**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

[Оглавление 2](#_Toc42887869)

[Реферат 3](#_Toc42887870)

[Глава 1. Идеалы, аффинные многообразия и связь между ними 6](#_Toc42887871)

[§1. Аффинные многообразия. 6](#_Toc42887872)

[1. Определение и свойства аффинных многообразий. 6](#_Toc42887873)

[§2. Идеалы. 7](#_Toc42887874)

[Глава 2. Базисы Грёбнера 9](#_Toc42887875)

[§1. Основные задачи об идеалах. 9](#_Toc42887876)

[§2. Упорядочение мономов в . 9](#_Toc42887877)

[1. Мономиальное упорядочение. 11](#_Toc42887878)

[2. Лексикографическое упорядочение. 12](#_Toc42887879)

[§3. Алгоритм деления. 16](#_Toc42887880)

[1. Алгоритм деления полинома от одной переменной. 16](#_Toc42887881)

[2. Основные следствия алгоритма деления в . 18](#_Toc42887882)

[3. Наибольший общий делитель полиномов. 19](#_Toc42887883)

[§4. Мономиальные идеалы и лемма Диксона. 26](#_Toc42887884)

[1. Определение и свойства мономиальных идеалов. 26](#_Toc42887885)

[2. Лемма Диксона. 27](#_Toc42887886)

[§5. Теорема Гильберта о базисе и базисы Грёбнера. 29](#_Toc42887887)

[1. Теорема Гильберта о базисе. 30](#_Toc42887888)

[2. Базисы Грёбнера. 31](#_Toc42887889)

[3. Свойства базисов Грёбнера. 32](#_Toc42887890)

[4. Критерий Бухбергера. 34](#_Toc42887891)

[§6. Алгоритм Бухбергера. 38](#_Toc42887892)

[Глава 3. Применения базисов Грёбнера 46](#_Toc42887893)

[§1. Теоремы об исключении и продолжении. 46](#_Toc42887894)

[§2. Суммы, произведения и пересечения идеалов. 47](#_Toc42887895)

[1. Суммы идеалов. 47](#_Toc42887896)

[2. Произведение идеалов. 48](#_Toc42887897)

[3. Пересечение идеалов. 49](#_Toc42887898)

[ПРИЛОЖЕНИЕ А 51](#_Toc42887899)

[Литература 53](#_Toc42887900)

# Реферат

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

Ключевые слова и понятия: *Идеал, Полином, Моном, Аффинное Мно-гообразие, Упорядочение, Алгоритм Деления, Базис Грёбнера, Алгоритм Бух-бергера.*

***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 не-которых задач, а так-же практическое применение их в качестве упражнений.

В первой главе дипломной работы рассмотрены понятия аффинных много-образий 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 вто-рой 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 приме-нении 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 старонкi.  
3 выкарыстаных крыніц інфармацыі.

Ключавыя словы і паняцці: *Iдэал, Паліном, Маном, Аффiнная Разнастай-насць, Упарадкаваньне, Алгарытм Дзялення, Базіс Гробнара, Алгарытм Бух-бергера.*

***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 ал-гарытмаў, якія дазваляюць прымяняць Базісы Гребнера да рашэнняў для нека-торых 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. Так-сама ў другой чале было разгледжана паняцце манамияльнага ўпарадкавання, уведзены паняцці базісаў Гребнера, прыведзены алгарытмы дзялення палiномаў 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 дак-ладныя і адпавядаюць ужо вядомым раней вынікамі. У якасці прыкладаў некаторых алгарытмаў, аўтарам работы ў якасці практыкаванняў былі выра-шаны 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.

# 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,*  *– полиномы в . Положим* *.*  *– называется* ***аффинным многообразием****, определен­ным полиномами .*

**Лемма 1.1** (Свойства аффинных многообразий). *Если* *- аффин­ные многообразия, то и также являются аффинными многообра­зиями*.

**Доказательство**. Пусть  и . Мы утвер­ждаем, что

1. Если точка принадлежит , то функции и в этой точке обращаются в нуль.
2. Если то все в этой точке обращаются в нуль; значит и все функции обращаются в нуль в . Таким образом,  
    и, аналогично, . Следовательно, . С другой стороны, пусть . Если эта точка принадлежит *V*, то все доказано, если же нет, то для некоторого . Поскольку функции обращаются в нуль в при всех *j*, то все в этой точке равны нулю. Значит, и

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

## §2. Идеалы.

**Определение 2.1**. *Подмножество называется идеалом, если выполнены следующие условия:*

1. *Если , то ;*
2. *Если и , то .*

**Лемма 2.1**. *Пусть принадлежат кольцу ; тогда множе­ство является идеалом в . Оно называется идеалом, порожденным полиномами , а полиномы – образующими этого идеала или его порождаю­щими элементами.*

**Доказательство**. Прежде всего, , поскольку . Пусть теперь , и . Тогда из равенств

вытекает, что – идеал.

Идеал может быть интепретирован на языке полиномиальных уравне­ний. Пусть . Рассмотрим следующую систему уравнений:

Из этих уравнений, с помощью обычных алгеб­раических преобразований, мы можем вывести другие. Так, например, если мы умножим первое уравнение на , второе – на и т.д., а затем сложим произве­дения, то получим уравнение:

которое является следствием уравнений первоначальной системы. Отме­тим, что левая часть этого уравнения принадлежит идеалу , т.е. идеал можно рассматривать в качестве множества всех «полиномиальных след­ствий» системы .

Идеал *I* называется ***конечно порожденным****,* если существуют полиномы , такие, что ; при этом множество полино­мов называется *базисом* идеала *I.*

**Определение 2.2.** *Пусть – аффинное многообразие. Положим*

*–* ***идеал****.*

**Лемма 2.2.** *Пусть – аффинное многообразие. Тогда – идеал, ко­торый мы будем называть идеалом многообразия V.*

**Доказательство**.Нулевой полином обращается в нуль на и на *V* в частности, так что . Пусть и . Пусть () – произвольная точка из *V.* Тогда

Отсюда следует, что *I(V)* - идеал.

# Глава 2. Базисы Грёбнера

## §1. Основные задачи об идеалах.

В этой главе мы рассмотрим следующие задачи:

1. *Задача описания идеала*. Является ли произвольный идеал   
    конечно порожденным? Или, другими словами, верно ли, что для некоторых ?
2. *Задача о принадлежности идеалу*. Пусть , и пусть задан идеал . Принадлежит ли полином *f* идеалу *I*? На геомет­рическом языке эту задачу можно сформулировать так: со­держится ли многообразие в многообразии ?
3. *Задача решения полиномиальных уравнений*. Описать множество реше­ний в системы полиномиальных уравнений:  
     
   Другими словами, это то же самое, что описать аффинное многообразие .
4. *Задача неявного представления*. Пусть *V –* подмножество в , которое задано па­раметрически:

Если – полиномы (или рациональные функции) от переменных , то *V* будет аффинным многообразием или его частью. Задача состоит в следу-ющем: задать *V* полиномиальными уравнениями от переменных .

## §2. Упорядочение мономов в .

Внимательное рассмотрение алгоритма деления в и алгоритма при-веде­ния 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:

Аналогично, когда мы приводим матрицы к ступенчатому виду, мы сис-тематически главные элементы, т.е. первые слева ненулевые элементы в стро-ках, обращаем в нуль. Переводя на язык линейных систем, это означает сле-дующий порядок перемен­ных:

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 и *n*-наборами (*n*-векторами) показателей степеней существует взаимно однозначное соответствие. Упорядочение, которое мы определим на , определит и упорядочение на множестве мономов: если на в , то мы будем гово­рить что .

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

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 , а – произвольный моном, то . В терминах векторов – показателей степеней это означает, что если в , то для лю­бого , .

Теперь мы можем дать определение.

### 1. Мономиальное упорядочение.

**Определение 2.3**. ***Мономиальным упорядочением*** *на*  *называ­ется любое бинарное отношение > на , обладающее следующими свой­ствами*:

1. > *является* ***линейным*** *(для любых можно однозначно определить одно из следующих отношений: , , ) упорядочением на .*
2. *Если и* ,  *то .*
3. *> вполне упорядочивает , т.е. любое непустое подмножество в имеет минимальный (наименьший) элемент (по соотношению к упорядо­чению >).*

**Лемма 2.3**.(условие вполне упорядоченности): *Упорядочение > на вполне упорядочивает это множество тогда и только тогда, когда каждая строго убывающая последовательность элементов из*

*обрывается.*

**Доказательство**. Докажем эквивалентное утверждение: > не является вполне упорядочением тогда и только тогда, когда существует бесконечная строго убывающая последовательность элементов из .

Если > не есть вполне упорядочение, то существует непустое подмноже­ство , которое не имеет минимального элемента. В качестве возь-мем произвольный элемент из *S.* Так как он не минимален, то в *S* найдется эле­мент . Так как не минимален, то в *S* найдется элемент . Продолжая этот процесс, мы получим бесконечную строго убывающую последовательность:

Обратно, если существует такая бесконечная строго убывающая после-дова­тельность, то множество является непустым подмно-же­ством в , которое не имеет минимального элемента, т.е. > не является вполне упорядочением.

В качестве примера мономиального упорядочения мы рассмотрим обычное упорядочение натуральных чисел из :

Все три условия определения 2.1 выполнены. Значит упорядочение мо­номов из 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 . Мы говорим, что , если самая левая ненулевая координата вектора положительна. Мы будем писать , если .*

Вот несколько примеров *lex*-упорядочения:

1. , так как
2. , так как
3. Обычный порядок переменных является *lex-*упорядочением. Так как

то .

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

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

**Предложение 2.1**. *Лексикографическое упорядочение на является моно­миальным упорядочением.*

**Доказательство**. (i) Тот факт, что – линейное упорядочение, прямо сле­дует из определения и из того, что обычное упорядочение на линейно.  
(ii) Пусть . Тогда самая левая ненулевая координата вектора . Пусть это, например, . Но и   
. Тогда , и самой левой ненулевой коор­динатой опять является .  
(iii) Предположим, что не является вполне упорядочением. Тогда по лемме 2.1 должна существовать строго убывающая бесконечная последовательность

элементов из . Докажем, что это невозможно.

По определению *lex-*упорядочения, первые координаты векторов образуют невозрастающую последова­тельность неотрицательных целых чисел. Так как вполне упорядочено, то эта последовательность «стабили-зируется», т.е. существует такое *k*, что первые координаты векторов одина-ковы при . Начиная с , будем рассматривать вторые (а затем третьи и т.д.) коорди­наты. Последовательность вторых координат векторов не воз­растает. Это значит, что она «стабилизируется». Продолжая это рас-суждение, мы мо­жем найти такое *l*, что у векторов равны все координаты. Зна­чит, это одинаковые векторы, что противоречит строгому убы-ванию последова­тельности.

При *lex-*упорядочении, переменная больше *любого монома*, который соде-ржит только меньшие переменные. Это не зависит от его степени. Так, при упо-рядочении мы имеем . В слу­чаях, когда нам будет необ-ходимо учитывать также степени мономов и сравнивать сначала именно степе-ни, мы будем это делать с помощью градуированного лексикографического упорядочения (сокращенно *grlex*-*упорядочения*).

**Определение 2.5** *(градуированное лексикографическое упорядочение). Пусть . Тогда мы говорим, что , если:*

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

Вот пример:

, так как .

**Определение 2.6** *(градуированное обратное лексикографическое упорядо­чение grevlex). Пусть . Тогда мы говорим, что , если  
или и самая правая ненулевая координата вектора отрица­тельна.*

**Пример**, так как .

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 , и пусть выбрано мономиаль­ное упорядочение >. С помощью мономиальных упорядочений мы можем однозначно упорядочить члены полинома в соответствии с >.

Пусть, например, Тогда:

1. При *lex*-упорядочении мы записываем полином в порядке убывания чле­нов так:
2. Запись при *grlex*-упорядочении:
3. Запись при *grevlex*-упорядочении:

**Определение 2.7.** *Пусть - ненулевой полином в , и пусть > - мономиальное упорядочение.*

1. ***Мультистепень*** *полинома f определяется так:  
     
   (максимум берется по отношению к >).*
2. ***Старший коэффицент*** *полинома f – это*
3. ***Старший моном*** *полинома f – это  
     
   (с коэффициентом 1).*
4. ***Старший член*** *полинома f – это*

Для примера, пусть , как и выше, и пусть > обозначает *lex*-упорядочение. Тогда:

**Лемма 2.4** (свойства мультистепени). *Пусть – ненуле­вые полиномы. Тогда* :

1. *Если , то   
   Если, кроме того, , то указанное неравен­ство становится равенством.*

## §3. Алгоритм деления.

### 1. Алгоритм деления полинома от одной переменной.

При работе с алгоритмами, мы будем использовать «псевдокод». Это об-легчит 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 – ненулевой полином,*

*где и (т.е. ). Тогда называется старшим членом полинома f и обозначается .*

Теперь мы можем дать описание алгоритма деления.

**Предложение 2.2** (алгоритм деления). *Пусть – ненулевой поли­ном. Тогда любой полином может быть записан в виде*

*где и либо , либо Более того, q и r определены однозначно, и имеется алгоритм для их вычисления.*

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

Докажем корректность алгоритма. Для начала, равенство выполняется при начальных значениях и . Далее, на каждом шаге после переопределения и это равенство должно выпол­нятся, потому что

Отметим, что выполнение оператора цикла WHILE … DO прекра­щается, когда утверждение «» становится ложным, т.е. когда или или . Когда алгоритм прекращает ра­боту, он выдает требуемые и .

Осталось доказать, что утвер­ждение между WHILE … DO в какой-то момент станет ложным и алгоритм остановится. Самым важ­ным тут является тот факт, что полином или равен нулю, или имеет степень, меньшую, чем степень полинома *r*. Докажем это. Пусть:

и пусть . Тогда:

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 .

**Следствие 2.1**. *Пусть*  *– ненулевой полином. Тогда он имеет в k не более чем корней.*

**Доказательство.** Применим индукцию по . Если , то *f –* ненулевая константа, и утверждение справедливо. Пусть утверждение выполня­ется для всех полиномов степени , и пусть *f* имеет степень . Если *f* не имеет корней в *k,* то утверждение доказано. Пусть теперь – корень поли­нома . Поделим *f* на . Тогда по предположению имеем  
, где , так как имеет степень один. Положив в этом равенстве , получим , т.е. , и, значит степень полинома *q* равна .

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

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

**Доказательство.** Пусть – некоторый идел. Если , то и утверждение доказано. Пусть теперь , и пусть – ненуле­вой полином минимальной степени (в множестве полиномов, содержащихся в *I*). Мы утверждаем, что . Включение очевидно, так как *I* - идеал. Рассмотрим теперь полином . В соответствии с алгоритмом деления,   
, где или , или . Так как *I* – идеал, то и, значит . Если , то , что противоречит вы­бору полинома *f*. Значит , т.е. , что доказывает равенство .

Теперь докажем единственность. Пусть . Так как , то для некоторого полинома *h*. Имеем

т.е. . Аналогично получаем, поменяв местами , что , т.е. . Из равенства следует, что . Значит, - ненулевая константа.

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

### 3. Наибольший общий делитель полиномов.

**Определение 2.9**. *Наибольшим общим делителем полиномов называется полином h, такой, что*

1. *h делит и , и ;*
2. *если p – некоторый полином, который делит и , и , то р делит h.*

Наибольший общий делитель будет обозначаться через *.* В следующем предложении сформулированы основ­ные свойства наибольших общих делителей.

**Предложение 2.3**. *Пусть Тогда*

1. НОД *существует и единственен с точностью до умножения на нену­левую константу из k;*
2. НОД *является образующим идеала ;*
3. *существует алгоритм для вычисления* НОД*.*

**Алгоритм Евклида** позволяет вычислить наибольший общий делитель двух полиномов в .

Введём необходимые определения. Пусть , . За­пишем в виде , где *q* и *r* определены, как в предложении 1.1. Тогда *r* называется остатком от деления . Теперь мы можем дать описание алго­ритма Евклида:

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 алгоритма. На каждом шаге алгоритма . Работа алгоритма должна прекратиться, так как сте­пени полинома *s* уменьша-ются и в некоторый момент *s*  станет равным нулю. В момент остановки алго-ритма , т.е. .

**Определение 2.10**. ***Наибольшим общим делителем*** *полиномов называется полином h, такой, что*

1. *h делит ;*
2. *если p – некоторый полином, который делит , то р делит h.*

Такой полином *h* обозначается через *.* В следующем предложении сформулированы его основ­ные свойства.

**Предложение 2.4**. *Пусть , . Тогда*

1. *существует и определен однозначно с точностью до умно­жения на ненулевую константу из k;*
2. *порождает идеал ;*
3. *Если , то ;*
4. *существует алгоритм для вычисления .*

**Доказательство.** Доказательство пп. (*i*) и (*ii*) аналогично доказательству тех же пунктов предложению 2.4. Докажем (*iii*). Пусть .   
Тогда

Из (*ii*) следует, что

Для доказания существования алгоритма, вычисляющего , нужно объединить п.(*iii*) и алгоритм Евклида.

4. Алгоритм деления в .

Выше мы рассматрели алгоритм деления для полиномов от одной пере­менной. Он может быть применен для решения задачи о принадлежности иде­алу. Если , то, для того, чтобы узнать, принадлежит идеалу или нет, мы делим :

где и или . Мы доказали, что в том и только том случае, когда . 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 на общий случай полиноми­ального кольца . Наша цель – научиться делить полином на полиномы . Это означает научиться представлять в виде

где «частные» и остаток *r* принадлежат . Чтобы кор­ректно определить остаток, тут будут использованы мономиальные упорядоче­ния.

**Теорема 2.1** (Алгоритм деления в ). *Зафиксируем некоторое мо­номиальное упорядочение > на , и пусть – упорядоченный s-набор полиномов из Тогда любой полином мо­жет быть записан в виде*

*где и или , или r - есть линейная комбинация моно­мов (с коэффициентами из k, ни один из которых не делится ни на один из старших членов . Мы называем r* ***остатком*** *от деления поли­нома f на F. Более того, если , то*

**Доказательство**. Ниже приведено формальное описание алгоритма:

В этом алгоритме переменная *p* на каждом шаге выполняет роль промежу­точного делимого, переменная *r* выполняет роль остатка, а переменные выполняют роль частных. Логическая переменная «естьделение» гово­рит нам, делится ли старший член промежуточного переменного на какой-либо из . Каждый раз, когда мы находимся в главном цикле мо­жет произойти ровно одно из двух событий:

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

Для проверки корректности алгоритма, сначала докажем, что равен­ство  
 выполняется на каждом шаге. Очевидно, что оно вы­полнено для начальных значений . Пусть на некотором шаге оно имеет место. Если следующим является шаг деления, то некоторый делит и равенство  
показывает, что сумма 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

И опять равенство выполняется на следующем шаге.

Далее, обратим внимание, что алгоритм прекращает работу, когда . В этом случае

Так как к *r* добавлялись только такие члены, которые не делятся ни на один из , то это означает, что 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:

Согласно свойству мультистепени мы имеем:

так что *р* и имеют одинаковые старшие члены. Следовательно, их разность имеет строго меньшую мультистепень (если ). Пусть теперь *р* меняется в ходе шага вычисления остатка:

Очевидно, что здесь , 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 Каждый член полинома равен для некоторого значения переменной *р.* Началь­ное значение *p* есть *f*, и мы только что доказали, что мультистепень *p* строго убывает; значит, . Таким образом , если .

**Пример**. Рассмотрим полином:

при *lex-*упорядочение с .

Применим алгоритм деления из теоремы 2.1 и поделим на

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

Будем записывать делители частные и *r* в отдельный столбец:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | |  |
|  | | | |  |
|  | | |
|  | | |
|  | | |
|  | | |
|  |  | | |  |
|  |  | | |  |
|  |  | | |
|  |  | | |
|  |  |  | |
|  |  |  | |
|  |  |  | |

В результате получаем:

## §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* *называется* ***мономиальным****, если существует подмножество (которое может быть бесконеч­ным), такое, что I состоит из конечных сумм вида , где . Такой идеал I будет обозначаться через .*

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

**Лемма 2.5**. П*усть – мономиальный идеал. Тогда моном принадлежит I в том и только том случае, когда делится на некоторый мо­ном .*

**Доказательство.** Если делится на некоторый , то, по опреде-ле­нию мономиального идеала, . Докажем обратное. Пусть тогда , где , а . Если мы рассмотрим каж­дый член в равенстве справа делится на некоторый . Значит, и левая часть равенства, т.е. , обладает тем же свойством, так как моном содержится как член хотя бы в одном слагаемом .

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

**Лемма 2.6**. *Пусть I – некоторый мономиальный идеал, а . Тогда следующие условия эквивалентны:*

1. *;*
2. *каждый член полинома принадлежит I;*
3. *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 может быть представлен в виде , где . В частности, I имеет конечный базис.*

**Доказательство**. Доказательство проводится с помощью индукции по *n* - числу пе­ременных. Если , то *I* порожден мономами , где . Пусть – наибольший элемент в Тогда для всех имеем . Таким обра­зом, делит все образующие , т.е. .

Пусть и теорема справедлива для . Обозначим переменные че­рез , так что мономы в будут записаны в виде , где , а .

– мономиальный идеал. Рассмотрим идеал  
 , порожденный такими мономами , что для некото­рого . Так как – мономиальный идеал в , то по пред­положению индукции он конечно порожден, . Идеал может юыть рассмотрен , как «проекция» идеала в .

По определению для каждого , существует такое, что . Допустим *m –* наибольшее из . Для каждого , рас­смотрим идеал , порожденный такими мономами , что . Неформально можно сказать, что – это «срез» идеала , порожден­ный мономами, которые содержат *y* точно в степени *l.* По предположению ин­дукции,конечно порожден,

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

Докажем, что каждый моном в *I* делится хотя бы на один моном из списка. Пусть . Если , то по определению моном делится на некото­рый моном . С другой же стороны, если , то по определе­нию идеала моном делится на некоторый моном 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, . Тогда . Нам нужно доказать, что , где . Поскольку , то по лемме 2.5 каждый моном делится на некоторый моном , где . Теперь очевидно, что   
.

Лемма Диксона применяется для доказательства следующего важного утверждения о мономиальных упорядочениях на .

**Следствие 2.4**. *Пусть > - некоторое отношение на удовлетворяющее следующим условиям:*

1. *> - линейное упорядочение на ;*
2. *если и , то .*

*Тогда > является вполне упорядочением в том и только том случае, когда для всех .*

**Доказательство.** . Пусть > является вполне упорядочением, и пусть – наименьший элемент в . Достаточно доказать, что . Если , то по (ii) мы можем прибавить к обеим частям и получить , что противоречит тому, что – наименьший элемент в .

. Пусть для всех , и пусть – некоторое непустое множество. Нам нужно доказать, что в существует наменьший элемент. Рас­смотрим мономиальный идеал . По лемме Диксона существуют мономы , такие, что . Пусть (в противном случае переименуем мономы). Мы утверждаем, что – наименьший элемент множества . Докажем это. Рассмотрим произволь­ный элемент . Тогда . По лемме 2.5 моном делится на некоторый моном , т.е. . Тогда и по (ii) мы имеем

Значит, – 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 – ненулевой идеал.*

1. *Обозначим через множество старших членов элементов из I, т.е.*
2. *Обозначим через идеал, порожденный элементами из*

Отметим важный момент в определении . Пусть *I* конечно порож­ден, . Тогда и могут быть *разными* идеа­лами. Конечно, ; поэтому .

Докажем, что является мономиалным идеалом.

**Предложение 2.5**. *Пусть – некоторый идеал. Тогда:*

1. *– мономиальный идеал;*
2. *существуют полиномы , такие, что*

**Доказательство**. (i) Старшие мономы элементов поро-ж­дают мономиальный идеал Так как отлича­ется от на ненулевой множитель из поля *k*, то этот идеал совпадает с идеа­лом . Следовательно, является мономиаль­ным идеалом.

(ii) Поскольку порожден мономами , , то по лемме Диксона для конечного набора . Так как отличается от на ненулевой множитель из поля *k,* то .

### 1. Теорема Гильберта о базисе.

Используя алгоритм деления и предложение 2.5 , мы можем дать доказательство ко­нечной порожденности *любого* полиномиального идеала. Пусть – некото­рый идеал, и пусть – его идеал старших членов. Также мы будем считать, что задано некоторое мономиальное упо-рядочение, используемое в алгоритме деления.

**Теорема 2.3** (Гильберта о базисе). *Каждый идеал явля­ется конечно порожденным, т.е. , где .*

**Доказательство**. Если , то порождающее множество состоит из единственного элемента – нулевого полинома. Если – ненулевой идеал, то порожда­ющее множество мы будем строить следующим образом. Из предложения 2.5 следует, что существуют полиномы , такие, что . Мы утверждаем, что .

Поскольку каждый принадлежит *I*, то . Пусть теперь – некоторый элемент. Применяя алгоритм деления, поделим на . В результате будет представлен в виде:

где ни один член полинома *r* нельзя поделить ни на один из . Мы утверждаем, что . Имеем:

Если , то . Тогда по лемме 2.5 должен делится хотя бы на один . Однако это противоречит определе­нию остатка. Значит , т.е.

Откуда следует, что .

### 2. Базисы Грёбнера.

**Определение 2.13**. *Пусть задано мономиальное упорядочение. Конечное подмножество элементов идеала I называется его* ***базисом Грёбнера*** *(или стандартным базисом), если*

Приведенное определение можно переформулировать следующим образом: множество 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 .

Из доказательства теоремы 2.3 вытекает следующий результат.

**Следствие 2.5**. *Пусть задано некоторое мономиальное упорядочение. То­гда любой ненулевой идеал обладает базисом Грёбнера. Более того, базис Грёбнера идеала является его базисом.*

**Доказательство**. Пусть – ненулевой идеал в – 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 , то , т.е. является бази­сом в .

**Упражнение**. Пусть используется grlex-упорядочение с . Верно ли, что множество является базисом Грёбнера? Объясните ваш ответ.

**Решение.**

*;*

*;*

*.*

Рассмотрим полином:

Очевидно, что . Значит, .

С другой же стороны, не делится ни на один из старших членов поли­номов . А именно, не делится ни на , ни на , ни на . Следовательно, имеем следующее:

В результате мы получаем, что . Но по определению ба­зисом Грёбнера является такое конечное подмножество элемен­тов идеала *I*, для которого

Значит, рассмотренное нами множество не является базисом Грёбнера.

### 3. Свойства базисов Грёбнера.

**Предложение 2.6**. *Пусть – базис идеала , и пусть . Тогда существует единственный полином , который обладает следующими свойствами:*

1. *ни один член полинома не делится ни на один из старших членов ;*
2. *существует , такой, что .*

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

**Доказательство**. Алгоритм деления позволяет нам записать *f*  в виде , где удовлетворяет условию (i). Условие (ii) тоже выпол­няется, поскольку . Существование полинома дока­зано.

Докажем единственность. Пусть , где удовле­творяют условиям (i), (ii). Тогда . Поэтому если , то . Тогда по лемме 2.5 де­лится на какой-то старший член . Но это невозможно в силу условия (i). Значит, , и единственность доказана.

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

Отметим, что хотя остаток и единственен, но «частные» , которые вычисляются алгоритмом деления в , зависят от по­рядка делителей даже в случае базиса Грёбнера.

**Следствие 2.6** (Условие принадлежности идеалу). *Пусть – базис Грёбнера идеала , и пусть . Тогда в том и только том случае, когда остаток от деления полинома на равен нулю.*

**Доказательство**. Если остаток равен нулю, то . В обратную сторону, пусть . Тогда равенство удовлетворяет обоим усло­виям предложения 2.6. Из единственности представления полинома в таком виде следует, что 0 является остатком от деления на *.*

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 на упорядоченный* ***s****-набор будет обозначаться . Если является базисом Грёб­нера идеала , то по предложению 2.6 его можно рассматривать как (неупорядоченное) множество.*

**Определение 2.16**. *Пусть – ненулевые полиномы.*

1. *Пусть и . Положим для любого i. Тогда – называется* ***наименьшим общим кратным*** *мономов и . Используется обозначение ,.*
2. ***S-полиномом*** *от называется комбинация*

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

**Лемма 2.7**. *Рассмотрим сумму , где , a для всех . Если , то является линейной комбинацией с коэффицентами в*  *S-полиномов . Более того, мультистепень каждого меньше .*

Если удовлетворяют условиям леммы 2.7, то

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 – базис идеала является базисом Грёбнера в том и только том случае, когда для всех пар остаток от деления (в   
любом порядке) равен нулю.*

**Доказательство**. Пусть – ненулевой полином. Мо должны дока­зать, что если остатки от деления всех S-полиномов на равны нулю, то .

Так как , то существуют полиномы , та­кие, что

Из леммы 2.4 следует, что

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 с меньшим числом сокращаемых стар­ших членов. Продолжая этот процесс, мы в итоге получим выраже­ние типа (2) для , причем в (3) будет иметь место равенство. Тогда для некоторого *i*, т.е. делится на не­который . Значит, , что и требуется дока­зать.

Рассмотрим (2). Пусть , и положим . Теперь нера­венство (3) имеет вид . Рассмотрим *все* способы, какими может быть записано в виде (2). Для каждого способа мы буем иметь свое . Поскольку мономиальное упорядочение является вполне упорядочением, то мы можем выбрать такое выражение (2), для которого ***минимально***.

Покажем, что если минимально, то . Тогда в (3) имеет место равен­ство. Отсюда следует, что . Это доказывает теорему.

Осталось доказать, что . Мы докажем это от противного. Если равенство не имеет места, то . Перепишем (2) в следую­щем виде:

Мономы во второй и третьей суммах в самой правой части равенства имеют мультистепени . Поэтому предположение означает, что первая сумма также имеет мультистепень .

Если , то сумма:

Имеет в точности тот вид, который описан в условии леммы 2.7 с . Теперь из леммы 2.7 следует, что эта сумма есть линейная комбина­ция S-полиномов . Но

Где Значит, существуют константы , та­кие, что

Вспомним, что, согласно нашему предположению, остаток от деле­ния на равен нулю, т.е. каждый S-полином может быть запи­сан в виде:

Где . Из алгоритма деления также следует, что:

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

Теперь умножим (6) на и получим:

где . Теперь из (7) и леммы 2.7 следует, что:

Теперь подставляя полученное нами выражение для в (5), получаем равенство:

Но по (8) для всех *i*

Теперь, для завершения доказательства, следует подставить равенство в (4) и получить выражение для *f* в виде полиноми-аль­ной комбинации полиномов , где *все*  члены имеют мультисте­пень . Этот факт противоречит минимальности .

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.

*grlex-*упорядочение.

**Решение**.

Пусть *I* – некоторый идеал. Тогда базис идеала *I* является бази­сом Грёбнера в том и только том случае, когда для всех пар остаток от деле­ния в любом порядке на равен нулю.

;

;

*.*

.

не является бази­сом Грёбнера.

является базисом Грёбнера для иде­ала, порожденного .

## §6. Алгоритм Бухбергера.

В данном параграфе будет решаться следующая задача: как построить базис Грёбнера заданного идеала ?

**Теорема 2.5**. *Пусть дан некоторый ненулевой полиномиальный идеал Тогда базис Грёбнера для может быть построен за конечное число шагов с помощью следующего алгоритма:*

**Доказательство**. Для начала введем удобные обозначения. Если   
, то через и будем обозначать следующие идеалы:

Докажем, что условие выполняется на каждом шаге алго­ритма. Это верно в начале работы алгоритма. Далее, при каждом расширении множества мы добавляем остаток , где . Если , то и принадлежат . А так как мы делим на , то и остаток принадле­жит ; следовательно . Кроме того, содержит исходный базис , а значит, является базисом идеала

Алгоритм закончит работу, когда , т.е. когда для всех . Следовательно, является базисом Грёбнера для по   
тео­реме 2.4.

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

так как . Мы утверждаем, что если , то строго меньше, чем . Докажем это. Пусть ненулевой остаток *r* от деления S-поли­номов на был добавлен к . Тогда, так как *r* – остаток, не делится ни на один старший член элемента из , т.е. . Однако .

По (1) идеалы , которые получаются в результате после-довательных вы­полнений основного цикла, образуют возрастающую цепь в . Тогда условие обрыва возрастающих цепей утверждает, что эта цепь стабилизируется, т.е. условие станет выполнятся после конечного числа итера­ций основного цикла. Это означает, что условие станет выпол­няться и алгоритм остановится через конечное число шагов.

**Лемма 2.8**. *Пусть – базис Грёбнера полиномиального идеала , и пусть . Тогда также является базисом Грёбнера для .*

**Доказательство**. Нам известно, что . Если , то . Значит, является бази­сом Грёбнера по определению.

Подберём константы и сделаем все старшие коэффициенты единицами, а также исключим из все , такие, что В результате мы получим *минимальный* базис Грёбнера.

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

1. *для всех ;*
2. *для всех .*

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

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

1. *для всех ;*
2. *никакой моном никакого не пренадлежит .*

Редуцированные базисы обладают следующим полезным свойством.

**Предложение 2.7**. *Пусть – полиномиальный идеал, и пусть задано некоторое мономиальное упорядочение. Тогда существует единственный ре­дуцированный базис Грёбнера идеала .*

**Доказательство**. Пусть – некоторый минимальный базис Грёбнера для . Элемент будем называть ***редуцированным***для *,* если ни один моном из не принадлежит . Будем преобразовывать до тех пор, пока все его элементы не станут редуцированными.

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

Пусть . Положим и . Мы утверждаем, что также является минимальным базисом Грёбнера для Чтобы доказать это, сначала отметим, что . Поэтому . Поскольку , то - базис Грёбнера для (минимальность очевидна). В конце концов, реду­цирован для по построению.

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

Докажем единственность. Пусть и – редуцированные (а, значит, и мини­мальные) базисы Грёбнера для . Минимальные базисы идеала имееют одно и то же множество старших членов:

Таким образом, для данного найдется , такой, что Если мы докажем, что из этого следует равенство , то тем самым и равенство , и единственность редуцированного базиса будут доказаны.

Рассмотрим разность . Эта разность принадлежит , а так как – ба­зис Грёбнера, то . Но мы тоже знаем, что . Следовательно, старшие члены сократились, а оставшиеся члены не делятся ни на один элемент из так как редуцированные. Поэтому .

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

**УПРАЖНЕНИЯ**

**Упражнение 2.1.** Вычислить базисы Грёбнера для следующих идеалов:

Использовать *lex*-упорядочение.

**Решение.**

;

;

.

1. .  
   .
2. ;  
   :  
   .  
   .
3. . Заметим, что , а значит, можно «вы­бросить» из . Таким образом, на этом шаге .
4. :  
   .  
   .
5. :  
   .  
      
   .

Таким образом, базис Грёбнера идеала имеет вид:

;

;

;

1. :  
   .  
   .
2. .
3. :  
   .  
   .
4. .  
    Значит, .
5. :  
   .  
   .
6. .
7. Значит, .
8. :  
   .  
   .
9. :  
   .  
   .

Таким образом, базис Грёбнера идеала имеет вид:

;

;

;

1. .
2. :  
   .  
   .
3. .
4. ;  
   :  
   .  
   .
5. :  
   .  
   .

Таким образом, базис Грёбнера идеала имеет вид:

# Глава 3. Применения базисов Грёбнера

## §1. Теоремы об исключении и продолжении.

**Определение 3.1**. *Пусть дан идеал . Тогда l-м* ***исключающим идеалом*** *называется идеал в , равный*

**Теорема 3.1** (об исключении). *Пусть – идеал и G – его ба­зис Грёбнера по отношению к lex-упорядочению с . Тогда для любого множество*

*является базисом Грёбнера l-го исключающего идеала .*

**Доказательство**. Зафиксируем *l* в интервале между 0 и *n.* Так как по построению, то достаточно доказать, что

(по определению базиса Грёбнера). Включение в одну сторону очевидно. Для доказательства другого включения нам достаточно дока­зать, что старший член , где – произвольный полином из , делится на некоторый старший член для некоторого .

Докажем это. Сначала отметим, что принадлежит тоже и *I, т.е.* де­лится на для некоторого (так как является базисом Грёбнера идеала *I*). Так как , то содержит только переменные . Решающее замечание: так как используется *lex*-упорядочение с , то любой моном, содержащий хотя бы одну из переменных , больше всех мономов из . Значит из включения следует, что . Значит, .

**Теорема 3.2** (о продолжении). *Пусть , и пусть – первый исклющающий идеал для . Для каждого запишем в виде*

*где , а – ненулевые полиномы. Рассмотрим частич­ное решение . Тогда если , то существует , такое, что .*

## §2. Суммы, произведения и пересечения идеалов.

### 1. Суммы идеалов.

**Определение 3.2**. *Пусть – идеалы кольца .* ***Сумма*** *идеалов – это множество*

**Предложение 3.1**. *Если – идеалы в , то также идеал в , причем – это наименьший идеал, содержащий . Кроме того, если и , то*

*.*

**Доказательство**. Для начала, . Далее, пусть . Тогда где . Имеем , так как и по определению идеала. Пусть теперь , а – произвольный полином. Тогда , где , . Имеем , так как и по опре­делению идеала. Таким образом – идеал.

Если – некоторый идеал, содержащий , то содержит все элементы и все элементы . Так как – идеал, то он содержит все суммы . Значит, . Таким образом, каждый идеал, содержащий , обязан содер­жать и , т.е. – наименьший из идеалов с этим свойством. Нако­нец, если и , то идеал содер­жит . Поэтому . Обратное включение очевидно.  
Значит .

**Следствие 3.1**. *Пусть . Тогда*

**Теорема 3.3**. *Пусть – идеалы в . Тогда*

*.*

### 2. Произведение идеалов.

**Определение 3.3**. *Пусть – идеалы в . Тогда их* ***произведе­ние***  *– это идеал, порожденный всеми полиномами вида где и .*

Следовательно, произведение идеалов – это множество:

Докажем, что это множество – идеал. Действительно, . Очевидно, что если , то и . Наконец, если и – произвольный полином, то

так как для всех . Стоить отметить, что множество произведе­ний не является идеалом – оно не замкнуто относительно сложения.

**Предложение 3.2**. *Пусть и . Тогда порож­дается множеством всех произведений образующих идеалов :*

**Доказательство**. Очевидно, что идеал, порожденный произведениями , содержится в . Докажем обратное включение. Любой полином из явля­ется суммой полиномов вида , где , . Но могут быть выра­жены через образующие:

где – некоторые полиномы. Тогда и любая сумма полиномов этого вида есть сумма , где .

**Теорема 3.4**. *Пусть – идеалы в . Тогда .*

**Доказательство**. Пусть . Тогда для всех и всех . Если , то . Если для некоторого , то для всех . Значит . В обоих случаях .

Пусть теперь . Тогда или для всех , или для всех . Значит, для всех , т.е. .

### 3. Пересечение идеалов.

**Определение 3.4**.***Пересечение***  *двух идеалов идеалов – это множество полиномов, принадлежащих и , и .*

**Предложение 3.3**. *Пусть и – идеалы в . Тогда – тоже идеал.*

**Доказательство**. Прежде всего, , так как и . Далее, пусть . Тогда , так как . Аналогично, , откуда   
. Пусть теперь и - произвольный полином из *.* Тогда *,* так как *,* и *–* идеал.Аналогично, . Зна­чит, .

**Теорема 3.5**. *Пусть и – идеалы из . Тогда*

Пустьи– идеалы в *.* Тогда рас­сматриваем идеал:

и находим его базис Грёбнера по отношению к *lex*-упорядочению, в кото­ром . Тогда элементы этого базиса, не зависящие от , обра­зуют базис Грёбнера идеала .

# 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 присваива-ются 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:

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.

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.

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

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

4. Условный оператор.

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

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