МИНИСТЕРСТВО ВЫСШЕГО И СРЕДНЕГО СПЕЦИАЛЬНОГО ОБРАЗОВАНИЯ РЕСПУБЛИКИ УЗБЕКИСТАН

САМАРКАНДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ имени АЛИШЕРА НАВОИ

На правах рукописи

УДК: 519.6

КАРИМОВА МАФТУНА АБДУРАУФОВНА

МЕТОД БАЗИСОВ ГРЕБНЕРА И ЕГО ПРИЛОЖЕНИЯ

5А130101 – Математика (по направлениям)

Д И С С Е Р Т А Ц И Я

на сосикание академической степени магистра

Работа рассмотрена на
заседании кафедры и
допущена к защите.
И.о.заведующий кафедрой
«Алгебры и геометрии»
доцент Г.А.Хасанов

_____

Научный руководитель
доцент У.Х.Нарзуллаев

_____

Самарканд 2015

СОДЕРЖАНИЕ

Введение

Подготовка высококвалифицированных кадров играет важную роль в развитии экономики и общества. Позитивные преобразования в сфере среднего и высшего образования, как отметил Президент Узбекистана И.А.Каримов [11], являются практическим воплощением политики реализации целенаправленных реформ. В этом отношении необходимо отметить постоянное внимание государства к среднему и высшему образованию, подготовке высококвалифицированных научных кадров, развитию информационных технологий.

Данная диссертационная работа посвящена изложению некоторых результатов бурно развивающийся области, связанной с алгоритмами, превращающими базисные понятия коммутативной алгебры и алгебраической геометрии из абстрактно-теоритических в конкретно вычислимые. Изучение алгоритмов основывается на обобщении алгоритма деления для полиномов от одной переменной, найденном лишь в шестидесятых годах 20 века.

Базисы Грёбнера идеалов в полиномиальных кольцах были открыты Б.Бухбергером в 1965 г. и названы им честь В.Грёбнера (1899-1980)-научного руководителя Бухбергера. Родственное понятие «стандартного базиса» идеала в кольце степенных рядов было независимо введено Х.Хиронакой в 1964 г. Как мы увидим далее, Бухбергер также разработал алгоритмы для работы с базисами Грёбнера. Термин «базис Грёбнера» используется в английском написании «Groebner base» в качестве команды в некоторых системах компьютерной алгебры.

Актуальность работы. Диссертационная работа на тему «Метод базисов Грёбнера и его приложения» посвящена изучению связей между алгебраическими свойствами полиномиальных колец $k[\, x_1, \ldots\ldots x_n\,]$ и геометрическими свойствами аффинных многообразий. В работе изучены базисы Грёбнера, которые позволяют решать алгоритмические задачи о полиноминальных идеалах. В работе сформулированы ряд проблем, касающихся алгебраических свойств полиномиальных идеалов и геометрии аффинных многообразий и успешно решены следующие задачи: задача о принадлежности идеалу; задача решения полиномиальных уравнений.

Цели и задачи исследования: Исследовать алгебраические свойства полиномиальных идеалов и геометрию аффинных многообразий, решить задачу о принадлежности идеалу, найти решения систем полиномиальных уравнений.

Степень изученности проблемы: В последние годы бурно развивается область, связанная с алгоритмами, превращающими базисные понятия коммутативной алгебры и алгебраической геометрии из абстрактно-теоретических в конкретно вычислимые. Речь идёт о способах явного нахождения объектов, существование которых устанавливается в ключевых утверждениях теории. Ответы на возникающие вопросы, удаётся получить за счет объединения классических методов, в последние десятилетия ушедшие в тень и современных идей, основанных на относительно новой теории базисов Грёбнера.

Научная новизна: Основные результаты являются новыми, важными и состоят в следующем:

- Показана связь между алгебраическими свойствами полиномиальных колец $k[\, x_1, \ldots \ldots . x_n\,]$ и геометрическими свойствами аффинных многообразий.
- Описан алгоритм деления в кольце $k[x_1, \ldots \ldots . x_n]$ в зависимости от упорядочения мономов.
- Описан алгоритм решения задачи о принадлежности идеалу.
- Найдены решения некоторых систем полиномиального уравнений, основанные на вычислении базисов Грёбнера по отношению к различным типам упорядочений.

Объект и предмет исследования: Объектом исследования являются базисы Грёбнера и их приложения. Предметом исследования являются полиномы в кольце $k[x_1, \ldots \ldots . x_n]$, а также системы полиномиальных уравнений.

Методы исследования: В работе используются методы алгебры полиномиальных колец, геометрии аффинных многообразий, метод базисов Грёбнера и компьютерных вычислений.

Основые положения, выносимые на защиту:

- Описан алгоритм решения задачи о принадлежности идеалу.
- Найдены решения некоторых систем полиномиальных уравнений.

Научная и практическая значимость результатов исследования:

Работа носит теоретический и практический характер. Результаты диссертации могут быть использованы в различных задачах о принадлежности идеалу, в решении систем нелинейных уравнений.

Апробация работы: Результаты диссертации докладывались на семинаре *«Методы степенной геометрии и компьютерной алгебры в исследовании алгебраических и дифференциальных уравнений»* под руководством профессоров А.Солеева и И.Икрамова (СамГУ 2013-2015 гг.)

- « Амалий математика ва ахборот хавфсизлиги» илмий-техник конференция, 2014
- Магистрантларнинг XIV илмий конференцияси, 2014
- Замонавий ахборот-коммуникация технологиялари, ТАТУ Самарканд филиали профессор- укитувчиларининг X илмий-амалий конференцияси, 2015

Опубликованность результатов: Основные результаты диссертации опубликованы в работах

1. Сеттарова Э.С., Каримова М.А., Задача о принадлежности идеалу;
2. Каримова М.А., Задача о принадлежности идеалу;
3. Нарзуллаев У.Х., Каримова М.А., Грёбнер базислари хакида;

Структура и объем диссертации: Диссертация состоит из введения, трех глав и списка литературы. Польный объем диссертации 70 страниц, библиография включает 34 наименований.

Во введении отражена история вопросов, рассмотренных в диссертации, и приведен обзор результатов, связанных с темой исследования. Кратко излагается содержание работы и формулируются основные результаты.

Первая глава «Идеалы и аффинные многообразия» посвящена изучению основных понятий алгебраической геометрии. Под геометрией мы здесь понимаем геометрию аффинных многообразий, которые являются точками, кривыми и поверхностями (а также объектами более высокой размерности), задаваемых полиномами. Понимание теории аффинных многообразий требует знания теории идеалов в кольцах полиномов $k[x_1, \dots \dots . x_n]$. А также мы рассматриваем полиномы от одной переменной, чтобы проиллюстрировать роль алгоритмов.

Во второй главе «Базисы Грёбнера» изучается упорядочение мономов в полиномиальном кольце от n переменных, алгоритм деления в $k[x_1, \dots \dots . x_n]$, мономиальные идеалы, лемма Диксона, теорема Гильберта о базисе, базисы Грёбнера, свойства базисов Грёбнера, алгоритм Бухбергера для вычисления базисов Грёбнера. Рассмотрение алгоритма деления в $k[x]$ и алгоритма приведения системы (или матрицы) к ступенчатому виду методом исключения Гаусса показывает, что понятие упорядочение членов полинома является ключевым в обоих алгоритмах. Поэтому обобщение алгоритмов деления и приведения к ступенчатому виду на случай произвольных полиномов от нескольких переменных должно базироваться на упорядочении членов полиномов из $k[x_1, \dots \dots . x_n]$.

В главе 1 было объяснено, как алгоритм деления для полиномов от одной переменной может быть применен для решения задачи о принадлежности идеалу. Для решения этой задачи в случае нескольких переменных необходимо было обобщить алгоритм деления в $k[x]$ на общий случай полиномиального кольца $k[x_1, \dots \dots . x_n]$. Научившись делить полином $f \in k[\, x_1, \dots \dots . x_n\,]$ на полиномы $f_1, \dots \dots f_s \in k[\, x_1, \dots \dots . x_n\,]$, мы смогли представить 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 $k[\, x_1, \dots \dots . x_n\,]$. Самое трудное в этом вопросе – это корректно определить остаток. Остаток не был определен однозначно, как это было в кольце полиномов от одной переменной, он менялся при изменении порядка делителей. Именно здесь были использованы мономиальные упорядочения и, с помощью системы компьютерной алгебры Maple 12, была написана программа, позволяющая делить полином от нескольких переменных на упорядоченную совокупность полиномов.

Далее была рассмотрена задача описания идеала для частного случая мономиальных идеалов. Для этого мы подробно изучили свойства таких идеалов и главным результатом явилось то, что все мономиальные идеалы конечно порождены (лемма Диксона). Эта же задача в общем случае решается с помощью переопределения базисов, образующих идеал. Для этого нам будет необходимо определить базисы с «хорошими» (по отношению к алгоритму деления) свойствами. Используя базисы Грёбнера удалось доказать конечную порожденность любого полиномиального идеала (теорема Гильберта о базисе). В следующем параграфе рассматриваются свойства базисов Грёбнера и особенно тот факт, что нежелательные свойства алгоритма деления в $k[x_1, \dots \dots . x_n]$ не проявляются, если делители образуют

базис Грёбнера (т.е. в этом случае остаток от деления определен однозначно). Также, используя алгоритм Бухбергера, научились строить базис Грёбнера любого заданного идеала $I \subset k[x_1, \dots \dots . x_n]$.

В третьей главе «Приложения базисов Грёбнера» решаются следующие задачи: задача о принадлежности идеалу, решение систем полиномиальных уравнений. Одновременное использование базисов Грёбнера и алгоритма деления дало нам алгоритм решения задачи о принадлежности идеалу. С помощью этого алгоритма нам удалось решить ряд интересных задач. Также техника базисов Грёбнера была применена для решения систем полиномиальных уравнений. Практика показывает, что вычисление базиса Грёбнера по отношению к lex-упорядочению существенно упрощает форму уравнений. В частности, мы получаем уравнения с последовательно исключенными переменными. Системы такого вида легко решаются, особенно если последнее уравнение зависит только от одной переменной. Полученные выводы теоретически основываются на теореме об исключении и теореме о продолжении.

Автор выражает глубокую благодарность кандидату физико-математических наук, доценту У.Х.Нарзуллаеву за постановку задачи и постоянное внимание при работе над диссертацией, а также ассистенту кафедры алгебры и геометрии Э.С.Сеттаровой за полезные обсуждения и замечания.

ГЛАВА 1

ИДЕАЛЫ И АФФИННЫЕ МНОГООБРАЗИЯ

§1. Полиномы и аффинные многообразия

Определение 1.1. *Мономом* от переменных x_1, x_2 ,…, x_n , называется произведение вида

$$x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n},$$

где показатели степеней α_1 ,α_2 ,…, α_n ,-неотрицательные целые числа.

Пример 1.1. $2x^3y^2z$-полная степень равна 6.

Для упрощения мономов будем пользоваться записью $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$ - набор n неотрицательных чисел. Положим $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$.

Отметим, что если α =(0,0,…,0), то x^α=1.

Через $|\alpha|=\alpha_1 +\alpha_2 +\dots+ \alpha_n$ мы будем обозначать *полную степень монома* x^α.

Определение 1.2. *Полином* f от переменных x_1, x_2 , …, x_n с коэффициентами из произвольного поля k называется конечная линейная комбинация мономов (с коэффициентами из k).
Полином f будет записываться в виде

$$f = \sum a_\alpha x^\alpha, a_\alpha \in k,$$

где суммирование производится по конечному множеству наборов

$\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n)$.

Множество всех полиномов от переменных x_1, x_2, …, x_n с коэффициентами из k обозначается $k[x_1, x_2, \dots, x_n]$.

Когда мы будем работать с полиномами от малого количества переменных, то обычно будем обходиться без индексов. Так, полиномы от одной, двух или трех переменных принадлежат множествам $k[x]$, $k[x,y]$, $k[x,y,z]$ соответственно. Например

$$f=2x^3y^2z+3/2y^3z^3-3xyz+y^2$$

является полиномом из $Q[x,y,z]$. Как правило, будем использовать для обозначения полиномов буквы f ,g, h, p, q ,r.

Определение 1.3. Пусть $f=\sum a_\alpha x^\alpha,\ a_\alpha \in k$ полином из $k[x_1,\ x_2,\dots,x_n]$:

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

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

3) *Полной степенью полинома* f , обозначаемой *deg*(*f*), называется максимум степеней $|\alpha|$ по всем мономам с ненулевыми коэффициентами.

Например, полином

$$f=2x^3y^2z+3/2y^3z^3-3xyz+y^2$$

рассмотренный выше, содержит четыре члена и имеет полную степень шесть. Отметим, что f содержит два члена максимальной степени, что невозможно в случае полинома от одной переменной.

Сумма и произведение двух полиномов являются полиномами. Мы говорим, что полином f *делит* полином g, если $g=fh$ для некоторого полинома $h\in k[x_1,\ x_2,\dots,x_n]$.

Операции сложения и умножения на множестве $k[x_1,\ x_2,\dots,x_n]$ удовлетворяют всем аксиомам поля, за исключением аксиомы существования обратного элемента по умножению (1/g, например не являются полиномами). Такая структура называется коммутативным кольцом и, по этой причине, мы будем называть $k[x_1,\ x_2,\dots,x_n]$ кольцом полиномов или полиномиальным кольцом.

Определение 1.4. Пусть дано поле k и натуральное число *n*; тогда *n- мерным аффинным пространством* над k называется множество

$$k^n=\{(\alpha_1,\alpha_2,\dots,\alpha_n)\colon \alpha_1,\alpha_2,\dots,\alpha_n\ \in k\ \}.$$

Пусть, например, k =***R*.** Пространство ***R*** - объект, знакомый из курсов линейной алгебры. Отметим также, что k^1 - называется *аффинной прямой*, k^2 - *аффинной плоскостью*.

Связь между полиномами и аффинными пространствами.

Полином $f=\sum a_\alpha x^\alpha \in k[x_1,\ x_2, \dots, x_n]$ задает функцию $f: k^n \to k$.

Пусть $(\alpha_1, \alpha_2, \dots, \alpha_n) \in k$. В формуле, определяющей f, заменим каждое x_i на α_i .Так как коэффициенты из k , то эта операция дает элемент $f(\alpha_1, \alpha_2, \dots, \alpha_n) \in k$.

Двойная природа полинома приводит к некоторым неожиданным следствиям. Например, вопрос «верно ли, что *f=0*?» допускает два истолкования: «является ли f нулевым полиномом?» т.е. верно ли, что все коэффициенты f равны нулю, или «является ли f нулевой функцией?», т.е. верно ли, что $f(\alpha_1, \alpha_2, \dots, \alpha_n)$=0 для всех $(\alpha_1, \alpha_2, \dots, \alpha_n) \in k^n$.

Удивительно, но эти два утверждения в общем случае не эквивалентны! Рассмотрим, например, множество из двух элементов 0 и 1. Это множество можно сделать полем, в котором 1+1=0. Это поле обычно обозначается F_2. Теперь рассмотрим полином $x^2 - x = x(x-1) \in F_2$. Так как этот полином обращается в нуль в точках 0 и 1, то он дает пример ненулевого полинома, являющегося нулевой функцией на аффинном пространстве F_2 .

Однако если k бесконечно, то никаких проблем не возникает.

Предложение 1.1. [15] Пусть k - бесконечное поле и $f \in k[x_1,\ x_2, \dots, x_n]$. Тогда *f=0* в том и только в том случае, когда $f: k^n \to k$ является нулевой функцией.

Доказательство. В одну сторону доказательство очевидно: нулевой полином определяет нулевую функцию.

Обратно, надо доказать, что если $f\ (\alpha_1, \alpha_2, \dots, \alpha_n)$ =0 для всех $(\alpha_1, \alpha_2, \dots, \alpha_n) \in k$, то f - нулевой полином. Доказательство по индукции по числу переменных n.

Пусть n=1. Ненулевой полином из $k[x]$ степени m имеет более m различных корней. Пусть $f \in k[x]$ и *f(a)=0* для всех $a \in k$. Так как -бесконечно, то f имеет бесконечно много корней; следовательно, f - нулевой полином.

Пусть предложение справедливо для n-1 и пусть $f \in k[x_1,\ x_2, \dots, x_n]$ - полином, обращающийся в нуль во всех точках из k^n. Объединяя члены по степеням переменной x_n, запишем f в виде:

$$f\ = \sum g_i(x_1, x_2, \dots, x_{n-1}) x_n^i\ ,$$

где $g_i \in k[x_1, x_2, \dots, x_n]$. Покажем что g_i -нулевой полином от (n-1)-переменных, откуда будет следовать, что f нулевой полином из $k[x_1, x_2, \dots, x_n]$.

Если мы зафиксируем $(a_1, a_2, \dots, a_{n-1}) \in k^{n-1}$, то получим полином $f(a_1, a_2, \dots, a_{n-1}, x_n) \in k[x_n]$ от одной переменной. По предложению f обращается в нуль в каждой точке $a_n \in k$, следовательно, $f(a_1, a_2, \dots, a_{n-1}, x_n)$ является нулевым полиномом из $k[x_n]$. Значит, его коэффициенты равны нулю, т.е. $g_i(a_1, a_2, \dots, a_{n-1})$ для любого i. Так как точка $(a_1, a_2, \dots, a_{n-1})$ выбрана в k^{n-1} произвольно, то каждый $g_i \in k[x_1, x_2, \dots, x_{n-1}]$ является нулевой функцией на k^{n-1}. Тогда по предложению индукции каждый g_i является нулевым полиномом в $k[x_1, x_2, \dots, x_{n-1}]$. Отсюда следует, что f является нулевым полиномом в $k[x_1, x_2, \dots, x_n]$. Что и требовалось доказать. ■

Отметим, что в формулировке предложения утверждение «*f=0 в* $k[x_1, x_2, \dots, x_n]$» означает, что f является нулевым полиномом, т.е. все его коэффициенты равны нулю. Таким образом, символ 0 обозначает и нулевой элемент в k, и нулевой полином в $k[x_1, x_2, \dots, x_n]$.

Следствие 1.1. Пусть k - бесконечное поле и $f, g \in k[x_1, x_2, \dots, x_n]$. Тогда $f=g$ в том и только в том случае, когда функции $f: k^n \to k$ и $g: k^n \to k$ равны.

Доказательство. В одну сторону утверждение тривиально. Пусть f и g задают одну и ту же функцию на k^n. Тогда полином f-g обращается в нуль во всех точках из k^n, т.е. по предложению полином f-g является нулевым. Значит, $f=g$ в $k[x_1, x_2, \dots, x_n]$. ■

Теорема 1.1. Каждый постоянный полином $f \in C[x]$ имеет корень в C (основная теорема алгебры).

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

Определение 1.5. Пусть k - некоторое поле, а $f_1, f_2, \dots f_s$ - полиномы в $k[x_1, x_2, \dots, x_n]$. Положим

$V(f_1, f_2, \dots f_s) = \{(a_1, a_2, \dots, a_n) \in k^n : f_i(a_1, a_2, \dots, a_n) = 0$ для всех $1 \leq i \leq s\}$.

$V(f_1, f_2, \dots f_s)$ называется *аффинным многообразием*, определенным полиномами $f_1, f_2, \dots f_s$.

Другими словами, аффинное многообразие $V(f_1, f_2, \dots f_s) \subset k^n$ - это множество решений системы уравнений

$f_1(a_1, a_2, \dots, a_n) = \dots = f_s(a_1, a_2, \dots, a_n) = 0$.

Например, многообразие V($x^2 + y^2 - 1$) на плоскости R^2 - окружность радиуса 1 с центром в начале координат(графики полиномов являются аффинными многообразиями, *y=f(x)* есть аффинное многообразие V(*y-f*(*x*)). Графики рациональных функций также являются аффинными многообразиями

$$y = \frac{x^3 - 1}{x} \Longrightarrow V(xy - x^3 + 1)$$

Лемма 1.1. Если *V*, *W*- аффинные многообразия, то $V \cup W$ и $V \cap W$ также являются аффинными многообразиями.

Доказательство. Пусть *V*=V($f_1, f_2, \dots f_s$) и *W*=V($g_1, g_2, \dots g_t$). Мы утверждаем, что

$V \cap W$= V ($f_1, f_2, \dots f_s, g_1, g_2, \dots g_t$)

$V \cup W$= V($f_i g_j : 1 \leq i \leq s, 1 \leq j \leq t$).

Первое утверждение тривиально: если точка принадлежит $V \cap W$, то как функции $f_1, f_2, \dots, f_s$, так и функции $g_1, g_2, \dots, g_t$ обращаются в этой точке в нуль. Это то же самое, что обращение в нуль набора функций

$f_1, f_2, \dots, f_s,\ g_1, g_2, \dots, g_t$.

Докажем второе утверждение: если $(a_1,\ a_2, \dots, a_n) \in$ V, то все f_i обращаются в нуль в этой точке; значит и все функции $f_i g_j$ обращаются в нуль в $(a_1,\ a_2, \dots, a_n)$. Таким образом $V \subset V(f_i g_j)$ и аналогично $W \subset$ V $(f_i g_j)$. Следовательно, $V \cup W \subset$ V$(f_i g_j)$. С другой стороны, пусть $(a_1,\ a_2, \dots, a_n) \in V(f_i g_j)$. Если эта точка принадлежит V, то все доказано, если же нет, то $f_{1_0}(a_1,\ a_2, \dots, a_n) \neq 0$ для некоторого i_0. Так как функции $f_{i_0} g_j$ обращаются в нуль в $(a_1,\ a_2, \dots, a_n)$ при всех j , то все g_j равны нулю в этой точке. Значит, $(a_1,\ a_2, \dots, a_n) \in W$ и V$\left(f_i g_j\right) \subset V \cup W$.■

§2.Идеалы

Определение 1.6. Подмножество $I \subset k[x_1,\ x_2, \dots, x_n]$ называется *идеалом,* если выполнены следующие условия:

1) $0 \in I$
2) если $f,g \in I$, то $f+g \in I$
3) если $f \in I$ и $h \in k[x_1,\ x_2, \dots, x_n]$, то $hf \in I$.

Определение 1.7. Пусть $f_1, f_2, \dots, f_s$- полиномы в $k[x_1,\ x_2, \dots, x_n]$. Положим

$$< f_1, f_2, \dots, f_s >= \left\{ \sum_{i=1}^{s} h_i\, f_i : h_i, \dots, h_s \in k[x_1, \dots, x_n] \right\}$$

.

Оказывается, что множество $<f_1, f_2, \dots, f_s>$ - идеал.

Лемма 1.2. Пусть $f_1, f_2, \dots, f_s$ принадлежат кольцу $k[x_1,\ x_2, \dots, x_n]$; тогда множество $< f_1, f_2, \dots, f_s >$ является идеалом в $k[x_1,\ x_2, \dots, x_n]$. Оно называется *идеалом, порожденным полиномами* $f_1, f_2, \dots, f_s$, а полиномы $f_1, f_2, \dots, f_s$ - *образующими* этого идеала, или его *порождающими элементами.*

Идеал $< f_1, f_2, \dots, f_s >$ имеет изящную интерпретацию на языке полиномиальных уравнений. Пусть $f_1, f_2, \dots, f_s \in k[x_1,\ x_2, \dots, x_n]$. Рассмотрим систему уравнений

$$f_1 = 0$$

……

$$f_s = 0$$

Из этих уравнений мы можем вывести другие, используя обычные алгебраические преобразования. Так, например, если мы умножим первое уравнение на $h_1 \in k[x_1,\ x_2, \dots, x_n]$, второе – на $h_2 \in k[x_1,\ x_2, \dots, x_n]$ 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 уравнения принадлежит идеалу $<f_1, f_2, \dots, f_s>$, т.е. идеал $<f_1, f_2, \dots, f_s>$ можно рассматривать как множество всех «полиномиальных следствий» системы $f_1 = f_2 = \cdots = f_s = 0$.

Идеал I называется *конечно порожденным,* если существуют полиномы $f_1, f_2, \dots, f_s \in k[x_1, x_2, \dots, x_n]$, такие, что $I=< f_1, f_2, \dots, f_s >$; при этом множество полиномов $f_1, f_2, \dots, f_s$, называется *базисом* идеала I.

Отметим, что идеал может иметь много различных базисов. Далее мы покажем, что можно определить особенно удобный базис, называемый *базисом Грёбнера*.

Следует обратить внимание на аналогию с линейной алгеброй. Определение идеала похоже на определение подпространства: и то, и другое множества замкнуты относительно операций сложения и умножения, только в случае подпространства идет речь об умножении на скаляры, а в случае идеала мы умножаем на полиномы.

О роли идеалов говорит и следующее предложение, в котором доказывается, что многообразие зависит лишь от *идеала,* порожденного определяющими уравнениями.

Предложение 1.2. Пусть $f_1, f_2, \dots, f_s$ и $g_1, g_2, \dots, g_t$ - базисы одного и того же идеала в $k[x_1, x_2, \dots, x_n]$, так что $< f_1, f_2, \dots, f_s >=< g_1, g_2, \dots, g_t >$. Тогда $V(f_1, f_2, \dots, f_s) = V(g_1, g_2, \dots, g_t)$.

Таким образом, изменяя базис идеала, мы упрощаем процедуру описания многообразия.

Возможность изменять базис, не меняя многообразия, очень важна и полезна.

Рассмотрим в качестве примера многообразие $V(2x^2 + 3y^2 - 11, x2-y2-3$. Легко показать, что $<2x2+3y2-11, x2-y2-3>=<x2-4, y^2 - 1 >$, так что в силу предложение 1.2.

$V(2x^2 + 3y^2 - 11, x^2 - y^2 - 3) = V(x^2 - 4, y^2 - 1)=\{(\pm 2, \pm 1)\}$.

Теперь мы обсудим, как аффинные многообразия связаны с интересным классом идеалов. Пусть V=V $(f_1, f_2, \dots, f_s) \subset k^n$ - аффинное многообразие, определенное полиномами $f_1, f_2, \dots, f_s \in k[x_1, x_2, \dots, x_n]$. Мы знаем, что $f_1, f_2, \dots, f_s$ обращаются в нуль на V, но только ли они? Есть ли другие полиномы, равные нулю на V?

Определение 1.8. Пусть $V \subset k^n$ -аффинное многообразие. Положим

I(V)=$\{f \in k[x_1, x_2, \dots, x_n]: f(a_1, a_2, \dots, a_n) = 0$ для всех $(a_1, a_2, \dots, a_n) \in$ V$\}$.

Оказывается, что I(V) – идеал.

Лемма 1.3. Пусть $V \subset k^n$ - аффинное многообразие. Тогда I(V) – идеал, который мы будем называть *идеалом многообразия* V.

Пример. Рассмотрим многообразие {(0,0)}, состоящее только из одной точки - начала координат в k^2. Элементами его идеала I({(0,0)}) являются полиномы, равные нулю в точке (0,0). Мы утверждаем, что

I({(0,0)})=<x,y>.

В одну сторону доказательство тривиально – любой полином вида A(*x*,*y*)*x*+B(*x*,*y*)*y* обращается в нуль в начале координат. Пусть теперь полином $\sum_{i,j} a_{ij}\, x^i y^j$ равен нулю в точке (0,0). Тогда $a_{00} = f(0,0) = 0$ и, следовательно,

$$f = a_{00} + \sum_{i,j\neq 0} a_{ij}\, x^i y^j = 0 + \left(\sum_{\substack{i,j \\ i>0}} a_{ij}\, x^{i-1} y^j \right) x + \left(\sum_{j>0} a_{0j}\, y^{j-1} \right) y \in \langle x, y \rangle$$

Доказательство окончено.■

Пусть $f_1, f_2, \dots, f_s \in k[x_1,\ x_2, \dots, x_n]$. Имеем полиномы $f_1, f_2, \dots, f_s \rightarrow$ многообразие $\mathrm{V}(f_1, f_2, \dots, f_s) \rightarrow$ идеал $I(\mathrm{V}(f_1, f_2, \dots, f_s))$.

Возникает естественный вопрос: верно ли, что $I(\mathrm{V}(f_1, f_2, \dots, f_s))$=< $f_1, f_2, \dots, f_s$>?

К сожалению, ответ здесь не всегда оказывается положительным. Наилучший ответ, который мы можем дать – это следующее утверждение:

Лемма 1.4. Пусть $f_1, f_2, \dots, f_s \in k[x_1,\ x_2, \dots, x_n]$. Тогда $< f_1, f_2, \dots, f_s > \subset I(\mathrm{V}(f_1, f_2, \dots, f_s))$, но эти два идеала не всегда совпадают.

Теперь нам нужно привести пример, когда идеал $I(\mathrm{V}(f_1, f_2, \dots, f_s))$ строго больше идеала < $f_1, f_2, \dots, f_s$>.

Мы докажем, что включение

$$< x^2, y^2 > \subset I(\mathrm{V}(x^2, y^2))$$

не является равенством. Сначала опишем идеал $I(\mathrm{V}(x^2, y^2))$. Система уравнений $x^2 = y^2 = 0$ определяет многообразие, состоящее из одной точки $\mathrm{V}(x^2, y^2) = \{(0,0)\}$. Но мы видели раньше, что идеал многообразия {(0,0)} есть <*x*,*y*>, т.е. $\mathrm{V}(x^2, y^2)$ = <*x*,*y*>. Для того чтобы убедиться, что этот идеал строго больше идеала $< x^2, y^2 >$, достаточно заметить, что $x \notin < x^2, y^2 >$, так как все члены полинома $h_1(x,y)x^2 + h_2(x,y)y^2$ имеют степень не меньше двух.

Хотя в общем случае $I(\mathrm{V}(f_1, f_2, \dots, f_s)\ )$ не равен < $f_1, f_2, \dots, f_s$ >, идеал многообразия всегда определяет многообразие однозначно.

Предложение 1.3. Пусть V и W – аффинные многообразия в k^n. Тогда

(i) V⊂W в том и только в том случае, когда $I(\mathrm{V}) \supset I(\mathrm{W})$

(ii) V=W в том и только в том случае, когда $I(\mathrm{V}) = I(\mathrm{W})$

Связь между аффинными многообразиями и идеалами сложна и разнообразна. Здесь мы затронули только верхушку айсберга. А теперь сформулируем три проблемы, касающиеся идеалов в $k[x_1,\ x_2, \dots, x_n]$:

- (Описание идеала) Каждый ли идеал $I \subset k[x_1,\ x_2, \dots, x_n]$ является конечно порожденным, т.е. всегда ли I=< $f_1, f_2, \dots, f_s$> для некоторых $f_1, f_2, \dots, f_s \in k[x_1,\ x_2, \dots, x_n]$?

- (Принадлежность идеалу) Пусть $f_1, f_2, \dots, f_s \in k[x_1,\ x_2, \dots, x_n]$. Существует ли алгоритм, позволяющий решить вопрос о принадлежности полинома
  $f \in k[x_1,\ x_2, \dots, x_n]$ идеалу $< f_1, f_2, \dots, f_s >$?
- (Решение полиномиальных уравнений) Описать множество решений в системы полиномиальных уравнений. Конечно, это то же самое, что описать аффинное многообразие V($f_1, f_2, \dots, f_s$).

§3. Полиномы от одной переменной

Определение 1.9. 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)= $a_0 x^m$ («LT» - первые буквы английского термина «leading term»). Например, если $f=2x^3 - 4x + 3$, то LT(f)=$2x^3$. Следует отметить, что если f и g - ненулевые полиномы, то

$$\deg(f) \leq \deg(g) \Leftrightarrow \text{LT}(f) \text{ делит LT}(g).$$

Теперь мы можем дать описание алгоритма деления.

Предложения 1.4. (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 $g,r \in k[x]$ и либо r=0, либо deg(r)<deg(g). *Более того, g и r определены однозначно и имеется алгоритм для их вычисления.*

Вот алгоритм вычисления g и r, записанный на псевдокоде:

Вход: g, f

Выход: q,r

q:0; r:=f

WHILE $r \neq 0$ AND LT(g) делит LT(r) DO

g:=q+LT(r)/LT(g)

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

Операции, подчиненные оператору цикла WHILE… DO, выполняются, пока выполняется условие, записанное между WHILE и DO; q:=… и r:=… - это операторы определения или переопределения значений q и r. И q и r являются *переменными* в этом алгоритме – на каждом шаге их значения меняются. Следствием существование алгоритма деления является такое утверждение о количестве корней полинома от одной переменной:

Следствием 1.2. *Пусть $f \in k[x]$ - ненулевой полином. Тогда он имеет в k не более чем* deg(f) *корней.*

Предложение 1.4. позволяет также описать все идеалы в $k[x]$.

Следствием 1.3. *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.*

Идеал, порожденный одним элементом, называется *главным идеалом.* Таким образом, ввиду следствия 1.3. мы говорим, что $k[x]$ является *областью главных идеалов* или сокращенно ОГИ.

Определение 1.10. *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 GCD(*f, g)* (GCD начальные буквы английского термина greatest common divisor).

Основные свойства наибольших общих делителей сформулированы в следующем предложении.

Предложение 1.5. *Пусть* $f,g \in k[x]$. *Тогда*

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

(ii) GCD(*f, g) является образующим идеала <f, g>;*

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

Дадим сначала 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 1.4. Тогда r называется *остатком от деления* f на g (мы будем писать r= остаток (f, g)). Теперь мы можем дать описание алгоритма Евклида:

Вход: f,g

Выход: h

$h:=f$

$s:=g$

WHILE $s \neq 0$ DO

rem:=остаток (h,s)

$h:=s$

s:=rem

Как пример работы алгоритма Евклида рассмотрим процесс вычисления GCD(x^4-1, x^6-1). Сначала мы применяем алгоритм деления:

$x^4-1 = 0(x^6-1)+x^4-1,$

$x^6-1 = x^2(x^4-1)+x^2-1,$

$x^4-1 = (x^2+1)(x^2-1)+0.$

Тепер мы имеем

GCD(x^4-1, x^6-1)=GCD(x^6-1, x^4-1)=GCD(x^4-1, x^2-1)=

GCD($x^2-1, 0$)

Следует отметить, что вычисление GCD дает ответ и на вопрос об определении порождающего элемента идеала $<x^4-1, x^6-1>$, а именно из предложения и того факта, что GCD(x^4-1, x^6-1)= x^2-1, следует, что $<x^4-1, x^6-1> = <x^2-1>$.

Однако здесь можно задать естественный вопрос: а как быть, когда идеал порожден тремя или большим количеством полиномов? Для этого необходимо определить наибольший общий делитель нескольких полиномов.

Определение 1.11. *Наибольшим общим делителем* полиномов $f_1, f_2, \dots, f_s \in k[x]$ называется полином h, такой, что

(i) h делит $f_1, f_2, \dots, f_s$;

(ii) если p -некоторый полином, который делит $f_1, f_2, \dots, f_s$, то p делит h. Такой полином h обозначается через GCD($f_1, f_2, \dots, f_s$) .Основные свойства наибольшего общего делителя сформулированы в следующем предложении.

Предложение 1.6. *Пусть* $f_1, f_2, \dots, f_s \epsilon k[x], s \geq 2$. *Тогда*

(i) GCD($f_1, f_2, \dots, f_s$) *существует и определен однозначно с точностью до умножения на ненулевую константу из* k*;*

(ii) GCD($f_1, f_2, \dots, f_s$) *порождает идеал* $< f_1, f_2, \dots, f_s >$ *;*

(iii) *если* $s \geq 3$*, то* GCD($f_1, f_2, \dots, f_s$)=GCD(f_1,GCD(f_2,……f_s))*;*

(iv) *существует алгоритм для вычисления* GCD($f_1, f_2, \dots, f_s$).

Пусть, например, мы хотим найти наибольший общий делитель четырех полиномов f_1, f_2, f_3, f_4. Имеем

GCD(f_1, f_2, f_3, f_4) = GCD((f_1,GCD(f_2, f_3, f_4)) = GCD(f_1,GCD(f_2,GCD(f_3, f_4))).

Таким образом, для вычисления наибольшего общего делителя полиномов f_1, f_2, f_3, f_4 нам нужно применить алгоритм Евклида три раза.

Процедура вычисления GCD в большинстве систем компьютерной алгебры может находить наибольший общий делитель только двух полиномов. Поэтому в случае трех и более полиномов необходимо использовать метод предложения 1.6. Рассмотрим, например, идеал

$$< x^3 - 3x + 2, x^4 - 1, x^6 - 1 > \subset k[x].$$

Мы знаем, что GCD($x^3 - 3x + 2, x^4 - 1, x^6 - 1$) порождает этот идеал. Далее, легко проверить, что

GCD($x^3 - 3x + 2, x^4 - 1, x^6 - 1$) =GCD($x^3 - 3x + 2$,GCD($x^4 - 1, x^6 - 1$)) =

= GCD($x^3 - 3x + 2, x^2 - 1$) = $x - 1$,

т.е.

$< x^3 - 3x + 2, x^4 - 1, x^6 - 1 > = < x - 1 >$.

Теперь понятно, как должен быть построен алгоритм вычисления порождающего элемента идеала $< f_1, f_2, \dots, f_s >$, $f_1, f_2, \dots, f_s \epsilon\ k[x]$.

В качестве следующего приложения алгоритмов деления и вычисления GCD рассмотрим *задачу о принадлежности идеалу:* существует ли алгоритм, позволяющий определить для произвольного полинома $f \epsilon\ k[x]$ и заданных полиномов $f_1, f_2, \dots, f_s \epsilon\ k[x]$, лежит f в идеале $< f_1, f_2, \dots, f_s >$ или нет. Ответ

утвердительный, и такой алгоритм несложно описать. Первый шаг – это вычисление GCD($f_1, f_2, \dots, f_s$), т.е. определение порождающего элемента h идеала $< f_1, f_2, \dots, f_s >$. Так как включение $f \epsilon < f_1, f_2, \dots, f_s >$ эквивалентно включению $f \epsilon < h >$, то нам осталось только поделить f на h с остатком: $f=qh+r$, $\deg(r)<\deg(h)$. Таким образом, f принадлежит идеалу в том и только в том случае, когда $r = 0$.

Заключение по главе I

В первой главе изучены основные понятия алгебраической геометрии. Под геометрией понимается геометрия аффинных многообразий задаваемых полиномами. Понимание теории аффинных многообразий требует знания теории идеалов в кольцах полиномов $k[x_1, \dots \dots . x_n]$. А также были рассмотрены полиномы от одной переменной.

Основные результаты по главе I:

- Изучена связь между алгебраическими свойствами полиномиальных колец и геометрическими свойствами аффинных многообразий.
- Изучены идеалы и их связь с полиномиалными уравнениями.
- Сформулированны три проблемы касающиеся идеалов в $k[x_1, \dots \dots . x_n]$, т.е. задача описания идеала, задача о принадлежности идеалу, нахождение решения полиномиальных уравнений.
- Дано описание алгоритма деления в кольце $k[x]$.
- Полностью решены задачи описания идеала и о принадлежности идеалу в случае $k[x]$.

ГЛАВА 2
БАЗИСЫ ГРЁБНЕРА

§1.Упорядочение мономов в $k[x_1, x_2, \dots, x_n]$

Алгоритм деления полиномов от одной переменной имеет дело со следующим упорядочением мономов:

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

Результативность алгоритма связана именно с тем, что мы работаем последовательно со старшими членами полиномов f и g, а не «случайным образом» убираем члены из f, используя произвольные члены из g. Обобщение алгоритмов деления и приведения к ступенчатому виду на случай произвольных полиномов от нескольких переменных должно базироваться на упорядочении членов из $k[x_1, x_2, \dots, x_n]$.

Отметим сначала, что существует взаимно однозначное соответствие между мономами $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$ и n-наборами (n-векторами) показателей степеней $\alpha = (\alpha_1, \dots \alpha_n) \in Z_{\geq 0}^n$. Упорядочение, которое мы определим на $Z_{\geq 0}^n$, определит и упорядочение на множестве мономов: если $\alpha > \beta$ в $Z_{\geq 0}^n$, то мы будем говорить, что $x^\alpha > x^\beta$.

Упорядочение на $Z_{\geq 0}^n$ можно задать многими способами. Так как полином есть сумма мономов, то мы должны уметь расположить его члены в порядке убывания (или возрастания). Для этого мы должны уметь сравнивать любую пару мономов и определять, какой из них больше, т.е. наше упорядочение должно быть *линейным*. Это означает, что для любой пары мономов x^α и x^β должно выполняться ровно одно из следующих соотношений:

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

Еще мы потребуем, чтобы упорядочение мономов обладало следующим дополнительным 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 $Z_{\geq 0}^{n}$, то для любого $\gamma \in Z_{\geq 0}^{n}$, $\alpha + \gamma > \beta + \gamma$

Теперь мы можем дать следующее определение.

Определение 2.1. *Мономиальным упорядочением* на $k[x_1, x_2, \dots, x_n]$ называется любое бинарное отношение $>$ на $Z_{\geq 0}^{n}$, обладающее следующими свойствами:

(i) $>$ является линейным упорядочением на $Z_{\geq 0}^{n}$.

(ii) если $\alpha > \beta$ и $\gamma \in Z_{\geq 0}^{n}$, то $\alpha + \gamma > \beta + \gamma$;

(iii) $>$ вполне упорядочивает $Z_{\geq 0}^{n}$, т.е. любое непустое подмножество в $Z_{\geq 0}^{n}$ имеет минимальный (наименьший) элемент (по отношению к упорядочиванию $>$).

Следующая лемма помогает понять, что означает условие вполне упорядоченности (iii).

Лемма 2.1. [15] *Упорядочение* $>$ *на* $Z_{\geq 0}^{n}$ *вполне упорядочивает это множество тогда и только тогда, когда каждая строго убывающая последовательность элементов из* $Z_{\geq 0}^{n}$

$$\alpha(1) > \alpha(2) > \alpha(3) > \dots$$

обрывается.

Нашим первым примером упорядочивания n-векторов будет лексикографическое упорядочение (или сокращенно lex - *упорядочение*).

Определение 2.2. (*лексикографическое упорядочение*). Пусть

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

Вот несколько примеров:

(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 $x_1 > x_2 > \cdots > x_n$ переменных $x_1, x_2, \dots, x_n$ является lex- упорядочением. Так как

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

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

Работая с полиномами от двух или трех переменных, мы обозначаем переменные через x,y,z, а не x_1, x_2, x_3. В дальнейшем мы будем также, как правило, предполагать, что алфавитный порядок $x > y > z$ переменных и определяет упорядочение мономов.

Предложение 2.1. [15] *Лексикографическое упорядочение на $Z_{\geq 0}^n$ является мономиальным упорядочением.*

Необходимо отметить, что существует много лексикографических упорядочений: каждому упорядочению переменных отвечает свое. До сих пор мы рассматривали лексикографическое упорядочение, порожденное упорядочением $x_1 > x_2 > \cdots > x_n$. Но, задав *произвольный* порядок переменных $x_1, x_2, \dots, x_n$, мы получим соответствующее ему лексикографическое упорядочение. Пусть, например, переменных две, скажем, x и y. Тогда мы можем определить два лексикографических упорядочения: одно порождается порядком $x > y$, а другое – порядком $y > x$. В общем случае n переменных имеется $n!$ лексикографических упорядочений. В дальнейшем термин «лексикографическое упорядочение» будет означать, что имеется в виду порядок $x_1 > x_2 > \cdots > x_n$.

В случае лексикографического упорядочения переменная больше любого монома, который содержит только меньшие переменные, вне зависимости от его степени. Так, при упорядочении $x > y > z$ мы имеем $x >_{lex} y^5 z^3$. В ряде случаев нам будет необходимо учитывать также степени мономов и сравнивать сначала именно степени. Это можно сделать с помощью *градуированного лексикографического упорядочения* (сокращенно grlex-упорядочения).

Определение 2.3. (*градуированное лексикографическое упорядочение*). Пусть $\alpha, \beta \in Z_{\geq 0}^n$. 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 степени, а если степени равны, то использует лексикографическое упорядочение.

Вот несколько примеров:

(a) $(1,2,3) >_{grlex} (3,2,0)$ так как $|(1,2,3)| = 6 > |(3,2,0)| = 5$

(b) $(1,2,4) >_{grlex} (1,2,4)$, так как $|(1,2,4)| = |(1,1,5)|$, но $(1,2,4) >_{lex} (1,1,5)$

(c) Переменные упорядочиваются в соответствии с лексикографическим порядком, т.е. $x_1 >_{lex} x_2 >_{lex} \ldots >_{lex} x_n$.

Следующее (интуитивно несколько менее естественное) упорядочение является для некоторых операций наиболее эффективным при вычислениях.

Определение 2.4. (*градуированное обратное лексикографическое упорядочение* grevlex). Пусть $\alpha, \beta \in Z_{\geq 0}^n$. 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

$\alpha - \beta \in Z_{\geq 0}^{n}$ отрицательна.

Как и grlex, grevlex сначала сравнивает степени мономов, но упорядочивает мономы по-другому в случае равенства их степеней. Например:

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

(b) $(1,5,2) >_{grevlex} (4,1,3)$ так как $|(1,5,2)| = |(4,1,3)|$, и

$$\alpha - \beta = (-3,4,-1)$$

Для того чтобы объяснить связь между grlex и grevlex, отметим сначала, что оба эти упорядочения 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.

Мы обсудим то, как мономиальные упорядочения могут помочь при работе с полиномами. Пусть $f = \sum_{\alpha} a_{\alpha} x^{\alpha} \in k[x_1, x_2, \dots, x_n]$ и пусть выбрано мономиальное упорядочение $>$. Тогда 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:

(a) при lex-упорядочении мы записываем полином f в порядке убывания членов так:

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

(b) при grlex -упорядочении запись такова:

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

(c) при grevlex -упорядочении запись такова:

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

Далее мы будем пользоваться следующими понятиями.

Определение 2.5. Пусть $f = \sum_\alpha a_\alpha x^\alpha$ - ненулевой полином в $k[x_1, x_2, \dots, x_n]$ и пусть $>$ - мономиальное упорядочение.

(i) *Мультистепень* полинома f определяется так :

$$multideg(f) = max(\alpha \in Z^n_{\geq 0} : a_\alpha \neq 0)$$

(максимум берется по отношению к $>$).

(ii) *Старший коэффициент* полинома f - это

$$\mathrm{LC}(f) = a_{multi\ \deg(f)} \in k$$

(iii) *Старший моном* полинома f - это

$$\mathrm{LM}(f) = x^{multi\ \deg(f)}$$

(с коэффициентом 1).

(iv) *Старший член* полинома f - это

$$\mathrm{LT}(f) = \mathrm{LC}(f) * \mathrm{LM}(f).$$

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

$$multideg(f) = (3,0,0),$$

$$\mathrm{LC}(f) = -5,$$

$$\mathrm{LM}(f) = x^3,$$

$$\mathrm{LT}(f) = -5x^3$$

Лемма 2.2. *Пусть* $f, g \in k[x_1, x_2, \dots, x_n]$ - *ненулевые полиномы. Тогда*

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

(ii) *Если* $f + g \neq 0$, *то*

$$multideg(f + g) \leq \max\ (multideg(f), multideg(g)).$$

Если, кроме того, $multideg(f) \neq multideg(g)$ *, то указанное неравенство становится равенством.*

§2.Алгоритм деления в $k[x_1, x_2, \ldots, x_n]$

В главе 1 было объяснено, как алгоритм деления для полиномов от одной переменной может быть применен для решения задачи о принадлежности идеалу. Для решения этой же задачи в случае нескольких переменных необходимо обобщить алгоритм деления в $k[x]$ на общий случай полиномиального кольца $k[x_1, x_2, \ldots, x_n]$. Наша цель – научиться делить полином $f \in k[x_1, x_2, \ldots, x_n]$ на полиномы $f_1, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$. Как мы увидим, это означает научиться представлять f в виде

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r,$$

где «частные» $a_1, \ldots, a_s$ и остаток r принадлежат $k[x_1, x_2, \ldots, x_n]$. Самое трудное в этом вопросе – это корректно определить остаток. Именно здесь будут использованы мономиальные упорядочения. После этого мы применим этот алгоритм для решения задачи о принадлежности идеалу.

Основная идея алгоритма та же, что и в случае одной переменной: мы должны уничтожать старший член полинома f (определенный заданным мономиальным *упорядочением), умножая некоторый* f_i *на подходящий моном и вычитая. Этот моном* будет членом соответствующего a_i. Будет использоваться та же схема, что и в случае одной переменной, но теперь у нас несколько делителей и частных. Будем записывать делители $f_1, f_2, \ldots, f_s$ и частные $a_1, a_2, \ldots, a_s$ *в столбец* слева, т.е. мы имеем следующую схему:

a_1:

a_2:

f_1:

f_2: $\sqrt{f}$

Причем остаток должен обладать свойством: ни один член остатка нельзя поделить на старший член хотя бы одного делителя.

Теорема 2.1. [15] (алгоритм деления в $k[x_1, x_2, \dots, x_n]$). *Зафиксируем некоторое мономиальное упорядочение* $>$ *на* $Z_{\geq 0}^n$ *, и пусть* $F = (f_1, \dots, f_s)$ *- упорядоченный* s *-набор полиномов из* $k[x_1, x_2, \dots, x_n]$. *Тогда любой полином* $f \in k[x_1, x_2, \dots, x_n]$ *может быть записан в виде*

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r ,$$

где $a_i, r \in k[x_1, x_2, \dots, x_n]$ *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),…,LT(f_s). *Мы называем* r *остатком от деления полинома* f *на F. Более того, если* $a_i f_i \neq 0$, *то* $multideg(f) \geq multideg(a_i f_i)$

Вот 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 $i \le s$ AND есть_деление= false DO

IF LT (f_i) делит LT(p) THEN

$a_i := a_i +$ LT(p)/LT(f_i)

p:= p-(LT(p)/LT(f_i)) f_i

есть_деление:= true

ELSE

i:= i+1

IF есть_деление:=false THEN

r: =r+LT(p)

p: =p-LT(p)

Алгебраическая техника, использованная в алгоритме, очень проста. Тем более удивительно, что этот алгоритм был разработан и применен только 40 лет назад.

На основании этого алгоритма была написана программа, позволяющая делить любой полином от трех переменных на любую упорядоченную совокупность полиномов. Алгоритм был реализован в системе компьютерной алгебры Maple 12.

>**restart;with(Groebner):**

>s: =2 plx:='plex(x,y,z)':

>fs:=[x*y^2-x, x-y^3];

fs:=[$xy^2 - x, x - y^3$]

>f:=x^7*y^2+x^3*y^2-y+1;

$$f:=x^7y^2+x^3y^2-y+1$$

>a:=array(1..s):

>for j from1 to s do a[j]:=0: od:

>r:=0;

$$r:=0$$

>p:=f:

>while p<>0 do

>i:=1: isdiv:=0:

>while (i<=s) and (isdiv=0) do

>if divide(leadterm(p, plx), leadterm(fs[i], plx), 'rt')=true then

>a[i]:=a[i]+(leadcoeff(p, plx)*leadterm(p, plx))/(leadcoeff(fs[i], plx)*leadterm(fs[i], plx)):

a[i]:=normal(a[i], expanded): printf("a[%d]:=%a\n", i, a[i]):

>p:=p-((leadcoeff(p, plx)*leadterm(p, plx))/(leadcoeff(fs[i], plx)*leadterm(fs[i], plx)))*fs[i]:

p:=normal(p, expanded): prinrf("p:=%a\n", p):

>isdiv:=1:

>else i:=i+1: end if:

>end do:

>if isdiv=0 then

>r:= r+leadcoeff(p,plx)*leadterm(p,plx): r:=normal(r, expanded): printf("r:=%a\n", r):

>p:=p-leadcoeff(p,plx)*leadterm(p,plx): p:=normal(p, expanded): printf("p:=%a\n", p):

>end if:

>end do;

i:=1

a[1]:=x^6

p:=x^3*y^2+1+x^7

a[2]:=x^6

p:=x^3*y^2-y+1+x^6*y^3

a[1]:=x^6+y*x^5

p:=x^3*y^2-y+1+y*x^6

a[2]:=x^6+y*x^5

p:=x^3*y^2-y+1+y^4*x^5

a[1]:=x^6+y*x^5+y^2*x^4

p:=x^3*y^2-y+1+y^2*x^5

a[1]:=x^6+y*x^5+y^2*x^4+x^4

p:=x^3*y^2-y+1+x^5

a[2]:=x^6+y*x^5+x^4

p:=x^3*y^2-y+1+x^4*y^3

a[1]:=x^6+y*x^5+y^2*x^4+x^4+y*x^3

p:=x^3*y^2-y+1+y*x^4

a[2]:=x^6+y*x^5+x^4+y*x^3

p:=x^3*y^2-y+1+y^4*x^3

a[1]:=x^6+y*x^5+y^2*x^4+x^4+y*x^3+y^2*x^2

p:=2*x^3*y^2-y+1

a[1]:= x^6+y*x^5+y^2*x^4+x^4+y*x^3+y^2*x^2+2*x^2

p:= 2*x^3-y+1

a[2]:= x^6+y*x^5+x^4+y*x^3+2*x^2

p:= 2*x^2*y^3-y+1

a[1]:= x^6+y*x^5+y^2*x^4+x^4+y*x^3+y^2*x^2+2*x^2+2*x*y

p:= 2*x^2*y-y+1

a[2]:= x^6+y*x^5+x^4+y*x^3+2*x^2+2*x*y

p:= 2*x*y^4-y+1

a[1]:= x^6+y*x^5+y^2*x^4+x^4+y*x^3+y^2*x^2+2*x^2+2*x*y+2*y^2

p:= 2*x*y^2-y+1

a[1]:= x^6+y*x^5+y^2*x^4+x^4+y*x^3+y^2*x^2+2*x^2+2*x*y+2*y^2+2

p:= 2*x-y+1

a[2]:= x^6+y*x^5+x^4+y*x^3+2*x^2+2*x*y+2

p:= 2*y^3-y+1

r:=2*y^3

p:=-y+1

r:=2*y^3-y

p:=1

r:=-y+1+2*y^3

p:=0

>print(a);

$$[x^6 + yx^5 + y^2x^4 + x^4 + yx^3 + y^2x^2 + 2x^2 + 2xy + 2y^2 + 2, x^6 + yx^5 + x^4 + yx^3 + 2x^2 + 2yx + 2]$$

>print(r);

$$[-y + 1 + 2y^3]$$

В заключении параграфа мы обсудим, имеет ли в общем случае алгоритм деления те хорошие свойства, которыми он обладает в случае одной переменной. К сожалению, ответ отрицательный – примеры ниже показывают, что алгоритм весьма несовершенен. На самом деле он работает в полную силу только при использовании базисов Грёбнера.

Первым важным свойством алгоритма деления в $k[x]$ является то, что остаток определен однозначно. Покажем на примере, что в случае нескольких переменных это свойство не выполняется.

Пример 2.1. Поделим $f = x^7y^2 + x^3y^2 - y + 1$ на $f_1 = x - y^3$ и на $f_2 = xy^2 - x$. Мы используем lex-упорядочение с $x>y$. Если проведем деление сами, то получим следующую схему:

$$1.a_1 = x^6y^2 + x^5y^5 + x^4y^8 + x^3y^{11} + x^2y^{14} + x^2y^2 + xy^{17} + xy^5 + y^{21} + y^8$$

$$a_2 = 0$$

$$\begin{array}{l|l}
x - y & x^7y^2 + x^3y^2 - y + 1 \\
xy^2 - x & \underline{x^7y^2 - x^7y^6} \\
& x^7y^5 + x^3y^2 - y + 1 \\
& \underline{x^6y^5 - x^5y^8} \\
& x^5y^8 + x^3y^2 - y + 1 \\
& \underline{x^5y^8 - x^4y^{11}} \\
& x^4y^{11} + x^3y^2 - y + 1 \\
& \underline{x^4y^{11} - x^3y^{14}} \\
& x^3y^{14} + x^3y^2 - y + 1 \\
& \underline{x^3y^{14} - x^5y^{17}} \\
& x^3y^2 + x^3y^2 - y + 1 \\
& \underline{x^3y^2 - x^2y^5} \\
& x^2y^{17} + x^2y^5 - y + 1 \\
& \underline{x^2 - xy^{21}} \\
& x^2y^5 + xy^{21} - y + 1 \\
& \underline{x^2y^5 - xy^8} \\
& xy^{21} + xy^8 - y + 1 \\
& \underline{xy^{21} - xy^{24}} \\
& xy^8 + y^{24} - y + 1 \\
& \underline{xy^8 - y^{11}} \\
& y^{24} + y^{11} - y + 1 = r
\end{array}$$

$\Rightarrow \quad x^7y^2 + x^3y^2 - y + 1 \;=\; (x^6y^2 + x^5y^5 + x^4y^8 + x^4y^8 + x^3y^{11} + x^2y^{14} +$ *x2y2+xy17+xy5+y20+y8·x−y3+0·xy2−x+(y23+y11−y+1)*

Пример 2.2. Этот пример отличается от примера 2.1. только переменой порядка делителей. Если мы сравним пример 2.1. с примером 2.2., то увидим, что полученный нами остаток не равен остатку в примере 2.1.

$$3.a_1 = x^6 + x^5y + x^4y^2 + x^4 + x^3y + x^2y^2 + 2x^2 + 2xy + 2y^2 + 2$$

$$a_2 = x^6 + x^5y + x^4 + x^3y + 2x^2 + 2xy + 2$$

$$\begin{array}{l|l}
xy^2 - x & x^7y^2 + x^3y^2 - y + 1 \\
x - y^3 & \underline{x^7y^2 - x^7} \\
 & x^7 + x^3y^2 - y + 1 \\
 & \underline{x^7 - x^6y^3} \\
 & x^6y^3 + x^3y^2 - y + 1 \\
 & \underline{x^6y^3 - x^6y} \\
 & x^6y + x^3y^2 - y + 1 \\
 & \underline{x^6y - x^5y^4} \\
 & x^5y^4 + x^3y^2 - y + 1 \\
 & \underline{x^5y^4 - x^5y^2} \\
 & x^5y^2 + x^3y^2 - y + 1 \\
 & \underline{x^5y^2 - x^5} \\
 & x^5 + x^3y^2 - y + 1 \\
 & \underline{x^5 - x^4y^3} \\
 & x^4y^3 + x^3y^2 - y + 1 \\
 & \underline{x^4y^3 - x^4y} \\
 & x^4y + x^3y^2 - y + 1 \\
 & \underline{x^4y - x^3y^4} \\
 & x^3y^4 + x^3y^2 - y + 1 \\
 & \underline{x^3y^4 - x^3y^2} \\
 & 2x^3y^2 - y + 1 \\
 & \underline{2x^3y^2 - 2x^3} \\
 & 2x^3 - y + 1 \\
 & \underline{2x^3 - 2x^2y^3} \\
 & 2x^2y^3 - y + 1 \\
 & \underline{2x^2y^3 - 2x^2y} \\
 & 2x^2y - y + 1 \\
 & \underline{2x^2y - 2xy^4} \\
 & 2xy^4 - y + 1 \\
 & \underline{2xy^4 - 2xy^2} \\
 & 2xy^2 - y + 1 \\
 & \underline{2xy^2 - 2x} \\
 & 2x - y + 1 \\
 & \underline{2x - 2y^3} \\
 & 2y^3 - y + 1
\end{array}$$

Этот пример показывает, что остаток r не определен однозначно требованием, чтобы ни один его член не делился ни на один из LT(f_1),…,LT(f_s).

Важным достоинством алгоритма деления в $k[x]$ является возможность с его помощью решать задачу о принадлежности идеалу. Обладает ли подобным свойством обобщенный алгоритм деления? Вот простое следствие теоремы 2.1: если остаток от деления f на $F = (f_1, \dots, f_s)$ равен нулю, r =0, т.е.

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s,$$

то $f \in < f_1, \dots, f_s >$. Другими словами, r =0 - это *достаточное* условие принадлежности идеалу. Следующий пример показывает, однако, что r =0 не является *необходимым* условием.

Пример 2.3. Пусть $f_1 = xy + 1,\ f_2 = y^2 - 1 \in k[x, y]$ с lex-упорядочением. Если мы разделим $f = xy^2 - x$ на $F = (f_1, f_2)$, то в результате получим

$$xy^2 - x = y(xy + 1) + 0(y^2 - 1) + (-x - y)$$

С другой стороны, деля f на $F = (f_2, f_1)$, получаем

$$xy^2 - x = x(xy + 1) + 0(xy + 1) + 0.$$

Из второго равенства следует, что $f \in < f_1, f_2 >$. Но тогда первое равенство демонстрирует, что, хотя f и принадлежит идеалу $< f_1, f_2 >$ остаток от деления f на F не равен нулю.

Таким образом, алгоритм деления, определенный теоремой 2.1, является несовершенным обобщением алгоритма деления в $k[x]$. Чтобы исправить ситуацию, следует вспомнить об одном правиле, сформулированном в главе 1: если мы работаем с набором полиномов $f_1, f_2, \dots, f_s \in k[x_1, x_2, \dots, x_n]$, то следует рассматривать идеал I, ими порожденный. Другими словами, следует рассматривать и другие наборы полиномов, порождающие тот же

идеал. Можно сформулировать естественную задачу: существует ли для произвольного идеала I «хорошее» порождающее множество, т.е. такое, что остаток r от деления на множество «хороших» образующих элементов был бы однозначно определен и условие r =0 было бы *необходимым* и *достаточным* условием принадлежности идеалу. Далее мы увидим, что базисы Грёбнера обладают этими «хорошими» свойствами.

§3.Мономиальные идеалы и лемма Диксона

В этом параграфе мы рассмотрим задачу описания идеала для частного случая мономиальных идеалов. Полученные результаты найдут неожиданное применение в теории мономиальных упорядочений.

Определение 2.6. Идеал $I \subset k[x_1, x_2, \dots, x_n]$ называется *мономиальным*, если существует подмножество $A \subset Z_{\geq 0}^n$ (которое может быть бесконечным), такое, что I состоит из всех конечных сумм вида $\sum_{\alpha \epsilon A} h_\alpha x^\alpha$, где

$h \in k[x_1, x_2, \dots, x_n]$. Такой идеал I будет обозначаться через $< x^\alpha : \alpha \in A >$.

Вот, пример мономиального идеала $I =< x^4y^2, x^3y^4, x^2y^5 > \subset k[x, y]$. Сначала мы охарактеризуем *все* мономы, принадлежащие заданному мономиальному идеалу.

Лемма 2.3. *Пусть* $I =< x^\alpha : \alpha \in A >$ *-мономиальный идеал. Тогда моном* x^β *принадлежит* I *в том и только в том случае, когда* x^β *делится на некоторый моном* $x^\alpha, \alpha \in A$.

Напомним, что x^β делится на x^α , если $x^\beta = x^\alpha x^\gamma$ для некоторого $\gamma \epsilon Z_{\geq 0}^n$. Значит, $\beta = \alpha + \gamma$, т.е. множество $\alpha - Z_{\geq 0}^n = \{\alpha + \gamma : \gamma \epsilon Z_{\geq 0}^n\}$ состоит из показателей степеней всех мономов, которые делятся на x^α . Это наблюдение и лемма 2.3 позволяют графически представить множество всех

мономов, принадлежащих данному мономиальному идеалу. Например, если $I =< x^4y^2, x^3y^4, x^2y^5 >$, то показатели степени мономов принадлежащих I, образуют множество

((4,2)+ $Z^n_{\geq 0}$) ∪ ((3,4)+ $Z^n_{\geq 0}$) ∪ ((2,5)+ $Z^n_{\geq 0}$).

Мы можем изобразить это множество, как объединение целочисленных точек в трех сдвинутых экземплярах первого квадранта на плоскости:

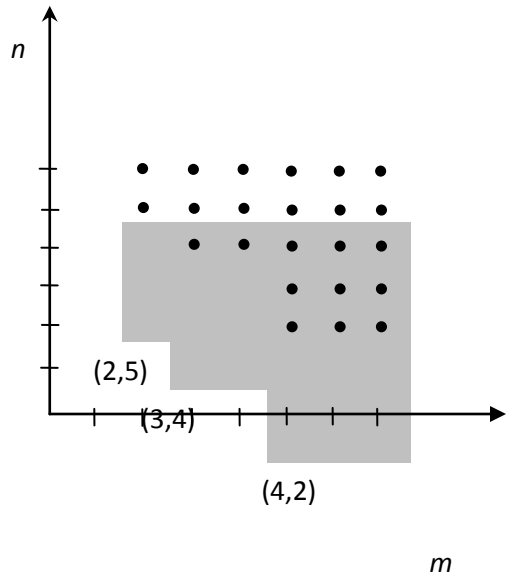


Рис.1. $(m, n) \leftrightarrow x^m y^n$

Лемма 2.4. *Пусть I -некоторый мономиальный идеал, $f \in k[x_1, x_2, \ldots, x_n]$. Тогда следующие условия эквивалентны:*

(i) $f \in I$

(ii) *каждый член полинома f принадлежит I;*

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

Следствие 2.1. *Два мономиальных идеала совпадают в том и только в том случае, когда совпадают множества мономов, содержащихся в них.*

Теорема 2.2.[11](лемма Диксона) *Любой мономиальный идеал* $I =< x^{\alpha} : \alpha \in A >\subset k[x_1, x_2, \dots, x_n]$ *может быть представлен в виде* $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$, *где* $\alpha(1), \dots, \alpha(s) \in A$. *В частности,* I *имеет конечный базис.*

Доказательство. Доказательство проводится индукцией по n-числу переменных. Если n=1, то I порожден мономами x_1^{α}, где $\alpha \in A \subset Z_{\geq 0}^{n}$. Пусть β - наименьший элемент в A. Тогда для всех, $\alpha \in A$ имеем $\beta \leq \alpha$. Таким образом, x_1^{β} делит все образующие x_1^{α}, т.е. $I =< x_1^{\beta} >$.

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

Пусть $I \subset k[x_1, \dots, x_{n-1}, y]$ - мономиальный идеал. Рассмотрим идеал $J \subset k[x_1, \dots, x_{n-1}]$, порожденный мономами x^{α}, что $x^{\alpha} y^{m}$ 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, $J = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$. Идеал J может рассматриваться, 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 $x^{\alpha(i)} y^{m_i} \in I$. Пусть 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 - это «срез» идеала I, порожденный мономами, которые содержат y точно в степени l. По предположению индукции J_l конечно порожден, $J_l = \langle x^{\alpha_2(1)}, \dots, x^{\alpha_l(s_l)} \rangle$

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

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

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

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

$\vdots$

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

Сначала докажем, что каждый моном в I делится хотя бы на один моном из списка. Пусть $x^\alpha y^p \in I$. Если $p \geq m$, то по определению J моном $x^\alpha y^p$ делится на некоторый моном $x^{\alpha(i)}y^m$. С другой стороны, если $p \leq m-1$, то по определению идеала J_p моном $x^\alpha y^p$ делится на некоторый моном $x^{\alpha_p(j)}y^p$. Из леммы 2.4. следует, что мономы из списка порождают идеал, содержащий те же мономы, которые содержит I. Тогда по следствию 2.1. эти идеалы совпадают, и наше утверждение доказано.

Чтобы закончить доказательство теоремы, нам нужно доказать, что конечное множество образующих можно выбрать из заданного множества образующих идеал I. Будем обозначать переменные, как и раньше, $x_1, x_2, \dots, x_n$. Тогда $I =< x^\alpha : \alpha \in A > \subset k[x_1, x_2, \dots, x_n]$. Нам нужно доказать, что I порожден конечным набором $x^\alpha : \alpha \in A$. Выше мы уже доказали, что $I = \langle x^{\beta(1)}, \dots, x^{\beta(s)} \rangle$, где $x^{\beta(i)} \epsilon\, I$. Так как $x^{\beta(i)} \epsilon\, I =< x^\alpha : \alpha \in A >$, то по лемме 2.4. каждый моном $x^{\beta(i)}$ делится на некоторый моном $x^{\alpha(i)}$, где $\alpha(i) \in A$. Теперь очевидно, что $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$. Доказательство теоремы закончено.

Чтобы лучше понять структуру доказательства теоремы 2.2 разберем пример идеала $I =< x^4y^2, x^3y^4, x^2y^5 >$, с которым мы уже имели дело в этом параграфе. Из рисунка видно, что «проекция» есть $J =< x^2 > \subset k[x]$. Так как, $x^2y^5 \in I$, то $m = 5$. Выпишем теперь «срезы» J_l, $0 \leq l \leq 4 = m-1$, порожденные мономами, содержащими y^l:

$$J_0 = J_1 = \{0\},$$

$$J_2 = J_3 = < x^4 >,$$

$$J_4 = < x^3 >.$$

Эти «срезы» легко увидеть на рисунке. Теперь из доказательства теоремы 2.2 следует, что $I = < x^4y^2, x^3y^4, x^2y^5 >$.

Теорема 2.2 решает задачу описания идеала в мономиальном случае, так как доказывает существование у него конечного базиса. Этот факт, в свою очередь, позволяет решить задачу о принадлежности мономиальному идеалу. А именно, пусть $I = \langle x^{\alpha(1)}, \dots, x^{\alpha(s)} \rangle$. Тогда легко доказать, что данный полином f принадлежит I в том и только в том случае, когда остаток от деления f на $x^{\alpha(1)}, \dots, x^{\alpha(s)}$ равен нулю.

Следствие 2.2. *Пусть* $>$ *- некоторое отношение на* $Z_{\geq 0}^n$*, удовлетворяющее следующим условиям:*

(i) $>$ *- линейное упорядочение на* $Z_{\geq 0}^n$*;*

(ii) *если* $\alpha > \beta$ *и* $\gamma \in Z_{\geq 0}^n$*, то* $\alpha + \gamma > \beta + \gamma$.

Тогда $>$ *является вполне упорядочением в том и только в том случае, когда* $\alpha \geq 0$ *для всех* $\alpha \in Z_{\geq 0}^n$.

Теперь мы можем упростить определение мономиального упорядочения. Условия (i) и (ii) определения сохраняются, а условие (iii) заменяется на более простое: $\alpha \geq 0$ для всех $\alpha \in Z_{\geq 0}^n$. Новое условие *значительно* упрощает проверку того, что данное упорядочение является мономиальным.

§4.Теорема Гильберта о базисе и базисы Грёбнера

В этом параграфе мы дадим полное решение *задачи описания идеала.* Для этого нам будет необходимо определить базисы с «хорошими» (по отношению к алгоритму деления) свойствами. Ключевая идея состоит в том, что как только заданно мономиальное упорядочение, то однозначно определен старший член каждого полинома $f \in k[x_1, x_2, \dots, x_n]$. Тогда для каждого идеала I мы можем определить его *идеал старших членов* следующим образом.

Определение 2.7. Пусть $I \subset k[x_1, x_2, \dots, x_n]$-ненулевой идеал.

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

(ii) Обозначим через $<$LT(I)$>$ идеал, порожденный элементами из LT(I).

Мы уже видели важную роль старших членов в алгоритме деления. Следует отметить один тонкий, но важный момент в определении $<$LT(I)$>$. А именно, пусть I конечно порожден, $I =< f_1, f_2, \dots, f_s >$. Тогда $<$LT(f_1), ..., LT(f_s)$>$ и <LT(I)> могут быть *разными* идеалами. Конечно, LT(f_i) $\in$ LT(I)$\subset$<LT(I)>; поэтому $<$LT(f_1), ..., LT(f_s)$>$ $\subset$<LT(I)>. Однако <LT(I)> может быть строго больше. Рассмотрим следующий пример.

Пример 2.4. Пусть $I =< f_1, f_2 >$, где $f_1 = x^3 - 2xy$, $f_2 = x^2y - 2y^2 + x$, и на мономах из $k[x, y]$ задано grlex-упорядочение. Тогда

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

так что $x^2 \in I$, $x^2 = LT(x^2) \in < LT(I) >$. С другой стороны, x^2 не делится на $LT(f_1) = x^3$ и на $LT(f_2) = x^2y$. Поэтому $x \notin < LT(f_1), LT(f_2) >$ по лемме 1.4. из главы 1.

Мы докажем, что <LT(*I*)> - мономиальный идеал. Это позволит нам применить результаты. В частности, это означает, что <LT(*I*)> порожден конечным множеством старших членов.

Предложение 2.1. *Пусть* $I \subset k[x_1, x_2, \dots, x_n]$ - *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), …,LT(g_s)>.

Теперь, используя предложение 2.1. и алгоритм деления, мы можем доказать конечную порожденность *любого* полиномиального идеала. Это дает утвердительный ответ на вопрос об описании идеала. Пусть $I \subset k[x_1, x_2, \dots, x_n]$ - некоторый идеал, и пусть <LT(*I*)> - его идеал старших членов. Как всегда, мы считаем, что заданно некоторое мономиальное упорядочение, используемое в алгоритме деления.

Теорема 2.3. (теорема Гильберта о базисе) *Каждый идеал* $I \subset k[x_1, x_2, \dots, x_n]$ *является конечно порожденным, т.е.* $I =< g_1, \dots, g_s >$, *где* $g_1, \dots, g_s \in I$.

Доказательство. Если I={0}, то наше порождающее множество состоит из одного элемента – нулевого полинома. Если I - ненулевой идеал, то порождающее множество $g_1, \dots, g_s$ мы будем строить следующим образом. Из предложения 2.1. вытекает, что существуют полиномы $g_1, \dots, g_s \in I$, такие, что <LT(*I*)>=<LT(g_1), …,LT(g_s)>. Мы утверждаем, что $I =< g_1, \dots, g_s >$.

Так как каждый g_i принадлежит I, то $< g_1, \dots, g_s > \subset I$. Пусть теперь $f \in I$-некоторый элемент. Применим алгоритм деления из §2 и поделим f на $g_1, \dots, g_s$. В результате f будет представлен в виде

$$f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + r,$$

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

$$r = f - a_1 f_1 - a_2 f_2 - \cdots - a_s f_s \in I.$$

Если $r \neq 0$, то LT(r) ∈ <LT(I)>=< LT(g_1),…,LT(g_s)>.Тогда по лемме 2.3 из §3 LT(r) должен делиться хотя бы на один LT(g_i). Но это противоречит определению остатка. Значит, r=0, т.е.

$$f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + 0 \in < g_1, \ldots, g_s >$$

откуда $I \subset < g_1, \ldots, g_s >$. Теорема доказана.

Базис $\{g_1, \ldots, g_s\}$ из теоремы 2.3. не только дает описание идеала, он обладает еще и специальным свойством <LT(I)>=< LT(g_1),…,LT(g_s)> . Как мы видели в примере 2.2. , не все базисы идеала обладают этим свойством. Таким базисам мы дадим специальное название.

Определение 2.8. Пусть задано мономиальное упорядочение. Конечное подмножество $G = \{g_1, \ldots, g_s\}$ элементов идеала I называется его базисом Гребнера (или стандартным базисом), если

<LT(g_1),…,LT(g_s)>=<LT(I)>.

Чуть менее формально это определение можно переформулировать так: множество $\{g_1, \ldots, g_s\} \subset I$ называется *базисом Грёбнера идеала I в том и только в том случае, когда старший член любого элемента из I делится на хотя бы один старший член $LT(g_i)$.* Из доказательства теоремы 2.3. также вытекает следующий результат.

Следствие 2.3. *Пусть задано некоторое мономиальное упорядочение. Тогда любой ненулевой идеал $I \subset k[x_1, x_2, \ldots, x_n]$ обладает базисом Грёбнера. Более того, базис Грёбнера идеала I является его базисом.*

Доказательство. Пусть I - ненулевой идеал и $G = \{g_1, \dots, g_s\}$ - 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),…,LT(g_s)>, то $I = < g_1, \dots, g_s >$, т.е. G является базисом в I.

В следующем параграфе мы подробно рассмотрим свойства базисов Грёбнера, в частности, мы увидим, что с их помощью можно решить задачу о принадлежности идеалу. Базисы Грёбнера и являются теми «хорошими» порождающими множествами, о которых мы говорили в конце §2.

Базисы Грёбнера идеалов в полиномиальных кольцах были открыты Б.Бухбергером в 1965 г. и названы им в честь В.Грёбнера (1899-1980) – научного руководителя Бухбергера. Родственное понятие «стандартного базиса» идеала в кольце степенных рядов было независимо введено Х.Хиронакой в 1964 г. Как мы увидим далее, Бухбергер также разработал основные алгоритмы для работы с базисами Грёбнера. Термин «базис Грёбнера» используется в английском написании «Groebner base» в качестве команды в некоторых системах компьютерной алгебры.

В конце этого параграфа мы рассмотрим два приложения теоремы Гильберта о базисе. Первое из них – это чисто алгебраическое утверждение об идеалах в $k[x_1, x_2, \dots, x_n]$.

Возрастающей цепью идеалов называется последовательность:

$$I_1 \subset I_2 \subset I_3 \subset \cdots \qquad (1)$$

Например, последовательность $< x_1 > \subset < x_1, x_2 > \subset \cdots \subset < x_1, \dots, x_n >$ образует конечную возрастающую цепь идеалов. Если мы попытаемся *продолжить* эту цепь идеалов с большим числом образующих, то мы столкнемся с одной из двух возможностей. Рассмотрим идеал $< x_1, \dots, x_n, f >$, $f \in k[x_1, x_2, \dots, x_n]$. Если же $f \in < x_1, \dots, x_n >$, то наш идеал

совпадает с идеалом $< x_1, \dots, x_n >$. Если же $f \notin < x_1, \dots, x_n >$, то $< x_1, \dots, x_n, f >= k[x_1, x_2, \dots, x_n]$, Другими словами, возрастающая цепь (1) может быть продолжена двумя способами: или путем повторения последнего идеала, или добавлением $k[x_1, x_2, \dots, x_n]$, а потом повторением его. В любом случае возрастающая цепь «стабилизируется» после конечного числа шагов в том смысле, что, начиная с некоторого момента, все идеалы в цепи одинаковы. Нашим следующим результатом будет теорема о том, что «стабилизация»происходит в *каждой* возрастающей цепи идеалов в $k[x_1, x_2, \dots, x_n]$.

Теорема 2.4.[15] (условие обрыва возрастающих цепей). *Пусть*

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

– *возрастающая цепь идеалов в* $k[x_1, x_2, \dots, x_n]$. *Тогда существует* $N \geq 1$, *такое, что*

$$I_N = I_{N+1} = I_{N+2} = \cdots$$

Утверждение о том, что возрастающая цепь идеалов в $k[x_1, x_2, \dots, x_n]$ стабилизируется, часто называется *условием обрыва возрастающих цепей* или, сокращенно, УОВЦ. УОВЦ будет играть ключевую роль в алгоритме Бухбергера для построения базисов Грёбнера.

Теорема Гильберта о базисе показывает, что имеет смысл говорить об аффинном многообразии, определенном *идеалом* $I \subset k[x_1, x_2, \dots, x_n]$.

Определение 2.9. Пусть $I \subset k[x_1, x_2, \dots, x_n]$ - некоторый идеал. Положим

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

Хотя ненулевой идеал содержит бесконечно много различных полиномов, множество $V(I)$ определено конечным числом полиномиальных уравнений.

Предложение 2.2. $V(I)$ *является аффинным многообразием. В частности, если* $I =< f_1, \dots, f_n >$, , *то* $V(I)=V(f_1, \dots, f_n)$.

Наиболее важным следствием этого предложения является то, что *многообразия определены идеалами.*

§5.Свойства базисов Гребнера

Предложение 2.3. *Пусть* $G = \{g_1, \dots, g_s\}$ *-базис Грёбнера идеала* $I \subset k[x_1, x_2, \dots, x_n]$*, и пусть* $f \in k[x_1, x_2, \dots, x_n]$*. Тогда существует единственный полином* $r \in k[x_1, x_2, \dots, x_n]$ *, который обладает следующими двумя свойствами:*

(i) *ни один член полинома* r *не делится ни на один из старших членов* $\langle \mathrm{LT}(g_1), \dots, \mathrm{LT}(g_s) \rangle$*;*

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

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

Остаток r называется *нормальной формой* полинома f. Фактически базисы Грёбнера могут быть охарактеризованы требованием единственности остатка.

Хотя единственность остатка и имеет место, но «частные» a_i , вычисляемые алгоритмом деления $f = a_1 g_1 + a_2 g_2 + \cdots + a_s g_s + r,$

зависят от порядка делителей даже в том случае, когда G – базис Грёбнера.

Рассмотрим это на следующем примере:

Пример 2.5. Поделим $f = xy^2z^2 + xy - yz$ на $f_1 = y - z^3$, на $f_2 = z^2 - 1$ и на $f_3 = x - y^2$, а также поделим $f = xy^2z^2 + xy - yz$ на $f_1 = x - y^2$, на $f_2 = y - z^3$ и на $f_3 = z^2 - 1$. Мы используем lex-упорядочение с $x>y>z$. Если проведем деление сами, то получим следующие схемы:

1. $a_1 : xyz^2 + xz^5 + x + yz + y + z^4 + z^3 - z$

$a_2 : xz^6 + xz^2 + xz + x + z^5 + z^4 + z^3 - z$

$a_3 : z + 1$

$$
\begin{array}{l}
y - z^3 \\
z^2 - 1 \\
x - y^2
\end{array}
\sqrt{\begin{array}{l}
xy^2z^2 + xy - yz \\
\underline{xy^2z^2 - y^4z^2} \\
\quad xyz^5 + xy - yz \\
\quad \underline{xyz^5 - xz^8} \\
\qquad xy + xz^8 - yz \\
\qquad \underline{xy - xz^3} \\
\qquad\quad xz^8 + xz^3 - yz \\
\qquad\quad \underline{xz^8 - xz^6} \\
\qquad\qquad xz^6 + xz^3 - yz \\
\qquad\qquad \underline{xz^6 - xz^4} \\
\qquad\qquad\quad xz^4 + xz^3 - yz \\
\qquad\qquad\quad \underline{xz^4 - xz^2} \\
\qquad\qquad\qquad xz^3 + xz^2 - yz \\
\qquad\qquad\qquad \underline{xz^3 - xz} \\
\qquad\qquad\qquad\quad xz^2 + xz - yz \\
\qquad\qquad\qquad\quad \underline{xz^2 - x} \\
\qquad\qquad\qquad\qquad xz + x - yz \\
\qquad\qquad\qquad\qquad \underline{xz - y^2z} \\
\qquad\qquad\qquad\qquad\quad x + y^2z - yz \\
\qquad\qquad\qquad\qquad\quad \underline{x - y^2} \\
\qquad\qquad\qquad\qquad\qquad y^2z + y^2 - yz \\
\qquad\qquad\qquad\qquad\qquad \underline{y^2z - yz^4} \\
\qquad\qquad\qquad\qquad\qquad\quad y^2 + y^4 - yz \\
\qquad\qquad\qquad\qquad\qquad\quad \underline{y^2 - yz^3} \\
\qquad\qquad\qquad\qquad\qquad\qquad yz^4 + yz^3 - yz \\
\qquad\qquad\qquad\qquad\qquad\qquad \underline{yz^4 - z^7} \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad yz^3 + yz - z^7 \\
\qquad\qquad\qquad\qquad\qquad\qquad\quad \underline{yz^3 - z^6} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad -yz + z^7 - z^6 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad \underline{-yz + z^4} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad z^7 + z^6 + z^4 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \underline{z^7 - z^5} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad z^6 + z^5 - z^4 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \underline{z^6 - z^4} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad z^5 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad \underline{z^5 - z} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad z^3 \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \underline{z^3 - z} \\
\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\quad z = r
\end{array}}
$$

$$a_1 : y^2z^2 + z$$
$$a_2 : y^3z^2 + y^2z^5 + yz^8 + yz^3 + z^{11} + z^6 - z$$
$$a_3 : z^{12} + z^{10} + z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z$$

$$\begin{array}{l} x - y^2 \\ y - z^3 \\ z^2 - 1 \end{array} \sqrt{\begin{array}{l} xy^2z^2 + xy - yz \\ \underline{xy^2z^2 - y^4z^2} \end{array}}$$

$$xy + y^4z^2 - yz$$
$$\underline{xy - y^3}$$
$$y^4z^2 + y - yz$$
$$\underline{y^4z^2 - y^3z^5}$$
$$y^3z^5 + y^3 - yz$$
$$\underline{y^3z^5 - y^2z^8}$$
$$y^3 + y^2z^8 - yz$$
$$\underline{y^3 - y^2z^3}$$
$$y^2z^8 + y^2z^3 - yz$$
$$\underline{y^2z^8 - yz^{11}}$$
$$y^2z^8 + yz^{11} - yz$$
$$\underline{y^2z^3 - yz^6}$$
$$yz^{11} + yz^6 - yz$$
$$\underline{yz^{11} - z^{14}}$$
$$yz^6 + yz - z^{14}$$
$$\underline{yz^6 - z^9}$$
$$-yz + z^{14} + z^9$$
$$\underline{-yz - z^4}$$
$$z^{14} + z^9 - z^4$$
$$\underline{z^{14} - z^{12}}$$
$$z^{12} + z^9 - z^4$$
$$\underline{z^{12} - z^{10}}$$
$$z^{10} + z^9 - z^4$$
$$\underline{z^{10} - z^8}$$
$$xyz + xy - yz$$
$$\underline{xyz - yz}$$
$$z^9 + z^8 - z^4$$
$$\underline{z^9 - z^7}$$
$$z^8 + z^7 - z^4$$
$$\underline{z^8 - z^6}$$
$$z^7 + z^6 - z^4$$
$$\underline{z^7 - z^6}$$
$$z^6 + z^5 - z^4$$
$$\underline{z^6 - z^4}$$
$$z^5$$
$$\underline{z^3 - z}$$
$$z = r$$

Следствие 2.4. *Пусть* $G = \{g_1, \dots, g_s\}$ *-базис Грёбнера идеала* $I \subset k[x_1, x_2, \dots, x_n]$*, и пусть* $f \in k[x_1, x_2, \dots, x_n]$*. Тогда* $f \in I$ *в том и только в том случае, когда остаток от деления* f *на* G *равен нулю.*

Доказательство. Если остаток равен нулю, то, как уже отмечалось, $f \in I$. Обратно, пусть $f \in I$. Тогда равенство $f = f + 0$ удовлетворяет обоим условиям предложения 2.3. Из единственности представления полинома f в таком виде следует, что 0 является остатком от деления f на G.

Свойство, сформулированное в следствии 2.4., иногда используется как определение базиса Грёбнера: можно доказать, что G обладает этим свойством в том и только в том случае, когда является базисом Грёбнера.

Определение 2.10. 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 2.3 его можно рассматривать как (неупорядоченное) множество.

Пусть, например, $F = (x^2y - y^2, x^4y^2 - y^2) \subset k[x, y]$ и используется lex–упорядочение. Тогда

$$\overline{x^5y}^F = xy^3,$$

потому что применение алгоритма деления дает

$$x^5y = (x^3 + xy)(x^2y - y^2) + 0 \cdot (x^4y^2 - y^2) + xy^3.$$

Теперь мы обсудим, как определить, является данный базис идеала его базисом Грёбнера или нет. Как мы уже отмечали, «препятствием» к тому, чтобы набор $\{f_1, \dots, f_s\}$ был базисом Грёбнера, является существование такой полиномиальной комбинации полиномов f_i, что ее старший член не принадлежит идеалу) < LT(f_1),…,LT(f_s)>,. Это может произойти, например, в том случае, когда в некоторой комбинации $\alpha x^\alpha f_i - b x^\beta f_j$ старшие члены полиномов $\alpha x^\alpha f_i$ и $b x^\beta f_j$ *сокращаются.* Но $\alpha x^\alpha f_i - b x^\beta f_j \in I$, так что

старший член этой комбинации принадлежит <LT(I)>. Именно это и происходит в примере 2.3 из §2 . Для изучения сокращений мы определим специальные комбинации.

Определение 2.11. Пусть $f, g \in k[x_1, x_2, \dots, x_n]$– ненулевые полиномы.

(i) Пусть $multideg(f) = \alpha$ и $multideg(g) = \beta$. Положим $\gamma = (\gamma_1, \dots, \gamma_n) = max(\alpha_i, \beta_i)$ для любого i. Тогда x^γ называется *наименьшим общим кратным* мономов LM(f) и LM(g). Используется обозначение x^γ = LCM(LM(f), LM(g)).LCM-аббревиатура английского термина least common multiple.

(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.)

Пусть, например, $f = x^3y^2 - x^2y^3 + x$, $g = 3x^4y + y^2$, $f, g \in R[x, y]$, и используется grlex–упорядочение. Тогда $\gamma = (4,2)$ и

$$S(f, g) = \frac{x^4y^2}{x^3y^2} \cdot f - \frac{x^4y^2}{3x^4y} \cdot g =$$

$$= x \cdot f - (1/3) \cdot y \cdot g =$$

$$= -x^3y^3 + x^2 - (1/3)y^3.$$

S-полином S(f, g) специально «сконструирован» для сокращения старших членов. Фактически следующая лемма утверждает, что любое сокращение старших членов в комбинациях полиномов одинаковой мультистепени связано с сокращениями в S–полиномах.

Лемма 2.5. *Рассмотрим сумму* $\sum_{i=1}^{s} c_i f_i$, *где* $multideg(f_i) = \delta \in Z_{\geq 0}^n$, *а* $c_i \in k$ *для всех* i. *Если* $multideg(\sum_{i=1}^{s} c_i f_i) < \delta$, *то* $\sum_{i=1}^{s} c_i f_i$ *является линейной комбинацией с коэффициентами в* k S –*полиномов* $S(f_j, f_l)$, $1 \leq j, 1 \leq l$. *Более того, мультистепень каждого* $S(f_j, f_l)$ *меньше* δ.

Если $f_1, \dots, f_s$ удовлетворяют условиям леммы 2.5., то

$$\sum_{i=1}^{n} c_i f_i = \sum_{j,l} c_{jl}\, S(f_j, f_l)$$

Посмотрим, где именно происходит сокращение. В сумме слева каждое слагаемое $c_i f_i$ имеет мультистепень δ, т.е. сокращение получается в результате суммирования. С другой стороны, в сумме справа каждое слагаемое $c_{jl} S(f_j, f_l)$ имеет мультистепень $< \delta$, т.е. сокращение уже произошло. Интуитивно это означает, что S–полиномы как бы «ответственны» за все сокращения.

Используя S–полиномы и лемму 2.5 мы можем теперь доказать следующий критерий (принадлежащий Бухбергеру) того, что базис идеала является базисом Грёбнера.

Теорема 2.5. *Пусть I – некоторый полиномиальный идеал. Тогда базис $G = \{g_1, \dots, g_s\}$ идеала является базисом Грёбнера в том и только в том случае, когда для всех пар $i \neq j$ остаток от деления $S(g_i, g_j)$ на G (в любом порядке) равен нулю.*

§6.Алгоритм Бухбергера

В следствии 2.3. из § 4 доказано, что каждый ненулевой идеал в $k[x_1, x_2, \dots, x_n]$ имеет базис Грёбнера. К сожалению, доказательство неконструктивно в том смысле, что оно не дает никаких указаний, как можно построить базис Грёбнера. В этом параграфе будет решаться следующая задача: как построить базис Грёбнера заданного идеала $I \subset k[x_1, x_2, \dots, x_n]$?

Теорема 2.6. *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 $\{p, q\}$, в G' DO

$S \coloneqq \overline{S(p,q)}^{G'}$

$IF\ S \neq 0\ THEN\ G \coloneqq G \cup \{S\}$

$UNTIL\ G = G'$

Базисы Грёбнера, построенные с помощью алгоритма теоремы 2.6., часто оказывается избыточными – большими, чем необходимо. Мы можем исключить лишние образующие, используя следующий факт.

Лемма 2.6. *Пусть* G *– базис Грёбнера полиномиального идеала* I*, и пусть* $p \in G$, $LT(p) \in < LT(G - \{p\}) >$. *Тогда* $G - \{p\}$ *также является базисом Грёбнера для* I.

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

Определение 2.12. *Минимальным базисом Грёбнера* полиномиального идеала I называется его базис Грёбнера G, такой, что

(i) LC(p)=1 для всех $p \in G$;

(ii) $LT(p) \notin < LT(G - \{p\}) >$ для всех $p \in G$.

Минимальный базис Грёбнера для данного ненулевого идеала можно построить с помощью алгоритма из теоремы 2.6. с последующим применением леммы 2.6. для исключения лишних образующих.

Определение 2.13. *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 принадлежит $< LT(G - \{p\}) >$.

Предложение 2.4. *Пусть* $I \neq 0$ *- полиномиальный идеал, и пусть задано некоторое мономиальное упорядочение. Тогда существует единственный редуцированный базис Грёбнера идеала* I.

Во многих системах компьютерной алгебры реализован алгоритм Бухбергера для вычисления базисов Грёбнера. Эти системы, как правило, находят базис, элементы которого отличаются от элементов редуцированного базиса постоянным множителем. Это означает, что базисы, вычисляемые разными системами, по существу совпадают. Таким образом, полученные результаты легко проверить, переходя от одной системы к другой.

Другим следствием единственности, доказанной в предложении 2.4., является то, что теперь у нас есть *алгоритм проверки равенства идеалов.* Пусть нам даны два множества $\{f_1, \dots, f_s\}$ и $\{g_1, \dots, g_t\}$. Как выяснить, порождают они разные идеалы или один и тот же? Ответ: задайте мономиальное упорядочение и вычислите редуцированные базисы Грёбнера для $< f_1, \dots, f_s >$ и $< g_1, \dots, g_t >$. Идеалы совпадают в том и только в том случае, когда совпадают редуцированные базисы.

Заключение по главе II

Во второй главе изучены упорядочения мономов в полиномиальном кольце от n переменных, алгоритм деления в $k[x_1, \ldots \ldots . x_n]$, мономиальные идеалы, лемма Диксона, теорема Гильберта о базисе, базисы Грёбнера, свойства базисов Грёбнера, алгоритм вычисления базисов Грёбнера.

Основные результаты по главе II:

- Изучены мономиальные упорядочения на $k[x_1, \ldots \ldots . x_n]$, такие как lex- упорядочение, grlex- упорядочение, grevlex- упорядочение.
- Обобщен алгоритм деления в кольце $k[x]$ на общий случай полиномиального кольца $k[x_1, \ldots \ldots . x_n]$.
- Изучены мономиальные идеалы, лемма Диксона, позволяющая решить задачи описания идеала и принадлежности идеалу в мономиальном случае.
- Изучены теорема Гильберта о базисе, базисы Грёбнера, свойства базисов Грёбнера. Нежелательные свойства алгоритма деления в $k[x_1, \ldots \ldots . x_n]$ не проявляются, если делители образуют базис Грёбнера, т.е. в этом случае остаток от деления определен однозначно.
- Изучен алгоритм Бухбергера позволяющий строить базис Грёбнера любого заданного идеала $I \subset k[x_1, \ldots \ldots . x_n]$.

ГЛАВА 3

ПРИЛОЖЕНИЯ БАЗИСОВ ГРЁБНЕРА

§1.Задача о принадлежности идеалу

В первой главе мы сформулировали три задачи об идеалах и многообразиях. Первая из этих задач – задача описания идеала, была решена в § 4 главы второй с помощью теоремы Гильберта о базисе. Здесь мы рассмотрим, как базисы Грёбнера могут помочь нам при решении двух оставшихся задач.

Одновременное использование базисов Грёбнера и алгоритма деления дает следующий *алгоритм решения задачи о принадлежности идеалу:* пусть даны идеал $I =< f_1, \dots, f_s >$ и полином f; надо выяснить, принадлежит f идеалу I или нет. Сначала, применяя алгоритм Бухбергера (или аналогичный), находим базис Грёбнера $G = \{g_1, \dots, g_t\}$ для I. Тогда

$f \in I$ в том и только в том случае, когда $\bar{f}^G = 0$.

Пример 3.1. Пусть $I =< f_1, f_2 >=< xz - y^2, x^3 - z^2 > \subset C[x, y, z]$, и пусть используется grlex-упорядочение. Рассмотрим полином

$f = -4x^2y^2z^2 + y^6 + 3z^5$. Верно ли, что $f \in I$?

Множество образующих не является базисом Грёбнера, потому что LT(I) содержит, например, полином LT(S(f_1, f_2))=LT($-x^2y^2 + z^3$) $= x^2y^2$, который не принадлежит идеалу $<$ LT(f_1),LT(f_2) $>=< xz, x^3 >$. Следовательно, на первом шаге необходимо найти базис Грёбнера G для I.
Сначала используя S-полиномы вручную найдем базиси Грёбнера:
$I =< f_1, f_2 >=< xz - y^2, x^3 - z^2 > \subset C[x, y, z]$, grlex-упорядочение,
$f_1 = xz - y^2$, $f_2 = x^3 - z^2$, $f_1, f_2 \in C[x, y, z]$
Так как $\alpha = (1,0,1)$, $\beta = (3,0,0)$ $\Rightarrow \gamma = (3,0,1)$.

$\Rightarrow \quad S(f_1, f_2) = \frac{x^3 z}{xz} \cdot f_1 - \frac{x^3 z}{x^3} \cdot f_2 = x^2(xz - y^2) - z(x^3 - z^2) = x^3 z - x^2 y^2 - x^3 z + z^3 = -x^2 y^2 + z^3;$

$I =< f_1, f_2 >=< xz - y^2, x^3 - z^2 >, \quad S(f_1, f_2) = -x^2 y^2 + z^3 \in I$ и остаток от деления $(-x^2 y^2 + z^3)$ на $F = \{f_1, f_2\}$ равен $-x^2 y^2 + z^3 \neq 0.$

Добавим остаток $f_3 = -x^2 y^2 + z^3$ в порождающее множество. Теперь $F = \{f_1, f_2, f_3\}$. Применим критерий того, что базис идеала является базисом Грёбнера (Th. G).

Имеем $S(f_1, f_2) = -x^2 y^2 + z^3 = f_3,$ значит $\overline{S(f_1, f_2)}^F = 0.$

Вычислим $S(f_1, f_3)$. Так как $\alpha = (1,0,1), \ \beta = (2,2,0) \ \Rightarrow \ \gamma = (2,2,1).$

$\Rightarrow \quad S(f_1, f_3) = \frac{x^2 y^2 z}{xz} \cdot f_1 - \frac{x^2 y^2 z}{(-x^2 y^2)} \cdot f_3 = xy^2(xz - y^2) + z(-x^2 y^2 + z^3) = x^2 y^2 z - xy^4 - x^2 y^2 z + z^4 = -xy^4 + z^4,$ но $\overline{S(f_1, f_3)}^F = -xy^4 + z^4 \neq 0.$

Следовательно, мы должны добавить остаток $f_4 = -xy^4 + z^4$ к порождающему множеству, т.е. $F = \{f_1, f_2, f_3, f_4\}$. Имеем

$$\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = 0.$$

Вычислим $S(f_1, f_4)$. Так как $\alpha = (1,0,1), \ \beta = (1,4,0) \ \Rightarrow \ \gamma = (1,4,1).$

$\Rightarrow \quad S(f_1, f_4) = \frac{xy^4 z}{xz} \cdot f_1 - \frac{xy^4 z}{(-xy^4)} \cdot f_4 = y^4(xz - y^2) + z(-xy^4 + z^4) = xy^4 z - y^6 - xy^4 z + z^5 = -y^6 + z^5.$

Следовательно, мы должны добавить остаток $f_5 = -y^6 + z^5$ к порождающему множеству, т.е. $F = \{f_1, f_2, f_3, f_4, f_5\}$. Имеем

$$\overline{S(f_1, f_2)}^F = \overline{S(f_1, f_3)}^F = \overline{S(f_1, f_4)}^F = 0.$$

Вычислим $S(f_1, f_5)$. Так как $\alpha = (1,0,1), \ \beta = (0,6,0) \ \Rightarrow \ \gamma = (1,6,1).$

$\Rightarrow \quad S(f_1, f_5) = \frac{xy^6 z}{xz} \cdot f_1 - \frac{xy^6 z}{(-y^6)} \cdot f_5 = y^6(xz - y^2) + xz(-y^6 + z^5) = xy^6 z - y^8 - xy^6 z + xz^6 = xz^6 - y^8 = z^5 \cdot f_1 - y^2 \cdot f_5.$

$\Rightarrow \overline{S(f_1, f_5)}^F = 0.$

Вычислим $S(f_2, f_3)$. Так как $\alpha = (3,0,0), \ \beta = (2,2,0) \ \Rightarrow \ \gamma = (3,2,0).$

$\Rightarrow \ S(f_2, f_3) = \frac{x^3 y^2}{x^3} \cdot f_2 - \frac{x^3 y^2}{(-x^2 y^2)} \cdot f_3 = y^2(x^3 - z^2) + x(-x^2 y^2 + z^3) = x^3 y^2 - y^2 z^2 - x^3 y^2 + xz^3 = xz^3 - y^2 z^2 = z^2 \cdot f_1.$

$\Rightarrow$ легко проверить, что $\overline{S(f_2,f_3)}^F = 0$.

Вычислим $S(f_2,f_4)$. Так как $\alpha = (3,0,0),\ \beta = (1,4,0) \Rightarrow \gamma = (3,4,0)$.

$\Rightarrow \quad S(f_2,f_4) = \frac{x^3y^4}{x^3}\cdot f_2 - \frac{x^3y^4}{(-xy^4)}\cdot f_4 = y^4(x^3-z^2) + x^2(-xy^4+z^4) = x^3y^4 - y^4z^2 - x^3y^4 + x^2z^4 = x^2z^4 - y^4z^2 = (xz^3+y^2z^2)\cdot f_1$.

$\Rightarrow$легко вычислить, что $\overline{S(f_2,f_4)}^F = 0$.

Вычислим $S(f_2,f_5)$. Так как $\alpha = (3,0,0),\ \beta = (0,6,0) \Rightarrow \gamma = (3,6,0)$.

$\Rightarrow \quad S(f_2,f_5) = \frac{x^3y^6}{x^3}\cdot f_2 - \frac{x^3y^6}{(-y^6)}\cdot f_5 = y^6(x^3-z^2) + x^3(-y^6+z^5) = x^3y^6 - y^6z^2 - x^3y^6 + x^3z^5 = x^3z^5 - y^6z^2 = (x^2z^4 + xy^2z^3 + y^4z^2)\cdot f_1$.

$\Rightarrow$ легко проверить, что $\overline{S(f_2,f_5)}^F = 0$.

Вычислим $S(f_3,f_4)$. Так как $\alpha = (2,2,0),\ \beta = (1,4,0) \Rightarrow \gamma = (2,4,0)$.

$\Rightarrow \quad S(f_3,f_4) = \frac{x^2y^4}{(-x^2y^2)}\cdot f_3 - \frac{x^2y^4}{(-xy^4)}\cdot f_4 = -y^2(-x^2y^2+z^3) + x(-xy^4+z^4) = x^2y^4 - y^2z^3 - x^2y^4 + xz^4 = xz^4 - y^2z^3 = z^3\cdot f_1$.

$\Rightarrow$ легко вычислить, что $\overline{S(f_3,f_4)}^F = 0$.

Вычислим $S(f_3,f_5)$. Так как $\alpha = (2,2,0),\ \beta = (0,6,0) \Rightarrow \gamma = (2,6,0)$.

$S(f_3,f_5) = \frac{x^2y^6}{(-x^2y^2)}\cdot f_3 - \frac{x^2y^6}{(-y^6)}\cdot f_5 = -y^4(-x^2y^2+z^3) + x^2(-y^6+z^5) = x^2y^6 - y^4z^3 - x^2y^6 + x^2z^5 = x^2z^5 - y^4z^3 = (xz^4+y^2z^3)\cdot f_1$.

$\Rightarrow$ легко вычислить, что $\overline{S(f_3,f_5)}^F = 0$.

Вычислим $S(f_4,f_5)$. Так как $\alpha = (1,4,0),\ \beta = (0,6,0) \Rightarrow \gamma = (1,6,0)$.

$S(f_4,f_5) = \frac{xy^6}{(-xy^4)}\cdot f_4 - \frac{xy^6}{(-y^6)}\cdot f_5 = -y^2(-xy^4+z^4) + x(-y^6+z^5) = xy^6 - y^2z^4 - xy^6 + xz^5 = xz^5 - y^2z^4 = z^4\cdot f_1$.

$\Rightarrow$ легко проверить, что $\overline{S(f_4,f_5)}^F = 0$.

Таким образом, $\overline{S(f_i,f_j)}^F = 0$ для $1 \le i \le j \le 5$ и $F = (f_1,f_2,f_3,f_4,f_5)$.

$\Rightarrow \quad \{f_1,f_2,f_3,f_4,f_5\} = \{xz-y^2, x^3-z^2, -x^2y^2+z^3, -xy^4+z^4, -y^6+z^5\}$ – базис Грёбнера

Используя компьютерную систему, получаем

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{xz - y^2, x^3 - z^2, x^2y^2 - z^3, xy^4 - z^4, y^6 - z^5\}.$$

Отметим, что это редуцированный базис.

Теперь вопрос о принадлежности идеалу сводится к делению f на G:

$$f = 0 \cdot f_1 + 0 \cdot f_2 - 4z^2 f_3 + 0 \cdot f_4 + 1 \cdot f_5 + 0.$$

Так как остаток от деления равен нулю, то $f \in I$.

Пример 3.2. Пусть $I =< f_1, f_2 >=< -x^3 + y,\ x^2y - z >\subset C[x, y, z]$, и пусть используется lex-упорядочение. Рассмотрим полином

$f = xy^3 + y^5 - z^3 - z^2$. Верно ли, что $f \in I$?

Множество образующих не является базисом Грёбнера. Следовательно, на первом шаге необходимо найти базис Грёбнера G для I. Используя компьютерную систему, получаем

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{x^3 - y, x^2y - z, xy^3 - z^2, xz - y^2, y^5 - z^3\}.$$

Отметим, что это редуцированный базис.

Теперь вопрос о принадлежности идеалу сводится к делению f на G:

$$f = 0 \cdot f_1 + 0 \cdot f_2 + 1 \cdot f_3 + 0 \cdot f_4 + 1 \cdot f_5 + 0.$$

Так как остаток от деления равен нулю, то $f \in I$.

Пример 3.3. Необходимо выяснить, принадлежит ли полином

$f = x^3z - 2y^2$ идеалу

$I =< f_1, f_2, f_3 >=< xz - y, xy + 2z^2, y - z >\subset C[x, y, z]$.

Множество образующих не является базисом Грёбнера. Следовательно, на первом шаге необходимо найти базис Грёбнера G для I. Используя компьютерную систему, получаем

$$G = \{f_1, f_2, f_3\} = \{xz - z, y - z, 2z^2 + z\}.$$

Отметим, что это редуцированный базис.

Теперь вопрос о принадлежности идеалу сводится к делению f на G:

$$f = (x^2 + x + 1) \cdot f_1 + (-2y - 2z) \cdot f_2 - 1 \cdot f_3 + 2z.$$

Так как остаток от деления равен $2z$ то $f \notin I$.

В качестве другого примера возьмем $f = xy - 5z^2 + x$. Здесь можно даже не проводить процесс деления – очевидно, что $f \notin I$. Причина состоит в том, что LT(f) $= xy$ не принадлежит идеалу $< LT(G) >=< xz, x^3, x^2y^2, xy^4, y^6 >$, т.е. $\bar{f}^G \neq 0$, так что $f \notin I$.

Последнее наблюдение иллюстрирует, как форма элементов базиса Грёбнера отражает свойства идеала.

§2. Решение полиномиальных уравнений

Техника базисов Грёбнера может быть применена для решения систем полиномиальных уравнений. Рассмотрим несколько примеров.

Пример 3.4. Рассмотрим систему уравнений

$$z^2 - 2xyz + 5x = 0,$$

$$xy^2 + yz^3 = -2,$$

$$3xy^2 - 8z^3 = 0$$

в C^3. Эти уравнения задают идеал

$I =< z^2 - 2xyz + 5x, xy^2 + yz^3 + 2{,}3xy^2 - 8z^3 > \subset C[x, y, z]$. Наша задача – найти все точки многообразия V(I). Мы можем это сделать, используя любой базис идеала. Посмотрим, что получится, если мы будем работать с базисом Грёбнера.

Мы будем использовать lex-упорядочение.

Подключение пакета Groebner

>with(groebner);

[*finduni*, *finite*, *gbasis*, *gsolve*, *leadmon*, *normalf*, *solvable*, *spoly*]

Исходная система нелинейных алгебраических уравнений

>Poly:=[$z^2 - 2xyz + 5x, xy^2 + yz^3 + 2{,}3xy^2 - 8z^3$]:

Построение базиса Грёбнера

>G:=gbasis(Poly, [x, y, z], plex);

>G:=[$75x - 32z^5 - 16z^3 + 15z^2 - 12, 9y - 64z^5 - 60z^4 - 32z^3 - 48z - 24,$ $9 + 24z^3 + 24z^5 + 32z^8 + 16z^6 + 30z^7$]

Если мы внимательно посмотрим на эти полиномы, то увидим нечто замечательное. Во-первых, зависит только от и его корни легко вычисляются (найдем его корни численным методом)

>Solution3:=fsolve(G[3], {z}, complex);

>Solution3:={z=-1.257524095}, {z=-0.6585138286},

{z=-0.3731823784-0.9314701991 i}, {z=-0.3731823784+0.9314701991 i}

{z=0.2884504292-0.7377676589 i} {z=0.2884504292+0.7377676589 i}

{z=0.5740009112-0.4561342620 i} {z=0.5740009112-0.4561342620 i}

что дает нам восемь возможных значений *z*. Далее, подставляя каждое из этих значений в g_1 и в g_2, мы однозначно определяем *x* и *y*.

>for SolutionZ in Solution3 do

>SolutionY:=solve(subs(SolutionZ, G[2]),{y}):

>SolutionX:=solve(subs(SolutionY, SolutionZ, G[1]), {x}):

>print(SolutionX, SolutionY, SolutionZ);

>od:

{x=-1.922255456},{y=-1.660937467},{z=-1.257524095};

{x=-0.04048115000},{y=4.337158513},{z=-0.6585138286};

{x=0.09180008067+0.09284298307 i},{y=-4.467891369+0.8209128856 i},

{z=-0.3731823784-0.9314701991 i};

{x=0.09180008067-0.09284298307 i},{y=-4.467891369-0.8209128856 i},

{z=-0.3731823784+0.9314701991 i};

{x=0.284281410+0.1699085812 i},{y=0.9515756133+1.759803448 i},

{z=0.2884504292-0.7377676589 i};

{x=0.284281410-0.1699085812 i},{y=0.9515756133-1.759803448 i},

{z=0.2884504292+0.7377676589 i}

{x=0.01133844519+0.04814451309 i},{y=-0.488461424-4.583563612 i},

{z=0.5740009112-0.4561342620 i};

{x=0.01133844519-0.04814451309 i},{y=-0.488461424+4.583563612 i},

{z=0.5740009112+0.4561342620 i}.

Таким образом, система имеет восемь решений, два вещественных и шесть комплексных. Так как $V(I) = V(g_1, g_2, g_3)$,то тем самым мы нашли все решения системы.

Пример 3.5. Найдем точки в C^3, принадлежащие многообразию

$$V(x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z).$$

Используя lex-упорядочение, найдем базис Грёбнера для идеала

$$I =< x^2 + y^2 + z^2 - 1, x^2 + y^2 + z^2 - 2x, 2x - 3y - z >.$$

Получим следующий базис:

$$g_1 = 2x - 1,$$

$$g_2 = 3y + z - 1,$$

$$g_3 = 40z^2 - 8z - 23.$$

Отметим, что g_3 зависит только от z, и его корни легко вычисляются (они являются корнями квадратного уравнения):

$$z_1 = \frac{1}{10} + \frac{3}{20}\sqrt{26},$$

$$z_2 = \frac{1}{10} - \frac{3}{20}\sqrt{26}.$$

Далее, подставляя каждое из этих значений в уравнения $g_1 = 0$ и $g_2 = 0$, мы однозначно определяем x и y.

Таким образом, система $g_1 = g_2 = g_3 = 0$ имеет два решения:

$$x_1 = \frac{1}{2}, y_1 = \frac{3}{10} - \frac{1}{20}\sqrt{26}, z_1 = \frac{1}{10} + \frac{3}{20}\sqrt{26},$$

$$x_2 = \frac{1}{2}, y_2 = \frac{3}{10} + \frac{1}{20}\sqrt{26}, z_2 = \frac{1}{10} - \frac{3}{20}\sqrt{26}.$$

Так как $V(I) = V(g_1, g_2, g_3)$, то тем самым мы нашли все решения системы.

Как нам удалось решить эти системы? Ответ на этот вопрос дают теоремы об исключении и продолжении.

Теоремы об исключении и продолжении

Чтобы понять, как работает процедура исключения, рассмотрим пример. Мы будем решать систему уравнений

$$\begin{aligned} x^2 + y + z &= 1, \\ x + y^2 + z &= 1, \\ x + y + z^2 &= 1. \end{aligned} \tag{1}$$

Пусть

$$I = (\, x^2 + y + z = 1, x + y^2 + z = 1, x + y + z^2 = 1). \tag{2}$$

Тогда базис Грёбнера этого идеала по отношению к lex-упорядочению состоит из четырех полиномов

$$\begin{aligned} g_1 &= x + y + z^2 - 1, \\ g_2 &= y^2 - y - z^2 + z, \\ g_3 &= 2yz^2 + z^4 - z^2, \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2. \end{aligned} \tag{3}$$

Системы (1) и (3) имеют одинаковое множество решений. Но так как

$$g_4 = z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z^2 + 2z - 1)$$

зависит только от z то возможными значениями z могут быть только корни полинома g_4, т.е. 0, 1 и $-1 \pm \sqrt{2}$. Подставляя их в $g_2 = y^2 - y - z^2 + z = 0$ и в $g_3 = 2yz^2 + z^4 - z^2 = 0$, мы можем определить возможные значения y. А затем $g_1 = x + y + z^2 - 1 = 0$ позволит

определить x. Таким образом, мы получаем, что система (1) имеет в точности 5 решений:

$$(1,0,0), (0,1,0), (0,0,1),$$

$$\left(-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}\right),$$

$$\left(-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}\right).$$

Как же нам удалось решить систему? Наш успех стал возможным по двум причинам:

- (Шаг исключения) Мы смогли найти следствие $g_4 = z^6 - 4z^4 + 4z^3 - z^2 = 0$ исходных уравнений системы, которое зависит только от z, т.е. мы исключили x и y из системы уравнений.
- (Шаг продолжения) Как только мы нашли решения простого уравнения $g_4 = 0$, т.е. нашли значения z то смогли продолжить эти решения до решений исходных уравнений.

Основная идея *теории исключения* состоит в том, что и шаг исключения, и шаг продолжения должны рассматриваться в большей общности.

Посмотрим, как работает шаг исключения. Тот факт, что g_4 зависит только от z, означает, что

$g_4 \in I \cap C[z]$,

где идеал I задан равенством (2). На самом деле множество $I \cap C[z]$ состоит из *всех* тех следствий исходных уравнений, которые не зависят от x и y. Обобщая это наблюдение, приходим к следующему определению.

Определение 3.1. Пусть дан идеал $I =< f_1, \dots, f_s > \subset k[x_1, x_2, \dots, x_n]$. Тогда l-м *исключающим идеалом* I_l называется идеал в $k[x_{l+1}, \dots, x_n]$, равный

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

Другими словами, I_l состоит из всех следствий системы $f_1 = \cdots = f_s = 0$, которые не зависят от переменных $x_1, \dots, x_l$. В упражнениях мы проверим, что I_l в самом деле является идеалом в $k[x_{l+1}, \dots, x_n]$. Отметим, что $I = I_0$ является нулевым (по номеру) исключающим идеалом. Также отметим, что изменение порядка переменных приводит к другим исключающим идеалам.

На этом языке исключение переменных $x_1, \dots, x_l$ означает нахождение ненулевых полиномов в l-м исключающем идеале I_l. Таким образом, *решение шага исключения означает предъявление процедуры построения элементов из* I_l. При правильном упорядочении базисы Грёбнера сразу решают эту задачу.

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

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

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

Теорема об исключении показывает, что базис Грёбнера в случае lex-упорядочения исключает не только первую переменную, но и первые две переменные, первые три переменные и т.д.

Теперь рассмотрим шаг продолжения. Пусть дан идеал $I \subset k[x_1, \dots, x_n]$. Мы будем рассматривать аффинное многообразие

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

Как найти все его точки? Основная идея – строить решения, определяя одну координату за другой. Пусть $1 \leq l \leq n$. Рассмотрим исключающий идеал I_l.

Точка $(a_{l+1}, \dots, a_l) \in V(I_l)$ называется *частичным решением* исходной системы. Чтобы продолжить $(a_{l+1}, \dots, a_n)$ до полного решения системы, нам сначала нужно добавить одну координату. Это означает, что надо найти a_l такое, что $(a_l, \dots, a_n) \in V(I_{l-1})$. Точнее, пусть $I_{l-1} = \langle g_1, \dots, g_r \rangle \subset k[x_1, \dots, x_n]$. Нам нужно найти решения $x_l = a_l$ системы уравнений

$$g_1(x_l, a_{l+1}, \dots, a_n) = \cdots = g_r(x_l, a_{l+1}, \dots, a_n) = 0.$$

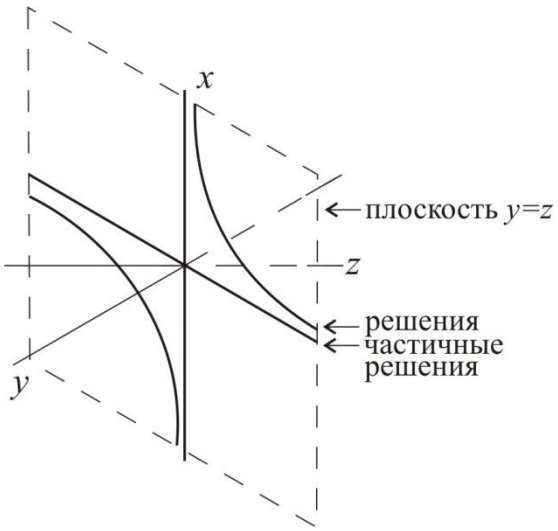
Так как здесь мы работаем с полиномами от одной переменной x_l, то a_l является корнем наибольшего делителя этих r полиномов.

Это рассуждение позволяет сформулировать основную проблему: приведенные выше полиномы могут не иметь общего корня, т.е. может существовать частичное решение, не имеющее продолжения до полного. В качестве примера рассмотрим систему

$$xy = 1$$

$$xz = 1 \qquad (4)$$

Здесь $I = \langle xy - 1, xz - 1 \rangle$, и из теоремы об исключении следует, что $y - z$ порождает первый исключающий идеал I_1. Частичные решения описываются формулой (a, a) и все они продолжаются до полного решения $(1, a, a, a)$, кроме частичного решения $(0,0)$. Рассмотрим геометрию этого явления. Уравнение $y = z$ задает плоскость в трехмерном пространстве. Многообразие (4) – гипербола, лежащая в этой плоскости:



Очевидно, что многообразие, определенное уравнениями (4), не имеет точек, лежащих над частичным решением $(0,0)$. Теперь наша цель – понять, как определить *заранее*, какие частичные решения могут быть продолжены до полного.

Ограничимся случаем исключения первой переменной x_1, т.е. мы хотим узнать, может ли частичное решение $(a_2, \dots, a_n) \in V(I_1)$ быть продолжено до решения $(a_1, a_2, \dots, a_n) \in V(I)$? Следующая теорема отвечает на этот вопрос.

Теорема 3.2. (теорема о продолжении). *Пусть* $I = \langle f_1, \dots, f_s \rangle \subset C[x_1, x_2, \dots, x_n]$, *и пусть* I_1- *первый исключающий идеал для* I. *Для каждого* $1 \le i \le s$ *запишем* f_i *в виде*

$f_i = g_i(x_2, \dots, x_n)x_1^{N_i} +$ *члены, содержащие* x_1 *в степени* $< N_i$, *где* $N_i \ge 0$, *а* $g_i \in C[x_2, \dots, x_n]$ - *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* $a_1 \in C$, *такое, что* $(a_1, a_2, \dots, a_n) \in V(I)$.

Отметим сначала, что теорема формулируется для поля $k = C$. Чтобы понять почему, положим $k = R$ и рассмотрим систему

$$x^2 = y$$

$$x^2 = z.$$

Исключая x, получаем $y = z$, т.е. (a, a) является частичным решением для всех $a \in R$. Так как старшие коэффициенты по x в $x^2 - y$ и $x^2 - z$ не обращаются в нуль, то теорема о продолжении гарантирует продолжаемость решений (a, a) *при условии*, что мы работаем над C. Над R ситуация иная. Уравнение $x^2 = a$ не имеет вещественных решений, если a отрицательно, т.е. только частичные решения с $a \geq 0$ продолжаются до вещественных решений системы (5). Этот пример показывает, что теорема о продолжении не имеет места над R.

Теперь рассмотрим условие $(a_2, \dots, a_n) \notin V(g_1, \dots, g_s)$. Напомним, что g_i - это старшие коэффициенты полиномов f_i по отношению к переменной x_1, т.е. условие $(a_2, \dots, a_n) \notin V(g_1, \dots, g_s)$ означает, что старшие коэффициенты не обращаются одновременно в нуль на частичном решении. Чтобы понять необходимость этого условия, вернемся к системе (4). Эта система

$$xy = 1,$$

$$xz = 1$$

имеет частичные решения $(y, z) = (a, a)$. Единственное непродолжаемое решение (0,0) - как раз то, которое обращает в нуль старшие коэффициенты при x (т.е. y и z). Теорема о продолжении утверждает, что *шаг продолжения может не выполниться, если старшие коэффициенты одновременно равны нулю*.

Наконец, следует отметить, что многообразие $V(g_1, \dots, g_s)$, где старшие коэффициенты $g_1, \dots, g_s$ обращаются в нуль, зависит от базиса $\{f_1, \dots, f_s\}$ идеала I: изменяя базис идеала, мы можем изменить $V(g_1, \dots, g_s)$.

Хотя теорема о продолжении сформулирована для случая исключения первой переменной x_1, она может применяться для исключения любого набора переменных. Рассмотрим, например, уравнения

$$x^2 + y^2 + z^2 = 1,$$

$$xyz = 1.$$

Базис Грёбнера идеала $I = \langle x^2 + y^2 + z^2 - 1, xyz - 1\rangle$ по отношению к lex-упорядочению состоит из двух элементов

$$g_1 = y^4z^2 + y^2z^4 - y^2z^2 + 1,$$

$$g_2 = x + y^3z + yz^3 - yz.$$

По теореме об исключении

$$I_1 = I \cap C[y, z] = \langle g_1\rangle,$$

$$I_2 = I \cap C[z] = \{0\}.$$

Так как $I_2 = \{0\}$, то $V(I_2) = C$ и, значит, *любое* $c \in C$ является частичным решением. Теперь требуется решить следующий вопрос:

Какие частичные решения $c \in C = V(I_2)$ продолжаются до $(a, b, c) \in V(I)$?

Идея состоит в пошаговом продолжении c: сначала до (b, c), потом до (a, b, c). На каждом шаге теорема указывает, какие решения продолжаются. Ключевым здесь является факт, что I_2 есть первый исключающий идеал для I_1. Это очевидно для нашего примера, а общий случай разобран в упражнениях. Применим теорему о продолжении, чтобы перейти от $c \in V(I_2)$ к $(b, c) \in V(I_1)$, а затем к $(a, b, c) \in V(I)$. Тогда мы и узнаем, какие c продолжаются.

Сначала применим теорему о продолжении для перехода от I_2 к $I_1 = \langle g_1\rangle$. Старший коэффициент в g_1 (при y^4) равен z^2; поэтому $c \in C = V(I)$ продолжается до (b, c), если $c \neq 0$. Следует отметить, что уравнение $g_1 = 0$ вообще не имеет решений при $c = 0$. Следующий шаг – это переход от I_1 к I, т.е. поиск такого a, что $(a, b, c) \in V(I)$. Если мы подставим $(y, z) = (b, c)$ в (6), то получим два уравнения относительно x, причем совсем не очевидно,

что они имеют общее решение $x = a$. Здесь теорема о продолжении показывает свою силу. Старшие коэффициенты при x в $x^2 + y^2 + z^2 - 1$ и $xyz - 1$- это 1 и yz соответственно. Так как 1 не обращается в нуль, то теорема о продолжении *гарантирует* существование общего решения a. Мы доказали, что все частичные решения $c \neq 0$ продолжаются до элемента из $V(I)$.

Особенно удобно применять теорему о продолжении, когда один из старших коэффициентов – константа. Зафиксируем этот полезный случай как отдельное утверждение.

Следствие 3.1. *Пусть* $I = \langle f_1, \dots, f_s \rangle \subset C[x_1, x_2, \dots, x_n]$, *и пусть* f_i *для некоторого* i *имеет следующий вид:*

$$f_i = cx_1^N + \textit{члены, которые содержат } x_1 \textit{ в степени } < N,$$

где $c \in C$- *ненулевая константа и* $N > 0$. *Пусть* I_1 - *первый исключающий идеал и* $(a_2, \dots, a_n) \in V(I_1)$. *Тогда существует* $a_1 \in C$, *такое, что* $(a_1, a_2, \dots, a_n) \in V(I)$.

Доказательство. Это утверждение прямо следует из теоремы о продолжении: так как $g_i = c \neq 0$, то многообразие $V(g_1, \dots, g_s)$ пусто и $(a_2, \dots, a_n) \notin V(g_1, \dots, g_s)$ для всех частичных решений. □

В заключение мы рассмотрим систему уравнений, не имеющую хороших решений. Пусть даны уравнения

$$xy = 4,$$

$$y^2 = x^3 - 1.$$

Базис Грёбнера для lex-упорядочения имеет вид

$$g_1 = 16x - y^2 - y^4,$$

$$g_2 = y^5 + y^3 - 64.$$

Полином $y^5 + y^3 - 64$, однако, не имеет рациональных корней (на самом деле он неприводим над Q). Нам остается найти приближенные значения корней. Получаем

$$y = 2.21363,\ -1.78719 \pm 1.3984i \text{ или } 0.680372 \pm 2.26969i.$$

Эти значения можно подставить в $g_1 = 16x - y^2 - y^4 = 0$ и найти x. Здесь, в отличие от предыдущих примеров, мы можем найти только приближенные решения.

Заключение по главе III

Одновременное использование базисов Грёбнера и алгоритма деления дало алгоритм решения задачи о принадлежности идеалу. Для этого, во первых, найдем базис Грёбнера для заданного идеала $I =< f_1, \dots, f_s >$; во вторых, поделим полином f на этот базис, используя алгоритм деления. Тогда полином f принадлежит идеалу I в том и только в том случае, когда остаток от деления равен нулю.

Техника базисов Грёбнера была применена для решения систем полиномиальных уравнений. Полученные выводы теоретически основываются на теореме об исключении и теореме о продолжении.

ЗАКЛЮЧЕНИЕ

В диссертационной работе на тему: «Базисы Грёбнера и их приложения» были изучены основные понятия алгебраической геометрии, а именно: идеал, аффинные многообразия, идеалы в кольце $k[x]$, упорядочение мономов в полиномиальном кольце от n переменных, алгоритм деления в $k[x_1, \dots, x_n]$, мономиальные идеалы, лемма Диксона, теорема Гильберта о базисе, базисы Грёбнера, свойства базисов Грёбнера, алгоритм Бухбергера для вычисления базисов Грёбнера и их приложения к ряду задач.

В этой диссертационной работе были успешно решены следующие задачи:

- задача о принадлежности идеалу;
- решение систем полиномиальных уравнений;
- написана программа, позволяющая делить любой многочлен $f \in k[x_1, \dots, x_n]$ на конечную совокупность многочленов $f_1, \dots, f_s \in k[x_1, \dots, x_n]$ с получением промежуточных частных и остатка.

Одновременное использование базисов Грёбнера и алгоритма деления дало нам алгоритм решения задачи о принадлежности идеалу. Для этого для заданного идеала $I =< f_1, \dots, f_s >$ необходимо найти базис Грёбнера, а затем, используя алгоритм деления, поделить полином f на этот базис. Тогда полином f принадлежит идеалу I в том и только в том случае, когда остаток от деления равен нулю.

Техника базисов Грёбнера была также применена для решения систем полиномиальных уравнений.

ЛИТЕРАТУРА

1. Adams W., Loustaunan P. (1994), An Intoduction to Groebner Bases, Graduate Studias in Mathematics, 3 Amer. Soc. Providence.

2. Cox D., Little J., O'Shea D. (1998), Using Algebraic Geometry, Springer – Verlag, New York – Berlin – Heidelberg.

3. Dube T.W. (1990) The structure of polynomial ideals and Groebner bases, SIAM J.Comput., 19. 750-755.

4. Акритас А. Основы компьютерной алгебры с приложениями. М.: Мир, 1995.

5. Аржанцев И.В. Базисы Грёбнера и системы алгебраических уравнений// М. Ж. МЦНМО, 2003.

6. Атья М., Макдональд И. Введение в коммутативную алгебру.- М.: Мир, 1972

7. Бухбергер Б. Алгоритмический метод в теории полиномиальных идеалов// Компьютерная алгебра. Символика и алгебраические вычисления. М.: Мир, 1986.

8. Ван дер Варден Б.Л. Алгебра. – М.:Наука,1979.

9. Говорухин В., Цибулин П., Компьютер в математическом исследовании. –С-Питербург, Питер, 2002.

10. Давенпорт Дж., Сире Й., Турнье Е. Компьютерная алгебра. – М.: Мир,1991.

11. Каримов И.А. Обеспечить поступательное и устойчивое развитие страны - важнейшая задача. Ташкент, март 2009.

12. Каримова М.А. Задача о принадлежности идеалу.- Самарканд, Магистрантларнинг XIV илмий конференцияси материаллари, 2014.

13. Кириенко Денис Павлович, Система компьютерной алгебры Maple, Среднее общеобразовательная школа №179 МИОО, г.Москва.

14. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. – М.:Мир,2000.

15. Курош А.Г. Курс высшей алгебры. – М.:Наука,1971.

16. Ленг С. Алгебра. – М.:Мир, 1968.

17. Мамфорд Д. Алгебраическая геометрия. Комплексные алгебраические многообразия.- М. Мир, 1979.

18. Нарзуллаев У.Х. Алгебра и теория чисел. Часты 1,2,3,4. Lambert Academic Publishing, Germany, 2012

19. Нарзуллаев У.Х., Каримова М. Грёбнер базислари хакида.- Ташкент: Замонавий ахборот-коммуникация технологиялари// ТАТУ Самарканд филиали профессор-укитувчиларининг X илмий-амалий конференцияси материаллари туплами, 2015.

20. Нарзуллаев У.Х., Сэттарова Э.С. Применение алгоритма Бухбергера для решения задачи о принадлежности идеалу. – Ташкент: Труды международной научно-практической конференции Инновация, 2006.

21. Прохоров Г.В., Колбеев В.В., Желнов К.И., Леденев М.А., Математический пакет Maple V Release 4.- Калуга, «Облиздат», 1998.

22. Сэттарова Э.С. Задача о принадлежности идеалу. – Самарканд, Магистрантларнинг V илмий анжумани материаллари, 2005.

23. Сэттарова Э.С., Каримова М.А. Задача о принадлежности идеалу. – Ташкент: «Амалий математика ва ахборот хавфсизлиги» илмий-техник конференция материаллари, 2014.

24. Сэттарова Э.С. Решение систем полиномиальных уравнений. – Самарканд, Магистрантларнинг VI илмий анжумани материаллари, 2006.

25. Уокер Р. Алгебраические кривые. –М.: ИЛ, 1952.

26. Ходж В., Пидо Д. Методы алгебраической геометрии. Тт. I-III - М.: ИЛ, 1954,1955.

27. Шарафаревич И.Р. Основы алгебраической геометрии. – М.:Наука, 1972.

28. Яцкин Н.И. Теоремы и алгоритмы. Изд.: «Ивановский государственный университет», 2006.

29. www.ziyonet.uz.

30.www.math.ru.

31.www.wikipedia.ru.

32.www.math.net.

33.www.mat-net.ru.