идеала.

Пусть $f = \sum_{\beta} b_\beta x^\beta \in I$. Тогда из определения мономиального идеала имеем $\sum_{\beta} b_\beta x^\beta = \sum_{i=1}^{s} h_i x^{\alpha(i)}$, где $h_i \in k[x_1,\ldots,x_n]$, $\alpha(i) \in A$. Представляя h_i в виде линейных комбинаций мономов, получаем, что каждый $b_\beta x^\beta$ содержится как член хотя бы в одном слагаемом из $h_i x^{\alpha(i)}$, т.е. $b_\beta x^\beta = b_\beta x^{\alpha(i)+\gamma}$.

Следовательно, $b_\beta x^\beta \in I$, $x^\beta \in I$, а значит, имеет место импликация 1) $\Rightarrow$ 3). □

Следствие 1. *Два мономиальных идеала совпадают в том и только в том случае, когда совпадают множества мономов, содержащиеся в них.*

Доказательство вытекает из п. 3) предложения 2.

Теорема 1 (лемма Диксона). *Любой мономиальный идеал* $I = < x^\alpha : \alpha \in A > \subset k[x_1,\ldots,x_n]$ *может быть представлен в виде* $I = < x^{\alpha(1)},\ldots,x^{\alpha(s)} >$, *где* $\alpha(i) \in A$, $i = \overline{1,s}$. *В частности, I имеет конечный базис.*

Доказательство. Доказательство проведем методом математической индукции. Индукцию осуществим по числу переменных n. Пусть $n = 1$. Тогда I порожден мономом x_1^{α}, где $\alpha \in A \subset \mathbf{Z}_{\geq 0}$. Пусть β – наименьший элемент в А. Для любого $\alpha \in$ А имеем $\beta \leq \alpha$. Таким образом, x_1^{β} делит все образующие x_1^{α}, т.е. $I = < x_1^{\beta} >$.

Пусть $n > 1$ и теорема справедлива для $n - 1$. Обозначим переменные через $x_1,\ldots,x_{n-1}, y$, так что мономы в $k[x_1,\ldots,x_{n-1}, y]$ будем записывать в виде $x^\alpha y^m$, где $\alpha \in \mathbf{Z}_{\geq 0}^{n-1}$, $m \in \mathbf{Z}_{\geq 0}$. Пусть $I \subset k[x_1,\ldots,x_{n-1}, y]$ – мономиальный идеал. Рассмотрим идеал $J \subset k[x_1,\ldots,x_{n-1}]$, порожденный такими мономами x^α, что $x^\alpha y^m \in I$ для некоторого $m \in \mathbf{Z}_{\geq 0}$. Так как мономиальный идеал $J \subset k[x_1,\ldots,x_{n-1}]$, то по предположению индукции он конечно порожден, т.е. $J = < x^{\alpha(1)},\ldots,x^{\alpha(s)} >$. Идеал J можно рассматривать как «проекцию» идеала I в $k[x_1,\ldots,x_{n-1}]$. Из определения J для любого $i = \overline{1,s}$ существует $m_i \geq 0$, такое, что $x^{\alpha(i)} y^{m_i} \in I$. Пусть $m = \max(m_1,\ldots,m_s)$. Из определения идеала следует, что мономы $x^{\alpha(i)} y^{m_i} y^{m-m_i} = x^{\alpha(i)} y^m \in I$, $i = \overline{1,s}$. Для каждого l, $0 \leq l \leq m - 1$, рассмотрим идеал $J_l \subset k[x_1,\ldots,x_{n-1}]$, порожденный такими мономами x^β, что $x^\beta y^l \in I$. Можно считать, что J_l – это «срез» идеала I, порожденный мономами, содержащими y только в степени l. По предположению индукции J_l конечно порожден, т.е. $J_l = < x^{\alpha_l(1)},\ldots,x^{\alpha_l(s_l)} >$. Ясно, что все мономы $x^{\alpha_l(i)} y^l$, $l = \overline{0,m}$, $i = \overline{1,s}$, принадлежат идеалу I.

Докажем, что I порожден мономами, перечисленными в следующем списке:

из J : $x^{\alpha(1)}y^m,\ldots,x^{\alpha(s)}y^m$,

из J_0 : $x^{\alpha_0(1)},\ldots,x^{\alpha_0(s_0)}$,

из J_1: $x^{\alpha_1(1)}y,\ldots,x^{\alpha_1(s_1)}y$,

……..

из J_{m-1}: $x^{\alpha_{m-1}(1)}y^{m-1},\ldots,x^{\alpha_{m-1}(s_{m-1})}y^{m-1}$.

Докажем сначала, что каждый моном в I делится хотя бы на один моном из списка. Пусть $x^{\alpha}y^{p} \in I$. Если $p \geq m$, то из определения J и предложения 1 следует, что моном $x^{\alpha}y^{p}$ делится на некоторый моном $x^{\alpha(i)}y^{m}$. Далее, если $p \leq m-1$. то из определения идеала J_p и предложения 1 следует, что моном $x^{\alpha}y^{p}$ делится на некоторый моном $x^{\alpha_p(j)}y^{p}$. Таким образом, любой моном $x^{\alpha}y^{p} \in I$ делится на некоторый моном из списка. Из предложения 1 следует, что мономы из списка порождают идеал, содержащий те же мономы, которые содержит I. Согласно следствию 1 эти идеалы совпадают. Итак, доказано, что мономиальный идеал I является конечно порожденным.

Докажем теперь, что конечное множество образующих можно выбрать из заданного множества образующих идеала I. Будем обозначать переменные, как и раньше, $x_1,\ldots,x_n$. Имеем $I = < x^{\alpha}: \alpha \in A > \subset k[x_1,\ldots,x_n]$. Докажем, что I порожден конечным набором x^{α}, $\alpha \in A$. Выше было доказано, что $I = < x^{\beta(1)},\ldots,x^{\beta(s)} >$, где $x^{\beta(i)} \in I$, $i = \overline{1,s}$. Так как $x^{\beta(i)} \in I = < x^{\alpha}: \alpha \in A >$, то из предположения 1 следует, что каждый моном $x^{\beta(i)}$, $i = \overline{1,s}$ делится на некоторый моном $x^{\alpha(i)}$, где $\alpha(i) \in A$. Рассмотрим мономиальный идеал $I_1 = < x^{\alpha(1)},\ldots,x^{\alpha(s)} >$. Так как $x^{\beta(i)} \in I_1$, $i = \overline{1,s}$, то $I \subset I_1$. С другой стороны, очевидно, $I_1 \subset I$, т.е. $I = < x^{\alpha(1)},\ldots,x^{\alpha(s)} >$. □

Теорема 2. *Пусть мономиальный идеал* $I = < x^{\alpha(1)},\ldots,x^{\alpha(s)} >$. *Полином* $f \in k[x_1,\ldots,x_n]$ *принадлежит идеалу* I *тогда и только тогда, когда остаток от деления* f *на набор* $\{x^{\alpha(1)},\ldots,x^{\alpha(s)}\}$ *равен нулю.*

Доказательство. Пусть $f \in I$. На основании алгоритма деления $f = \sum_{i=1}^{s} a_i x^{\alpha(i)} + r$, где a_i, $r \in k[x_1,\ldots,x_n]$, причем ни один из членов r не делится ни на один $x^{\alpha(i)}$, $i = \overline{1,s}$. Но $r \in I$. Предположим, что $r \neq 0$. На основании предложения 2 каждый член полинома r принадлежит I, т.е. каждый член r делится на некоторый моном $x^{\alpha(i)}$, получили противоречие. Таким образом, $r = 0$. Пусть теперь остаток от деления f на s-набор $\{x^{\alpha(1)},\ldots,x^{\alpha(s)}\}$ равен нулю. Тогда $f = \sum_{i=1}^{s} a_i x^{\alpha(i)}$, где $a_i \in k[x_1,\ldots,x_n]$. Отсюда $f \in I$. □

Теорема 3. *Пусть* $>$ *– некоторое отношение на* $\mathbf{Z}_{\geq 0}^n$, *удовлетворяющее следующим условиям:*

1) отношение $>$ *– линейное упорядочение на* $\mathbf{Z}_{\geq 0}^n$,

2) *если* $\alpha, \beta, \gamma \in \mathbf{Z}_{\geq 0}^n$, $\alpha > \beta$, *то* $\alpha + \gamma > \beta + \gamma$.

Тогда отношение $>$ является вполне упорядочением тогда и только тогда, когда для всех $\alpha \in \mathbf{Z}_{\geq 0}^n$ верно $\alpha \geq 0$.

Доказательство. Пусть отношение $>$ является вполне упорядочением. Тогда для всех $\alpha \in \mathbf{Z}_{\geq 0}^n$ $\alpha \geq 0$ (см. п. 1 предложения 1 п. 1.3). Пусть теперь для всех $\alpha \in \mathbf{Z}_{\geq 0}^n$ $\alpha \geq 0$. Возьмем любое непустое подмножество $A \subset \mathbf{Z}_{\geq 0}^n$. Докажем, что в A существует наименьший элемент. Рассмотрим мономиальный идеал $I = < x^{\alpha}: \alpha \in A > \subset k[x_1,\ldots,x_n]$. По лемме Диксона существуют $\alpha(i) \in A$, $i = \overline{1,s}$ такие, что $I = < x^{\alpha(1)},\ldots,x^{\alpha(s)} >$. Пусть $\alpha(1) < \alpha(2) < \ldots < \alpha(s)$ (в противном случае перенумеруем $\alpha(i)$). Возьмем любой элемент $\alpha \in A$. Тогда $x^{\alpha} \in < x^{\alpha(1)},\ldots,x^{\alpha(s)} >$. На основании предложения 1 п. 1.3 имеем $\alpha \geq \alpha(i) \geq \alpha(1)$, т.е. $\alpha(1)$ – наименьший элемент в A. □

Определение 2. Базис $\{x^{\alpha(1)},\ldots,x^{\alpha(s)}\}$ мономиального идеала $I \subset k[x_1,\ldots,x_n]$ называется *минимальным*, если $x^{\alpha(i)}$ не делит $x^{\alpha(j)}$ ни при каких $i \neq j$.

Теорема 4. *Любой мономиальный идеал* $I \subset k[x_1,\ldots,x_n]$ *имеет единственный минимальный базис.*

Доказательство. Пусть задан произвольный мономиальный идеал $I = < x^{\alpha} : \alpha \in A >$. Из леммы Диксона имеем $I = < x^{\alpha(1)},\ldots,x^{\alpha(s)} >$. Не умаляя общности будем считать, что $\alpha(1) < \alpha(2) < \ldots < \alpha(s)$. Если $x^{\alpha(s)}$ делится на некоторый $x^{\alpha(i)}$, $i < s$, то $x^{\alpha(s)}$ можно исключить из базиса. В результате будем иметь $I = < x^{\alpha(1)},\ldots,x^{\alpha(s-1)} >$. Если среди оставшихся $x^{\alpha(j)}$, где $j < s$, существуют такие, которые делятся на некоторый $x^{\alpha(k)}$, где $k < j$, то $x^{\alpha(j)}$ исключаем из базиса. Очевидно, что в результате мы получим для идеала I минимальный базис. Докажем его единственность. Допустим, что идеал I имеет два минимальных базиса $\{x^{\alpha(1)},\ldots,x^{\alpha(s)}\}$и $\{x^{\beta(1)},\ldots,x^{\beta(m)}\}$, где $\alpha(1) < \alpha(2) < \ldots < \alpha(s)$, $\beta(1) < \beta(2) < \ldots < \beta(m)$. На основании предложения 1 для $x^{\beta(1)}$ существует моном $x^{\alpha(i_1)}$, который делит $x^{\beta(1)}$, т.е. $x^{\beta(1)}/ x^{\alpha(i_1)}$ – моном. Аналогично, для монома $x^{\alpha(i_1)}$ существует $x^{\beta(j)}$, который делит $x^{\alpha(i_1)}$, т.е. $x^{\alpha(i_1)}/x^{\beta(j)}$ – моном. Тогда выражение $\dfrac{x^{\beta(1)}}{x^{\alpha(i_1)}} \cdot \dfrac{x^{\alpha(i_1)}}{x^{\beta(j)}} = \dfrac{x^{\beta(1)}}{x^{\beta(j)}}$ – моном. Из минимальности базиса $\{x^{\beta(1)},\ldots,x^{\beta(m)}\}$имеем $j = 1$. Отсюда $\beta(1) \geq \alpha(i_1)$, $\alpha(i_1) \geq \beta(1)$, т.е. $\beta(1) = \alpha(i_1)$. Аналогично $\beta(2) = \alpha(i_2),\ldots,\beta(m) = \alpha(i_m)$, где $i_1 < i_2 <$

… < i_m. Таким образом, $m \le s$. Меняя местами базисы, получаем $s \le m$, т.е. $s = m$. Тогда $\beta(i) = \alpha(i)$, $i = \overline{1,s}$. □

1.5. ТЕОРЕМА ГИЛЬБЕРТА О БАЗИСЕ И БАЗИСЫ ГРЁБНЕРА

Определение 1. Пусть $I \subset k[x_1,\ldots,x_n]$ – ненулевой идеал. Обозначим через LT(I) множество старших членов из I, т.е. LT(I) = $\{cx^\alpha : \exists\, f \in I$, что LT($f$) = $cx^\alpha\}$. Обозначим через < LT(I) > идеал, порожденный элементами из LT(I). Идеал < LT(I) > называется *идеалом старших членов* идеала I.

Предложение 1. *Пусть идеал I конечно порожден, т.е. $I = < f_1,\ldots,f_s >$. Тогда $< LT(f_1),\ldots,LT(f_s) > \subset < LT(I) >$.*

Доказательство. LT(I) $\subset$ < LT(I) >, т.к. идеал < LT(I) > порожден элементами из LT(I). Т.к. LT(f_i) $\in$ LT(I), то < LT(f_1),…,LT(f_s) > $\subset$ < LT(I) >. □

Пример 1. Пусть на мономах из $k[x, y]$ задано grlex-упорядочение. Пусть $I = < f_1, f_2 >$, где $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$. Тогда $-yf_1 + xf_2 = x^2$, т.е. $x^2 \in I$, $x^2 \in$ < LT(I) >. Однако $x^2 \notin$ < LT(f_1), LT(f_2) >, т.е. < LT(f_1), LT(f_2) > $\neq$ < LT(I) >.

Предложение 2. *Пусть $I \subset k[x_1,\ldots,x_n]$ – некоторый идеал. Тогда*

1) $< LT(I) >$ – мономиальный идеал;

2) *существуют $g_i \in I$, $i = \overline{1,s}$ такие, что $< LT(I) > = < LT(g_1),\ldots,LT(g_s) >$.*

Доказательство. 1) Старшие мономы LM(g) элементов $g \in I - \{0\}$ порождают мономиальный идеал < LM(g) : $g \in I - \{0\}$ >. Так как LT(g) = LC(g)LM(g), то из определения идеала следует, что < LT(g) : $g \in I - \{0\}$ > = < LT(I) > $\subset$ < LM(g) : $g \in I - \{0\}$ >. С другой стороны LM(g) $\in$ < LT(I) >, т.к. LM(g) = LT(g) / LC(g), т.е. < LM(g) : $g \in I - \{0\}$ > $\subset$ < LT(I) >. Следовательно, < LT(I) > = < LM(g) : $g \in I - \{0\}$ >, а значит, < LT(I) > – мономиальный идеал.

1) Так как < LT(I) > = < LM(g) : $g \in I - \{0\}$ >, т.е. идеал < LT(I) > порожден мономами из < LM(g) : $g \in I - \{0\}$ >, то по лемме Диксона из п. 1.4 < LT(I) > = < LM(g_1),…,LT(g_s) >, где $g_i \in I$, $i = \overline{1,s}$. Так как LM(g_i) отличаются от LT(g_i) на ненулевой множитель из поля k, то < LT(I) > = < LT(g_1),…,LT(g_s) >. □

Как всегда, мы считаем, что задано некоторое мономиальное упорядочение, используемое в алгоритме деления.

Теорема 1 (теорема Гильберта о базисе). *Каждый идеал* $I \subset k[x_1,\ldots,x_n]$ *является конечно порожденным, т.е.* $I = < g_1,\ldots,g_s >$, *где* $g_i \in I$, $i = \overline{1,s}$.

Доказательство. Если $I = \{0\}$, то $I = < 0 >$. Пусть I – ненулевой идеал. Из предложения 2 следует, что существуют $g_i \in I$, $i = \overline{1,s}$, такие, что $< \mathrm{LT}(I) > = < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >$. Покажем, что $I = < g_1,\ldots,g_s >$. Очевидно, $< g_1,\ldots,g_s > \subset I$. Возьмем любой полином $f \in I$. Поделим f на s-набор $\{g_1,\ldots,g_s\}$. Применяя алгоритм деления (п. 1.3), f представляем в виде: $f = \sum_{i=1}^{s} a_i g_i + r$, где $a_i, r \in k[x_1,\ldots,x_n]$, причем ни один член полинома r не делится ни на один из $\mathrm{LT}(g_i)$, $i = \overline{1,s}$. Покажем, что $r = 0$. Имеем $r = f - \sum_{i=1}^{s} a_i g_i \in I$. Если $r \neq 0$, то $\mathrm{LT}(r) \in < \mathrm{LT}(I) >$, а тогда на основании предложения 1 п. 1.4 $\mathrm{LT}(r)$ будет делиться хотя бы на один $\mathrm{LT}(g_i)$. Но это противоречит определению остатка. Значит, $r = 0$, т.е. $f = \sum_{i=1}^{s} a_i g_i$. Отсюда $I \subset < g_1,\ldots,g_s >$. □

Базис $\{g_1,\ldots,g_s\}$ из теоремы 1 обладает специальным свойством $< \mathrm{LT}(I) > = < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >$. Пример 1 показывает, что не все базисы идеала обладают этим свойством. Дадим этим базисам специальное название.

Определение 2. Пусть задано некоторое мономиальное упорядочение и задан идеал $I \subset k[x_1,\ldots,x_n]$. Конечное подмножество $G = \{g_1,\ldots,g_s\}$ элементов идеала I называется *базисом Грёбнера* идеала I (или *стандартным базисом*), если $< \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) > = < \mathrm{LT}(I) >$.

Предложение 3. *Пусть задан идеал* $I \subset k[x_1,\ldots,x_n]$. *Множество* $\{g_1,\ldots,g_s\} \subset I$ *является базисом Грёбнера идеала I тогда и только тогда, когда для любого* $f \in I$ $LT(f)$ *делится хотя бы на один* $LT(g_i)$.

Доказательство. Пусть множество $\{g_1,\ldots,g_s\} \subset I$ – базис Грёбнера идеала I. Тогда $< \mathrm{LT}(I) > = < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >$. Возьмем любой $f \in I$. Так как $\mathrm{LT}(f) \in < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >$, то $\mathrm{LT}(f)$ делится хотя бы на один $\mathrm{LT}(g_i)$. Пусть теперь для всех $f \in I$ $\mathrm{LT}(f)$ делится хотя бы на один $\mathrm{LT}(g_i)$. Тогда $\mathrm{LT}(f) \in < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >$, т.е. $< \mathrm{LT}(I) > \subset < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >$. □

Следствие 1. *Пусть задано некоторое мономиальное упорядочение. Тогда любой идеал* $I \subset k[x_1,\ldots,x_n]$ *имеет базис Грёбнера. При этом базис Грёбнера идеала I является его базисом.*

Доказательство. Пусть I – ненулевой идеал и $G = \{g_1,\ldots,g_s\}$ – множество, построенное в теореме 1. Это множество является базисом Грёбнера по определению, т.е. $< \mathrm{LT}(I) > = < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >$. Из доказательства теоремы 1 имеем $I = < g_1,\ldots,g_s >$, т.е. G является базисом идеала I. Следствие доказано.

Определение 3. *Возрастающей цепью идеалов* в $k[x_1,\ldots,x_n]$ называется последовательность $I_1 \subset I_2 \subset I_3 \subset \ldots$, где $I_k \subset k[x_1,\ldots,x_n]$.

Теорема 2 (условие обрыва возрастающих цепей). *Пусть $I_1 \subset I_2 \subset I_3 \subset \ldots$ – возрастающая цепь идеалов в $k[x_1,\ldots,x_n]$. Тогда существует $N \geq 1$ такое, что $I_N = I_{N+1} = I_{N+2} = \ldots$.*

Доказательство. Пусть $I_1 \subset I_2 \subset I_3 \subset \ldots$ – возрастающая цепь идеалов. Образуем множество $I = \bigcup_{i=1}^{\infty} I_i$. Докажем, что I – идеал в $k[x_1,\ldots,x_n]$. Имеем $0 \in I$, т.к. для любого i $0 \in I_i$. Далее, если $f, g \in I$, то существуют i, j такие, что $f \in I_i$, $g \in I_j$. Пусть, например, $i \leq j$. Тогда $I_i \subset I_j$, а значит, $f, g \in I_j$. Так как I_j – идеал, то $f + g \in I_j$, т.е. $f, g \in I$. Пусть теперь $f \in I$, $h \in k[x_1,\ldots,x_n]$. Тогда существует i такое, что $f \in I_i$. Отсюда $hf \in I_i$, т.е. $hf \in I$. Следовательно, I – идеал. По теореме Гильберта о базисе $I = < f_1,\ldots,f_s >$, где $f_i \in I$, $i = \overline{1,s}$. Каждый из f_i содержится в некотором идеале из цепи, т.е. существует j_i такое, что $f_i \in I_{ji}$, $i = \overline{1,s}$. Пусть $N = \max(j_1,\ldots,j_s)$. Тогда $f_i \in I_N$ для всех i, $i = \overline{1,s}$. Следовательно, $I = < f_1,\ldots,f_s > \subset I_N = I_{N+1} = \ldots = I$. Таким образом, возрастающая цепь стабилизируется, начиная с I_N. Все идеалы в цепи равны друг другу, начиная с I_N, т.е. $I_N = I_{N+1} = \ldots$. □

Теорему 2 часто называют *условием обрыва возрастающих цепей* или сокращенно *УОВЦ*.

Определение 4. Пусть $I \subset k[x_1,\ldots,x_n]$ – некоторый идеал. Положим $\mathbf{V}(I) = \{(a_1,\ldots,a_n) \in k^n : \forall\ f \in I \quad f(a_1,\ldots,a_n) = 0\}$.

Предложение 4. *Пусть $I \subset k[x_1,\ldots,x_n]$ – некоторый идеал. Тогда $\mathbf{V}(I)$ является аффинным многообразием, которое мы будем называть многообразием идеала I. В частности, если $I = < f_1,\ldots,f_s >$, то $\mathbf{V}(I) = \mathbf{V}(f_1,\ldots,f_s)$.*

Доказательство. По теореме Гильберта о базисе идеал $I = < f_1,\ldots,f_s >$. Покажем, что $\mathbf{V}(I) = \mathbf{V}(f_1,\ldots,f_s)$. Возьмем любой элемент $(a_1,\ldots,a_n) \in \mathbf{V}(I)$. Тогда из определения $\mathbf{V}(I)$ для любого $f \in I$ $f(a_1,\ldots,a_n) = 0$. Так как $f_i \in I$, $i = \overline{1,s}$, то и $f_i(a_1,\ldots,a_n) = 0$, $i = \overline{1,s}$, т.е. $\mathbf{V}(I) \subset \mathbf{V}(f_1,\ldots,f_s)$. Возьмем теперь любой элемент $(a_1,\ldots,a_n) \in \mathbf{V}(f_1,\ldots,f_s)$. Из определения многообразия $\mathbf{V}(f_1,\ldots,f_s)$ $f_i(a_1,\ldots,a_n) = 0$, $i = \overline{1,s}$. Выберем любой $f \in I$. Так как $I =$

$< f_1,\ldots,f_s >$, то существует $h_i \in k[x_1,\ldots,x_n]$ такое, что $f = \sum_{i=1}^{s} h_i f_i$. Тогда $f(a_1,\ldots,a_n) = \sum_{i=1}^{s} h_i(a_1,...,a_n) f_i(a_1,...,a_n) = \sum_{i=1}^{s} h_i(a_1,...,a_n) \cdot 0 = 0$. Следовательно, $\mathbf{V}(f_1,\ldots,f_s) \subset \mathbf{V}(I)$, т.е. $\mathbf{V}(I) = \mathbf{V}(f_1,\ldots,f_s)$. □

Следствие 2. *Пусть* $I_1 \subset I_2 \subset \ldots \subset I_k \subset \ldots$, *где* $I_k = < f_1,\ldots,f_k >$, $f_i \in k[x_1,\ldots,x_n]$. *Тогда для идеала* $I = \bigcup_{k=1}^{\infty} I_k$ *существует* N *такое, что* $I = < f_1,\ldots,f_N >$. *При этом* $\mathbf{V}(I) = \mathbf{V}(f_1,\ldots,f_N)$.

Доказательство. На основании теоремы УОВЦ существует N такое, что $I_N = I_{N+1} = \ldots = I$. Отсюда $I = < f_1,\ldots,f_N >$. Далее из предложения 4 имеем $\mathbf{V}(I) = \mathbf{V}(f_1,\ldots,f_N)$. □

1.6. СВОЙСТВА БАЗИСОВ ГРЁБНЕРА

Предложение 1. *Пусть* $G = \{g_1,\ldots,g_s\}$ *– базис Грёбнера идеала* $I \subset k[x_1,\ldots,x_n]$ *и пусть* $f \in k[x_1,\ldots,x_n]$. *Тогда существует единственный полином* $r \in k[x_1,\ldots,x_n]$, *который обладает следующими двумя свойствами:*

1) ни один член полинома r *не делится ни на один из старших членов* $LT(g_1),\ldots,LT(g_s)$;

2) существует $g \in I$ *такой, что* $f = g + r$.

То есть r *является остатком от деления* f *на* G, *не зависящим от порядка делителей в* G.

Доказательство. На основании алгоритма деления в $k[x_1,\ldots,x_n]$ f представляем в виде $f = \sum_{i=1}^{s} a_i g_i + r$, где a_i, $r \in k[x_1,\ldots,x_n]$, где ни один член полинома r не делится ни на один из $\mathrm{LT}(g_i)$, $i = \overline{1,s}$. Таким образом, $f = g + r$, где $g = \sum_{i=1}^{s} a_i g_i \in I$, а r удовлетворяет условию 1). Условие 2) также выполняется. Существование r доказано. Докажем единственность r. Пусть $f = g + r = g' + r'$, где $g, g' \in I$, а r, r' удовлетворяют условию 1). Отсюда $r - r' = g - g' \in I$. Пусть $r - r' \neq 0$. Тогда $\mathrm{LT}(r - r') \in < \mathrm{LT}(I) > = < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >$. На основании предложения 1 п. 1.4 $\mathrm{LT}(r - r')$ делится на какой-то старший член $\mathrm{LT}(g_i)$. Но это невозможно в силу условия 1). Значит, $r = r'$. □

Предложение 2. *Пусть задано некоторое мономиальное упорядочение и пусть $I \subset k[x_1,\ldots,x_n]$ – некоторый идеал. Тогда любой элемент f может быть представлен в виде $f = g + r$, где $g \in I$ и ни один член полинома r не делится ни на один элемент из $LT(I)$. При этом r определяется единственным образом.*

Доказательство. Пусть $G = \{g_1,\ldots,g_s\}$ – произвольный фиксированный базис Грёбнера идеала I. Тогда на основании предложения 1 любой элемент $f \in k[x_1,\ldots,x_n]$ можно представить в виде $f = g + r$, где $g, r \in k[x_1,\ldots,x_n]$, $g \in I$, причем ни один член полинома r не делится ни на один из $\mathrm{LT}(g_i)$, $i = \overline{1,s}$. Покажем, что для любого $h \in I$, $h \neq 0$ ни один член полинома r не делится на $\mathrm{LT}(h)$. Допустим, что существует член $r_\alpha x^\alpha$ полинома r, который делится на $\mathrm{LT}(h)$. Так как $\mathrm{LT}(h) \in <\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s)>$, то существует i, $1 \le i \le s$ такое, что $\mathrm{LT}(h)$ делится на $\mathrm{LT}(g_i)$. Тогда выражение $\dfrac{r_\alpha x^\alpha}{\mathrm{LT}(g_i)} = \dfrac{r_\alpha x^\alpha}{\mathrm{LT}(h)} \cdot \dfrac{\mathrm{LT}(h)}{\mathrm{LT}(g_i)}$ – моном, что невозможно. Итак, доказано, что любой элемент $f \in k[x_1,\ldots,x_n]$ можно представить в виде $f = g + r$, где $g \in I$ и ни один член полинома r не делится ни на один элемент из $\mathrm{LT}(I)$. Докажем единственность r. Пусть $f = g + r = g' + r'$, где $g, g' \in I$, и ни один член полиномов r, r' не делится ни на один элемент из $\mathrm{LT}(I)$. Тогда $r - r' = g - g' \in I$. Пусть $r - r' \neq 0$. Тогда $\mathrm{LT}(r - r') \in <\mathrm{LT}(I)>$, а поэтому на основании предложения 1 п. 1.4 $\mathrm{LT}(r - r')$ делится на какой-то старший член $\mathrm{LT}(h)$, где $h \in I$, что невозможно. □

Определение 1. Пусть задано некоторое мономиальное упорядочение и идеал $I \subset k[x_1,\ldots,x_n]$. *Нормальной формой полинома* $f \in k[x_1,\ldots,x_n]$ называется полином $r = f - g \in k[x_1,\ldots,x_n]$, где $g \in I$ и ни один член полинома r не делится ни на один элемент из $\mathrm{LT}(I)$.

Следствие 1. *Пусть $G = \{g_1,\ldots,g_s\}$ – базис Грёбнера идеала $I \subset k[x_1,\ldots,x_n]$ и пусть $f \in k[x_1,\ldots,x_n]$. Тогда $f \in I$ тогда и только тогда, когда остаток от деления полинома f на G равен нулю.*

Доказательство. Если $r = 0$, то $f \in I$. Пусть $f \in I$. Тогда равенство $f = f + 0$ удовлетворяет обоим условиям предложения 1. Из единственности представления f в таком виде следует, что 0 – остаток от деления f на G. □

Определение 2. Остаток от деления полинома $f \in k[x_1,\ldots,x_n]$ на упорядоченный s-набор $F = (f_1,\ldots,f_s)$, где $f_i \in k[x_1,\ldots,x_n]$, будет обозначаться через $\overline{f}^F$.

Следствие 2. *Пусть G и G' – базисы Грёбнера идеала I по отношению к одному и тому же мономиальному упорядочению в $k[x_1,\ldots,x_n]$. Тогда для любого $f \in k[x_1,\ldots,x_n]$* $\overline{f}^{G} = \overline{f}^{G'}$.

Доказательство. Пусть $G = \{g_1,\ldots,g_s\}$ и $G' = \{g_1',\ldots,g_{s'}'\}$ – базисы Грёбнера идеала I. Возьмем любой элемент $f \in k[x_1,\ldots,x_n]$. Произведя деление f на G, получим $f = \sum_{i=1}^{s} a_i g_i + r$, т.е. $\overline{f}^{G} = r$. Деление же f на G' дает $\sum_{i=1}^{s'} a_i' g_i' + r'$, $\overline{f}^{G'} = r'$. Из предложения 2 заключаем, что ни один член полиномов r, r' не делится ни на один элемент из LT(I). Из единственности представления f в виде $f = g + r$, где $g \in I$, и из того, что ни один член r не делится ни на один элемент из LT(I), заключаем, что $r = r'$. □

Определение 3. Пусть $f, g \in k[x_1,\ldots,x_n]$ – ненулевые полиномы.

1) Пусть multideg(f) = $\alpha = (\alpha_1,\ldots,\alpha_n)$, multideg($g$) = $\beta = (\beta_1,\ldots,\beta_n)$. Положим $\gamma = (\gamma_1,\ldots,\gamma_n)$, $\gamma_i = \max(\alpha_i, \beta_i)$, $i = \overline{1,n}$. Тогда x^{γ} называется *наименьшим общим кратным мономов* LM(f), LM(g). Используется обозначение x^{γ} = LCM(LM(f), LM(g)).

2) *S-полиномом* от f, g называется комбинация

$$S(f, g) = \frac{x^{\gamma}}{LT(f)} \cdot f - \frac{x^{\gamma}}{LT(g)} \cdot g .$$

Лемма 1. *Рассмотрим сумму* $\sum_{i=1}^{s} c_i f_i$, *где* multideg(f_i) = $\delta \in \mathbf{Z}_{\geq 0}^{n}$, *а* $c_i \in k$, $i = \overline{1,s}$. *Если* multideg($\sum_{i=1}^{s} c_i f_i$) < δ, *то* $\sum_{i=1}^{s} c_i f_i$ *является линейной комбинацией S-полиномов* $S(f_j, f_l)$, $1 \leq j, l \leq s$ *с коэффициентами в* k. *При этом* multideg($S(f_j, f_l)$) < δ, $j, l = \overline{1,s}$.

Доказательство. Пусть d_i = LC(f_i). Тогда $c_i d_i$ = LC($c_i f_i$). Так как multideg($c_i f_i$) = δ, а multideg($\sum_{i=1}^{s} c_i f_i$) < δ, то $\sum_{i=1}^{s} c_i d_i = 0$. Положим $p_i = \frac{f_i}{d_i}$. Тогда LC(p_i) = 1. Преобразуем рассматриваемую сумму: $\sum_{i=1}^{s} c_i f_i = \sum_{i=1}^{s} c_i d_i p_i$ = $c_1 d_1 p_1 + (c_1 d_1 + c_2 d_2 - c_1 d_1) p_2 + (c_1 d_1 + c_2 d_2 + c_3 d_3 - c_1 d_1 - c_2 d_2) p_3 + \ldots +$

$(c_1d_1 + \ldots + c_sp_s - c_1d_1 - \ldots - c_{s-1}d_{s-1})p_s = c_1d_1(p_1 - p_2) + (c_1d_1 + c_2d_2)(p_2 - p_3) + \ldots + (c_1d_1 + \ldots + c_{s-1}d_{s-1})(p_{s-1}\, p_s) + (c_1d_1 + \ldots + c_sd_s)p_s$.

Но $\mathrm{LT}(f_i) = d_ix^{\delta}$, поэтому $\mathrm{LCM}(\mathrm{LM}(f_j), \mathrm{LM}(f_l)) = x^{\delta}$. Значит, $S(f_j, f_l) = \frac{x^{\delta}}{LT(f_j)} f_j - \frac{x^{\delta}}{LT(f_l)} f_l = \frac{x^{\delta}}{d_j x^{\delta}} f_j - \frac{x^{\delta}}{d_l x^{\delta}} f_l = p_j - p_l$.

Далее имеем $\sum_{i=1}^{s} c_i f_i = c_1d_1S(f_1, f_2) + (c_1d_1 + c_2d_2)S(f_2, f_3) + \ldots + (c_1d_1 + \ldots + c_{s-1}d_{s-1})S(f_{s-1}, f_s)$, т.е. получили линейную комбинацию S-полиномов. Так как $\mathrm{multideg}(p_i) = \delta$, а $\mathrm{LC}(p_i) = 1$, то $\mathrm{multideg}(p_j - p_l) = \mathrm{multideg}(S(f_j, f_l)) < \delta$. □

Теорема 1 (критерий Бухбергера). *Пусть идеал $I \subset k[x_1,\ldots,x_n]$. Тогда базис $G = \{g_1,\ldots,g_s\}$ идеала I является базисом Грёбнера тогда и только тогда, когда для всех пар $i \neq j$ остаток от деления $S(g_i, g_j)$ на G (в любом порядке) равен нулю.*

Доказательство. Пусть G – базис Грёбнера идеала I. Так как $S(g_i, g_j) \in I$, то в силу следствия 1 остаток от деления $S(g_i, g_j)$ на G равен нулю.

Пусть f – произвольный ненулевой полином из I. Мы должны доказать, что если остатки от деления всех S-полиномов на G равны нулю, то $\mathrm{LT}(f) \in < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >$. Так как $f \in I = < g_1,\ldots,g_s >$, то существуют $h_i \in k[x_1,\ldots,x_n]$ такие, что

$$f = \sum_{i=1}^{s} h_i g_i . \qquad (1)$$

Из предложения 5 п. 1.3 следует, что

$$\mathrm{multideg}(f) \leq \max_i (\mathrm{multideg}(h_i f_i)). \qquad (2)$$

Пусть $m_i = \mathrm{multideg}(h_ig_i)$. Положим $\delta = \max(m(1),\ldots,m(s))$. Тогда неравенство (2) имеет вид $\mathrm{multideg}(f) \leq \delta$. Рассмотрим все возможные способы, какими f может быть записано в виде (1). Для каждого такого способа будем иметь свой δ. Так как мономиальное упорядочение является вполне упорядочением, то мы можем выбрать такое выражение (1), для которого δ является минимальным. В дальнейшем будем считать, что мы выбрали выражение (1) с минимальным δ. Покажем, что в этом случае $\mathrm{multideg}(f) = \delta$. Докажем этот факт от противного. Допустим, что $\mathrm{multideg}(f) < \delta$. Представим (1) в виде

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i + \sum_{m(i)=\delta} (h_i - \mathrm{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i . \quad (3)$$

Мономы во второй и третьей суммах в самой правой части равенства (3) имеют мультистепени $< \delta$. Поэтому из предположения $\mathrm{multideg}(f) < \delta$ вытекает, что и первая сумма правой части (3) также имеет мультистепень $< \delta$. Пусть $\mathrm{LT}(h_i) = c_i x^{\alpha(i)}$. Тогда сумма $\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{m(i)=\delta} c_i x^{\alpha(i)} g_i$ имеет в точности тот вид, который описан в условии леммы 1 с $f_i = x^{\alpha(i)} g_i$. Из леммы 1 следует, что эта сумма является линейной комбинацией S-полиномов $S(x^{\alpha(j)} g_j, x^{\alpha(l)} g_l)$. Имеем $S(x^{\alpha(j)} g_j, x^{\alpha(l)} g_l) = \frac{x^{\delta}}{x^{\alpha(j)} \mathrm{LT}(g_j)} x^{\alpha(j)} g_j - \frac{x^{\delta}}{x^{\alpha(l)} \mathrm{LT}(g_l)} x^{\alpha(l)} g_l = \frac{x^{\delta}}{\mathrm{LT}(g_j)} g_j - \frac{x^{\delta}}{\mathrm{LT}(g_l)} g_l$.

Пусть $x^{\gamma_{jl}} = \mathrm{LCM}(\mathrm{LM}(g_j), \mathrm{LM}(g_l))$. Тогда $S(x^{\alpha(j)} g_j, x^{\alpha(l)} g_l) = x^{\delta - \gamma_{jl}} \cdot \left(\frac{x^{\gamma_{jl}}}{\mathrm{LT}(g_j)} g_j - \frac{x^{\gamma_{jl}}}{\mathrm{LT}(g_l)} g_l\right) = x^{\delta - \gamma_{jl}} S(g_j, g_l)$. Заметим, что $\alpha(j) + \mathrm{multideg}(g_j) = \alpha(l) + \mathrm{multideg}(g_l) = \delta$, а поэтому $x^{\delta - \gamma_{jl}}$ – моном. Значит, существуют $c_{jl} \in k$ такие, что

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_{j,l} c_{jl} x^{\delta - \gamma_{jl}} S(g_j, g_l). \quad (4)$$

Так как остаток от деления $S(g_j, g_l)$ на G равен нулю, то каждый такой S-полином может быть записан в виде

$$S(g_j, g_l) = \sum_{i=1}^{s} a_{ijl} g_i , \quad (5)$$

где $a_{ijl} \in k[x_1, \ldots, x_n]$. Из алгоритма деления следует, что для любых i, j, l с $a_{ijl} g_i \neq 0$

$$\mathrm{multideg}(a_{ijl} g_i) \leq \mathrm{multideg}(S(g_j, g_l)). \quad (6)$$

Умножая (5) на $x^{\delta - \gamma_{jl}}$, получаем

$$x^{\delta-\gamma_{jl}} S(g_j, g_l) = \sum_{i=1}^{s} b_{ijl} g_i , \qquad (7)$$

где $b_{ijl} = x^{\delta-\gamma_{jl}} a_{ijl}$. Из неравенства (6) и леммы 1 следует, что

$$\text{multideg}(b_{ijl}g_i) \le \text{multideg}(x^{\delta-\gamma_{jl}} S(g_j, g_l)) < \delta. \qquad (8)$$

Из (4) с учетом (7) получаем равенство

$$\sum_{m(i)=\delta} \text{LT}(h_i) g_i = \sum_{j,l} c_{jl} x^{\delta-\gamma_{jl}} S(g_j, g_l) = \sum_{j,l} c_{jl} (\sum_{i=1}^{s} b_{ijl} g_i) = \sum_{i=1}^{s} \tilde{h}_i g_i . \qquad (9)$$

Из (8) имеем для всех i

$$\text{multideg}(\tilde{h}_i g_i) < \delta. \qquad (10)$$

Из формул (3), (9) получаем $f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)=\delta} (h_i - \text{LT}(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{i=1}^{s} w_i g_i$. Отсюда из неравенств (10) заключаем, что multideg($w_i g_i$) < δ, $i = \overline{1,s}$. Эти неравенства противоречат выбору δ. Итак, доказано, что multideg(f) = δ. Из (1) следует, что существует i такое, что multideg(f) = multideg($h_i g_i$). Из предложения 5 п. 1.3 получаем, что multideg(f) = multideg(h_i) + multideg(g_i), т.е. LT(f) делится на LT(g_i). Таким образом, LT(f) ∈ < LT(g_1),…,LT(g_s) >. □

1.7. АЛГОРИТМ БУХБЕРГЕРА

В следствии 1 п. 1.5 доказано, что каждый ненулевой идеал $I \subset k[x_1,\ldots,x_n]$ имеет базис Грёбнера. Базис Грёбнера для идеала I можно построить расширяя какой-нибудь базис $F = \{f_1,\ldots,f_s\}$ идеала I путем последовательного добавления ненулевых остатков $\overline{S(f_i, f_j)}^{F}$ к F. Эта идея естественно возникает из критерия S-пар Бухбергера, и алгоритм Бухбергера, который мы будем рассматривать, является реализацией этой идеи.

Теорема 1 (алгоритм Бухбергера). *Пусть дан некоторый ненулевой идеал $I = < f_1,\ldots,f_s > \subset k[x_1,\ldots,x_n]$. Тогда базис Грёбнера для I может*

быть построен за конечное число шагов с помощью следующего алгоритма:

Вход: $F = (f_1,\ldots,f_s)$
Выход: базис Грёбнера $G = (g_1,\ldots,g_t)$ идеала I, где $F \subset G$.
$G := F$
REPEAT
$G' = G$
FOR для каждой пары $\{p, q\}$, $p \neq q$ в G' DO
$S := \overline{S(p,q)}^{G'}$
IF $S \neq 0$ THEN $G := G \cup \{S\}$
UNTIL $G = G'$.

Доказательство. Сначала введем удобные обозначения. Если $G = \{g_1,\ldots,g_s\}$, то через $< G >$ и $< \mathrm{LT}(G) >$ будем обозначать следующие идеалы:

$$< G > = < g_1,\ldots,g_s >, < \mathrm{LT}(G) > = < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_s) >.$$

Докажем, что условие $G \subset I$ выполняется на каждом шаге алгоритма. Это верно в начале работы алгоритма, так как в этом случае $G = F = (f_1,\ldots,f_s) \subset I$. Далее полагаем $G' = G$. Будем рассматривать множество G. Находим остаток $S = \overline{S(p,q)}^{G'}$, где $p, q \in G'$. Если $G' \subset I$, то $p, q, S(p, q) \in I$. Так как $G' \subset I$, то и $S = \overline{S(p,q)}^{G'} \in I$. Следовательно, $(G \cup \{S\}) \subset I$. Так как $(G \cup \{S\}) \supset F$, где F – исходный базис идеала I, то и множество $G \cup \{S\}$, которое является расширением множества G, является базисом идеала I. Если $S \neq 0$, то $G' \subset G$. Если $G' \neq G$, то полагаем $G' = G$ и снова находим остаток $S = \overline{S(p,q)}^{G'}$, где $p, q \in G'$. Далее рассматриваем множество $G \cup \{S\}$, являющееся расширением G. Алгоритм заканчивает работу, когда $G = G'$, т.е. когда $\overline{S(p,q)}^{G'} = 0$ для любых $p, q \in G'$. В этом случае из теоремы 1 п. 1.6 следует, что G – базис Грёбнера для идеала $I = < G >$. Осталось доказать, что алгоритм через конечное число шагов останавливается. Посмотрим, что происходит во время выполнения каждого шага алгоритма. Множество G состоит из G' (старое G) и ненулевых остатков от деления S-полиномов от элементов из G' на G', т.е. $< \mathrm{LT}(G') > \subset < \mathrm{LT}(G) >$, так как $G' \subset G$. Докажем, что если $G' \neq G$, то $< \mathrm{LT}(G') >$ строго меньше, чем $< \mathrm{LT}(G) >$. Пусть ненулевой остаток r от деления S-полинома на G' был добавлен к G. Тогда, так как r – остаток, то $\mathrm{LT}(r)$ не

делится ни на один старший член элемента из G', т.е. $LT(r) \notin < LT(G') >$. Но $LT(r) \in < LT(G) >$, т.е. $< LT(G') > \subset < LT(G) >$, $< LT(G') > \neq < LT(G) >$. Так как $< LT(G') > \subset < LT(G) >$, то идеалы, получающиеся в результате последовательных выполнений каждого шага алгоритма, образуют возрастающую цепь в $k[x_1,\ldots,x_n]$. Тогда из УОВЦ (теорема 2 п. 1.5) следует, что эта цепь стабилизируется, т.е. условие $< LT(G') > = < LT(G) >$ будет выполняться в результате выполнения конечного числа шагов алгоритма. Это означает, что условие $G = G'$ станет выполняться и алгоритм остановится через конечное число шагов. □

В алгоритме нам нужно вычислить остатки $\overline{S(p,q)}^{G'}$ при $i < j$ (т.е. для новых порождающих элементов). Базисы Грёбнера могут быть избыточными, т.е. большими, чем необходимо. Мы можем исключить лишние образующие, используя следующую теорему.

Теорема 2. *Пусть G – базис Грёбнера полиномиального идеала $I \subset k[x_1,\ldots,x_n]$ и пусть $p \in G$, $LT(p) \in < LT(G - \{p\}) >$. Тогда $G - \{p\}$ также является базисом Грёбнера для I.*

Доказательство. Так как G – базис Грёбнера для I, то $< LT(G) > = < LT(I) >$. Если для $p \in G$ $LT(p) \in < LT(G - \{p\}) >$, то $< LT(G - \{p\}) > = < LT(G) >$. Значит, $< LT(G - \{p\}) > = < LT(I) >$, т.е. $G - \{p\}$ – базис Грёбнера идеала I по определению. □

Можно в базисе Грёбнера G сделать все старшие коэффициенты единицами, а также исключить из G все p такие, что $LT(p) \in < LT(G - \{p\}) >$. В результате получим минимальный базис Грёбнера.

Определение 1. *Минимальным базисом Грёбнера* идеала $I \subset k[x_1,\ldots,x_n]$ называется его базис Грёбнера такой, что:

1) для любого $p \in G$ $LC(p) = 1$;
2) для любого $p \in G$ $LT(p) \notin < LT(G - \{p\}) >$.

Теорема 3. *Базис Грёбнера G полиномиального идеала $I \subset k[x_1,\ldots,x_n]$ является минимальным тогда и только тогда, когда для всех $g \in G$ $LC(g) = 1$ и $< LT(G) >$ является минимальным базисом полиномиального идеала $< LT(I) >$.*

Доказательство. Пусть G – минимальный базис Грёбнера полиномиального идеала $I \subset k[x_1,\ldots,x_n]$. Тогда для всех $g \in G$ $LC(g) = 1$, $< LT(I) > = < LT(G) >$, а значит, $LT(G)$ – базис мономиального идеала $< LT(I) >$. Базис $LT(G)$ является минимальным базисом мономиального идеала $< LT(I) >$, так как для всех $g \in G$ $LT(g) \notin < LT(G - \{g\}) >$, т.е. никакой моном $LT(g) \in LT(G)$ не делится ни на один из мономов, принадлежащих множеству $LT(G - \{g\})$. Пусть теперь для всех $g \in G$

LC(g) = 1 и LT(G) является минимальным базисом мономиального идеала < LT(I) >. Тогда для всех $g \in G$ LT(g) $\notin$ < LT($G - \{g\}$) >, так как никакой моном LT(g) $\in$ LT(G) не делится ни на один из мономов, принадлежащих множеству LT($G - \{g\}$). Следовательно, G – минимальный базис Грёбнера идеала I. □

Минимальный базис Грёбнера для ненулевого идеала $I \subset k[x_1,\ldots,x_n]$ можно построить с помощью алгоритма из теоремы 1 с последующим применением теоремы 2 для исключения лишних образующих. Идеал может иметь несколько минимальных базисов Грёбнера. Однако

Теорема 4. *Пусть задано некоторое мономиальное упорядочение, и пусть G и $\tilde{G}$ – минимальные базисы Грёбнера идеала $I \subset k[x_1,\ldots,x_n]$. Тогда LT(G) = LT($\tilde{G}$).*

Доказательство. Пусть G и $\tilde{G}$ – минимальные базисы Грёбнера идеала I. Тогда на основании теоремы 3 заключаем, что LT(G) и LT($\tilde{G}$) – минимальные базисы мономиального идеала < LT(I) >. Из теоремы 4 п. 1.4 заключаем, что LT(G) = LT($\tilde{G}$). □

Определение 2. Пусть G – минимальный базис Грёбнера идеала $I \subset k[x_1,\ldots,x_n]$. Элемент $g \in G$ называется *редуцированным* для G, если никакой моном из g не принадлежит < LT($G - \{g\}$) >.

Определение 3. *Редуцированным базисом Грёбнера* идеала $I \subset k[x_1,\ldots,x_n]$ называется его минимальный базис Грёбнера G такой, что все элементы базиса G являются редуцированными для G.

Теорема 5. *Пусть $I \neq \{0\}$ – идеал из $k[x_1,\ldots,x_n]$, и пусть задано некоторое мономиальное упорядочение. Тогда существует единственный редуцированный базис Грёбнера идеала I.*

Доказательство. Пусть G – некоторый минимальный базис Грёбнера идеала I. Будем преобразовывать G до тех пор, пока все его элементы не станут редуцированными. Пусть $g \in G$. Положим $g' = \overline{g}^{G-\{g\}}$ и $G' = (G - \{g\})$ **U** $\{g'\}$. Покажем, что G' является минимальным базисом Грёбнера для I. Действительно, имеем LT(g') = LT(g), ибо при делении g на $G - \{g\}$ LT(g) пойдет в остаток, так как этот моном не делится ни на один элемент из LT($G - \{g\}$) в силу минимальности базиса G. Следовательно, < LT(G') > = < LT(G) >. Так как $G' \subset I$, то G' – базис Грёбнера для I, причем минимальный ввиду минимальности G. Далее элемент g' является редуцированным для G', ибо никакой моном из g' не принадлежит < LT($G' - \{g'\}$) > ввиду свойства алгоритма деления. Преобразуем таким способом каждый элемент из G. Заметим, что базис Грёбнера может из-

мениться при каждом преобразовании G. Однако если элемент становится редуцированным, то он останется таковым и при дальнейших преобразованиях элементов из G, так как старшие члены в G при этом не меняются. В конце концов мы получим редуцированный базис Грёбнера. Докажем его единственность. Пусть G и $\tilde{G}$ – редуцированные, а значит, и минимальные базисы Грёбнера идеала I. Из теоремы 4 имеем LT(G) = LT($\tilde{G}$). Отсюда для каждого $g \in G$ существует $\tilde{g} \in \tilde{G}$ такой, что LT(g) = LT($\tilde{g}$). Докажем, что $g = \tilde{g}$. Имеем $g - \tilde{g} \in I$, а так как G – базис Грёбнера для I, то $\overline{g - \tilde{g}}^{G} = 0$. Но LT($g$) = LT($\tilde{g}$), т.е. старшие члены в $g - \tilde{g}$ сократились, а оставшиеся члены не делятся ни на один элемент из LT(G) = LT($\tilde{G}$) в силу редуцированности базисов G, $\tilde{G}$. Поэтому из $\overline{g - \tilde{g}}^{G} = 0$ следует $g = \tilde{g}$. Следовательно, $G = \tilde{G}$. □

1.8. УСОВЕРШЕНСТВОВАНИЯ АЛГОРИТМА ВЫЧИСЛЕНИЯ БАЗИСОВ ГРЁБНЕРА

Определение 1. Пусть задано мономиальное упорядочение и множество $G \subset k[x_1,\ldots,x_n]$. Функция $f \in k[x_1,\ldots,x_n]$ называется *редуцируемой к нулю* по модулю G, если f может быть представлена в виде $f = \sum_{i=1}^{n} a_i g_i$, причем multideg($f$) ≥ multideg($a_i g_i$), если $a_i g_i \neq 0$. Это записывается так: $f \to_G 0$.

Лемма 1. *Пусть $G = (g_1,\ldots,g_s)$ – упорядоченное множество элементов из $k[x_1,\ldots,x_n]$ и пусть дана функция $f \in k[x_1,\ldots,x_n]$. Тогда если $\overline{f}^{G} = 0$, то $f \to_G 0$. Обратное утверждение, как правило, неверно.*

Доказательство. Если $\overline{f}^{G} = 0$, то из алгоритма деления следует, что $f = \sum_{i=1}^{n} a_i g_i$. При этом multideg($f$) ≥ multideg($a_i g_i$), если $a_i g_i \neq 0$, т.е. $f \to_G 0$. Покажем, что обратное утверждение не всегда выполняется. Пусть G = ($xy + 1$, $y^2 - 1$) с lex-упорядочением. В этом случае $\overline{xy^2 - x}^{G} = -x - y$, так как $xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$. С другой стороны $xy^2 - x = 0(xy + 1) + x(y^2 - 1)$, т.е. $xy^2 - x \to_G 0$. □

Дадим более общую формулировку теоремы 1 п. 1.6.

Теорема 1. *Базис $G = \{g_1,\ldots,g_s\}$ идеала I является базисом Грёбнера тогда и только тогда, когда для всех $i \neq j$ $S(g_i, g_j) \to_G 0$.*

Заметим, что в теореме 1 п. 1.6 условие формулировалось так: для всех $i \neq j$ $\overline{S(g_i, g_j)}^G = 0$.

Доказательство. Если $S(g_i, g_j) \to_G 0$, то $S(g_j, g_l) = \sum_{i=1}^{s} a_{ijl} g_i$, где multideg$(a_{ijl}g_i) \leq$ multideg$(S(g_j, g_l))$. Дальнейшее в точности повторяет доказательство теоремы 1 п. 1.6. □

Предложение 1. *Пусть дано конечное множество $G \subset k[x_1,\ldots,x_n]$, и пусть $f, g \in G$ таковы, что $LCM(LM(f), LM(g)) = LM(f)\cdot LM(g)$, т.е. старшие мономы полиномов f и g взаимно просты. Тогда $S(f, g) \to_G 0$.*

Доказательство. Предположим для простоты, что LC(f) = LC(g) = 1. Тогда f = LM(f) + p, g = LM(g) + q. Из условия теоремы имеем

$$S(f, g) = \frac{\mathrm{LM}(f)\,\mathrm{LM}(g)\,f}{\mathrm{LM}(f)} - \frac{\mathrm{LM}(f)\,\mathrm{LM}(g)\,g}{\mathrm{LM}(g)} = \mathrm{LM}(g)f - \mathrm{LM}(f)g =$$

$$= (g - q)f - (f - p)g = gf - qf - fg + pg = pg - qf. \qquad (1)$$

Докажем, что

$$\mathrm{multideg}(S(f, g)) = \max(\mathrm{multideg}(pg), \mathrm{multideg}(qf)). \qquad (2)$$

Для этого покажем, что в полиноме $pg - qf$ старшие мономы полиномов pg и qf различны. Действительно, если бы они были одинаковыми, то LM(p)LM(g) = LM(q)LM(f), т.е. LM$(p) = \frac{\mathrm{LM}(q)\,\mathrm{LM}(f)}{\mathrm{LM}(g)}$. Так как LM$(f)$ и LM(g) взаимно просты, то LM(q) делится на LM(g). Но это невозможно, ибо LM(g) > LM(q). Из (1), (2) вытекает, что $S(f, g) \to_G 0$. □

Заметим, что предложение 1 позволяет усовершенствовать теорему 1: достаточно проверить условие $S(g_i, g_j) \to_G 0$, $i < j$, только в тех случаях, когда LM(g_i) и LM(g_j) не взаимно просты.

Определение 2. Пусть $F = (f_1,\ldots,f_s)$. *Сизигией старших членов* LT(f_1),…,LT(f_s) называется S-полином $S = (h_1,\ldots,h_s) \in (k[x_1,\ldots,x_n])^S$ такой, что $\sum_{i=1}^{s} h_i\,\mathrm{LT}(f_i) = 0$. Будем обозначать через $S(F)$ подмножество в $(k[x_1,\ldots,x_n])^S$, состоящее из всех сизигий старших членов набора F.

Обозначим через e_i набор $(0,\ldots,0,\ 1,\ 0,\ldots,0) \in (k[x_1,\ldots,x_n])^S$, где 1 стоит на i-м месте. Тогда сизигия $S \in S(F)$ может быть записана в виде $S = \sum_{i=1}^{s} h_i e_i$. В качестве примера использования этих обозначений рассмотрим сизигии, порожденные S-полиномами. Для этого рассмотрим $\{f_i, f_j\} \subset F$, где $i < j$ и пусть $x^\gamma = \mathrm{LCM}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))$. Тогда

$$S_{ij} = \frac{x^\gamma}{\mathrm{LT}(f_i)} e_i - \frac{x^\gamma}{\mathrm{LT}(f_j)} e_j \qquad (3)$$

является сизигией старших членов набора F, так как $\frac{x^\gamma}{\mathrm{LT}(f_i)}\mathrm{LT}(f_i) - \frac{x^\gamma}{\mathrm{LT}(f_j)}\mathrm{LT}(f_j) = 0$.

Предложение 2. *Пусть $S = (c_1,\ldots,c_s)$, $T = (d_1,\ldots,d_s) \in (k[x_1,\ldots,x_n])^S$ – сизигии старших членов набора $F = (f_1,\ldots,f_s)$. Тогда $S + T$ и gS, где $g \in k[x_1,\ldots,x_n]$, также являются сизигиями.*

Доказательство. Так как S и T – сизигии, то $\sum_{i=1}^{s} c_i \mathrm{LT}(f_i) = 0$, $\sum_{i=1}^{s} d_i \mathrm{LT}(f_i) = 0$. Имеем $\sum_{i=1}^{s} (c_i + d_i)\mathrm{LT}(f_i) = \sum_{i=1}^{s} c_i \mathrm{LT}(f_i) + \sum_{i=1}^{s} d_i \mathrm{LT}(f_i) = 0$, $\sum_{i=1}^{s} g c_i \mathrm{LT}(f_i) = g\sum_{i=1}^{s} c_i \mathrm{LT}(f_i) = 0$, т.е. $S + T$ и gS – сизигии. □

Определение 3. Элемент $S \in S(F)$ называется *однородным* мультистепени α, где $\alpha \in \mathbf{Z}^n_{\geq 0}$, если $S = (c_1 x^{\alpha(1)},\ldots,c_s x^{\alpha(s)})$, где $c_i \in k$ и $\alpha(i) + \mathrm{multideg}(f_i) = \alpha$ при $c_i \neq 0$.

Предложение 3. *Сизигия S_{ij} из (3) является однородной мультистепени γ.*

Доказательство. Сизигия S_{ij} из (3) является однородной мультистепени γ, так как $S_{ij} = \frac{1}{\mathrm{LC}(f_i)} x^{\gamma - \mathrm{multideg}(f_i)} e_i - \frac{1}{\mathrm{LC}(f_j)} x^{\gamma - \mathrm{multideg}(f_j)} e_j$ и $\gamma - \mathrm{multideg}(f_i) + \mathrm{multideg}(f_i) = \gamma - \mathrm{multideg}(f_j) + \mathrm{multideg}(f_j) = \gamma$. □

Лемма 2. *Каждый элемент из $S(F)$ единственным образом может быть разложен в сумму однородных сизигий из $S(F)$.*

Доказательство. Пусть $S = (h_1,\ldots,h_s) \in S(F)$. Зафиксируем вектор $\alpha \in \mathbf{Z}^n_{\geq 0}$. Пусть $h_{i\alpha}$ – член полинома h_i (если он существует) такой, что multideg$(h_{i\alpha}f_i) = \alpha$. Тогда $\sum_{i=1}^{s} h_{i\alpha}\,\mathrm{LT}(f_i) = 0$, так как $h_{i\alpha}\mathrm{LT}(f_i)$, $i = \overline{1,s}$, – это все члены степени α в $\sum_{i=1}^{s} h_i\,\mathrm{LT}(f_i) = 0$. Таким образом, $S_\alpha = (h_{1\alpha},\ldots,h_{s\alpha}) \in S(F)$ – однородный элемент мультистепени α и $S = \sum_{\alpha} S_\alpha$. Докажем единственность S_α. Пусть $\sum_{\alpha} S'_\alpha$, где S_α' – однородный элемент степени α из $S(F)$. Тогда $S_\alpha' = (h'_{1\alpha},\ldots,h'_{s\alpha})$, где $h'_{i\alpha} = \mathrm{LC}(h_{i\alpha})\, x^{\alpha-\mathrm{multideg}(f_i)}$, так как $h'_{i\alpha}\mathrm{LT}(f_i) = \mathrm{LC}(h_{i\alpha})\mathrm{LC}(f_i)x^\alpha$. □

Докажем теперь, что S_{ij} образуют базис всех сизигий старших членов.

Предложение 4. *Если $F = (f_1,\ldots,f_s)$, то каждая сизигия $S \in S(F)$ может быть представлена в виде*

$$S = \sum_{i<j} a_{ij} S_{ij}\,, \tag{4}$$

где $a_{ij} \in k[x_1,\ldots,x_n]$, а сизигии S_{ij} определены в (3).

Доказательство. Так как по лемме 2 любую сизигию можно представить в виде однородных сизигий, то не умаляя общности мы можем считать S однородной сизигией мультистепени α. Сизигия S имеет по меньшей мере две ненулевые компоненты, например $c_i x^{\alpha(i)}$ и $c_i x^{\alpha(j)}$, где $i < j$ и $\alpha(i)$ + multideg(f_i) = $\alpha(j)$ + multideg(f_j) = α. Отсюда следует, что x^γ = LCM(LM(f_i), LM(f_j)) делит x^α. Так как $S_{ij} = \dfrac{x^\gamma}{\mathrm{LT}(f_i)}e_i - \dfrac{x^\gamma}{\mathrm{LT}(f_j)}e_j$, то i-я компонента сизигии $S - c_i\mathrm{LC}(f_i)x^{\alpha-\gamma}S_{ij}$ равна нулю, а все другие компоненты, кроме j-й, не изменились. Таким образом, построена новая однородная сизигия, у которой количество ненулевых компонент меньше, чем у S. Продолжая этот процесс, мы представим S в виде (4). □

Теорема 2. *Базис $G = \{g_1,\ldots,g_s\}$ идеала I является его базисом Грёбнера тогда и только тогда, когда для каждого элемента $S = (h_1,\ldots,h_s)$ из однородного базиса пространства сизигий $S(G)$ выполняется условие* $S(G) = \sum_{i=1}^{s} h_i g_i \;\to_G 0$.

Доказательство. Будем следовать схеме доказательства теоремы 1 п. 1.6. Для любого $f \in I$ $f = \sum_{i=1}^{s} h_i g_i$. Пусть m($i$) = multideg($h_i g_i$), δ = $\max_i(m(i))$. Мы выбираем такое представление f в виде линейной комбинации g_i, чтобы мультистепень δ была минимальной. Предположение multideg(f) < δ должно привести нас к противоречию. В силу формулы (3) из п. 1.6 из неравенства multideg(f) < δ следует, что multideg($\sum_{m(i)=\delta} LT(h_i) g_i$) < δ. Это означает, что $\sum_{m(i)=\delta} LT(h_i) LT(g_i) = 0$. Поэтому $S = \sum_{m(i)=\delta} LT(h_i) e_i$ является сизигией из $S(G)$. Заметим, что S – однородная сизигия мультистепени δ. Пусть $S_1,\ldots,S_m$ – однородный базис пространства сизигий. Из условии теоремы следует, что для любого j $S_j G \to_G 0$. Запишем S в виде

$$S = \sum_{j=1}^{m} u_j S_j , \tag{5}$$

где $u_j \in k[x_1,\ldots,x_n]$. Разложение u_j в сумму членов позволяет нам представить S в виде суммы однородных сизигий. Так как S – однородная сизигия мультистепени δ, то на основании леммы 2 из единственности представления следует, что в (5) или $u_j = 0$ или $u_j S_j$ – однородная сизигия мультистепени δ. Пусть S_j имеет мультистепень γ_j. Если $u_j \neq 0$, то $u_j = c_j x^{\delta-\gamma_j}$, где $c_j \in k$. Таким образом, из (5) находим $S = \sum_j c_j x^{\delta-\gamma_j} S_j$, где сумма берется по таким j, для которых $u_j \neq 0$. Скалярно умножая это равенство на G, получаем

$$\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = S \cdot G = \sum_j c_j x^{\delta-\gamma_j} S_j \cdot G. \tag{6}$$

По условию

$$S_j G \to_G 0, \text{ т.е. } S_j G = \sum_{i=1}^{s} a_{ij} g_i , \tag{7}$$

где для всех i, j

$$\mathrm{multideg}(a_{ij} g_i) \le \mathrm{multideg}(S_j G). \tag{8}$$

Так как S_j – однородная сизигия мультистепени γ_j, то multideg(S_jG) < γ_j. Отсюда с учетом (8) multideg($a_{ij}g_i$) < γ_j. Из (7) имеем $x^{\delta-\gamma_j} S_jG = x^{\delta-\gamma_j} \sum_{i=1}^{s} a_{ij} g_i = \sum_{i=1}^{s} b_{ij} g_i$, где $b_{ij} = x^{\delta-\gamma_j} a_{ij}$, multideg($b_{ij}g_i$) < δ. Таким образом, из (6) находим $\sum_{m(i)=\delta} \mathrm{LT}(h_i) g_i = \sum_j c_j \sum_{i=1}^{s} b_{ij} g_i = \sum_{i=1}^{s} \tilde{h}_i g_i$, где multideg($\tilde{h}_i g_i$) < δ. Далее доказательство повторяет доказательство теоремы 1 п. 1.6. □

Отметим, что теорема 2 является частным случаем теоремы 1 п. 1.6. А именно, если мы возьмем $\{S_{ij}\}$ в качестве базиса пространства сизигий $S(G)$, то анализ полиномов $S_{ij}G$ будет происходить точно так же, как происходил ранее анализ S-полиномов $S(g_i, g_j)$.

Предложение 5. *Пусть $G = (g_1,\ldots,g_s)$, и пусть подмножество $S \subset \{S_{ij} : 1 \le i < j \le s\}$ является базисом в $S(G)$. Предположим, что существуют три разных полинома $g_i, g_j, g_l \in G$ такие, что $LT(g_l)$ делит $LCM(LT(g_i), LT(g_j))$. Если $S_{il}, S_{jl} \in S$, то $S – \{S_{ij}\}$ также является базисом в $S(G)$ (если $i > j$, то полагаем $S_{ij} = S_{ji}$).*

Доказательство. Пусть для определенности $i < j < l$. Положим $x^{\gamma_{ij}} = \mathrm{LCM}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$, $x^{\gamma_{il}} = \mathrm{LCM}(\mathrm{LM}(g_i), \mathrm{LM}(g_l))$, $x^{\gamma_{jl}} = \mathrm{LCM}(\mathrm{LM}(g_j), \mathrm{LM}(g_l))$. Тогда $\mathrm{LT}(g_i)$, $\mathrm{LT}(g_j)$, $\mathrm{LT}(g_l)$ делят $x^{\gamma_{ij}}$. Следовательно, $x^{\gamma_{il}}$ делит $x^{\gamma_{ij}}$. Аналогично, $x^{\gamma_{jl}}$ делит $x^{\gamma_{ij}}$. Покажем, что $S_{ij} = x^{\gamma_{ij}-\gamma_{il}} S_{il} - x^{\gamma_{ij}-\gamma_{il}} S_{jl}$. Действительно, $x^{\gamma_{ij}-\gamma_{il}} S_{il} - x^{\gamma_{ij}-\gamma_{il}} S_{jl} = x^{\gamma_{ij}-\gamma_{il}} \left(\frac{x^{\gamma_{il}}}{\mathrm{LT}(g_i)} e_i - \frac{x^{\gamma_{il}}}{\mathrm{LT}(g_l)} e_l \right) - x^{\gamma_{ij}-\gamma_{il}} \left(\frac{x^{\gamma_{jl}}}{\mathrm{LT}(g_j)} e_j - \frac{x^{\gamma_{il}}}{\mathrm{LT}(g_l)} e_l \right) = \left(\frac{x^{\gamma_{ij}}}{\mathrm{LT}(g_i)} e_i - \frac{x^{\gamma_{ij}}}{\mathrm{LT}(g_j)} e_j \right) = S_{ij}$.

Следовательно, $S – \{S_{ij}\}$ – базис в $S(G)$. □

Предложение 5 показывает, как из базиса $\{S_{ij}, i < j\}$можно исключать «лишние» элементы.

Введем следующее обозначение:

$$[i, j] = \begin{cases} (i, j), \text{если } i < j, \\ (j, i), \text{если } i > j. \end{cases}$$

Из предложения 1, предложения 5 и теоремы 2 вытекает следующая *усовершенствованная версия алгоритма Бухбергера*.

Теорема 3. *Пусть* $I = < f_1,\ldots,f_s > -$ *полиномиальный идеал. Его базис Грёбнера может быть построен за конечное число шагов с использованием следующего алгоритма:*

Вход: $F = (f_1,\ldots,f_s)$
Выход: G, базис Грёбнера идеала $I = < f_1,\ldots,f_s >$
{инициализация}
B: = $\{(i, j) \mid 1 \le i < j \le s\}$
G: = F
t: = s
{итерация}
WHILE $B \neq \varnothing$ DO
Выбрать $(i, j) \in B$
IF LCM(LT(f_i), LT(f_j)) ≠ LT(f_i)LT(f_j) AND
критерий (f_i, f_j, B) не выполняется THEN
S: = $\overline{S(f_i, f_j)}^{G}$
IF $S \neq 0$ THEN
t: = $t + 1$; f_t: = S
G: = G **U** $\{f_t\}$
B: = B **U** $\{(i, t) \mid 1 \le i \le t - 1\}$
B: = $B - \{(i, j)\}$.

Здесь критерий (f_i, f_j, B) выполняется >>, если существует некоторое $l \notin \{i, j\}$, для которого пары $[i, l]$ и $[j, l]$ не принадлежат B и LT(f_l) делит LCM(LT(f_i), LT(f_j)) (основа этого критерия – предложение 5).

В этом алгоритме вводится список пар B, которые нужно проверить. Здесь мы вычисляем остаток от деления только для тех S-полиномов $S(f_i, f_j)$, которые не удовлетворяют условиям предложения 1 или предложения 5.

1.9. СИЗИГИИ БАЗИСОВ ИДЕАЛА

Определение 1. Пусть идеал $I = < f_1,\ldots,f_s > \subset k[x_1,\ldots,x_n]$. *Сизигией базиса* $F = (f_1,\ldots,f_s)$ идеала I называется элемент $h = (h_1,\ldots,h_s) \subset (k[x_1,\ldots,x_n])^s$, удовлетворяющий условию $\sum_{i=1}^{s} h_i f_i = 0$. Будем обозначать через Syz(F) подмножество в $(k[x_1,\ldots,x_n])^s$, состоящее из всех сизигий набора F.

Будем предполагать, что мы имеем фиксированное мономиальное упорядочение в $k[x_1,\ldots,x_n]$.

Пусть $G = < g_1,\ldots,g_t >$, где $\mathrm{LC}(g_i) = 1$, – базис Грёбнера идеала $I = < f_1,\ldots,f_s >$. Найдем $\mathrm{Syz}(g_1,\ldots,g_t)$. Имеем $\mathrm{Syz}(\mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t)) = S(G)$. *Базисом пространства сизигий* $S(G)$ является множество $\{S_{ij},\ 1 \le i < j \le s\}$, где $S_{ij} = \dfrac{x^{\gamma_{ij}}}{\mathrm{LM}(g_i)} e_i - \dfrac{x^{\gamma_{ij}}}{\mathrm{LM}(g_j)} e_j$, $x^{\gamma_{ij}} = \mathrm{LCM}(\mathrm{LM}(g_i), \mathrm{LM}(g_j))$.

Для g_i, g_j S-полином имеет вид $S(g_i, g_j) = \dfrac{x^{\gamma_{ij}}}{\mathrm{LM}(g_i)} g_i - \dfrac{x^{\gamma_{ij}}}{\mathrm{LM}(g_j)} g_j$. С помощью алгоритма деления находим $S(g_i, g_j) = \sum\limits_{\nu=1}^{t} h_{ij\nu} g_\nu$, где $h_{ij\nu} \in k[x_1,\ldots,x_n]$, $\max\limits_{1\le\nu\le t} (\mathrm{LM}(h_{ij\nu})\mathrm{LM}(g_\nu)) = \mathrm{LM}(S(g_i, g_j))$.

Для всех $i, j = 1,\ldots,t,\ i \ne j$, определяем $s_{ij} = \dfrac{x^{\gamma_{ij}}}{\mathrm{LM}(g_i)} e_i - \dfrac{x^{\gamma_{ij}}}{\mathrm{LM}(g_j)} e_j - \sum\limits_{\nu=1}^{t} h_{ij\nu} e_\nu$. Заметим, что $s_{ij} \in \mathrm{Syz}(g_1,\ldots,g_t)$, так как $\left(\sum\limits_{k=1}^{t} g_k e_k\right) s_{ij} = \left(\sum\limits_{k=1}^{t} g_k e_k\right)\left(\dfrac{x^{\gamma_{ij}}}{\mathrm{LM}(g_i)} e_i - \dfrac{x^{\gamma_{ij}}}{\mathrm{LM}(g_j)} e_j\right) - \left(\sum\limits_{k=1}^{t} g_k e_k\right)\left(\sum\limits_{\nu=1}^{t} h_{ij\nu} e_\nu\right) = S(g_i, g_j) - \sum\limits_{\nu=1}^{t} h_{ij\nu} g_\nu = 0$.

Теорема 1. *Совокупность $\{s_{ij},\ 1 \le i < j \le t\}$ образует базис пространства сизигий $\mathrm{Syz}(g_1,\ldots,g_t)$.*

Доказательство. Пусть $u = \sum\limits_{\nu=1}^{t} u_\nu e_\nu \in \mathrm{Syz}(g_1,\ldots,g_t)$. Пусть $x^\alpha = \max\limits_{1\le i\le t} (\mathrm{LM}(u_i)\ \mathrm{LM}(g_i))$. Положим $S = \{i \in \{1,\ldots,t\} \mid \mathrm{LM}(u_i)\mathrm{LM}(g_i) = x^\alpha\}$. Для любого $i \in \{1,\ldots,t\}$ определим u_i' следующим образом:

$$u_i' = \begin{cases} u_i, & \text{если } i \notin S, \\ u_i - LT(u_i), & \text{если } i \in S. \end{cases}$$

Пусть для $i \in S$ $\mathrm{LT}(u_i) = c_i x^{\alpha_i}$. Так как $u \in \mathrm{Syz}(g_1,\ldots,g_t)$, то $\sum_{i\in S} c_i x^{\alpha_i} \mathrm{LT}(g_i) = 0$. Таким образом, $\sum_{i\in S} c_i x^{\alpha_i} \in S(G)$. Следовательно, $\sum_{i\in S} c_i x^{\alpha_i} e_i = \sum_{i<j} a_{ij} S_{ij}$, где $a_{ij} \in k[x_1,\ldots,x_n]$. Из доказательства предложения 4 п. 1.8 следует, что $a_{ij} = d_{ij} x^{\alpha-\alpha_{ij}}$, где $d_{ij} \in k$. Таким образом, мы имеем

$$\sum_{j=1}^{t} u_j e_j = \sum_{i\in S} c_i x^{\alpha_i} e_i + \sum_{j=1}^{t} u_j' e_j = \sum_{\substack{i<j \\ i,j\in S}} a_{ij}\left(\frac{x^{\gamma_{ij}}}{\mathrm{LM}(g_i)} - \frac{x^{\gamma_{ij}}}{\mathrm{LM}(g_j)}\right) + \sum_{j=1}^{t} u_j' e_j =$$

$$\sum_{\substack{i<j \\ i,j\in S}} a_{ij} s_{ij} + \sum_{\nu=1}^{t} u_\nu' e_\nu + \sum_{\substack{i<j \\ i,j\in S}} a_{ij}\left(h_{ij1}e_1 + \ldots + h_{ijt}e_t\right).$$

Так как $\sum_{i<j} a_{ij} s_{ij} \in \mathrm{Syz}(g_1,\ldots,g_t)$, то $\sum_{\nu=1}^{t} u_\nu' e_\nu + \sum_{\substack{i<j \\ i,j\in S}} a_{ij}\left(h_{ij1}e_1 + \ldots + h_{ijt}e_t\right) \in \mathrm{Syz}(g_1,\ldots,g_t)$

Положим $\sum_{\nu=1}^{t} v_\nu e_\nu = \sum_{\nu=1}^{t} u_\nu' e_\nu + \sum_{\substack{i<j \\ i,j\in S}} a_{ij}\left(h_{ij1}e_1 + \ldots + h_{ijt}e_t\right)$.

Пусть $x^\beta = \max_{1\le\nu\le t}(\mathrm{LM}(v_\nu)\mathrm{LM}(g_\nu))$. Покажем, что $x^\beta < x^\alpha$. Действительно, для любого $\nu \in \{1,\ldots,t\}$ $\mathrm{LM}(v_\nu)\mathrm{LM}(g_\nu) = \mathrm{LM}(u_\nu' + \sum_{\substack{i<j \\ i,j\in S}} a_{ij} h_{ij\nu})\mathrm{LM}(g_\nu) \le \max(\mathrm{LM}(u_\nu'), \max_{\substack{i<j \\ i,j\in S}}(\mathrm{LM}(a_{ij})\mathrm{LM}(h_{ij\nu}))\mathrm{LM}(g_\nu)$. Из определения u_ν' имеем $\mathrm{LM}(u_\nu')\mathrm{LM}(g_\nu) < x^\alpha$. Так как $a_{ij} = d_{ij} x^{\alpha-\gamma_{ij}}$, то для любых $i, j \in S$, $i < j$, имеем $\mathrm{LM}(a_{ij})\mathrm{LM}(h_{ij\nu})\mathrm{LM}(g_\nu) = x^{\alpha-\gamma_{ij}} \mathrm{LM}(h_{ij\nu})\mathrm{LM}(g_\nu) \le x^{\alpha-\gamma_{ij}} \mathrm{LM}(S(g_i, g_j)) < x^{\alpha-\gamma_{ij}} x^{\gamma_{ij}} = x^\alpha$. Следовательно, для любого $\nu \in \{1,\ldots,t\}$ $\mathrm{LM}(v_\nu)\mathrm{LM}(g_\nu) < x^\alpha$, т.е. $x^\beta < x^\alpha$.

Далее аналогично случаю сизигии $\sum_{i=1}^{t} u_i e_i$ сизигию $\sum_{\nu=1}^{t} v_\nu e_\nu$ представляем в виде $\sum_{\nu=1}^{t} v_\nu e_\nu = \sum_{i<j} b_{ij} s_{ij} + \sum_{\nu=1}^{t} \omega_\nu e_\nu$, где для сизигии $\sum_{\nu=1}^{t} \omega_\nu e_\nu$

$\max(\mathrm{LM}(\omega_v), \mathrm{LM}(g_v)) < x^{\beta}$. Продолжая этот процесс, мы представляем сизигию u в виде $\sum_{i=1}^{t} u_i e_i = \sum_{i<j} \gamma_{ij} s_{ij}$, где $\gamma_{ij} \in k[x_1,\ldots,x_n]$. □

Будем теперь находить сизигии $F = \{f_1,\ldots,f_s\}$ идеала $I = < f_1,\ldots,f_s >$, базисом Грёбнера которого является множество $G = \{g_1,\ldots,g_t\}$. Используя алгоритм деления, получаем $f_l = \sum_{i=1}^{t} g_i h_{il}$, $l = \overline{1,s}$, где $h_{il} \in k[x_1,\ldots,x_n]$. Положим $F = (f_1,\ldots,f_s)$, $G = (g_1,\ldots,g_t)$, $H = \begin{pmatrix} h_{11} & \mathbf{L} & h_{1s} \\ \mathbb{M} & & \mathbb{M} \\ h_{t1} & \mathbf{L} & h_{ts} \end{pmatrix}$. Тогда $F = GH$. Так как $g_i \in < f_1,\ldots,f_s >$, $i = \overline{1,t}$, то существует матрица $W = \begin{pmatrix} w_{11} & \mathbf{L} & w_{1t} \\ \mathbb{M} & & \mathbb{M} \\ w_{s1} & \mathbf{L} & w_{st} \end{pmatrix}$, где $w_{ij} \in k[x_1,\ldots,x_n]$, такая, что $G = FW$. Элементы матрицы W могут быть найдены в результате выполнения алгоритма Бухбергера при нахождении базиса Грёбнера G идеала I. На основании теоремы 1 найдем базис пространства сизигий $\mathrm{Syz}(g_1,\ldots,g_t)$, состоящий из $\{s_{ij},\ 1 \le i < j \le t\}$. Из координат векторов s_{ij} образуем векторы-столбцы s_i, $i = \overline{1,r}$, где r – количество всех s_{ij}. Так как множество $\{s_1,\ldots,s_r\}$ образует базис пространства сизигий $\mathrm{Syz}(g_1,\ldots,g_t)$, то для любого i, $i = \overline{1,r}$ $0 = Gs_i = (FW)s_i = F(Ws_i)$. Следовательно, для любого i, $i = \overline{1,r}$, $Ws_i \in \mathrm{Syz}(F)$. Пусть I_s – единичная матрица размера $s \times s$. Тогда $F(I_s - WH) = F - FWH = F - GH = F - F = 0$. Следовательно, столбцы $r_1,\ldots,r_s$ матрицы F принадлежат пространству сизигий $\mathrm{Syz}(F)$.

Теорема 2. *С учетом введенных выше обозначений базисом пространства сизигий Syz(F) является множество* $\{ws_1,\ldots,ws_r,\ r_1,\ldots,r_s\} \subset (k[x_1,\ldots,x_n])^s$.

Доказательство. Возьмем любой $h = \begin{pmatrix} h_1 \\ \mathbb{M} \\ h_s \end{pmatrix} \in \mathrm{Syz}(f_1,\ldots,f_s)$. Тогда $0 = Fh = GHh$, а поэтому $Hh \in \mathrm{Syz}(g_1,\ldots,g_t)$. С учетом определения $s_1,\ldots,s_r$ имеем $Hh = \sum_{i=1}^{r} a_i s_i$, где $a_i \in k[x_1,\ldots,x_n]$. Следовательно, $WHh = W\left(\sum_{i=1}^{r} a_i s_i\right) =$

$\sum_{i=1}^{r} a_i(Ws_i)$. Отсюда $h = h - WHh + WHh = (I_s - WH)h + \sum_{i=1}^{r} a_i(Ws_i) = \sum_{i=1}^{s} h_i r_i$ $+ \sum_{i=1}^{r} a_i(Ws_i)$, а поэтому множество $\{ws_1,\ldots,ws_r, r_1,\ldots,r_s\}$ образует базис пространства сизигий Syz(F). □

ГЛАВА 2. ТЕОРИЯ ИСКЛЮЧЕНИЯ

2.1. ИСКЛЮЧАЮЩИЕ ИДЕАЛЫ

Определение 1. Пусть дан идеал $I = < f_1,\ldots,f_s > \subset k[x_1,\ldots,x_n]$. Тогда *l-м исключающим идеалом* I_l идеала I называется идеал в $k[x_{l+1},\ldots,x_n]$ такой, что $I_l = I \cap k[x_{l+1},\ldots,x_n]$.

Таким образом, идеал I_l состоит из всех полиномиальных следствий системы $f_1 = 0,\ldots,f_s = 0$, которые не зависят от $x_1,\ldots,x_l$. Докажем корректность определения 1, т.е. покажем, что I_l – идеал в $k[x_{l+1},\ldots,x_n]$. Действительно, $0 \in I_l$, ибо $0 \in I$, $0 \in k[x_{l+1},\ldots,x_n]$. Если $f, g \in I$, а значит, $f + g \in I$. Так как $f, g \in k[x_{l+1},\ldots,x_n]$, то и $f + g \in k[x_{l+1},\ldots,x_n]$, т.е. $f + g \in I_l$. Если $f \in I_l$, то для любого $h \in k[x_{l+1},\ldots,x_n]$ $hf \in I$, $hf \in k[x_{l+1},\ldots,x_n]$, а тогда $hf \in I_l$. Таким образом, доказана корректность определения 1.

Предложение 1. *Пусть $I \subset k[x_1,\ldots,x_n]$ – идеал. Тогда для любого l, $l = \overline{0,n-1}$, $I_{l+1} \subset I_l$. При этом положим $I_0 = I$.*

Доказательство. Пусть $f \in I_{l+1}$. Тогда $f \in I$, $f \in k[x_{l+2},\ldots,x_n]$. Отсюда $f \in k[x_{l+1},\ldots,x_n]$, т.е. $f \in I_l$. □

Предложение 2. *Пусть $I \subset k[x_1,\ldots,x_n]$ – идеал. Тогда для любого l, $l = \overline{0,n-1}$, идеал $I_{l+1} \subset k[x_{l+2},\ldots,x_n]$ является первым исключающим идеалом идеала $I_l \subset k[x_{l+1},\ldots,x_n]$.*

Доказательство. Пусть $\tilde{I}_{l+1} \subset k[x_{l+2},\ldots,x_n]$ – первый исключающий идеал идеала $I_l \subset k[x_{l+1},\ldots,x_n]$. Если $f \in \tilde{I}_{l+1}$, то $f \in I_l$ и $f \in k[x_{l+2},\ldots,x_n]$. Отсюда $f \in I$, $f \in k[x_{l+2},\ldots,x_n]$, т.е. $f \in I_{l+1}$. Следовательно, $\tilde{I}_{l+1} \subset I_{l+1}$. Наоборот, если $f \in I_{l+1}$, то на основании предложения 1 $f \in I_l$. Отсюда, и с учетом того, что $f \in I_{l+1}$, имеем $f \in \tilde{I}_{l+1}$. Следовательно, $I_{l+1} \subset \tilde{I}_{l+1}$. □

Определение 2. Мономиальное упорядочение $>$ на $k[x_1,\ldots,x_n]$ называется *упорядочением l-исключающего типа*, где $0 \le l \le n$, если любой моном, содержащий хотя бы одну из переменных $x_1,\ldots,x_l$ больше любого монома из $k[x_{l+1},\ldots,x_n]$.

Мономиальное упорядочение $>_{lex}$ с $x_1 > x_2 > \ldots > x_n$ для любого l, где $0 \le l \le n$, является упорядочением l-исключающего типа.

Теорема 1 (теорема об исключении). *Пусть $I \subset k[x_1,\ldots,x_n]$ – идеал и G – его базис Грёбнера по отношению к мономиальному упорядочению*

l-исключающего типа. Тогда множество $G_l = G \cap k[x_{l+1},\ldots,x_n]$ *является базисом Грёбнера l-го исключающего идеала* $I_l = I \cap k[x_{l+1},\ldots,x_n]$.

Доказательство. По построению $G_l \subset I_l$. Покажем, что $< \mathrm{LT}(I_l) > = < \mathrm{LT}(G_l) >$. Включение $< \mathrm{LT}(G_l) > \subset < \mathrm{LT}(I_l) >$ очевидно. Докажем обратное включение $< \mathrm{LT}(I_l) > \subset < \mathrm{LT}(G_l) >$. Возьмем любой полином $f \in I_l$. Покажем, что $\mathrm{LT}(f)$ делится на некоторый старший член $\mathrm{LT}(g)$, где $g \in G_l$. Так как $f \in I_l$, то $f \in I$. Так как G – базис Грёбнера идеала I, то существует $g \in G$ такой, что $\mathrm{LT}(f)$ делится на $\mathrm{LT}(g)$. Полином $f \in I_l$, а поэтому $\mathrm{LT}(g)$ содержит только переменные $x_{l+1},\ldots,x_n$. Так как используется упорядочение $>$ l-исключающего типа, то любой моном, содержащий хотя бы одну из переменных $x_1,\ldots,x_l$ больше любого монома из $k[x_{l+1},\ldots,x_n]$. Следовательно, из включения $\mathrm{LT}(g) \in k[x_{l+1},\ldots,x_n]$ следует, что $g \in k[x_{l+1},\ldots,x_n]$. Значит, $g \in G_l$. □

Пусть дан идеал $I = < f_1,\ldots,f_s > \subset k[x_1,\ldots,x_n]$. Аффинное многообразие $\mathbf{V}(I) = \{(a_1,\ldots,a_n) \in k^n : f(a_1,\ldots,a_n) = 0 \ \forall \ f \in I\}$. Для идеала I рассмотрим исключающий идеал I_l, где $1 \le l \le n$. Точка $(a_{l+1},\ldots,a_n) \in \mathbf{V}(I_l)$ называется *частичным решением* исходной системы $f_i = 0$, $i = \overline{1,s}$. Чтобы продолжить $(a_{l+1},\ldots,a_n)$ до полного решения системы, нужно добавить одну координату, т.е. нужно найти a_l такое, что $(a_l,\ldots,a_n) \in \mathbf{V}(I_{l-1})$. Если $I_{l-1} = < g_1,\ldots,g_r > \subset k[x_l,\ldots,x_n]$, то $x_l = a_l$ – решение системы уравнений $g_1(x_l, a_{l+1},\ldots,a_n) = 0,\ldots,g_r(x_l, a_{l+1},\ldots,a_n) = 0$.

Предложение 2 показывает, что для нахождения $a_1,\ldots,a_{l-1}$ можно использовать пошаговое продолжение. Когда a_l найдено, с использованием исключающего идеала I_{l-2} находим a_{l-1} и т.д. В дальнейшем будут указаны условия, при которых частичные решения могут быть продолжены до полных решений.

Пусть дано аффинное многообразие $V = \mathbf{V}(f_1,\ldots,f_s) \subset k^n$. Для исключения первых l переменных $x_1,\ldots,x_l$ рассмотрим отображение проекции $\pi_l : k^n \to k^{n-l}$, которое вектор $(a_1,\ldots,a_n)$ переводит в вектор $(a_{l+1},\ldots,a_n)$. Применяя отображение π_l к многообразию $V \subset k^n$, получим множество $\pi_l(V) \subset k^{n-l}$.

Предложение 3. *Пусть* $I_l = < f_1,\ldots,f_s > \subset k[x_{l+1},\ldots,x_n]$ *– l-й исключающий идеал. Тогда* $\pi_l(V) \subset \mathbf{V}(I_l) \subset k^{n-l}$.

Доказательство. Пусть $f \in I_l$. Возьмем любую точку $(a_1,\ldots,a_n) \in V$. Тогда $f(a_1,\ldots,a_n) = 0$, так как $f \in < f_1,\ldots,f_s >$. Здесь f зависит только от $x_{l+1},\ldots,x_n$. Следовательно, $f(a_{l+1},\ldots,a_n) = f(\pi_l(a_1,\ldots,a_n)) = 0$, т.е. f равен нулю во всех точках из $\pi_l(V)$. Отсюда $\pi_l(V) \subset \mathbf{V}(I_l)$. □

Точки множества $\pi_l(V)$ описываются следующим образом:

$$\pi_l(V) = \{(a_{l+1},\ldots,a_n) \in \mathbf{V}(I_l) : \exists\ a_1,\ldots,a_l \in k \text{ такие, что}$$

$$(a_1,\ldots,a_l, a_{l+1},\ldots,a_n) \in V\}.$$

Таким образом, множество $\pi_l(V)$ состоит в точности из тех частичных решений, которые могут быть продолжены до полных. В дальнейшем будут указаны условия, при которых частичные решения могут быть продолжены до полных.

2.2. РЕЗУЛЬТАНТЫ

Определение 1. Полином $f \in k[x_1,\ldots,x_n]$ называется *неприводимым* над полем k, если он не постоянен и не является произведением двух непостоянных полиномов из $k[x_1,\ldots,x_n]$.

Если полином f неприводим, то с точностью до постоянного множителя его делителем может быть только он сам.

Предложение 1. *Каждый непостоянный полином $f \in k[x_1,\ldots,x_n]$ является произведением неприводимых над k полиномов.*

Доказательство. Если f неприводим, то утверждение доказано, если нет, то $f = gh$, где $g, h \in k[x_1,\ldots,x_n]$ – непостоянные полиномы, $\deg(g) < \deg(f)$, $\deg(h) < \deg(f)$. К полиномам g, h применим то же рассуждение, что и к f. Если они приводимы, то их раскладываем в произведение непостоянных множителей с меньшими степенями. Этот процесс завершается за конечное число шагов, так как полная степень уменьшается, когда мы переходим к множителям. Таким образом, f является произведением неприводимых полиномов. □

Теорема 1. *Пусть $f \in k[x_1,\ldots,x_n]$ – неприводимый полином над k. Предположим, что gh, где $g, h \in k[x_1,\ldots,x_n]$ делится на f. Тогда f делит g или h.*

Доказательство. Воспользуемся методом математической индукции. Индукцию будем проводить по числу переменных n. Пусть $n = 1$ и f делит h. Рассмотрим $p = \mathrm{GCD}(f, g)$. Если $\deg(p) > 0$, то с точностью до постоянного множителя $f = p$, так как f неприводим. В этом случае f делит g. Если же $p = 1$, то тогда существуют $A, B \in k[x_1]$ такие, что $Af + Bg = 1$. Умножая это равенство на h, имеем

$$h = h(Af + Bg) = Ahf + Bhg.$$

Так как f делит gh, то $gh = fs$. Следовательно, $h = Ahf + Bfs = f(Ah + Bs)$, т.е. f делит h. Теорема для $n = 1$ доказана.

Пусть теорема справедлива для $n-1$. Сначала рассмотрим случай, когда неприводимый полином не зависит от x_1, т.е. $u \in k[x_2,\ldots,x_n]$ неприводим и делит $gh \in k[x_1,\ldots,x_n]$. Докажем, что u делит g или h. Имеем $g = \sum_{i=0}^{l} a_i x_1^i$, $h = \sum_{j=0}^{m} b_j x_1^j$, где $a_i, b_j \in k[x_2,\ldots,x_n]$. Если u делит каждый полином a_i, то u делит g. Аналогично, если u делит каждый полином b_j, то u делит h. Пусть теперь ни одно, ни другое не выполнено. Тогда существуют $i, j \geq 0$ такие, что u не делит a_i и не делит b_j. Будем считать, что i, j – это наименьшие числа с такими свойствами, т.е. u делит a_r, если $r < i$ и u делит b_s, если $s < j$. Имеем $gh = \sum_{q=0}^{l+m} c_q x_1^q$, где $c_q \in k[x_2,\ldots,x_n]$, $q = \overline{0, l+m}$. В частности,

$$c_{i+j} = (a_0 b_{i+j} + a_1 b_{i+j-1} + \ldots + a_{i-1} b_{j+1}) + a_i b_j + (a_{i+1} b_{j-1} + \ldots + a_{i+j} b_0). \quad (1)$$

Ясно, что u делит каждое слагаемое в первой и во второй скобке. Из индуктивного предположения следует, что u не делит $a_i b_j$. Таким образом, в (1) u делит каждое слагаемое, кроме одного, а значит, u не делит c_{i+j}. Покажем, что u не делит gh. Действительно, если u делит gh, то $\sum_{q=0}^{l+m} c_q x_1^q = u \sum_{q=0}^{l+m} d_q x_1^q$, где $d_q \in k[x_2,\ldots,x_n]$, т.е. $c_q = u d_q$, $q = \overline{0, l+m}$, а значит, u делит c_{i+j}, что невозможно. Заметим, что в рассматриваемом случае u не делит g и u не делит h. В результате получили, что u не делит gh, что противоречит условию теоремы. Таким образом, доказано, что u делит g или h.

Теперь рассмотрим общий случай. Пусть f делит gh. Если f не зависит от x_1, то все доказано. Если f зависит от x_1, то рассмотрим кольцо $k(x_2,\ldots,x_n)[x_1]$. Это кольцо полиномов от одной переменной x_1 над полем $k(x_2,\ldots,x_n)$. Элементами поля $k(x_2,\ldots,x_n)$ являются полиномы из кольца $k[x_2,\ldots,x_n]$. В дальнейшем кольцо $k[x_1,\ldots,x_n]$ будем рассматривать как подкольцо в $k(x_2,\ldots,x_n)[x_1]$. Будем работать в большем кольце, где теорема верна, а затем вернемся в меньшее кольцо. Покажем сначала, что f неприводим в $k(x_2,\ldots,x_n)[x_1]$. Пусть f приводим, т.е. $f = AB$, где A, B – полиномы от x_1 с коэффициентами из $k(x_2,\ldots,x_n)$. Покажем, что или A или B имеет степень 0 по x_1. Пусть $d \in k[x_2,\ldots,x_n]$ – произведение всех знаменателей в A и B. Тогда $\tilde{A} = Ad \in k[x_1,\ldots,x_n]$, $\tilde{B} = Bd \in k[x_1,\ldots,x_n]$, $d^2 f = \tilde{A}\,\tilde{B} \in k[x_1,\ldots,x_n]$. Запишем d^2 как произведение неприводимых множителей из $k[x_2,\ldots,x_n]$, что возможно в силу предложения 1. Каждый из этих множителей делит $\tilde{A}\,\tilde{B}$, а значит, по доказанному каждый из них делит $\tilde{A}$

или $\tilde{B}$. Поделим обе части равенства $d^2f = \tilde{A}\,\tilde{B}$ на эти множители. В результате получим, что $f = \tilde{A}_1\,\tilde{B}_1$, где $\tilde{A}_1$, $\tilde{B}_1 \in k[x_1,\ldots,x_n]$. Так как f неприводим в $k[x_1,\ldots,x_n]$, то $\tilde{A}_1$ или $\tilde{B}_1$ – константа. Так как полиномы $\tilde{A}_1$, $\tilde{B}_1$ были получены из A, B при помощи умножения и деления на полиномы из $k[x_2,\ldots,x_n]$, то отсюда следует, что или A, или B не зависит от x_1. Это и требовалось доказать.

Таким образом, f неприводим в $k(x_2,\ldots,x_n)[x_1]$, а поэтому f делит g или h в $k(x_2,\ldots,x_n)[x_1]$. Пусть, например, $g = Af$, где $A \in k(x_2,\ldots,x_n)[x_1]$. Избавляясь в этом равенстве от знаменателей, получаем $dg = \tilde{A}f$, где $\tilde{A} \in k[x_1,\ldots,x_n]$, $d \in k[x_2,\ldots,x_n]$. По доказанному каждый неприводимый делитель полинома d делит $\tilde{A}$ или f. Этот неприводимый делитель делить f не может, так как f неприводим и имеет положительную степень по x_1. Следовательно, каждый неприводимый делитель полинома d делит $\tilde{A}$. Производя в $dg = \tilde{A}f$ сокращение, получаем $g = \tilde{\tilde{A}}f$, где $\tilde{\tilde{A}} \in k[x_1,\ldots,x_n]$. Таким образом, f делит g в $k[x_1,\ldots,x_n]$. □

Следствие 1. *Пусть полиномы $f, g \in k[x_1,\ldots,x_n]$ имеют положительные степени по x_1. Тогда f и g имеют общий делитель в $k[x_1,\ldots,x_n]$ положительной степени по x_1 тогда и только тогда, когда они имеют общий делитель в $k(x_2,\ldots,x_n)[x_1]$.*

Доказательство. Если f и g имеют общий делитель в $k[x_1,\ldots,x_n]$ положительной степени по x_1, то они, конечно, имеют его и в большем кольце $k(x_2,\ldots,x_n)[x_1]$. Пусть теперь f и g имеют общий делитель $\tilde{h} \in k(x_2,\ldots,x_n)[x_1]$. Имеем $f = \tilde{h}\,\tilde{f}_1$, $g = \tilde{h}\,\tilde{g}_1$, где $\tilde{f}_1$, $\tilde{g}_1 \in k(x_2,\ldots,x_n)[x_1]$. Заметим, что $\tilde{h}$, $\tilde{f}_1$, $\tilde{g}_1$ могут иметь знаменатели – полиномы из $k[x_2,\ldots,x_n]$. Пусть $d \in k[x_2,\ldots,x_n]$ – общий знаменатель полиномов $\tilde{h}$, $\tilde{f}_1$, $\tilde{g}_1$. Положим $h = d\tilde{h}$, $f_1 = d\tilde{f}_1$, $g_1 = d\tilde{g}_1$. Тогда $h, f_1, g_1 \in k[x_1,\ldots,x_n]$. Далее имеем $d^2f = hf_1$, $d^2g = hg_1$. Пусть h_1 – неприводимый делитель полинома h положительной степени по x_1. Так как $\tilde{h} = \dfrac{h}{d}$ имеет положительную степень по x_1, то такой делитель существует. Тогда h_1 делит d^2 или f (по теореме 1). h_1 не может делить d^2, так как $d^2 \in k[x_2,\ldots,x_n]$. Следовательно, h_1 делит f в $k[x_1,\ldots,x_n]$. Рассуждая аналогично, получаем, что h_1 делит g в $k[x_1,\ldots,x_n]$, т.е. h_1 – требуемый общий делитель. □

Теорема 2. *Каждый непостоянный полином $f \in k[x_1,\ldots,x_n]$ может быть записан как произведение неприводимых над k полиномов $f = f_1f_2\ldots f_r$. Более того, если $f = g_1g_2\ldots g_s$ – другое разложение в произведение*

неприводимых над k полиномов, то $r = s$ *и, с точностью до перестановки и до постоянных множителей* $f_i = g_i$.

Доказательство. Существование разложения полинома f на неприводимые множители доказано в предложении 1. Докажем единственность разложения. Допустим, что полином f двумя способами может быть представлен в виде произведения неприводимых множителей: $f = f_1 f_2 \dots f_r$ и $f = g_1 g_2 \dots g_s$, где f_i, g_j неприводимы. Покажем, что f_1 делит некоторый полином g_j, где $1 \le j \le s$. Если ни один из g_j, где $j = \overline{1,s}$, не делится на f_1, то на основании предложения 1 $g_2 \dots g_s$ делится на f_1. Отсюда $g_3 \dots g_s$ делится на f_1. В результате получаем, что $g_{s-1} g_s$ делится на f_1, т.е. f_1 делит g_{s-1} или g_s. Противоречие показывает, что существует j такое, что f_1 делит g_j. Так как g_j неприводим, то с точностью до постоянного множителя $g_j = f_1$. Полагая $g_j = g_1$, а g_1 равным g_j, имеем $g_1 = f_1$. Сокращая обе части равенства $f_1 f_2 \dots f_r = g_1 g_2 \dots g_s$ на f_1, получаем $f_2 \dots f_r = g_2 \dots g_s$. Далее, с точностью до перестановки и до постоянных множителей аналогичным образом находим $f_2 = g_2, \dots, f_r = g_r$. Следовательно, $r \le s$. Очевидно, $s \le r$, а тогда $r = s$ и $f_i = g_i$, $i = \overline{1,r}$. □

Лемма 1. *Пусть* $f, g \in k[x]$ *– полиномы степеней* $l > 0$ *и* $m > 0$ *соответственно.* f *и* g *имеют общий делитель тогда и только тогда, когда существуют* $A, B \in k[x]$ *такие, что*

1) *полиномы* A *и* B *не равны одновременно нулю;*
2) $\deg(A) \le m - 1, \deg(B) \le l - 1;$
3) $Af + Bg = 0.$

Доказательство. Пусть f и g имеют общий делитель $h(x) \in k[x]$. Тогда $f = hf_1$, $g = hg_1$, где f_1, $g_1 \in k[x]$, $\deg(f_1) \le l - 1$, $\deg(g_1) \le m - 1$. Следовательно, $g_1 f + (-f_1 g) = g_1 h f_1 - f_1 h g_1 = 0$, т.е. $A = g_1$, $B = -f_1$ обладают всеми требуемыми свойствами.

Пусть, наоборот, A, B обладают свойствами 1) – 3) из леммы 1. Пусть для определенности $B \ne 0$. Если f и g не имеют общего делителя, то $\mathrm{GCD}(f, g) = 1$, а поэтому существуют $\tilde{A}$, $\tilde{B} \in k[x]$ такие, что $\tilde{A} f + \tilde{B} g = 1$. Тогда $Bg = -Af$ и $B = (\tilde{A} f + \tilde{B} g)B = \tilde{A} Bf + \tilde{B} Bg = \tilde{A} Bf - \tilde{B} Af = (\tilde{A} B - \tilde{B} A)f$, что невозможно ввиду $B \ne 0$, $\deg(f) = l$, $\deg(B) \le l - 1$. Отсюда следует, что f и g имеют общий делитель положительной степени. □

Будем искать A, B, удовлетворяющие условию $Af + Bg = 0$ (1) методом неопределенных коэффициентов. Пусть $A = c_0 x^{m-1} + \dots + c_{m-1}$, $B = d_0 x^{l-1} + \dots + d_{l-1}$, где коэффициенты $c_0, \dots, c_{m-1}$, $d_0, \dots, d_{l-1}$ считаем неизвестными. Условия леммы 1 будут выполняться, если существуют c_i, $d_j \in k$, $i = \overline{0, m-1}$, $j = \overline{0, l-1}$ не все равные нулю, такие, что $Af + Bg = 0$. Пусть

$f = a_0x^l + \ldots + a_l$, $a_0 \neq 0$, $g = b_0x^m + \ldots + b_m$, $b_0 \neq 0$, $a_i, b_j \in k$. Подставим формулы для A, B, f, g в уравнение (1). Сравнивая коэффициенты при одинаковых степенях x, получаем следующую систему:

$$a_0c_0 + b_0d_0 = 0 \text{ (коэффициент при } x^{l+m-1}),$$

$$a_1c_0 + a_0c_1 + b_1d_0 + b_0d_1 = 0 \text{ (коэффициент при } x^{l+m-2}), \qquad (2)$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_lc_{m-1} + b_md_{l-1} = 0 \text{ (коэффициент при } x^0).$$

Однородная линейная система (2) состоит из $l + m$ уравнений с $l + m$ неизвестными. Такая система имеет ненулевое решение тогда и только тогда, когда определитель матрицы коэффициентов системы равен нулю.

Определение 2. Рассмотрим полиномы $f, g \in k[x]$ положительной степени $f = a_0x^l + \ldots + a_l$, $a_0 \neq 0$, $g = b_0x^m + \ldots + b_m$, $b_0 \neq 0$. *Матрицей Сильвестра* $S_x(f, g)$ полиномов f и g относительно x называется матрица коэффициентов системы (2), т.е. $S_x(f, g)$ – это $(l + m)\times(l + m)$-матрица

$$S_x(f,g) = \begin{bmatrix}
a_0 & & & & b_0 & & & \\
a_1 & a_0 & & & b_1 & b_0 & & \\
a_2 & a_1 & \mathbf{O} & & b_2 & b_1 & \mathbf{O} & \\
\vdots & & \mathbf{O} & a_0 & \vdots & & \mathbf{O} & b_0 \\
a_l & & & a_1 & b_m & & & b_1 \\
 & a_l & & & & b_m & & \\
 & & \mathbf{O} & \vdots & & & \mathbf{O} & \vdots \\
 & & & a_l & & & & b_m
\end{bmatrix}$$

Здесь первые m столбцов отведены a_i, оставшиеся l столбцов отведены b_j, пустые места в матрице заняты нулями. *Результантом* $R_x(f, g)$ *полиномов* f и g относительно x называется определитель матрицы Сильвестра: $R_x(f, g) = \det(S_x(f, g))$.

Определение 3. Полином называется *целочисленным*, если его координаты – целые числа.

Предложение 2. *Пусть $f, g \in k[x]$ – полиномы положительной степени. Тогда $R_x(f, g)$ является целочисленным полиномом от коэффициен-*

тов полиномов f, g. Полиномы f и g имеют общий делитель в k[x] только и только тогда, когда $R_x(f, g) = 0$.

Доказательство. Так как определитель матрицы $A = (a_{ij})_{1 \le i, j \le s}$ размера $s \times s$ определяется формулой $\det(A) = \sum_{\sigma} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \ldots a_{s,\sigma(s)}$, где σ пробегает все перестановки множества {1,…,s}, а sgn(σ) = 1, если σ – четная перестановка, и sgn(σ) = – 1, если нечетная, то $R_x(f, g)$ – целочисленный полином от коэффициентов полиномов f и g.

Далее $R_x(f, g) = 0 \Leftrightarrow$ матрица коэффициентов системы (2) вырождена $\Leftrightarrow$ система (2) имеет ненулевое решение.

Теперь предложение 2 вытекает из леммы 1, ибо система (2) имеет ненулевое решение $\Leftrightarrow$ существуют $A, B \in k[x]$, обладающие всеми свойствами из леммы 1. □

Предложение 3. *Пусть* $f, g \in k[x]$ *– полиномы положительной степени. Тогда существуют* $A, B \in k[x]$ *такие, что* $Af + Bg = R_x(f, g)$. *При этом коэффициенты полиномов A и B являются целочисленными полиномами от коэффициентов полиномов f и g.*

Доказательство. Если $R_x(f, g) = 0$, то в качестве A,B можно взять A = 0, B = 0, т.е. в этом случае предложение 3 очевидно справедливо. Пусть теперь $R_x(f, g) \neq 0$. Будем искать решение уравнения

$$\tilde{A} f + \tilde{B} g = 1, \qquad (3)$$

где $\tilde{A}$, $\tilde{B} \in k[x]$. Пусть $f = a_0 x^l + \ldots + a_l$, $a_0 \neq 0$, $g = b_0 x^m + \ldots + b_m$, $b_0 \neq 0$. Полиномы $\tilde{A}$, $\tilde{B}$ будем искать в виде $\tilde{A} = c_0 x^{m-1} + \ldots + c_{m-1}$, $\tilde{B} = d_0 x^{l-1} + \ldots + d_{l-1}$, где коэффициенты $c_0,\ldots,c_{m-1}$, $d_0,\ldots,d_{l-1}$ являются неизвестными из поля k. Если мы подставим f, g, $\tilde{A}$, $\tilde{B}$ в (3) и сравним коэффициенты при одинаковых степенях x, то получим следующую систему с неизвестными c_i, d_j и коэффициентами a_i, b_j:

$$\begin{aligned}
&a_0 c_0 + b_0 d_0 = 0 \text{ (коэффициент при } x^{l+m-1}\text{)},\\
&a_1 c_0 + a_0 c_1 + b_1 d_0 + b_0 d_1 = 0 \text{ (коэффициент при } x^{l+m-2}\text{)}, \qquad (4)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&a_l c_{m-1} + b_m d_{l-1} = 1 \text{ (коэффициент при } x^0\text{)}.
\end{aligned}$$

Система (4) имеет единственное решение, так как $R_x(f, g) \neq 0$. Используя правило Крамера, получим, что

$$c_0 = \frac{1}{R_x(f,g)} \det \begin{bmatrix} 0 & & & & b_0 & & & \\ \vdots & a_0 & & & b_1 & b_0 & & \\ & a_1 & \mathbf{O} & & b_2 & b_1 & \mathbf{O} & \\ \vdots & & \mathbf{O} & a_0 & \vdots & & \mathbf{O} & b_0 \\ 1 & & & a_1 & b_m & & & b_1 \\ & a_l & & & & b_m & & \\ & & \mathbf{O} & \vdots & & & \mathbf{O} & \vdots \\ & & & a_l & & & & b_m \end{bmatrix}.$$

Так как определитель является целочисленным полиномом от своих элементов, то

$$c_0 = \frac{\text{целочисленный полином от } a_i, b_j}{R_x(f,g)}.$$

Аналогичными формулами определяются остальные c_i, а также d_j. Таким образом, $\tilde{A} = c_0 x^{m-1} + \ldots + c_{m-1}$ может быть записан в виде $\tilde{A} = \frac{1}{R_x(f,g)}$A, где $A \in k[x]$, причем коэффициенты A являются целочисленными полиномами от a_i, b_j. Аналогично, $\tilde{B} = \frac{1}{R_x(f,g)}$B, где $B \in k[x]$, и B обладает теми же свойствами, что и A. Так как $\tilde{A}f + \tilde{B}g = 1$, то $Af + Bg = R_x(f, g)$. □

2.3. ТЕОРЕМА О ПРОДОЛЖЕНИИ

Определение 1. Пусть полиномы $f, g \in k[x_1,\ldots,x_n]$ имеют положительную степень относительно x_1:

$$f = a_0 x^l + \ldots + a_l,\ g = b_0 x^m + \ldots + b_m, \qquad (1)$$

где $a_i, b_j \in k[x_2, \ldots, x_n]$, $i = \overline{0,l}$, $j = \overline{0,m}$, $a_0 \neq 0$, $b_0 \neq 0$.

Результантом полиномов f и g относительно x_1 называется определитель

$$R_{x_1}(f,g)=\det\begin{bmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \mathbf{O} & & b_2 & b_1 & \mathbf{O} & \\ \mathbb{M} & & \mathbf{O} & a_0 & \mathbb{M} & & \mathbf{O} & b_0 \\ a_1 & & & a_1 & b_m & & & b_1 \\ & a_1 & & & & b_m & & \\ & & \mathbf{O} & \mathbb{M} & & & \mathbf{O} & \mathbb{M} \\ & & & a_1 & & & & b_m \end{bmatrix}$$

порядка $l + m$. Здесь первые m столбцов заняты элементами a_i, а следующие l столбцов – элементами b_j, при этом в пустых местах матрицы стоят нули.

Предложение 1. *Пусть $f, g \in k[x_1,\ldots,x_n]$ – полиномы положительной степени относительно x_1. Тогда*

1) $R_{x_1}(f,g)$ принадлежит первому исключающему идеалу $< f, g > \mathbf{I}\ k[x_2,\ldots,x_n]$;

2) $R_{x_1}(f,g) = 0$ тогда и только тогда, когда f и g имеют общий делитель в $k[x_1,\ldots,x_n]$ положительной степени относительно x_1.

Доказательство. 1) Так как результант является целочисленным Полиномом от коэффициентов полиномов f, g, то $R_{x_1}(f,g) \in k[x_2,\ldots,x_n]$. Далее, сущеествуют полиномы A, B относительно x_1, коэффициенты которых являются целочисленными полиномами от a_i, b_j, т.е. $A, B \in k[x_2,\ldots,x_n][x_1] = k[x_1,\ldots,x_n]$, для которых $Af + Bg = R_{x_1}(f,g)$. Следовательно, $R_{x_1}(f,g) \in < f, g > \mathbf{I}\ k[x_2,\ldots,x_n]$.

2) Полиномы f, g можно рассматривать как полиномы относительно переменной x_1 с коэффициентами из $k[x_2,\ldots,x_n]$, а значит, f, g можно считать полиномами от x_1 с коэффициентами из $k(x_2,\ldots,x_n)$, т.е. $f, g \in k(x_2,\ldots,x_n)[x_1]$. Из предложения 2 п. 2.1 имеем, что $R_{x_1}(f,g) = 0$ тогда и только тогда, когда f и g имеют общий делитель в $k(x_2,\ldots,x_n)[x_1]$ положительной степени по x_1. Но это эквивалентно тому, что f и g имеют общий делитель в $k[x_1,\ldots,x_n]$ положительной степени относительно x_1. □

Следствие 1. *Если $f, g \in \mathbf{C}[x]$, то $R_x(f, g) = 0$ тогда и только тогда, когда f и g имеют общий корень в* **C**.

Доказательство вытекает из того, что два полинома из $\mathbf{C}[x]$ имеют общий корень тогда и только тогда, когда они имеют общий делитель. □

Предложение 2. *Пусть* $f, g \in \mathbf{C}[x_1,\ldots,x_n]$ *и пусть* $a_i, b_j \in \mathbf{C}[x_2,\ldots,x_n]$ *как в (1). Если* $R_{x_1}(f,g) \in \mathbf{C}[x_2,\ldots,x_n]$ *равен нулю в точке* $(c_2,\ldots,c_n) \in \mathbf{C}^{n-1}$, *то или*

1) a_0 *или* b_0 *равно нулю в точке* $(c_2,\ldots,c_n)$, *или*

2) *существует* $c_1 \in \mathbf{C}$ *такое, что* f *и* g *равны нулю в точке* $(c_1,\ldots,c_n) \in \mathbf{C}^n$.

Доказательство. Пусть $c = (c_2,\ldots,c_n)$ и $f(x_1, c) = f(x_1, c_2,\ldots,c_n)$. Покажем, что полиномы от одной переменной $f(x, c)$, $g(x, c)$ имеют общий корень, если $a_0(c) \neq 0$, $b_0(c) \neq 0$. Имеем

$$f(x_1, c) = a_0(c)x_1^{\,l} + \ldots + a_l(c),\ g(x_1, c) = b_0(c)x_1^{\,m} + \ldots + b_m(c), \qquad (2)$$

где $a_0(c)b_0(c) \neq 0$. По условию $h = R_{x_1}(f,g)$ равен нулю в точке c, т.е. $h(c) = 0$. Но для полиномов (2) $R_{x_1}(f(x_1,c), g(x_1,c)) = h(c) = 0$. На основании следствия 1 имеем, что полиномы $f(x_1, c)$, $g(x_1, c)$ имеют общий корень. □

Теорема 1 (теорема о продолжении для двух полиномов). *Пусть* $I = \langle f, g \rangle \subset \mathbf{C}[x_1,\ldots,x_n]$ *и пусть* I_1 *– первый исключающий идеал идеала* I, *т.е.* $I_1 = I \cap \mathbf{C}[x_2,\ldots,x_n]$, *а* a_0, b_0 *такие же, как в (1). Пусть* $(c_2,\ldots,c_n) \in \mathbf{V}(I_1)$ *– частичное решение. Тогда, если* $(c_2,\ldots,c_n) \notin \mathbf{V}(a_0,b_0)$, *то существует* $c_1 \in \mathbf{C}$ *такое, что* $(c_1,\ldots,c_n) \in \mathbf{V}(I)$.

Доказательство. В этом случае $h = R_{x_1}(f,g) \in I_1$. Значит, $h(c) = 0$. Если $a_0(c)b_0(c) \neq 0$, то существование требуемого c_1 следует из предложения 2. Пусть теперь одно из чисел $a_0(c)$, $b_0(c)$ равно нулю. Допустим для определенности $b_0(c) = 0$. Тогда $a_0(c) \neq 0$, ибо $c \notin \mathbf{V}(a_0, b_0)$. В этом случае степень полинома $g(x_1, c)$ относительно x_1 строго меньше m. Так как $\mathbf{V}(f, g)$ зависит лишь от идеала $\langle f, g \rangle$, но не зависит от выбора его базиса, то для идеала $\langle f, g \rangle$ можно использовать другой базис. Пусть $N \in \mathbf{N}$. Тогда $\langle f, g \rangle = \langle f, g + x_1^N f \rangle$. Действительно, если $h \in \langle f, g \rangle$, то существуют $p_1, p_2 \in \mathbf{C}[x_1,\ldots,x_n]$ такие, что $h = p_1 f + p_2 g = (p_1 - p_2 x_1^N)f + p_2(g + x_1^N f)$, т.е. $h \in \langle f, g + x_1^N f \rangle$. Наоборот, если $h \in \langle f, g + x_1^N f \rangle$, то существуют $q_1, q_2 \in \mathbf{C}[x_1,\ldots,x_n]$ такие, что $h = q_1 f + q_2(g + x_1^N f) = (q_1 + q_2 x_1^N)f + q_2 g$, т.е. $h \in \langle f, g \rangle$. Выберем N таким, чтобы степень полинома $x_1^N f$ относительно x_1 была больше, чем степень g относительно x_1. Тогда старший коэффициент полинома $g + x_1^N f$ относительно x_1 равен $a_0(\mathrm{c}) \neq 0$. Следовательно, существует $\mathrm{c}_1 \in \mathbf{C}$ такое, что $(\mathrm{c}_1, \mathrm{c}) \in \mathbf{V}(f, g + x_1^N f)$, и тогда $(\mathrm{c}_1, \mathrm{c}) \in \mathbf{V}(f, g)$. □

Определение 2. Пусть задан идеал $< f_1,\ldots,f_s > \subset \mathbf{C}[x_1,\ldots,x_n]$. Образуем полином $\sum_{k=2}^{s} u_k f_k \in \mathbf{C}[u_2,\ldots,u_s,\ x_1,\ldots,x_n]$. Тогда $R_{x_1}(f_1, \sum_{k=2}^{s} u_k f_k) = \sum_{\alpha} h_\alpha(x_2,\ldots,x_n)u^\alpha \in \mathbf{C}[u_2,\ldots,u_s,\ x_1,\ldots,x_n]$, где $h_\alpha \in \mathbf{C}[x_2,\ldots,x_n]$, $u^\alpha = u_2^{\alpha_2}\ldots u_s^{\alpha_s}$. Полиномы h_α называются *обобщенными результантами* полиномов $f_1,\ldots,f_s$. Обобщенные результанты зависят от того, какой полином считается первым.

Теорема 2 (теорема о продолжении). *Пусть* $I = < f_1,\ldots,f_s > \subset \mathbf{C}[x_1,\ldots,x_n]$, *а* $I_1 = I \cap k[x_2,\ldots,x_n]$ *– первый исключающий идеал. Пусть для каждого* i, $i = \overline{1,s}$, $f_i = g_i(x_2,\ldots,x_n)x_1^{N_i}$ + *члены, содержащие* x_1 *в степени* $< N_i$, *где* $N_i \geq 0$, $g_i \in \mathbf{C}[x_2,\ldots,x_n]$ *– ненулевые полиномы. Пусть* $(c_2,\ldots,c_n) \in \mathbf{V}(I_1)$ *– частичное решение. Тогда, если* $(c_2,\ldots,c_n) \notin \mathbf{V}(g_1,\ldots,g_s)$, *то существует* $c_1 \in \mathbf{C}$ *такое, что* $(c_1,\ldots,c_n) \in \mathbf{V}(I)$.

Доказательство. Пусть $c = (c_2,\ldots,c_n)$. Будем искать общий корень c_1 полиномов $f_1(x_1, c),\ldots,f_s(x_1, c)$. Случай $s = 2$ рассмотрен в теореме 1, случай же $s = 1$ сводится к случаю $s = 2$, так как $\mathbf{V}(f_1) = \mathbf{V}(f_1, f_1)$. Будем доказывать теорему для $s \geq 3$. Так как $c \notin \mathbf{V}(g_1,\ldots,g_s)$, то можно считать, что $g_1(c) \neq 0$. Пусть $h_\alpha \in \mathbf{C}[x_2,\ldots,x_n]$ – обобщенные результанты полиномов $f_1,\ldots,f_s$, т.е.

$$R_{x_1}(f_1, \sum_{k=2}^{s} u_k f_k) = \sum_{\alpha} h_\alpha u^\alpha . \qquad (3)$$

Покажем, что $h_\alpha \in I_1$. Из предложения 1 следует, что существуют A, $B \in \mathbf{C}[u_2,\ldots,u_s, x_1,\ldots,x_n]$ такие, что $Af_1 + B(\sum_{k=2}^{s} u_k f_k) = R_{x_1}(f_1, \sum_{k=2}^{s} u_k f_k)$. Пусть $A = \sum_{\alpha} A_\alpha u^\alpha$, $B = \sum_{\beta} B_\beta u^\beta$, где $A_\alpha, B_\beta \in \mathbf{C}[x_1,\ldots,x_n]$. Покажем, что $h_\alpha \in I$. Положим $e_2 = (1, 0,\ldots,0),\ldots,e_s = (0,\ldots,0, 1)$. Тогда

$$\sum_{\alpha} h_\alpha u^\alpha = (\sum_{\alpha} A_\alpha u^\alpha) f_1 + (\sum_{\beta} B_\beta u^\beta)(\sum_{i\geq 2} u^{e_i} f_i) = \sum_{\alpha} (A_\alpha f_1)u^\alpha +$$

$$+ \sum_{i\geq 2,\beta} B_\beta f_i u^{\beta+e_i} = \sum_{\alpha} (A_\alpha f_1)u^\alpha + \sum_{\alpha} \left(\sum_{\substack{i\geq 2,\beta \\ \beta+e_i=\alpha}} B_\beta f_i \right) u^\alpha . \qquad (4)$$

Приравнивая в (4) коэффициенты при u^{α}, имеем $h_\alpha = A_\alpha f_1 + \sum_{\substack{i\geq 2,\beta \\ \beta+e_i=\alpha}} B_\beta f_i$, т.е. $h_\alpha \in I$. Так как $h_\alpha \in \mathbf{C}[x_2,\ldots,x_n]$, то $h_\alpha \in I_1$ для всех α. Так как $c \in \mathbf{V}(I_1)$, то для всех α $h_\alpha(c) = 0$. Из (3) следует, что $h = R_{x_1}(f_1, \sum_{k=2}^{s} u_k f_k)$ равен нулю в c, т.е. при любом u_k, $k = \overline{2,s}$ $h(c, u_2,\ldots,u_s) = 0$. Предположим, что $g_2(c) \neq 0$ и степень полинома f_2 относительно x_1 больше степеней полиномов $f_3,\ldots,f_s$. В этом случае $h(c, u_2,\ldots,u_s) = R_{x_1}(f_1(x_1,c), \sum_{k=2}^{s} u_k f_k(x_1,c))$, ибо старшие коэффициенты полиномов f_1 и $\sum_{k=2}^{s} u_k f_k$ относительно x_1 не равны нулю в точке c. Заметим, что старший коэффициент полинома $\sum_{k=2}^{s} u_k f_k$ относительно x_1 в точке c равен $u_2 g_2(c)$. Из $h(c, u_2,\ldots,u_s) = 0$ следует, что полиномы $f_1(x_1, c)$, $\sum_{k=2}^{s} u_k f_k(x_1,c) \in \mathbf{C}[x_1, u_2,\ldots,u_s]$ имеют общий множитель F положительной степени относительно x_1. Так как F делит $f_1(x_1, c)$, то $F \in \mathbf{C}[x_1]$. Покажем, что F делит каждый из полиномов $f_2(x_1, c),\ldots,f_s(x_1, c)$. Действительно, существует $A \in \mathbf{C}[x_1, u_2,\ldots,u_s]$ такой, что

$$F(x_1)A(x_1, u_2,\ldots,u_s) = \sum_{k=2}^{s} u_k f_k(x_1,c). \qquad (5)$$

Из сравнения в (5) коэффициентов при u_2 имеем $F(x_1)\tilde{A} = f_2(x_1, c)$, т.е. $F(x_1)$ делит $f_2(x_1, c)$. Аналогично, $F(x_1)$ делит все $f_k(x_1, c)$, $k = \overline{3,s}$. Таким образом, $F(x_1)$ является общим делителем положительной степени для всех $f_i(x_1, c)$, $i = \overline{1,s}$. Пусть c_1 – корень полинома F. Этот корень существует, так как $\mathbf{C}$ – алгебраически замкнутое поле. Тогда c_1 будет общим корнем для всех $f_i(x_1, c)$, $i = \overline{1,s}$. Таким образом, в случае $g_2(c) \neq 0$ и когда степень полинома f_2 относительно x_1 больше степеней полиномов $f_3,\ldots,f_s$, теорема доказана. Если эти условия не выполняются, то для идеала I будем использовать новый базис. Для этого заменим f_2 на $f_2 + x_1^N f_1$, где $N \in \mathbf{N}$. Тогда аналогично случаю $s = 2$ имеем $I = \langle f_1,\ldots,f_s \rangle = \langle f_1, f_2 + x_1^N f_1, f_3,\ldots,f_s \rangle$. Если N достаточно велико, то старший коэффициент полинома $f_2 + x_1^N f_1$ будет g_1, который не равен нулю в c. Ясно, что N можно

выбрать таким, что $f_2 + x_1^N f_1$ имеет относительно x_1 большую степень, чем $f_3,\ldots,f_s$. Тогда существует общий корень c_1 полиномов $f_1(x_1, c)$, $f_2(x_1, c) + x_1^N f_1(x_1, c)$, $f_3(x_1, c),\ldots,f_s(x_1, c)$. Отсюда следует, что c_1 – общий корень всех $f_i(x_1, c)$. □

Заметим, что теорема о продолжении справедлива над любым алгебраически замкнутым полем.

Теорема 3. *Пусть дано многообразие* $V = \mathbf{V}(f_1,\ldots,f_s) \subset \mathbf{C}^n$, *и пусть* g_i *определены так же, как в формулировке теоремы 2. Если* I_1 *– первый исключающий идеал для идеала* $I = < f_1,\ldots,f_s >$, *то в* $\mathbf{C}^{n-1}$ *имеет место равенство:*

$$\mathbf{V}(I_1) = \pi_1(V) \ \mathbf{U} \ (\mathbf{V}(g_1,\ldots,g_s) \ \mathbf{I} \ V(I_1)),$$

где $\pi_1 : \mathbf{C}^n \to \mathbf{C}^{n-1}$ *– отображение проекции на последние* $n - 1$ *координат.*

Доказательство. Пусть $(a_2,\ldots,a_n) \in \mathbf{V}(I_1)$. Если $(a_2,\ldots,a_n) \in \mathbf{V}(g_1,\ldots,g_s)$, то $(a_2,\ldots,a_n) \in \mathbf{V}(g_1,\ldots,g_s) \ \mathbf{I} \ \mathbf{V}(I_1)$, а значит, $(a_2,\ldots,a_n) \in \pi_1(V) \ \mathbf{U} \ (\mathbf{V}(g_1,\ldots,g_s) \ \mathbf{I} \ V(I_1))$. В случае $(a_2,\ldots,a_n) \notin \mathbf{V}(g_1,\ldots,g_s)$ на основании теоремы 2 существует $a_1 \in C$ такое, что $(a_1, a_2,\ldots,a_n) \in \mathbf{V}(I) = V$. Значит, $(a_2,\ldots,a_n) \in \pi_1(V)$. Следовательно, $\mathbf{V}(I_1) \subset \pi_1(V) \ \mathbf{U} \ (\mathbf{V}(g_1,\ldots,g_s) \ \mathbf{I} \ V(I_1))$.

Пусть теперь $(a_2,\ldots,a_s) \in \pi_1(V) \ \mathbf{U} \ (\mathbf{V}(g_1,\ldots,g_s) \ \mathbf{I} \ V(I_1))$. Если $(a_2,\ldots,a_s) \in \pi_1(V)$, то из предложения 3 п. 2.1 заключаем, что $(a_2,\ldots,a_s) \in \mathbf{V}(I_1)$. В случае $(a_2,\ldots,a_s) \in \mathbf{V}(g_1,\ldots,g_s) \ \mathbf{I} \ V(I_1)$, очевидно, $(a_2,\ldots,a_s) \in \mathbf{V}(I_1)$, а поэтому $\pi_1(V) \ \mathbf{U} \ (\mathbf{V}(g_1, \ldots,g_s) \ \mathbf{I} \ V(I_1)) \subset \mathbf{V}(I_1)$. □

ГЛАВА 3. СООТВЕТСТВИЯ МЕЖДУ АФФИННЫМИ МНОГООБРАЗИЯМИ И ИДЕАЛАМИ.

3.1. ТЕОРЕМА ГИЛЬБЕРТА О НУЛЯХ

Теорема 1 (слабая теорема о нулях). *Пусть поле k алгебраически замкнуто, и пусть $I \subset k[x_1,\ldots,x_n]$ – идеал, такой, что $\mathbf{V}(I) = \emptyset$. Тогда $I = k[x_1,\ldots,x_n]$.*

Доказательство. Покажем, что $1 \in I$. Если $1 \in I$, то для любого $f \in k[x_1,\ldots,x_n]$ $f = f\cdot 1 \in I$, т.е. в этом случае $I = k[x_1,\ldots,x_n]$. Будем использовать метод математической индукции. Индукцию будем проводить по числу переменных n. Если $n = 1$, то $I = < f >$. Здесь $\mathbf{V}(I)$ – множество корней полинома $f(x_1)$. Так как $\mathbf{V}(I) = \emptyset$, то из алгебраической замкнутости поля k заключаем, что f – ненулевая константа. Тогда $\frac{1}{f} \in k$, а поэтому $1 = f\cdot\frac{1}{f} \in I$, т.е. для любого $g \in k[x_1]$ $g = g\cdot 1 \in I$. Поэтому $I = k[x_1]$.

Пусть теорема справедлива для полиномиального кольца $k[x_2,\ldots,x_n]$ от $n-1$ переменных. Возьмем любой идеал $I = < f_1,\ldots,f_s > \subset k[x_1,\ldots,x_n]$ такой, что $\mathbf{V}(I) = \emptyset$. Можно считать, что $f_1 \neq 0$, причем f_1 – не константа; в противном случае доказывать нечего. Пусть полная степень полинома f_1 равна N, где $N > 1$. Будем проводить замену переменных, приводящую полином f_1 к удобному виду. Рассмотрим линейную замену

$$x_1 = \tilde{x}_1,\ x_2 = \tilde{x}_2 + a_2\tilde{x}_1,\ldots,x_n = \tilde{x}_n + a_n\tilde{x}_1, \qquad (1)$$

где константы $a_i \in k$, $i = \overline{2,n}$, мы определим ниже. В новых координатах f_1 имеет вид $f_1(x_1,\ldots,x_n) = f_1(\tilde{x}_1,\ \tilde{x}_2 + a_2\tilde{x}_1,\ldots,\tilde{x}_n + a_n\tilde{x}_1) = c(a_2,\ldots,a_n)\tilde{x}_1^{\,N} +$ члены, в которых $\tilde{x}_1$ имеет степень, меньшую N. Покажем, что $c(a_2,\ldots,a_n)$ – ненулевой полином от переменных $a_2,\ldots,a_n$. Пусть $f_1 = h_N + h_{N-1} + \ldots + h_0$, где h_i, $i = \overline{0,n}$, – однородные полиномы полной степени i, т.е. каждый моном в h_i имеет степень i, причем $h_N \neq 0$ имеет вид $h_N = \sum_i c_i x^i = \sum_i c_i x_1^{\,i_1}\ldots x_n^{\,i_n}$, где $i_1 + \ldots + i_N = N$. В этом случае $h_N(x_1,\ldots,x_n) = \sum_i c_i\tilde{x}_1^{\,i_1}\,(\tilde{x}_2 + a_2\tilde{x}_1)^{i_2}\ \ldots\ (\tilde{x}_n + a_n\tilde{x}_1)^{i_n} = \sum_i c_i a_2^{\,i_2}\ldots a_n^{\,i_n}\tilde{x}_1^{\,N} +$ члены, в кото-

рых $\tilde{x}_1$ имеет степень, меньшую N. Таким образом, $h_N(x_1,\ldots,x_n) = h_N(1, a_2,\ldots,a_n)\tilde{x}_1^{\,N}$ + члены, в которых $\tilde{x}_1$ имеет степень, меньшую N.

Покажем, что $h_N(1, a_2,\ldots,a_n)$ – ненулевой полином относительно $a_2,\ldots,a_n$. Если $h_N(1, a_2,\ldots,a_n)$ – нулевой полином, то для любого $x_1 \neq 0$ и для всех a_i, $i = \overline{2,n}$, $h_N\left(1,\frac{a_2}{x_1},\ldots,\frac{a_n}{x_1}\right) = \sum_i c_i \frac{a_2^{\,i_2}\ldots a_n^{\,i_n}}{x_1^{\,i_2+\ldots+i_n}} = \sum_i c_i \frac{a_2^{\,i_2}\ldots a_n^{\,i_n}}{x_1^{\,N-i_1}} = \sum_i c_i \frac{x_1^{\,i_1} a_2^{\,i_2}\ldots a_n^{\,i_n}}{x_1^{\,N}} = \frac{h_N(x_1,a_2,\ldots,a_n)}{x_1^{\,N}} = 0$, что невозможно, ибо $h_N(x_1, a_2,\ldots,a_n)$ – ненулевой полином. Таким образом, $h_N(1, a_2,\ldots,a_n) = c(a_2,\ldots,a_n)$ – ненулевой полином. Так как $f_1(x_1,\ldots,x_n) = h_N(1, a_2,\ldots,a_n)\tilde{x}_1^{\,N}$ + члены, в которых $\tilde{x}_1$ имеет степень, меньшую N, то $f_1(x_1,\ldots,x_n) = c(a_2,\ldots,a_n)\ \tilde{x}_1^{\,N}$ + члены, в которых $\tilde{x}_1$ имеет степень, меньшую N, где $c(a_2,\ldots,a_n)$ – ненулевой полином. Покажем, что алгебраически замкнутое поле k бесконечно. Допустим, что k конечно, т.е. состоит из $c_i \in k$, где $i = \overline{1,m}$. Рассмотрим полином $f(x) = 1 + (x - c_1)(x - c_2)\ldots(x - c_m)$. Тогда $f(c_i) = 1$ для любого i, $i = \overline{1,m}$, т.е. $f(x)$ не имеет корней, что противоречит замкнутости поля k. Следовательно, алгебраически замкнутое поле k бесконечно. Отсюда следует, что существуют $a_2,\ldots,a_n \in k$ такие, что $c(a_2,\ldots,a_n) \neq 0$, ибо в противном случае полином $c(a_2,\ldots,a_n)$ был бы нулевым. Выбрав $a_2,\ldots,a_n$ так, что $c(a_2,\ldots,a_n) \neq 0$, мы преобразуем каждый полином $f \in k[x_1,\ldots,x_n]$ в полином $\tilde{f} \in k[\tilde{x}_1,\ldots,\tilde{x}_n]$. Покажем, что $\tilde{I} = \{\tilde{f} : f \in I\}$ является идеалом в $k[\tilde{x}_1,\ldots,\tilde{x}_n]$. Действительно, $0 \in \tilde{I}$, ибо $0 \in I$ и 0 переходит в 0; $\tilde{f}_i \in \tilde{I}$, $i = \overline{1,s}$, так как $f_i \in I$. Если $\tilde{h} \in \tilde{I}$, то $h(x_1,\ldots,x_n) = \tilde{h}\,(x_1, x_2 - a_2x_1,\ldots,x_n - a_nx_1) \in I$. Отсюда $h = \sum_{k=1}^{s} p_k f_k$, а тогда $\tilde{h} = \sum_{k=1}^{s} \tilde{p}_k \tilde{f}_k$, т.е. $\tilde{h} \in <\tilde{f}_1,\ldots,\tilde{f}_s>$. Значит, $\tilde{I} \subset <\tilde{f}_1,\ldots,\tilde{f}_s>$. С другой стороны, если $\tilde{h} \in <\tilde{f}_1,\ldots,\tilde{f}_s>$, то $\tilde{h} = \sum_{k=1}^{s} \tilde{p}_k \tilde{f}_k \in \tilde{I}$, ибо $\tilde{\text{h}}$ получаем из $h = \sum_{k=1}^{s} p_k f_k \in I$. Таким образом, множество $\tilde{I} = <\tilde{f}_1,\ldots,\tilde{f}_s>$, т.е. $\tilde{I}$ является идеалом в $k[\tilde{x}_1,\ldots,\tilde{x}_n]$. Заметим, что $\mathbf{V}(\tilde{I}) = \varnothing$, ибо если бы преобразованные уравнения имели решение $(\tilde{c}_1,\ldots,\tilde{c}_n)$, то и исходные уравнения имели бы решение $(\tilde{c}_1,\ \tilde{c}_2 + \text{a}_1\tilde{c}_1,\ldots,\tilde{c}_n + a_n\tilde{c}_1)$, что невозможно.

Покажем, что $1 \in \widetilde{I}$. Имеем $\widetilde{f}_1(\widetilde{x}_1,...,\widetilde{x}_n) = c(a_2,\ldots,a_n)\widetilde{x}_1^{\,N}$ + члены, где $\widetilde{x}_1$ имеет степень, меньшую N, причем $c(a_2,\ldots,a_n) \neq 0$. Пусть $\pi_1 : k^n \to k^{n-1}$ – проекция на последние $n-1$ координат. Положим $\widetilde{I}_1 = \widetilde{I}\ \mathbf{I}\ k[\widetilde{x}_2,\ldots,\widetilde{x}_n]$. Так как теорема о продолжении справедлива над любым алгебраически замкнутым полем, то в данном случае ввиду $c(a_2,\ldots,a_n) \neq 0$ все частичные решения в k^{n-1} можно продолжить до полных. Следовательно, на основании теоремы 3 п. 2.3 $\mathbf{V}(\widetilde{I}_1) = \pi_1(\mathbf{V}(\widetilde{I})) = \pi_1(\varnothing) = \varnothing$. Из индуктивного предположения заключаем, что $\widetilde{I}_1 = k[x_2,\ldots,x_n]$. Значит, $1 \in \widetilde{I}_1$. Отсюда $1 \in \widetilde{I}$, ибо $\widetilde{I}_1 \subset \widetilde{I}$. □

В случае $k = \mathbf{C}$ слабую теорему о нулях можно назвать «основной теоремой алгебры для полиномов от нескольких переменных»: каждая система полиномов, которая порождает идеал, меньший чем $\mathbf{C}[x_1,\ldots,x_n]$ имеет общий нуль в $\mathbf{C}^n$.

Система полиномиальных уравнений $f_1 = 0,\ldots,f_s = 0$ не имеет решений тогда и только тогда, когда $\mathbf{V}(f_1,\ldots,f_s) = \varnothing$. По слабой теореме о нулях это выполняется в том и только в том случае, когда $1 \in < f_1,\ldots,f_s >$. Таким образом, для решения задачи совместности нужно уметь определять, принадлежит ли единица данному идеалу.

Предложение 1. *Для любого мономиального упорядочения {1} – это единственный редуцированный базис Грёбнера идеала* $< 1 >$.

Доказательство. Пусть $\{g_1,\ldots,g_t\}$ – базис Грёбнера идеала $I = < 1 >$. Тогда $1 \in < \mathrm{LT}(I) > = < \mathrm{LT}(g_1),\ldots,\mathrm{LT}(g_t) >$. Следовательно, 1 делится на какой-то $\mathrm{LT}(g_i)$, например, 1 делится на $\mathrm{LT}(g_1)$. Значит, $\mathrm{LT}(g_2),\ldots,\mathrm{LT}(g_t)$ делятся на $\mathrm{LT}(g_1)$, а поэтому $g_2,\ldots,g_t$ могут быть удалены из базиса. Так как $\mathrm{LT}(g_1)$ – константа, то g_1 – константа, так как любой непостоянный моном больше 1. Таким образом, g_1 можно считать равным 1, т.е. редуцированный базис Грёбнера идеала $< 1 >$ состоит из одного элемента 1. □

Итак, имеем следующий *алгоритм проверки совместности*: пусть даны полиномы $f_1,\ldots,f_s \in \mathbf{C}[x_1,\ldots,x_n]$. Находим редуцированный базис Грёбнера идеала, порожденного этими полиномами по отношению к любому мономиальному упорядочению. Если этот базис есть {1}, то система $f_1 = 0,\ldots,f_s = 0$ не имеет решений; в противном случае эта система имеет решение в $\mathbf{C}^n$. Этот алгоритм работает в случае любого алгебраически замкнутого поля.

Теорема 2 (теорема Гильберта о нулях). *Пусть* k *– алгебраически замкнутое поле. Если* $f, f_1,\ldots,f_s \in k[x_1,\ldots,x_n]$ *такие, что* $f \in \mathbf{I}(\mathbf{V}(f_1,\ldots,f_s))$, *то существует* $m \in \mathbf{N}$ *такое, что* $f^m \in < f_1,\ldots,f_s >$.

Доказательство. Образуем идеал $\tilde{I} = < f_1,\ldots,f_s, 1 - yf > \subset k[x_1,\ldots,x_n, y]$, где y – новая переменная. Покажем, что $\mathbf{V}(\tilde{I}) = \varnothing$. Возьмем любую точку $(a_1,\ldots,a_n, a_{n+1}) \in k^{n+1}$. Тогда или $(a_1,\ldots,a_n) \in \mathbf{V}(f_1,\ldots,f_s)$, или $(a_1,\ldots,a_n) \notin \mathbf{V}(f_1,\ldots,f_s)$. Если $(a_1,\ldots,a_n) \in \mathbf{V}(f_1,\ldots,f_s)$, то $f(a_1,\ldots,a_n) = 0$, так как f равна нулю на $\mathbf{V}(f_1,\ldots,f_s)$. Тогда $1 - yf$ равен 1 в точке $(a_1,\ldots,a_n, a_{n+1})$, т.е. $(a_1,\ldots,a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$. Если $(a_1,\ldots,a_n) \notin \mathbf{V}(f_1,\ldots,f_s)$, то существует i, $1 \le i \le s$ такое, что $f_i(a_1,\ldots,a_n) \neq 0$. Мы можем рассматривать, f_i как функцию от $n + 1$ переменной, которая не зависит от a_{n+1}, т.е. $f_i(a_1,\ldots,a_n, a_{n+1}) \neq 0$. Следовательно, $(a_1,\ldots,a_n, a_{n+1}) \notin \mathbf{V}(\tilde{I})$. Отсюда $\mathbf{V}(\tilde{I}) = \varnothing$. Из слабой теоремы о нулях следует, что $1 \in \tilde{I}$. Значит, существуют p_i, $q \in k[x_1,\ldots,x_n, y]$, $i = \overline{1,s}$ такие, что

$$1 = \sum_{i=1}^{s} p_i(x_1,\ldots,x_n, y) f_i + q(x_1,\ldots,x_n, y)(1 - yf). \qquad (2)$$

Пусть y^m – наибольшая из степеней y, входящих во все p_i и q. Если умножим обе части равенства (2) на f^m, то получим соотношение вида

$$f^m = \sum_{i=1}^{s} \tilde{p}_i(x_1,\ldots,x_n, yf) f_i + \tilde{q}(x_1,\ldots,x_n, yf)(1 - yf), \qquad (3)$$

где $\tilde{p}_i = p_i f^m$, $\tilde{q} = q f^m$ – полиномы, записанные от переменных $x_1,\ldots,x_n, yf$. Так как равенство (3) является тождественным относительно $x_1,\ldots,x_n, yf$, то полагая в (3) $yf = 1$, имеем

$$f^m = \sum_{i=1}^{s} \tilde{p}_i(x_1,\ldots,x_n, 1) f_i = \sum_{i=1}^{s} A_i f_i,$$

где $A_i = \tilde{p}_i(x_1,\ldots,x_n, 1) \in k[x_1,\ldots,x_n]$. □

Предложение 2. *Пусть многообразие $V \subset k^n$. Если $f^m \in \mathbf{I}(V)$, то $f \in \mathbf{I}(V)$.*

Доказательство. Возьмем любую точку $x \in V$. Если $f^m \in \mathbf{I}(V)$, то $(f(x))^m = 0$, т.е. $f(x) = 0$. Значит, $f \in \mathbf{I}(V)$.

Определение 1. Идеал $I \subset k[x_1,\ldots,x_n]$ называется *радикальным*, если из $f^m \in I$ для некоторого $m \in N$ следует, что $f \in I$.

Следствие 1. **I***(V) является радикальным идеалом.*

Доказательство вытекает из предложения 2.

Идеал I не является идеалом всех полиномов, равных нулю на $\mathbf{V}(I)$ только тогда, когда этот идеал содержит f^m, где $m \geq 2$, причем $f \notin I$.

Определение 2. Пусть $\subset k[x_1,\ldots,x_n]$ – некоторый идеал. *Радикалом идеала* I называется множество $\sqrt{I} = \{f : \exists\, m \in \mathbf{N} \Rightarrow f^m \in I\}$.

Предложение 3. *Идеал I является радикальным тогда и только тогда, когда $I = \sqrt{I}$.*

Доказательство. Пусть I – радикальный идеал. Возьмем любой полином $f \in \sqrt{I}$. Тогда существует $m \in \mathbf{N}$ такое, что $f^m \in I$. Значит, $f \in I$. Следовательно, $\sqrt{I} \subset I$. Если $f \in I$, то $f^1 \in I$, т.е. $f \in \sqrt{I}$. Отсюда $I \subset \sqrt{I}$, а значит, $I = \sqrt{I}$. Пусть теперь $I = \sqrt{I}$. Если $f^m \in I$, то $f \in \sqrt{I}$, т.е. $f \in I$. Отсюда следует, что I – радикальный идеал. □

Предложение 4. *Если I – идеал в $k[x_1,\ldots,x_n]$, то $\sqrt{I} \supset I$. Более того, $\sqrt{I}$ – радикальный идеал.*

Доказательство. Если $f \in I$, то $f = f^1 \in I$, т.е. $f \in \sqrt{I}$. Значит, $I \subset \sqrt{I}$. Покажем, что $\sqrt{I}$ – идеал. Очевидно, $0 \in \sqrt{I}$. Пусть $f, g \in \sqrt{I}$. Тогда существуют $m, l \in \mathbf{N}$ такие, что $f^m, g^l \in I$. Рассмотрим полином $(f + g)^{m+l-1}$. Имеем

$$(f + g)^{m+l-1} = \sum_{i=0}^{m+l-1} C_{m+l-1}^{i} f^i g^{m+l-i-1}. \qquad (4)$$

В (4) либо $i \geq m$, либо $m + l - i - 1 \geq l$, т.е. для любого i $f^i g^{m+l-i-1} \in I$. Следовательно, $(f + g)^{m+l-1} \in I$, т.е. $f + g \in \sqrt{I}$. Пусть теперь $f \in \sqrt{I}$ и $h \in k[x_1,\ldots,x_n]$. Тогда существует $m \in \mathbf{N}$ такое, что $f^m \in I$. Следовательно, $f^m h^m = (fh)^m \in I$, а поэтому $fh \in \sqrt{I}$. Значит, $\sqrt{I}$ – идеал. Покажем, что $\sqrt{I}$ – радикальный идеал. Если $g = f^m \in \sqrt{I}$, то существует $k \in \mathbf{N}$ такое, что $g^k = (f^m)^k = f^{mk} \in I$. Отсюда на основании определения радикала заключаем, что $f \in \sqrt{I}$, т.е. $\sqrt{I}$ – радикальный идеал. □

Теорема 3 (сильная теорема о нулях). *Пусть k – алгебраически замкнутое поле и I – идеал в $k[x_1,\ldots,x_n]$. Тогда* $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.

Доказательство. Пусть $f \in \sqrt{I}$. Тогда существует $m \in \mathbf{N}$ такое, что $f^m \in I$. Следовательно, $f^m = 0$ на $\mathbf{V}(I)$, а значит, и $f = 0$ на $\mathbf{V}(I)$. Поэтому $f \in \mathbf{I}(\mathbf{V}(I))$, т.е. $\sqrt{I} \subset \mathbf{I}(\mathbf{V}(I))$. Предположим теперь, что $f \in \mathbf{I}(\mathbf{V}(I))$, где $I = \langle f_1,\ldots,f_s \rangle \subset k[x_1,\ldots,x_n]$. Тогда $\mathbf{V}(I) = \mathbf{V}(f_1,\ldots,f_s)$, т.е. $f \in \mathbf{I}(\mathbf{V}(f_1,\ldots,f_s))$. Из

теоремы Гильберта о нулях заключаем, что существует $m \in \mathbf{N}$ такое, что $f^m \in I$. Следовательно, $f \in \sqrt{I}$, а значит, $\mathbf{I}(\mathbf{V}(I)) \subset \sqrt{I}$. □

Теорему 3 обычно называют теоремой о нулях.

3.2. СООТВЕТСТВИЕ ИДЕАЛ – МНОГООБРАЗИЕ

Теорема 1 (соответствие идеал – многообразие). *Пусть k – произвольное поле. Тогда*

1) отображения

$$\text{аффинные многообразия} \xrightarrow{\mathbf{I}} \text{идеалы}$$

и

$$\text{идеалы} \xrightarrow{\mathbf{V}} \text{аффинные многообразия}$$

обращают включение, т.е. если $I_1 \subset I_2$ – идеалы, то $\mathbf{V}(I_1) \supset \mathbf{V}(I_2)$, и аналогично, если $V_1 \subset V_2$ – многообразия, то $\mathbf{I}(V_1) \supset \mathbf{I}(V_2)$. При этом равенство $\mathbf{V}(\mathbf{I}(V)) = V$ справедливо для любого V, т.е. отображение **I** *взаимно однозначно.*

2) Если k алгебраически замкнуто, а идеалы являются радикальными, то отображения

$$\text{аффинные многообразия} \xrightarrow{\mathbf{I}} \text{радикальные идеалы}$$

и

$$\text{радикальные идеалы} \xrightarrow{\mathbf{V}} \text{аффинные многообразия}$$

являются взаимно обратными биекциями, которые обращают включение.

Доказательство. 1) Пусть $I_1 \subset I_2$. Возьмем любой элемент $a \in \mathbf{V}(I_2)$. Тогда для любого $f \in I_1$ имеем $f \in I_2$, а значит, $f(a) = 0$, т.е. $a \in \mathbf{V}(I_1)$. Следовательно, $\mathbf{V}(I_2) \subset \mathbf{V}(I_1)$. Пусть теперь $V_1 \subset V_2$. Выберем любой элемент $f \in \mathbf{I}(V_2)$. Тогда для любого $a \in V_1$ имеем $a \in V_2$, а поэтому $f(a) = 0$, т.е. $f \in \mathbf{I}(V_1)$. Таким образом, $\mathbf{I}(V_2) \subset \mathbf{I}(V_1)$. Докажем, что $\mathbf{V}(\mathbf{I}(V)) = V$, где $V = \mathbf{V}(f_1,\ldots,f_s) \subset k^n$. Возьмем любой элемент $a \in V$. Тогда для любого $f \in \mathbf{I}(V)$ $f(a) = 0$, т.е. $f \in \mathbf{V}(\mathbf{I}(V))$. Значит, $V \subset \mathbf{V}(\mathbf{I}(V))$. Из определения идеала $\mathbf{I}(V)$ следует, что $f_1,\ldots,f_s \in \mathbf{I}(V)$. Следовательно, $< f_1,\ldots,f_s > \subset \mathbf{I}(V)$. Так как $\mathbf{V}(< f_1,\ldots,f_s >) = V$, то $\mathbf{V}(\mathbf{I}(V)) \subset \mathbf{V}(< f_1,\ldots,f_s >) = V$, т.е. $\mathbf{V}(\mathbf{I}(V)) = V$. Отображение **I** – взаимно однозначное отображение, так как оно имеет левое обратное **V**.

2) По следствию 1 из п. 3.1 $\mathbf{I}(V)$ является радикальным идеалом. Следовательно, мы можем рассматривать **I** как отображение множества многообразий в множество радикальных идеалов. Покажем, что $\mathbf{I}(\mathbf{V}(I)) = I$, если I – радикальный идеал. Действительно, по теореме 3 из п. 3.1

$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. Так как I радикален, то $\mathbf{I}(\mathbf{V}(I)) = I$. Таким образом, отображения **V** и **I** взаимно обратны и определяют биекции между множеством радикальных идеалов и множеством аффинных многообразий. □

Предложение 1 (принадлежность радикальному идеалу). *Пусть k – произвольное поле и $I = < f_1,\ldots,f_s > \subset k[x_1,\ldots,x_n]$ – некоторый идеал. Тогда $f \in \sqrt{I}$ в том и только в том случае, когда $1 \in \tilde{I}$, где $\tilde{I} = < f_1,\ldots,f_s,1 - yf > \subset k[x_1,\ldots,x_n,y]$, т.е. $\tilde{I} = k[x_1,\ldots,x_n,y]$.*

Доказательство. Пусть $1 \in \tilde{I}$. Тогда из доказательства теоремы Гильберта о нулях следует, что существует m такое, что $f^m \in I$, т.е. $f \in \sqrt{I}$. Пусть теперь наоборот $f \in \sqrt{I}$. Тогда существует m такое, что $f^m \in I \subset \tilde{I}$. Так как $1 - yf \in \tilde{I}$, то $1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + \ldots + y^{m-1} f^{m-1}) \in \tilde{I}$. □

Предложение 2. *Пусть $f \in k[x_1,\ldots,x_n]$ и пусть $I = < f >$ – главный идеал, порожденный полиномом f. Если $f = f_1^{a_1} f_2^{a_2} \ldots f_r^{a_r}$ – представление f в виде произведения неприводимых полиномов, то $\sqrt{I} = \sqrt{< f >} = < f_1 f_2 \ldots f_r >$.*

Доказательство. Покажем, что $f_1 f_2 \ldots f_r \in \sqrt{I}$. Пусть $N > \max(a_1, a_2,\ldots,a_r)$. Тогда $(f_1 f_2 \ldots f_r)^N = f_1^{N-a_1} f_2^{N-a_2} \ldots f_r^{N-a_r} f \in I$, т.е. $f_1 f_2 \ldots f_r \in \sqrt{I}$. Следовательно, $< f_1 f_2 \ldots f_r > \subset \sqrt{I}$. Пусть теперь $g \in \sqrt{I}$. Тогда существует $M \in \mathbf{N}$ такое, что $g^M \in I$, т.е. $g^M = hf$, где $h \in k[x_1,\ldots,x_n]$. Пусть $g = g_1^{b_1} g_2^{b_2} \ldots g_s^{b_s}$ – разложение полинома g в произведение различных неприводимых полиномов. Тогда $g^M = g_1^{Mb_1} g_2^{Mb_2} \ldots g_s^{Mb_s} = h f_1^{a_1} f_2^{a_2} \ldots f_r^{a_r}$. Так как разложение на неприводимые множители единственно, то каждый полином f_i равен (с точностью до постоянного множителя) некоторому полиному g_i. Следовательно, g делится на $f_1 f_2 \ldots f_r$, т.е. $g \in < f_1 f_2 \ldots f_r >$, а значит, $\sqrt{I} \subset < f_1 f_2 \ldots f_r >$. □

Определение 1. Пусть $f \in k[x_1,\ldots,x_n]$. *Редукцией полинома f* называется такой полином f_{red}, что $< f_{\text{red}} > = \sqrt{< f >}$. Полином называется *редуцированным* (или *свободным от квадратов*), если $f = f_{\text{red}}$.

Определение 2. Пусть $f, g \in k[x_1,\ldots,x_n]$. Тогда $h \in k[x_1,\ldots,x_n]$ называется *наибольшим общим делителем* полиномов f и g и обозначается $h = \text{GCD}(f, g)$, если

1) h делит и f, и g,
2) если полином p делит f и g, то p делит h.

Предложение 3. *Пусть* $f, g \in k[x_1,\ldots,x_n]$. *Тогда GCD(f, g) существует и определяется единственным образом с точностью до постоянного множителя.*

Доказательство. Пусть $f = f_1^{a_1} f_2^{a_2} \ldots f_r^{a_r}$, $g = g_1^{b_1} g_2^{b_2} \ldots g_t^{b_t}$, где f_i, g_j – различные неприводимые множители полиномов f, g. Возьмем произвольный полином h, который делит и f, и g. Тогда $h = h_1^{c_1} h_2^{c_2} \ldots h_k^{c_k}$, где h_p – различные неприводимые множители полинома h, определяемые единственным образом, причем каждый h_p, $p = \overline{1,k}$, должен встречаться как среди f_i, так и среди g_j, ибо в противном случае h не будет делить и f и g. Пусть h_p среди f встречается α_p раз, а среди g – β_p раз. Тогда в h $c_p \le \min(\alpha_p, \beta_p)$. Следовательно, $GCD(f, g) = h_1^{d_1} h_2^{d_2} \ldots h_k^{d_k}$, где $d_p = \min(\alpha_p, \beta_p)$, $p = \overline{1,k}$. □

Предложение 4. *Пусть поле k содержит поле рациональных чисел Q и пусть* $I = < f >$ *– главный идеал в* $k[x_1,\ldots,x_n]$. *Тогда* $\sqrt{I} = < f_{red} >$, *где* $f_{red} = \dfrac{f}{GCD(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n})}$.

Доказательство. Будем записывать f как в предложении 2. Тогда $\sqrt{I} = < f_1 f_2 \ldots f_r >$. Покажем, что

$$GCD(f, \frac{\partial f}{\partial x_1}, \frac{\partial f}{\partial x_2}, \ldots, \frac{\partial f}{\partial x_n}) = f_1^{a_1-1} f_2^{a_2-1} \ldots f_r^{a_r-1}. \quad (1)$$

Имеем $\dfrac{\partial f}{\partial x_j} = f_1^{a_1-1} f_2^{a_2-1} \ldots f_r^{a_r-1} (a_1 \dfrac{\partial f_1}{\partial x_j} f_2 \ldots f_r + \ldots + a_r f_1 \ldots f_{r-1} \dfrac{\partial f_r}{\partial x_j})$. Таким образом, $f_1^{a_1-1} f_2^{a_2-1} \ldots f_r^{a_r-1}$ делит GCD. Покажем, что для любого i существует $\dfrac{\partial f}{\partial x_j}$, который не делится на $f_i^{a_i}$. Запишем $f = f_i^{a_i} h_i$, где h_i не делится на f_i. Так как f_i имеет положительную степень, то некоторая переменная x_j встречается в f_i. Тогда $\dfrac{\partial f}{\partial x_j} = f_i^{a_i-1} (a_i \dfrac{\partial f_i}{\partial x_j} h_i + f_i \dfrac{\partial h_i}{\partial x_j})$. Если $\dfrac{\partial f}{\partial x_j}$ делится на $f_i^{a_i}$, то $\dfrac{\partial f_i}{\partial x_j} h_i$ делится на f_i. Так как f_i неприводим, а h_i не

делится на f_i, то f_i делит $\frac{\partial f}{\partial x_j}$. Полином $\frac{\partial f}{\partial x_j}$ является ненулевым, ибо переменная x_j встречается в f_j, а поле k бесконечно. Так как при дифференцировании по x_j полная степень полинома f_i уменьшится хотя бы на единицу, то f_i не может делить $\frac{\partial f}{\partial x_j}$, а значит, $f_i^{a_i}$ не может делить $\frac{\partial f}{\partial x_j}$. Отсюда вытекает (1). □

Определение 3. Пусть I и J – идеалы в $k[x_1,\ldots,x_n]$. *Сумма* $I + J$ – это множество $I + J = \{f + g : f \in I, g \in J\}$.

Предложение 5. *Если I и J – идеалы в $k[x_1,\ldots,x_n]$, то $I + J$ – также идеал в $k[x_1,\ldots,x_n]$, причем $I + J$ – наименьший идеал, содержащий I и J. Если $I = < f_1,\ldots,f_r >$, $J = < g_1,\ldots,g_s >$, то $I + J = < f_1,\ldots,f_r,g_1,\ldots,g_s >$.*

Доказательство. Так как $0 \in I$, $0 \in J$, то $0 = 0 + 0 \in I + J$. Пусть h_1, $h_2 \in I + J$. Тогда $h_1 = p_1 + q_1$, $h_2 = p_2 + q_2$, где p_1, $p_2 \in I$, q_1, $q_2 \in J$. По определению идеала $p_1 + p_2 \in I$, $q_1 + q_2 \in J$. Значит, $h_1 + h_2 = (p_1 + q_1) + (p_2 + q_2) = (p_1 + p_2) + (q_1 + q_2) \in I + J$. Пусть $h \in I + J$, а $l \in k[x_1,\ldots,x_n]$ – приводимый полином. Тогда $h = f + g$, где $f \in I$, $g \in J$. Имеем $lh = l(f + g) = lf + lg \in I + J$, так как $lf \in I$, $lg \in J$. Таким образом, $I + J$ – идеал.

Пусть H – произвольный фиксированный идеал, содержащий I и J. Тогда H содержит все элементы $f \in I$ и все элементы $g \in J$. Так как H – идеал, то он содержит все суммы $f + g$, где $f \in I$, $g \in J$. Значит, $I + J \subset H$, т.е. $I + J$ – наименьший идеал, содержащий I и J. Пусть $I = < f_1,\ldots,f_r >$, $J = < g_1,\ldots,g_s >$. Возьмем любой $h \in I + J$. Тогда $h = f + g$, где $f \in I$, $g \in J$. Значит, $h = \sum_{i=1}^{r} a_i f_i + \sum_{j=1}^{s} b_j g_j$, где a_i, $b_j \in k[x_1,\ldots,x_n]$. Следовательно, $h \in < f_1,\ldots,f_r, g_1,\ldots,g_s >$. Отсюда, $I + J \subset < f_1,\ldots,f_r, g_1,\ldots,g_s >$. Очевидно, $< f_1,\ldots,f_r, g_1,\ldots,g_s > \subset I + J$. Значит, $I + J = < f_1,\ldots,f_r, g_1,\ldots,g_s >$. □

Следствие 1. *Пусть $f_1,\ldots,f_r \in k[x_1,\ldots,x_n]$. Тогда $< f_1,\ldots,f_r > = < f_1 > + \ldots + < f_r >$.*

Теорема 2. *Пусть I, J – идеалы в $k[x_1,\ldots,x_n]$. Тогда* $\mathbf{V}(I + J) = \mathbf{V}(I)$ **I** $\mathbf{V}(J)$.

Доказательство. Пусть $x \in \mathbf{V}(I + J)$. Так как $I \subset I + J$, то $\mathbf{V}(I) \supset \mathbf{V}(I + J)$, а значит, $x \in \mathbf{V}(I)$. Аналогично, $x \in \mathbf{V}(J)$, а значит, $x \in \mathbf{V}(I)$ **I** $\mathbf{V}(J)$, т.е. $\mathbf{V}(I + J) \subset \mathbf{V}(I)$ **I** $\mathbf{V}(J)$. Пусть теперь $x \in \mathbf{V}(I)$ **I** $\mathbf{V}(J)$. Тогда $x \in \mathbf{V}(I)$, $x \in \mathbf{V}(J)$. Тогда $h = f + g$, где $f \in I$, $g \in J$. Значит, $f(x) = 0$, $g(x) = 0$. Отсюда, $h(x) = f(x) + g(x) = 0$. Так как для любого $h \in I + J$ $h(x) = 0$, то $x \in V(I + J)$. Следовательно, $\mathbf{V}(I)$ **I** $\mathbf{V}(J) \subset \mathbf{V}(I + J)$. □

Определение 4. Пусть I, J – идеалы в $k[x_1,\ldots,x_n]$. *Произведение* IJ – это множество $IJ = \{h \in k[x_1,\ldots,x_n] : \exists\ m \in N$ такое, что $h = \sum_{i=1}^{m} f_i g_i$, где $f_i \in I$, $g_i \in I$, $i = \overline{1,\mathrm{m}}\}$.

Предложение 6. *Если I, J – идеалы в $k[x_1,\ldots,x_n]$, то и IJ – идеал в $k[x_1,\ldots,x_n]$.*

Доказательство. Так как $0 \in I$, $0 \in J$, то $0 = 0\cdot 0 \in IJ$. Если $h_1, h_2 \in IJ$, то $h_1 = \sum_{i=1}^{m_1} f_{1,i} g_{1,i}$, $h_2 = \sum_{j=1}^{m_2} f_{2,j} g_{2,j}$, где $f_{1,i}, f_{2,j} \in I$, $g_{1,i}, g_{2,j} \in J$. Значит, $h_1 + h_2 \in IJ$. Если $h \in IJ$, то $h = \sum_{i=1}^{m} f_i g_i$, где $f_i \in I$, $g_i \in J$. Тогда для любого $p \in k[x_1,\ldots,x_n]$ $\quad ph = \sum_{i=1}^{m} (pf_i) g_i \in IJ$, ибо $pf_i \in I$, $i = \overline{1,m}$. □

Предложение 7. *Пусть $I = < f_1,\ldots,f_r >$, $J = < g_1,\ldots,g_s >$, где f_i, $g_i \in k[x_1,\ldots,x_n]$. Тогда идеал IJ порождается множеством всех произведений образующих идеалов I, J, т.е. $IJ = < f_i g_j : 1 \le i \le r, 1 \le j \le s >$.*

Доказательство. Пусть $h \in < f_i g_j : 1 \le i \le r,\ 1 \le j \le s >$. Тогда $h = \sum_{i=1}^{r}\sum_{j=1}^{s} c_{ij} f_i g_j$, где $c_{ij} \in k[x_1,\ldots,x_n]$. Значит, $h \in IJ$, т.е. $< f_i g_j : 1 \le i \le r, 1 \le j \le s > \subset IJ$. Пусть теперь $h \in IJ$. Тогда $h = \sum_{k=1}^{m} f_k g_k$, где $f_k \in I$, $g_k \in J$, $k = \overline{1,m}$. Имеем $f_k = \sum_{i=1}^{r} f_{k,i} f_i$, $g_k = \sum_{j=1}^{s} g_{k,j} g_j$, где $f_{k,i}, g_{k,j} \in k[x_1,\ldots,x_n]$. Следовательно, $h = \sum_{k=1}^{m} f_k g_k = \sum_{k=1}^{m}\left(\sum_{i=1}^{r} f_{k,i} f_i\right)\left(\sum_{j=1}^{s} g_{k,j} g_j\right) = \sum_{i=1}^{r}\sum_{j=1}^{s} c_{ij} f_i g_j$, где $c_{ij} \in k[x_1,\ldots,x_n]$. Отсюда, $h \in < f_i g_j : 1 \le i \le r, 1 \le j \le s >$, *т.е.* $IJ \subset < f_i g_j : 1 \le i \le r, 1 \le j \le s >$. □

Теорема 3. *Пусть I, J – идеалы в $k[x_1,\ldots,x_n]$. Тогда* $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$.

Доказательство. Пусть $x \in \mathbf{V}(IJ)$. Тогда для любых $f \in I$, $g \in J$ $\quad fg \in IJ$, а значит, $f(x)g(x) = 0$. Если для любого $f \in I$ $\quad f(x) = 0$, то $x \in \mathbf{V}(I)$. Если же существует $f \in I$ с $f(x) \neq 0$, то для любого $g \in J$ $\quad g(x) = 0$, т.е. $x \in \mathbf{V}(J)$. Итак, в обоих случаях $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Значит, $\mathbf{V}(IJ) \subset \mathbf{V}(I) \cup \mathbf{V}(J)$. Пусть теперь $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Если $x \in \mathbf{V}(I)$, то для любого $f \in I$ $\quad f(x) = 0$. В случае $x \in \mathbf{V}(J)$ для любого $g \in J$ $\quad g(x) = 0$. Значит, для любых $f \in I$,

$g \in J \quad f(x)g(x) = 0$. Возьмем любой $h \in IJ$. Тогда $h = \sum_{k=1}^{m} f_k g_k$, где $f_i \in I$, $g_j \in J$. Следовательно, для любого $h \in IJ \quad h(x) = \sum_{i=1}^{m} f_i(x)g_i(x) = 0$, т.е. $x \in \mathbf{V}(IJ)$. Отсюда, $\mathbf{V}(I) \cup \mathbf{V}(J) \subset \mathbf{V}(IJ)$. □

Определение 5. *Пересечение* $I \cap J$ двух идеалов $I, J \subset k[x_1,\ldots,x_n]$ – это множество полиномов, принадлежащих и I, и J.

Предложение 8. *Пусть I и J – идеалы в $k[x_1,\ldots,x_n]$. Тогда $I \cap J$ – идеал в $k[x_1,\ldots,x_n]$.*

Доказательство. Так как $0 \in I$ и $0 \in J$, то $0 \in I \cap J$. Пусть $f, g \in I \cap J$. Тогда $f + g \in I$, так как $f, g \in I$. Аналогично, $f + g \in J$. Следовательно, $f + g \in I \cap J$. Пусть теперь $f \in I \cap J$. Тогда для любого $h \in k[x_1,\ldots,x_n] \quad hf \in I$ и $hf \in J$, так как $f \in I$ и $f \in J$. Значит, $hf \in I \cap J$. □

Заметим, что $IJ \subset I \cap J$, так как элементы из IJ – это суммы произведений вида fg, где $f \in I$, $g \in J$. Так как $f \in I$, а $g \in J$, то $fg \in I$ и $fg \in J$, т.е. $fg \in I \cap J$. Следовательно, $IJ \subset I \cap J$. Идеал IJ может строго содержаться в $I \cap J$. Пусть, например, $I = J = < x, y >$. Тогда $IJ = < x^2, xy, y^2 >$ строго содержится в $I \cap J = I = < x, y >$, так как $x \in I \cap J$, но $x \notin IJ$.

Пусть $I \subset k[x_1,\ldots,x_n]$ – идеал, а $f(t) \in k[t]$ – полином от одной переменной t. Тогда fI обозначает идеал в $k[x_1,\ldots,x_n, t]$, порожденный множеством полиномов $\{fh : h \in I\}$. Заметим, что $I \subset k[x_1,\ldots,x_n]$ не является идеалом в $k[x_1,\ldots,x_n, t]$, так как он не замкнут относительно умножения на t. Когда мы хотим подчеркнуть, что f – полином только от t, мы пишем $f = f(t)$. Подчеркивая, что полином $h \in k[x_1,\ldots,x_n]$ зависит только от переменных $x_1,\ldots,x_n$, мы пишем $h = h(x)$. Рассматривая полином $g \in k[x_1,\ldots,x_n, t]$, зависящий как от $x_1,\ldots,x_n$, так и от t, мы пишем $g = g(x, t)$. В этих обозначениях $fI = f(t)I = < f(t)h(x) : h(x) \in I >$.

Лемма 1. *1) Если I порожден как идеал кольца $k[x_1,\ldots,x_n]$ полиномами $p_1(x),\ldots,p_r(x)$, то $f(t)I$ порожден как идеал кольца $k[x_1,\ldots,x_n, t]$ полиномами $f(t)p_1(x),\ldots,f(t)p_r(x)$.*

2) Если $g(x, t) \in f(t)I$, а a – любой элемент из поля k, то $g(x, a) \in I$.

Доказательство. Покажем, что любой полином $g(x, t) \in f(t)I$ может быть представлен как сумма полиномов вида $h(x,t)f(t)p(x)$, где $h \in k[x_1,\ldots,x_n, t]$, $p \in I$. Так как I порожден полиномами $p_1,\ldots,p_r$, то $p(x) = \sum_{i=1}^{r} q_i(x)\,p_i(x)$. Следовательно, $h(x, t)f(t)p(x) = \sum_{i=1}^{r} h(x,t)q_i(x)\,f(t)\,p_i(x)$. Так как для любого i, $1 \le i \le r \quad h(x, t)q_i(x) \in k[x_1,\ldots,x_n, t]$, то полином $h(x,$

$t)f(t)p(x) \in < f(t)p_1(x),\ldots,f(t)p_r(x) >$. Поэтому $g(x, t) \in < f(t)p_1(x),\ldots, f(t)p_r(x) >$. П. 1) доказан. Для любого $a \in k$ $g(x, a) \in < f(a)p_1(x),\ldots, f(a)p_r(x) >$, т.е. $g(x, a) \in I$. □

Теорема 4. *Пусть I, J – идеалы из $k[x_1,\ldots,x_n]$. Тогда $I \cap J = (tI + (1 - t)J) \cap k[x_1,\ldots,x_n]$.*

Доказательство. Пусть $f \in I \cap J$. Тогда $f \in I$, а значит, $tf \in tI$. Аналогично, $(1 - t)f \in (1 - t)J$. Следовательно, $f = tf + (1 - t)f \in tI + (1 - t)J$. Так как $I, J \subset k[x_1,\ldots,x_n]$, то $f \in (tI + (1 - t)J) \cap k[x_1,\ldots,x_n]$. Значит, $I \cap J \subset (tI + (1 - t)J) \cap k[x_1,\ldots,x_n]$. Пусть теперь $f \in (tI + (1 - t)J) \cap k[x_1,\ldots,x_n]$. Тогда $f(x) = g(x, t) + h(x, t)$, где $g(x, t) \in tI$ и $h(x, t) \in (1 - t)J$. Положим $t = 0$. Так как любой полином в tI делится на t, то $g(x, 0) = 0$. Значит, $f(x) = h(x, 0)$. По лемме 1 $f(x) \in J$. Положим теперь $t = 1$. Так как любой полином в $(1 - t)J$ делится на $1 - t$, то $h(x, 1) = 0$. Следовательно, $f(x) = g(x, 1)$ и по лемме 1 $f(x) \in I$. Отсюда следует, что $f \in I \cap J$ и $(tI + (1 - t)J) \cap k[x_1,\ldots,x_n] \subset I \cap J$. □

Из теоремы 1 вытекает следующий *алгоритм для вычисления пересечения идеалов*: если $I = < f_1,\ldots,f_s >$, $J = < g_1,\ldots,g_s >$ – идеалы в $k[x_1,\ldots,x_n]$, то мы рассматриваем идеал $< tf_1,\ldots,tf_s, (1 - t)g_1,\ldots,(1 - t)g_s > \subset k[x_1,\ldots,x_n, t]$ и находим его базис Грёбнера по отношению к lex-упорядочению, в котором t больше любого x_i. Тогда элементы этого базиса, не зависящие от t, образуют базис идеала $I \cap J$ (базис Грёбнера).

Определение 6. *Пересечение* $\bigcap_{j=1}^{m} I_j$ идеалов $I_1,\ldots,I_m \subset k[x_1,\ldots,x_n]$ – множество полиномов, принадлежащих всем I_j, $j = \overline{1,m}$. Заметим, что $I = \bigcap_{j=1}^{m} I_j$ – идеал в $k[x_1,\ldots,x_n]$.

Теорема 5. *Пусть $I_1,\ldots,I_m$ – идеалы в $k[x_1,\ldots,x_n]$ и пусть $J = < 1 - \sum_{j=1}^{m} t_j > + \sum_{j=1}^{m} t_j I_j$ – идеал в $k[x_1,\ldots,x_n, t_1,\ldots,t_m]$. Тогда $\bigcap_{j=1}^{m} I_j = J \cap k[x_1,\ldots,x_n]$.*

Доказательство. Пусть $I_j = < f_{i,1},\ldots, f_{j,k_j} > \subset k[x_1,\ldots,x_n]$, $j = \overline{1,m}$. Тогда $t_jI_j = < t_j f_{i,1},\ldots,t_j f_{j,k_j} >$, $j = \overline{1,m}$. Возьмем любой $f \in J \cap k[x_1,\ldots,x_n]$. Тогда $f \in J$, а поэтому $f = h(1 - \sum_{j=1}^{m} t_j) + \sum_{j=1}^{m}\sum_{s=1}^{k_j} h_{j,s} t_j f_{j,s}$, где $h, h_{j,s} \in k[x_1,\ldots,x_n, t_1,\ldots,t_m]$. Пусть $1 \le l \le m$. Полагая $t_l = 1$ и $t_j = 0$ для любых $j \ne l$,

полином f представляем в виде $f = \sum_{s=1}^{k_l} \tilde{h}_{ls} f_{ls}$, где $\tilde{h}_{ls} \in k[x_1,\ldots,x_n]$. Таким образом, для любого l, где $1 \le l \le m$, $f \in I_l$, т.е. $f \in \prod_{j=1}^{m} I_j$. Значит, $J \subset k[x_1,\ldots,x_n] \subset \prod_{j=1}^{m} I_j$. Пусть теперь $f \in \prod_{j=1}^{m} I_j$. Тогда $f \in I_j$, а значит, $f = \sum_{s=1}^{k_j} h_{js} f_{js}$, где $h_{js} \in k[x_1,\ldots,x_n]$, $j = \overline{1,m}$. Отсюда, $f = f(1 - \sum_{j=1}^{m} t_j) + \sum_{j=1}^{m}\sum_{s=1}^{k_j} h_{j,s} t_j f_{j,s}$, т.е. $f \in J \subset k[x_1,\ldots,x_n]$. □

Определение 7. Полином $h \in k[x_1,\ldots,x_n]$ называется *наименьшим общим кратным* полиномов $f, g \in k[x_1,\ldots,x_n]$ (обозначение $h = \mathrm{LCM}(f, g)$), если

1) f делит h и g делит h,

2) для любого полинома $p \in k[x_1,\ldots,x_n]$, который делится и на f, и на g, h делит p.

Предложение 9. *Пусть $f, g \in k[x_1,\ldots,x_n]$. Тогда LCM(f, g) существует и определяется с точностью до постоянного множителя.*

Доказательство. Пусть $f = f_1^{a_1} f_2^{a_2} \ldots f_s^{a_s}$, $g = g_1^{b_1} g_2^{b_2} \ldots g_t^{b_t}$ – разложения полиномов f и g в произведение различных неприводимых полиномов. Возьмем произвольный полином h, который делится и на f, и на g. Тогда $h = h_1^{c_1} h_2^{c_2} \ldots h_k^{c_k}$, где h_p – различные неприводимые множители полинома h, определяемые единственным образом. Каждый h_p должен встречаться или среди f_i, $i = \overline{1,s}$, или среди g_j, $j = \overline{1,t}$, ибо в противном случае h не будет делиться и на f, и на g. Пусть h_p среди f встречается α_p раз, а среди g – β_p раз. Тогда в h $c_p \ge \max(\alpha_p, \beta_p)$. Следовательно, $\mathrm{LCM}(f, g) = h_1^{d_1} h_2^{d_2} \ldots h_k^{d_k}$, где $d_p = \max(\alpha_p, \beta_p)$, $p = \overline{1,k}$. □

Предложение 10. *Пересечение $I \cap J$ двух главных идеалов $I, J \subset k[x_1,\ldots,x_n]$ является главным идеалом. Если $I = < f >$ и $J = < g >$, то $I \cap J = < h >$, где $h = LCM(f, g)$.*

Доказательство. Пусть $p \in I \cap J$. Тогда $p \in I$, $p \in J$, а значит, существуют $a_1, a_2 \in k[x_1,\ldots,x_n]$ такие, что $p = a_1 f$, $p = a_2 g$, т.е. p делится и на f, и на g. Следовательно, h делит p, а значит, $p \in < \mathrm{LCM}(f, g) >$. Пусть теперь $p \in < \mathrm{LCM}(f, g) >$. Тогда существует $c \in k[x_1,\ldots,x_n]$ такое, что $p = ch$, где

h = LCM(f, g). Отсюда следует, что p делится и на f, и на g, т.е. $p \in I$, $p \in J$, а тогда $p \in I \cap J$. □

Предложение 11. *Пусть* $f, g \in k[x_1,\ldots,x_n]$. *Тогда* $LCM(f, g)GCD(f, g) = fg$.

Доказательство следует из выражений GCD(f, g) и LCM(f, g) через неприводимые множители полиномов f и g и единственности разложения на неприводимые множители. □

Из предложения 11 следует, что $\mathrm{GCD}(f, g) = \dfrac{fg}{\mathrm{LCM}(f, g)}$.

Заметим, что $< \mathrm{LCM}(f, g) > = < f > \cap < g >$.

Теорема 6. *Пусть идеалы* $I, J \subset k[x_1,\ldots,x_n]$. *Тогда* $\mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$.

Доказательство. Пусть $x \in \mathbf{V}(I) \cup \mathbf{V}(J)$. Тогда $x \in \mathbf{V}(I)$ или $x \in \mathbf{V}(J)$, т.е. или $f(x) = 0$ для любого $f \in I$ или $f(x) = 0$ для любого $f \in J$. В этом случае для любого $f \in I \cap J$ $f(x) = 0$. Следовательно, $x \in \mathbf{V}(I \cap J)$, а значит, $\mathbf{V}(I) \cup \mathbf{V}(J) \subset \mathbf{V}(I \cap J)$. Так как $IJ \subset I \cap J$, то $\mathbf{V}(I \cap J) \subset \mathbf{V}(IJ)$. Из $\mathbf{V}(IJ) = \mathbf{V}(I) \cup \mathbf{V}(J)$ имеем $\mathbf{V}(I \cap J) \subset \mathbf{V}(I) \cup \mathbf{V}(J)$. □

Таким образом, пересечению двух идеалов соответствует то же многообразие, что и их произведению. Хотя пересечение идеалов находится труднее их произведения, интерес к пересечениям объясняется тем, что пересечение радикальных идеалов – радикальный идеал. Произведение же радикальных идеалов может и не быть радикальным идеалом.

Предложение 12. *Пусть* I, J *– произвольные идеалы в* $k[x_1,\ldots,x_n]$. *Тогда* $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

Доказательство. Пусть $f \in \sqrt{I \cap J}$. Тогда существует число $m \in \mathbf{N}$ такое, что $f^m \in I \cap J$. Следовательно, $f^m \in I$ и $f^m \in J$, т.е. $f \in \sqrt{I}$, $f \in \sqrt{J}$, а тогда $f \in \sqrt{I} \cap \sqrt{J}$. Отсюда $\sqrt{I \cap J} \subset \sqrt{I} \cap \sqrt{J}$. Пусть теперь $f \in \sqrt{I} \cap \sqrt{J}$. Тогда существуют числа $m, p \in \mathbf{N}$ такие, что $f^m \in I$ и $f^p \in J$. Отсюда $f^m f^p = f^{m+p} \in I \cap J$, т.е. $f \in \sqrt{I \cap J}$. □

3.3. ЗАМЫКАНИЕ ЗАРИССКОГО И ЧАСТНЫЕ ИДЕАЛОВ

Предложение 1. *Пусть* $S \subset k^n$ *– произвольное множество. Тогда множество* $\mathbf{I}(S) = \{f \in k[x_1,\ldots,x_n] : \forall\ a \in S\ f(a) = 0\}$ *– радикальный идеал.*

Доказательство. Очевидно, что $0 \in \mathbf{I}(S)$. Пусть $f, g \in \mathbf{I}(S)$. Тогда для любого элемента $a \in S \quad (f+g)(a) = f(a) + g(a) = 0$, т.е. $f + g \in \mathbf{I}(S)$. Если $f \in \mathbf{I}(S)$, то для любого $h \in k[x_1,\ldots,x_n] \quad (hf)(a) = h(a)f(a) = 0$ для любого $a \in S$, т.е. $hf \in \mathbf{I}(S)$. Таким образом, $\mathbf{I}(S)$ – идеал. Если $f^m \in \mathbf{I}(S)$, то для любого $a \in S \quad (f(a))^m = 0$. Отсюда для любого $a \in S \quad f(a) = 0$, т.е. $f \in \mathbf{I}(S)$, а значит, $\mathbf{I}(S)$ – радикальный идеал. □

Предложение 2. *Пусть* $S \subset k^n$. *Тогда* $\mathbf{V}(\mathbf{I}(S))$ *– наименьшее многообразие, содержащее S, т.е. если многообразие* $W \supset S$, *где* $W \subset k^n$, *то* $\mathbf{V}(\mathbf{I}(S)) \subset W$.

Доказательство. Пусть многообразие $W \supset S$. Тогда $\mathbf{I}(W) \subset \mathbf{I}(S)$, т.к. $\mathbf{I}$ обращает включение. Следовательно, $\mathbf{V}(\mathbf{I}(W)) \supset \mathbf{V}(\mathbf{I}(S))$, а тогда $W \supset \mathbf{V}(\mathbf{I}(S))$, ибо $\mathbf{V}(\mathbf{I}(W)) = W$. □

Определение 1. *Замыканием Зарисского* подмножества аффинного пространства называется наименьшее аффинное алгебраическое многообразие, содержащее это подмножество.

Если $S \subset k^n$, то замыкание Зарисского множества S обозначается через $\overline{S}$. При этом $\overline{S} = \mathbf{V}(\mathbf{I}(S))$.

Теорема 1. *Пусть поле k алгебраически замкнуто,* $V = \mathbf{V}(f_1,\ldots,f_s) \subset k^n$, $\pi_l : k^n \to k^{n-l}$ *– проекция на последние* $n - l$ *компонент. Если* I_l *есть l-й исключающий идеал, т.е.* $I_l = \langle f_1,\ldots,f_s \rangle \ \mathbf{I} \ k[x_{l+1},\ldots,x_n]$, *то* $\mathbf{V}(I_l)$ *– замыкание Зарисского множества* $\pi_l(V)$.

Доказательство. Имеем $\pi_l(V) \subset \mathbf{V}(I_l)$ (предложение 3 из п. 3.1). На основании предложения 2 $\mathbf{V}(I_l) \supset \mathbf{V}(\mathbf{I}(\pi_l(V)))$. Пусть теперь $f \in \mathbf{I}(\pi_l(V))$. Тогда для любого набора $(a_{l+1},\ldots,a_n) \in \pi_l(V) \quad f(a_{l+1},\ldots,a_n) = 0$. Считая $f \in k[x_1,\ldots,x_n]$, имеем для любого $(a_1,\ldots,a_n) \in V \quad f(a_1,\ldots,a_n) = 0$. По теореме Гильберта о нулях существует $N \in \mathbf{N}$ такое, что $f^N \in \langle f_1,\ldots,f_s \rangle$. Так как f не зависит от переменных $x_1,\ldots,x_l$, то и f^N также не зависит от этих переменных, т.е. $f^N \in \langle f_1,\ldots,f_s \rangle \ \mathbf{I} \ k[x_{l+1},\ldots,x_n] = I_l$. Отсюда $f \in \sqrt{I_1}$. Следовательно, $\mathbf{I}(\pi_l(V)) \subset \sqrt{I_1}$, а значит, $\mathbf{V}(\sqrt{I_1}) = \mathbf{V}(I_l) \subset \mathbf{V}(\mathbf{I}(\pi_l(V)))$. □

Предложение 3. *Пусть V, W – многообразия в* k^n *и* $V \subset W$. *Тогда* $W = V \cup \overline{W - V}$.

Доказательство. Так как $W - V \subset W$, а W – многообразие, то $\overline{W - V} \subset W$. Значит, $V \cup \overline{W - V} \subset W$. С другой стороны, из $V \subset W$ следует, что $W = V + (W - V)$. Так как $W - V \subset \overline{W - V}$, то $W \subset V \cup \overline{W - V}$. □

Определение 2. Пусть идеалы $I, J \subset k[x_1,\ldots,x_n]$. Обозначим через $I : J$ множество $\{f \in k[x_1,\ldots,x_n] : fg \in I \ \forall \ g \in J\}$. Множество $I : J$ называется *частным* идеалов I и J.

Таким образом, $I : J = \{f \in k[x_1,\ldots,x_n] : fg \in I \ \forall \ g \in J\}$.

Предложение 4. *Пусть идеалы $I, J \subset k[x_1,\ldots,x_n]$. Тогда $I : J$ – идеал в $k[x_1,\ldots,x_n]$, причем $I \subset I : J$.*

Доказательство. Пусть $f \in I$. Тогда для любого $g \in k[x_1,\ldots,x_n]$ $fg \in I$, а значит, для любого $g \in J$ $fg \in I$, т.е. $f \in I : J$. Следовательно, $I \subset I:J$. Докажем, что $I : J$ – идеал. Так как $0 \in I$, то $0 \in I : J$. Пусть $f_1, f_2 \in I : J$. Тогда для любого $g \in J$ $f_1g, f_2g \in I$, а значит, $f_1g + f_2g = (f_1 + f_2)g \in I$, т.е. $f_1 + f_2 \in I : J$. Если $f \in I : J$, а $h \in k[x_1,\ldots,x_n]$, то для любого $g \in J$ $fg \in I$ и $hfg \in I$. Следовательно, $hf \in I : J$. □

Теорема 2. *Пусть идеалы $I, J \subset k[x_1,\ldots,x_n]$. Тогда* $\mathbf{V}(I : J) \supset \overline{\mathbf{V}(I) - \mathbf{V}(J)}$. *Если k – алгебраически замкнутое поле и I – радикальный идеал, то* $\mathbf{V}(I : J) = \overline{\mathbf{V}(I) - \mathbf{V}(J)}$.

Доказательство. Покажем, что $I : J \subset \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. Пусть $f \in I : J$ и $x \in \mathbf{V}(I) - \mathbf{V}(J)$. Тогда для любого $g \in J$ $fg \in I$. Так как $x \in \mathbf{V}(I)$, то $f(x)g(x) = 0$ для любого $g \in J$. Поскольку $x \notin \mathbf{V}(J)$, то существует элемент $g \in J$ такой, что $g(x) \neq 0$. Значит, для любого $x \in \mathbf{V}(I) - \mathbf{V}(J)$ $f(x) = 0$. Следовательно, $f \in \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$, т.е. $I : J \subset \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. Отсюда $\mathbf{V}(I : J) \supset \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))) = \overline{\mathbf{V}(I) - \mathbf{V}(J)}$. Первая часть теоремы доказана. Пусть теперь k алгебраически замкнуто и $I = \sqrt{I}$. Пусть $x \in \mathbf{V}(I : J)$. Тогда, если для любого $g \in J$ $hg \in I$, то $h \in I : J$, т.е. $h(x) = 0$. Пусть теперь $h \in \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. Тогда h обращается в 0 на $\mathbf{V}(I) - \mathbf{V}(J)$. Для любого $g \in J$ hg обращается в 0 на $\mathbf{V}(I) - \mathbf{V}(J)$ и на $\mathbf{V}(J)$, т.е. hg обращается в 0 на $\mathbf{V}(I)$. По теореме Гильберта о нулях $hg \in \sqrt{I}$, а значит, $hg \in I$ для любого $g \in J$. Следовательно, $h \in I : J$ и $h(x) = 0$. Так как для любого $h \in \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$ $h(x) = 0$, то $x \in \mathbf{V}(\mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))) = \overline{\mathbf{V}(I) - \mathbf{V}(J)}$. Отсюда $\mathbf{V}(I : J) \subset \overline{\mathbf{V}(I) - \mathbf{V}(J)}$. □

Следствие 1. *Пусть V, W – многообразия в k^n. Тогда* $\mathbf{I}(V) : \mathbf{I}(W) = \mathbf{I}(V - W)$.

Доказательство. Из доказательства теоремы 2 $I : J \subset \mathbf{I}(\mathbf{V}(I) - \mathbf{V}(J))$. Положим $I = \mathbf{I}(V)$, $J = \mathbf{I}(W)$. Тогда $\mathbf{I}(V) : \mathbf{I}(W) \subset \mathbf{I}(\mathbf{V}(\mathbf{I}(V)) - \mathbf{V}(\mathbf{I}(W))) = \mathbf{I}(V - W)$. Пусть теперь $f \in \mathbf{I}(V - W)$. Тогда для любого $x \in V - W$ $f(x) = 0$. Для любого $g \in \mathbf{I}(W)$ $fg \in \mathbf{I}(V)$, так fg обращается в 0 на $V - W$ и на W, а значит, и на V. Из определения частного идеалов следует, что $f \in \mathbf{I}(V) : \mathbf{I}(W)$, т.е. $\mathbf{I}(V - W) \subset \mathbf{I}(V):\mathbf{I}(W)$. □

Предложение 5. *Пусть идеалы* $I, J, K \subset k[x_1,\ldots,x_n]$. *Тогда*

1) $I : K[x_1,\ldots,x_n] = I$;

2) $IJ \subset K$ *тогда и только тогда, когда* $I \subset K : J$;

3) $J \subset I$ *тогда и только тогда, когда* $I : J = k[x_1,\ldots,x_n]$.

Доказательство. 1) Пусть $f \in I$. Тогда для любого $g \in k[x_1,\ldots,x_n]$ $fg \in I$, т.е. $f \in I : k[x_1,\ldots,x_n]$, а значит, $I \subset I : k[x_1,\ldots,x_n]$. Если $f \in I : k[x_1,\ldots,x_n]$, то для любого $g \in k[x_1,\ldots,x_n]$ и, в частности, для $g = 1$ $f\cdot 1 = f \in I$. Отсюда $I : k[x_1,\ldots,x_n] \subset I$.

2) Пусть $IJ \subset K$. Возьмем $f \in I$. Тогда для любого $g \in J$ $fg \in IJ$, а значит, $fg \in K$. Следовательно, $fg \in K : J$, т.е. $I \subset K : J$. Пусть теперь $I \subset K : J$. Выберем $h \in IJ$. На основании определения произведения идеалов $h = \sum_{i=1}^{m} f_i g_i$, где $f_i \in I$, $g_i \in J$, $i = \overline{1,\mathrm{m}}$. Так как $I \subset K : J$, то $f_i \in K : J$, а значит, $f_i g_i \in K$. Отсюда $h \in K$, т.е. $IJ \subset K$.

3) Пусть $J \subset I$. Тогда для любого $f \in k[x_1,\ldots,x_n]$ и для любого $g \in J$ $fg \in J$, а значит, $fg \in I$. Отсюда $f \in I : J = k[x_1,\ldots,x_n]$. Пусть теперь $I : J = k[x_1,\ldots,x_n]$. Тогда для любого $f \in k[x_1,\ldots,x_n]$ и для любого $g \in J$ $fg \in I$. В частности, для $f = 1$ $1\cdot g = g \in I$. Следовательно, $J \subset I$. □

Предложение 6. *Пусть* I, I_i, J, J_i, *и* K *– идеалы в* $k[x_1,\ldots,x_n]$, *где* $1 \le i \le r$. *Тогда*

$$\left(\prod_{i=1}^{r} I_i\right) : J = \prod_{i=1}^{r} (I_i : J) \tag{1}$$

$$I : \left(\sum_{i=1}^{r} J_i\right) = \prod_{i=1}^{r} (I : J_i) \tag{2}$$

$$(I : J) : K = I : JK \tag{3}$$

Доказательство. Докажем (1). Пусть $f \in \left(\prod_{i=1}^{r} I_i\right) : J$. Тогда для любого $g \in J$ $fg \in \prod_{i=1}^{r} I_i$, т.е. $fg \in I_i$, где $1 \le i \le r$. Отсюда $f \in I_i : J$, т.е. $f \in \prod_{i=1}^{r} (I_i : J)$. Пусть теперь $f \in \prod_{i=1}^{r} (I_i : J)$. Тогда $f \in I_i : J$, где $1 \le i \le r$. Для

любого $g \in J$ $fg \in I_i$, $i = \overline{1,r}$, т.е. $fg \in \prod_{i=1}^{r} I_i$. Следовательно, $f \in \left(\prod_{i=1}^{r} I_i\right) : J$.
Формула (1) доказана.

Докажем (2). Пусть $f \in I : \left(\sum_{i=1}^{r} J_i\right)$. Тогда для любого $g \in \sum_{i=1}^{r} J_i$ $fg \in I$. Отсюда для любого $g \in J_i$, где $1 \le i \le r$, $fg \in I$, т.е. $f \in I : J_i$. Следовательно, $f \in \prod_{i=1}^{r} (I : J_i)$, а значит, $I : \left(\sum_{i=1}^{r} J_i\right) \subset \prod_{i=1}^{r} (I : J_i)$. Пусть далее $f \in \prod_{i=1}^{r} (I : J_i)$. Тогда для $1 \le i \le r$ $f \in I : J_i$, т.е. для любых $g_i \in J_i$, $i = \overline{1,r}$, $fg_i \in I$. Отсюда для любого $g = \sum_{i=1}^{r} g_i \in \sum_{i=1}^{r} J_i$ $fg \in I$, т.е. $f \in I : \left(\sum_{i=1}^{r} J_i\right)$.
Итак, формула (2) справедлива.

Докажем (3). Пусть $f \in (I : J) : K$. Тогда для любого $h \in K$ $fh \in I : J$. Отсюда для любого $g \in J$ $fhg \in I$. Таким образом, для любого $h \in K$ и любого $g \in J$ $fhg \in I$. Возьмем любой элемент $p \in JK$. Тогда $p = \sum_{i=1}^{n} h_i g_i$, где $h_i \in K$, $g_i \in J$. Так как для $1 \le i \le n$ $fh_i g_i \in I$, то $fp = \sum_{i=1}^{n} fh_i g_i \in I$. Следовательно, $f \in I : JK$, т.е. $(I : J) : K \subset I : JK$. Пусть теперь $f \in I : JK$. Тогда для любого $p \in JK$ $fp \in I$. Следовательно, для любого $h \in K$ и любого $g \in J$ $fhg \in I$. Отсюда для любого $h \in K$ $fh \in I : J$, т.е. $f \in (I : J) : K$. □

Если f – полином, а I – идеал, то будем писать $I : f$ вместо $I : < f >$.

Следствие 2. $I : < f_1,\ldots,f_r > = \prod_{i=1}^{r} I : f_i$.

Теорема 3. *Пусть идеал* $I \subset k[x_1,\ldots,x_n]$ *и* $g \in k[x_1,\ldots,x_n]$. *Если* $I \cap < g > = < h_1,\ldots,h_p >$, *где* $h_i \in k[x_1,\ldots,x_n]$, *то* $I : g = < \frac{h_1}{g},\ldots,\frac{h_p}{g} >$.

Доказательство. Возьмем любой элемент $a \in < g >$. Тогда существует $b \in k[x_1,\ldots,x_n]$ такой, что $a = bg$. Так как $I \cap < g > = < h_1,\ldots,h_p >$, то $h_i \in < g >$, а поэтому g делит все h_i, где $1 \le i \le p$. Поэтому $\frac{h_i}{g}$ – полиномы. Пусть $f \in < \frac{h_1}{g},\ldots,\frac{h_p}{g} >$. Тогда для любого $a \in < g >$ $af = bgf =$

$bg(\sum_{i=1}^{p}\frac{c_i h_i}{g}) = b\sum_{i=1}^{p} c_i h_i \in < h_1,\ldots,h_p > = I \ \mathbf{I} \ < g > \subset I$. Следовательно, $f \in I : g$. Пусть теперь $f \in I : g$. Тогда $fg \in I$. Так как $fg \in < g >$, то $fg \in I \ \mathbf{I} < g >$. Следовательно, $fg = \sum_{i=1}^{p} c_i h_i$, где $c_i \in k[x_1,\ldots,x_n]$. Отсюда $f = \sum_{i=1}^{p}\frac{c_i h_i}{g}$, т.е. $f \in < \frac{h_1}{g},\ldots,\frac{h_p}{g} >$. □

Эта теорема позволяет построить *алгоритм для вычисления базиса частного идеалов*. Пусть $I = < f_1,\ldots,f_r >$ и $J = < g_1,\ldots,g_s > = < g_1 > + \ldots + < g_s >$. Для нахождения базиса идеала $I : J$ сначала строим базис каждого идеала $I : g_i$, где $1 \le i \le s$. Для этого находим базис Грёбнера идеала $< tf_1, tf_2,\ldots,tf_r, (1 - t)g_i >$ по отношению к lex-упорядочению, где t больше всех x_j, и исключаем все элементы базиса, зависящие от t. Далее с помощью алгоритма деления делим каждый элемент построенного базиса на g_i и в результате получаем базис идеала $I : g_i$. Затем находим базис идеала $I : J$, вычисляя сначала базис идеала $I : < g_1, g_2 > = (I : g_1) \ \mathbf{I} \ (I : g_2)$, затем базис идеала $I : < g_1, g_2, g_3 > = (I : < g_1, g_2 >) \ \mathbf{I} \ (I : g_3)$ и т.д., и наконец базис идеала $I : J = (I : < g_1,\ldots,g_{s-1} >) \ \mathbf{I} \ (I : g_s)$.

3.4. НЕПРИВОДИМЫЕ МНОГООБРАЗИЯ И ПРОСТЫЕ ИДЕАЛЫ

Определение 1. Аффинное многообразие $V \subset k^n$ называется *неприводимым*, если оно может быть представлено в виде $V = V_1 \ \mathbf{U} \ V_2$, где V_1 и V_2 – аффинные многообразия, в том и только в том случае, когда или $V_1 = V$, или $V_2 = V$.

Определение 2. Идеал $I \subset k[x_1,\ldots,x_n]$ называется *простым*, если для любых $f, g \in k[x_1,\ldots,x_n]$ из $fg \in I$ следует, что или $f \in I$, или $g \in I$.

Теорема 1. *Пусть $V \subset k^n$ – аффинное многообразие. Тогда оно неприводимо тогда и только тогда, когда идеал $\mathbf{I}(V)$ является простым.*

Доказательство. Пусть V – неприводимо и $fg \in \mathbf{I}(V)$. Положим $V_1 = V \ \mathbf{I} \ \mathbf{V}(f)$, $V_2 = V \ \mathbf{I} \ \mathbf{V}(g)$. V_1, V_2 являются аффинными многообразиями. Покажем, что $V = V_1 \ \mathbf{U} \ V_2$. Имеем $V = \mathbf{V}(f_1,\ldots,f_s)$, где $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,s}$. Тогда $V_1 = \mathbf{V}(f_1,\ldots,f_s, f)$, $V_2 = \mathbf{V}(f_1,\ldots,f_s, g)$. Если $(a_1,\ldots,a_n) \in V$, то $f_i(a_1,\ldots,a_n) = 0$, $i = \overline{1,s}$. Так как $fg \in \mathbf{I}(V)$, то $f(a_1,\ldots,a_n)g(a_1,\ldots,a_n) = 0$. В случае $f(a_1,\ldots,a_n) = 0$ $(a_1,\ldots,a_n) \in V_1$, в случае же $g(a_1,\ldots,a_n) = 0$ $(a_1,\ldots,a_n) \in V_2$, т.е.

в любом случае $(a_1,\ldots,a_n) \in V_1 \cup V_2$, а поэтому $V \subset V_1 \cup V_2$. Если $(a_1,\ldots,a_n) \in V_1 \cup V_2$, то $f(a_1,\ldots,a_n)g(a_1,\ldots,a_n) = 0$, $f_i(a_1,\ldots,a_n) = 0$, $i = \overline{1,s}$. Следовательно, $(a_1,\ldots,a_n) \in V$ и $V_1 \cup V_2 = V$. Так как V неприводимо, то $V_1 = V$ или $V_2 = V$. Пусть $V = V_1 = V \mathbf{I} \mathbf{V}(f)$. Тогда на V f равен нулю, т.е. $f \in \mathbf{I}(V)$ и идеал $\mathbf{I}(V)$ является простым.

Пусть теперь идеал $\mathbf{I}(V)$ прост, а $V = V_1 \cup V_2$. Предположим, что $V_1 \neq V$. Покажем, что $\mathbf{I}(V) = \mathbf{I}(V_2)$. Так как $V_2 \subset V$, то $\mathbf{I}(V) \subset \mathbf{I}(V_2)$. Имеем $\mathbf{I}(V) \subsetneq \mathbf{I}(V_1)$, ибо $V_1 \subsetneq V$. Следовательно, существует $f \in \mathbf{I}(V_1) - \mathbf{I}(V)$. Пусть произвольный элемент $g \in \mathbf{I}(V_2)$. Так как $V = V_1 \cup V_2$, то $fg = 0$ на V, а значит, $fg \in \mathbf{I}(V)$. Следовательно, или $f \in \mathbf{I}(V)$, или $g \in \mathbf{I}(V)$. Так как $f \notin \mathbf{I}(V)$, то $g \in \mathbf{I}(V)$. Отсюда следует, что $\mathbf{I}(V) = \mathbf{I}(V_2)$. Тогда ввиду инъективности $\mathbf{I}$ имеем $V = V_2$, т.е. V неприводимо. □

Предложение 1. *Простой идеал $I \subset k[x_1,\ldots,x_n]$ является радикальным.*

Доказательство. Пусть $f^m \in I$. Покажем, что $f \in I$. Если $f \notin I$, то $f \cdot f^{m-1} \in I$, а значит, $f^{m-1} \in I$. Далее заключаем, что $f^{m-2} \in I, \ldots, f^2 \in I$, т.е. $f \in I$. □

Следствие 1. *Пусть поле k алгебраически замкнуто. Тогда отображения $\mathbf{I}$ и $\mathbf{V}$ задают взаимно однозначное соответствие между неприводимыми многообразиями в k^n и простыми идеалами в $k[x_1,\ldots,x_n]$.*

Предложение 2. *Пусть полином $f \in \mathbf{C}[x_1,\ldots,x_n]$ неприводим. Тогда многообразие $\mathbf{V}(f)$ неприводимо.*

Доказательство. Покажем, что идеал $\mathbf{I}(\mathbf{V}(f)) = \langle f \rangle$ прост. Действительно, если $f_1 f_2 \in \langle f \rangle$, то $f_1 f_2 = fh$, где $h \in \mathbf{C}[x_1,\ldots,x_n]$. На основании теоремы 1 из п. 2.2 f делит f_1 или f_2, т.е. $f_1 \in \langle f \rangle$ или $f_2 \in \langle f \rangle$. □

В случае задания многообразия V параметрическими уравнениями в задаче неявного представления требуется найти уравнения, определяющие замыкание Зарисского параметризованного множества. Рассмотрение задачи неявного представления начнем со случая полиномиальной параметризации

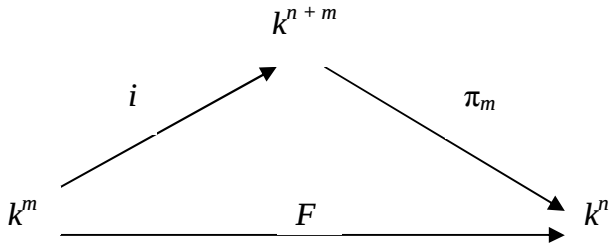
$$\begin{aligned} x_1 &= f_1(t_1,\ldots,t_m), \\ &\ldots\ldots\ldots\ldots\ldots \\ x_n &= f_n(t_1,\ldots,t_m), \end{aligned} \qquad (1)$$

где $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,n}$. Система (1) описывает функцию $F : k^m \to k^n$, определяемую формулой $F(t_1,\ldots,t_m) = (f_1(t_1,\ldots,t_m),\ldots,f_n(t_1,\ldots,t_m))$. В этом случае $F(k^m) \subset k^n$ – подмножество в k^n, которое параметризовано уравнениями (1). Множество $F(k^m)$ может не быть аффинным многообразием, однако $\overline{F(k^m)}$ – аффинное многообразие. Образуем идеал $I = < x_1 - f_1,\ldots,x_n - f_n > \subset k[t_1,\ldots,t_m, x_1,\ldots,x_n]$. Точки многообразия $\mathbf{V}(I)$ имеют координаты $(t_1,\ldots,t_m, f_1(t_1,\ldots,t_m),\ldots,f_n(t_1,\ldots,t_m))$, т.е. $\mathbf{V}(I)$ можно рассматривать как график функции F. Рассмотрим две функции $i : k^m \to k^{n+m}$, $\pi_m : k^{n+m} \to k^n$, определенные следующим образом:

$$i(t_1,\ldots,t_m) = (t_1,\ldots,t_m, f_1(t_1,\ldots,t_m),\ldots,f_n(t_1,\ldots,t_m)),$$

$$\pi_m(t_1,\ldots,t_m, x_1,\ldots,x_n) = (x_1,\ldots,x_n).$$

Эти функции задают следующую диаграмму множеств и отображений:



(2)

Заметим, что $F = \pi_m \circ i$, $i(k^m) = \mathbf{V}(I)$. Таким образом, $F(k^m) = \pi_m(i(k^m)) = \pi_m(\mathbf{V}(I))$, т.е. параметризованное множество – проекция графика параметризации.

Теорема 2 (полиномиальное неявное представление). *Пусть k – бесконечное поле и $F : k^m \to k^n$ – функция, определенная полиномиальной параметризацией (1). Пусть $I_m = I \cap k[x_1,\ldots,x_n]$ – m-й исключающий идеал для $I = < x_1 - f_1,\ldots,x_n - f_n > \subset k[t_1,\ldots,t_m, x_1,\ldots,x_n]$. Тогда $\mathbf{V}(I_m) = \overline{F(k^m)}$.*

Доказательство. Рассмотрим многообразие $V = \mathbf{V}(I) \subset k^{n+m}$, тогда V – график функции $F : k^m \to k^n$. Пусть сначала $k = \mathbf{C}$. Так как $\mathbf{C}$ – алгебраически замкнутое поле, а $F(C^m) = \pi_m(V)$, то из теоремы 1 п. 3.3 заключаем, что $\overline{F(k^m)} = \overline{\pi_m(V)} = \mathbf{V}(I_m)$. Итак, в случае $k = \mathbf{C}$ теорема доказана.

Пусть теперь k – подполе в $\mathbf{C}$, т.е. $k \subset \mathbf{C}$ и операции в k такие же как в $\mathbf{C}$. Такое поле $k \supset \mathbf{Q}$, ибо $1 \in k$, а тогда $\mathbf{Z}$, $\mathbf{Q} \subset k$. Следовательно, k – бесконечное поле. Будем далее заменять k на $\mathbf{C}$, а затем возвращаться в k.

Индекс k или $\mathbf{C}$ будет указывать, с каким полем мы работаем. Таким образом, $\mathbf{V}_k(I_m)$ – многообразие в k^n, а $V_{\mathbf{C}}(I_m)$ – большее множество решений в $\mathbf{C}^n$. Заметим, что переход к большему полю не меняет исключающего идеала I_m, так как на алгоритм, вычисляющий I_m, не влияет переход от k к $\mathbf{C}$. Покажем, что $\mathbf{V}_k(I_m) = \overline{F(k^m)}$. Имеем $F(k^m) = \pi_m(V_k) \subset \mathbf{V}_k(I_m)$. Рассмотрим произвольное многообразие $Z_k = \mathbf{V}_k(g_1,\ldots,g_s) \subset k^n$ такое, что $Z_k \supset F(k^m)$. По определению многообразия Z_k полиномы g_i обращаются в нуль на Z_k, а тогда они равны нулю и на меньшем множестве $F(k^m)$. Следовательно, $g_i \circ F$ равны нулю на всем k^m. Так как $g_i \in k[x_1,\ldots,x_n]$, а $f_i \in k[t_1,\ldots,t_m]$, то $g_i \circ F \in k[t_1,\ldots,t_m]$. Таким образом, $g_i \circ F$ – полиномы, тождественно равные нулю на k^m. Так как поле k бесконечно, то полиномы $g_i \circ F$ – нулевые. Это означает, что $g_i \circ F$ обращаются в нуль на $\mathbf{C}^m$, а значит, g_i равны нулю на $F(\mathbf{C}^m)$. Следовательно, $Z_{\mathbf{C}} = V_{\mathbf{C}}(g_1,\ldots,g_s) \subset \mathbf{C}^n$ – многообразие, содержащее $F(\mathbf{C}^m)$. Так как $V_{\mathbf{C}}(I_m) \subset Z_{\mathbf{C}}$, то $(V_{\mathbf{C}}(I_m)\ \mathbf{I}\ k^n) \subset (Z_{\mathbf{C}}\ \mathbf{I}\ k^n)$, т.е. $\mathbf{V}_k(I_m) \subset Z_k$. Значит, $\mathbf{V}_k(I_m) = \overline{F(k^m)}$.

Пусть теперь поле k не содержится в $\mathbf{C}$. Тогда существует алгебраически замкнутое поле K такое, что $k \subset K$. Теперь осталось заменить в наших рассуждениях $\mathbf{C}$ на K. □

Теорема 2 дает следующий *алгоритм построения неявного представления для полиномиальной параметризации*: пусть даны параметрические уравнения (1). Рассмотрим идеал $I = \langle x_1 - f_1,\ldots,x_n - f_n \rangle$ и найдем его базис Грёбнера по отношению к lex-упорядочению, где каждое t_i больше любого x_j. По теореме об исключении элементы базиса, не зависящие от $t_1,\ldots,t_m$, образуют базис Грёбнера идеала I_m, и по теореме 2 они определяют замыкание Зарисского в k^n, содержащее параметризованное множество.

Теорема 3. *Пусть поле k бесконечно, а многообразие $V \subset k^n$ задано параметрически уравнениями (1), где $f_i \in k[t_1,\ldots,t_m]$, $i = \overline{1,n}$. Тогда V неприводимо.*

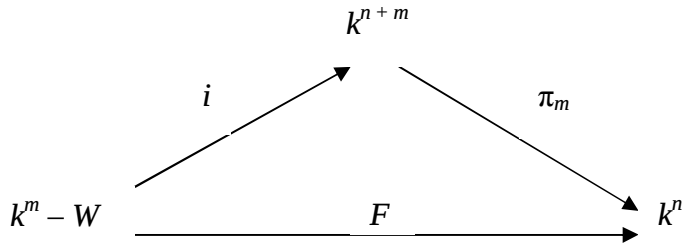
Доказательство. Пусть $F : k^m \to k^n$ – отображение, заданное формулой $F(t_1,\ldots,t_m) = (f_1(t_1,\ldots,t_m),\ldots,f_n(t_1,\ldots,t_m))$. Тогда $V = \overline{F(k^m)}$, $\mathbf{I}(V) = \mathbf{I}(F(k^m))$. Для любого $g \in k[x_1,\ldots,x_n]$ функция $g \circ F \in k[t_1,\ldots,t_m]$. При этом $g \circ F = g(f_1(t_1,\ldots,t_m),\ldots,f_n(t_1,\ldots,t_m))$. Так как поле k бесконечно, то $\mathbf{I}(V) = \mathbf{I}(F(k^m))$ – множество полиномов в $k[x_1,\ldots,x_n]$, композиция которых с F является нулевым полиномом в $k[t_1,\ldots,t_m]$, т.е. $\mathbf{I}(V) = \{g \in k[x_1,\ldots,x_n] : g \circ F = 0\}$. Пусть теперь $gh \in \mathbf{I}(V)$. Тогда $(gh) \circ F = (g \circ F)(h \circ F) = 0$. Следовательно, либо $g \circ F = 0$, либо $h \circ F = 0$. Это означает, что или $g \in \mathbf{I}(V)$,

или $h \in \mathbf{I}(V)$. Таким образом, $\mathbf{I}(V)$ – простой идеал, а значит, V неприводимо. □

Перейдем теперь к рациональной параметризации. Рациональная параметризация задается системой

$$x_1 = \frac{f_1(t_1,...,t_m)}{g_1(t_1,...,t_m)},\ldots, x_n = \frac{f_n(t_1,...,t_m)}{g_n(t_1,...,t_m)}, \tag{3}$$

где $f_i, g_i \in k[t_1,\ldots,t_m]$, $i = \overline{1,n}$. Пусть $W = \mathbf{V}(g_1g_2\ldots g_n) \subset k^m$. Тогда $F(t_1,\ldots,t_m) = (\frac{f_1(t_1,...,t_m)}{g_1(t_1,...,t_m)},\ldots,\frac{f_n(t_1,...,t_m)}{g_n(t_1,...,t_m)})$ задает отображение $F : k^m - W \to k^n$. Решить задачу неявного представления многообразия в этом случае – это найти наименьшее многообразие в k^n, содержащее $F(k^m - W)$. В этом случае диаграмма множеств и отображений имеет вид



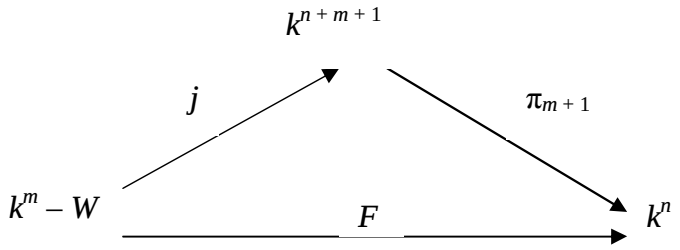
(4)

Имеет место включение $i(k^m - W) \subset \mathbf{V}(I)$, где $I = < g_1x_1 - f_1,\ldots,g_nx_n - f_n >$ – идеал, построенный освобождением от знаменателей. В этом случае $\mathbf{V}(I)$ не обязательно является наименьшим многообразием, содержащим $i(k^m - W)$. Поэтому мы изменим идеал I с помощью добавления лишней размерности для контроля знаменателей. Рассмотрим кольцо полиномов $k[y, t_1,\ldots,t_m, x_1,\ldots,x_n]$, соответствующее аффинному пространству k^{n+m+1}. Пусть $g = g_1g_2\ldots g_n$. Тогда $W = \mathbf{V}(g)$. Рассмотрим идеал $J = < g_1x_1 - f_1,\ldots,g_nx_n - f_n, 1 - gy > \subset k[y, t_1,\ldots,t_m, x_1,\ldots,x_n]$. Из уравнения $1 - gy = 0$ имеем, что знаменатели $g_1,\ldots,g_n$ не равны нулю на $\mathbf{V}(J)$. Преобразуем диаграмму (4). Для этого рассмотрим отображения $j : k^m - W \to k^{n+m+1}$, $\pi_{m+1} : k^{n+m+1} \to k^n$, заданные формулами:

$$j(t_1,\ldots,t_m) = (\frac{1}{g(t_1,...,t_m)}, t_1,\ldots,t_m, \frac{f_1(t_1,...,t_m)}{g_1(t_1,...,t_m)},\ldots,\frac{f_n(t_1,...,t_m)}{g_n(t_1,...,t_m)}),$$

$$\pi_{m+1}(y, t_1,\ldots,t_m, x_1,\ldots,x_n) = (x_1,\ldots,x_n).$$

В этом случае диаграмма имеет вид



Имеем $F = \pi_{m+1} \circ j$. Покажем, что $j(k^m - W) = \mathbf{V}(J)$ в k^{n+m+1}. Из определений j и J получаем $j(k^m - W) \subset \mathbf{V}(J)$. Пусть теперь $(y, t_1,\ldots,t_m, x_1,\ldots,x_n) \in \mathbf{V}(J)$. Тогда из уравнения $g(t_1,\ldots,t_m)y = 1$ следует, что ни один полином g_i не равен нулю в точке $(t_1,\ldots,t_m)$. Значит, равенства $g_i(t_1,\ldots,t_m)x_i = f_i(t_1,\ldots,t_m)$ могут быть разрешены относительно x_i. $x_i = \dfrac{f_i(t_1,\ldots,t_m)}{g_i(t_1,\ldots,t_m)}$. Так как $y = \dfrac{1}{g(t_1,\ldots,t_m)}$, то $(y, t_1,\ldots,t_m, x_1,\ldots,x_n) \in j(k^m - W)$, т.е. $\mathbf{V}(J) \subset j(k^m - W)$. Далее из равенств $F = \pi_{m+1} \circ j$ и $j(k^m - W) = \mathbf{V}(J)$ получаем

$$F(k^m - W) = \pi_{m+1}(j(k^m - W)) = \pi_{m+1}(\mathbf{V}(J)). \qquad (5)$$

Таким образом, параметризованное множество равно проекции многообразия $\mathbf{V}(J)$.

Теорема 4. *Пусть k – бесконечное поле, а $F : k^m - W \to k^n$ – функция, заданная рациональной параметризацией (3). Пусть $J_m = J \cap k[x_1,\ldots,x_n]$ есть $(m+1)$-й исключающий идеал идеала $J = < g_1x_1 - f_1,\ldots,g_nx_n - f_n, 1 - gy > \subset k[y, t_1,\ldots,t_m, x_1,\ldots,x_n]$, где $g = g_1g_2\ldots g_n$. Тогда $\mathbf{V}(J_{m+1}) = \overline{F(k^m - W)}$ в k^n.*

Доказательство. Доказательство этой теоремы повторяет доказательство теоремы 2. Здесь нужно исследовать уравнение (5) и учитывать, что полином, равный нулю на $k^m - W$, является нулевым полиномом. Действительно, если $g \neq 0$, а f обращается в нуль на $k^m - \mathbf{V}(g)$, то $fg = 0$ на k^m, т.е. f –нулевой полином. □

Суть теоремы 4 состоит в следующем: рассматриваем рациональную параметризацию (2), избавляемся от знаменателей и добавляем новую переменную y, чтобы не дать знаменателям обратиться в ноль: $g_1x_1 = f_1,\ldots,g_nx_n = f_n$, $g_1\ldots g_n = 1$. Тогда исключение переменных $y, t_1,\ldots,t_m$ решает задачу неявного представления.

Итак, теорема 4 определяет следующий *алгоритм построения неявного представления в случае рациональной параметризации*. А именно, пусть $x_i = \frac{f_i}{g_i}$, где $f_i, g_i \in k[t_1,\ldots,t_m]$, $i = \overline{1,n}$. Введем новую переменную y и рассмотрим идеал $J = < g_1x_1 - f_1,\ldots,g_nx_n - f_n,\ 1 - gy >$, где $g = g_1g_2\ldots g_n$. Найдем базис Грёбнера идеала J по отношению к lex-упорядочению, где y и каждое t_i больше любого x_j. Элементы базиса Грёбнера, не зависящие от y, $t_1,\ldots,t_m$ определяют в k^n замыкание Зарисского параметризованного множества.

Теорема 5. *Пусть поле k бесконечно, а многообразие V задано рациональной параметризацией (3). Тогда V неприводимо.*

Доказательство. Пусть $W = \mathbf{V}(g_1,\ldots,g_n)$, а $F : k^m - W \to k^n$ – отображение, определенное формулой $F(t_1,\ldots,t_m) = (\frac{f_1(t_1,\ldots,t_m)}{g_1(t_1,\ldots,t_m)},\ldots,\frac{f_n(t_1,\ldots,t_m)}{g_n(t_1,\ldots,t_m)})$. Тогда $V = \overline{F(k^m - W)}$, а значит, $\mathbf{I}(V)$ – это множество полиномов $h \in k[x_1,\ldots,x_n]$ таких, что функция $h \circ F$ равна нулю для всех $(t_1,\ldots,t_m) \in k^m - V$. Пусть $h \in k[x_1,\ldots,x_n]$. Так как $g_1(t_1,\ldots,t_m)g_2(t_1,\ldots,t_m)\ldots g_n(t_1,\ldots,t_m) \neq 0$ для всех $(t_1,\ldots,t_m) \in k^m - W$, то функция $(g_1\ldots g_n)^N(h \circ F)$ обращается в нуль в точности в тех точках из $k^m - W$, в которых обращается в нуль функция $h \circ F$. Если N – полная степень полинома $h \in k[x_1,\ldots,x_n]$, то $(g_1\ldots g_n)^N(h \circ F) \in k[t_1,\ldots,t_m]$. Таким образом, $h \in \mathbf{I}(V)$ в том и только в том случае, когда $(g_1\ldots g_n)^N(h \circ F) = 0$ для всех $t \in k^m - W$. Тогда $(g_1\ldots g_n)^N(h \circ F) = 0$ – нулевой полином в $k[t_1,\ldots,t_m]$. Таким образом, доказано, что $h \in \mathbf{I}(V)$ тогда и только тогда, когда $(g_1\ldots g_n)^N(h \circ F) = 0 \in k[t_1,\ldots,t_m]$. Покажем теперь, что $\mathbf{I}(V)$ – простой идеал. Пусть $p, q \in k[x_1,\ldots,x_n]$ и $pq \in \mathbf{I}(V)$. Если полная степень полинома p равна M, а полная степень полинома q равна N, то полная степень полинома pq равна $M + N$. Тогда $(g_1\ldots g_n)^{M+N}(p \circ F)(q \circ F) = 0$. Но этот полином – произведение полиномов $(g_1\ldots g_n)^M(p \circ F)$ и $(g_1\ldots g_n)^N(q \circ F)$ из $k[t_1,\ldots,t_m]$. Таким образом, один из них должен быть нулевым полиномом, а значит, или $p \in \mathbf{I}(V)$, или $q \in \mathbf{I}(V)$. Следовательно, идеал $\mathbf{I}(V)$ прост и многообразие V неприводимо. □

Простейшее многообразие в k^n, которое можно задать с помощью полиномиальной параметризации, это точка $\{(a_1,\ldots,a_n)\}$. Это многообразие можно задать параметрически так: $f_i(t_1,\ldots,t_m) = a_i$, $1 \le i \le n$. Очевидно, что оно неприводимо. Отсюда следует, что идеал $\mathbf{I}(\{(a_1,\ldots,a_n)\})$ является простым. Покажем, что $\mathbf{I}(\{(a_1,\ldots,a_n)\}) = < x_1 - a_1,\ldots,x_n - a_n >$. Действи-

тельно, $x_k^i = (x_k - a_k)q_k(x_k) + \alpha_{i,\,k}$, где $\alpha_{i,\,k} \in k$, а значит, $f \in \mathbf{I}(\{(a_1,\ldots,a_n)\})$ имеет вид $f = \sum_{k=1}^{n} h_k(x_k - a_k)$, $h_k \in k[x_1,\ldots,x_n]$.

Определение 3. Идеал $I \subset k[x_1,\ldots,x_n]$ называется *максимальным*, если $I \neq k[x_1,\ldots,x_n]$, и любой идеал J, содержащий I, равен либо I, либо $k[x_1,\ldots,x_n]$.

Определение 4. Идеал $I \subset k[x_1,\ldots,x_n]$ называется *собственным*, если он не совпадает с $k[x_1,\ldots,x_n]$.

Теорема 6. *Пусть k – произвольное поле, а $a_1,\ldots,a_n \in k$. Тогда идеал I вида $< x_1 - a_1,\ldots,x_n - a_n >$ максимален.*

Доказательство. Предположим, что идеал J строго содержит I. Тогда существует элемент $f \in J$ такой, что $f \notin I$. Используя алгоритм деления, запишем f в виде $f = A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n) + b$, где $b \in k$. Так как $A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n) \in I$ и $f \in I$, то $b \neq 0$. Но $f \in J$ и $I \subset J$, следовательно, $b = f - (A_1(x_1 - a_1) + \ldots + A_n(x_n - a_n)) \in J$. Так как $b \neq 0$, то $\frac{1}{b} \cdot b = 1 \in J$, а значит, $J = k[x_1,\ldots,x_n]$. □

Так как $\mathbf{V}(x_1 - a_1,\ldots,x_n - a_n) = \{(a_1,\ldots,a_n)\}$, то любая точка $(a_1,\ldots,a_n) \in k^n$, соответствует максимальному идеалу в $k[x_1,\ldots,x_n]$, а именно идеалу $< x_1 - a_1,\ldots,x_n - a_n >$. Если k не является алгебраически замкнутым, то обратное утверждение неверно.

Теорема 7. *Пусть k – произвольное поле. Тогда любой максимальный идеал в $k[x_1,\ldots,x_n]$ прост.*

Доказательство. Пусть I – собственный идеал, не являющийся простым. Тогда существуют $f, g \notin I$ такие, что $fg \in I$. Рассмотрим идеал $< f > + I$. Этот идеал строго содержит I, потому что $f \notin I$. Если $< f > + I = k[x_1,\ldots,x_n]$, то существует $c \in k[x_1,\ldots,x_n]$, существует $h \in I$ такие, что $1 = cf + h$. Умножая это равенство на g, получаем $g = cfg + hg \in I$, но это противоречит выбору g. Следовательно, $< f > + I$ – собственный идеал, строго содержащий I, т.е. I не максимален. □

Заметим, что идеал $< x_1 - a_1,\ldots,x_n - a_n >$ прост в $k[x_1,\ldots,x_n]$, даже если поле k конечно.

Теорема 8. *Пусть поле k алгебраически замкнуто. Тогда любой максимальный идеал в $k[x_1,\ldots,x_n]$ имеет вид $< x_1 - a_1,\ldots,x_n - a_n >$, где $a_1,\ldots,a_n \in k$.*

Доказательство. Пусть $I \subset k[x_1,\ldots,x_n]$ – максимальный идеал. Так как $I \neq k[x_1,\ldots,x_n]$, то $\mathbf{V}(I) \neq \varnothing$, ибо в противном случае $I = k[x_1,\ldots,x_n]$ (теорема

1 из п. 3.1). Поэтому существует $(a_1,\ldots,a_n) \in \mathbf{V}(I)$. Следовательно, $\mathbf{I}(\mathbf{V}(I)) \subset \mathbf{I}(\{(a_1,\ldots,a_n)\})$. Но по сильной теореме о нулях $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. Так как I максимален, то он прост и, следовательно, радикален, т.е. $\sqrt{I} = I$. Поэтому $I \subset \mathbf{I}(\{(a_1,\ldots,a_n)\}) = < x_1 - a_1,\ldots,x_n - a_n > \subset k[x_1,\ldots,x_n]$. Так как I $\neq$ максимален, то $I = < x_1 - a_1,\ldots,x_n - a_n >$.

Следствие 2. *Пусть поле k алгебраически замкнуто. Тогда существует взаимно однозначное соответствие между точками в k^n и максимальными идеалами кольца $k[x_1,\ldots,x_n]$.*

3.5. РАЗЛОЖЕНИЕ МНОГООБРАЗИЯ В ОБЪЕДИНЕНИЕ НЕПРИВОДИМЫХ

Предложение 1 (условие обрыва убывающих цепей). *Любая убывающая цепь многообразий $V_1 \supset V_2 \supset V_3 \supset \ldots$ в k^n стабилизируется, т.е. существует $N \in \mathbf{N}$ такое, что $V_N = V_{N+1} = V_{N+2} = \ldots$.*

Доказательство. Переходя к идеалам, получим возрастающую цепь $\mathbf{I}(V_1) \subset \mathbf{I}(V_2) \subset \ldots \subset \mathbf{I}(V_s) \subset \ldots$ Из условия обрыва возрастающих цепей идеалов следует, что существует N такое, что $\mathbf{I}(V_N) = \mathbf{I}(V_{N+1}) = \ldots$ Так как $\mathbf{V}(\mathbf{I}(V)) = V$ для любого многообразия V, то $V_N = V_{N+1} = V_{N+2} = \ldots$. □

Теорема 1. *Пусть $V \subset k^n$ – аффинное многообразие. Тогда V может быть представлено в виде конечного объединения неприводимых многообразий V_i : $V = V_1 \cup \ldots \cup V_m$.*

Доказательство. Пусть V – аффинное многообразие, которое нельзя представить в виде конечного объединения неприводимых многообразий. Тогда V не является неприводимым, а значит, $V = V_1 \cup V_1'$, где $V \neq V_1$, $V \neq V_1'$. Хотя бы одно из многообразий V_1, V_1' не является объединением конечного числа неприводимых многообразий, ибо в противном случае V можно было бы представить в этом виде. Пусть, например, V_1 не является конечным объединением неприводимых многообразий. Аналогично получаем, что $V_1 = V_2 \cup V_2'$, где $V_1 \neq V_2$, $V_1 \neq V_2'$ и V_2 не является объединением конечного числа неприводимых многообразий. Продолжая это построение, мы получим бесконечную последовательность многообразий $V \supset V_1 \supset V_2 \supset \ldots$, где $V \neq V_1 \neq V_2 \neq \ldots$, но это противоречит предложению 1. □

Определение 1. Пусть $V \subset k^n$ – аффинное многообразие. Разложение $V = V_1 \cup \ldots \cup V_m$, где многообразия V_i неприводимы, называется *минимальным разложением* (или *неизбыточным объединением*), если V_i не принадлежит V_j при $i \neq j$.

Теорема 2. *Пусть $V \subset k^n$ – аффинное многообразие. Тогда существует минимальное разложение $V = V_1 \cup \ldots \cup V_m$ (т.е. каждое V_i – неприводимое многообразие и $V_i \neq V_j$ при $i \neq j$), причем это разложение единственно с точностью до порядка, в котором записаны многообразия.*

Доказательство. На основании теоремы 1 V может быть представлено в виде $V = V_1 \cup \ldots \cup V_m$, где V_i – неприводимы. Предположим, что некоторое V_i лежит в каком-то V_j, где $i \neq j$. Тогда мы можем исключить V_i из разложения, и тогда V будет объединением V_l при $l \neq i$. Продолжая этот процесс, мы получим минимальное разложение. Докажем единственность этого разложения. Пусть $V = V_1' \cup \ldots \cup V_l'$ – другое минимальное разложение многообразия V. Тогда $V_i = V_i \cap V = V_i \cap (V_1' \cup \ldots \cup V_l') = (V_i \cap V_1') \cup \ldots \cup (V_i \cap V_l')$. Так как V_i неприводимо, то $V_i = V_i \cap V_j'$ для некоторого j, т.е. $V_i \subset V_j'$. Аналогично, существует такое s, что $V_j' \subset V_s$. Таким образом, $V_i \subset V_j' \subset V_s$. Из минимальности разложения следует, что $i = s$, т.е. $V_i = V_j'$. Следовательно, любое V_i содержится в разложении $V = V_1' \cup \ldots \cup V_l'$, а поэтому $m \leq l$. Аналогично доказывается, что $l \leq m$, т.е. $l = m$. Следовательно, $l = m$, а набор V_j' – перестановка набора V_i. □

Предложение 2. *Пусть $f \in \mathbf{C}[x_1,\ldots,x_n]$ и пусть $f = f_1^{a_1} \ldots f_s^{a_s}$ – разложение полинома f на неприводимые множители. Тогда $\mathbf{V}(f) = \mathbf{V}(f_1) \cup \ldots \cup \mathbf{V}(f_s)$ – разложение многообразия $V(f)$ на неприводимые компоненты и $\mathbf{I}(\mathbf{V}(f)) = \langle f_1 \ldots f_s \rangle$.*

Доказательство. На основании теоремы 1 из п. 1.1 $\mathbf{V}(f) = \mathbf{V}(f_1^{a_1}) \cup \mathbf{V}(f_2^{a_2}) \cup \ldots \cup \mathbf{V}(f_s^{a_s})$. Так как $\mathbf{V}(f_i^{a_i}) = \mathbf{V}(f_i)$, а $\mathbf{V}(f_i)$ неприводимы на основании предложения 2 из п. 3.4, то $\mathbf{V}(f) = \mathbf{V}(f_1) \cup \ldots \cup \mathbf{V}(f_s)$ – разложение многообразия $V(f)$ на неприводимые компоненты. Равенство $\mathbf{I}(\mathbf{V}(f)) = \langle f_1 \ldots f_s \rangle$ вытекает из предложения 2 п. 3.2. □

Предложение 3. *Идеал $I \subset k[x_1,\ldots,x_n]$ является простым тогда и только тогда, когда для любых идеалов J, K таких, что $JK \subset I$, либо $J \subset I$, либо $K \subset I$.*

Доказательство. Пусть идеал I является простым. Покажем, что либо $J \subset I$, либо $K \subset I$. В случае $J \subset I$ все доказано. Если J не содержится в I, то существует $f \in J$ такой, что $f \notin I$. Тогда для любого $g \in K$ $fg \in I$, а значит, $g \in I$. Следовательно, $K \subset I$. Пусть теперь для любых идеалов J, K таких, что $JK \subset I$, либо $J \subset I$, либо $K \subset I$. Покажем, что I – простой идеал. Если I не прост, то существуют $f \notin I$, $g \notin I$ такие, что $fg \in I$, а значит, $< fg > \subset I$. Следовательно, $< fg > = < f >< g > \subset I$, но $< f >$ не содержится в I, т.к. $f \notin I$, и $< g >$ не содержится в I. Получили противоречие. □

Предложение 4. *Пусть $I_1,\ldots,I_n$ – конечное множество идеалов, идеал P прост и $\bigcap_{i=1}^{n} I_i \subset P$. Тогда существует i, $1 \le i \le n$, такое, что $I_i \subset P$. Более того, если $P = \bigcap_{i=1}^{n} I_i$, то существует i такое, что $P = I_i$.*

Доказательство. Так как $\bigcap_{i=1}^{n} I_i \subset P$, то $I_1 \ldots I_n \subset I_1 \ldots I_{n-1} \cap I_n \subset I_1 \cap I_2 \cap \ldots \cap I_n \subset P$. Тогда на основании предложения 2 либо $I_n \subset P$, либо $I_1 \ldots I_{n-1} \subset P$. Если $I_n \subset P$, то все доказано. В противном случае $I_1 \ldots I_{n-1} \subset P$. Отсюда либо $I_{n-1} \subset P$, либо $I_1 \ldots I_{n-2} \subset P$. Следовательно, существует i такое, что $I_i \subset P$. Если $P = \bigcap_{i=1}^{n} I_i$, то для любого k $I_k \supset P$. С другой стороны, по доказанному существует i такое, что $I_i \subset P$, т.е. $I_i = P$. □

Теорема 3. *Пусть поле k алгебраически замкнуто. Тогда каждый радикальный идеал $I \subset k[x_1,\ldots,x_n]$ может быть однозначно записан в виде пересечения простых идеалов $I = P_1 \cap P_2 \cap \ldots \cap P_r$, где $P_i \not\subset P_j$ при $i \ne j$. (Как и в случае многообразий такое представление радикального идеала будем называть минимальным разложением или неизбыточным пересечением.)*

Доказательство. Имеем $\mathbf{V}(I) = V_1 \cup V_2 \cup \ldots \cup V_r$, где V_i, $i = \overline{1,r}$, – неприводимые многообразия и $V_i \not\subset V_j$ при $i \ne j$. Тогда $I = \mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(V_1) \cap \mathbf{I}(V_2) \cap \ldots \cap \mathbf{I}(V_r) = P_1 \cap P_2 \cap \ldots \cap P_r$, где P_i – простые идеалы. □

Частные идеалов следующим образом описывают простые идеалы, участвующие в минимальном разложении радикального идеала.

Теорема 4. *Пусть поле k алгебраически замкнуто, I – собственный радикальный идеал и $I = \bigcap_{i=1}^{r} P_i$ – минимальное разложение I. Тогда P_i – это в точности те простые собственные идеалы, которые имеют вид $I : f$, где $f \in k[x_1,\ldots,x_n]$.*

Лемма 1. *Пусть $P \subset k[x_1,\ldots,x_n]$ – простой идеал. Тогда $P : f = P$, если $f \notin P$, и $P : f = <1>$, если $f \in P$.*

Доказательство. Пусть $f \notin P$. Тогда для любого $g \in P : f \quad fg \in P$. Так как P – простой идеал, то $g \in P$. Следовательно, $P : f \subset P$. С другой стороны, $P \subset P : f$, т.е. $P : f = P$. Если $f \in P$, то для любого $g \in <1> \quad fg \in P$, т.е. $g \in P : f$. Значит, $P : f = <1>$.

Доказательство теоремы 4. Так как идеал I – собственный, то и идеалы P_i также являются собственными, ибо в противном случае было бы нарушено условие минимальности. Для любого $f \in k[x_1,\ldots,x_n]$ имеем $I : f = (\bigcap_{j=1}^{r} P_j) : f = \bigcap_{j=1}^{r} (P_j : f)$ (формула (1) из п. 3.3). Пусть теперь $I : f$ – собственный простой идеал. Тогда из предложения 4 и леммы 1 $I : f = P_i : f = P_i$ для некоторого i. Покажем, что любой простой идеал P_i можно получить таким образом. Возьмем полином $f \in (\bigcap_{\substack{j=1 \\ j\neq i}}^{r} P_j) - P_i$. Такой полином существует, так как разложение $\bigcap_{j=1}^{r} P_j$ минимально. Тогда $P_i : f = P_i$, $P_j : f = <1>$ при $j \neq i$. Следовательно, $I : f = \bigcap_{j=1}^{r} (P_j : f) = P_i$, т.е. $I : f$ – собственный простой идеал. □

В качестве примера рассмотрим многообразие $V = \mathbf{V}(f_1,\ldots,f_5)$, где $f_1 = B(A + C) + L + N$, $f_2 = B(2B^2 - AC + 2K + M) + CL - 2AN$, $f_3 = L(6B^2 - AC + K + M) - B(CK + AM) + N(A^2 - 2K)$, $f_4 = B(6L^2 - KM) - L(CK + AM) + 2AKN$, $f_5 = L(2L^2 - KM) + K^2N$. Найдем разложение многообразия на неприводимые компоненты. Заметим, что V принадлежит многообразию центра кубической системы нелинейных колебаний

$$\dot{x} = y,\ \dot{y} = -x + Ax^2 + 3Bxy + Cy^2 + Kx^3 + 3Lx^2y + Mxy^2 + Ny^3.$$

Образуем идеал $J = <f_1,\ldots,f_5> \subset \mathbf{C}[L, M, K, N, B, C, A]$. Будем использовать lex-упорядочение с порядком $L > M > K > N > B > C > A$. На-

ходя для J базис Грёбнера (используем систему Mathematica 5.0), имеем $J = <\alpha\beta_1, \beta_2,\ldots\beta_{21}>$, где $\alpha = (BC + N)^3 + 2B^4[AB + 2(BC + N)]$, $\beta_1 = A^3(2A + C)^2 + 4B^2[A^2(4A + 3C) + B^2(5A + 4C)]$, $\beta_i \in \mathbf{C}[L, M, K, N, B, C, A]$, $i = \overline{2,21}$. Далее находим $J + <\alpha> = <\alpha, A^3(137A^4 + 244A^3C + 153A^2C^3 + 41AC^3 + 4C^4)\beta, \alpha_3,\ldots,\alpha_{17}>$, где $\beta = (BC + N)[B(A + C) + N] - B^2K$, $\alpha_i \in \mathbf{C}[L, M, K, N, B, C, A]$, $i = \overline{3,17}$. Идеал $J + <\alpha, \beta>$ через базис Грёбнера представляется в виде

$J + <\alpha, \beta> = <\alpha, \beta, A^3\gamma, \gamma_4,\ldots,\gamma_{10}>$, где $\gamma = AB(2B^2 - K) + (BC + N)(A^2 + 4B^2 + K)$, $\gamma_i \in \mathbf{C}[L, M, K, N, B, C, A]$, $i = \overline{4,10}$. Образуем идеал $I_1 = J + <\alpha, \beta, \gamma>$. Находя для I_1 базис Грёбнера, имеем $I_1 = <\alpha, \beta, \gamma, g_4, g_5, g_6, f_1>$, где $g_4 = B[A^2(4B^2 - K) + K^2] + (BC + N)[A(A^2 + 10B^2) + 4B(BC + N)]$, $g_5 = B(2B^2 + 2K + M) - (2A + C)(BC + N)$, $g_6 = B[2B^2(2A + C) + C(3K + M)] + (BC + N)[6B^2 - C(3A + C) - M]$. Найдем теперь по методу, изложенному в п. 3.3 частное идеалов J и I_1. Имеем $J : I_1 = <\beta_1, v_2,\ldots,v_{10}, f_1>$, где $v_2 = B(3A + 2C)(6A^2 + 9AC + 4C^2) + 2(5A + 4C)[B^3 + N(2A + C)]$, $v_3 = A^3(2A + C) - 2B(5A + 4C)[B(A + 2C) + 2N]$, $v_4 = 2B^3(5A + 4C) + AB(10A^2 + 15AC + 6C^2) + 2N[4B^2 + 3A(2A + C)]$, $v_5 = 2(5A + 4C)[B^2(A^2 + 6AC + 6C^2) - 6N^2] - A^2[A(8A^2 + 15AC + 6C^2) + 4BN]$, $v_6 = 2B[B(A + 2C) + 2N] - A(A^2 + 3K)$, $v_7 = A^2(2A - 3C) - 10B^2(A + 2C) - 4(3CK + 5BN)$, $v_8 = B[A(4A + 5C) + 2(B^2 + C^2 + K)] + 2N(2A + C)$, $v_9 = 48(K^2 + N^2 - B^4) - A^3(2A - 3C) - 2B[B(31A^2 + 38AC + 24C^2) + 14AN]$, $v_{10} = A(4A + C) + 2[3(B^2 + K) + M]$. Покажем, что многообразие $\mathbf{V}(J : I_1)$ является неприводимым. Действительно, это многообразие допускает рациональную параметризацию, определяемую уравнениями

$$A = \frac{2uv}{2u^2+1},\ B = -\frac{v(2u^2-1)}{2(2u^2+1)},\ C = -\frac{uv(5+4u^2+4u^4)}{2(2u^2+1)},\ K = -\frac{v^2}{4(u^2+1)},\ L = \frac{uv^2}{4(u^2+1)},\ M = \frac{u^2v^2(2u^2-1)}{4(u^2+1)},\ N = -\frac{u^3v^2(2u^2+1)}{4(u^2+1)},$$

ибо замыкание Зарисского R множества, задаваемого этими параметрическими уравнениями, имеет вид:

$R = \mathbf{V}(<A(1 + 2u^2) - 2uv, 2B(1 + 2u^2) + v(2u^2 - 1), 2C(1 + 2u^2) + uv(5 + 4u^2 + 4u^4), 4K(1 + u^2) + v^2, 4L(1 + u^2) - uv^2, 4M(1 + u^2) - u^2v^2(2u^2 - 1), 4N(1 + u^2) + u^3v^2(1 + 2u^2), t(1 + u^2)(1 + 2u^2) - 1> \mathbf{I}\ \mathbf{C}[L, M, K, N, B, C, A]) = \mathbf{V}(J : I_1)$.

Здесь при вычислении базиса Грёбнера идеала использовалось упорядочение lex с порядком $t > v > u > L > M > K > N > B > C > A$.

Найдем теперь частное идеалов I_1 и $< L, N, B >$. Имеем $I_1 : < L, N, B > = < \alpha, \beta, \gamma, g_4, w_5, w_6, g_5, g_6, w_9, w_{10}, f_1 >$, где $w_5 = 2(BC + N)[8B^3(4A + C) - A^2B(5A + 9C) - N(9A^2 - 8B^2)] - 2A^2B^2(A^2 - 14B^2) - K^3$, $w_6 = A^2[CK - AM - 2B^2(5A + 2C)] - K^2(2A + C) - 2(2A + C)(BC + N)[B(5A + 2C) + 2N]$, $w_9 = 2AB^2(3A + C) + K(2K - AC) + M(A^2 + K) + 2(BC + N)[B(5A + 3C) + N]$, $w_{10} = 2B^2[2B^2 + A(10A + 3C)] + 4K^2 - M^2 + (2A - C)(AM - CK) + 4(BC + N)[B(8A + 5C) + 2N]$. Многообразие $\mathbf{V}(I_1 : < L, N, B >)$ допускает рациональную параметризацию, задаваемую уравнениями:

$$B = u,\ C = v,\ N = w,\ L = \frac{(uv + w)[(uv + w)^2 + 2u^4]}{2u^4},$$

$$M = -2u^2 - \frac{(uv + w)(uv + 2w)}{u^2},\ K = -\frac{(uv + w)^2[2u^4 + (uv + w)^2]}{2u^6},$$

$$A = -\frac{(uv + w)[4u^4 + (uv + w)^2]}{2u^5}.$$

Действительно, $< B - u, C - v, N - w, 2Lu^4 - (uv + w)[2u^4 + (uv + w)^2], u^2(M + 2u^2) + (uv + w)(uv + 2w), 2Ku^6 + (uv + w)^2[2u^4 + (uv + w)^2], 2Au^5 + (uv + w)[4u^4 + (uv + w)^2], tu - 1 >$ **I** $\mathbf{C}[L, M, K, N, B, C, A]) = I_1 : < L, N, B >$. В данном случае при вычислении базиса Грёбнера идеала использовалось упорядочение lex с порядком $t > u > v > w > L > M > K > N > B > C > A$. Следовательно, многообразие $\mathbf{V}(I_1 : < L, N, B >)$ неприводимо. Так как $I_1 : < L, N, B > \supset J$, $J : I_1 \supset J$, то $\mathbf{V}(I_1 : < L, N, B >) \subset \mathbf{V}(J)$, $\mathbf{V}(J : I_1) \subset \mathbf{V}(J)$. Очевидно, $< L, N, B > \subset \mathbf{V}(J)$. Используя алгоритм нахождения пересечения идеалов, получаем $< L, N, B >$ **I** $(J : I_1)$ **I** $(I_1 : < L, N, B >) = J$.

Равенство идеалов, фигурирующих в левой и правой частях этого равенства, вытекает из совпадения их базисов Грёбнера. Таким образом, $\mathbf{V}(J) = \mathbf{V}(< L, N, B >)$ **U** $\mathbf{V}(I_1 : < L, N, B >)$ **U** $\mathbf{V}(J : I_1)$.

Так как базисы Грёбнера идеалов $< \beta_1, v_2, \ldots, v_{10}, f_1 >$ и $< v_6, \ldots, v_{10}, f_1 >$ совпадают, то $< \beta_1, v_2, \ldots, v_{10}, f_1 > = < v_6, \ldots, v_{10}, f_1 >$. Следовательно, $\mathbf{V}(J : I_1) = \mathbf{V}(J_1)$, где

$J_1 = < 2B[B(A + 2C) + 2N] - A(A^2 + 3K), A^2(2A - 3C) - 10B^2(A + 2C) - 4(3CK + 5BN), B[A(4A + 5C) + 2(B^2 + C^2 + K) + 2N(2A + C), 48(K^2 + N^2 - B^4) - A^3(2A - 3C) - 2B[B(31A^2 + 38AC + 24C^2) + 14AN], A(4A + C) + 2[3(B^2 + K) + M], B(A + C) + L + N >$.

Заметим, что $< \alpha, \beta, \gamma, g_4, w_5, w_6, g_5, g_6, w_9, w_{10}, f_1 > = < \beta, \gamma, g_4, w_5, w_6, g_5, g_6, w_9, w_{10}, f_1 >$. Поэтому $\mathbf{V}(I_1 : < L, N, B >) = \mathbf{V}(J_2)$, где $J_2 = < \beta, \gamma, g_4, w_5, w_6, g_5, g_6, w_9, w_{10}, f_1 >$.

Таким образом, справедлива

Теорема 5. *Многообразие* $V = \mathbf{V}(f_1,\ldots,f_5)$ *состоит из трех неприводимых компонент* $\mathbf{V}(J_1)$, $\mathbf{V}(J_2)$, $\mathbf{V}(L, N, B)$, *т.е.* $\mathbf{V}(f_1,\ldots,f_5) = \mathbf{V}(J_1) \cup \mathbf{V}(J_2) \cup \mathbf{V}(L, N, B)$.

3.6. ПРИМАРНОЕ РАЗЛОЖЕНИЕ ИДЕАЛОВ

Определение 1. Идеал I называется *примарным*, если из $fg \in I$ следует, что или $f \in I$, или $g^m \in I$ для некоторого целого $m > 0$.

Очевидно, что простой идеал примарен.

Лемма 1. *Если идеал* I *примарен, то идеал* $\sqrt{I}$ *прост и является наименьшим простым идеалом, содержащим* I.

Доказательство. Пусть $fg \in \sqrt{I}$. Тогда существует k такое, что $(fg)^k = f^k g^k \in I$. Так как I – примарный идеал, то либо $f^k \in I$, либо $(g^k)^m \in I$ для некоторого целого $m > 0$. Таким образом, из $fg \in \sqrt{I}$ следует, что либо $f \in \sqrt{I}$, либо $g \in \sqrt{I}$, т.е. идеал $\sqrt{I}$ прост. Пусть теперь J – простой идеал и такой, что $J \supset I$. Покажем, что $\sqrt{I} \subset J$. Возьмем любой элемент $g \in \sqrt{I}$. Тогда для некоторого целого $k > 0$ $g^k \in I$, а значит, $g^k \in J$. Так как идеал J прост, то он и радикален. Следовательно, $g \in J$. Отсюда $\sqrt{I} \subset J$. □

Определение 2. Пусть I – примарный идеал и $\sqrt{I} = P$. Тогда I называется *P-примарным идеалом*.

Определение 3. Идеал I называется *неприводимым*, если из равенства $I = I_1 \cap I_2$ следует, что или $I = I_1$, или $I = I_2$.

Лемма 2. *Если I – неприводимый идеал, то он примарен*.

Доказательство. Пусть $fg \in I$, причем $f \notin I$. Покажем, что некоторая степень g принадлежит I. Рассмотрим идеалы $I : g^n$, где $n \geq 1$. Покажем, что для любого n $I : g^n \subset I : g^{n+1}$. Действительно, если $f \in I : g^n$, то $fg^n \in I$. Любой элемент $h \in < g^{n+1} >$ имеет вид $h = pg^{n+1}$, где $p \in k[x_1,\ldots,x_n]$. Так как $fh = fg^n pg \in I$, то $f \in I : g^{n+1}$. Итак, доказано, что для любого n $I : g^n \subset I : g^{n+1}$. Значит, имеем возрастающую цепь идеалов $I : g \subset I : g^2 \subset \ldots$. Следовательно, из условия обрыва возрастающих цепей идеалов существует $N \geq 1$ такое, что $I : g^N = I : g^{N+1}$. Покажем, что $(I + < g^N >) \cap (I + < f >) = I$. Так как $I \subset I + < g^N >$, $I \subset I + < f >$, то $I \subset (I + < g^N >) \cap (I + < f >)$. Пусть $h \in (I + < g^N >) \cap (I + < f >)$. Тогда h можно представить в виде $h = a + bg^N = c + df$, где $a, c \in I$, $b, d \in k[x_1,\ldots,x_n]$. Отсюда $hg = ag +$

$bg^{N+1} = cg + dfg$. Так как $fg \in I$, то $bg^{N+1} = cg + dfg - ag \in I$. Отсюда $b \in I : g^N$, т.е. $bg^N \in I$. Таким образом, $h \in I$. Итак, $I = (I + < g^N >) \cap (I + < f >)$. Так как I неприводим, то или $I = I + < g^N >$, или $I = I + < f >$. Но $I \neq I + < f >$ ввиду того, что $f \notin I$. Значит, $I = I + < g^N >$, т.е. $g^N \in I$. □

Теорема 1. *Любой идеал $I \subset k[x_1,\ldots,x_n]$ может быть представлен в виде конечного пересечения примарных идеалов.*

Доказательство. Покажем, что любой идеал I является пересечением конечного числа неприводимых идеалов. Пусть I – идеал, который нельзя представить в виде конечного пересечения неприводимых идеалов. Тогда I не является неприводимым идеалом, а значит, $I = I_1 \cap I_1'$, где $I \neq I_1$, $I \neq I_1'$. Хотя бы один из идеалов I_1, I_1' нельзя представить в виде пересечения конечного числа неприводимых идеалов, ибо в противном случае I можно было бы представить в виде пересечения конечного числа неприводимых идеалов. Пусть, например, I_1 не является пересечением конечного числа неприводимых идеалов. Тогда $I_1 = I_2 \cap I_2'$, где $I_1 \neq I_2$, $I_1 \neq I_2'$. Продолжая это рассуждение, мы получим бесконечную последовательность идеалов $I \subset I_1 \subset I_2 \subset \ldots$, причем $I \neq I_1 \neq I_2 \neq \ldots$. Это противоречит теореме об УОВЦ. Теперь из леммы 2 и вытекает заключение теоремы. □

Определение 4. *Примарным разложением идеала I* называется его представление в виде конечного пересечения примарных идеалов: $I = \bigcap_{j=1}^{r} Q_j$. Это разложение называется *минимальным*, или *неизбыточным*, если идеалы $\sqrt{Q_j}$ различны и $\bigcap_{\substack{j=1,\\ j\neq i}}^{r} Q_j$ не лежит в Q_i ни для какого i.

Лемма 3. *Пусть I, J – примарные идеалы и $\sqrt{I} = \sqrt{J}$. Тогда идеал $I \cap J$ примарен.*

Доказательство. Пусть $fg \in I \cap J$. Тогда $fg \in I$, $fg \in J$. Отсюда $fg \in \sqrt{I} = \sqrt{J}$. На основании леммы 1 либо $f \in \sqrt{I}$, $f \in \sqrt{J}$, либо $g \in \sqrt{I}$, $g \in \sqrt{J}$. Следовательно, из $fg \in I \cap J$ вытекает, что либо $f^m \in I$, $f^k \in J$, либо $g^p \in I$, $g^q \in J$. Если $f^m \in I$, $f^k \in J$, то $f^{mk} \in I$, $f^{mk} \in J$, а тогда $f^{mk} \in I \cap J$. В случае же $g^p \in I$, $g^q \in J$ имеем $g^{pq} \in I \cap J$, т.е. идеал $I \cap J$ – примарен. □

Теорема 2 (Ласкера-Нётер). *Для каждого идеала* $I \subset k[x_1,\ldots,x_n]$ *существует минимальное примарное разложение.*

Доказательство. На основании теоремы 1 существует примарное разложение $I = \bigcap_{i=1}^{r} Q_i$. Предположим, что $\sqrt{Q_i} = \sqrt{Q_j}$ при $i \neq j$. Тогда по лемме 3 идеал $Q = Q_i \cap Q_j$ является примарным, и в разложении идеала I мы можем заменить два идеала Q_1, Q_j одним идеалом $Q_i \cap Q_j$. Продолжая этот процесс, будем иметь, что все примарные идеалы в разложении идеала I имеют различные радикалы. Пусть теперь $\bigcap_{\substack{j=1 \\ j\neq i}}^{r} Q_j \subset Q_i$, тогда идеал Q_i можно из разложения исключить. Продолжая этот процесс, мы добьемся того, что условие $\bigcap_{\substack{j=1 \\ j\neq i}}^{r} Q_j \not\subset Q_i$ будет выполнено для всех i. □

Отметим, что минимальное примарное разложение не единственно.

Лемма 4. *Пусть идеал I примарен,* $\sqrt{I} = P$ *и* $f \in k[x_1,\ldots,x_n]$. *Тогда*

1) если $f \in I$, *то* $I : f = \langle 1 \rangle$,

2) если $f \notin I$, *то* $I : f$ *P-примарен,*

3) *если* $f \notin P$, *то* $I : f = I$.

Доказательство. 1) Если $f \in I$, то $I : f = \langle 1 \rangle$, ибо для любого $h \in k[x_1,\ldots,x_n]$ $hf \in I$.

2) Пусть $f \notin I$. Если $g \in I : f$, то $fg \in I$. Так как $f \notin I$, то $g \in \sqrt{I}$, т.е. $I \subset I : f \subset \sqrt{I}$. Отсюда $\sqrt{I : f} = \sqrt{I}$. Если $gh \in I : f$, где $g \notin P$, то $fgh \in I$. Значит, $fh \in I$, т.е. $h \in I : f$. Последнее означает, что $I : f$ P-примарен.

3) Пусть $f \notin$ P. Если $g \in I : f$, то $fg \in I$. Отсюда $g \in I$, ибо в противном случае $f^m \in I$, что невозможно. □

Теорема 3 (Ласкера-Нётер). *Пусть* $I = \bigcap_{i=1}^{r} Q_i$ *– минимальное примарное разложение собственного идеала* $I \subset k[x_1,\ldots,x_n]$ *и пусть* $P_i = \sqrt{Q_i}$. *Тогда* P_i *– это в точности те собственные простые идеалы, которые содержатся в множестве идеалов* $\{\sqrt{I : f} \ : f \in k[x_1,\ldots,x_n]\}$.

Доказательство. Идеалы $\sqrt{Q_i}$ являются собственными, ибо Q_i – собственные простые идеалы. Так как $\sqrt{I} = \bigcap_{i=1}^{r} \sqrt{Q_i}$ (предложение 12 из п. 3.2), то на основании теоремы 2 и леммы 4 $P_i = \sqrt{Q_i} = \sqrt{I : f} : f$, где $f \in \bigcap_{\substack{j=1 \\ j \neq i}}^{r} P_j - P_i$. □

Заметим, что идеалы P_i не зависят от примарного разложения идеала I. Мы будем говорить, что P_i принадлежит идеалу I.

Следствие 1. *Пусть* $I = \bigcap_{i=1}^{r} \sqrt{Q_i}$ *– минимальное примарное разложение собственного радикального идеала* $I \subset k[x_1,\ldots,x_n]$. *Тогда идеалы* Q_i *просты и в точности являются собственными простыми идеалами, которые имеют вид* $I : f$, *где* $f \in k[x_1,\ldots,x_n]$.

Доказательство. Так как идеал I радикален, то на основании теоремы 3 $I = \sqrt{I} = \bigcap_{i=1}^{r} \sqrt{Q_i} = \bigcap_{i=1}^{r} P_i$, где $P_i = \sqrt{I : f} : f$ – собственные простые идеалы; при этом $f \in \bigcap_{\substack{j=1 \\ j \neq i}}^{r} P_j - P_i$. На основании леммы 4 $I : f = I$. Значит, $\sqrt{I : f} = \sqrt{I} = I$, т.е. $P_i = I : f$. □

Таким образом, теорема о разложении для радикальных идеалов справедлива для любого поля k.

Определение 5. Пусть идеал $I \subset k[x_1,\ldots,x_n]$ и $f \in k[x_1,\ldots,x_n]$. *Насыщением идеала* I по отношению к f называется множество $I : f^{\infty} = \{g \in k[x_1,\ldots,x_n] : \exists\, m \in \mathbf{N}$ такое, что $f^m g \in I\}$.

Предложение 1. *Пусть* $I \subset k[x_1,\ldots,x_n]$ *– идеал и* $f \in k[x_1,\ldots,x_n]$. *Тогда*

1) множество $I : f^{\infty}$ *– идеал;*

2) $\exists\, n \in \mathbf{N}$ *такое, что* $I : f^{\infty} = I : f^n$.

Доказательство. 1) Заметим, что $0 \in I : f^{\infty}$, ибо $f \cdot 0 = 0 \in I$. Пусть g_1, $g_2 \in I : f^{\infty}$. Тогда существуют m_1, $m_2 \in \mathbf{N}$ такие, что $f^{m_1} g_1 \in I$, $f^{m_2} g_2 \in I$. Отсюда, $f^{m_1+m_2}(g_1 + g_2) = f^{m_1} g_1 f^{m_2} + f^{m_2} g_2 f^{m_1} \in I$, т.е. $g_1 + g_2 \in I : f^{\infty}$. Если $g \in I : f^{\infty}$, то существует $m \in \mathbf{N}$ такое, что $f^m g \in I$. Тогда для любо-

го $h \in k[x_1,\ldots,x_n]$ $f^m(hg) \in I$, а поэтому $hg \in I : f^\infty$. Таким образом, $I : f^\infty$ – идеал.

2) Из доказательства леммы 2 следует, что для любого $k \in \mathbf{N}$ $I : f^k \subset I : f^{k+1}$, причем существует $n \in \mathbf{N}$ такое, что $I : f^n = I : f^{n+1} = \ldots$. Покажем, что $I : f^\infty = I : f^n$. Возьмем любой $g \in I : f^\infty$. Тогда существует $m \in \mathbf{N}$ такое, что $f^m g \in I$, а значит, $g \in I : f^m$. Отсюда следует, что $g \in I^{m+n}$, а тогда $g \in I : f^n$. Таким образом, $I : f^\infty \subset I : f^n$. Если $g \in I : f^n$, то $f^n g \in I$, т.е. $g \in I : f^\infty$. □

Теорема 4. *Пусть идеал* $I = < f_1,\ldots,f_s > \subset k[x_1,\ldots,x_n]$ *и* $f \in k[x_1,\ldots,x_n]$ *– ненулевой полином. Тогда* $I : f^\infty = (I + < 1 - yf >) \cap k[x_1,\ldots,x_n]$. *Если* $I : f^\infty = < g_1,\ldots,g_t >$ *с* $g_i = h_i(1 - yf) + \sum_{j=1}^{s} h_{ij} f_j$ $(i = \overline{1,s},\ h_i,\ h_{ij} \in k[y, x_1,\ldots,x_n])$, *то* $I : f^\infty = I : f^n$, *где* $n = \max\{\deg_y(h_{ij}),\ i = \overline{1,s},\ j = \overline{1,t}\}$.

Доказательство. Возьмем любой $g \in (I + < 1 - yf >) \cap k[x_1,\ldots,x_n]$. Тогда $g = q_1 p + q_2(1 - yf)$, где $p \in I$, $q_1, q_2 \in k[y, x_1,\ldots,x_n]$. Пусть $d = \deg_y(q_1)$. Имеем $f^d g = qp + f^d q_2(1 - yf)$, где $q = f^d q_1 = v(x_1,\ldots,x_n, yf)$. Полагая здесь $yf = 1$, находим $f^d g = \tilde{q} p$, где $\tilde{q} \in k[x_1,\ldots,x_n]$. Следовательно, $f^d g \in I$, а поэтому $g \in I : f^\infty$. Значит, $(I + < 1 - yf >) \cap k[x_1,\ldots,x_n] \subset I : f^\infty$. Пусть теперь $g \in I : f^\infty$. Тогда существует d такое, что $f^d g \in I$. Следовательно, $g = f^d g y^d + g(1 - f^d y^d) = f^d g y^d + g(1 - yf)(1 + yf + \ldots + y^{d-1} f^{d-1}) \in (I + < 1 - yf >) \cap k[x_1,\ldots,x_n]$.

Итак, доказано, что $I : f^\infty = (I + < 1 - yf >) \cap k[x_1,\ldots,x_n]$. Покажем теперь, что $I : f^\infty = I : f^n$. Возьмем любой $g \in I : f^\infty$. Тогда $g = \sum_{i=1}^{t} q_i g_i$, где $q_i \in k[x_1,\ldots,x_n]$. Отсюда $g = \sum_{i=1}^{t} q_i \left(h_i(1 - yf) + \sum_{j=1}^{s} h_{ij} f_j \right)$. Так как $n = \max\{\deg_y(h_{ij})\}$, то $f^n g = \sum_{i=1}^{t} q_i (h_i f^n (1 - yf) + \sum_{j=1}^{s} \tilde{h}_{ij} f_j)$, где $\tilde{h}_{ij} = v_{ij}(x_1,\ldots,x_n, yf)$. Полагая здесь $yf = 1$, получаем $f^n g = \sum_{j=1}^{s} w_{ij} f_j$, где $w_{ij} \in k[x_1,\ldots,x_n]$. Следовательно, $f^n g \in I : f^n$. Значит, $I : f^\infty = I : f^n$. □

ГЛАВА 4. ПОЛИНОМИАЛЬНЫЕ И РАЦИОНАЛЬНЫЕ ФУНКЦИИ НА МНОГООБРАЗИЯХ

4.1. ПОЛИНОМИАЛЬНЫЕ ОТОБРАЖЕНИЯ И ФАКТОР-КОЛЬЦА ПОЛИНОМИАЛЬНЫХ КОЛЕЦ

Определение 1. Пусть $V \subset k^m$ и $W \subset k^n$ – многообразия. Функция $\Phi : V \to W$ называется *полиномиальным* или *регулярным отображением*, если существуют полиномы $f_1,\ldots,f_n \in k[x_1,\ldots,x_m]$ такие, что для любой точки $(a_1,\ldots,a_m) \in V$ $\Phi(a_1,\ldots,a_m) = (f_1(a_1,\ldots,a_m),\ldots,f_n(a_1,\ldots,a_m))$. Будем говорить, что n-набор полиномов $(f_1,\ldots,f_n) \in (k[x_1,\ldots,x_m])^n$ представляет Φ.

Полиномиальное отображение Φ многообразия $V \subset k^m$ в многообразие $W \subset k^n$, представленное набором $(f_1,\ldots,f_n)$ означает, что полиномы, определяющие многообразие W, равны нулю в точках $(f_1(a_1,\ldots,a_m),\ldots,f_n(a_1,\ldots,a_m))$ для любой точки $(a_1,\ldots,a_m) \in V$. В случае $W = k$ Φ является скалярной полиномиальной функцией, заданной на многообразии V. Если $V \subset k^m$, то $\Phi : V \to k$ по определению 1 является полиномиальной функцией, если существует, полином $f \in k[x_1,\ldots,x_m]$, который представляет Φ.

Полиномиальная функция задается обычно указанием ее полиномиального представителя. Вообще говоря, полиномиальное представление функции на многообразии определяется неоднозначно.

Предложение 1. *Пусть $V \subset k^m$ – аффинное многообразие. Тогда*

1) $f, g \in k[x_1,\ldots,x_m]$ представляют на V одну и ту же полиномиальную функцию тогда и только тогда, когда $f - g \in \mathbf{I}(V)$.

2) $(f_1,\ldots,f_n)$ и $(g_1,\ldots,g_n)$ представляют одно и то же полиномиальное отображение $\Phi : V \to k^n$ тогда и только тогда, когда $f_i - g_i \in \mathbf{I}(V)$ для $i = \overline{1,n}$.

Доказательство. 1). Если $f - g \in \mathbf{I}(V)$, то для любой точки $p = (a_1,\ldots,a_m) \in V$ $f(p) - g(p) = 0$, т.е. $f(p) = g(p)$, а значит, f и g представляют одну и ту же функцию на V. Наоборот, если f и g представляют одну и ту же функцию на V, то для любой точки $p \in V$ $f(p) - g(p) = 0$. Следовательно, $f - g \in \mathbf{I}(V)$.

2). Если $(f_1,\ldots,f_n)$ и $(g_1,\ldots,g_n)$ представляют одну и ту же функцию на V, то для $p \in V$ $f_i(p) - g_i(p) = 0$, где $i = \overline{1,n}$. Отсюда $f_i - g_i \in \mathbf{I}(V)$. Если же $f_i - g_i \in \mathbf{I}(V)$ для $i = \overline{1,n}$, то для любой точки $p \in V$ $f_i(p) - g_i(p) = 0$, где $i = \overline{1,n}$, т.е. $(f_1,\ldots,f_n)$ и $(g_1,\ldots,g_n)$ представляют одну и ту же функцию на V. □

Таким образом, соответствие между полиномами из $k[x_1,\ldots,x_m]$ и полиномиальными функциями является взаимно однозначным тогда и только тогда, когда $\mathbf{I}(V) = \{0\}$. Заметим, что в случае бесконечного k $\mathbf{I}(V) = \{0\}$ тогда и только тогда, когда $V = k^m$. Действительно, если $\mathbf{I}(V) = \{0\}$, то $V = k^m$, так как нулевой полином обращается в нуль на всем k^m. Если же $V = k^m$, то для $f \in \mathbf{I}(V)$ $f(a_1,\ldots,a_m) = 0$ для любой точки $(a_1,\ldots,a_m) \in k^m$. Следовательно, $f = 0$.

Определение 2. Через $k[V]$ будем обозначать множество полиномиальных функций $\Phi : V \to k$.

Так как k – поле, то можно определить сумму и произведение любых двух функций $\varphi, \psi \in k[V]$, складывая и умножая их значения. Для любого $p \in V$ полагаем $(\varphi + \psi)(p) = \varphi(p) + \psi(p)$, $(\varphi\cdot\psi)(p) = \varphi(p)\psi(p)$. Если мы выберем представители $f, g \in k[x_1,\ldots,x_m]$ соответственно для φ, ψ, то сумма $f + g$ представляет $\varphi + \psi$, а произведение fg представляет $\varphi\psi$. Следовательно, $\varphi + \psi$, $\varphi\cdot\psi$ являются полиномиальными функциями на V. Таким образом, в $k[V]$ можно определить операции сложения и умножения, используя соответствующие операции в $k[x_1,\ldots,x_m]$. Все обычные свойства этих операций имеют место в $k[V]$. Следовательно, $k[V]$ является коммутативным кольцом.

Определение 3. Коммутативное кольцо R называется *областью целостности*, если из $a\cdot b = 0$ в R следует, что или $a = 0$, или $b = 0$.

Предложение 2. *Пусть $V \subset k^n$ – аффинное многообразие. Следующие утверждения эквивалентны:*

1) V – неприводимое многообразие;

2) идеал $\mathbf{I}(V)$ прост;

3) $k[V]$ является областью целостности.

Доказательство. 1) $\Leftrightarrow$ 2) было доказано ранее. Докажем, что 3) $\Rightarrow$ 1). Предположим, что $k[V]$ является областью целостности, но V приводимо. Тогда существуют V_1, V_2 такие, что $V = V_1 \cup V_2$, где $V_1 \subset V$, $V_2 \subset V$, $V_1 \neq V$, $V_2 \neq V$. Рассмотрим полиномы f_1, $f_2 \in k[x_1,\ldots,x_n]$ такие, что f_1 равен нулю на V_1, но не обращается тождественно в нуль на V_2, а f_2 равен нулю на V_2, но не обращается тождественно в нуль на V_1. Такие полиномы существуют, так как V_1 не содержит V_2, а V_2 не содержит V_1. Таким образом, ни f_1, ни f_2 не представляют нуль в $k[V]$. Однако $f_1f_2 = 0$ во всех точках из $V_1 \cup V_2 = V$. Следовательно, $f_1f_2 = 0$ в $k[V]$, что противоречит целостности кольца $k[V]$. Таким образом, V – неприводимое многообразие.

Докажем, что 1) $\Rightarrow$ 3). Предположим, что $k[V]$ не является областью целостности. Тогда существуют f_1, $f_2 \in k[x_1,\ldots,x_n]$ такие, что ни f, ни g

тождественно не равны нулю на V, но $fg = 0$ в каждой точке из V. Тогда $V = (V \mathbf{I} \mathbf{V}(f)) \mathbf{U} (V \mathbf{I} \mathbf{V}(g))$. Действительно, если $(a_1,\ldots,a_n) \in V$, то $f(a_1,\ldots,a_n)g(a_1,\ldots,a_n) = 0$. Отсюда или $f(a_1,\ldots,a_n) = 0$, или $g(a_1,\ldots,a_n) = 0$. Если $f(a_1,\ldots,a_n) = 0$, то$(a_1,\ldots,a_n) \in \mathbf{V}(f)$, а значит, $(a_1,\ldots,a_n) \in V \mathbf{I} \mathbf{V}(f)$. В случае $g(a_1,\ldots,a_n) = 0$ $(a_1,\ldots,a_n) \in V \mathbf{I} \mathbf{V}(g)$. Следовательно, $(a_1,\ldots,a_n) \in (V \mathbf{I} \mathbf{V}(f)) \mathbf{U} (V \mathbf{I} \mathbf{V}(g))$, т.е. $V \subset (V \mathbf{I} \mathbf{V}(f)) \mathbf{U} (V \mathbf{I} \mathbf{V}(g))$. Так как, очевидно, $(V \mathbf{I} \mathbf{V}(f)) \mathbf{U} (V \mathbf{I} \mathbf{V}(g)) \subset V$, то $V = (V \mathbf{I} \mathbf{V}(f)) \mathbf{U} (V \mathbf{I} \mathbf{V}(g))$. Имеем $V \mathbf{I} \mathbf{V}(f) \neq V$, ибо существует $(c_1,\ldots,c_n) \in V$ такое, что $f(c_1,\ldots,c_n) \neq 0$, т.е. $(c_1,\ldots,c_n) \notin \mathbf{V}(f)$. Аналогично, $V \mathbf{I} \mathbf{V}(g) \neq V$, что противоречит неприводимости многообразия V. □

Таким образом, изучение множества полиномиальных функций на аффинном многообразии позволяет обнаружить его приводимость или неприводимость.

Определение 4. Пусть $I \subset k[x_1,\ldots,x_n]$ – некоторый идеал. Полиномы $f, g \in k[x_1,\ldots,x_n]$ называются *сравнимыми по модулю* I, $f \equiv g \bmod I$, если $f - g \in I$.

Предложение 3. *Пусть $I \subset k[x_1,\ldots,x_n]$ – идеал. Тогда сравнимость по модулю I является отношением эквивалентности на множестве $k[x_1,\ldots,x_n]$.*

Доказательство. Сравнимость по модулю I рефлективна, так как $f - f = 0 \in I$ для любого $f \in k[x_1,\ldots,x_n]$. Докажем симметричность. Пусть $f \equiv g \bmod I$. Тогда $f - g \in I$, а значит, $g - f = (-1)(f - g) \in I$, т.е. $g \equiv f \bmod I$. Теперь докажем транзитивность. Пусть $f \equiv g \bmod I$, $g \equiv h \bmod I$. Тогда $f - g \in I$, $g - h \in I$. Следовательно, $f - g + g - h = f - h \in I$, т.е. $f \equiv h \bmod I$. □

Отношение эквивалентности на множестве S разбивает это множество на непересекающиеся подмножества, которые называются *классами эквивалентности*. Для любого $f \in k[x_1,\ldots,x_n]$ класс эквивалентности f – это множество $[f] = \{g \in k[x_1,\ldots,x_n] : g \equiv f \bmod I\}$. Если $I = \mathbf{I}(V)$, выражение $g \equiv f \bmod \mathbf{I}(V)$ означает, что f и g определяют одну и ту же функцию на многообразии V. Таким образом, собирание полиномов, которые определяют одну и ту же функцию на V, осуществляется с помощью перехода к классам эквивалентности по отношению сравнимости по модулю $\mathbf{I}(V)$.

Предложение 4. *Множество попарно различных полиномиальных функций $\Phi : V \to k$ находится во взаимно однозначном соответствии с множеством классов эквивалентности полиномов по отношению сравнимости по модулю $\mathbf{I}(V)$.*

Доказательство. Возьмем любое $\varphi \in k[V]$. Полиномиальная функция $\varphi : V \to k$ представлена некоторым полиномом $f \in k[x_1,\ldots,x_n]$. Если $g \in k[x_1,\ldots,x_n]$ представляет эту функцию, то из предложения 1 имеем $g \equiv f \bmod \mathbf{I}(V)$, т.е. единственный класс эквивалентности $[f]$ представляет φ. Наоборот, любой класс $[f]$ задает единственную полиномиальную функцию $\varphi : V \to k$, которую представляет любой элемент $g \in [f]$, ибо любой элемент $g \in [f]$ ввиду $f \equiv g \bmod \mathbf{I}(V)$ задает одну и ту же полиномиальную функцию на V. □

Определение 5. *Факторкольцом* $k[x_1,\ldots,x_n] / I$ кольца $k[x_1,\ldots,x_n]$ по идеалу I называется множество классов эквивалентности по отношению сравнимости по модулю I : $k[x_1,\ldots,x_n] / I = \{[f] : f \in k[x_1,\ldots,x_n]\}$.

Определим операции сложения и умножения для классов $[f], [g] \in k[x_1,\ldots,x_n] / I$, используя соответствующие операции для полиномов.

Определение 6. *Суммой классов* $[f], [g]$ в $k[x_1,\ldots,x_n] / I$ называется

$$[f] + [g] = [f + g]. \qquad (1)$$

Произведением классов $[f], [g]$ в $k[x_1,\ldots,x_n] / I$ называется

$$[f]\cdot[g] = [f\cdot g]. \qquad (2)$$

Предложение 5. *Операции сложения и умножения классов корректно определены равенствами (1), (2), т.е. класс $[f' + g']$ и класс $[f'\cdot g']$ не зависят от выбора полиномов $f' \in [f], g' \in [g]$.*

Доказательство. Пусть $f' \in [f]$, $g' \in [g]$. Тогда $f' = f + a$, $g' = g + b$, где $a, b \in I$. Имеем $f' + g' = (f + a) + (g + b) = (f + g) + (a + b)$, т.е. $f' + g' \equiv f + g \bmod I$. Следовательно, $[f' + g'] = [f + g]$. Аналогично, $f'\cdot g' = (f + a)(g + b) = fg + ag + fb + ab$. Так как $ag + fb + ab \in I$, то $f'\cdot g' \equiv f\cdot g \bmod I$, значит, $[f'g'] = [fg]$. □

Теорема 1. *Пусть I – идеал в $k[x_1,\ldots,x_n]$. Тогда факторкольцо $k[x_1,\ldots,x_n] / I$ является коммутативным кольцом, операции в котором заданы равенствами (1), (2).*

Доказательство. Покажем выполнимость всех аксиом коммутативного кольца. Возьмем любые классы $[f], [g], [h] \in k[x_1,\ldots,x_n] / I$. Имеем

$$([f] + [g]) + [h] = [f + g] + [h] = [(f + g) + h] = [f + (g + h)] = [f] + [g + h] = [f] + ([g] + [h]),$$

$$([f]\cdot[g])[h] = [fg][h] = [(fg)h] = [f(gh)] = [f][gh] = [f]([g]\cdot[h]),$$

$$[f] + [g] = [f + g] = [g + f] = [g] + [f],$$

$$[f][g] = [fg] = [gf] = [g][f],$$

$$[f]([g] + [h]) = [f][g + h] = [f(g + h)] = [fg + fh] = [fg] + [fh] = [f][g] + [f][h],$$

Далее получаем

$$[f] + [0] = [f + 0] = [f],\ [f][1] = [f\cdot 1] = [f],\ [f] + [-f] = [f - f] = [0].$$

Таким образом, все аксиомы кольца выполнены. Аддитивной единицей в $k[x_1,\ldots,x_n] / I$ является [0], а мультипликативной служит [1], обратным для $[f]$ является $[-f]$. □

Теорема 2. *Взаимно однозначное соответствие между элементами кольца $k[V]$ и элементами кольца $k[x_1,\ldots,x_n] / I$, определенное в предложении 4, сохраняет суммы и произведения.*

Доказательство. Определим отображение $\Phi : k[x_1,\ldots,x_n] / \mathbf{I}(V) \to k[V]$ следующим образом: для любого $f \in k[x_1,\ldots,x_n] / \mathbf{I}(V)$ положим $\Phi([f]) = \varphi$, где φ – полиномиальная функция $\varphi : V \to k$, представленная полиномом f. Так как любой элемент $\varphi \in k[V]$ представлен некоторым полиномом, то Φ – это отображение «на». Докажем его инъективность. Пусть $\Phi([f]) = \Phi([g])$. На основании предложения 4 $f \equiv g \bmod \mathbf{I}(V)$, т.е. $[f] = [g]$ в $k[x_1,\ldots,x_n] / \mathbf{I}(V)$. Рассмотрим теперь суммы и произведения. Пусть $[f], [g] \in k[x_1,\ldots,x_n] / \mathbf{I}(V)$. Из определения суммы в факторкольце $\Phi([f] + [g]) = \Phi([f + g])$. Если f представляет полиномиальную функцию φ, а g представляет ψ, то $f + g$ представляет $\varphi + \psi$. Таким образом, $\Phi([f] + [g]) = \varphi + \psi = \Phi([f]) + \Phi([g])$, т.е. Φ сохраняет суммы. Аналогично, $\Phi([f]\cdot[g]) = \Phi([f\cdot g]) = \varphi\cdot\psi = \Phi([f])\cdot\Phi([g])$, т.е. Φ сохраняет и произведения. Пусть $\Phi^{-1} = \Psi$. Тогда $\Psi(\varphi + \psi) = [f + g]$, где f представляет φ, а g представляет ψ. Значит, $\Psi(\varphi + \psi) = [f + g] = [f] + [g] = \Psi(\varphi) + \Psi(\psi)$, $\Psi(\varphi\cdot\psi) = [fg] = [f][g] = \Psi(\varphi)\Psi(\psi)$, т.е. обратное соответствие Ψ также сохраняет суммы и произведения. □

Определение 7. Пусть R, S – коммутативные кольца.

1) Отображение $\varphi : R \to S$ называется *кольцевым изоморфизмом*, если:

a) φ сохраняет суммы, т.е. для любых $r, r' \in R$ $\varphi(r + r') = \varphi(r) + \varphi(r')$;

b) φ сохраняет произведения, т.е. для любых $r, r' \in R$ $\varphi(r\cdot r') = \varphi(r)\cdot\varphi(r')$;

c) φ является инъективным отображением «на».

2) Кольца R, S называются *изоморфными*, если существует изоморфизм $\varphi : R \to S$. Если R изоморфно S, то будем писать $R \cong S$.

3) Отображение $\varphi : R \to S$ называется *кольцевым гомоморфизмом*, если φ удовлетворяет условиям a) и b) п.1), но не обязательно условию c) и, кроме того, переводит мультипликативную единицу $1 \in R$ в мультипликативную единицу $1 \in S$.

Заметим, что теорема 2 определяет кольцевой изоморфизм $k[V] \cong k[x_1,\ldots,x_n] / \mathbf{I}(V)$.

Предложение 6. *Пусть R и S – изоморфные кольца и, кроме того, R является полем. Тогда и S также является полем.*

Доказательство. Так как $R \cong S$, то существует изоморфизм $\varphi : R \to S$. Покажем, что $\varphi(1) = 1$. Так как φ является инъективным отображением «на», то для $1 \in S$ существует $r \in R$ такой, что $\varphi(c) = 1$, т.е. $\varphi(r\cdot 1) = \varphi(c)\varphi(1) = 1\cdot\varphi(1) = 1$. Следовательно, $r = 1$, $\varphi(1) = 1$. Покажем, то для любого $s \in S$ существует мультипликативный обратный элемент $s^{-1} \in S$. Для любого $s \in S$ существует $r \in R$ такой, что $\varphi(c) = s$. Так как R – поле, то для $r \in R$ существует мультипликативный обратный $r^{-1} \in R$. Имеем $\varphi(rr^{-1}) = \varphi(c)\varphi(r^{-1}) = \varphi(1) = 1$, т.е. $s\varphi(r^{-1}) = 1$, а значит, $\varphi(r^{-1}) = s^{-1} \in S$. Следовательно, S – поле. □

Определение 8. Элемент a в коммутативном кольце R называется *нильпотентным элементом*, если $a^n = 0$ для некоторого $n > 1$.

Рассмотрим факторкольца $k[x_1,\ldots,x_n] / \mathbf{I}(V)$, $k[x_1,\ldots,x_n] / I$, где $I \neq \mathbf{I}(V)$, но $\mathbf{V}(I) = V$. Если I не радикален, то существует $f \in \sqrt{I}$ такой, что $f \notin I$. Тогда $[f] \neq [0]$ в $k[x_1,\ldots,x_n] / I$, но $[f]^n = [0]$, так как $f^n \in I$ для некоторого $n > 1$. Факторкольцо $k[x_1,\ldots,x_n] / I$ имеет ненулевые нильпотентные элементы, а факторкольцо $k[x_1,\ldots,x_n] / \mathbf{I}(V)$ их иметь не может, так как $\mathbf{I}(V)$ является радикальным идеалом и потому $[f]^n = 0$ в том и только в том случае, когда $[f] = 0$.

Так как факторкольцо $k[x_1,\ldots,x_n] / I$ само является коммутативным кольцом, мы можем изучать идеалы в $k[x_1,\ldots,x_n] / I$. Идеал в коммутативном кольце определяется так же, как в кольце полиномов.

Определение 9. Подмножество I коммутативного кольца R называется *идеалом*, если

1) $0 \in I$, где 0 – нулевой элемент кольца R;
2) если $a, b \in I$, то $a + b \in I$;
3) если $a \in I$, $r \in R$, то $ra \in I$.

Между идеалами в факторкольце $k[x_1,\ldots,x_n] / I$ и идеалами в кольце $k[x_1,\ldots,x_n]$ существует тесная связь.

Предложение 7. *Пусть I – идеал в $k[x_1,\ldots,x_n]$. Тогда идеалы в факторкольце $k[x_1,\ldots,x_n] / I$ находятся во взаимно однозначном соответст-*

вии с идеалами в $k[x_1,\ldots,x_n]$, содержащими I (т.е. идеалами J такими, что $I \subset J \subset k[x_1,\ldots,x_n]$).

Доказательство. Покажем сначала, как построить идеал в $k[x_1,\ldots,x_n] / I$, соответствующий идеалу J, где $I \subset J \subset k[x_1,\ldots,x_n]$. Если $J \supset I$, то через J / I будем обозначать множество $J / I = \{[j] \in k[x_1,\ldots,x_n] / I : j \in J\}$. Покажем, что J / I – идеал в $k[x_1,\ldots,x_n] / I$. Прежде всего $[0] \in J / I$, так как $0 \in J$. Пусть теперь $[j], [h] \in J / I$. Тогда из определения сумы в факторкольце $[j] + [h] = [j + h]$. Так как $j + h \in J$, то $[j + h] \in J / I$. Если $[j] \in J / I$, $[r] \in k[x_1,\ldots,x_n] / I$, то из определения умножения в факторкольце $[r][j] = [rj]$. Так как $rj \in J$, то $[r][j] \in J / I$. Следовательно, J / I – идеал в $k[x_1,\ldots,x_n] / I$.

Пусть теперь $\tilde{J} \subset k[x_1,\ldots,x_n] / I$ – некоторый идеал. Покажем, как построить по $\tilde{J}$ идеал $J \in k[x_1,\ldots,x_n]$ и такой, что $J \supset I$. Положим $J = \{j \in k[x_1,\ldots,x_n] : [j] \in \tilde{J}\}$. Для любого $i \in I \quad i \in J$, так как $[i] = [0] \in \tilde{J}$. Следовательно, $J \supset I$. Покажем, что J – идеал в $k[x_1,\ldots,x_n]$. Имеем: $0 \in J$, так как $0 \in I \subset J$. Если $j, h \in J$, то $[j], [h] \in \tilde{J}$. Значит, $[j] + [h] = [j + h] \in \tilde{J}$, а поэтому $j + h \in J$. Пусть теперь $j \in J$, $r \in k[x_1,\ldots,x_n]$. Тогда $[j] \in \tilde{J}$, а значит, $[r][j] = [rj] \in \tilde{J}$. Следовательно, $rj \in J$, т.е. J – идеал в $k[x_1,\ldots,x_n]$. Таким образом, доказано, что существует соответствие между двумя множествами идеалов:

$$\{J : I \subset J \subset k[x_1,\ldots,x_n]\} \; \{\tilde{J} \subset k[x_1,\ldots,x_n] / I\}$$

$$J \to J / I = \{[j] : j \in J\} \qquad (3)$$

$$J = \{j : [j] \in \tilde{J}\} \leftarrow \tilde{J}.$$

Покажем, что отображения в (3) являются взаимно обратными. Действительно, пусть J – произвольный идеал в $k[x_1,\ldots,x_n]$ и $I \subset J$. Идеалу $J \subset k[x_1,\ldots,x_n]$ соответствует идеал $J / I \subset k[x_1,\ldots,x_n] / I$ и такой, что $J / I = \{[j] : j \in J\}$. При этом $[0] = [i]$, где $i \in I$. Отображение $J \to J / I = \{[j] : j \in J\}$ обратимо, ибо произвольному идеалу $J / I = \{[j] : j \in J\}$ соответствует единственный идеал $J = \{f \in k[x_1,\ldots,x_n] : [f] \in J / I\}$.

Пусть теперь $\tilde{J}$ – произвольный идеал в $k[x_1,\ldots,x_n] / I$. Идеалу $\tilde{J} \subset k[x_1,\ldots,x_n] / I$ соответствует идеал $J \subset k[x_1,\ldots,x_n]$ такой, что $J = \{j : [j] \in \tilde{J}\}$. При этом отображение $\tilde{J} \to J = \{j : [j] \in \tilde{J}\}$ обратимо, так как произвольному идеалу $J = \{j : [j] \in \tilde{J}\}$ соответствует единственный идеал $\tilde{J} = \{[f] \in k[x_1,\ldots,x_n] / I : f \in J\}$. □

Пример. Пусть $I = < x^3 - 4x > \subset R = \mathbf{R}[x]$. Так как R является областью главных идеалов, то каждый идеал в R порожден одним полиномом. Идеалы, содержащие I, – это в точности те идеалы, образующие которых делят $x^3 - 4x$. Таким образом, факторкольцо R / I содержит в точности 8 идеалов:

идеалы в R / I	идеалы в R, содержащие I
$\{[0]\}$,	I,
$< [x] >$, $< [x(x-2)] >$, $< [x-2] >$,	$< x >$, $< x(x-2) >$, $< x-2 >$,
$< [x(x+2)] >$, $< [x+2] >$, $< [x^2-4] >$	$< x(x+2) >$, $< x+2 >$, $< x^2-4 >$,
R / I	R

Здесь $R / I = \{[ax^2 + bx + c] : a, b, c \in \mathbf{R}\}$, так как любой $f \in \mathbf{R}[x]$ можно записать в виде $f = q(x^3 - 4x) + r$, где $q \in \mathbf{R}[x]$, $r = ax^2 + bx + c$, $a, b, c \in \mathbf{R}$.

Следствие 1. *Каждый идеал в факторкольце $k[x_1,\ldots,x_n] / I$ конечно порожден.*

Доказательство. Пусть $\tilde{J}$ – некоторый идеал в $k[x_1,\ldots,x_n] / I$. На основании предложения 7 существует идеал $J \subset k[x_1,\ldots,x_n]$ такой, что $I \subset J$ и $\tilde{J} = \{[j] : j \in J\}$. Из теоремы Гильберта о базисе идеал J конечно порожден, т.е. $J = < f_1,\ldots,f_s >$. Следовательно, любой элемент $j \in J$ имеет вид $j = h_1f_1 + \ldots + h_sf_s$, где $h_i \in k[x_1,\ldots,x_n]$. Отсюда $[j] = [h_1f_1 + \ldots + h_sf_s] = [h_1][f_1] + \ldots + [h_s][f_s]$. Таким образом, классы $[f_1],\ldots,[f_s]$ порождают идеал $\tilde{J}$ в $k[x_1,\ldots,x_n] / I$. □

4.2. АЛГОРИТМИЧЕСКИЕ ВЫЧИСЛЕНИЯ В ФАКТОРКОЛЬЦАХ

Предложение 1. *Зафиксируем мономиальное упорядочение в $k[x_1,\ldots,x_n]$. Пусть I – идеал в $k[x_1,\ldots,x_n]$, $< LT(I) >$ – идеал, порожденный старшими членами полиномов из I.*

1) Каждый полином $f \in k[x_1,\ldots,x_n]$ сравним по модулю I с единственным полиномом, который является k-линейной комбинацией мономов из дополнения к $< LT(I) >$.

2) *Элементы $\{x^\alpha : x^\alpha \notin < LT(I) >\}$ линейно независимы по модулю I, т.е. если $\sum_\alpha c_\alpha x^\alpha \equiv 0 \bmod I$, где x^α принадлежит дополнению $< LT(I) >$, то $c_\alpha = 0$ для всех α.*

Доказательство. 1) Пусть G – базис Грёбнера идеала I и $f \in k[x_1,\ldots,x_n]$. Тогда $f = q + r$, где $q \in G$, $r = \overline{f}^G$ – остаток от деления f на G. Из алгоритма деления имеем, что r – k-линейная комбинация мономов x^α, где $x^\alpha \notin < \mathrm{LT}(I) >$. Единственность остатка r вытекает из свойств базиса Грёбнера.

2) Если $\sum_\alpha c_\alpha x^\alpha \equiv 0 \bmod I$, то $\sum_\alpha c_\alpha x^\alpha \in I$. Пусть существует α_0 такое, что $c_{\alpha_0} \neq 0$. Тогда $\mathrm{LT}(\sum_\alpha c_\alpha x^\alpha) \in < \mathrm{LT}(I) >$, что ввиду $x^\alpha \notin < \mathrm{LT}(I) >$ невозможно. □

Предложение 2. *Пусть I – идеал в $k[x_1,\ldots,x_n]$. Тогда факторкольцо $k[x_1,\ldots,x_n] / I$ как векторное пространство изоморфно пространству $S = Span(x^\alpha : x^\alpha \notin < LT(I) >)$ (где Span обозначает линейную оболочку).*

Доказательство. Из предложения 1 следует, что отображение $\Phi : k[x_1,\ldots,x_n] / I \to S$, определенное формулой $\Phi[f] = \overline{f}^G$ устанавливает взаимно однозначное соответствие между классами эквивалентности в $k[x_1,\ldots,x_n] / I$ и элементами из S. Докажем, что Φ линейно. Рассмотрим операцию сложения в $k[x_1,\ldots,x_n] / I$. Пусть $[f], [g] \in k[x_1,\ldots,x_n] / I$. Предложение 1 определяет стандартные представители $[f]$, $[g]$, которые являются остатками $\overline{f}^G$, $\overline{g}^G$ от деления f, g на базис Грёбнера G. Имеем $f = a + \overline{f}^G$, $g = b + \overline{g}^G$, где $a, b \in I$. Отсюда $f + g = a + b + \overline{f}^G + \overline{g}^G = c + \overline{f+g}^G$, где $c \in I$. При этом $\overline{f}^G = \sum_\alpha c_\alpha x^\alpha$, $\overline{g}^G = \sum_\alpha d_\alpha x^\alpha$, $\overline{f+g}^G = \sum_\alpha h_\alpha x^\alpha$, где суммирование происходит по таким α, что $x^\alpha \notin < \mathrm{LT}(I) >$. В силу единственности стандартного представителя $[f + g]$ имеем $\overline{f}^G + \overline{g}^G = \overline{f+g}^G$. Следовательно, $\overline{f+g}^G = \sum_\alpha (c_\alpha + d_\alpha) x^\alpha$. Таким образом, для стандартных представителей операция сложения в $k[x_1,\ldots,x_n] / I$ совпадает с операцией сложения в k-векторном пространстве $S = \mathrm{Span}(x^\alpha : x^\alpha \notin < \mathrm{LT}(I) >)$. Пусть $c \in k$. Тогда $cf = ca + c\overline{f}^G = q + \overline{cf}^G$, где $q \in I$. В силу единственности стандартного представителя $[cf]$ $\overline{cf}^G = c\overline{f}^G$. Следовательно, $\overline{cf}^G = \sum_\alpha c c_\alpha x^\alpha$, т.е. умножение на c в $k[x_1,\ldots,x_n] / I$ совпадает со

скалярным умножением в S. Таким образом, отображение Ф линейно и является изоморфизмом векторных пространств. □

Предложение 3. *Пусть I – идеал в $k[x_1,\ldots,x_n]$ и пусть G – базис Грёбнера идеала I по отношению к некоторому мономиальному упорядочению. Для каждого $[f] \in k[x_1,\ldots,x_n] / I$ найдем стандартный представитель $\overline{f} = \overline{f}^G \in S$, где $S = Span(x^\alpha : x^\alpha \notin < LT(I) >)$. Тогда*

1) $\overline{f} + \overline{g}$ представляет $[f] + [g]$;

2) $\overline{\overline{f} \cdot \overline{g}}^G$ представляет $[f][g]$.

Доказательство. 1) То, что $\overline{f} + \overline{g}$ представляет $[f] + [g]$, следует из доказательства предложения 2. Докажем 2). Имеем $f = a + \overline{f}$, $g = b + \overline{g}$, $\overline{f}\,\overline{g} = c + \overline{\overline{f} \cdot \overline{g}}^G$, где $a, b, c \in I$. Отсюда $fg = ab + b\overline{f} + a\overline{g} + c + \overline{\overline{f} \cdot \overline{g}}^G = h + \overline{f}\,\overline{g}$, где $h \in I$. В силу единственности стандартного представителя $[fg] = [f][g]$ имеем $\overline{f}\,\overline{g} = \overline{\overline{f} \cdot \overline{g}}^G$, т.е. $\overline{\overline{f} \cdot \overline{g}}^G$ представляет $[f][g]$. □

Теорема 1. *Пусть $V = \mathbf{V}(I)$ – аффинное многообразие в $\mathbf{C}^n$. Зафиксируем мономиальное упорядочение в $\mathbf{C}[x_1,\ldots,x_n]$. Следующие условия эквивалентны:*

1) V – конечное множество;

2) для любого i, где $1 \le i \le n$, существует $m_i \ge 0$ такое, что $x_i^{m_i} \in < LT(I) >$;

3) если G – базис Грёбнера идеала I, то для любого i, где $1 \le i \le n$, существует $m_i \ge 0$ такое, что $x_i^{m_i} = LM(g)$ для некоторого $g \in G$;

4) $\mathbf{C}$-векторное пространство $S = Span(x^\alpha : x^\alpha \notin < LT(I) >)$ конечномерно;

5) $\mathbf{C}$-векторное пространство $\mathbf{C}[x_1,\ldots,x_n] / I$ конечномерно.

Доказательство. 1) $\Rightarrow$ 2). Если $V = \varnothing$, то $1 \in I$. В этом случае для любого i можно взять $m_i = 0$. Если V непусто, то зафиксируем i, и пусть a_j, $j = 1,\ldots,l$ – различные комплексные числа, являющиеся i-ми координатами точек из V. Рассмотрим полином от одной переменной $f(x_i) = \prod_{j=1}^{l}(x_i - a_j)$. Так как f равен нулю в каждой точке из V, то $f \in \mathbf{I}(\mathbf{V}(I))$. Из теоремы о нулях следует, что существует $m \ge 1$ такое, что $f^m \in I$. Это означает, что $\mathrm{LT}(f^m) \in < \mathrm{LT}(I) >$, т.е. $x_i^{lm} \in < \mathrm{LT}(I) >$.

2) $\Leftrightarrow$ 3). Пусть $x_i^{m_i} \in <\mathrm{LT}(I)>$. Так как G – базис Грёбнера идеала I, то $<\mathrm{LT}(I)> = <\mathrm{LT}(g) : g \in G>$. Из теории мономиальных идеалов следует, что существует $g \in G$ такой, что $\mathrm{LT}(g)$ делит $x_i^{m_i}$. Следовательно, $\mathrm{LT}(g)$ является степенью x_i. Если $x_i^{m_i} = \mathrm{LM}(g)$, то очевидно, $x_i^{m_i} \in <\mathrm{LT}(I)>$.

2) $\Rightarrow$ 4) Предположим, что некоторая степень $x_i^{m_i}$ принадлежит $<\mathrm{LT}(I)>$ для каждого i, $1 \le i \le n$. Тогда все мономы $x_1^{\alpha_1} \dots x_n^{\alpha_n}$, где $\alpha_i \ge m_i$ хотя бы для одного i, принадлежат $<\mathrm{LT}(I)>$. У мономов $x_1^{\alpha_1} \dots x_n^{\alpha_n}$, принадлежащих дополнению к $<\mathrm{LT}(I)>$ для любого i, $1 \le i \le n$, $\alpha_i < m_i$. Следовательно, число мономов в дополнении к $<\mathrm{LT}(I)>$ не превышает $m_1 \dots m_n$.

4) $\Leftrightarrow$ 5) следует из предложения 2.

5) $\Rightarrow$ 1). Для доказательства конечности многообразия V достаточно доказать, что для каждого i множество i-х координат точек из V конечно. Для любого фиксированного i рассмотрим классы $[x_i^j] \in \mathbf{C}[x_1,\dots,x_n] / I$, где $j = 0, 1, 2, \dots$. Так как $\mathbf{C}[x_1,\dots,x_n] / I$ конечномерно, то элементы множества $[x_i^j]$ линейно зависимы в $\mathbf{C}[x_1,\dots,x_n] / I$, т.е. существуют не все равные нулю постоянные c_j и натуральные m такие, что $\sum_{j=0}^{m} c_j [x_i^{\,j}] = \left[\sum_{j=0}^{m} c_j x_i^{\,j}\right] = [0]$.

Отсюда $\sum_{j=0}^{m} c_j x_i^{\,j} \in I$. Этот полином равен нулю во всех точках из V. Так как ненулевой полином имеет лишь конечное число корней в $\mathbf{C}$, то i-я координата точек из V имеет лишь конечное число значений. □

Заметим, что условие $k = \mathbf{C}$ нужно только для доказательства импликации 1) $\Rightarrow$ 2). Все другие утверждения справедливы, даже когда поле k не является алгебраически замкнутым. □

Следствие 1. *Пусть I – идеал в $\mathbf{C}[x_1,\dots,x_n]$ такой, что некоторая степень $x_i^{m_i}$ для каждого i лежит в $<LT(I)>$. Тогда число точек многообразия $\mathbf{V}(I)$ не превышает $m_1 \dots m_n$.*

Доказательство. Доказательство вытекает из п. 3 теоремы 1, предложения 2 и доказательства импликации 2) $\Rightarrow$ 4) этой теоремы. □

Предложение 4. *Пусть I – идеал в $\mathbf{C}[x_1,\dots,x_n]$ такой, что многообразие $V = \mathbf{V}(I)$ конечно.*

1) Число точек многообразия V не превышает размерности $\dim(\mathbf{C}[x_1,\ldots,x_n] / I)$ ($\dim$ обозначает размерность как векторного пространства над $\mathbf{C}$).

2) Если I – радикальный идеал, то число точек многообразия V равно $\dim(\mathbf{C}[x_1,\ldots,x_n] / I)$.

Доказательство. Докажем сначала, что для различных точек $p_1,\ldots,p_m \in \mathbf{C}^n$ существует полином $f_1 \in \mathbf{C}[x_1,\ldots,x_n]$ такой, что $f_1(p_1) = 1$, $f_1(p_i) = 0$, $i = \overline{2,m}$. Если $a \neq b$ в $\mathbf{C}^n$, то $a = (a_1,\ldots,a_n)$ и $b = (b_1,\ldots,b_n)$ различаются хотя бы одной координатой, например j-й. Тогда полином $g = \dfrac{x_j - b_j}{a_j - b_j}$ обладает тем свойством, что $g(a) = 1$, $g(b) = 0$. Применяя этот прием к каждой паре p_1, p_i, где $2 \le i \le m$, мы получаем полиномы g_i, $i \ge 2$ такие, что $g_i(p_1) = 1$, $g_i(p_i) = 0$ для $i = \overline{2,m}$. Тогда полином $f_1 = g_2 g_2 \ldots g_m$ обладает тем свойством, что $f_1(p_1) = 1$, $f_1(p_i) = 0$, $i = \overline{2,m}$. Указанным способом мы можем построить полиномы $f_2,\ldots,f_m$ такие, что $f_i(p_i) = 1$, а $f_i(p_j) = 0$, если $i \neq j$.

Пусть многообразие $V = \{p_1,\ldots,p_m\}$, где все точки p_i различны. Построим полиномы $f_1,\ldots,f_m$, как указано выше. Покажем, что $[f_1],\ldots,[f_m] \in \mathbf{C}[x_1,\ldots,x_n] / I$ линейно независимы. Предположим вопреки утверждению, что классы $[f_1],\ldots,[f_m]$ линейно зависимы. Тогда $\sum_{i=1}^{m} a_i [f_i] = [0]$, где $a_i \in \mathbf{C}$, причем среди a_i имеются ненулевые. Это равенство означает, что $g = \sum_{i=1}^{m} a_i f_i \in I$, а поэтому g обращается в нуль во всех точках многообразия $V = \mathbf{V}(I) = \{p_1,\ldots,p_m\}$. Таким образом, для всех j, $1 \le j \le m$, имеем $0 = g(p_j) = \sum_{i=1}^{m} a_i f_i(p_j) = 0 + a_j f_j(p_j) = a_j$, т.е. все $a_j = 0$, а значит, классы $[f_j]$, $j = \overline{1,m}$, линейно независимы. Отсюда следует, что $m \le \dim(\mathbf{C}[x_1,\ldots,x_n] / I)$, что и завершает доказательство п. 1.

Пусть теперь идеал I радикален. Покажем, что в этом случае $[f_1],\ldots,[f_m]$ образуют базис в $\mathbf{C}[x_1,\ldots,x_n] / I$. Линейная независимость классов уже доказана. Покажем, что линейная оболочка классов $[f_i]$ содержит все факторкольцо. Пусть $[g] \in \mathbf{C}[x_1,\ldots,x_n] / I$ – произвольный элемент и $a_i = g(p_i)$. Образуем полином $h = g - \sum_{i=1}^{m} a_i f_i$. Для всех j, где $j = \overline{1,m}$, $h(p_j) = 0$, т.е. $h \in \mathbf{I}(V)$. Из теоремы Гильберта о нулях $\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ в силу

алгебраической замкнутости поля **C**. Так как I радикален, то $h \in I$, т.е. $[h]$ = $[0]$ в $\mathbf{C}[x_1,\ldots,x_n] / I$. Следовательно, $[g] = \sum_{i=1}^{m} a_i [f_i]$. □

4.3. КООРДИНАТНОЕ КОЛЬЦО АФФИННОГО МНОГООБРАЗИЯ

Кольцо $k[V]$ полиномиальных функций на аффинном многообразии $V \subset k^n$ можно отождествить с факторкольцом $k[x_1,\ldots,x_n] / \mathbf{I}(V)$, ибо $k[V] \cong k[x_1,\ldots,x_n] / \mathbf{I}(V)$. Полиномиальную функцию из $k[V]$, которая представлена полиномом $f \in k[x_1,\ldots,x_n]$, будем обозначать через $[f]$. В частности, каждая переменная x_i определяет полиномиальную функцию $[x_i] : V \to k$, значением которой в точке $p \in V$ является i-я координата этой точки. Любая функция из $k[V]$ представляет k-линейную комбинацию произведений полиномиальных функций $[x_i]$.

Определение 1. Пусть $V \subset k^n$ – аффинное многообразие. Тогда кольцо $k[V]$ называется *координатным кольцом* многообразия V.

Определение 2. Пусть $V \subset k^n$ – аффинное многообразие.

1) Для любого идеала $J = < \varphi_1,\ldots,\varphi_s > \subset k[V]$ определим множество $\mathbf{V}_V(J) = \{(a_1,\ldots,a_n) \in V : \forall\ \varphi \in J\ \varphi(a_1,\ldots,a_n) = 0\}$, которое называется *подмногообразием* многообразия V.

2) для любого $W \subset V$ положим $\mathbf{I}_V(W) = \{\varphi \in k[V] : \forall\ (a_1,\ldots,a_n) \in W\ \varphi(a_1,\ldots,a_n) = 0\}$.

Определение 3. Идеал $J \subset k[V]$ называется *радикальным*, если из включения $[f]^m \in J$ для некоторого $m \geq 1$ следует, что $[f] \in J$.

Определение 4. Пусть $J \subset k[V]$ – некоторый идеал. *Радикалом* $\sqrt{J}$ идеала J называется множество $\sqrt{J} = \{[f] \in k[V] : \exists\ m \in \mathbf{N}\quad [f]^m \in J\}$.

Предложение 1. *Пусть $V \subset k^n$ – аффинное многообразие.*

1) Пусть J – идеал в $k[V]$. Тогда $W = \mathbf{V}_V(J)$ – аффинное многообразие в k^n, которое расположено в V;

2) Пусть $W \subset V$ – некоторое подмножество. Тогда $\mathbf{I}_V(W)$ – идеал в $k[V]$;

3) Если $J \subset k[V]$ – некоторый идеал, то $J \subset \sqrt{J} \subset \mathbf{I}_V(\mathbf{V}_V(J))$;

4) Если $W \subset V$ – некоторое подмногообразие, то $W = \mathbf{V}_V(\mathbf{I}_V(W))$.

Доказательство. 1) Для доказательства п. 1 воспользуемся взаимно однозначным соответствием между идеалами в $k[V]$ и идеалами в

$k[x_1,\ldots,x_n]$, содержащими $\mathbf{I}(V)$. Пусть $\widetilde{J} = \{f \in k[x_1,\ldots,x_n] : [f] \in J\} \subset k[x_1,\ldots,x_n]$ – идеал, который соответствует идеалу $J \subset k[V]$. Так как $\mathbf{I}(V) \subset \widetilde{J}$, то $\mathbf{V}(\widetilde{J}) \subset \mathbf{V}(\mathbf{I}(V)) = V$. Далее имеем $\mathbf{V}(\widetilde{J}) = \mathbf{V}_V(J)$, ибо элементами из $\widetilde{J}$ являются полиномиальные функции из J. Таким образом, $W = \mathbf{V}_V(J)$ – аффинное многообразие в k^n.

2) Пусть $W \subset V$. Покажем, что $\mathbf{I}_V(W)$ – идеал в $k[V]$. Очевидно, $[g] = [0] \in \mathbf{I}_V(W)$, ибо $g \equiv 0 \bmod \mathbf{I}(V)$, а значит, для любого $(a_1,\ldots,a_n) \in W$ $g(a_1,\ldots,a_n) = 0$. Если $[f], [g] \in \mathbf{I}_V(W)$, то для любого $(a_1,\ldots,a_n) \in W$ $[f(a_1,\ldots,a_n)] = 0$, $[g(a_1,\ldots,a_n)] = 0$. Следовательно, $[f(a_1,\ldots,a_n)] + [g(a_1,\ldots,a_n)] = [(f+g)(a_1,\ldots,a_n)] = 0$, т.е. $[f+g] \in \mathbf{I}_V(W)$. Если $[f] \in \mathbf{I}_V(W)$, то для любого $[h] \in k[V]$ $[f(a_1,\ldots,a_n)][h(a_1,\ldots,a_n)] = [(fh)(a_1,\ldots,a_n)] = 0$, т.е. $[fh] \in \mathbf{I}_V(W)$.

3) Пусть идеал $J \subset k[V]$. Если $[f] \in J$, то очевидно, $[f] \in \sqrt{J}$, т.е. $J \subset \sqrt{J}$. Пусть $[f] \in \sqrt{J}$. Тогда существует $m \in \mathbf{N}$ такое, что $[f]^m = [f^m] \in J$. Для любого $(a_1,\ldots,a_n) \in \mathbf{V}_V(J)$ имеем $[(f(a_1,\ldots,a_n))^m] = 0$. Отсюда $[f(a_1,\ldots,a_n)] = 0$, т.е. $[f] \in \mathbf{I}_V(\mathbf{V}_V(J))$. Значит, $\sqrt{J} \subset \mathbf{I}_V(\mathbf{V}_V(J))$.

4) Пусть $W \subset V$ – некоторое подмногообразие в k^n. Тогда $\mathbf{I}(V) \subset \mathbf{I}(W)$. Для идеала $I = \mathbf{I}_V(W) = \{f \in k[V] : \forall\ (a_1,\ldots,a_n) \in W \quad [f(a_1,\ldots,a_n)] = 0\}$ соответствующим идеалом в $k[x_1,\ldots,x_n]$ является $\widetilde{I} = \{f \in k[x_1,\ldots,x_n] : [f] \in \mathbf{I}_V(W)\}$. Покажем, что $\widetilde{I} = \mathbf{I}(W)$. Если $f \in \widetilde{I}$, то $[f] \in \mathbf{I}_V(W)$, а поэтому для любого $(a_1,\ldots,a_n)$ $[f(a_1,\ldots,a_n)] = 0$. Следовательно, $f(a_1,\ldots,a_n) = 0$, т.е. $f \in \mathbf{I}(W)$. Значит, $\widetilde{I} \subset \mathbf{I}(W)$. Если $f \in \mathbf{I}(W)$, то для любого $(a_1,\ldots,a_n) \in W$ $f(a_1,\ldots,a_n) = 0$. Последнее означает, что $[f] \in \mathbf{I}_V(W)$, а поэтому $f \in \widetilde{I}$. Таким образом, $\mathbf{I}(W) = \widetilde{I}$. Далее с учетом п. 1 имеем $\mathbf{V}_V(\mathbf{I}_V(W)) = \mathbf{V}(\widetilde{I}) = \mathbf{V}(\mathbf{I}(W)) = W$. □

Предложение 2. *Идеал $J \subset k[V]$ радикален тогда и только тогда, когда радикальным является идеал $\widetilde{J} = \{f \in k[x_1,\ldots,x_n] : [f] \in J\}$.*

Доказательство. Пусть J – радикальный идеал в $k[V]$ и $f^m \in \widetilde{J}$ для некоторого $m \in \mathbf{N}$. Тогда $[f^m] = [f]^m \in J$. Так как J радикален, то $[f] \in J$. Значит, $f \in \widetilde{J}$, т.е. идеал $\widetilde{J}$ является радикальным. Пусть теперь $\widetilde{J}$ радикален и $[f]^m \in J$. Тогда $[f]^m = [f^m] \in J$, а поэтому $f^m \in \widetilde{J}$. Следовательно, $f \in \widetilde{J}$ и $[f] \in J$, т.е. J – радикальный идеал. □

Теорема 1. *Пусть поле k алгебраически замкнуто и $V \subset k^n$ – аффинное многообразие.*

*1) (***Теорема о нулях в $k[V]$***). Если J – идеал в $k[V]$, то $\mathbf{I}_V(\mathbf{V}_V(J)) = \sqrt{J}$;*

2) Отображения

$$\left\{\begin{array}{c}\text{аффинные многообразия}\\ W \subset V\end{array}\right\} \underset{\mathbf{V}_V}{\overset{\mathbf{I}_V}{\rightleftarrows}} \left\{\begin{array}{c}\text{радикальные идеалы}\\ J \subset k[V]\end{array}\right\}$$

являются биекциями, обращающими включение, и взаимно обратны;

3) При отображениях, определенных в п. 2, точки многообразия V соответствуют максимальным идеалам в $k[V]$.

Доказательство. 1) Пусть идеал $J \subset k[V]$. Идеалу $J \subset k[V]$ соответствует идеал $\tilde{J} \subset k[x_1,\ldots,x_n]$. На основании предложения 1 $\mathbf{V}(\tilde{J}) = \mathbf{V}_V(J)$. Если $[f] \in \mathbf{I}_V(\mathbf{V}_V(J)) = \mathbf{I}_V(\mathbf{V}(\tilde{J}))$, то для любого $(a_1,\ldots,a_n) \in \mathbf{V}(\tilde{J})$ $[f(a_1,\ldots,a_n)] = 0$, т.е. $f(a_1,\ldots,a_n) = 0$. Следовательно, $f \in \mathbf{I}(\mathbf{V}(\tilde{J}))$. Из теоремы о нулях в k^n имеем $\mathbf{I}(\mathbf{V}(\tilde{J})) = \sqrt{\tilde{J}}$. Отсюда существует $m \in \mathbf{N}$ такое, что $f^m \in \tilde{J}$. Тогда $[f^m] = [f]^m \in J$, а значит $[f] \in \sqrt{J}$ в $k[V]$. Таким образом, $\mathbf{I}_V(\mathbf{V}_V(J)) \subset \sqrt{J}$. Так как $\sqrt{J} \subset \mathbf{I}_V(\mathbf{V}_V(J))$, то $\mathbf{I}_V(\mathbf{V}_V(J)) = \sqrt{J}$. Теорема о нулях для $k[V]$ доказана.

2) Для любых $W_1 \subset W_2 \subset V$, где W_1, W_2 – аффинные многообразия, $\mathbf{I}_V(W_1) \supset \mathbf{I}_V(W_2)$, ибо если $[f] \in \mathbf{I}_V(W_2)$, то для любого $(a_1,\ldots,a_n) \in W_2$, а значит, и для любого $(a_1,\ldots,a_n) \in W_1$ $[f(a_1,\ldots,a_n)] = 0$, т.е. $[f] \in \mathbf{I}_V(W_1)$. Далее для любых $J_1 \subset J_2 \subset k[V]$, где J_1, J_2 – идеалы, $\mathbf{V}_V(J_1) \supset \mathbf{V}_V(J_2)$, так как если $(a_1,\ldots,a_n) \in \mathbf{V}_V(J_2)$, то для любого $[f] \in J_2$, а вместе с тем и для любого $[f] \in J_1$ $[f(a_1,\ldots,a_n)] = 0$, т.е. $(a_1,\ldots,a_n) \in \mathbf{V}_V(J_1)$. Таким образом, отображения $\mathbf{I}_V$, $\mathbf{V}_V$ обращают включения.

Для любого $W \subset V$, где W – аффинное многообразие, $\mathbf{V}_V(\mathbf{I}_V(W)) = W$. Далее для любого $J \subset k[V]$, где J – радикальный идеал, $\mathbf{I}_V(\mathbf{V}_V(J)) = \sqrt{J}$. Таким образом, отображения $\mathbf{I}_V$, $\mathbf{V}_V$ являются взаимно обратными биекциями между множеством аффинных многообразий и множеством радикальных идеалов, обращающими включение.

3) Доказывается так же, как соответствующая теорема о мономиальных идеалах в $k[x_1,\ldots,x_n]$. □

Определение 5. Пусть $V \subset k^m$ и $W \subset k^n$ – аффинные многообразия. Они называются *изоморфными*, если существуют полиномиальные отображения $\alpha : V \to W$ и $\beta : W \to V$ таким, что $\alpha \circ \beta = \mathrm{id}_W$ и $\beta \circ \alpha = \mathrm{id}_V$ (для любого многообразия V через id обозначается тождественное отображение V на себя).

Если $W \subset k^n$ изоморфно $V = k^m$, то существует взаимно однозначное полиномиальное отображение $\alpha : k^m \to W$, у которого есть полиномиальное обратное, т.е. в этом случае существует полиномиальная параметризация многообразия W.

Предложение 3. *Пусть $V \subset k^m$ и $W \subset k^n$ – аффинные многообразия.*

1) Пусть $\alpha : V \to W$ – полиномиальное отображение. Тогда для каждой полиномиальной функции $\varphi : W \to k$ композиция $\varphi \circ \alpha : V \to k$ также является полиномиальной функцией. При этом отображение $\alpha^* : k[W] \to k[V]$, определенное формулой $\alpha^*(\varphi) = \varphi \circ \alpha$ является кольцевым гомоморфизмом, тождественным на постоянных функциях. (Отметим, что α^* «действует в противоположном направлении» по сравнению α, ибо отображает функции на W в функции на V. По этой причине α^* называется отображением обратного образа на функциях).

2) Обратно, пусть $f : k[W] \to k[V]$ – кольцевой гомоморфизм, тождественный на постоянных функциях. Тогда существ ует единственное полиномиальное отображение $\alpha : V \to W$ такое, что $f = \alpha^*$.

Доказательство. 1) Пусть $x_1,\ldots,x_m$ – координаты в $k^m \supset V$, а $y_1,\ldots,y_n$ – координаты в $k^n \supset W$. Тогда полиномиальная функция $\varphi : W \to k$ может быть представлена полиномом $f(y_1,\ldots,y_n)$, а полиномиальное отображение $\alpha : V \to W$ может быть представлено n-набором полиномов: $\alpha(x_1,\ldots,x_m) = (a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m))$. Найдем $\varphi \circ \alpha$, подставляя $\alpha(x_1,\ldots,x_m)$ в φ. Имеем $(\varphi \circ \alpha)(x_1,\ldots,x_m) = f(a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m))$. Ясно, что $\varphi \circ \alpha$ – полином от $x_1,\ldots,x_m$. Таким образом, $\varphi \circ \alpha \in k[V]$. Определим теперь $\alpha^* : k[W] \to k[V]$ формулой $\alpha^*(\varphi) = \varphi \circ \alpha$. Покажем, что α^* – кольцевой гомоморфизм. Пусть ψ – другая полиномиальная функция из $k[W]$, представленная полиномом $g(y_1,\ldots,y_n)$. Тогда $(\alpha^*(\varphi + \psi))(x_1,\ldots,x_m) = f(a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m))g(a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m)) = \alpha^*(\varphi)(x_1,\ldots,x_m) + \alpha^*(\psi)(x_1,\ldots,x_m)$, $(\alpha^*(\varphi\cdot\psi))(x_1,\ldots,x_m) = f(a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m))g(a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m)) = \alpha^*(\varphi)(x_1,\ldots,x_m)\cdot\alpha^*(\psi)(x_1,\ldots,x_m)$. Следовательно, $\alpha^*(\varphi + \psi) = \alpha^*(\varphi) + \alpha^*(\psi)$, $\alpha^*(\varphi\psi) = \alpha^*(\varphi)\alpha^*(\psi)$. Значит, α^* – кольцевой гомоморфизм.

Рассмотрим теперь постоянную функцию $[a] \in k[W]$, $a \in k$, на W со значением a. Тогда $\alpha^*([a]) = [a] \circ \alpha$ – постоянная функция на V с тем же значением a. Таким образом, отображение α^* тождественно на константах.

2) Пусть теперь $f : k[W] \to k[V]$ – кольцевой гомоморфизм, тождественный на постоянных функциях. Покажем, что существует полиномиальное отображение $\alpha : V \to W$ такое, что $f = \alpha^*$. Рассмотрим координатные функции $[y_1],\ldots,[y_n] \in k[W]$. Тогда $f([y_i]) \in k[V]$. При этом $f([y_i]) = [a_i(x_1,\ldots,x_m)] \in k[V]$ для некоторых полиномов $a_i \in k[x_1,\ldots,x_m]$. Рассмотрим полиномиальное отображение $\alpha = (a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m))$. Докажем, что α отображает V в W и что $f = \alpha^*$. Пусть $F = \sum_\gamma c_\gamma y^\gamma \in k[y_1,\ldots,y_n]$.

Тогда

$$[F \circ \alpha] = f([F]) \qquad (1).$$

Действительно, $[F \circ \alpha] = [F(a_1,\ldots,a_n)] = F([a_1],\ldots,[a_n]) = F(f([y_1]),\ldots,f([y_n]))$. Так как f является кольцевым гомоморфизмом, тождественным на постоянных функциях, а $[F]$ – k-линейная комбинация произведений $[y_i]$, то $f([F]) = f([F(y_1,\ldots,y_n)]) = f(F([y_1],\ldots,[y_n])) = f(\sum_\gamma d_\gamma [y]^\gamma) = \sum_\gamma d_\gamma (f[y])^\gamma = F(f([y_1]),\ldots,f([y_n]))$. Итак, равенство (1) доказано.

Пусть $(c_1,\ldots,c_m) \in V$. Покажем, что $\alpha(c_1,\ldots,c_m) \in W$. Если возьмем любую функцию $F \in \mathbf{I}(W)$, то $[F] = 0$ в $k[W]$. Так как f – кольцевой гомоморфизм, то $f([F]) = 0$ в $k[V]$. Из (1) следует, что $[F \circ \alpha]$ – нулевая функция на V. В частности, $[F \circ \alpha](c_1,\ldots,c_m) = F(\alpha(c_1,\ldots,c_m)) = 0$. Так как F – произвольная функция из $\mathbf{I}(W)$, а $W = \mathbf{V}(\mathbf{I}(W))$, то $\alpha(c_1,\ldots,c_m) \in W$. Таким образом, α отображает V в W. Отсюда следует с учетом (1), что для любой полиномиальной функции $[F] \in k[W]$ $[F] \circ \alpha = f([F])$. Так как $\alpha^*([F]) = [F] \circ \alpha$, то $f = \alpha^*$. Покажем теперь, что отображение α определено однозначно. Пусть существует отображение $\beta : V \to W$ такое, что $f = \beta^*$, и пусть $\beta(x_1,\ldots,x_m) = (b_1(x_1,\ldots,x_m),\ldots,b_n(x_1,\ldots,x_m))$. Тогда $\beta^*([y_i]) = [y_i] \circ \beta = [b_i(x_1,\ldots,x_m)]$. Но $\alpha^*([y_i]) = [a_i(x_1,\ldots,x_m)]$, а так как $\alpha^* = f = \beta^*$, то для всех i $[a_i] = [b_i]$. Таким образом, a_i и b_i определяют одну и ту же функцию на V, а значит, $\alpha = (a_1,\ldots,a_n)$ и $\beta = (b_1,\ldots,b_n)$ определяют одно и то же отображение из V в W. Значит, $\alpha = \beta$ и единственность доказана. □

Теорема 2. *Два аффинных многообразия $V \subset k^m$ и $W \subset k^n$ изоморфны тогда и только тогда, когда существует изоморфизм $k[V] \cong k[W]$ их координатных колец, тождественный на константах.*

Доказательство. Если $V \subset k^m$ и $W \subset k^n$ изоморфны, то существуют взаимно обратные полиномиальные отображения $\alpha : V \to W$ и $\beta : W \to V$. Тогда $\alpha \circ \beta = \mathrm{id}_W$. Это означает, что для любого $\varphi \in k[W]$ $(\alpha \circ \beta)^*(\varphi) = \mathrm{id}_W{}^*(\varphi) = (\varphi) \circ \mathrm{id}_W = \varphi$. С другой стороны

$$(\alpha \circ \beta)^*(\varphi) = \varphi \circ (\alpha \circ \beta) = (\varphi \circ \alpha) \circ \beta = \alpha^*(\varphi) \circ \beta =$$

$$= \beta^*(\alpha^*(\varphi)) = (\beta^* \circ \alpha^*)(\varphi). \qquad (2)$$

Следовательно, $(\alpha \circ \beta)^* = \beta^* \circ \alpha^* = \mathrm{id}_{k[W]}$ как отображение из $k[W]$ в себя. Аналогично, $(\beta \circ \alpha)^* = \alpha^* \circ \beta^* = \mathrm{id}_{k[V]}$. На основании предложения 3 заключаем, что $\alpha^* : k[W] \to k[V]$, где $\alpha^*(\varphi) = \varphi \circ \alpha$ – изоморфизм $k[V] \cong k[W]$ координатных колец многообразий V, W, тождественный на константах.

Пусть теперь существует кольцевой изоморфизм $f : k[W] \to k[V]$, тождественный на константах. Тогда f и f^{-1} задаются полиномиальными отображениями из V в W и из W в V соответственно. Из предложения 3 имеем $f = \alpha^*$ для некоторого $\alpha : V \to W$ и $f^{-1} = \beta^*$ для некоторого $\beta : W \to V$. Покажем, что отображения α и β взаимно обратны. Рассмотрим композицию $\alpha \circ \beta : W \to W$. Очевидно, что это отображение является полиномиальным. Для любой полиномиальной функции $\varphi \in k[W]$ из (2) имеем

$$(\alpha \circ \beta)^*(\varphi) = \beta^*(\alpha^*(\varphi)) = f^{-1}(f(\varphi)) = \varphi. \qquad (3)$$

Так как $\mathrm{id}_W : W \to W$ – полиномиальное отображение, и для любого $\varphi \in k[W]$ $\mathrm{id}_W^*(\varphi) = \varphi$, то из (3) заключаем, что $(\alpha \circ \beta)^* = \mathrm{id}_W^*$. Из единственности полиномиального отображения получаем $\alpha \circ \beta = \mathrm{id}_W$. Аналогично получаем, что $\beta \circ \alpha = \mathrm{id}_V$. Следовательно, α и β взаимно обратны. □

Лемма 1. *Пусть* $a_i, b_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,m}$. *Тогда* $a_1a_2\ldots a_m - b_1b_2\ldots b_m \in I$, *где* $I = < a_1 - b_1,\ldots,a_m - b_m > \subset k[x_1,\ldots,x_n]$.

Доказательство вытекает из равенства $a_1a_2\ldots a_m - b_1b_2\ldots b_m = a_1(a_2\ldots a_m - b_2\ldots b_m) + b_2\ldots b_m(a_1 - b_1)$ с использованием при этом метода математической индукции.

Теорема 3. *Аффинные многообразия* $V \subset k^m$ *и* $W \subset k^n$ *изоморфны тогда и только тогда, когда существует полиномиальное отображение* $\alpha : V \to W$, *представленное* n*-набором полиномов* $\alpha(x_1,\ldots,x_m) = (a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m))$ *и такое, что базис Грёбнера* G *идеала* $K = \mathbf{I}(V) + < y_1 - a_1(x_1,\ldots,x_m),\ldots,y_n - a_n(x_1,\ldots,x_m)) > \subset k[x_1,\ldots,x_m,y_1,\ldots,y_n]$ *по отношению к lex-упорядочению, где каждое* x_i *больше любого* y_j, *обладает следующими свойствами: для любого* i, $i = \overline{1,n}$, *существуют* $g_i \in G$ *такие, что* $g_i = x_i - h_i$, *где* $h_i \in k[y_1,\ldots,y_n]$.

Доказательство. Пусть многообразия V и W изоморфны. Тогда существуют полиномиальные отображения $\alpha : V \to W$ и $\alpha^{-1} : W \to V$, представленные соответственно n-наборами полиномов $\alpha(x_1,\ldots,x_m) = (a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m))$ и $\alpha^{-1}(y_1,\ldots,y_n) = (b_1(y_1,\ldots,y_n),\ldots,b_m(y_1,\ldots,y_n))$.

Пусть $\mathbf{I}(W) = < p_1,\ldots,p_s > \subset k[y_1,\ldots,y_n]$. Так как для любых $(x_1,\ldots,x_m) \in V$, $(y_1,\ldots,y_n) \in W$, где $y_k = a_k(x_1,\ldots,x_m)$, $k = \overline{1,n}$, то для любого j, $j = \overline{1,s}$, и для любого $(x_1,\ldots,x_m) \in V$ $p_j(a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m)) = 0$, т.е. $p_j(a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m)) \in \mathbf{I}(V)$. Образуем идеал $K = \mathbf{I}(V) + < y_1 - a_1(x_1,\ldots,x_m),\ldots,y_n - a_n(x_1,\ldots,x_m) >$, в котором при lex-упорядочении каждое

x_i больше любого y_j. Покажем, что для любого i, $i = \overline{1,n}$, $x_i - b_i(y_1,\ldots,y_n) \in K$. Имеем $x_i - b_i(y_1,\ldots,y_n) = x_i - b_i(a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m)) + b_i(a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m)) - b_i(y_1,\ldots,y_n)$. Так как $b_i(y_1,\ldots,y_n) = \sum_{\alpha} c_{i\alpha} {y_1}^{\alpha_1}\ldots{y_n}^{\alpha_n}$, то $b_i(a_1,\ldots,a_n) - b_i(y_1,\ldots,y_n) = \sum_{\alpha} c_{i\alpha}({a_1}^{\alpha_1}\ldots{a_n}^{\alpha_n} - {y_1}^{\alpha_1}\ldots{y_n}^{\alpha_n})$. На основании леммы 1 ${a_1}^{\alpha_1}\ldots{a_n}^{\alpha_n} - {y_1}^{\alpha_1}\ldots{y_n}^{\alpha_n} \in < y_1 - a_1,\ldots,y_n - a_n >$. Отсюда, с учетом того, что $x_i - b_i(a_1,\ldots,a_n) \in \mathbf{I}(V)$, заключаем, что $x_i - b_i(y_1,\ldots,y_n) \in K$. Образуем базис Грёбнера идеала K по отношению к lex-упорядочению, где каждое x_i больше любого y_i. Из свойств базисов Грёбнера заключаем, что существуют $g_i \in G$, где $\mathrm{LT}(g_i) = \mathrm{LT}(x_i - b_i(y_1,\ldots,y_n)) = x_i$. Так как $\bar{x}_i^{\,G} - \bar{b}_i^{\,G} = h_i$, где $h_i \in k[y_1,\ldots,y_n]$, то отсюда получаем, что $g_i = x_i - h_i(y_1,\ldots,y_n)$.

Если существует полиномиальное отображение $\alpha : V \to W$, представленное n-набором полиномов $\alpha(x_1,\ldots,x_m) = (a_1(x_1,\ldots,x_m),\ldots,a_n(x_1,\ldots,x_m))$ и такое, что в базисе Грёбнера G идеала K, где каждое x_i больше любого y_j, для любого i, $i = \overline{1,m}$, существуют $g_i \in G$ такие, что $g_i = x_i - h_i(y_1,\ldots,y_n)$, то $x_i - h_i(y_1,\ldots,y_n) = \sum_{j=1}^{n} q_{ij}(x_1,\ldots,x_m,y_1,\ldots,y_n)(y_j - q_j(x_1,\ldots,x_m)) + w(x_1,\ldots,x_m, y_1,\ldots,y_n)$, где $w(x_1,\ldots,x_m, y_1,\ldots,y_n) = \sum_{\alpha} \beta_\alpha(x_1,\ldots,x_m,y_1,\ldots,y_n)\nu_\alpha(x_1,\ldots,x_m)$, с $\nu_\alpha \in \mathbf{I}(V)$, q_{ij}, $\beta_\alpha \in k[x_1,\ldots,x_m]$. Отсюда для $y_j = a_j(x_1,\ldots,x_m)$ $x_i - h_i(y_1,\ldots,y_n) \in \mathbf{I}(V)$, т.е. $(h_1(y_1,\ldots,y_n),\ldots,h_m(y_1,\ldots,y_n)) \in V$. Следовательно, для отображения $\alpha : V \to W$ существует обратное $\alpha^{-1} : W \to V$, представленное n-набором полиномов $\alpha^{-1}(y_1,\ldots,y_n) = (h_1(y_1,\ldots,y_n),\ldots,h_m(y_1,\ldots,y_n))$. Таким образом, многообразия V и W изоморфны. □

Определение 6. Пусть $f_1,\ldots,f_m \in k[x_1,\ldots,x_n]$. Через $k[f_1,\ldots,f_m]$ будем обозначать подмножество в $k[x_1,\ldots,x_n]$ вида $k[f_1,\ldots,f_n] = \{f \in k[x_1,\ldots,x_n] : \exists\, g = \sum_{\alpha} g_\alpha {y_1}^{\alpha_1}\ldots{y_n}^{\alpha_m} \in k[y_1,\ldots,y_m]$ такой, что $f = g(f_1,\ldots,f_m) = \sum_{\alpha} g_\alpha {f_1}^{\alpha_1}\ldots{f_m}^{\alpha_m}\}$.

Множество $k[f_1,\ldots,f_n]$ является замкнутым относительно сложения и умножения и содержит все константы. Поэтому $k[f_1,\ldots,f_n]$ – подкольцо в $k[x_1,\ldots,x_n]$.

Определение 7. Пусть $F = (f_1,\ldots,f_m)$, где $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,m}$. Положим $I_F = \{h \in k[y_1,\ldots,y_m] : h(f_1,\ldots,f_m) = 0 \text{ в } k[x_1,\ldots,x_n]\}$.

Предложение 4. *Пусть* $F = (f_1,\ldots,f_m)$, *где* $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,m}$. *Тогда множество* I_F *– простой идеал в* $k[y_1,\ldots,y_m]$. Идеал I_F будем называть *идеалом сизигий* для F.

Доказательство. Очевидно, $0 \in I_F$. Если $h_1, h_2 \in I_F$, то $h_1(f_1,\ldots,f_m) = 0$, $h_2(f_1,\ldots,f_m) = 0$, т.е. $h_1 + h_2 \in I_F$. Если $h \in I_F$, то для любого $p \in k[y_1,\ldots,y_m]$ $p(f_1,\ldots,f_m)h(f_1,\ldots,f_m) = 0$, и значит, $ph \in I_F$. Таким образом, I_F – идеал в $k[y_1,\ldots,y_m]$. Если $fg \in I_F$, то $f(f_1,\ldots,f_m)g(f_1,\ldots,f_m) = 0$, т.е. $f \in I_F$ или $g \in I_F$. □

Предложение 5. *Пусть* $F = (f_1,\ldots,f_m)$, *где* $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,m}$, *и пусть* $I_F \subset k[y_1,\ldots,y_m]$ *– идеал сизигий для* F. *Тогда имеет место кольцевой изоморфизм*

$$k[y_1,\ldots,y_m] / I_F \cong k[f_1,\ldots,f_m].$$

Доказательство. Элементами факторкольца $k[y_1,\ldots,y_m] / I_F$ являются $[g]$, где $g \in k[y_1,\ldots,y_m]$. Если $[g] = [g_1]$, то $g - g_1 \in I_F$. Определим отображение $\varphi : k[y_1,\ldots,y_m] / I_F \to k[f_1,\ldots,f_m]$ следующим образом: $\varphi([g]) = g(f_1,\ldots,f_m)$. Так как каждый элемент из $k[f_1,\ldots,f_m]$ представлен некоторым полиномом $g(f_1,\ldots,f_m)$, то φ – отображение «на». Докажем инъективность φ. Пусть $\varphi([g_1]) = \varphi([g_2])$. Тогда $g_1(f_1,\ldots,f_m) = g_2(f_1,\ldots,f_m)$, а значит, $g_1 - g_2 \in I_F$. Следовательно, $[g_1] = [g_2]$, т.е. φ инъективно. Если $[g], [h] \in k[y_1,\ldots,y_m] / I_F$, то $\varphi([g] + [h]) = \varphi([g + h]) = g(f_1,\ldots,f_m) + h(f_1,\ldots,f_m) = \varphi([g]) + \varphi([h])$. Аналогично, $\varphi([g][h]) = \varphi([g])\varphi([h])$. Таким образом, φ сохраняет суммы и произведения и является инъективным отображением «на». □

Предложение 6. *Пусть* $F = (f_1,\ldots,f_m)$, *где* $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,m}$. *Тогда* $I_F = J_F \cap k[y_1,\ldots,y_m]$, *где* $J_F = < y_1 - f_1,\ldots,y_m - f_m > \subset k[x_1,\ldots,x_n,y_1,\ldots,y_m]$.

Доказательство. Пусть $g \in J_F \cap k[y_1,\ldots,y_m]$. Тогда $g(y_1,\ldots,y_m) = \sum_{i=1}^{m}\left(y_i - f_i(x_1,\ldots,x_n)\right)h_i(x_1,\ldots,x_m, y_1,\ldots,y_m)$, где $h_i \in k[x_1,\ldots,x_m,y_1,\ldots,y_m]$. Следовательно, $g(f_1,\ldots,f_m) = \sum_{i=1}^{m}\left(f_i(x_1,\ldots,x_n) - f_i(x_1,\ldots,x_n)\right)h_i(x_1,\ldots,x_m, f_1,\ldots,f_m)$, т.е. $g \in I_F$. Пусть теперь $g(y_1,\ldots,y_m) \in I_F$. Тогда $g(f_1,\ldots,f_m) = 0$. На основании леммы 1 $g(y_1,\ldots,y_m) = g(y_1,\ldots,y_m) - g(f_1,\ldots,f_m) \in J_F$, т.е. $g(y_1,\ldots,y_m) \in J_F \cap k[y_1,\ldots,y_m]$. □

Следствие 1. *Пусть* $F = (f_1,\ldots,f_m)$, *где* $f_i \in k[x_1,\ldots,x_n]$, $i = \overline{1,m}$. *Пусть в кольце* $k[x_1,\ldots,x_n, y_1,\ldots,y_m]$ *задано мономиальное упорядочение исключающего типа такое, что моном, содержащий хотя бы одну из переменных* $x_1,\ldots,x_n$, *больше любого монома из* $k[y_1,\ldots,y_m]$. *Если* G *– базис Грёбнера*

идеала $J_F = \langle y_1 - f_1,\ldots,y_m - f_m \rangle \subset k[x_1,\ldots,x_n, y_1,\ldots,y_m]$, *то* $G \cap k[y_1,\ldots,y_m]$ *является базисом Грёбнера идеала* $I_F = J_F \cap k[y_1,\ldots,y_m]$.

Предложение 7. *Пусть даны полиномы* $f_i \in k[x_1,\ldots,x_n]$, *где* $i = \overline{1,m}$. *Пусть задано мономиальное упорядочение в* $k[x_1,\ldots,x_n, y_1,\ldots,y_m]$ *такое, что любой моном, содержащий хотя бы одну из переменных* $x_1,\ldots,x_n$, *больше всех мономов из* $k[y_1,\ldots,y_m]$. *Пусть* G *– базис Грёбнера идеала* $\langle y_1 - f_1,\ldots,y_m - f_m \rangle \subset k[x_1,\ldots,x_n, y_1,\ldots,y_m]$. *Пусть задан полином* $f \in k[x_1,\ldots,x_n]$, *а* $g = \overline{f}^{G}$ *– остаток от деления* f *на* G. *Тогда*

1) $f \in k[f_1,\ldots,f_m]$ *тогда и только тогда, когда* $g \in k[y_1,\ldots,y_m]$;

2) если $f \in k[f_1,\ldots,f_m]$, *то* $f = g(f_1,\ldots,f_m)$.

Доказательство. Пусть для идеала $\langle y_1 - f_1,\ldots,y_m - f_m \rangle \subset k[x_1,\ldots,x_n, y_1,\ldots,y_m]$ базисом Грёбнера является $G = \{g_1,\ldots,g_t\}$. Произведя алгоритмом деления деление f на G, имеем равенство: $f = \sum_{k=1}^{t} A_k g_k + g$, где $A_1,\ldots,A_t$, $g \in k[x_1,\ldots,x_n, y_1,\ldots,y_m]$. Пусть $g \in k[y_1,\ldots,y_m]$. Так как $g_k(x_1,\ldots,x_n, y_1,\ldots,y_m) \in \langle y_1 - f_1,\ldots,y_m - f_m \rangle$, то $g_k(x_1,\ldots,x_n, y_1,\ldots,y_m) = 0$, $k = \overline{1,t}$. Следовательно, $f(x_1,\ldots,x_n) = \sum_{k=1}^{t} \tilde{A}_k g_k(x_1,\ldots,x_n, f_1,\ldots, f_m) + g(f_1,\ldots,f_m) = g(f_1,\ldots,f_m)$, а значит, $f \in k[f_1,\ldots,f_m]$. Пусть теперь существует $g \in k[y_1,\ldots,y_m]$ такое, что $f = g(f_1,\ldots,f_m)$. На основании леммы 1 $f - g(y_1,\ldots,y_m) = g(f_1,\ldots,f_m) - g(y_1,\ldots,y_m) \in \langle y_1 - f_1,\ldots,y_m - f_m \rangle$. Следовательно, $f - g(y_1,\ldots,y_m) = \sum_{k=1}^{m} h_k (y_k - f_k)$, т.е. $f = \sum_{k=1}^{m} h_k (y_k - f_k) + g(y_1,\ldots,y_m)$. Образуем множество $G' = G \cap k[y_1,\ldots,y_m]$. Не умаляя общности можно считать, что $G' = \{g_1,\ldots,g_s\}$, где $s \le t$. Пусть $\overline{g}^{G'} = g'$. Тогда $g = \sum_{i=1}^{s} B_i g_i + g'$, где B_i, $g' \in k[y_1,\ldots,y_m]$. Таким образом, $f = \sum_{k=1}^{m} h_k (y_k - f_k) + \sum_{i=1}^{s} B_i g_i + g' = \sum_{k=1}^{m} P_k (y_k - f_k) + g'$. Докажем, что g' является остатком от деления полинома f на G. Для этого достаточно показать, что ни один член полинома g' не делится ни на один старший член из $\mathrm{LT}(G)$. Допустим противное, и пусть существует $g_i \in G$ такой, что $\mathrm{LT}(g_i)$ делит некоторый член полинома g'. Так как $g' \in k[y_1,\ldots,y_m]$, то $\mathrm{LT}(g_i)$ содержит только переменные $y_1,\ldots,y_m$. Следовательно, с учетом заданного мономиального упорядочения заключаем, что $g_i \in k[y_1,\ldots,y_m]$. Таким об-

разом, $g_i \in G'$. Так как $g' = \overline{g}^{G'}$, то $\mathrm{LT}(g_i)$ не делит ни один из членов полинома g'. Получили противоречие. Таким образом, $g' = \overline{f}^{G}$. Итак, п. 1 доказан. Докажем п. 2. Если $f \in k[f_1,\ldots,f_m]$, то из доказательства п. 1 следует, что $f = \sum_{k=1}^{m} P_k(y_k - f_k) + g'$, где $g' = \overline{f}^{G} \in k[y_1,\ldots,y_m]$. Значит, $f = g'(f_1,\ldots,f_m)$. □

4.4. РАЦИОНАЛЬНЫЕ ФУНКЦИИ НА МНОГООБРАЗИИ

Кольцо полиномов $k[x_1,\ldots,x_n]$ является подкольцом поля рациональных функций $k(x_1,\ldots,x_n) = \{\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)} : f, g \in k[x_1,\ldots,x_n], g \neq 0\}$.

Пусть R – некоторая область целостности. Тогда можно построить ее поле частных, которое обозначается $QF(R)$. Элементами этого поля являются «дроби» $\frac{r}{s}$, где $r, s \in R$, $s \neq 0$. Сложение и умножение элементов из $QF(R)$ определяем так: $\frac{r}{s} + \frac{t}{u} = \frac{ru+ts}{su}$ и $\frac{r}{s}\cdot\frac{t}{u} = \frac{rt}{su}$. Так как R – область целостности, то знаменатели и суммы, и произведения не равны нулю. Две дроби $\frac{r}{s}$ и $\frac{r'}{s'}$ называются *равными* в $QF(R)$, если $rs' = r's$. Легко видеть, что все аксиомы поля в $QF(R)$ выполняются. Поле $QF(R)$ содержит подмножество $\{\frac{r}{1} : r \in R\}$, которое является подкольцом, изоморфным R.

Определение 1. Пусть V – неприводимое аффинное многообразие в k^n. Тогда поле $QF(k[V])$ называется *полем функций* или *полем рациональных функций* на V и обозначается $k(V)$.

Явно поле функций $k(V)$, где $V \subset k^n$, можно задать так: $k(V) = \{\frac{\varphi}{\psi} : \varphi, \psi \in k[V], \psi \neq 0\} = \{\frac{[f]}{[g]} : f, g \in k[x_1,\ldots,x_n], g \notin \mathbf{I}(V)\}$. Элемент $\frac{\varphi}{\psi} \in k(V)$ определяет функцию только на дополнении к $\mathbf{V}_V(\psi)$.

Определение 2. Пусть $V \subset k^n$, $W \subset k^m$ – неприводимые аффинные многообразия. *Рациональным отображением* многообразия V на W называется функция φ вида

$$\varphi(x_1,\ldots,x_m) = \left(\frac{f_1(x_1,\ldots,x_m)}{g_1(x_1,\ldots,x_m)},\ldots,\frac{f_n(x_1,\ldots,x_m)}{g_n(x_1,\ldots,x_m)}\right), \qquad (1)$$

где $\frac{f_i}{g_i} \in k(x_1,\ldots,x_m)$, которая удовлетворяет следующим условиям:

1) φ определена хотя бы в одной точке из V;

2) для любой точки $(a_1,\ldots,a_m) \in V$, в которой φ определена, $\varphi(a_1,\ldots,a_m) \in W$.

Рациональное отображение $\varphi : V \to W$ может не быть функцией из V в W в обычном смысле, ибо она не обязательно определена всюду на V. Для рационального отображения будем использовать следующее обозначение: $\varphi : V \dashrightarrow W$.

Из условия 1) следует, что множество точек, где рациональное отображение φ, заданное формулой (1), не определено, есть собственное подмногообразие $\mathbf{V}_V(g_1,\ldots,g_n)$ многообразия V.

Определение 3. Пусть $\varphi, \psi : V \dashrightarrow W$ – рациональные отображения, заданные формулами: $\varphi = \left(\frac{f_1}{g_1},\ldots,\frac{f_n}{g_n}\right)$, $\psi = \left(\frac{h_1}{l_1},\ldots,\frac{h_n}{l_n}\right)$. Тогда φ и ψ называются *равными*, если для всех i, $1 \le i \le n$, $f_i l_i - h_i g_i \in \mathbf{I}(V)$.

Предложение 1. *Два рациональных отображения $\varphi, \psi : V \dashrightarrow W$ равны тогда и только тогда, когда существует собственное подмногообразие $V' \subset V$ такое, что φ, ψ определены на $V - V'$ и для всех $p \in V - V'$ $\varphi(p) = \psi(p)$.*

Доказательство. Пусть $\varphi = \left(\frac{f_1}{g_1},\ldots,\frac{f_n}{g_n}\right)$, $\psi = \left(\frac{h_1}{l_1},\ldots,\frac{h_n}{l_n}\right)$. Предположим, что φ и ψ равны в смысле определения 3, и пусть $V_1 = \mathbf{V}_V(g_1,\ldots,g_n)$, $V_2 = \mathbf{V}_V(l_1,\ldots,l_n)$. Так как многообразие V неприводимо, а V_1, V_2 – собственные подмногообразия V, то и $V' = V_1 \cup V_2$ – собственное подмногообразие в V. Так как φ, ψ определены на $V - V'$, а $f_i l_i - h_i g_i \in \mathbf{I}(V)$, где $i = \overline{1,n}$, то $\frac{f_i}{g_i}$ и $\frac{h_i}{l_i}$, $i = \overline{1,n}$, представляют одну и ту же функцию на $V - V'$, т.е. для всех $p \in V - V'$ $\varphi(p) = \psi(p)$.

Пусть теперь наоборот φ и ψ определены и равны (как функции) на $V - V'$. Тогда для любого $i = \overline{1,n}$ $\frac{f_i}{g_i} = \frac{h_i}{l_i}$ на $V - V'$. Отсюда $f_i l_i - h_i g_i = 0$ на $V - V'$, а поэтому $V = \mathbf{V}_V(f_i l_i - h_i g_i)$ $\mathbf{U}$ V'. Так как V неприводимо, а V' – собственное подмногообразие многообразия V, то $V = \mathbf{V}_V(f_i l_i - h_i g_i)$. Таким образом, $f_i l_i - h_i g_i \in \mathbf{I}(V)$. □

Определение 4. Пусть даны отображения $\varphi : V - - \to W$, $\psi : W - - \to Z$. Будем говорить, что *композиция $\psi \circ \varphi$ определена*, если существует $p \in V$ такое, что φ определено в p, а ψ определено в φ(p).

Предложение 2. *Пусть $\varphi : V - - \to W$, $\psi : W - - \to Z$ – рациональные отображения такие, что композиция $\psi \circ \varphi$ определена. Тогда существует собственное подмногообразие $V' \subset V$, такое, что*

4) φ определено на $V - V'$, а ψ определено на $\varphi(V - V')$;

5) *$\psi \circ \varphi : V - - \to Z$ – рациональное отображение, определенное на $V - V'$.*

Доказательство. Пусть φ и ψ имеют вид:

$$\varphi(x_1,\ldots,x_m) = \left(\frac{f_1(x_1,\ldots,x_m)}{g_1(x_1,\ldots,x_m)},\ldots,\frac{f_n(x_1,\ldots,x_m)}{g_n(x_1,\ldots,x_m)}\right),$$

$$\psi(y_1,\ldots,y_n) = \left(\frac{h_1(y_1,\ldots,y_n)}{l_1(y_1,\ldots,y_n)},\ldots,\frac{h_s(y_1,\ldots,y_n)}{l_s(y_1,\ldots,y_n)}\right).$$

Тогда j-я координата отображения $\psi \circ \varphi$ равна $\dfrac{h_j\left(\frac{f_1}{g_1},\ldots,\frac{f_n}{g_n}\right)}{l_j\left(\frac{f_1}{g_1},\ldots,\frac{f_n}{g_n}\right)}$ и, очевидно, является рациональной функцией от $x_1,\ldots,x_m$. Для представления в виде частного полиномов запишем ее в виде $\frac{P_j}{Q_j} = \dfrac{(g_1\ldots g_n)^M h_j\left(\frac{f_1}{g_1},\ldots,\frac{f_n}{g_n}\right)}{(g_1\ldots g_n)^M l_j\left(\frac{f_1}{g_1},\ldots,\frac{f_n}{g_n}\right)}$, где M – достаточно большое натуральное число.

Положим $v' = \mathbf{V}_V([Q_1],\ldots,[Q_s],\ [g_1\ldots g_n]) \subset V$. Тогда φ определена на $V -$

V', а ψ определена на $\varphi(V - V')$. Покажем, что $V \neq V'$. По условию существует $p \in V$ такое, что φ определено в p, а ψ определено в φ(p). Это означает, что для любого i, где $i = \overline{1,n}$, $g_i(p) \neq 0$, а для любого j, где $j = \overline{1,s}$ $l_j(\frac{f_1(p)}{g_1(p)},\ldots,\frac{f_n(p)}{g_n(p)}) \neq 0$. Значит, для любого j $Q_j(p) \neq 0$, а поэтому $p \in V - V'$. □

Определение 5. 1) Два неприводимых многообразия $V \subset k^m$ и $W \subset k^n$ называются *бирационально эквивалентными*, если существуют рациональные отображения $\varphi : V - - \to W$, $\psi : W - - \to V$, такие, что композиции $\psi \circ \varphi$ и $\varphi \circ \psi$ определены (в смысле определения 4) и равны (в смысле определения 3) тождественным отображениям id_V и id_W соответственно.

2) Многообразие называется *рациональным*, если оно бирационально эквивалентно пространству k^n для некоторого n.

Теорема 1. *Два неприводимых многообразия V и W бирационально эквивалентны тогда и только тогда, когда существует изоморфизм $k[V] \cong k[W]$ их полей функций, тождественный на константах (по определению два поля изоморфны как коммутативные кольца).*

Доказательство. Предположим, что V и W бирационально эквивалентны и $\varphi : V - - \to W$, $\psi : W - - \to V$ – соответствующие отображения. Определим отображение $\varphi^* : k(W) \to k(V)$ формулой $\varphi^*(f) = f \circ \varphi$ и докажем, что это изоморфизм. Для этого докажем сначала, что для любого $f \in k(W)$ функция $f \circ \varphi$ определена в некоторой точке многообразия V. Из предложения 2 следует, что существует собственное подмногообразие $W_1 \subset W$ такое, что ψ определено на $W - W_1$, а φ определено на $\psi(W - W_1)$. Из предложения 1 с учетом $\varphi \circ \psi = \mathrm{id}_W$ заключаем, что существует собственное подмногообразие $W_2 \subset W$ такое, что $\varphi \circ \psi$ тождественно на $W - W_2$. Так как W неприводимо, то $W' = W_1 \cup W_2$ – собственное подмногообразие многообразия W. Таким образом, существует собственное подмногообразие $W' \subset W$ такое, что ψ определено на $W - W'$, φ определено на $\psi(W - W')$, а $\varphi \circ \psi$ тождественно на $W - W'$. Если $f \in k(W)$, то существует собственное подмногообразие $W'' \subset W$ такое, что f определена на $W - W''$. Так как W неприводимо, то $W' \cup W'' \neq W$. Возьмем любую функцию $g \in W - (W' \cup W'')$. Тогда отображение φ определено в точке $p = \psi(q) \in V$, а так как φ(p) $= q \notin W''$, то f определена в φ(p). Итак, доказано, что $f \circ \varphi$ определена в некоторой точке многообразия V. Из определения 3 заключаем, что функция $\varphi^*(f) = f \circ \varphi$ существует как элемент из поля $k(V)$. Таким образом, существует отображение $\varphi^* : k(W) \to k(V)$. Покажем, что φ^*

– кольцевой гомоморфизм. Наряду с f возьмем произвольную функцию $g \in k(W)$. Тогда $\varphi^*(f + g) = (f + g) \circ \varphi = (f \circ \varphi) + (g \circ \varphi) = \varphi^*(f) + \varphi^*(g)$. Аналогично, $\varphi^*(fg) = \varphi^*(f)\varphi^*(g)$. Возьмем теперь постоянную функцию $a \in k(W)$, где $a \in k$, со значением a. Тогда $\varphi^*(a) = a \circ \varphi$ является постоянной функцией на $k(V)$ с тем же значением a. Аналогично кольцевому гомоморфизму $\varphi^* : k(V) \to k(W)$ может быть построен кольцевой гомоморфизм $\psi^* : k(V) \to k(W)$. Покажем теперь, что отображения φ^*, ψ^* взаимно обратны. Рассмотрим функцию $(\psi^* \circ \varphi^*)(f) = \psi^*(\varphi^*(f)) = \varphi^*(f) \circ \psi = f \circ \varphi \circ \psi$, где $f \in k(W)$. В наших обозначениях функция $f \circ \varphi \circ \psi$ равна f как функция на множестве $W – (W' \cup W'')$. На основании предложения 1 $f \circ \varphi \circ \psi = f$ в $k(W)$. Отсюда $\psi^* \circ \varphi^* = \mathrm{id}_{k(W)}$. Аналогично, $\varphi^* \circ \psi^* = \mathrm{id}_{k(V)}$. Таким образом, $\varphi^* : k(W) \to k(V)$ является изоморфизмом полей.

Пусть теперь существует изоморфизм полей $\varphi^* : k(W) \to k(V)$, тождественный на константах. Тогда φ^* и $\psi^* = (\varphi^*)^{-1}$ задаются рациональными отображениями из V в W и из W в V соответственно. При этом отображению $\varphi^* : k(W) \to k(V)$ соответствует рациональное отображение $\varphi : V - - \to W$ такое, что для любого $f \in k(W)$ $\varphi^*(f) = f \circ \varphi$. Аналогично, отображению $\psi^* = (\varphi^*)^{-1} : k(V) \to k(W)$ соответствует рациональное отображение $\psi : W - - \to V$. Покажем, что отображения φ и ψ взаимно обратны. Рассмотрим композицию $\varphi \circ \psi : W - - \to W$. Очевидно, что это рациональное отображение, причем для любого $f \in k(W)$

$$(\varphi \circ \psi)^*(f) = f \circ \varphi \circ \psi = \psi^*(f \circ \varphi) = \psi^*(\varphi^*(f)) = (\varphi^*)^{-1}(\varphi^*(f)) = f. \quad (2)$$

Но $\mathrm{id}_W : W - - \to W$ – рациональное отображение, причем для любого $f \in k(W)$ $\mathrm{id}_W^*(f) = f$. Согласно (2) $(\varphi \circ \psi)^* = \mathrm{id}_W^*$, а тогда из предложения 1 заключаем, что $\varphi \circ \psi = \mathrm{id}_W$. Аналогично, $\psi \circ \varphi = \mathrm{id}_V$. □

ГЛАВА 5. ПРОЕКТИВНЫЕ МНОГООБРАЗИЯ

5.1. ПРОЕКТИВНЫЕ МНОГООБРАЗИЯ И ОДНОРОДНЫЕ ИДЕАЛЫ

Рассмотрим отношение эквивалентности ~ на множестве ненулевых точек аффинного пространства k^{n+1}, полагая $(x_0',\ldots,x_n') \sim (x_0,\ldots,x_n)$, если существует ненулевой элемент $\lambda \in k$ такой, что $(x_0',\ldots,x_n') = \lambda(x_0,\ldots,x_n)$. Обозначим через 0 нулевой вектор $(0,\ldots,0) \in k^{n+1}$.

Определение 1. *n-мерным проективным пространством* $\mathbf{P}^n(k)$ над полем k называется множество классов эквивалентности в $k^{n+1} - \{0\}$ по отношению ~, т.е. $\mathbf{P}^n(k) = (k^{n+1} - \{0\}) / \sim$. Каждый ненулевой $(n+1)$ мерный вектор $(x_0,\ldots,x_n) \in k^{n+1}$ определяет точку $p \in \mathbf{P}^n(k)$, при этом $(x_0,\ldots,x_n)$ называются *однородными координатами* точки p.

Предложение 1. *Пусть $U_0 = \{(x_0,\ldots,x_n) \in \mathbf{P}^n(k) : x_0 \neq 0\}$. Тогда отображение φ, переводящее точку $(a_0,\ldots,a_n) \in k^n$ в точку $(1, a_0,\ldots,a_n) \in \mathbf{P}^n(k)$, устанавливает взаимно однозначное соответствие между k^n и $U_0 \subset \mathbf{P}^n(k)$.*

Доказательство. Так как первая координата точки $\varphi(a_0,\ldots,a_n) = (1, a_0,\ldots,a_n)$ не равна нулю, то образ отображения принадлежит U_0. Определим обратное отображение $\psi : U_0 \to k^n$ следующим образом. Пусть $p = (x_0,\ldots,x_n) \in U_0$. Тогда $x_0 \neq 0$, а значит, $p = (1, \frac{x_1}{x_0},\ldots,\frac{x_n}{x_0})$. Положим $\psi(p) = (\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}) \in k^n$. Отображение ψ определено корректно, ибо каждому $p = (x_0,\ldots,x_n) \in U_0$ сопоставляется единственная точка $(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}) \in k^n$. Отображения φ и ψ взаимно обратны, так как $\varphi \circ \psi = \mathrm{id}_{U_0}$, $\psi \circ \varphi = \mathrm{id}_{k^n}$. □

Из определения множества U_0 имеем $\mathbf{P}^n(k) = U_0 \cup H$, где

$$H = \{p \in \mathbf{P}^n(k) : p = (0, x_1,\ldots,x_n)\}. \qquad (1)$$

Отождествляя U_0 с k^n, будем называть H *бесконечно удаленной гиперплоскостью*. Из (1) следует, что точки H определяются n-наборами $(x_1,\ldots,x_n)$, причем два набора определяют одну и ту же точку из H тогда и только тогда, когда каждый из наборов является скалярным кратным другого (нужно просто игнорировать первую нулевую координату из H). Таким

образом, H можно считать копией проективного пространства $\mathbf{P}^{n-1}(k)$ на единицу меньшей размерности. Отождествляя U_0 с k^n, а H с $\mathbf{P}^{n-1}(k)$, можно записать

$$\mathbf{P}^n(k) = k^n \cup \mathbf{P}^{n-1}(k). \qquad (2)$$

Следствие 1. *Для каждого* i, $i = \overline{0,n}$ *определим подмножество* $U_i = \{(x_0,\ldots,x_n) \in \mathbf{P}^n(k) : x_i \neq 0\}$. *Тогда*

1) Точки каждого множества U_i *находятся во взаимно однозначном соответствии с точками пространства* k^n;

2) Дополнение $\mathbf{P}^n(k) - U_i$ *может быть отождествлено с* $\mathbf{P}^{n-1}(k)$;

3) $\mathbf{P}^n(k) = \bigcup_{i=0}^{n} U_i$.

Доказательство. 1) следует из предложения 1, 2) – из формулы (2). Докажем 3). Пусть p = $(x_0,\ldots,x_n) \in \mathbf{P}^n(k)$. Тогда существует i такое, что $x_i \neq 0$, а значит, $p \in U_i$. Следовательно, $\mathbf{P}^n(k) \subset \bigcup_{i=0}^{n} U_i$. Обратное включение очевидно. □

Определение 2. Полином $f \in k[x_1,\ldots,x_n]$ называется *однородным полной степени* m, если каждый член из f имеет полную степень m.

Предложение 2. *Пусть* $f \in k[x_1,\ldots,x_n]$ *– однородный полином. Если* f *обращается в нуль в точке* $p \in \mathbf{P}^n(k)$ *для какого-то конкретного набора ее однородных координат, что* f *обращается в нуль при любом выборе ее координат. В частности,* $V(f) = \{p \in \mathbf{P}^n(k) : f(p) = 0\}$ *– это корректно определенное подмножество в* $\mathbf{P}^n(k)$.

Доказательство. Пусть $(a_0,\ldots,a_n)$ и $(\lambda a_0,\ldots,\lambda a_n)$ – два набора однородных координат точки $p \in \mathbf{P}^n(k)$. Предположим, что $f(a_0,\ldots,a_n) = 0$ и что f – однородный полином полной степени d. Тогда каждый член в f имеет вид

$$C x_0^{\alpha_0} \ldots x_n^{\alpha_n} \qquad (3),$$

где $\alpha_0 +\ldots + \alpha_n = d$. Подставляя в (3) λa_i вместо x_i, имеем $C(\lambda a_0)^{\alpha_0} \ldots (\lambda a_n)^{\alpha_n} = \lambda^d C a_0^{\alpha_0} \ldots a_n^{\alpha_n}$. Суммируя по всем членам полинома f, получаем $f(\lambda a_0,\ldots,\lambda a_n) = \lambda^d f(a_0,\ldots,a_n) = 0$. □

Если даже f и однороден, но уравнение $f = a$ не имеет смысла в $\mathbf{P}^n(k)$, если $a \neq 0$, $a \in k$.

Определение 3. Пусть $f_1,\ldots,f_s \in k[x_1,\ldots,x_n]$ – однородные полиномы. Положим $\mathbf{V}(f_1,\ldots,f_s) = \{(a_0,\ldots,a_n) \in \mathbf{P}^n(k) : f_i(a_0,\ldots,a_n) = 0,\ 1 \leq i \leq s\}$.

$\mathbf{V}(f_1,\ldots,f_s)$ называется *проективным многообразием*, определенным полиномами $f_1,\ldots,f_s$.

Предложение 3. *Рассмотрим проективное многообразие* $V = \mathbf{V}(f_1,\ldots,f_s)$. *Тогда* $W = V \cap U_0$ *может быть отождествлено с аффинным многообразием* $\mathbf{V}(g_1,\ldots,g_s) \subset k^n$, *где* $g_i(y_1,\ldots,y_n) = f_i(1, y_1,\ldots,y_n)$, $1 \le i \le s$. *При этом полиномы* g_i *называются дегомогенизацией полиномов* $f_i(y_0,\ldots,y_n)$ *относительно переменной* y_0.

Доказательство. Рассмотрим отображение $\psi : U_0 \to k^n$ из предложения 1. Пусть $(a_1,\ldots,a_n) \in \psi(W) = \psi(V \cap U_0)$. Тогда $(1, a_1,\ldots,a_n) \in U_0$, $g_i(a_1,\ldots,a_n) = f_i(1, a_1,\ldots,a_n) = 0$, т.е. $(a_1,\ldots,a_n) \in \mathbf{V}(g_1,\ldots,g_s)$. Следовательно, $\psi(W) \subset \mathbf{V}(g_1,\ldots,g_s)$. Наоборот, если $(a_1,\ldots,a_n) \in \mathbf{V}(g_1,\ldots,g_s)$, то $(1, a_1,\ldots,a_n) \in U_0$, причем $f_i(1, a_1,\ldots,a_n) = g_i(a_1,\ldots,a_n) = 0$. Поэтому $(1, a_1,\ldots,a_n) \in V$, а значит, $(1, a_1,\ldots,a_n) \in V \cap U_0$. Отсюда $\psi(1, a_1,\ldots,a_n) = (a_1,\ldots,a_n) \in \psi(W)$, т.е. $\mathbf{V}(g_1,\ldots,g_s) \subset \psi(W)$. Таким образом, $\psi(W) = \mathbf{V}(g_1,\ldots,g_s)$. □

Следствие 2. *Рассмотрим проективное многообразие* $V = \mathbf{V}(f_1,\ldots,f_s)$, *определенное однородными полиномами* $f_i \in k[x_1,\ldots,x_n]$. *Тогда подмножество* $W = V \cap U_i$ *может быть отождествлено с аффинным многообразием* $\mathbf{V}(g_1,\ldots,g_s) \subset k^n$, *где полиномы* $g_j(x_0,\ldots,x_{i-1}, x_{i+1},\ldots,x_n) = f_j(x_0,\ldots,x_{i-1}, 1, x_{i+1},\ldots,x_n)$, $i = \overline{1,s}$, *называются дегомогенизацией полиномов* $f_j(y_0,\ldots,y_n)$ *относительно переменной* y_i.

Доказательство вытекает из предложения 3 и следствия 1. □

Предложение 4. *Пусть* $g \in k[x_1,\ldots,x_n]$ *– полином полной степени* d.

1) Запишем g *в виде* $g = \sum_{i=0}^{d} g_i$, *где* g_i *– однородный полином полной степени* i. *Тогда* $g^h(x_0,\ldots,x_n) = \sum_{i=0}^{d} g_i(x_1,\ldots,x_n)x_0^{d-i}$ *является однородным полиномом в* $k[x_1,\ldots,x_n]$ *полной степени* d, *который называется гомогенизацией полинома* g;

2) Имеет место формула $g^h = x_0^d g(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0})$.

3) Дегомогенизация полинома g^h *относительно переменной* y_0 *дает снова* g, *т.е.* $g^h(1, x_1,\ldots,x_n) = g(x_1,\ldots,x_n)$.

4) Пусть $F(x_0,\ldots,x_n)$ *– однородный полином, и пусть* x_0^l *– наивысшая степень переменной* x_0, *которая делит* F.

Пусть $f = F(1, x_1,\ldots,x_n)$ *– дегомогенизация полинома* F. *Тогда* $F = x_0^l f^h$.

Доказательство. 1) Полином g^h является однородным полиномом полной степени d в $k[x_1,\ldots,x_n]$, так как $g_i(x_1,\ldots,x_n)x_0^{d-i}$ – однородный полином в $k[x_1,\ldots,x_n]$ полной степени d.

2) Так как g_i – однородные полиномы полной степени i, то $g^h(x_0,\ldots,x_n) = \sum_{i=0}^{d} g_i(x_1,\ldots,x_n)x_0^{d-i} = \sum_{i=0}^{d} g_i\left(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}\right)x_0^{i}x_0^{d-i} = \left[\sum_{i=0}^{d} g_i\left(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}\right)\right]x_0^{d} = x_0^{d}g\left(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}\right)$.

3) Так как $g^h(x_0,\ldots,x_n) = \sum_{i=0}^{d} g_i(x_1,\ldots,x_n)x_0^{d-i}$, то $g^h(1, x_0,\ldots,x_n) = \sum_{i=0}^{d} g_i(x_1,\ldots,x_n)$, т.е. дегомогенизация полинома g^h дает g.

4) Если $F(x_0,\ldots,x_n)$ – однородный полином полной степени d, а x_0^{l} – наивысшая степень переменной x_0, которая делит F, то $G = \frac{F}{x_0^{l}}$ – однородный полином полной степени $d-l$. Тогда $f = F(1, x_1,\ldots,x_n) = G(1, x_1,\ldots,x_n)$. Из п. 2) имеем $f^h = x_0^{d-l}G(1, \frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}) = x_0^{d-l}G(x_0, x_1,\ldots,x_n)x_0^{-(d-l)} = G(x_0, x_1,\ldots,x_n)$. Следовательно, $F = x_0^{l}G = x_0^{l}f^h$. □

Если дано аффинное многообразие $W = \mathbf{V}(g_1,\ldots,g_s) \subset k^n$, то гомогенизация уравнений, определяющих W, дает на основании предложения 4 проективное многообразие $V = \mathbf{V}(g_1^h,\ldots,g_s^h) \subset \mathbf{P}^n(k)$. На основании предложения 3 $V \cap U_0 = W$, т.е. исходное аффинное многообразие W является аффинной частью проективного многообразия V. Заметим, что проективное многообразие V, вообще говоря, определяется неоднозначно.

Лемма 1. *Пусть поле k бесконечно. Если полином $f \in k[x_0,\ldots,x_n]$ обращается в нуль в точке $p \in \mathbf{P}^n(k)$ на всех наборах ее однородных координат, то каждая однородная компонента f_i полинома f обращается в нуль в p.*

Доказательство. Представим f в виде суммы однородных компонент $f = \sum_{i=0}^{s} f_i$, где f_i, $i = \overline{0,s}$ – однородные полиномы полной степени i. Если f обращается в нуль в точке $p = (a_0,\ldots,a_n)$ на всех наборах ее однородных

координат, то для любого $\lambda \in k$, $\lambda \neq 0$ $f(\lambda a_0,\ldots,\lambda a_n) = \sum_{i=0}^{s} \lambda^i f_i(a_0,\ldots,a_n) =$ 0. Так как поле k бесконечно, то для всех i, $i = \overline{0,s}$, $f_i(a_0,\ldots,a_n) = 0$. □

Определение 4. Идеал $I \subset k[x_0,\ldots,x_n]$ называется *однородным*, если для любого $f \in I$ однородные компоненты f также принадлежат I.

Теорема 1. *Пусть идеал $I \subset k[x_0,\ldots,x_n]$. Следующие условия эквивалентны:*

1) I – однородный идеал;

2) $I = < f_1,\ldots,f_s >$, где полиномы f_i, $i = \overline{0,s}$ являются однородными;

3) *редуцированный базис Грёбнера идеала I (по отношению к любому мономиальному упорядочению) состоит из однородных полиномов.*

Доказательство. 1) $\Rightarrow$ 2). Пусть I – однородный идеал. На основании теоремы Гильберта о базисе $I = < F_1,\ldots,F_t >$, где $F_j \in k[x_0,\ldots,x_n]$, $j = \overline{1,t}$. Представим каждый полином F_j в виде суммы однородных компонент: $F_j = \sum_i F_{ji}$, где F_{ji} – однородные полиномы. Так как I – однородный идеал и $F_j \in I$, то каждый полином $F_{ji} \in I$. Рассмотрим идеал I', порожденный всеми однородными полиномами F_{ji}. Так как каждый полином F_j является суммой образующих идеала I', то $F_j \in I'$. Следовательно, $I \subset I'$. С другой стороны, так как все $F_{ji} \in I$, то $I' \subset I$. Отсюда $I = I'$, при этом идеал I имеет базис, состоящий из однородных полиномов F_{ji}.

2) $\Rightarrow$ 3). Пусть задан идеал $I = < f_1,\ldots,f_s >$, где полиномы $f_i \in k[x_0,\ldots,x_n]$ являются однородными. Фиксируем произвольное мономиальное упорядочение. Положим $F = \{f_1,\ldots,f_s\}$. Для нахождения базиса Грёбнера идеала I рассмотрим S-полиномы $S(f_i, f_j)$. Имеем $S(f_i, f_j) = \frac{x^{\gamma_{ij}}}{\mathrm{LT}(f_i)} f_i - \frac{x^{\gamma_{ij}}}{\mathrm{LT}(f_j)} f_j$, где $x^{\gamma_{ij}} = \mathrm{LCM}(\mathrm{LM}(f_i), \mathrm{LM}(f_j))$. Так как f_i, f_j однородны, то $S(f_i,f_j)$ – однородный полином, полная степень которого равна полной степени монома $x^{\gamma_{ij}}$. Из анализа алгоритма деления в случае однородных полиномов в $k[x_0,\ldots,x_n]$ заключаем, что $\overline{S(f_i, f_j)}^F$ – однородный полином, полная степень которого равна полной степени $S(f_i, f_j)$. Отсюда на основании алгоритма Бухбергера заключаем, что базис Грёбнера идеала I состоит из однородных полиномов. Редуцированный базис Грёбнера идеала I состоит из однородных полиномов, так как все редуцированные элементы этого идеала являются однородными полиномами.

3) $\Rightarrow$ 1). Пусть $I = < f_1,\ldots,f_s >$, где $F = \{f_1,\ldots,f_s\}$ – редуцированный базис Грёбнера идеала I. Возьмем любой элемент $f \in I$. Тогда $f = \sum_{j=1}^{s} A_j f_j$, где $A_j \in k[x_0,\ldots,x_n]$. Представим A_j в виде суммы однородных компонент: $A_j = \sum_{i=1}^{d} A_{ji}$. Подставляя A_j в f и собирая вместе члены одинаковой полной степени d, заключаем, что произвольная однородная компонента полинома f имеет вид $\sum_{j=1}^{s} A_{ji} f_j$, где сумма полных степеней однородных полиномов A_{ji}, f_j равна d. Следовательно, произвольная однородная компонента полинома f принадлежит I, т.е. идеал I является однородным. □

Следствие 3. *Пусть I_1, I_2 – однородные идеалы в $k[x_0, x_1,\ldots,x_n]$. Тогда $I_1 + I_2$, $I_1 I_2$, $I_1 \cap I_2$ являются однородными идеалами в $k[x_0, x_1,\ldots,x_n]$.*

Определение 5. Пусть $I \subset k[x_0,\ldots,x_n]$ – однородный идеал. Положим $\mathbf{V}(I) = \{p \in \mathbf{P}^n(k) : \text{для } \forall\ f \in I \quad f(p) = 0\}$.

Предложение 5. *Пусть $I \subset k[x_0,\ldots,x_n]$ – однородный идеал и пусть $I = < f_1,\ldots,f_s >$, где $f_i \in k[x_0,\ldots,x_n]$, $i = \overline{1,s}$ – однородные полиномы. Тогда множество $\mathbf{V}(I)$ – проективное многообразие, причем $\mathbf{V}(I) = \mathbf{V}(f_1,\ldots,f_s)$.*

Доказательство. Пусть $p \in \mathbf{V}(I)$. Тогда для любого $f \in I$ $f(p) = 0$. Так как $f_i \in I$, $i = \overline{1,s}$, то $f_i(p) = 0$, $i = \overline{1,s}$. Следовательно, $p \in \mathbf{V}(f_1,\ldots,f_s)$, а значит, $\mathbf{V}(I) \subset \mathbf{V}(f_1,\ldots,f_s)$.

Пусть теперь $p \in \mathbf{V}(f_1,\ldots,f_s)$. Тогда $f_i(p) = 0$, $i = \overline{1,s}$. Возьмем любой элемент $f \in I$. Имеем $f = \sum_{j=1}^{s} A_j f_j$, где $A_j \in k[x_0,\ldots,x_n]$. Следовательно, $f(p) = 0$, т.е. $p \in \mathbf{V}(I)$. □

Предложение 6. *Пусть $V \subset \mathbf{P}^n(k)$ – проективное многообразие. Положим $\mathbf{I}(V) = \{f \in k[x_0,\ldots,x_n] : \forall\ (a_0,\ldots,a_n) \in V\ f(a_0,\ldots,a_n) = 0\}$ (это означает, что f обращается в нуль на всех наборах однородных координат всех точек из V). Тогда, если k бесконечно, то $\mathbf{I}(V)$ является однородным идеалом в $k[x_0,\ldots,x_n]$.*

Доказательство. Множество $\mathbf{I}(V)$ является идеалом, так как оно замкнуто относительно сложения и относительно умножения на элементы из кольца $k[x_0,\ldots,x_n]$. Пусть теперь $f \in \mathbf{I}(V)$. Возьмем любую фиксированную точку $p \in V$. По условию f обращается в нуль на всех наборах $(a_0,\ldots,a_n)$ однородных координат точки p. Так как поле k бесконечно, то на основании леммы 1 заключаем, что все однородные компоненты f_i по-

линома f равны нулю в $(a_0,\ldots,a_n)$. Следовательно, $f_i \in \mathbf{I}(V)$, т.е. идеал $\mathbf{I}(V)$ является однородным. □

Теорема 2. *Пусть поле k бесконечно. Тогда отображения*

$$\textit{проективные многообразия} \xrightarrow{\mathbf{I}} \textit{однородные идеалы}$$

и

$$\textit{однородные идеалы} \xrightarrow{\mathbf{V}} \textit{проективные многообразия}$$

обращают включение. При этом для любого проективного многообразия $\mathbf{V}(\mathbf{I}(V)) = V$, *т.е. отображение I инъективно.*

Доказательство аналогично доказательству соответствующего аффинного случая.

Определение 6. Многообразие $V \subset \mathbf{P}^n(k)$ называется *неприводимым*, если оно не может быть представлено в виде объединения двух строго меньших проективных многообразий.

Теорема 3. *Пусть k – произвольное поле.*

1) Рассмотрим убывающую цепь проективных многообразий в $\mathbf{P}^n(k)$ $V_1 \supset V_2 \supset V_3 \supset \ldots$. *Тогда существует* $N \in \mathbf{N}$ *такое, что* $V_N = V_{N+1} = \ldots$.

2) Каждое проективное многообразие $V \subset \mathbf{P}^n(k)$ *может быть единственным образом представлено в виде объединения неприводимых проективных многообразий:* $V = V_1 \cup \ldots \cup V_m$, *где* $V_i \not\subset V_j$ *при* $i \neq j$.

Доказательство аналогично соответствующему аффинному случаю.

Радикал однородного идеала I определяется обычным образом: $\sqrt{I} = \{f \in k[x_0,\ldots,x_n] : \exists\, m \in \mathbf{N}$ такое, что $f^m \in I\}$.

Предложение 7. *Пусть* $I \subset k[x_0,\ldots,x_n]$ *– однородный идеал. Тогда радикал* $\sqrt{I}$ *также является однородным идеалом.*

Доказательство. Пусть $f \in \sqrt{I}$. Тогда $\exists\, m \in \mathbf{N}$ такое, что $f^m \in I$. Представим f в виде суммы однородных компонент: $f = \sum_i f_i = f_{\max} + \sum_{i<\max} f_i$, где $f_{\max}$ – это ненулевая однородная компонента полинома f максимальной полной степени. Имеем $(f^m)_{\max} = (f_{\max})^m$. Так как идеал I является однородным, то $(f^m)_{\max} \in I$. Следовательно, $(f_{\max})^m \in I$, т.е. $f_{\max} \in \sqrt{I}$. Положим теперь $g = f - f_{\max}$. Тогда $g \in \sqrt{I}$. Отсюда $g_{\max} \in \sqrt{I}$, при этом $g_{\max}$ представляет одну из компонент полинома f. Повторяя это рассуждение, мы в конце концов докажем, что все однородные компоненты по-

линома f принадлежат $\sqrt{I}$. Таким образом, радикал $\sqrt{I}$ является однородным идеалом. □

Лемма 2. *Пусть* $I \subset k[x_1,\ldots,x_n]$ *– идеал и пусть* $I \subset \sqrt{J}$. *Тогда существует* $m \in \mathbf{N}$ *такое, что* $I^m \subset J$.

Доказательство. На основании теоремы Гильберта о базисе $I = < f_1,\ldots,f_s >$, где $f_i \in k[x_1,\ldots,x_n]$. Так как для любого i, $i = \overline{1,s}$, $f_i \in \sqrt{J}$, то существует $n_i \in \mathbf{N}$ такое, что $f_i^{n_i} \in J$. Положим $n = \max\{n_1,\ldots,n_s\}$. Тогда для любого i, $i = \overline{1,s}$, $f_i^n \in J$. Покажем, что $I^{ns} \subset J$. Возьмем любой элемент $f \in I^{ns}$. На основании определения умножения идеалов имеем $f = \sum_{\alpha} a_\alpha f_1^{\alpha_1}\ldots f_s^{\alpha_s}$, где $a_\alpha \in k[x_1,\ldots,x_n]$, $\alpha_1 + \ldots + \alpha_s = ns$. Следовательно, существует j, $1 \le j \le s$, такое, что $\alpha_j \ge n$, т.е. $f_j^{\alpha_j} \in J$. Отсюда для любого α $a_\alpha f_1^{\alpha_1}\ldots f_s^{\alpha_s} \in J$, т.е. $f \in J$. Таким образом, существует $m = ns$ такое, что $I^{ns} \subset J$. □

Теорема 4 (проективная слабая теорема о нулях). *Пусть поле* k *алгебраически замкнуто и* $I \subset k[x_0,\ldots,x_n]$ *– однородный идеал. Следующие условия эквивалентны:*

1) многообразие $\mathbf{V}(I) \subset \mathbf{P}^n(k)$ *пусто;*

2) если G *– редуцированный базис Грёбнера идеала* I *(по отношению к некоторому мономиальному упорядочению), то для любого* i, $i = \overline{0,n}$, *существует полином* $g \in G$ *такой, что* $LT(g)$ *является неотрицательной степенью полинома* x_i;

3) для любого i, $i = \overline{0,n}$, *существует* $m_i \in \mathbf{Z}_{\ge 0}$ *такое, что* $x_i^{m_i} \in I$;

4) существует $r \in \mathbf{N}$ *такое, что* $< x_0,\ldots,x_n >^r \subset I$.

Доказательство. Во избежание путаницы для аффинного случая будем использовать обозначения $\mathbf{V}_a$, $\mathbf{I}_a$. Для заданного идеала I образуем проективное многообразие $V = V(I) \subset \mathbf{P}^n(k)$, а также аффинное многообразие $C_V = \mathbf{V}_a(I) \subset k^{n+1}$. Заметим, что если $I = < f_1,\ldots,f_s >$, где $f_i \in k[x_0,\ldots,x_n]$, то $C_V = < f_1,\ldots,f_s > \subset k^{n+1}$. При этом решения системы $f_i = 0$, $i = \overline{1,s}$, ищутся в аффинном пространстве k^{n+1}. Будем называть C_V *аффинным конусом* над V. Заметим, что C_V содержит все наборы однородных компонент точек из V.

Докажем, что 2) $\Rightarrow$ 1). По условию для любого i, $i = \overline{0,n}$ базис Грёбнера G идеала I содержит элемент g такой, что $\mathrm{LT}(g) = x_i^{m_i}$, где $m_i \in \mathbf{Z}_{\ge 0}$. Из теории факторколец следует, что множество C_V конечно. Если $p \in V$,

то все однородные координаты точки p принадлежат C_V. Таким образом, если $p = (a_0,\ldots,a_n)$, то при $\lambda \neq 0$, $\lambda \in k$ $\lambda(a_0,\ldots,a_n) \in C_V$. Поле k алгебраически замкнуто, а значит, и бесконечно. Получили противоречие. Следовательно, $V = \mathbf{V}(I) = \emptyset$.

Покажем теперь, что 3) $\Rightarrow$ 2). Пусть G – редуцированный базис Грёбнера идеала I. Так как для любого i, $i = \overline{0,n}$, $x_i^{m_i} \in I$, то существует $g \in G$ такой, что LT(g) делит $x_i^{m_i}$, т.е. LT(g) является степенью переменной x_i.

Покажем, что 4) $\Rightarrow$ 3). Так как $< x_0,\ldots,x_n >^r \subset I$, то для любого i, $i = \overline{0,n}$, $x_i^r \in I$, а тогда многообразие $V(I) \subset \mathbf{P}^n(k)$ задается уравнениями $x_0 = \ldots = x_n = 0$. Единственным решением этой системы является $(0,\ldots,0)$. Так как точки с такими координатами в $\mathbf{P}^n(k)$ нет, то $V = \mathbf{V}(I) = \emptyset$.

Осталось доказать, что 1) $\Rightarrow$ 4). Из условия $V = \emptyset$ следует, что $C_V = \{(0,\ldots,0)\} \subset k^{n+1}$, ибо в противном случае существует ненулевая точка $(a_0,\ldots,a_n) \in C_V$, т.е. точка $p \in \mathbf{P}^n(k)$ с однородными координатами $a_0,\ldots,a_n$ принадлежит V, а это невозможно. Таким образом, $\mathbf{I}_a(\{(0,\ldots,0)\}) \subset \mathbf{I}_a(C_V)$.

Так как $I_a(\{(0,\ldots,0)\}) = < x_0,\ldots,x_n >$, а поле k алгебраически замкнуто, то на основании аффинной сильной теоремы о нулях $\mathbf{I}_a(C_V) = \mathbf{I}_a(\mathbf{V}_a(I)) = \sqrt{I}$. Следовательно, $< x_0,\ldots,x_n > \subset \sqrt{I}$. Из леммы 2 заключаем, что существует $r \in \mathbf{N}$ такое, что $< x_0,\ldots,x_n >^r \subset I$. □

Теорема 5 (проективная сильная теорема о нулях). *Пусть поле k алгебраически замкнуто и I – однородный идеал в $k[x_0,\ldots,x_n]$. Если многообразие $V = \mathbf{V}(I)$ непусто, то* $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.

Доказательство. Будем одновременно рассматривать два многообразия: проективное многообразие $V = \mathbf{V}(I) \subset \mathbf{P}^n(k)$ и аффинное многообразие $C_V = \mathbf{V}_a(I) \subset k^{n+1}$. Покажем, что $\mathbf{I}_a(C_V) = \mathbf{I}(V)$, если $V \neq \emptyset$. Пусть $f \in \mathbf{I}_a(C_V)$. Если $p \in V$, то все наборы однородных координат точки p принадлежат C_V. Следовательно, $f \in \mathbf{I}(V)$, а значит, $\mathbf{I}_a(C_V) \subset \mathbf{I}(V)$. Пусть теперь $f \in \mathbf{I}(V)$. Полином f равен нулю на $C_V - \{0\}$, так как координаты любой ненулевой точки из C_V являются однородными координатами некоторой точки проективного многообразия V. Однородные компоненты f_i полинома f принадлежат $\mathbf{I}(V)$, ибо $\mathbf{I}(V)$ – однородный идеал. В частности, постоянный член f_0 однородной компоненты полной степени 0 принадлежит $\mathbf{I}(V)$. Так как $V \neq \emptyset$, то $f_0 = 0$. Следовательно, f равен нулю в начале координат, а значит, $f \in \mathbf{I}_a(C_V)$. Отсюда $\mathbf{I}_a(C_V) = \mathbf{I}(V)$. Из аффинной сильной теоремы о нулях $\sqrt{I} = \mathbf{I}_a(\mathbf{V}_a(I))$. Тогда $\sqrt{I} = \mathbf{I}_a(\mathbf{V}_a(I)) = \mathbf{I}_a(C_V) = \mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I))$. □

Существует взаимно однозначное соответствие между проективными многообразиями и радикальными однородными идеалами, при условии, что идеалы $\sqrt{I} = < x_0,\ldots,x_n >$ и $\sqrt{I} = < 1 >$ исключаются из рассмотрения.

Теорема 6. *Пусть поле k алгебраически замкнуто, и рассматриваются непустые проективные многообразия и однородные радикальные идеалы, строго содержащиеся в* $< x_0,\ldots,x_n >$. *Тогда отображения*

$$\left\{\begin{matrix}\text{непустые}\\ \text{проективные}\\ \text{многообразия}\end{matrix}\right\} \xrightarrow{\mathbf{I}} \left\{\begin{matrix}\text{радикальные однородные идеалы,}\\ \text{строго содержащиеся в} < x_0,\ldots,x_n >\end{matrix}\right\}$$

и

$$\left\{\begin{matrix}\text{радикальные однородные идеалы,}\\ \text{строго содержащиеся в} < x_0,\ldots,x_n >\end{matrix}\right\} \xrightarrow{\mathbf{V}} \left\{\begin{matrix}\text{непустые}\\ \text{проективные}\\ \text{многообразия}\end{matrix}\right\}$$

взаимно обратны и являются биекциями, обращающими включение.

Доказательство. Если I – радикальный однородный идеал и $\mathbf{V}(I) = \emptyset$, то на основании теоремы 4 для любого i, $i = \overline{0,n}$, $x_i \in I$. В этом случае $I = < x_0,\ldots,x_n >$, если $1 \notin I$ и $I = < 1 > = k[x_0,\ldots,x_n]$, если $1 \in I$. Если I – радикальный однородный идеал и $I \neq k[x_0,\ldots,x_n]$, то на основании алгоритма деления для любого $f \in I$ $f = \sum_{j=0}^{n} A_j x_j$, где $A_j \in k[x_0,\ldots,x_n]$. Отсюда $I \subset < x_0,\ldots,x_n >$. Из приведенных выше рассуждений следует, что если I – радикальный однородный идеал и $\mathbf{V}(I) \neq \emptyset$, то $I \underset{\neq}{\subset} < x_0,\ldots,x_n >$. Теперь из теоремы 5 имеем $\mathbf{I}(\mathbf{V}(I)) = I$ и $\mathbf{V}(\mathbf{I}(V)) = V$. □

5.2. ПРОЕКТИВНОЕ ЗАМЫКАНИЕ АФФИННОГО МНОГООБРАЗИЯ

Так как любое многообразие может рассматриваться как аффинная часть некоторого проективного многообразия, то было бы желательно найти наименьшее проективное многообразие, содержащее данное аффинное. Пусть $x_0, x_1,\ldots,x_n$ – однородные координаты на $\mathbf{P}^n(k)$. Рассмотрим подмножество $U_0 \subset \mathbf{P}^n(k)$, определенное условием $x_0 \neq 0$. Отождествим

U_0 с k^n и будем считать $x_1,\ldots,x_n$ координатами на k^n. Для аффинных вариантов отображений **I**, **V** будем использовать обозначения $\mathbf{I}_a$, $\mathbf{V}_a$.

Определение 1. Пусть идеал $I \subset k[x_1,\ldots,x_n]$. *Гомогенизацией идеала* I называется идеал $I^h = < f^h : f \in I > \subset k[x_0, x_1,\ldots,x_n]$, где f^h – гомогенизация полинома f.

Предложение 1. *Для любого идеала $I \subset k[x_1,\ldots,x_n]$ гомогенизация I^h является однородным идеалом в $k[x_0, x_1,\ldots,x_n]$.*

Доказательство. Пусть $g \in I^h$. Тогда $g = \sum_{\alpha} A_\alpha f_\alpha^h$. Представляя A_α в виде суммы однородных компонент и собирая вместе члены одинаковой полной степени, получаем, что однородные компоненты полинома g принадлежат I^h. □

Определение 2. Мономиальное упорядочение $>$ кольца $k[x_1,\ldots,x_n]$ называется *градуированным*, если для $|\alpha| > |\beta| \quad x^\alpha > x^\beta$.

Заметим, что grlex и grevlex – градуированные мономиальные упорядочения.

Определение 3. Пусть задано градуированное мономиальное упорядочение $>$ на $k[x_1,\ldots,x_n]$. Мономиальное упорядочение $>_h$ на $k[x_0, x_1,\ldots,x_n]$ называется *продолжением градуированного мономиального упорядочения* $>$ на $k[x_1,\ldots,x_n]$, если $x^\alpha x_0^{\,d} >_h x^\beta x_0^{\,e} \Leftrightarrow x^\alpha > x^\beta$ или $x^\alpha = x^\beta$ и $d > e$.

Докажем корректность этого определения, т.е. покажем, что отношение $>_h$ является мономиальным упорядочением в $k[x_0, x_1,\ldots,x_n]$. Действительно, любой моном в $k[x_0, x_1,\ldots,x_n]$ может быть записан в виде $x_1^{\alpha_1}\ldots x_n^{\alpha_n} x_0^{\,d} = x^\alpha x_0^{\,d}$, где x^α не делится на x_0. Поэтому из определения $>_h$ в $k[x_0, x_1,\ldots,x_n]$ и линейности отношения $>$ в $k[x_1,\ldots,x_n]$ следует линейность $>_h$ в $k[x_0,\ldots,x_n]$. Пусть $x^\alpha x_0^{\,d} >_h x^\beta x_0^{\,e}$. Тогда для любого $x^\gamma x_0^{\,i} \quad x^{\alpha+\gamma} x_0^{\,d+i} >_h x^{\beta+\gamma} x_0^{\,e+i}$, ибо в случае $x^\alpha > x^\beta$ будет $x^{\alpha+\gamma} > x^{\beta+\gamma}$, в случае же $x^\alpha = x^\beta$ $d > e$, а значит, $d + i > e + i$, т.е. в обоих случаях по определению $>_h$ $x^{\alpha+\gamma} x_0^{\,d+i} >_h x^{\beta+\gamma} x_0^{\,e+i}$. Так как отношение $>$ в $k[x_1,\ldots,x_n]$ является вполне упорядочением, то для любого $x^\alpha \quad x^\alpha \geq x^0$, т.е. $x^\alpha \geq 1$. Тогда для любого $d \geq 0 \quad x_0^{\,d} x^\alpha \geq x_0^{\,d} \geq 1$. Итак, корректность определения 2 доказана.

Лемма 1. *Пусть $f \in k[x_1,\ldots,x_n]$ и отношение $>$ – градуированное мономиальное упорядочение в $k[x_1,\ldots,x_n]$. Тогда $LM_{>h}(f^h) = LM_>(f)$.*

Доказательство. Так как отношение $>$ – градуированное мономиальное упорядочение, то $\mathrm{LM}_>(f)$ представляет один из мономов x^α, содержащихся в однородной компоненте полинома f максимальной полной степени. При гомогенизации этот член не меняется. Если $x^\beta x_0^{\,e}$ – один из

мономов в f^h, то $\alpha > \beta$, ибо $|\alpha| > |\beta|$. Из определения $>_h$ следует, что $x^\alpha >_h x^\beta x_0^e$. Следовательно, $x^\alpha = \mathrm{LM}_{>h}(f^h)$. □

Теорема 1. *Пусть идеал $I \subset k[x_1,\ldots,x_n]$ и $G = \{g_1,\ldots,g_s\}$ – базис Грёбнера идеала I относительно градуированного мономиального упорядочения $>$ в $k[x_1,\ldots,x_n]$. Тогда $G^h = \{g_1^h,\ldots,g_s^h\}$ является базисом Грёбнера идеала $I^h \subset k[x_0, x_1,\ldots,x_n]$ относительно мономиального упорядочения $>_h$ в $k[x_0, x_1,\ldots,x_n]$.*

Доказательство. Возьмем любой элемент $g_i^h \in G^h$. На основании определения I^h $g_i^h \in I^h$. Покажем, что $\mathrm{LT}_{>h}(G^h)$ порождает идеал старших членов $< \mathrm{LT}_{>h}(I^h) >$. Возьмем любой $F \in I^h$. Так как I^h – однородный идеал, то каждая однородная компонента полинома F принадлежит I^h. Таким образом, полином F можно считать однородным. В этом случае

$$F = \sum_j A_j f_j^h , \qquad (1)$$

где $A_j \in k[x_0, x_1,\ldots,x_n]$, $f_j \in I$. Так как F – однородный полином, то $f = F(1, x_1,\ldots,x_n)$ – дегомогенизация полинома f. Полагая в (1) $x_0 = 1$, имеем $f = F(1, x_1,\ldots,x_n) = \sum_j A_j(1, x_1,\ldots, x_n) f_j^h(1, x_1,\ldots, x_n) = \sum_j A_j(1, x_1,\ldots, x_n) f_j$, так как $f_j^h(1, x_1,\ldots,x_n) = f_j(1, x_1,\ldots,x_n)$. Отсюда $f \in I \subset k[x_1,\ldots,x_n]$. При этом существует $e \geq 0$ такое, что $F = x_0^e f^h$. На основании леммы 1

$$\mathrm{LM}_{>h}(F) = x_0^e \mathrm{LM}_{>h}(f^h) = x_0^e \mathrm{LM}_{>}(f). \qquad (2)$$

Так как G – базис Грёбнера идеала I, то $\mathrm{LM}_{>}(f)$ делится на некоторый старший моном $\mathrm{LM}_{>}(g_i) = \mathrm{LM}_{>h}(g_i^h)$. Из равенства (2) следует, что $\mathrm{LM}_{>}(F)$ делится на $\mathrm{LM}_{>h}(f)$, а значит, и на $\mathrm{LM}_{>h}(g_i^h)$. Следовательно, G^h – базис Грёбнера идеала I^h. □

Определение 3. Пусть аффинное многообразие $W \subset k^n$, где k^n отождествляется с подмножеством U_0 проективного пространства $\mathbf{P}^n(k)$. *Проективным замыканием* аффинного многообразия W называется проективное многообразие $\overline{W} = \mathbf{V}(\mathbf{I}_a(W)^h) \subset \mathbf{P}^n(k)$, где $\mathbf{I}_a(W)^h \subset k[x_0, x_1,\ldots,x_n]$ – гомогенизация идеала $\mathbf{I}_a(W) \subset k[x_1,\ldots,x_n]$.

Теорема 2. *Пусть $W \subset k^n$, а $\overline{W} \subset \mathbf{P}^n(k)$ – проективное замыкание W. Тогда:*

*1) $\overline{W}$ **I** $U_0 = \overline{W}$ **I** $k^n = W$;*

2) $\overline{W}$ является наименьшим проективным многообразием в $\mathbf{P}^n(k)$, содержащим W;

3) если W неприводимо, то $\overline{W}$ *также неприводимо;*

4) $\overline{W}$ *не имеет неприводимых компонент, принадлежащих бесконечно удаленной гиперплоскости* $\mathbf{V}(x_0) \subset \mathbf{P}^n(k)$.

Доказательство. 1) Пусть G – базис Грёбнера идеала $\mathbf{I}_a(W)$ относительно градуированного мономиального упорядочения в $k[x_1,\ldots,x_n]$. Тогда на основании теоремы 1 $I_a(W)^h = < g^h : g \in G >$. Заметим, что, положив $x_0 = 1$, мы отождествляем k^n с подмножеством $U_0 \subset \mathbf{P}^n(k)$. Значит, $\overline{W}$ **I** $U_0 = \mathbf{V}(g^h : g \in G)$ **I** $U_0 = V_a(g^h(1, x_1,\ldots,x_n) : g \in G)$. Так как $g^h(1, x_1,\ldots,x_n) = g$, то $\overline{W}$ **I** $U_0 = \mathbf{V}_a(g : g \in G)$, т.е. $\overline{W}$ **I** $U_0 = W$.

2) Пусть V – некоторое проективное многообразие, содержащее W. Покажем, что $\overline{W} \subset V$. Пусть $V = \mathbf{V}(F_1,\ldots,F_s)$. Полином F_i равен нулю на V, а тогда дегомогенизация F_i – полином $f_i = F_i(1, x_1,\ldots,x_n)$ обращается в нуль на W, т.е. $f_i \in \mathbf{I}_a(W)$ и $f_i^h \in \mathbf{I}_a(W)^h$. Так как f_i – дегомогенизация F_i, то существует e_i такое, что $F_i = x_0^{e_i} f_i^h$. Следовательно, F_i обращается в нуль на $\overline{W}$. Отсюда $\overline{W} \subset V$.

3) Предположим вопреки утверждению, что $\overline{W}$ не является неприводимым. Тогда $\overline{W} = V_1$ **U** V_2, где $V_1 \neq \overline{W}$, $V_2 \neq \overline{W}$ – проективные многообразия. Следовательно, $W = \overline{W}$ **I** $U_0 = (V_1$ **U** $V_2)$ **I** $U_0 = (V_1$ **I** $U_0)$ **U** $(V_2$ **I** $U_0)$. Покажем, что V_1 **I** $U_0 \neq W$. Действительно, если V_1 **I** $U_0 = W$, то из минимальности проективного замыкания следует, что $V_1 = \overline{W}$. Значит, V_1 **I** $U_0 \neq W$. Аналогично, V_2 **I** $U_0 \neq W$. Отсюда следует, что W не является неприводимым многообразием, что противоречит предположению.

4) Пусть $\overline{W} = V_1$ **U** … **U** V_m – разложение многообразия $\overline{W}$ в объединение неприводимых компонент, и пусть, например, компонента V_1 содержится в бесконечно удаленной гиперплоскости $\mathbf{V}(x_0)$. Тогда $W = \overline{W}$ **I** $U_0 = (V_1$ **U** … **U** $V_m)$ **I** $U_0 = (V_1$ **I** $U_0)$ **U** $((V_2$ **U** … **U** $V_m)$ **I** $U_0) = (V_2$ **U** … **U** $V_m)$ **I** U_0, ибо V_1 **I** $U_0 = \varnothing$. Значит, V_2 **U** … **U** V_m является проективным многообразием, содержащим W. Из минимальности многообразия $\overline{W}$ следует, что $\overline{W} = V_2$ **U** … **U** V_m. Тогда $V_1 \subset (V_2$ **U** … **U** $V_m)$, что невозможно, так как V_k – различные неприводимые компоненты многообразия $\overline{W}$. □

Лемма 2. *Пусть* $f, g \in k[x_1,\ldots,x_n]$. *Тогда* $(fg)^h = f^h g^h$.

Доказательство. Пусть f, g – полиномы соответственно полной степени d_1, d_2. Тогда $(fg)^h = x_0^{d_1+d_2} f\left(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}\right) \cdot g\left(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}\right) = f^h g^h$. □

Теорема 3. *Пусть поле k алгебраически замкнуто и $I \subset k[x_1,\ldots,x_n]$ – некоторый идеал. Тогда $\mathbf{V}(I^h) \subset \mathbf{P}^n(k)$ является проективным замыканием многообразия $\mathbf{V}_a(I) \subset k^n$, т.е. $\overline{\mathbf{V}_a(I)} = \mathbf{V}(I^h)$.*

Доказательство. Пусть $W = \mathbf{V}_a(I) \subset k^n$, а $Z = \mathbf{V}(I^h) \subset \mathbf{P}^n(k)$. Тогда $Z \supset W$. Покажем, что Z является наименьшим проективным многообразием, содержащим W. Пусть $V = \mathbf{V}(F_1,\ldots,F_s)$ – проективное многообразие, содержащее W. Тогда дегомогенизация $f_i = F_i(1, x_1,\ldots,x_n)$ принадлежит $\mathbf{I}_a(W)$. Так как k алгебраически замкнуто, то из теоремы о нулях $\mathbf{I}_a(W) = \sqrt{I}$. Следовательно, существует $m \in \mathbf{N}$ такое, что $f_i^m \in I$. Отсюда $(f_i^m)^h \in I^h$, а значит, $(f_i^m)^h$ обращается в нуль на Z. Из леммы 2 следует, что $(f_i^m)^h = (f_i^h)^m$, а поэтому f_i^h равен нулю на Z. Так как $F_i = x_0^{e_i} f_i^h$, то и F_i обращается в нуль на Z. Следовательно, $Z \subset V$, т.е. Z – наименьшее проективное многообразие, содержащее W. Отсюда $Z = \overline{W}$. □

Из теорем 1,3 вытекает следующий *алгоритм вычисления проективного замыкания аффинного многообразия* над алгебраически замкнутым полем k: если $W = \mathbf{V}(f_1,\ldots,f_s) \subset k^n$, то нужно вычислить базис Грёбнера G идеала $< f_1,\ldots,f_s >$ по отношению к какому-либо градуированному упорядочению, тогда проективное замыкание многообразия W в $\mathbf{P}^n(k)$ – множество нулей однородных полиномов g^h для $g \in G$.

5.3. ПРОЕКТИВНАЯ ТЕОРИЯ ИСКЛЮЧЕНИЯ

Пусть дана система уравнений $f_1(x_1,\ldots,x_n, y_1,\ldots,y_m) = 0,\ldots,f_s(x_1,\ldots,x_n, y_1,\ldots,y_m) = 0$, где $f_i \in k[x_1,\ldots,x_n, y_1,\ldots,y_m]$, $i = \overline{1,s}$. Эти уравнения задают многообразие $V = \mathbf{V}(f_1,\ldots,f_s) \subset k^n \times k^m$. Исключению переменных $x_1,\ldots,x_n$ соответствует образ $\pi(V)$, где $\pi : k^n \times k^m \to k^m$ – отображение проекции на последние m координат. С другой стороны исключение переменных $x_1,\ldots,x_n$ состоит в вычислении исключающего идеала $I_n = < f_1,\ldots,f_s > \mathbf{I} k[y_1,\ldots,y_m]$. Опишем связь между $\pi(V)$ и $\mathbf{V}(I_n)$. Для этого первый сомножитель в $\pi : k^n \times k^m \to k^m$ будем делать проективным, т.е. вместо k^n будем рассматривать $\mathbf{P}^n(k)$. Будем писать P^n вместо $\mathbf{P}^n(k)$, если ясно, о каком поле идет речь. Точка из $\mathbf{P}^n \times k^m$ имеет координаты $(x_0, \ldots,x_n, y_1,\ldots,y_m)$, где $(x_0,\ldots,x_n)$ – однородные координаты в P^n, а $(y_1,\ldots,y_m)$ – обычные координаты в k^m. Чтобы отождествить $k^n \times k^m$ с тем подмножеством в $\mathbf{P}^n \times k^m$, где $x_0 \neq 0$, будем использовать отображение $(x_1,\ldots,x_n, y_1,\ldots,y_m) \to (1, x_1,\ldots,x_n, y_1,\ldots,y_m)$.

Определение 1. Пусть k – произвольное поле.

1) Полином $F \in k[x_0,\ldots,x_n, y_1,\ldots,y_m]$ называется *$(x_0,\ldots,x_n)$-однородным*, если существует такое целое $l \geq 0$, что $F = \sum_{|\alpha|=l} h_\alpha(y_1,\ldots,y_m)x^\alpha$, где x^α – моном от $x_0,\ldots,x_n$ мультистепени α, а $h_\alpha \in k[y_1,\ldots,y_m]$.

2) *Многообразием* $\mathbf{V}(F_1,\ldots,F_s) \subset k^n \times k^m$, *определенным $(x_0,\ldots,x_n)$-однородными полиномами* $F_1,\ldots,F_s \in k[x_0,\ldots,x_n, y_1,\ldots,y_m]$, называется множество $\{(a_0,\ldots,a_n, b_1,\ldots,b_m)\} \in \mathbf{P}^n \times k^m$: $F_i(a_0,\ldots,a_n, b_1,\ldots,b_m) = 0 \ \forall\ i, i = \overline{1,s}\}$.

Предложение 1. *Многообразие $\mathbf{V}(F_1,\ldots,F_s)$ – корректно определенное подмножество в $\mathbf{P}^n \times k^m$, если полиномы F_i, $i = \overline{1,s}$ являются $(x_0,\ldots,x_n)$-однородными, т.е. если F_i обращаются в нуль на одном наборе координат некоторой точки из $\mathbf{P}^n \times k^m$, то F_i обращаются в нуль на всех координатах этой точки.*

Доказательство. Пусть $F_i = \sum_{|\alpha_i|=l_i} h_{\alpha_i}(y_1,\ldots,y_m)x^{\alpha_i}$, $i = \overline{1,s}$, где x^{α_i} – мономы от $x_0,\ldots,x_n$ мультистепени α_i, а $h_{\alpha_i} \in k[y_1,\ldots,y_m]$. Если $F_i(a_0,\ldots,a_n, b_1,\ldots,b_m) = 0$, то $F_i(\lambda a_0,\ldots,\lambda a_n, b_1,\ldots,b_m) = \lambda^{l_i} F_i(a_0,\ldots,a_n, b_1,\ldots,b_m) = 0$. □

Определение 2. Пусть $I \subset k[x_0,\ldots,x_n, y_1,\ldots,y_m]$ – идеал, порожденный $(x_0,\ldots,x_n)$-однородными полиномами. *Проективным исключающим идеалом* идеала I называется множество $\tilde{I} = \{f \in k[y_1,\ldots,y_m] : \forall\ i, i = \overline{0,n}\ \exists\ e_i \geq 0$ такое, что $x_i^{e_i} f \in I\}$.

Предложение 2. *Множество $\tilde{I}$ из определения 2 является идеалом в $k[y_1,\ldots,y_m]$.*

Доказательство. Так как для любого i, $i = \overline{0,n}$, $x_i^{e_i} 0 = 0 \in I$, то $0 \in \tilde{I}$. Пусть $f, g \in \tilde{I}$. Тогда $\forall\ i, i = \overline{0,n}\ \exists\ e_i \geq 0, d_i \geq 0$ такое, что $x_i^{e_i} f \in I$, $x_i^{d_i} g \in I$. Пусть для определенности $d_i \geq e_i$. Тогда $x_i^{d_i - e_i} x_i^{e_i} f = x_i^{d_i} f \in I$, а значит, $x_i^{d_i} f + x_i^{d_i} g = x_i^{d_i}(f + g) \in I$. Следовательно, $f + g \in \tilde{I}$. Если $f \in \tilde{I}$, то для любого i, $i = \overline{0,n}$, существует $e_i \geq 0$ такое, что $x_i^{e_i} f \in I$. Тогда для любого $h \in k[y_1,\ldots,y_m]$ $x_i^{e_i} fh \in I$, т.е. $fh \in \tilde{I}$. □

Предложение 3. *Пусть $V = \mathbf{V}(F_1,\ldots,F_s) \subset \mathbf{P}^n \times k^m$ – многообразие, определенное $(x_0,\ldots,x_n)$-однородными полиномами. Рассмотрим отображение проекции $\pi : \mathbf{P}^n \times k^m \to k^m$. Тогда $\pi(V) \subset \mathbf{V}(\tilde{I})$, где $\tilde{I}$ – проективный исключающий идеал идеала $I = \langle F_1,\ldots,F_s \rangle$.*

Доказательство. Пусть $(a_0,\ldots,a_n, b_1,\ldots,b_m) \in V$ и $f \in \mathfrak{F}$. Тогда для любого i, $i = \overline{0,n}$, существует $e_i \geq 0$ такое, что $x_i^{e_i} f(y_1,\ldots,y_m) \in I$. Значит, для любого i, $i = \overline{0,n}$, $a_i^{e_i} f(b_1,\ldots,b_m) = 0$. Так как $(a_0,\ldots,a_n)$ – набор однородных координат, то хотя бы одна компонента a_i отлична от нуля. Следовательно, $f(b_1,\ldots,b_m) = 0$. Таким образом, f обращается в нуль на $\pi(V)$. □

Теорема 1 (проективная теорема о продолжении). *Пусть поле k алгебраически замкнуто и многообразие $V = \mathbf{V}(F_1,\ldots,F_s) \subset \mathbf{P}^n \times k^m$ определено $(x_0,\ldots,x_n)$-однородными полиномами из $k[x_0,\ldots,x_n, y_1,\ldots,y_m]$. Пусть $I = \langle F_1,\ldots,F_s \rangle$, а $\mathfrak{F} \subset k[y_1,\ldots,y_m]$ – его проективный исключающий идеал. Если $\pi : \mathbf{P}^n \times k^m \to k^m$ – отображение проекции на последние m координат, то $\pi(V) = \mathbf{V}(\mathfrak{F})$.*

Доказательство. Включение $\pi(V) \subset \mathbf{V}(\mathfrak{F})$ доказано в предложении 3. Докажем обратное включение. Пусть $c = (c_1,\ldots,c_m) \in \mathbf{V}(\mathfrak{F})$. Положим $F_i(x_0,\ldots,x_n, c) = F_i(x_0,\ldots,x_n, c_1,\ldots,c_m)$, $i = \overline{1,s}$; F_i – однородный полином от переменных $x_0,\ldots,x_n$ полной степени d_i (его полная степень равна полной степени полинома $F_i(x_0,\ldots,x_n, y_1,\ldots,y_m)$ по переменным $x_0,\ldots,x_n$). Если $c \notin \pi(V)$, то уравнения $F_1(x_0,\ldots,x_n, c) = \ldots = F_s(x_0,\ldots,x_n, c) = 0$ определяют пустое многообразие в $\mathbf{P}^n$. Так как поле k алгебраически замкнуто, то из проективной слабой теоремы о нулях следует, что $\langle x_0,\ldots,x_n \rangle^r \subset \langle F_1(x_0,\ldots,x_n, c),\ldots,F_s(x_0,\ldots,x_n, c) \rangle$ для некоторого $r \geq 1$. Таким образом, мономы x^α, где $|\alpha| = r$, являются полиномиальными линейными комбинациями полиномов $F_i(x_0,\ldots,x_n, c)$, т.е. $x^\alpha = \sum_{i=1}^{s} H_i(x_0,\ldots,x_n) F_i(x_0,\ldots,x_n, c)$.

Рассматривая однородные компоненты, можно считать полиномы H_i однородными полиномами полной степени $r - d_i$. Записывая каждый полином H_i в виде линейной комбинации мономов x^{β_i}, где $|\beta_i| = r - d_i$, получаем, что линейная оболочка полиномов $x^{\beta_i} F_i(x_0,\ldots,x_n, c)$, $i = \overline{1,s}$, $|\beta_i| = r - d_i$ совпадает с линейным пространством всех однородных полиномов от переменных $x_0,\ldots,x_n$ полной степени r. Пусть размерность этого пространства равна N_r. Следовательно, можно найти N_r таких полиномов $G_j(x_0,\ldots,x_n, c)$, $j = \overline{1,N_r}$, которые образуют базис этого пространства. Полином $G_j(x_0,\ldots,x_n, c)$ возникает из полинома $G_j = G_j(x_0,\ldots,x_n, y_1,\ldots,y_m) \in k[x_0,\ldots,x_n, y_1,\ldots,y_m]$.

Для любого G_j существуют i, β_i такие, что однородный полином G_j полной степени r относительно $x_0,\ldots,x_n$ имеет вид $G_j = x^{\beta_i} F_i$. Таким образом,

$$G_j = \sum_{|\alpha|=r} a_{j\alpha}(y_1,...,y_m)x^{\alpha}. \qquad (1)$$

Так как x^{α}, где $|\alpha| = r$, образуют базис пространства всех однородных полиномов полной степени r, то их количество равно N_r. Следовательно, можно составить квадратную матрицу из полиномов $a_{j\alpha}(y_1,\ldots,y_m)$. Пусть $D(y_1,\ldots,y_m) = \det(a_{j\alpha}(y_1,\ldots,y_m)$: $1 \le j \le N_r$, $|\alpha| = r)$ – определитель этой матрицы. Подстановка c в (1) дает $C_j(x_0,\ldots,x_n, c) = \sum_{|\alpha|=r} a_{j\alpha}(c)x^{\alpha}$.

Так как полиномы $G_j(x_0,\ldots,x_n, c)$ и x^{α} образуют базисы одного и того же векторного пространства, то $D(c) \neq 0$. В частности, $D(y_1,\ldots,y_m) \neq 0$ в $k[y_1,\ldots,y_m]$. Работая над полем функций $k(y_1,\ldots,y_m)$, можно рассматривать (1) как систему линейных уравнений относительно переменных x^{α}. Из правила Крамера находим $x^{\alpha} = \dfrac{M_{\alpha}}{D(y_1,...,y_m)}$, где M_{α} – матрица, полученная из матрицы $(a_{j\alpha})$ при замене столбца, соответствующего α, столбцом $G_1,\ldots,G_{N_r}$. Умножая это равенство на $D(y_1,\ldots,y_m)$ и разлагая $\det(M_{\alpha})$ по этому столбцу, получаем равенство $x^{\alpha}D(y_1,\ldots,y_m) = \sum_{j=1}^{N_I} H_{j\alpha}(y_1,...,y_m)$ $G_j(x_0,\ldots,x_n, y_1,\ldots,y_m)$. Так как каждый полином G_j имеет вид $x^{\beta_i}F_i$, то $x^{\alpha}D(y_1,\ldots,y_m) \in \langle F_1,\ldots,F_s \rangle = I$. Значит, $D \in \sqrt{I}$, а тогда $D(c) = 0$, ибо $c \in \mathbf{V}(\sqrt{I})$. Получили противоречие. Следовательно, $c \in \pi(V)$. □

Предложение 4. *Пусть идеал $I \subset k[x_0,\ldots,x_n, y_1,\ldots,y_m]$. Тогда для достаточно большого целого e $\sqrt{I} = (I : \langle x_0^e,\ldots,x_n^e \rangle)$* **I** $k[y_1,\ldots,y_m]$.

Доказательство. Пусть $f \in I : \langle x_0^e,\ldots,x_n^e \rangle$. Тогда для любого i, $i = \overline{0,n}$, $x_i^e f \in I$. Следовательно, для любого $e \ge 0$ $(I : \langle x_0^e,\ldots,x_n^e \rangle)$ **I** $k[y_1,\ldots,y_m] \subset \sqrt{I}$. Покажем, что при достаточно большом e имеет место противоположное включение. Рассмотрим возрастающую цепь идеалов $I : \langle x_0,\ldots,x_n \rangle \subset I : \langle x_0^2,\ldots,x_n^2 \rangle \subset \ldots$. Тогда существует e такое, что $I : \langle x_0^e,\ldots,x_n^e \rangle = I : \langle x_0^{e+1},\ldots,x_n^{e+1} \rangle = \ldots$. Значит, для любого целого $d \ge 0$ $I : \langle x_0^d,\ldots,x_n^d \rangle \subset I : \langle x_0^e,\ldots,x_n^e \rangle$. Пусть $f \in \sqrt{I}$. Тогда для любого i, $i = \overline{0,n}$, существуют $e_i \ge 0$ такие, что $x_i^{e_i} f \in I$. Пусть $d = \max(e_0,\ldots,e_n)$. Для любого i, $i = \overline{0,n}$, $x_i^d f \in I$, т.е. $f \in I : \langle x_0^d,\ldots,x_n^d \rangle$. Следовательно, $f \in (I : \langle x_0^e,\ldots,x_n^e \rangle)$ **I** $k[y_1,\ldots,y_m]$. □

Определение 3. Пусть $F \in k[x_0,\ldots,x_n, y_1,\ldots,y_m]$. Фиксируем i, $0 \le i \le n$, и положим $x_i = 1$. Тогда $F^{(i)} = F(x_0,\ldots,1,\ldots,x_n, y_1,\ldots,y_m) \in k[x_0,$

$\ldots, \not{x}_i, \ldots, x_n, y_1, \ldots, y_m]$, где $\not{x}_i$ означает, что x_i исключена из списка переменных. *Дегомогенизацией идеала* $I \subset k[x_0,\ldots,x_n, y_1,\ldots,y_m]$ называется множество $I^{(i)} = \{F^{(i)} : F \in I\} \subset k[x_0,\ldots,\not{x}_i,\ldots,x_n, y_1,\ldots,y_m]$.

Предложение 5. *Пусть идеал* $I \subset k[x_0,\ldots,x_n, y_1,\ldots,y_m]$. *Тогда* $I^{(i)}$ *– идеал в* $k[x_0,\ldots,\not{x}_i,\ldots,x_n, y_1,\ldots,y_m]$. *Если* $I = < F_1,\ldots,F_s >$, *то* $I^{(i)} = < F_1^{(i)},\ldots,F_s^{(i)} >$.

Доказательство. Так как $0 \in I$, то $0 \in I^{(i)}$. Если $F^{(i)}, G^{(i)} \in I^{(i)}$, то $F, G \in I$. Тогда $F + G \in I$, а значит, $(F + G)^{(i)} = F^{(i)} + G^{(i)} \in I^{(i)}$. Если $F^{(i)} \in I^{(i)}$, то для любого $H^{(i)} \in k[x_0,\ldots,\not{x}_i,\ldots,x_n, y_1,\ldots,y_m]$ $FH \in I$. Следовательно, $(FH)^{(i)} = F^{(i)}H^{(i)} \in I^{(i)}$. Таким образом, доказано, что $I^{(i)}$ – идеал в $k[x_0,\ldots,\not{x}_i,\ldots,x_n, y_1,\ldots,y_m]$. Пусть теперь $I = < F_1,\ldots,F_s >$. Возьмем любой $F^{(i)} \in I^{(i)}$. Тогда $F \in I$, а значит, $F = \sum_{k=1}^{s} F_k H_k$, где $H_k \in k[x_0,\ldots,x_n, y_1,\ldots,y_m]$. Следовательно, $F^{(i)} = \sum_{k=1}^{s} F_k^{(i)} H_k^{(i)} \in < F_1^{(i)},\ldots,F_s^{(i)} >$. Таким образом, $I^{(i)} \subset < F_1^{(i)},\ldots,F_s^{(i)} >$. Если $F^{(i)} \in < F_1^{(i)},\ldots,F_s^{(i)} >$, то существуют $H_k^{(k)} \in k[x_0,\ldots,\not{x}_i,\ldots,x_n, y_1,\ldots,y_m]$, $k = \overline{1,s}$, такие, что $F^{(i)} = \sum_{k=1}^{s} F_k^{(i)} H_k^{(i)}$. Тогда $F = \sum_{k=1}^{s} F_k H_k \in I$, а значит, $F^{(i)} \in I^{(i)}$. Следовательно, $< F_1^{(i)},\ldots,F_s^{(i)} > \subset I^{(i)}$. □

Рассмотрим многообразие $V \subset \mathbf{P}^n \times k^m$, определенное идеалом I. Тогда идеал $I^{(i)}$ определяет аффинную часть $V \cap (U_i \times k^m)$, где $U_i \cong k^n$ – подмножество в $\mathbf{P}^n$, определенную условием $x_i \neq 0$. Для идеала $I^{(i)}$ n-й исключающий идеал $I_n^{(i)} = I^{(i)} \cap k[y_1,\ldots,y_m]$. Здесь индекс n указывает, что исключаются n переменных $x_0,\ldots,\not{x}_i,\ldots,x_n$.

Предложение 6. *Пусть идеал* $I \subset k[x_0,\ldots,x_n,y_1,\ldots,y_m]$ *порожден* $(x_0,\ldots,x_n)$*-однородными полиномами. Тогда* $\not{I} = I_n^{(0)} \cap I_n^{(1)} \cap \ldots \cap I_n^{(n)}$.

Доказательство. Так как $I_n^{(0)} \cap I_n^{(1)} \cap \ldots \cap I_n^{(n)} = I^{(0)} \cap I^{(1)} \cap \ldots \cap I^{(n)} \cap k[y_1,\ldots,y_m]$, то достаточно доказать, что $\not{I} = I^{(0)} \cap I^{(1)} \cap \ldots \cap I^{(n)} \cap k[y_1,\ldots,y_m]$.

Пусть $f \in \not{I}$. Тогда для любого i, $i = \overline{0,n}$, существует $e_i \geq 0$ такое, что $x_i^{e_i} f(y_1,\ldots,y_m) \in I$. Полагая $x_i = 1$, получаем, что для любого i, $i = \overline{0,n}$, $f(y_1,\ldots,y_m) \in I^{(i)}$, т.е. $f \in I^{(0)} \cap \ldots \cap I^{(n)} \cap k[y_1,\ldots,y_m]$. Следовательно, $\not{I} \subset I^{(0)} \cap \ldots \cap I^{(n)} \cap k[y_1,\ldots,y_m]$. Докажем теперь обратное включение. Для этого изучим сначала связь между идеалами I и $I^{(i)}$. Элемент $f \in I^{(i)}$ полу-

чается из некоторого элемента $F \in I$ с помощью подстановки $x_i = 1$. Покажем, что $F \in I$ можно выбрать $(x_0,\ldots,x_n)$-однородным. Действительно, $F = \sum_{j=0}^{d} F_j$, где F_j – $(x_0,\ldots,x_n)$-однородные полиномы полной степени j по переменным $x_0,\ldots,x_n$. Так как идеал I порожден $(x_0,\ldots,x_n)$-однородными полиномами, то $I = < H_1,\ldots,H_s >$, где H_i – $(x_0,\ldots,x_n)$-однородные полиномы. Тогда $F = \sum_{i=1}^{s} A_i H_i = \sum_{j=0}^{d} F_j$. Представляя A_i в виде суммы $(x_0,\ldots,x_n)$-однородных полиномов, получаем, что $F_j = A_{ij}H_i$, где A_{ij} – $(x_0,\ldots,x_n)$-однородные полиномы. Отсюда $F_j \in I$ для всех j, $j = \overline{1,d}$. Следовательно, $\sum_{j=0}^{d} x_i^{d-j} F_j \in I$ – $(x_0,\ldots,x_n)$-однородный полином полной степени d, причем его дегомогенизация при $x_i = 1$ равна f. Таким образом, можно считать, что $F \in I$ является $(x_0,\ldots,x_n)$-однородным полиномом. Применяя к полиному $f \in k[x_0,\ldots,x_n, y_1,\ldots,y_m]$ процедуру гомогенизации, используя при этом x_i в качестве дополнительной переменной, получаем $(x_0,\ldots,x_n)$-однородный полином $f^h \in k[x_0,\ldots,x_n, y_1,\ldots,y_m]$. Если f является дегомогенизацией $(x_0,\ldots,x_n)$-однородного полинома F, то существует $e \geq 0$ такое, что $F = x_i^e f^h$.

Пусть теперь $f \in I^{(i)}$ **I** $k[y_1,\ldots,y_m]$, где $i = \overline{0,n}$. Тогда, как показано выше, f получен дегомогенизацией $(x_0,\ldots,x_n)$-однородного полинома $F \in I$. Так как f не зависит от переменных $x_0,\ldots,x_n$, то $f^h = f$ и $x_i^e f \in I$. Отсюда следует, что для любого i $f \in I^{(i)}$, а значит, $I^{(0)}$ **I** … **I** $I^{(n)}$ **I** $k[y_1,\ldots,y_m] \subset I$. □

Предложение 6 можно интерпретировать так. Идеал $I_n^{(i)}$ исключает переменные $x_0,\ldots,x_i,\ldots,x_n$ на аффинной части пространства $\mathbf{P}^n \times k^m$ (там, где $x_i \neq 0$). Пересечение этих аффинных исключающих идеалов (которое, грубо говоря, соответствует исключению на объединении аффинных частей) и является проективным исключающим идеалом.

Предложение 6 дает следующий алгоритм для вычисления идеала I. Пусть $I = < F_1,\ldots,F_s >$. Тогда $I^{(i)} = < F_1^{(i)},\ldots,F_s^{(i)} >$, $i = \overline{0,n}$. Теперь с помощью алгоритма, вычисляющего пересечение идеалов, находим $I = I_n^{(0)}$ **I** $I_n^{(1)}$ **I** … **I** $I_n^{(n)}$.

Идеал $I \subset k[x_0,\ldots,x_n, y_1,\ldots,y_m]$ определяет многообразие $V = \mathbf{V}_a(I_n) \subset k^n \times k^m$, при этом $\pi(V) \subset \mathbf{V}(I_n)$, где $\pi : k^n \times k^m \to k^m$ – отображение проекции, а I_n – n-й исключающий идеал идеала I. В дальнейшем будет выяснена структура множества $\mathbf{V}(I_n) - \pi(V)$.

Определение 4. Пусть $f \in k[x_1,\ldots,x_n, y_1,\ldots,y_m]$ – полином полной степени d относительно $x_1,\ldots,x_n$. Запишем f в виде $f = \sum_{i=0}^{d} f_i$, где $f_i \in k[x_1, \ldots,x_n, y_1,\ldots,y_m]$ – однородный полином от переменных $x_1,\ldots,x_n$ полной степени i. Тогда $f^h(x_0, \ldots,x_n, y_1,\ldots,y_m) = \sum_{i=0}^{d} f_i(x_1,\ldots,x_n,y_1,\ldots,y_m)x_0^{d-i}$ является $(x_0,\ldots,x_n)$-однородным полиномом, который называется *$(x_0,\ldots,x_n)$-гомогенизацией полинома f.*

Предложение 7. *Пусть $f \in k[x_1,\ldots,x_n, y_1,\ldots,y_m]$ – полином полной степени d относительно $x_1,\ldots,x_n$.*

1) Имеет место формула $f^h(x_0,\ldots,x_n, y_1,\ldots,y_m) = x_0^d f(\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}, y_1,\ldots,y_m)$.

2) Дегомогенизируем полином f^h, положив $x_0 = 1$. Тогда $(f^h)^{(0)} = f$.

3) Пусть $f = F^{(0)}$ является дегомогенизацией $(x_0,\ldots,x_n)$-однородного полинома F. Тогда существует $e \geq 0$ такое, что $F = x_0^e f^h$.

Доказательство. 1) Полином f^h является однородным полиномом от переменных $x_0,\ldots,x_n$ полной степени d, так как $f_i(x_1,\ldots,x_n)x_0^{d-i}$ – однородный полином от переменных $x_0,\ldots,x_n$ полной степени d. Тогда

$$f^h(x_0,\ldots,x_n, y_1,\ldots,y_m) = \sum_{i=0}^{d} f_i(x_1,\ldots,x_n)x_0^{d-i} = \sum_{i=0}^{d} f_i\ (\frac{x_1}{x_0},\ldots,\frac{x_n}{x_0}, y_1,\ldots,y_m)x_0^i x_0^{d-i} = x_0^d f(\frac{x_1}{x_0}, \ldots,\frac{x_n}{x_0}, y_1,\ldots,y_m).$$

Так как $f^h(x_0,\ldots,x_n, y_1,\ldots,y_m) = \sum_{i=0}^{d} f_i(x_1,\ldots,x_n)x_0^{d-i}$, то $(f^h)^{(0)} = f^h(1, x_1,\ldots,x_n, y_1,\ldots,y_m) = \sum_{i=0}^{d} f_i\ (x_1,\ldots,x_n, y_1,\ldots,y_m) = f$.

3) Пусть $f = F^{(0)}$ является дегомогенизацией $(x_0,\ldots,x_n)$-однородного полинома F полной степени d, а x_0^e – наивысшая степень переменной x_0, которая делит F. Тогда $G = \frac{F}{x_0^e}$ – $(x_0,\ldots,x_n)$-однородный полином полной степени $d - e$ относительно $x_0,\ldots,x_n$. Отсюда $f = F^{(0)} = G^{(0)}$. Из п. 1 имеем f

$^h = (G^{(0)})^h = x_0^{d-e}G(1, \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}, y_1,\ldots,y_m) = x_0^{d-e}G(x_0, x_1,\ldots,x_n, y_1,\ldots,y_m)x_0^{-(d-e)}$
$= G(x_0, x_1,\ldots,x_n, y_1,\ldots,y_m)$. Следовательно, $F = x_0^e G = x_0^e f^h$. □

Определение 5. Пусть идеал $I \subset k[x_0,\ldots,x_n, y_1,\ldots,y_m]$. Тогда *$(x_0,\ldots,x_n)$-гомогенизацией идеала I* называется идеал $I^h = \langle f^h : f \in I \rangle \subset k[x_0,\ldots,x_n, y_1,\ldots,y_m]$.

Предложение 8. *Пусть идеал $I \subset k[x_0,\ldots,x_n, y_1,\ldots,y_m]$, а I^h – $(x_0,\ldots,x_n)$-гомогенизация идеала I. Тогда*

1) проективный исключающий идеал идеала I^h равен n-му исключающему идеалу идеала I, т.е. $\overline{I^h} = I_n \subset k[y_1,\ldots,y_m]$.

2) Если поле k алгебраически замкнуто, то многообразие $\overline{V} = \mathbf{V}(I^h)$ является наименьшим многообразием в $\mathbf{P}^n \times k^m$, содержащим аффинное многообразие $V = \mathbf{V}_a(I) \subset k^n \times k^m$. При этом многообразие $\overline{V}$ называется проективным замыканием многообразия V в $\mathbf{P}^n \times k^m$.

Доказательство. 1) Из предложения 7 следует, что дегомогенизация идеала I^h по переменной x_0 дает $(I^h)^{(0)} = I$. Из доказательства предложения 6 заключаем, что $\overline{I^h} \subset I_n$. Пусть $f \in I_n$. Так как $f \in k[y_1,\ldots,y_m]$, то f является $(x_0,\ldots,x_n)$-однородным полиномом. Значит, $f = f^h \in I^h$. Следовательно, для любого i $x_i^0 f \in I^h$, а поэтому $f \in \overline{I^h}$. П. 1 доказан. П. 2 доказывается аналогично доказательству теоремы 3 п. 5.2.

Следствие 1. *Пусть поле k алгебраически замкнуто, а $V = \mathbf{V}_a(I) \subset k^n \times k^m$, где идеал $I \subset k[x_1,\ldots,x_n, y_1,\ldots,y_m]$. Тогда $\mathbf{V}(I_n) = \pi(\overline{V})$, где $\overline{V} \subset \mathbf{P}^n \times k^m$ – проективное замыкание многообразия V, а $\pi : \mathbf{P}^n \times k^m \to k^m$ – отображение проекции.*

Доказательство. На основании предложения 8 $\overline{V} = \mathbf{V}(I^h)$ и $\overline{I^h} = I_n$. Теперь утверждение непосредственно следует из теоремы 1. □

Следствие 1 показывает, что точки множества $\mathbf{V}(I_n) - \pi(V)$ получаются из бесконечно удаленных точек проективного замыкания $\overline{V}$ многообразия V.

Предложение 9. *Пусть $>$ – мономиальное упорядочение в кольце $k[x_1,\ldots,x_n, y_1,\ldots,y_m]$, такое, что для всех мономов $x^\alpha y^\gamma$, $x^\beta y^\delta$ имеем $|\alpha| > |\beta| \Rightarrow x^\alpha y^\gamma > x^\beta y^\delta$. Пусть для идеала $I \subset k[x_1,\ldots,x_n, y_1,\ldots,y_m]$ $G = \{g_1,\ldots,g_s\}$ – базис Грёбнера по отношению к упорядочению $>$. Тогда $G^h = \{g_1^h,\ldots,g_s^h\}$ – базис идеала $I^h \subset k[x_0, \ldots,x_n,y_1,\ldots,y_m]$.*

Доказательство аналогично доказательству теоремы 1 п. 5.2. □

ЛИТЕРАТУРА.

1. *Кокс Д., Литтл Дж., О'Ши Д.* Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. – М.: Мир, 2000. 687 с.

2. *Adams W., Loustaunau P.* An Introduction to Gröbner Bases. Graduate Studies in Mathematics. Amer. Math. Soc. – Providence, 1994. 289 p.

3. *Becker T., Weispfenning V.* Gröbner Bases: A Computational Approach to Commutative Algebra. Springer Verlag, Berlin and New York, 1993. 512 p.

4. *Просолов В.В.* Многочлены. – МЦНМО, 2000, 336 с.

5. *Атья М., Макдональд И.* Введение в коммутативную алгебру. – М., Мир. 1972, 160 с.

6. *Рид М.* Алгебраическая геометрия для всех. – М., Мир. 1991, 152 с.

7. *Быков В.И., Кытманов А.М., Лазман М.З.* Методы исключения в компьютерной алгебре многочленов. – Новосибирск, «Наука». 1991, 232 с.

8. *Ван дер Верден Б.Л.* Алгебра. – М., Наука. 1976, 648 с.

9. *Курош А.Г.* Курс высшей алгебры. – М., Физматгиз. 1962, 432 с.

10. *Ленг С.* Алгебра. – М., Мир. 1968, 564 с.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

Р

С

Т

У

Ф

Ц

Ч

Э