МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра высшей алгебры и защиты информации

ЛАЗУКО
Серафим Александрович

ПРИМЕНЕНИЕ БАЗИСОВ ГРЁБНЕРА К РЕШЕНИЮ СИСТЕМ АЛГЕБРАИЧЕСКИХ УРАВНЕНИЙ И К РЕШЕНИЮ ЗАДАЧ ОБ ИДЕАЛАХ

Дипломная работа

Научный руководитель:
доктор физ.-мат. наук,
профессор В.В. Беняш-Кривец

Допущена к защите

«___» _____ 2020 г.

Зав. кафедрой высшей алгебры и защиты информации
доктор физ.-мат. наук, профессор В.В. Беняш-Кривец

Минск, 2020

Оглавление

Реферат

Дипломная работа содержит:
54 страницы.
3 использованных источников информации.

Ключевые слова и понятия: *Идеал, Полином, Моном, Аффинное Многообразие, Упорядочение, Алгоритм Деления, Базис Грёбнера, Алгоритм Бухбергера.*

Объектом исследования дипломной работы являются Базисы Грёбнера и их применение к решению систем алгебраических уравнений и задач об идеалах.

Целью дипломной работы является рассмотрение теоретических сведений и алгоритмов, которые позволяют применять Базисы Грёбнера для решений некоторых задач, а так-же практическое применение их в качестве упражнений.

В первой главе дипломной работы рассмотрены понятия аффинных многообразий и идеалов (представлены необходимые сведения из теории).

В начале второй главы представлены четыре основные задачи, связанные с идеалами. Эти задачи рассмотрены в последующих параграфах. Также, во второй главе было рассмотрено понятие мономиального упорядочения, введены понятия базисов Грёбнера, приведены алгоритмы деления полиномов от одной и нескольких переменных (алгоритм Бухбергера).

В третьей главе рассмотрены некоторые теоретические сведения о применении базисов Грёбнера.

Дипломная работа имеет реферативный характер. Все результаты работы достоверны и согласуются с уже известными ранее результатами. В качестве примеров некоторых алгоритмов, автором работы в качестве упражнений были решены практические задачи.

Рэферат

Дыпломная работа змяшчае:
54 старонкі.
3 выкарыстаных крыніц інфармацыі.

Ключавыя словы і паняцці: *Ідэал, Паліном, Маном, Аффінная Разнастайнасць, Упарадкаваньне, Алгарытм Дзялення, Базіс Гробнара, Алгарытм Бухбергера.*

Аб'ектам даследавання дыпломнай работы з'яўляюцца Базісы Гребнера і іх прымяненне да вырашэння сістэм алгебраічных раўнанняў і задач аб ідэалах.

Мэтай дыпломнай работы з'яўляецца разгляд тэарэтычных звестак і алгарытмаў, якія дазваляюць прымяняць Базісы Гребнера да рашэнняў для некаторых задач, а таксама практычнае прымяненне іх у якасці практыкаванняў.

У першай чале дыпломнай работы разгледжаны паняцці аффинных разнастайнасцяў і ідэалаў (прадстаўлены неабходныя звесткі з тэорыі).

У самым пачатку другой чалы прадстаўлены чатыры асноўныя задачы, звязаныя з ідэаламі. Гэтыя задачы разгледжаны у наступных параграфах. Таксама ў другой чале было разгледжана паняцце манамияльнага ўпарадкавання, уведзены паняцці базісаў Гребнера, прыведзены алгарытмы дзялення паліномаў ад адной і некалькіх зменных (алгарытм Бухбергера).

У трэцяй чале разгледжаны некаторыя тэарэтычныя звесткі аб прымяненні базісаў Гребнера.

Дыпломная работа мае рэфератыўны характар. Усе вынікі работы дакладныя і адпавядаюць ужо вядомым раней вынікамі. У якасці прыкладаў некаторых алгарытмаў, аўтарам работы ў якасці практыкаванняў былі вырашаны практычныя задачы.

Abstract

Diploma contains:
54 pages.
3 sources of information used.

Keywords and concepts: *Ideal, Polynomial, Monomial, Affine Variety, Term Orders, Division Algorithm, Gröbner Basis, Buchberger's Algorithm.*

The object of research of the Diploma is the Gröbner Bases and their application to solving algebraic equations systems and ideals.

The purpose of the diploma is to consider theoretical information and algorithms that allow you to use the Gröbner bases for solving some problems, as well as practically apply them as exercises.

In the first chapter of the diploma, the concepts of affine varieties and ideals are considered (the necessary information from the theory is presented).

At the beginning of the second chapter, four main tasks related to ideals are presented. These tasks are discussed in the following paragraphs. Also, in the second chapter, the concept of monomial ordering was considered, the concepts of Gröbner bases were introduced, algorithms for dividing polynomials in one and several variables (Buchberger's algorithm) are presented.

The third chapter discusses some theoretical information about the application of Gröbner bases.

Diploma is abstract in nature. All results of the work are reliable and are consistent with previously known results. As examples of some algorithms, the author of the work as exercises solved practical problems.

Введение.

В данной дипломной работе объектом исследования являются Базисы Грёбнера и их применение для решений алгебраических уравнений и задач об идеалах.

На протяжении всей работы вводятся понятия и теоретические сведения о таких математических объектах, как идеалы, аффинные многообразия, мономиальные упорядочения, полиномы. На основе этих сведений и понятий в разное время возникали алгоритмы поиска НОД полиномов, деления полиномов от одной и нескольких переменных. Эти алгоритмы рассмотрены как теоретически, так и на практике, в качестве упражнений.

В целом же эта работа направлена на рассмотрение и доказательства утверждений из теории о Базисах Грёбнера.

Глава 1. Идеалы, аффинные многообразия и связь между ними

§1. Аффинные многообразия.

1. Определение и свойства аффинных многообразий.

Определение 1.1. *Пусть* k *– некоторое поле,* $f_1, \dots, f_n$ *– полиномы в* $k[x_1, \dots, x_n]$. *Положим* $V(f_1, \dots, f_n) = \{(a_1, \dots, a_n) \in k^n : f_i(a_1, \dots, a_n) = 0, \forall\, i, 1 \le i \le s\}$. $V(f_1, \dots, f_n)$ *– называется* ***аффинным многообразием****, определенным полиномами* $f_1, \dots, f_n$.

Лемма 1.1 (Свойства аффинных многообразий). *Если* $V, W \subset k^n$*- аффинные многообразия, то* $V \cap W$ *и* $V \cup W$ *также являются аффинными многообразиями*.

Доказательство. Пусть $V = \mathrm{V}(f_1, \dots, f_s)$ и $W = \mathrm{V}(g_1, \dots, g_t)$. Мы утверждаем, что

$$V \cap W = \mathrm{V}(f_1, \dots, f_s, g_1, \dots, g_t),$$
$$V \cup W = \mathrm{V}\big(f_i g_j : 1 \le i \le s, 1 \le j \le t\big).$$

1. Если точка принадлежит $V \cap W$, то функции $f_1, \dots, f_n$ и $g_1, \dots, g_t$ в этой точке обращаются в нуль.
2. Если $a_1, \dots, a_n \in V$ то все f_i в этой точке обращаются в нуль; значит и все функции $f_i g_j$ обращаются в нуль в $(a_1, \dots, a_n)$. Таким образом, $W \subset \mathrm{V}(f_i g_j)$ и, аналогично, $V \subset \mathrm{V}(f_i g_j)$. Следовательно, $V \cup W \subset \mathrm{V}(f_i g_j)$. С другой стороны, пусть $(a_1, \dots, a_n) \in \mathrm{V}(f_i g_j)$. Если эта точка принадлежит V, то все доказано, если же нет, то $f_{i_0}(a_1, \dots, a_n) \neq 0$ для некоторого i_0. Поскольку функции $f_{i_0} g_j$ обращаются в нуль в $(a_1, \dots, a_n)$ при всех j, то все g_j в этой точке равны нулю. Значит, $(a_1, \dots, a_n) \in W$ и $\mathrm{V}\big(f_i g_j\big) \subset V \cup W$. ■

Из этой леммы следует, что пересечения аффинных многообразий и конечные объединения являются аффинными многообразиями.

§2. Идеалы.

Определение 2.1. *Подмножество* $I \subset k[x_1, \dots, x_n]$ *называется идеалом, если выполнены следующие условия:*

i) *Если* $f, g \in I$, *то* $f + g \in I$;
ii) *Если* $f \in I$ *и* $h \in k[x_1, \dots, x_n]$, *то* $hf \in I$.

Лемма 2.1. *Пусть* $f_1, \dots, f_s$ *принадлежат кольцу* $k[x_1, \dots, x_n]$; *тогда множество* $(f_1, \dots, f_s) = \{u_1 f_1 + \dots + u_s f_s \mid u_i \in k[x_1, \dots, x_n], i = \overline{1,n}\}$ *является идеалом в* $k[x_1, \dots, x_n]$. *Оно называется идеалом, порожденным полиномами* $f_1, \dots, f_s$, *а полиномы* $f_1, \dots, f_s$ *– образующими этого идеала или его порождающими элементами.*

Доказательство. Прежде всего, $0 \in (f_1, \dots, f_s)$, поскольку $0 = \sum_{i=1}^{s} 0 \cdot f_i$. Пусть теперь $f = \sum_{i=1}^{s} p_i f_i$, $g = \sum_{i=1}^{s} g_i f_i$ и $h \in k[x_1, \dots, x_n]$. Тогда из равенств

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i$$

$$hf = \sum_{i=1}^{s} (hp_i) f_i$$

вытекает, что $(f_1, \dots, f_s)$ – идеал. ■

Идеал $(f_1, \dots, f_s)$ может быть интепретирован на языке полиномиальных уравнений. Пусть $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Рассмотрим следующую систему уравнений:

$$\begin{cases} f_1 = 0, \\ \vdots \\ f_s = 0. \end{cases}$$

Из этих уравнений, с помощью обычных алгебраических преобразований, мы можем вывести другие. Так, например, если мы умножим первое уравнение на $h_1 \in k[x_1, \dots, x_n]$, второе – на $h_2 \in k[x_1, \dots, x_n]$ и т.д., а затем сложим произведения, то получим уравнение:

$$h_1 f_1 + h_2 f_2 + \cdots + h_s f_s = 0$$

которое является следствием уравнений первоначальной системы. Отметим, что левая часть этого уравнения принадлежит идеалу $(f_1, \dots, f_s)$, т.е. идеал $(f_1, \dots, f_s)$ можно рассматривать в качестве множества всех «полиномиальных следствий» системы $f_1 = f_2 = \cdots = f_s = 0$.

Идеал I называется ***конечно порожденным***, если существуют полиномы $f_1, \dots, f_s \in k[x_1, \dots, x_n]$, такие, что $I = (f_1, \dots, f_s)$; при этом множество полиномов $f_1, \dots, f_s$ называется *базисом* идеала *I*.

Определение 2.2. *Пусть $V \subset k^n$ – аффинное многообразие. Положим*

$$I(V) = \{f \in k[x_1, \dots, x_n] : f(a_1, \dots, a_n) = 0 \text{ для всех } (a_1, \dots, a_n) \in V\}.$$

$I(V)$ – ***идеал***.

Лемма 2.2. *Пусть $V \subset k^n$ – аффинное многообразие. Тогда $I(V)$ – идеал, который мы будем называть идеалом многообразия V.*

Доказательство. Нулевой полином обращается в нуль на k^n и на *V* в частности, так что $0 \in I(V)$. Пусть $f, g \in I(V)$ и $h \in k[x_1, \dots, x_n]$. Пусть $(a_1, \dots, a_n)$ – произвольная точка из *V*. Тогда

$$f(a_1, \dots, a_n) + g(a_1, \dots, a_n) = 0 + 0 = 0,$$

$$h(a_1, \dots, a_n) f(a_1, \dots, a_n) = h(a_1, \dots, a_n) \cdot 0 = 0$$

Отсюда следует, что *I(V)* - идеал. ■

Глава 2. Базисы Грёбнера

§1. Основные задачи об идеалах.

В этой главе мы рассмотрим следующие задачи:

a. *Задача описания идеала*. Является ли произвольный идеал $I \subset k[x_1, \dots, x_n]$ конечно порожденным? Или, другими словами, верно ли, что $I = (f_1, \dots, f_s)$ для некоторых $f_i \in k[x_1, \dots, x_n]$?

b. *Задача о принадлежности идеалу*. Пусть $f \in k[x_1, \dots, x_n]$, и пусть задан идеал $I = (f_1, \dots, f_s)$. Принадлежит ли полином f идеалу I? На геометрическом языке эту задачу можно сформулировать так: содержится ли многообразие $\mathrm{V}(f_1, \dots, f_s)$ в многообразии $\mathrm{V}(f)$?

c. *Задача решения полиномиальных уравнений*. Описать множество решений в k^n системы полиномиальных уравнений:

$$f_1(x_1, \dots, x_n) = \dots = f_s(x_1, \dots, x_n) = 0.$$

Другими словами, это то же самое, что описать аффинное многообразие $\mathrm{V}(f_1, \dots, f_s)$.

d. *Задача неявного представления*. Пусть V – подмножество в k^n, которое задано параметрически:

$$\begin{cases} x_1 = g_1(t_1, \dots, t_n) \\ \vdots \\ x_n = g_n(t_1, \dots, t_n) \end{cases}$$

Если g_i – полиномы (или рациональные функции) от переменных t_j, то V будет аффинным многообразием или его частью. Задача состоит в следующем: задать V полиномиальными уравнениями от переменных x_i.

§2. Упорядочение мономов в $k[x_1, \dots, x_n]$.

Внимательное рассмотрение алгоритма деления в $k[x]$ и алгоритма приведения системы (или матрицы) к ступенчатому виду методом исключения Гаусса показывает, что понятие ***упорядочения членов*** полинома является

ключевым в обоих алгоритмах. Как правило, алгоритм деления полиномов от одной переменной имеет дело со следующим упорядочением мономов:

$$\dots > x^{m+1} > x^m > \cdots > x^2 > x > 1.$$

Аналогично, когда мы приводим матрицы к ступенчатому виду, мы систематически главные элементы, т.е. первые слева ненулевые элементы в строках, обращаем в нуль. Переводя на язык линейных систем, это означает следующий порядок переменных:

$$x_1 > x_2 > \cdots > x_n.$$

Все уравнения записываются в порядке убывания членов. Более того, в ступенчатом виде уравнения системы записаны в порядке убывания старших (главных) членов.

Отметим, что между мономами $x^a = x_1^{a_1} \dots x_n^{a_n}$ и n-наборами (n-векторами) показателей степеней $a = (a_1, \dots, a_n) \in \mathbb{Z}_{\geq 0}^n$ существует взаимно однозначное соответствие. Упорядочение, которое мы определим на $\mathbb{Z}_{\geq 0}^n$, определит и упорядочение на множестве мономов: если на $\alpha > \beta$ в $\mathbb{Z}_{\geq 0}^n$, то мы будем говорить что $x^\alpha > x^\beta$.

Поскольку полином это сумма мономов, мы должны уметь располагать его члены в порядке убывания (или по возрастанию). Для этого наше упорядочение должно быть ***линейным***. Другими словами, для любой пары мономов x^α и x^β должно выполнятся ровно одно из следующих условий:

$$x^\alpha > x^\beta, x^\alpha = x^\beta, x^\alpha < x^\beta.$$

Далее мы должны учитывать связь упорядочения с операциями сложения и умножения полиномов. Когда мы складываем полиномы, то, после приведения подобных, мы можем переписать члены суммы в требуемом порядке. В случае с произведением ситуация более сложная. Дистрибутивность умножения по отношению к сложению позволяет нам свести задачу к случаю умножения монома на полином.

Мы потребуем, чтобы упорядочение мономов обладало следующим свойством. Если $x^\alpha > x^\beta$, а x^γ – произвольный моном, то $x^\alpha x^\gamma > x^\beta x^\gamma$. В терминах

векторов – показателей степеней это означает, что если $\alpha > \beta$ в $\mathbb{Z}_{\geq 0}^n$, то для любого $\gamma \in \mathbb{Z}_{\geq 0}^n$, $\alpha + \gamma > \beta + \gamma$.

Теперь мы можем дать определение.

1. Мономиальное упорядочение.

Определение 2.3. ***Мономиальным упорядочением*** *на* $k[x_1, \dots, x_n]$ *называется любое бинарное отношение* $>$ *на* $\mathbb{Z}_{\geq 0}^n$, *обладающее следующими свойствами*:

i) $>$ *является* ***линейным*** *(для любых* α, β *можно однозначно определить одно из следующих отношений:* $\alpha > \beta$, $\alpha < \beta$, $\alpha = \beta$ *) упорядочением на* $\mathbb{Z}_{\geq 0}^n$.

ii) Если $\alpha > \beta$ *и* $\gamma \in \mathbb{Z}_{\geq 0}^n$, *то* $\alpha + \gamma > \beta + \gamma$.

iii) $>$ *вполне упорядочивает* $\mathbb{Z}_{\geq 0}^n$, *т.е. любое непустое подмножество в* $\mathbb{Z}_{\geq 0}^n$ *имеет минимальный (наименьший) элемент (по соотношению к упорядочению* $>$*).*

Лемма 2.3. (условие вполне упорядоченности): *Упорядочение* $>$ *на* $\mathbb{Z}_{\geq 0}^n$ *вполне упорядочивает это множество тогда и только тогда, когда каждая строго убывающая последовательность элементов из* $\mathbb{Z}_{\geq 0}^n$

$$a(1) > a(2) > a(3) > \cdots$$

обрывается.

Доказательство. Докажем эквивалентное утверждение: $>$ не является вполне упорядочением тогда и только тогда, когда существует бесконечная строго убывающая последовательность элементов из $\mathbb{Z}_{\geq 0}^n$.

Если $>$ не есть вполне упорядочение, то существует непустое подмножество $S \subset \mathbb{Z}_{\geq 0}^n$, которое не имеет минимального элемента. В качестве $a(1)$ возьмем произвольный элемент из S. Так как он не минимален, то в S найдется элемент $a(2) < a(1)$. Так как $a(2)$ не минимален, то в S найдется элемент $a(3) < a(2)$. Продолжая этот процесс, мы получим бесконечную строго убывающую последовательность:

$$a(1) > a(2) > a(3) > \cdots$$

Обратно, если существует такая бесконечная строго убывающая последовательность, то множество $\{a(1), a(2), a(3), \dots\}$ является непустым подмножеством в $\mathbb{Z}_{\geq 0}^n$, которое не имеет минимального элемента, т.е. > не является вполне упорядочением. ■

В качестве примера мономиального упорядочения мы рассмотрим обычное упорядочение натуральных чисел из $\mathbb{Z}_{\geq 0}$:

$$\dots > m+1 > m > \dots > 3 > 2 > 1 > 0.$$

Все три условия определения 2.1 выполнены. Значит упорядочение мономов из $k[x]$ по степени (1) является мономиальным упорядочением.

2. Лексикографическое упорядочение.

Первым примером упорядочения n-векторов будет лексикографическое упорядочение (сокр. *lex*-упорядочение).

Определение 2.4 *(лексикографическое упорядочение). Пусть* $\alpha = (\alpha_1, \dots, \alpha_n), \beta = (\beta_1, \dots, \beta_n) \in \mathbb{Z}_{\geq 0}^n$. *Мы говорим, что* $\alpha >_{lex} \beta$, *если самая левая ненулевая координата вектора* $\alpha - \beta \in \mathbb{Z}^n$ *положительна. Мы будем писать* $x^n >_{lex} x^\beta$, *если* $\alpha >_{lex} \beta$.

Вот несколько примеров *lex*-упорядочения:

a) $(1,2,0) >_{lex} (0,3,4)$, так как $\alpha - \beta = (1,-1,-4)$.
b) $(3,2,4) >_{lex} (3,2,1)$, так как $\alpha - \beta = (0,0,3)$.
c) Обычный порядок переменных $x_1, \dots, x_n$ является *lex*-упорядочением. Так как

$$(1,0,\dots,0) >_{lex} (0,1,0,\dots,0) >_{lex} \dots >_{lex} (0,\dots,0,1),$$

то $x_1 >_{lex} x_2 >_{lex} \dots >_{lex} x_n$.

При работе с полиномами от двух или трёх переменных, мы будем обозначать переменные через x, y, z.

Проверим, что лексикографическое упорядочение удовлетворяет трем условиям из определения 2.1.

Предложение 2.1. *Лексикографическое упорядочение на* $\mathbb{Z}_{\geq 0}^n$ *является мономиальным упорядочением.*

Доказательство. (i) Тот факт, что $>_{lex}$ – линейное упорядочение, прямо следует из определения и из того, что обычное упорядочение на $\mathbb{Z}_{\geq 0}^n$ линейно. (ii) Пусть $\alpha >_{lex} \beta$. Тогда самая левая ненулевая координата вектора $\alpha - \beta$ положительна. Пусть это, например, $\alpha_k - \beta_k$. Но $x^\alpha \cdot x^\gamma = x^{\alpha+\gamma}$ и $x^\beta \cdot x^\gamma = x^{\beta+\gamma}$. Тогда $(\alpha + \gamma) - (\beta + \gamma) > \alpha - \beta$, и самой левой ненулевой координатой опять является $\alpha_k - \beta_k > 0$. (iii) Предположим, что $>_{lex}$ не является вполне упорядочением. Тогда по лемме 2.1 должна существовать строго убывающая бесконечная последовательность

$$a_1 >_{lex} a_2 >_{lex} a_3 >_{lex} \dots$$

элементов из $\mathbb{Z}_{\geq 0}^n$. Докажем, что это невозможно.

По определению *lex*-упорядочения, первые координаты векторов $a(i) \in \mathbb{Z}_{\geq 0}^n$ образуют невозрастающую последовательность неотрицательных целых чисел. Так как $\mathbb{Z}_{\geq 0}$ вполне упорядочено, то эта последовательность «стабилизируется», т.е. существует такое *k*, что первые координаты векторов $a(i)$ одинаковы при $i \geq k$. Начиная с $a(k)$, будем рассматривать вторые (а затем третьи и т.д.) координаты. Последовательность вторых координат векторов $a(k), a(k+1)$, ... не возрастает. Это значит, что она «стабилизируется». Продолжая это рассуждение, мы можем найти такое *l*, что у векторов $a(l), a(l+1)$, ... равны все координаты. Значит, это одинаковые векторы, что противоречит строгому убыванию последовательности. ■

При *lex*-упорядочении, переменная больше *любого монома*, который содержит только меньшие переменные. Это не зависит от его степени. Так, при упорядочении $x > y > z$ мы имеем $x >_{lex} y^5 z^3$. В случаях, когда нам будет необходимо учитывать также степени мономов и сравнивать сначала именно степени, мы будем это делать с помощью градуированного лексикографического упорядочения (сокращенно *grlex-упорядочения*).

Определение 2.5 *(градуированное лексикографическое упорядочение). Пусть* $\alpha, \beta \in \mathbb{Z}_{\geq 0}^n$. *Тогда мы говорим, что* $\alpha >_{grlex} \beta$, *если:*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i \text{ или } |\alpha| = |\beta| \text{ и } \alpha >_{lex} \beta.$$

Таким образом, *grlex* сначала упорядочивает по степеням, а если степени равны, то использует лексикографическое упорядочение.

Вот пример:

$$(1,2,3) >_{grlex} (3,2,0), \text{ так как } |(1,2,3)| = 6 >_{lex} |(3,2,0)| = 5.$$

Определение 2.6 *(градуированное обратное лексикографическое упорядочение grevlex). Пусть* $\alpha, \beta \in \mathbb{Z}_{\geq 0}^{n}$. *Тогда мы говорим, что* $\alpha >_{grevlex} \beta$, *если*

$$|\alpha| = \sum_{i=1}^{n} \alpha_i > |\beta| = \sum_{i=1}^{n} \beta_i$$

или $|\alpha| = |\beta|$ *и самая правая ненулевая координата вектора* $\alpha - \beta \in \mathbb{Z}^n$ *отрицательна.*

Пример $(4,7,1) >_{grevlex} (4,2,3)$, так как $|(4,7,1)| = 12 > |(4,2,3)| = 9$.

И *grlex* и *grevlex*, одинаково оценивают степень монома. В случае равенства степеней *grlex* использует *lex*-упорядочение, т.е. обращает внимание на самую левую (большую) переменную и «предпочитает» *большую* степень. Напротив, *grevlex* в случае равенства степеней обращает внимание на самую правую (меньшую) переменную и «предпочитает» меньшую степень.

Пусть $f = \sum_{\alpha} a^{\alpha} x^{\alpha} \in k[x_1, \dots, x_n]$, и пусть выбрано мономиальное упорядочение >. С помощью мономиальных упорядочений мы можем однозначно упорядочить члены полинома f в соответствии с >.

Пусть, например, $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2 \in k[x, y, z]$. Тогда:

а) При *lex*-упорядочении мы записываем полином f в порядке убывания членов так:

$$f = -5x^3 + 7x^2z^2 + 4xy^2z + 4z^2;$$

b) Запись f при *grlex*-упорядочении:

$$f = 7x^2z^2 + 4xy^2z - 5x^3 + 4z^2;$$

c) Запись f при *grevlex*-упорядочении:

$$f = 4xy^2z + 7x^2z^2 - 5x^3 + 4z^2.$$

Определение 2.7. *Пусть* $f = \sum_\alpha a^\alpha x^\alpha$ *- ненулевой полином в* $k[x_1, \dots, x_n]$*, и пусть* $>$ *- мономиальное упорядочение.*

i) ***Мультистепень*** *полинома f определяется так:*

$$multideg(f) = \max\,(\alpha \in \mathbb{Z}_{\geq 0}^n : a_\alpha \neq 0)$$

(максимум берется по отношению к $>$*).*

ii) ***Старший коэффициент*** *полинома f – это*

$$LC(f) = a_{multideg(f)} \in k.$$

iii) ***Старший моном*** *полинома f – это*

$$LM(f) = x^{multideg(f)}$$

(с коэффициентом 1).

iv) ***Старший член*** *полинома f – это*

$$LT(f) = LC(f) \cdot LM(f).$$

Для примера, пусть $f = 4xy^2z + 4z^2 - 5x^3 + 7x^2z^2$, как и выше, и пусть $>$ обозначает *lex*-упорядочение. Тогда:

$$multideg(f) = (3,0,0),$$
$$LC(f) = -5,$$
$$LM(f) = x^3,$$
$$LT(f) = -5x^3.$$

Лемма 2.4 (свойства мультистепени). *Пусть* $f, g \in k[x_1, \dots, x_n]$ *– ненулевые полиномы. Тогда* :

i) $multideg(fg) = multideg(f) + multideg(g)$.

ii) Если $f + g \neq 0$, *то* $multideg(f + g) \leq \max\big(multideg(f), multideg(g)\big)$. *Если, кроме того,* $multideg(f) \neq multideg(g)$, *то указанное неравенство становится равенством.*

§3. Алгоритм деления.

1. Алгоритм деления полинома от одной переменной.

При работе с алгоритмами, мы будем использовать «псевдокод». Это облегчит понимание формальных структур. Описание псевдокода приведено в **приложении А**.

Важной частью алгоритма является понятие «старшего члена» полинома от одной переменной. Введём точное определение.

Определение 2.8. *Пусть* $f \in k[x]$ *– ненулевой полином,*

$$f = a_0 x^m + a_1 x^{m-1} + \cdots + a_m,$$

где $a_i \in k$ *и* $a_0 \neq 0$ *(т.е.* $\deg(f) = m$*). Тогда* $a_0 x^m$ *называется старшим членом полинома* f *и обозначается* $LT(f) = a_0 x^m$.

Теперь мы можем дать описание алгоритма деления.

Предложение 2.2 (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* $\deg(r) < \deg(g)$. *Более того,* q *и* r *определены однозначно, и имеется алгоритм для их вычисления.*

Доказательство. Алгоритм вычисления q и r, записанный в псевдокоде:

Вход: g, f
Выход: q, r
$q := 0; r := f$
$WHILE\ r \neq 0\ AND\ LT(g)$ делит $LT(r)\ DO$
$$q := q + \frac{LT(r)}{LT(g)}$$

$$r := r - (LT(r)/LT(g))g$$

Докажем корректность алгоритма. Для начала, равенство $f = qg + r$ выполняется при начальных значениях q и r. Далее, на каждом шаге после переопределения q и r это равенство должно выполнятся, потому что

$$f = qg + r = \left(q + \frac{LT(r)}{LT(g)}\right)g + \left(r - \left(\frac{LT(r)}{LT(g)}\right)g\right).$$

Отметим, что выполнение оператора цикла WHILE … DO прекращается, когда утверждение «$r \neq 0$ и $LT(g)$ делит $LT(r)$» становится ложным, т.е. когда или $r = 0$ или $LT(g)$ не делит $LT(r)$. Когда алгоритм прекращает работу, он выдает требуемые q и r.

Осталось доказать, что утверждение между WHILE … DO в какой-то момент станет ложным и алгоритм остановится. Самым важным тут является тот факт, что полином $r - \left(\frac{LT(r)}{LT(g)}\right)g$ или равен нулю, или имеет степень, меньшую, чем степень полинома r. Докажем это. Пусть:

$$r = a_0x^m + \cdots + a_m, \qquad LT(r) = a_0x^m,$$
$$g = b_0x^k + \cdots + a_m, \qquad LT(g) = b_0x^k,$$

и пусть $m \geq k$. Тогда:

$$\left(r - \left(\frac{LT(r)}{LT(g)}\right)g\right) = (a_0x^m + \cdots) - \left(\frac{a_0}{b_0}\right)x^{m-k}(b_0x^k + \cdots),$$

и степень полинома r обязана уменьшиться (или r обращается в нуль). Так как степень конечна, то алгоритм останавливается после конечного числа шагов. ■

2. Основные следствия алгоритма деления в $k[x]$.

Следствие 2.1. *Пусть $f \in k[x]$ – ненулевой полином. Тогда он имеет в k не более чем* $\deg(f)$ *корней.*

Доказательство. Применим индукцию по $m = \deg(f)$. Если $m = 0$, то f – ненулевая константа, и утверждение справедливо. Пусть 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 полинома f. Поделим f на $x - a$. Тогда по предположению имеем $f = q(x - a) + r$, где $r \in k$, так как $x - a$ имеет степень один. Положив в этом равенстве $x = a$, получим $0 = f(a) = q(a)(a - a) + r = r$, т.е. $f = q(x - a)$, и, значит степень полинома q равна $m - 1$.

Мы утверждаем, что любой корень полинома f, отличный от a, является корнем полинома q. Если $b \neq a$ – корень полинома f, то $0 = f(b) = q(b)(b - a)$, откуда $q(b) = 0$ (так как k - поле). По предположению индукции q имеет не более $m - 1$ корней; значит, f имеет не более m корней в k. ■

Следствие 2.2. *Пусть k - поле. Тогда каждый идеал в $k[x]$ может быть представлен в виде (f) для некоторого полинома $f \in k[x]$. Более того, f определен однозначно с точностью до умножения на ненулевую константу из k.*

Доказательство. Пусть $I \subset k[x]$ – некоторый идел. Если $I = \{0\}$, то $I = (0)$ и утверждение доказано. Пусть теперь $I \neq \{0\}$, и пусть $f \in I$ – ненулевой полином минимальной степени (в множестве полиномов, содержащихся в I). Мы утверждаем, что $I = (f)$. Включение $(f) \subset I$ очевидно, так как I - идеал. Рассмотрим теперь полином $g \in I$. В соответствии с алгоритмом деления, $g = qf + r$, где или $r = 0$, или $\deg(r) < \deg(f)$. Так как I – идеал, то $qf \in I$ и, значит $r = g - gf \in I$. Если $r \neq 0$, то $\deg(r) < \deg(f)$, что противоречит выбору полинома f. Значит $r = 0$, т.е. $g = gf \in \langle f \rangle$, что доказывает равенство $I = (f)$.

Теперь докажем единственность. Пусть $(f) = (g)$. Так как $f \in (g)$, то $f = hg$ для некоторого полинома h. Имеем

$$\deg(f) = \deg(h) + \deg(g),$$

т.е. $\deg(f) \geq \deg(g)$. Аналогично получаем, поменяв местами f и g, что $\deg(g) \geq \deg(f)$, т.е. $\deg(g) = \deg(f)$. Из равенства $\deg(f) = \deg(h) + \deg(g)$ следует, что $\deg(h) = 0$. Значит, h - ненулевая константа. ■

Идеал, который порожден одним элементом, называют ***главным идеалом***. Таким образом, ввиду следствия 2.2 мы говорим, что $k[x]$ является ***областью главных идеалов*** или сокращенно ОГИ.

3. Наибольший общий делитель полиномов.

Определение 2.9. *Наибольшим общим делителем полиномов* $f, g \in k[x]$ *называется полином* h*, такой, что*

i) h *делит и* f*, и* g*;*
ii) если p *– некоторый полином, который делит и* f*, и* g*, то* p *делит* h*.*

Наибольший общий делитель будет обозначаться через НОД(f, g). В следующем предложении сформулированы основные свойства наибольших общих делителей.

Предложение 2.3. *Пусть* $f, g \in k[x]$. *Тогда*

i) НОД(f, g) *существует и единственен с точностью до умножения на ненулевую константу из* k*;*
ii) НОД(f, g) *является образующим идеала* (f, g)*;*
iii) существует алгоритм для вычисления НОД(f, g).

Алгоритм Евклида позволяет вычислить наибольший общий делитель двух полиномов в $k[x]$.

Введём необходимые определения. Пусть $f, g \in k[x]$, $g \neq 0$. Запишем f в виде $f = qg + r$, где q и r определены, как в предложении 1.1. Тогда r

называется остатком от деления f на g. Теперь мы можем дать описание алгоритма Евклида:

Вход: f, g
Выход: h
$h \coloneqq f$
$s \coloneqq g$
$WHILE\ s \neq 0\ DO$
$rem \coloneqq \text{остаток}(h, s)$
$h \coloneqq s$
$s \coloneqq rem$

Переменными алгоритма являются h и s. Значением h является первый полином в каждом НОД, а значением s – второй. Переход от очередного НОД к следующему происходит так же, как и соответствующий переход в цикле $WHILE$ ... DO алгоритма. На каждом шаге алгоритма $\text{НОД}(h, s) = \text{НОД}(f, g)$. Работа алгоритма должна прекратиться, так как степени полинома s уменьшаются и в некоторый момент s станет равным нулю. В момент остановки алгоритма $h = \text{НОД}(h, 0)$, т.е. $h = \text{НОД}(f, g)$.

Определение 2.10. ***Наибольшим общим делителем*** *полиномов* $f_1, \dots, f_s \in k[x]$ *называется полином h, такой, что*

i) h *делит* $f_1, \dots, f_s$*;*
ii) если p – некоторый полином, который делит $f_1, \dots, f_s$*, то p делит h.*

Такой полином h обозначается через $\text{НОД}(f_1, \dots, f_s)$. В следующем предложении сформулированы его основные свойства.

Предложение 2.4. *Пусть* $f_1, \dots, f_s \in k[x]$, $s \geq 2$. *Тогда*

i) $\text{НОД}(f_1, \dots, f_s)$ *существует и определен однозначно с точностью до умножения на ненулевую константу из k;*
ii) $\text{НОД}(f_1, \dots, f_s)$ *порождает идеал* $(f_1, \dots, f_s)$*;*
iii) Если $s \geq 3$*, то* $\text{НОД}(f_1, \dots, f_s) = \text{НОД}(f_1, \text{НОД}(f_2, \dots, f_s))$*;*
iv) существует алгоритм для вычисления $\text{НОД}(f_1, \dots, f_s)$.

Доказательство. Доказательство пп. (i) и (ii) аналогично доказательству тех же пунктов предложению 2.4. Докажем (iii). Пусть $h = \text{НОД}(f_2, \dots, f_s)$. Тогда

$$(f_1, h) = (f_1, \dots, f_s).$$

Из (ii) следует, что

$$(\text{НОД}(f_1, h)) = (\text{НОД}(f_1, \dots, f_s)).$$

Для доказания существования алгоритма, вычисляющего $\text{НОД}(f_1, \dots, f_s)$, нужно объединить п.$(iii)$ и алгоритм Евклида. ■

4. Алгоритм деления в $k[x_1, \dots, x_n]$.

Выше мы рассмотрели алгоритм деления для полиномов от одной переменной. Он может быть применен для решения задачи о принадлежности идеалу. Если $f \in k[x]$, то, для того, чтобы узнать, принадлежит f идеалу $I = (g)$ или нет, мы делим f на g:

$$f = qg + r,$$

где $q, r \in k[x]$ и $r = 0$ или $\deg(r) < \deg(g)$. Мы доказали, что $f \in I$ в том и только том случае, когда $r = 0$. Таким образом, этот алгоритмический метод пригоден для проверки принадлежности полинома идеалу.

Для решения этой же задачи в случае нескольких переменных необходимо обобщить алгоритм деления алгоритм деления в $k[x]$ на общий случай полиномиального кольца $k[x_1, \dots, x_n]$. Наша цель – научиться делить полином $f \in k[x_1, \dots, x_n]$ на полиномы $f_1, \dots, f_s \in k[x_1, \dots, x_n]$. Это означает научиться представлять f в виде

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

где «частные» $a_1, \dots, a_s$ и остаток r принадлежат $k[x_1, \dots, x_n]$. Чтобы корректно определить остаток, тут будут использованы мономиальные упорядочения.

Теорема 2.1 (Алгоритм деления в $k[x_1, \dots, x_n]$). *Зафиксируем некоторое мономиальное упорядочение > на $\mathbb{Z}_{\geq 0}^n$, и пусть $F = (f_1, \dots, f_s)$ – упорядоченный s-набор полиномов из $k[x_1, \dots, x_n]$. Тогда любой полином $f \in k[x_1, \dots, x_n]$ может быть записан в виде*

$$f = a_1 f_1 + \cdots + a_s f_s + r,$$

где $a_i, r \in k[x_1, \dots, x_n]$ 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 $LT(f_1), \dots, LT(f_s)$. Мы называем r ***остатком*** *от деления полинома f на F. Более того, если $a_i f_i \neq 0$, то*

$$multideg(f) \geq multideg(a_i f_i).$$

Доказательство. Ниже приведено формальное описание алгоритма:

Вход: $f_1, \dots, f_s, f$
Выход: $a_1, \dots, a_s, r$
$a_1 := 0; \dots; a_s := 0; r := 0$
$p := f$
$WHILE\ p \neq 0\ DO$
    $i := 1$
    есть_деление $:= false$
    $WHILE\ i \leq s\ AND$ есть_деление $= false\ DO$
        $IF\ LT(f_i)$ делит $LT(p)\ THEN$
            $a_i := a_i + \frac{LT(p)}{LT(f_i)}$
            $p := p - \left(\frac{LT(p)}{LT(f_i)}\right) f_i$
            есть_деление $= true$
        $ELSE$
            $i := i + 1$
    IF есть_деление $= false\ THEN$
        $r := r + LT(p)$
        $p := p - LT(p)$

В этом алгоритме переменная p на каждом шаге выполняет роль промежуточного делимого, переменная r выполняет роль остатка, а переменные $a_1, \dots, a_s$ выполняют роль частных. Логическая переменная «есть_деление» гово-

рит нам, делится ли старший член промежуточного переменного на какой-либо из $LT(f_i)$. Каждый раз, когда мы находимся в главном цикле $WHILE$ ... DO может произойти ровно одно из двух событий:

- (Шаг деления) Если никоторый член $LT(f_i)$ делит $LT(p)$, то алгоритм продолжает работу, как в случае одной переменной.
- (Шаг вычисления остатка) Если никакой из $LT(f_i)$ не делит $LT(p)$, то алгоритм прибавляет $LT(p)$ к остатку.

Для проверки корректности алгоритма, сначала докажем, что равенство $f = a_1 f_1 + \cdots + a_s f_s + p + r$ выполняется на каждом шаге. Очевидно, что оно выполнено для начальных значений $a_1, \dots, a_s, p$ и r. Пусть на некотором шаге оно имеет место. Если следующим является шаг деления, то некоторый $LT(f_i)$ делит $LT(p)$ и равенство

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

показывает, что сумма $a_i f_i + p$ не изменилась. Так как все остальные переменные остались теми же, то изначальное равенство выполняется и на этом шаге тоже. Если же следующим шагом является шаг вычисления остатка, то меняются и p, и r, но их сумма остается неизменной, так как

$$p + r = \big(p - LT(p)\big) + \big(r + LT(p)\big).$$

И опять равенство выполняется на следующем шаге.

Далее, обратим внимание, что алгоритм прекращает работу, когда $p = 0$. В этом случае

$$f = a_1 f_1 + \cdots + a_s f_s + r.$$

Так как к r добавлялись только такие члены, которые не делятся ни на один из $LT(f_i)$, то это означает, что $a_1, \dots, a_s$ и r удовлетворяют условиям теоремы 4.1 в случае остановки работы алгоритма.

Для того, чтобы доказать, что алгоритм в какой-то момент остановится, нужно заметить, что каждый раз, когда мы заново вычисляем переменную p, или ее мультистепень уменьшается (относительно заданного упорядочения), или p обращается в нуль. Предположим сначала, что p изменилось в ходе шага

деления:

$$p' = p - \frac{LT(p)}{LT(f_i)} f_i.$$

Согласно свойству мультистепени мы имеем:

$$LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p),$$

так что p и $\frac{LT(p)}{LT(f_i)} f_i$ имеют одинаковые старшие члены. Следовательно, их разность p' имеет строго меньшую мультистепень (если $p' \neq 0$). Пусть теперь p меняется в ходе шага вычисления остатка:

$$p' = p - LT(p).$$

Очевидно, что здесь $multideg(p') < multideg(p)$, если $p' \neq 0$, т.е. в обоих случаях мультистепень уменьшается. Если алгоритм не останавливается, то мы получаем бесконечную строго убывающую последовательность мультистепеней. Но так как $>$ является вполне упорядочением, то это противоречит лемме о свойстве мультистепени. Таким образом, в какой-то момент p обратится в нуль, и алгоритм остановится после конечного числа шагов.

Осталось установить связь между $multideg(f)$ и $multideg(a_i f_i)$. Каждый член полинома a_i равен $\frac{LT(p)}{LT(f_i)}$ для некоторого значения переменной p. Начальное значение p есть f, и мы только что доказали, что мультистепень p строго убывает; значит, $LT(p) \leq LT(f)$. Таким образом $multideg(a_i f_i) \leq multideg(f)$, если $a_i f_i \neq 0$. ■

Пример. Рассмотрим полином:

$$f(x, y) = x^3 y^3 + x^2 y^2 + x^2 y + xy + 1$$

при *lex*-упорядочение с $x > y$.

Применим алгоритм деления из теоремы 2.1 и поделим f на

$$g_1 = x^2y + 1$$
$$g_2 = y + 2$$

В результате выполнения алгоритма мы получим новое представление полинома f в виде:

$$f = a_1g_1 + a_2g_2 + r$$

Будем записывать делители частные a_1, a_2 и r в отдельный столбец:

$a_1 = xy + 1$
$a_2 = y - 2$
$r = x^2 + 4$

$$\begin{array}{r|l}
x^3y^3 + x^2y^2 + x^2y + xy + 1 & x^2y + 1 \\
\underline{-(x^3y^2 + xy)} & xy + 1 \\
x^2y + x^2 + y^2 + 1 & \\
\underline{-(x^2y + 1)} & \\
x^2 + y^2 & \\
\underline{-x^2} & \\
y^2 & y + 2 \\
\underline{-(y^2 + 2y)} & y - 2 \\
-2y & \\
\underline{-(-2y - 4)} & \\
4 & \\
\underline{-4} & \\
0 &
\end{array}$$

В результате получаем:

$$f = (xy + 1)(x^2y + 1) + (y - 2)(y + 2) + x^2 + 4.$$

§4. Мономиальные идеалы и лемма Диксона.

В этом параграфе рассмотрим задачу описания идеала для частного случая мономиальных идеалов.

1. Определение и свойства мономиальных идеалов.

Определение 2.11. *Идеал* $I \subset k[x_1, \dots, x_n]$ *называется* ***мономиальным****, если существует подмножество* $A \subset \mathbb{Z}_{\geq 0}^n$ *(которое может быть бесконечным), такое, что I состоит из конечных сумм вида* $\sum_{\alpha \in A} h_\alpha x^\alpha$*, где* $h_\alpha \in k[x_1, \dots, x_n]$*. Такой идеал I будет обозначаться через* $(x^\alpha : \alpha \in A)$.

В следующей лемме охарактеризуем все мономы, которые принадлежат заданному мономиальному идеалу.

Лемма 2.5. П*усть* $I = (x^\alpha : \alpha \in A)$ *– мономиальный идеал. Тогда моном* x^β *принадлежит I в том и только том случае, когда* x^β *делится на некоторый моном* $x^\alpha : \alpha \in A$.

Доказательство. Если x^β делится на некоторый $x^\alpha : \alpha \in A$, то, по определению мономиального идеала, $x^\beta \in I$. Докажем обратное. Пусть $x^\beta \in I$; тогда $x^\beta = \sum_{i=1}^s h_i x^{\alpha(i)}$, где $h_i \in k[x_1, \dots, x_n]$, а $\alpha(i) \in A$. Если мы рассмотрим каждый член в равенстве справа делится на некоторый $x^{\alpha(i)}$. Значит, и левая часть равенства, т.е. x^β, обладает тем же свойством, так как моном x^βсодержится как член хотя бы в одном слагаемом $h_i x^{\alpha(i)}$. ■

Теперь мы докажем, что принадлежность полинома f мономиальному идеалу определяется мономами, линейной комбинацией которых является f.

Лемма 2.6. *Пусть I – некоторый мономиальный идеал, а* $f \in k[x_1, \dots, x_n]$. *Тогда следующие условия эквивалентны:*

i) $f \in I$;
ii) каждый член полинома f *принадлежит I;*
iii) f *является k-линейной комбинацией мономов из I.*

Следствием п(iii) является факт, что мономиальный идеал однозначно определяется своими мономами. То есть имеет место следующее утверждение.

Следствие 2.3. *Два мономиальных идеала совпадают в том и только том случае, когда совпадают множества мономов, содержащихся в них.*

2. Лемма Диксона.

Теорема 2.2. *Любой мономиальный идеал* $I = (x^{\alpha} : \alpha \in A) \subset k[x_1, \dots, x_n]$ *может быть представлен в виде* $I = (x^{\alpha(1)}, \dots, x^{\alpha(s)})$, *где* $\alpha(1), \dots \alpha(s) \in A$. *В частности, I имеет конечный базис.*

Доказательство. Доказательство проводится с помощью индукции по n - числу переменных. Если $n = 1$, то I порожден мономами x_1^a, где $\alpha \in A \subset \mathbb{Z}_{\geq 0}$. Пусть β – наибольший элемент в A. Тогда для всех $\alpha \in A$ имеем $\beta \leq a$. Таким образом, x_1^{β} делит все образующие x_1^a, т.е. $I = (x_1^{\beta})$.

Пусть $n > 1$ и теорема справедлива для $n - 1$. Обозначим переменные через $x_1, \dots, x_{n-1}, y$, так что мономы в $k[x_1, \dots, x_{n-1}, y]$ будут записаны в виде $x^a y^m$, где $\alpha \in \mathbb{Z}_{\geq 0}^{n-1}$, а $m \in \mathbb{Z}_{\geq 0}$.

$I \subset k[x_1, \dots, x_{n-1}, y]$ – мономиальный идеал. Рассмотрим идеал $J \subset k[x_1, \dots, x_{n-1}]$, порожденный такими мономами x^{α}, что $x^a y^m \in I$ для некоторого $m \geq 0$. Так как J – мономиальный идеал в $k[x_1, \dots, x_{n-1}]$, то по предположению индукции он конечно порожден, $J = (x^{\alpha(1)}, \dots, x^{\alpha(s)})$. Идеал J может юыть рассмотрен , как «проекция» идеала I в $k[x_1, \dots, x_{n-1}]$.

По определению J для каждого $i, 1 \leq i \leq s$, существует $m_i \geq 0$, такое, что $x^{\alpha(i)} y^{m(i)} \in I$. Допустим m – наибольшее из m_i. Для каждого $l, 0 \leq l \leq m - 1$, рассмотрим идеал $J_l \subset k[x_1, \dots, x_{n-1}]$, порожденный такими мономами x^{β}, что $x^{\beta} y^l \in I$. Неформально можно сказать, что J_l – это «срез» идеала I, порожденный мономами, которые содержат y точно в степени l. По предположению индукции, J_l конечно порожден, $J_l = (x^{\alpha_l(1)}, \dots, x^{\alpha_l(s_l)})$.

Мы утверждаем, что I порожден мономами, перечисленными в следующем списке:

$$\begin{aligned} &\text{из} \quad J \quad : x^{\alpha(1)} y^{m(1)}, \dots, x^{\alpha(s)} y^{m(s)}, \\ &\text{из} \quad J_0 \quad : x^{\alpha_0(1)}, \dots, x^{\alpha_0(s_0)}, \\ &\text{из} \quad J_1 \quad : x^{\alpha_1(1)} y, \dots, x^{\alpha_1(s_1)} y, \end{aligned}$$

$$\vdots$$

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

Докажем, что каждый моном в I делится хотя бы на один моном из списка. Пусть $x^a y^p \in$ I. Если $p \geq m$, то по определению J моном $x^a y^p$ делится на некоторый моном $x^{a(i)}y^m$. С другой же стороны, если $p \leq m-1$, то по определению идеала J_p моном $x^a y^p$ делится на некоторый моном $x^{\alpha_p(j)}y^m$. Из леммы 2.5 следует, что мономы из списка порождают идеал, содержащий те же мономы, которые содержит I. По следствию 2.3 эти идеалы совпадают, и наше утверждение доказано.

Для завершения доказательство теоремы, осталось доказать, что из заданного множества образующих идеала I можно выбрать конечное множество образующих. Будем обозначать переменные, как и раньше, $x_1, \dots, x_n$. Тогда $I = (x^\alpha : \alpha \in A) \subset k[x_1, \dots, x_n]$. Нам нужно доказать, что $I = (x^{\beta(1)}, \dots, x^{\beta(s)})$, где $x^{\beta(i)} \in I$. Поскольку $x^{\beta(1)} \in (x^\alpha : \alpha \in A)$, то по лемме 2.5 каждый моном $x^{\beta(i)}$ делится на некоторый моном $x^{\alpha(i)}$, где $\alpha(i) \in A$. Теперь очевидно, что $I = (x^{a(1)}, \dots, x^{a(s)})$. ■

Лемма Диксона применяется для доказательства следующего важного утверждения о мономиальных упорядочениях на $k[x_1, \dots, x_n]$.

Следствие 2.4. *Пусть > - некоторое отношение на $\mathbb{Z}_{\geq 0}^n$, удовлетворяющее следующим условиям:*

i) > *- линейное упорядочение на $\mathbb{Z}_{\geq 0}^n$;*
ii) если $\alpha > \beta$ и $\gamma \in \mathbb{Z}_{\geq 0}^n$, то $\alpha + \gamma > \beta + \gamma$.

Тогда > является вполне упорядочением в том и только том случае, когда $a \geq 0$ для всех $a \in \mathbb{Z}_{\geq 0}^n$.

Доказательство. $\Rightarrow$. Пусть > является вполне упорядочением, и пусть a_0 – наименьший элемент в $\mathbb{Z}_{\geq 0}^n$. Достаточно доказать, что $a_0 \geq 0$. Если $0 > a_0$, то по (ii) мы можем прибавить a_0 к обеим частям и получить $a_0 > 2a_0$, что противоречит тому, что a_0 – наименьший элемент в $\mathbb{Z}_{\geq 0}^n$.

$\Leftarrow$. Пусть $a \geq 0$ для всех $a \in \mathbb{Z}_{\geq 0}^n$, и пусть $A \subset \mathbb{Z}_{\geq 0}^n$ – некоторое непустое множество. Нам нужно доказать, что в A существует наменьший элемент. Рас-

смотрим мономиальный идеал $I = (x^{\alpha} : \alpha \in A)$. По лемме Диксона существуют мономы $\alpha(1), \dots, \alpha(s) \in A$, такие, что $I = (x^{a(1)}, \dots, x^{a(s)})$. Пусть $\alpha(1) < \alpha(2) < \cdots < \alpha(s)$ (в противном случае переименуем мономы). Мы утверждаем, что $\alpha(1)$ – наименьший элемент множества A. Докажем это. Рассмотрим произвольный элемент $\alpha \in A$. Тогда $x^{\alpha} \in (x^{a(1)}, \dots, x^{a(s)})$. По лемме 2.5 моном x^{α} делится на некоторый моном $x^{a(i)}$, т.е. $\alpha = a(i) + \gamma, \gamma \in \mathbb{Z}_{\geq 0}^{n}$. Тогда $\gamma \geq 0$ и по (ii) мы имеем

$$\alpha = a(i) + \gamma \geq a(i) + 0 = a(i) \geq a(1).$$

Значит, $a(1)$ – наименьший элемент в A. ■

§5. Теорема Гильберта о базисе и базисы Грёбнера.

В данном параграфе будет приведено полное решение *задачи описания идеала*. Для каждого идеала I мы можем определить его *идеал старших членов* следующим образом.

Определение 2.12. *Пусть $I \subset k[x_1, \dots, x_n]$ – ненулевой идеал.*

i) Обозначим через $LT(I)$ множество старших членов элементов из I, т.е.
$$LT(I) = \{cx^{a} : \text{существует } f \in I \text{ и } LT(f) = cx^{a}\}.$$
ii) Обозначим через $(LT(I))$ идеал, порожденный элементами из $LT(I)$.

Отметим важный момент в определении $\langle LT(I) \rangle$. Пусть I конечно порожден, $I = (f_1, \dots, f_n)$. Тогда $(LT(f_1), \dots, LT(f_s))$ и $(LT(I))$ могут быть *разными* идеалами. Конечно, $LT(f_i) \in LT(I) \subset (LT(I))$; поэтому $(LT(f_1), \dots, LT(f_s)) \subset (LT(I))$.

Докажем, что $(LT(I))$ является мономиалным идеалом.

Предложение 2.5. *Пусть $I \subset k[x_1, \dots, x_n]$ – некоторый идеал. Тогда:*

i) $(LT(I))$ – мономиальный идеал;
ii) существуют полиномы $g_1, \dots, g_s \in I$, такие, что $LT(I)) = (LT(g_1), \dots, LT(g_s))$

Доказательство. (i) Старшие мономы $LM(g)$ элементов $g \in I - \{0\}$ порождают мономиальный идеал $(LM(g) : g \in I - \{0\})$. Так как $LM(g)$ отличается от $LT(g)$ на ненулевой множитель из поля k, то этот идеал совпадает с идеалом $(LT(g) : g \in I - \{0\} = (LT(I)))$. Следовательно, $(LT(I))$ является мономиальным идеалом.

(ii) Поскольку $(LT(I))$ порожден мономами $LM(g)$, $g \in I - \{0\}$, то по лемме Диксона $(LT(I)) = (LM(g_1), \dots, LM(g_t))$ для конечного набора $g_1, \dots, g_t \in I$. Так как $LM(g_i)$ отличается от $LT(g_i)$ на ненулевой множитель из поля k, то $(LT(I)) = (LM(g_1), \dots, LM(g_t))$. ■

1. Теорема Гильберта о базисе.

Используя алгоритм деления и предложение 2.5 , мы можем дать доказательство конечной порожденности *любого* полиномиального идеала. Пусть $I \subset k[x_1, \dots, x_n]$ – некоторый идеал, и пусть $(LT(I))$ – его идеал старших членов. Также мы будем считать, что задано некоторое мономиальное упорядочение, используемое в алгоритме деления.

Теорема 2.3 (Гильберта о базисе). *Каждый идеал* $I \subset k[x_1, \dots, x_n]$ *является конечно порожденным, т.е.* $I = (g_1, \dots, g_s)$, *где* $g_1, \dots, g_s \in I$.

Доказательство. Если $I = \{0\}$, то порождающее множество состоит из единственного элемента – нулевого полинома. Если I – ненулевой идеал, то порождающее множество $g_1, \dots, g_s$ мы будем строить следующим образом. Из предложения 2.5 следует, что существуют полиномы $g_1, \dots, g_s \in I$, такие, что $(LT(I)) = (LT(g_1), \dots, LT(g_s))$. Мы утверждаем, что $I = (g_1, \dots, g_s)$.

Поскольку каждый g_i принадлежит I, то $(g_1, \dots, g_s) \subset I$. Пусть теперь $f \in I$ – некоторый элемент. Применяя алгоритм деления, поделим f на $g_1, \dots, g_s$. В результате f будет представлен в виде:

$$f = a_1 g_1 + \cdots + a_s g_s + r,$$

где ни один член полинома r нельзя поделить ни на один из $LT(g_1), \dots, LT(g_s)$. Мы утверждаем, что $r = 0$. Имеем:

$$r = f - a_1 g_1 - \cdots - a_s g_s \in I.$$

Если $r \neq 0$, то $LT(r) \in (LT(I)) = (LT(g_1), \dots, LT(g_s))$. Тогда по лемме 2.5 $LT(r)$ должен делится хотя бы на один $LT(g_i)$. Однако это противоречит определению остатка. Значит $r = 0$, т.е.

$$f = a_1 g_1 + \cdots + a_s g_s + 0 \in \langle g_1, \dots, g_s \rangle,$$

Откуда следует, что $I \subset (g_1, \dots, g_s)$. ■

2. Базисы Грёбнера.

Определение 2.13. *Пусть задано мономиальное упорядочение. Конечное подмножество $G = \{g_1, \dots, g_s\}$ элементов идеала I называется его* ***базисом Грёбнера*** *(или стандартным базисом), если*

$$(LT(g_1), \dots, LT(g_s)) = (LT(I)).$$

Приведенное определение можно переформулировать следующим образом: множество $\{g_1, \dots, g_s\} \subset I$ называется базисом Грёбнера идеала I в том и только том случае, когда старший член любого элемента из I делится на хотя бы один старший член $LT(g_i)$.

Из доказательства теоремы 2.3 вытекает следующий результат.

Следствие 2.5. *Пусть задано некоторое мономиальное упорядочение. Тогда любой ненулевой идеал $I \subset k[x_1, \dots, x_n]$ обладает базисом Грёбнера. Более того, базис Грёбнера идеала I является его базисом.*

Доказательство. Пусть I – ненулевой идеал в $G = \{g_1, \dots, g_s\}$ – множество, построенное в теореме 2.3. Это множество является базисом Грёбнера по определению. Что касается второго утверждения, то, как доказано в теореме 2.3, если $(LT(I)) = (LT(g_1), \dots, LT(g_s))$, то $I = (g_1, \dots, g_s)$, т.е. G является базисом в I. ■

Упражнение. Пусть используется grlex-упорядочение с $x > y > z$. Верно ли, что множество $\{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$ является базисом Грёбнера? Объясните ваш ответ.

Решение.

$f_1 = x^4y^2 - z^5;$

$f_2 = x^3y^3 - 1;$

$f_3 = x^2y^4 - 2z.$

Рассмотрим полином:

$$f = y \cdot f_1 - x \cdot f_2 + 0 \cdot f_3 = y \cdot (x^4y^2 - z^5) - x \cdot (x^3y^3 - 1) + 0 \cdot (x^2y^4 - 2z)$$
$$= x^4y^3 - yz^5 - x^4y^3 + x = -yz^5 + x.$$

Очевидно, что $f \in I$. Значит, $-yz^5 = LT(-yz^5 + x) \in (LT(I))$.

С другой же стороны, $-yz^5$ не делится ни на один из старших членов полиномов f_1, f_2, f_3. А именно, $-yz^5$ не делится ни на $x^4y^2 = LT(x^4y^2 - z^5)$, ни на $x^3y^3 = LT(x^3y^3 - 1)$, ни на $x^2y^4 = LT(x^2y^4 - 2z)$. Следовательно, имеем следующее:

$$-yz^5 \notin \langle LT(f_1), LT(f_2), LT(f_3) \rangle.$$

В результате мы получаем, что $(LT(I)) \neq (LT(f_1), LT(f_2), LT(f_3))$. Но по определению базисом Грёбнера является такое конечное подмножество $G = \{g_1, \dots, g_s\}$ элементов идеала I, для которого

$$(LT(g_1), \dots, LT(g_s)) = (LT(I)).$$

Значит, рассмотренное нами множество не является базисом Грёбнера.

3. Свойства базисов Грёбнера.

Предложение 2.6. *Пусть $G = \{g_1, \dots, g_s\}$ – базис идеала $I \subset k[x_1, \dots, x_n]$, и пусть $f \in k[x_1, \dots, x_n]$. Тогда существует единственный полином $r \in k[x_1, \dots, x_n]$, который обладает следующими свойствами:*

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

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

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

Доказательство. Алгоритм деления позволяет нам записать f в виде $f = a_1 g_1 + \cdots + a_s g_s + r$, где r удовлетворяет условию (i). Условие (ii) тоже выполняется, поскольку $g = a_1 g_1 + \cdots + a_s g_s \in I$. Существование полинома r доказано.

Докажем единственность. Пусть $f = g + r = g' + r'$, где g, r, g', r' удовлетворяют условиям (i), (ii). Тогда $r - r' = g' - g \in I$. Поэтому если $r \neq r'$, то $LT(r - r') \in (LT(I)) = (LT(g_1), \dots, LT(g_s))$. Тогда по лемме 2.5 $LT(r - r')$ делится на какой-то старший член $LT(g_i)$. Но это невозможно в силу условия (i). Значит, $r = r'$, и единственность доказана. ■

Определение 2.14. *Остаток* r *называется* ***нормальной формой*** *полинома* f. *Его единственность характеризует базисы Грёбнера.*

Отметим, что хотя остаток и единственен, но «частные» a_i, которые вычисляются алгоритмом деления в $f = a_1 g_1 + \cdots + a_s g_s + r$, зависят от порядка делителей даже в случае базиса Грёбнера.

Следствие 2.6 (Условие принадлежности идеалу). *Пусть* $G = \{g_1, \dots, g_s\}$ – *базис Грёбнера идеала* $I \subset k[x_1, \dots, x_n]$, *и пусть* $f \in k[x_1, \dots, x_n]$. *Тогда* $f \in I$ *в том и только том случае, когда остаток от деления полинома* f *на* G *равен нулю.*

Доказательство. Если остаток равен нулю, то $f \in I$. В обратную сторону, пусть $f \in I$. Тогда равенство $f = f + 0$ удовлетворяет обоим условиям предложения 2.6. Из единственности представления полинома f в таком виде следует, что 0 является остатком от деления f на G. ■

Это следствие позволяет нам построить алгоритм принадлежности к идеалу: необходимо найти остаток от деления полинома на базис Грёбнера идеала. Построение этого базиса будет обсуждено в следующих параграфах.

Определение 2.15. *Остаток от деления полинома f на упорядоченный* ***s****-набор $F = (f_1, \dots, f_s)$ будет обозначаться $\bar{f}^F$. Если F является базисом Грёбнера идеала $(f_1, \dots, f_s)$, то по предложению 2.6 его можно рассматривать как (неупорядоченное) множество.*

Определение 2.16. *Пусть $f, g \in k[x_1, \dots, x_n]$ – ненулевые полиномы.*

i) Пусть $multideg(f) = \alpha$ и $multideg(g) = \beta$. Положим $\gamma = (\gamma_1, \dots, \gamma_n), \gamma_i = \max(\alpha_i \beta_i)$ для любого i. Тогда x^γ – называется ***наименьшим общим кратным*** *мономов $LM(f)$ и $LM(g)$. Используется обозначение $x^\gamma = \text{НОК}(LM(f), LM(g))$.*

ii) ***S-полиномом*** *от f и g называется комбинация*

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

Заметим, что в знаменателе стоят не мономы, а старшие члены. S-полином $S(f, g)$ «сконструирован» таким образом, чтобы было удобно сокращать старшие члены.

Лемма 2.7. *Рассмотрим сумму $\sum_{i=0}^{s} c_i f_i$, где $multideg(f_i) = \delta \in \mathbb{Z}_{\geq 0}^n$, а $c_i \in k$ для всех i. Если $multideg(\sum_{i=0}^{s} c_i f_i) < \delta$, то $\sum_{i=0}^{s} c_i f_i$ является линейной комбинацией с коэффициентами в k S-полиномов $S(f_i, f_l), 1 \leq j, l \leq s$. Более того, мультистепень каждого $S(f_i, f_l)$ меньше δ.*

Если $f_1, \dots, f_s$ удовлетворяют условиям леммы 2.7, то

$$\sum_{i=0}^{s} c_i f_i = \sum_{j,l} c_{jl} S(f_j f_l).$$

Используя S-полиномы и лемму 2.7 мы можем теперь доказать критерий Бухбергера о том, что базис идеала является базисом Грёбнера.

4. Критерий Бухбергера.

Теорема 2.4. *Пусть I – некоторый полиномиальный идеал. Тогда базис $G = \{g_1, \dots, g_s\}$ – базис идеала I является базисом Грёбнера в том и только том случае, когда для всех пар $i \neq j$ остаток от деления $S(g_i, g_j)$ на G (в любом порядке) равен нулю.*

Доказательство. $\Longrightarrow$. Пусть $f \in I$ – ненулевой полином. Мо должны доказать, что если остатки от деления всех S-полиномов на G равны нулю, то $LT(f) \in (LT(g_1), \dots, LT(g_s))$.

Так как $f \in I = (g_1, \dots, g_s)$, то существуют полиномы $h_i \in k[x_1, \dots, x_n]$, такие, что

$$f = \sum_{i=0}^{s} h_i g_i. \tag{2}$$

Из леммы 2.4 следует, что

$$multideg(f) \leq \max\big(multideg(h_i g_i)\big). \tag{3}$$

Если здесь нет равенства, то, следовательно, произошло сокращение старших членов в (2). Лемма 2.7 позволяет выразить это в терминах S-полиномов. Тогда наше условие, что S-полиномы на выражения с меньшим числом сокращений, то есть мы получаем выражения для f с меньшим числом сокращаемых старших членов. Продолжая этот процесс, мы в итоге получим выражение типа (2) для f, причем в (3) будет иметь место равенство. Тогда $multideg(f) = \max\big(multideg(h_i g_i)\big)$ для некоторого i, т.е. $LT(f)$ делится на некоторый $LT(g_i)$. Значит, $LT(f) \in (LT(g_1), \dots, LT(g_s))$, что и требуется доказать.

Рассмотрим (2). Пусть $m(i) = multideg(h_i g_i)$, и положим $\delta = \max(m(1), \dots, m(s))$. Теперь неравенство (3) имеет вид $multideg(f) \leq \delta$. Рассмотрим *все* способы, какими f может быть записано в виде (2). Для каждого способа мы буем иметь свое δ. Поскольку мономиальное упорядочение является вполне упорядочением, то мы можем выбрать такое выражение (2), для которого δ ***минимально***.

Покажем, что если δ минимально, то $multideg(f) = \delta$. Тогда в (3) имеет место равенство. Отсюда следует, что $LT(f) \in (LT(g_1), \dots, LT(g_s))$. Это доказывает теорему.

Осталось доказать, что $multideg(f) = \delta$. Мы докажем это от противного. Если равенство не имеет места, то $multideg(f) < \delta$. Перепишем (2) в следующем виде:

$$f = \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i$$
$$= \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \quad (4)$$

Мономы во второй и третьей суммах в самой правой части равенства имеют мультистепени $< \delta$. Поэтому предположение $multideg(f) < \delta$ означает, что первая сумма также имеет мультистепень $< \delta$.

Если $LT(h_i) = c_i x^{a(i)}$, то сумма:

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)=\delta} c_i x^{a(i)} g_i$$

Имеет в точности тот вид, который описан в условии леммы 2.7 с $f_i = c_i x^{a(i)} g_i$. Теперь из леммы 2.7 следует, что эта сумма есть линейная комбинация S-полиномов $S(x^{a(j)} g_j, x^{a(l)} g_l)$. Но

$$S\left(x^{a(j)} g_j, x^{a(l)} g_l\right) = \frac{x^\delta}{x^{a(j)} LT(g_j)} x^{a(j)} g_j - \frac{x^\delta}{x^{a(l)} LT(g_l)} x^{a(l)} g_l = x^{\delta - \gamma jl} S\left(g_j, g_l\right),$$

Где $x^{\gamma jl} = \text{НОК}\left(LM\left(g_j\right), LM(g_l)\right)$. Значит, существуют константы $c_{jl} \in k$, такие, что

$$\sum_{m(i)=\delta} LT(h_i) g_i = \sum_{m(i)=\delta} c_{jl} x^{\delta - \gamma jl} S\left(g_j, g_l\right). \quad (5)$$

Вспомним, что, согласно нашему предположению, остаток от деления $S\left(g_j, g_l\right)$ на $g_1, \dots, g_s$ равен нулю, т.е. каждый S-полином может быть записан в виде:

$$S\left(g_j, g_l\right) = \sum_{i=0}^{s} a_{ijl} g_l, \quad (6)$$

Где $a_{ijl} \in k[x_1, \dots, x_n]$. Из алгоритма деления также следует, что:

$$multideg(a_{ijl}g_l) \leq multideg\left(S(g_j, g_l)\right) \quad (7)$$

Для всех *i,j,l.* Значит, можно сказать, что если остаток равен нулю, то существует такое представление $S(g_j, g_l)$ в виде комбинации g_i, что старшие члены слагаемых этой комбинации не сокращаются.

Теперь умножим (6) на $x^{\delta-\gamma jl}$ и получим:

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

где $b_{ijl} = x^{\delta-\gamma jl}a_{ijl}$. Теперь из (7) и леммы 2.7 следует, что:

$$multideg(b_{ijl}g_l) \leq multideg\left(x^{\delta-\gamma jl}S(g_j, g_l)\right) \leq \delta. \quad (8)$$

Теперь подставляя полученное нами выражение для $x^{\delta-\gamma jl}S(g_j, g_l)$ в (5), получаем равенство:

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{m(i)=\delta} c_{jl}x^{\delta-\gamma jl}S(g_j, g_l) = \sum_{j,l} c_{jl}\left(\sum_i b_{ijl}g_i\right) = \sum_i \tilde{h}_i g_i.$$

Но по (8) для всех i

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

Теперь, для завершения доказательства, следует подставить равенство $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_i \tilde{h}_i g_i$ в (4) и получить выражение для f в виде полиномиальной комбинации полиномов g_i, где *все* члены имеют мультистепень $< \delta$. Этот факт противоречит минимальности δ. ■

Таким образом, примененяя критерий Бухбергера мы можем легко устанавливать, является данный базис базисом Грёбнера или нет.

Упражнение. Определить, являются ли следующее множество базисом Грёбнера для идеала, который он порождает.

$G = \{x^2 - y, x^3 - z\}$, *grlex*-упорядочение.

Решение.

Пусть I – некоторый идеал. Тогда базис $G = \{g_1, \dots, g_s\}$ идеала I является базисом Грёбнера в том и только том случае, когда для всех пар $i \neq j$ остаток от деления $S(g_i, g_j)$ в любом порядке на G равен нулю.

$LT(f_1) = x^2, (2,0,0), multideg(f_1) = 2;$

$LT(f_2) = x^3, (3,0,0), multideg(f_2) = 3;$

$\gamma = (3,0,0), X^\gamma = x^3.$

$S(f_1, f_2) = \frac{x^3}{x^2} \cdot (x^2 - y) - \frac{x^3}{x^3} \cdot (x^3 - z) = x \cdot (x^2 - y) - 1 \cdot (x^3 - z) = -xy + z.$

$-xy + z = 0 \cdot f_1 + 0 \cdot f_2 - xy + z \Longrightarrow G = \{x^2 - y, x^3 - z\}$ не является базисом Грёбнера.

$G' = \{y^3 - z^2, -y^2 + xz, xy - z, x^2 - y\}$ является базисом Грёбнера для идеала, порожденного G.

§6. Алгоритм Бухбергера.

В данном параграфе будет решаться следующая задача: как построить базис Грёбнера заданного идеала $I \in k[x_1, \dots, x_n]$?

Теорема 2.5. *Пусть дан некоторый ненулевой полиномиальный идеал* $I = (f_1, \dots, f_s)$. *Тогда базис Грёбнера для* I *может быть построен за конечное число шагов с помощью следующего алгоритма:*

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

Доказательство. Для начала введем удобные обозначения. Если $G = \{g_1, \dots, g_s\}$, то через (G) и $(LT(G))$ будем обозначать следующие идеалы:

$$(G) = (g_1, \dots, g_s),$$
$$(LT(G)) = (LT(g_1), \dots, LT(g_s)).$$

Докажем, что условие $G \subset I$ выполняется на каждом шаге алгоритма. Это верно в начале работы алгоритма. Далее, при каждом расширении множества G мы добавляем остаток $\overline{S(p,q)}^{G'}$, где $p, q \in G$. Если $G \subset I$, то p, q и $S(p,q)$ принадлежат I. А так как мы делим на $G' \subset I$, то и остаток S принадлежит I; следовательно $G \cup \{S\} \subset I$. Кроме того, G содержит исходный базис F, а значит, является базисом идеала I.

Алгоритм закончит работу, когда $G = G'$, т.е. когда $\overline{S(p,q)}^{G'} = 0$ для всех $p, q \in G$. Следовательно, G является базисом Грёбнера для $I = \langle G \rangle$ по теореме 2.4.

Осталось только доказать, что алгоритм в какой-то момент остановится. Во время выполнения каждого основного цикла множество G состоит из G' (старое G) и ненулевых остатков от деления S-полиномов от элементов из G' на G', т.е.

$$\langle LT(G') \rangle \subset \langle LT(G) \rangle, \qquad (1)$$

так как $G' \subset G$. Мы утверждаем, что если $G' \neq G$, то $\langle LT(G') \rangle$ строго меньше, чем $\langle LT(G) \rangle$. Докажем это. Пусть ненулевой остаток r от деления S-полиномов на G' был добавлен к G. Тогда, так как r – остаток, $LT(r)$ не делится

ни на один старший член элемента из G', т.е. $LT(r) \notin \langle LT(G')\rangle$. Однако $LT(r) \in \langle LT(G)\rangle$.

По (1) идеалы $\langle LT(G')\rangle$, которые получаются в результате последовательных выполнений основного цикла, образуют возрастающую цепь в $k[x_1, \dots, x_n]$. Тогда условие обрыва возрастающих цепей утверждает, что эта цепь стабилизируется, т.е. условие $\langle LT(G')\rangle = \langle LT(G)\rangle$ станет выполнятся после конечного числа итераций основного цикла. Это означает, что условие $G = G'$ станет выполняться и алгоритм остановится через конечное число шагов. ■

Лемма 2.8. *Пусть G – базис Грёбнера полиномиального идеала I, и пусть $p \in G$, $LT(p) \in \langle LT(G - \{p\})\rangle$. Тогда $G - \{p\}$ также является базисом Грёбнера для I.*

Доказательство. Нам известно, что $\langle LT(G)\rangle = \langle LT(I)\rangle$. Если $LT(p) \in \langle LT(G - \{p\})\rangle$, то $\langle LT(G - \{p\})\rangle = \langle LT(G)\rangle$. Значит, $G - \{p\}$ является базисом Грёбнера по определению. ■

Подберём константы и сделаем все старшие коэффициенты единицами, а также исключим из G все p, такие, что $LT(p) \in \langle LT(G - \{p\})\rangle$. В результате мы получим *минимальный* базис Грёбнера.

Определение 2.17. *Минимальным базисом Грёбнера полиномиального идеала I называется его базис Грёбнера G, такой, что*

i) $LC(p) = 1$ *для всех* $p \in G$;
ii) $LC(p) \notin (LT(G - \{p\}))$ *для всех* $p \in G$.

Идеал может иметь не только один минимальный базис Грёбнера. Поэтому введем понятие редуцированного базиса Грёбнера.

Определение 2.18. *Редуцированным базисом Грёбнера полиномиального идеала I называется его базис Грёбнера G, такой, что*

i) $LC(p) = 1$ *для всех* $p \in G$;
ii) никакой моном никакого $p \in G$ *не пренадлежит* $(LT(G - \{p\}))$.

Редуцированные базисы обладают следующим полезным свойством.

Предложение 2.7. *Пусть $I \neq \{0\}$ – полиномиальный идеал, и пусть задано некоторое мономиальное упорядочение. Тогда существует единственный редуцированный базис Грёбнера идеала I.*

Доказательство. Пусть G – некоторый минимальный базис Грёбнера для I. Элемент $g \in G$ будем называть ***редуцированным*** для G, если ни один моном из g не принадлежит $(LT(G - \{p\}))$. Будем преобразовывать G до тех пор, пока все его элементы не станут редуцированными.

Сначала отметим, что если g редуцирован для G, то g редуцирован для любого другого минимального базиса Грёбнера (идеала I), содержащего g и имеющего то же множество старших членов. Данное утверждение справедливо, поскольку определение редуцированности оперирует только старшими членами.

Пусть $g \in G$. Положим $\overline{g}^{G-\{g\}}$ и $G' = (G - \{g\}) \cup \{g'\}$. Мы утверждаем, что G' также является минимальным базисом Грёбнера для I. Чтобы доказать это, сначала отметим, что $LT(g') = LT(g)$. Поэтому $(LT(g')) = (LT(g))$. Поскольку $G' \subset I$, то G' - базис Грёбнера для I (минимальность очевидна). В конце концов, g' редуцирован для G' по построению.

Таким образом мы преобразуем каждый элемент из G. Теперь стоит отметить, что базис Грёбнера может изменяться при каждом преобразовании, но как только элемент стал редуцированным, то при дальнейших преобразованиях элементов из G он и останется таковым (так как старший член не меняется). В конечном итоге мы получим редуцированный базис Грёбнера.

Докажем единственность. Пусть G и $\tilde{G}$ – редуцированные (а, значит, и минимальные) базисы Грёбнера для I. Минимальные базисы идеала I имееют одно и то же множество старших членов:

$$LT(G) = LT(\tilde{G}).$$

Таким образом, для данного $g \in G$ найдется $\tilde{g} \in \tilde{G}$, такой, что $LT(g) = LT(\tilde{g})$. Если мы докажем, что из этого следует равенство $g = \tilde{g}$, то тем самым и равенство $G = \tilde{G}$, и единственность редуцированного базиса будут доказаны.

Рассмотрим разность $g - \tilde{g}$. Эта разность принадлежит I, а так как G – базис Грёбнера, то $\overline{g - \tilde{g}}^G = 0$. Но мы тоже знаем, что $LT(g) = LT(\tilde{g})$. Следовательно, старшие члены $g - \tilde{g}$ сократились, а оставшиеся члены не делятся ни на один элемент из $LT(G) = LT(\tilde{G})$, так как G и $\tilde{G}$ редуцированные. Поэтому $\overline{g - \tilde{g}}^G = g - \tilde{g} = 0$. ■

Как следствие данного предложения мы получаем ***алгоритм проверки равенства идеалов***: порождают ли два множества $\{g_1, \dots, g_s\}$ и $\{f_1, \dots, f_t\}$ один и тот же идеал? Чтобы дать ответ на этот вопрос достаточно задать мономиальное упорядочение и вычислить редуцированные базисы Грёбнера для $(g_1, \dots, g_s)$ и $(f_1, \dots, f_t)$. Идеалы совпадают в том и только том случае, когда совпадают их редуцированные базисы.

УПРАЖНЕНИЯ

Упражнение 2.1. Вычислить базисы Грёбнера для следующих идеалов:

a) $I = (x^2y - 1, xy^2 - x)$;
b) $I = (x^2 + y, x^4 + 2x^2y + y^2 + 3)$;
c) $I = (x - z^4, y - z^5)$.

Использовать *lex*-упорядочение.

Решение.

а) $I = (x^2y - 1, xy^2 - x)$;

$LT(f_1) = x^2y, (2,1), multideg(f_1) = 3;$

$LT(f_2) = xy^2, (1,2), multideg(f_2) = 3.$

1. $G \coloneqq \{x^2y - 1, xy^2 - x\}$.
2. (f_1, f_2):
   $\gamma = (2,2), X^\gamma = x^2y^2$.
   $S(f_1, f_2) = \frac{x^2y^2}{x^2y} \cdot (x^2y - 1) - \frac{x^2y^2}{xy^2}(xy^2 - x) = y \cdot (x^2y - 1) - x \cdot (xy^2 - x) = x^2y^2 - y - x^2y^2 + x^2 = x^2 - y.$
3. $f_3 = x^2 - y; G \coloneqq G \cup \{f_3\}$.

4. $LT(f_3) = x^2, (2,0), multideg(f_3) = 2;$
   (f_1, f_3):
   $\gamma = (2,1), X^\gamma = x^2y.$
   $S(f_1, f_3) = \frac{x^2y}{x^2y} \cdot (x^2y - 1) - \frac{x^2y}{x^2}(x^2 - y) = x^2y - 1 - y \cdot (x^2 - y) = x^2y - 1 - yx^2 + y^2 = y^2 - 1.$
5. $f_4 = y^2 - 1, G \coloneqq G \cup \{f_4\}$. Заметим, что $f_2 = x \cdot f_4$, а значит, f_2 можно «выбросить» из G. Таким образом, на этом шаге $G = \{f_1, f_3, f_4\}$.
6. $LT(f_4) = y^2, (0,2), multideg(f_4) = 2$
   (f_1, f_4):
   $\gamma = (2,2), X^\gamma = x^2y^2.$
   $S(f_1, f_4) = \frac{x^2y^2}{x^2y} \cdot (x^2y - 1) - \frac{x^2y^2}{y^2}(y^2 - 1) = y \cdot (x^2y - 1) - x^2 \cdot (y^2 - 1) = x^2y^2 - y - x^2y^2 + x^2 = x^2 - y = f_3.$
7. (f_3, f_4):
   $\gamma = (2,2), X^\gamma = x^2y^2.$
   $S(f_3, f_4) = \frac{x^2y^2}{x^2} \cdot (x^2 - y) - \frac{x^2y^2}{y^2}(y^2 - 1) = y^2 \cdot (x^2 - y) - x^2 \cdot (y^2 - 1) = x^2 - y^3 = x^2 - y - y^3 + y = (x^2 - y) - y \cdot (y^2 - 1) = f_3 - y \cdot f_4.$

Таким образом, базис Грёбнера идеала $I = (x^2y - 1, xy^2 - x)$ имеет вид:

$$G = \{x^2y - 1, x^2 - y, y^2 - 1\}.$$

b) $I = (x^2 + y, x^4 + 2x^2y + y^2 + 3);$

$LT(f_1) = x^2, (2,0), multideg(f_1) = 2;$

$LT(f_2) = x^4, (4,0), multideg(f_2) = 4;$

1. $G \coloneqq \{x^2 + y, x^4 + 2x^2y + y^2 + 3\}.$
2. (f_1, f_2):
   $\gamma = (4,0), X^\gamma = x^4.$
   $S(f_1, f_2) = \frac{x^4}{x^2} \cdot (x^2 + y) - \frac{x^4}{x^4} \cdot (x^4 + 2x^2y + y^2 + 3) = -x^2y - y^2 - 3 = -y \cdot f_1 - 3.$
3. $f_3 = -x^2y - y^2 - 3; G \coloneqq G \cup \{f_3\}.$
4. $LT(f_3) = -x^2y, (2,1), multideg(f_3) = 3;$
   (f_1, f_3):

$\gamma = (2,1), X^{\gamma} = x^2y.$

$S(f_1, f_3) = \frac{x^2y}{x^2} \cdot (x^2 + y) - \frac{x^2y}{-x^2y} \cdot (-x^2y - y^2 - 3) = y^2 - y^2 - 3 = -3.$

5. $f_4 = -x^2y - y^2 - 3, G \coloneqq G \cup \{f_4\}.$
   $f_3 = -y \cdot f_1 - 3 = -y \cdot f_1 + f_4 + 0.$ Значит, $G \coloneqq G \backslash \{f_3\}.$
6. $LT(f_4) = -3, (0,0), multideg(f_3) = 0$
   (f_1, f_4):
   $\gamma = (2,0), X^{\gamma} = x^2.$
   $S(f_1, f_2) = \frac{x^2}{x^2} \cdot (x^2 + y) - \frac{x^2}{-3} \cdot (-3) = y.$
7. $f_5 = y, G \coloneqq G \cup \{f_5\}.$
8. $f_2 = x^4 + 2x^2y + y^2 + 3 = (x^2 + y) \cdot (x^2 + y) + 3 = (x^2 + y) \cdot f_1 - f_4.$
   Значит, $G \coloneqq G \backslash \{f_2\}.$
9. $LT(f_5) = y, (0,1), multideg(f_5) = 1.$
   (f_1, f_5):
   $\gamma = (2,1), X^{\gamma} = x^2y.$
   $S(f_1, f_5) = \frac{x^2y}{x^2} \cdot (x^2 + y) - \frac{x^2y}{y}(y) = y^2 = -y \cdot f_5 + 0.$
10. (f_4, f_5):
    $\gamma = (0,1), X^{\gamma} = y.$
    $S(f_4, f_5) = \frac{y}{-3}(-3) - \frac{y}{y}(y) = 0.$

Таким образом, базис Грёбнера идеала $I = (x^2 + y, x^4 + 2x^2y + y^2 + 3)$ имеет вид:

$$G = \{x^2 + y, -3, y\}.$$

c) $I = (x - z^4, y - z^5);$

$LT(f_1) = x, (1,0,0), multideg(f_1) = 1;$

$LT(f_1) = y, (0,1,0), multideg(f_2) = 1;$

1. $G \coloneqq \{x - z^4, y - z^5\}.$
2. (f_1, f_2):
   $\gamma = (1,1,0), X^{\gamma} = xy.$
   $S(f_1, f_2) = \frac{xy}{x} \cdot (x - z^4) - \frac{xy}{y} \cdot (y - z^5) = y \cdot (x - z^4) - x \cdot (y - z^5) =$
   $xz^5 - yz^4.$

3. $f_3 = xz^5 - yz^4; G \coloneqq G \cup \{f_3\}$.
4. $LT(f_3) = xz^5, (1,0,5), multideg(f_3) = 6;$
   (f_1, f_3):
   $\gamma = (1,0,5), X^\gamma = xz^5.$
   $S(f_1, f_3) = \frac{xz^5}{x} \cdot (x - z^4) - \frac{xz^5}{xz^5} \cdot (xz^5 - yz^4) = z^5 \cdot (x - z^4) - 1 \cdot$
   $(xz^5 - yz^4) = yz^4 - z^9 = z^4(y - z^5) = z^4 \cdot f_2 + 0.$
5. (f_2, f_3):
   $\gamma = (1,1,5), X^\gamma = xyz^5.$
   $S(f_2, f_3) = \frac{xyz^5}{y} \cdot (y - z^5) - \frac{xyz^5}{xz^5}(xz^5 - yz^4) = xz^5 \cdot (y - z^5) - y \cdot$
   $(xz^5 - yz^4) = -z^5 \cdot f_3 + yz^4 + 0.$

Таким образом, базис Грёбнера идеала $I = (x - z^4, y - z^5)$ имеет вид:

$$G = \{x - z^4, y - z^5, xz^5 - yz^4\}.$$

Глава 3. Применения базисов Грёбнера

§1. Теоремы об исключении и продолжении.

Определение 3.1. *Пусть дан идеал* $I = (f_1, \dots, f_n) \subset k[x_1, \dots, x_n]$. *Тогда* l*-м* ***исключающим идеалом*** I_l *называется идеал в* $k[x_{l+1}, \dots, x_n]$, *равный*

$$I \cap k[x_{l+1}, \dots, x_n].$$

Теорема 3.1 (об исключении). *Пусть* $I \subset k[x_1, \dots, x_n]$ *– идеал и* G *– его базис Грёбнера по отношению к* lex*-упорядочению с* $x_1 > x_2 > \dots > x_n$. *Тогда для любого* $0 \leq l \leq n$ *множество*

$$G_1 = G \cap k[x_{l+1}, \dots, x_n]$$

является базисом Грёбнера l*-го исключающего идеала* I_l.

Доказательство. Зафиксируем l в интервале между 0 и n. Так как $G_l \subset I_l$ по построению, то достаточно доказать, что

$$\big(LT(I_l)\big) = (LT(G_l))$$

(по определению базиса Грёбнера). Включение в одну сторону очевидно. Для доказательства другого включения $\big(LT(I_l)\big) \subset (LT(G_l))$ нам достаточно доказать, что старший член $LT(f)$, где f – произвольный полином из I_l, делится на некоторый старший член $LT(g)$ для некоторого $g \in G_l$.

Докажем это. Сначала отметим, что f принадлежит тоже и I, *т.е.* $LT(f)$ делится на $LT(g)$ для некоторого $g \in G$ (так как G является базисом Грёбнера идеала I). Так как $f \in I_l$, то $LT(g)$ содержит только переменные $x_{l+1}, \dots, x_n$. Решающее замечание: так как используется lex-упорядочение с $x_1 > \dots > x_n$, то любой моном, содержащий хотя бы одну из переменных $x_1, \dots, x_l$, больше всех мономов из $k[x_{l+1}, \dots, x_n]$. Значит из включения $LT(g) \in k[x_{l+1}, \dots, x_n]$ следует, что $g \in k[x_{l+1}, \dots, x_n]$. Значит, $g \in G_l$. ■

Теорема 3.2 (о продолжении). *Пусть* $I = (f_1, \dots, f_s) \subset \mathbb{C}[x_1, \dots, x_n]$, *и пусть* I_1 *– первый исключающий идеал для* I. *Для каждого* $1 \leq i \leq s$ *запишем* f_i *в виде*

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

где $N_i \geq 0$, *а* $g_i \in \mathbb{C}[x_2, \dots, x_n]$ *– ненулевые полиномы. Рассмотрим частичное решение* $(a_2, \dots, a_n) \in V(I_1)$. *Тогда если* $(a_2, \dots, a_n) \notin V(g_1, \dots, g_s)$, *то существует* $a_1 \in \mathbb{C}$, *такое, что* $(a_1, a_2, \dots, a_n) \in V(I)$.

§2. Суммы, произведения и пересечения идеалов.

1. Суммы идеалов.

Определение 3.2. *Пусть* I и J *– идеалы кольца* $k[x_1, \dots, x_n]$. ***Сумма*** $I + J$ *идеалов* I и J *– это множество*

$$I + J = \{f + g : f \in I \text{ и } g \in J\}.$$

Предложение 3.1. *Если* I и J *– идеалы в* $k[x_1, \dots, x_n]$, *то* $I + J$ *также идеал в* $k[x_1, \dots, x_n]$, *причем* $I + J$ *– это наименьший идеал, содержащий* I и J. *Кроме того, если* $I = (f_1, \dots, f_r)$ *и* $J = (g_1, \dots, g_s)$, *то*

$$I + J = (f_1, \dots, f_r, g_1, \dots, g_s).$$

Доказательство. Для начала, $0 = 0 + 0 \in I + J$. Далее, пусть $h_1, h_2 \in I + J$. Тогда $h_1 = p_1 + q_1, h_2 = p_2 + q_2$, где $p_1, p_2 \in I$ и $q_1, q_2 \in J$. Имеем $h_1 + h_2 = (p_1 + q_1) + (p_2 + q_2) = (p_1 + p_2) + (q_1 + q_2) \in I + J$, так как $p_1 + p_2 \in I$ и $q_1 + q_2 \in J$ по определению идеала. Пусть теперь $h \in I + J$, а $l \in k[x_1, \dots, x_n]$ – произвольный полином. Тогда $h = f + g$, где $f \in I$, $g \in J$. Имеем $l \cdot h = l \cdot (f + g) = l \cdot f + l \cdot g \in I + J$, так как $l \cdot f \in I$ и $l \cdot g \in J$ по определению идеала. Таким образом $I + J$ – идеал.

Если H – некоторый идеал, содержащий I и J, то H содержит все элементы $f \in I$ и все элементы $g \in J$. Так как H – идеал, то он содержит все суммы $f + g$. Значит, $I + J \in H$. Таким образом, каждый идеал, содержащий I и J, обязан содержать и $I + J$, т.е. $I + J$ – наименьший из идеалов с этим свойством. Наконец, если $I = (f_1, \dots, f_r)$ и $J = (g_1, \dots, g_s)$, то идеал $(f_1, \dots, f_r, g_1, \dots, g_s)$ содержит I и J. Поэтому $I + J \subset (f_1, \dots, f_r, g_1, \dots, g_s)$. Обратное включение очевидно. Значит $I + J = (f_1, \dots, f_r, g_1, \dots, g_s)$. ■

Следствие 3.1. *Пусть* $f_1, \dots, f_r \in k[x_1, \dots, x_n]$. *Тогда*

$$(f_1, \dots, f_r) = (f_1) + \cdots + (f_r).$$

Теорема 3.3. *Пусть* I и J *– идеалы в* $k[x_1, \dots, x_n]$. *Тогда*

$$V(I + J) = V(I) + V(J).$$

2. Произведение идеалов.

Определение 3.3. *Пусть* I и J *– идеалы в* $k[x_1, \dots, x_n]$. *Тогда их* ***произведение*** $I \cdot J$ *– это идеал, порожденный всеми полиномами вида* $f \cdot g$ *где* $f \in I$ *и* $g \in J$.

Следовательно, произведение идеалов I и J – это множество:

$$I \cdot J = \{f_1 g_1 + \cdots + f_m g_m : f_1, \dots, f_m \in I, g_1, \dots, g_m \in J, m \geq 1\}.$$

Докажем, что это множество – идеал. Действительно, $0 = 0 \cdot 0 \in I \cdot J$. Очевидно, что если $h_1, h_2 \in I \cdot J$, то и $h_1 + h_2 \in I \cdot J$. Наконец, если $h = f_1 g_1 + \cdots + f_m g_m \in I \cdot J$ и p – произвольный полином, то

$$ph = (pf_1)g_1 + \cdots + (pf_m)g_m \in I \cdot J,$$

так как $pf_i \in I$ для всех $i, 1 \leq i \leq m$. Стоить отметить, что множество произведений не является идеалом – оно не замкнуто относительно сложения.

Предложение 3.2. *Пусть* $I = (f_1, \dots, f_r)$ *и* $J = (g_1, \dots, g_s)$. *Тогда* $I \cdot J$ *порождается множеством всех произведений образующих идеалов* I и J*:*

$$I \cdot J = (f_i g_i : 1 \leq i \leq r, 1 \leq j \leq s).$$

Доказательство. Очевидно, что идеал, порожденный произведениями $f_i g_i$, содержится в $I \cdot J$. Докажем обратное включение. Любой полином из $I \cdot J$ является суммой полиномов вида fg, где $f \in I$, $g \in J$. Но f и g могут быть выражены через образующие:

$$f = a_1 f_1 + \cdots + a_r f_r, \qquad g = b_1 g_1 + \cdots + b_r g_r,$$

где a_i, b_j – некоторые полиномы. Тогда fg и любая сумма полиномов этого вида есть сумма $\sum c_{ij} f_i g_j$, где $c_{ij} \in k[x_1, \dots, x_n]$. ■

Теорема 3.4. *Пусть I и J – идеалы в $k[x_1, \dots, x_n]$. Тогда $V(I \cdot J) = V(I) \cup V(J)$.*

Доказательство. Пусть $x \in V(I \cdot J)$. Тогда $f(x)g(x) = 0$ для всех $f \in I$ и всех $g \in J$. Если $f(x) = 0$, то $x \in V(I)$. Если $f(x) \neq 0$ для некоторого $f \in I$, то $g(x) = 0$ для всех $g \in J$. Значит $x \in V(J)$. В обоих случаях $x \in V(I) \cup V(J)$.

Пусть теперь $x \in V(I) \cup V(J)$. Тогда или $f(x) = 0$ для всех $f \in I$, или $g(x) = 0$ для всех $g \in J$. Значит, $h(x) = 0$ для всех $h \in I \cdot J$, т.е. $x \in V(I \cdot J)$. ■

3. Пересечение идеалов.

Определение 3.4. ***Пересечение*** *$I \cap J$ двух идеалов идеалов $I, J \in k[x_1, \dots, x_n]$ – это множество полиномов, принадлежащих и I, и J.*

Предложение 3.3. *Пусть I и J – идеалы в $k[x_1, \dots, x_n]$. Тогда $I \cap J$ – тоже идеал.*

Доказательство. Прежде всего, $0 \in I \cap J$, так как $0 \in I$ и $0 \in J$. Далее, пусть $f, g \in I \cap J$. Тогда $f + g \in I$, так как $f, g \in I$. Аналогично, $f, g \in J$, откуда $f + g \in I \cap J$. Пусть теперь $f \in I \cap J$ и h - произвольный полином из $k[x_1, \dots, x_m]$. Тогда $h \cdot f \in I$, так как $f \in I$, и I – идеал. Аналогично, $h \cdot f \in J$. Значит, $f \cdot g \in I \cap J$. ■

Теорема 3.5. *Пусть I и J – идеалы из $k[x_1, \dots, x_n]$. Тогда*

$$I \cap J = (tI + (1 - t)J) \cap k[x_1, \dots, x_n].$$

Пусть $I = (f_1, \dots, f_r)$ и $J = (g_1, \dots, g_s)$ – идеалы в $k[x_1, \dots, x_n]$. Тогда рассматриваем идеал:

$$I \cap J = (tf_1, \dots, tf_r, (1 - t)g_1, \dots, (1 - t)g_s) \subset k[x_1, \dots, x_n, t].$$

и находим его базис Грёбнера по отношению к *lex*-упорядочению, в котором $t > x_1 > x_2 > \cdots > x_n$. Тогда элементы этого базиса, не зависящие от t, образуют базис Грёбнера идеала $I \cap J$.

ПРИЛОЖЕНИЕ А

Псевдокод

Псевдокоды используются в математике и информатике для того, чтобы дать описание алгоритмам.

Алгоритм – это набор инструкций для выполнения определённых численных или символьных вычислений. Алгоритм имеет *вход* или *входные данные* (информацию, которую он обрабатывает), и *выход* – результат его вычислений. На каждом шаге очередная операция полностью определена текущим состоянием алгоритма. Алгоритм прекращает работу после конечного числа шагов.

Большинство алгоритмов содержит следующие специальные структурные компоненты:

- Структуры повторения (циклы);
- Структуры условного перехода.

Описание этих структур, а так же других компонентов, использованных в данной дипломной работе, будет приведено ниже.

1. Вход, выход, переменные, константы.

Вход и выход алгоритма указывается перед началом алгоритма. Входу и выходу в соответствии с правилами математических обозначений присваиваются имена. Иногда указывается тип данных (если не указан, считается, что тип данных понятен из контекста). Переменные также имеют свои имена, их типы определяются самим процессом вычисления. Булевые константы *true* и *false* используются для обозначения истинности или ложности утверждений.

2. Оператор присваивания.

Оператор *присваивания* является одним из наиболее часто встречаемых типов инструкций. Правило записи этого оператора:

$$< \text{переменная} > := < \text{выражение} >.$$

Перед присваиванием вычисляется выражение справа, если переменная хранила значение, оно стирается и заменяется результатом вычисления выражения.

3. Операторы цикла.

В представленных в работе алгоритмах используются 3 типа структур повторения.

$$WHILE < \text{условие} > DO < \text{действие} >.$$

Первая и наиболее часто встречаемая. «Действие» - это и есть последовательность инструкций, которая повторяется. «Условие» - утверждение, которое может быть истинным или ложным на каждом шаге алгоритма.

$$REPEAT < \text{действие} > UNTIL < \text{условие} >.$$

Вторая использованная в этой работе структура. Действие будет повторяться, пока условие ложно. Действие выполнится как минимум один раз.

$$FOR\ each\ s\ in\ S\ DO < \text{действие} >$$

Последняя структура повторения. Она означает «выполняй действие для каждого элемента $s \in S$». S – конечное множество объектов. Выполняется фиксированное количество раз (столько, сколько объектов в S).

4. Условный оператор.

В данной работе мы используем только один тип условного оператора, который записывается так:

$$IF < \text{условие} > THEN < \text{действие1} > ELSE < \text{действие2} >.$$

Если условие истинно в тот момент, когда выполняется IF, то выполняется «действие1» (один раз). В противном случае, выполняется «действие2» (тоже один раз). В некоторых случаях *опускается* $ELSE$ *и* «действие2». Тогда если условие IF ложно, ничего не выполняется.

Литература

1. Cox, Little, and O'Shea – “Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra”. (пер. с англ. – М.: Мир, 2000. - 687 с., ил.)
2. Аржанцев И. – “Лекции о базисах Гребнера” (ПГУ, г. Москва, 1998г.).
3. Adams W.W. – “An introduction to Gröbner bases” (1996г.).