СИСТЕМЫ ПОЛИНОМИАЛЬНЫХ УРАВНЕНИЙ, ИДЕАЛЫ И ИХ БАЗИСЫ-ДЕЛИТЕЛИ

Методическая разработка для 1 курса ММФ

Автор — проф. НГУ Чуркин В.А.

ПРЕДИСЛОВИЕ

Алгебру обычно понимают как искусство символьных вычислений. Такие вычисления часто возникают при моделировании практических задач, а искусство заключается не только в решении одной конкретной задачи, но и в умении разделить класс данных символьных задач на разрешимые и неразрешимые, оценить трудоемкость решения, найти наиболее экономное решение и т.п.

Одна из старейших символьных систем — алгебра многочленов от одной или нескольких переменных — казалось бы хорошо известна. Более двух тысяч лет алгоритму Евклида для вычисления наибольшего общего делителя, позволяющего, в частности, определить совместность конечной системы полиномиальных уравнений от одной переменной. Разложение на множители, отыскание точной формулы для корней многочлена от одной переменной или приближенный поиск корней — классические задачи алгебры. Успех в частных случаях и понимание причин сложности решения задач в общем случае были достигнуты трудом многих математиков. Здесь можно вспомнить славные имена Ньютона, Гаусса, Галуа, Лобачевского ....

Для многочленов от нескольких переменных метод их исключения в системах *линейных* уравнений, часто называемый методом Гаусса, на самом деле был известен в Китае по крайней мере за два тысячелетия до нашего времени. Решение *нелинейных* систем

полиномиальных уравнений от нескольких переменных — гораздо более трудная задача. Только в прошлом веке появились методы исследования некоторых таких систем с помощью результантов Сильвестра (аналогов детерминантов) в предположении, что удается решить полиномиальные уравнения от одной переменной. Чуть позднее появились результаты общего характера — знаменитые теоремы Гильберта о базисе и о корнях для полиномиальных идеалов. Стало ясно, что, во-первых, всякая бесконечная система полиномиальных уравнений от конечного числа переменных равносильна некоторой конечной подсистеме и, во-вторых, имеется взаимно однозначное соответствие между алгебраическими многообразиями (множествами решений систем полиномиальных уравнений) над алгебраически замкнутым полем и радикальными идеалами в алгебре многочленов. Оба факта лежат в основе алгебраической геометрии, недавно увенчавшей свой путь решением великой проблемы Ферма. Тем не менее и после Гильберта на вопрос: "Как решить данную систему полиномиальных уравнений?" — ответа не было. Многие другие задачи конструктивного характера о многочленах оставались нерешенными. Отметим, что здесь нас интересуют, в основном, точные решения систем, а не их аппроксимация.

Удивительный сдвиг произошел в этой области на наших глазах в последние тридцать лет. В 1965 г. молодой австрийский математик Бруно Бухбергер защитил докторскую диссертацию под руководством алгебро-геометра Вольфганга Грёбнера. В диссертации был представлен метод вычисления базиса (как векторного пространства) для фактор-алгебры $K[X]/I$ алгебры многочленов от нескольких переменных над полем K, если идеал I задан конечным порождающим множеством. Заключается он в переработке данного порождающего множества идеала в такой конечный "базис", что *старший член любого многочлена идеала делится на старший член подходящего многочлена этого базиса*. Через 10–15 лет этот, на первый взгляд, рядовой результат привел к серьезным успехам в символьном решении широкого класса математических задач — от решения систем полиномиальных и дифференциальных уравнений к конструктивизации части алгебраической геометрии, теории инвариантов, теории Галуа вплоть до проблемы автоматического доказательства геометрических теорем и построения криптографических систем.

Сама идея вычисления "базиса-делителя" идеала по старшим членам настолько проста, что могла бы с успехом излагаться в средней школе, и настолько естественна, что алгоритм Евклида и метод Гаусса — частные случаи метода вычислений. И ранее, и позднее подобные идеи возникала и развивалась независимо другими математиками для решения аналогичных задач. Так А.И. Ширшов еще в 1962 г. реализовал ее для некоторых идеалов свободных алгебр Ли, используя представимость элементов свободной алгебры Ли в виде многочленов от нескольких переменных с *некоммутативным*, но ассоциативным умножением. Кнут и Бендикс в 1970 г. предложили аналогичный "метод переписывающих систем", годный для очень широкого класса символьных языков. Поэтому мы будем использовать для такого базиса идеала нейтральное и напоминающее его основное свойство название "базис-делитель", хотя более распространены названия "базис Грёбнера", "базис

Грёбнера-Ширшова", "стандартный базис" и др.

Вместе с серьезными достижениями прежних лет в области кодирования информации и ввиду успешной реализации символьных вычислений на компьютерах эти результаты позволили в итоге заявить о новой области математики — компьютерной алгебре. В короткое время по этой теме было опубликовано не менее пятисот статей. Параллельно были созданы мощные пакеты прикладных программ, основанные на символьных вычислениях. Появилась явная необходимость познакомить с новыми идеями и студентов-математиков. Наша цель — изложить достаточно подробно, с полными доказательствами, метод построения базисов-делителей идеалов и показать на примерах, как они используются для решения конкретных задач.

Отметим, что вплоть до недавнего времени на русском языке не было учебной литературы по данной теме, доступной для студентов. Недавно появился перевод [3] замечательной книги Кокса, Литтла и О'Ши, которую мы рекомендуем для всех желающих глубже познакомиться с теорией базисов-делителей. Изложенный там материал конечно шире и богаче примерами, чем это краткое пособие для студентов 1 курса.

ТЕОРЕМА ГИЛЬБЕРТА О БАЗИСЕ

Как известно, системы уравнений называются равносильными, если множества их решений совпадают. Другими словами, каждое уравнение одной системы должно быть "следствием" уравнений другой системы. Для полиномиальных уравнений можно указать следующий простейший способ вывода "следствий": уравнение $f = 0$ следует из уравнений $f_1 = 0,\ f_2 = 0, \ldots,\ f_s = 0$, если $f = f_1u_1 + f_2u_2 + \ldots + f_su_s$ для некоторых многочленов $u_1, \ldots,\ u_s$. Таким образом, множество левых частей следствий замкнуто относительно умножения на произвольный многочлен и относительно сложения. Мы пришли к широко используемому понятию идеала.

Определение. Непустое подмножество I коммутативного кольца R называется *идеалом*, если для любых a, b из I, c из R элементы $a - b$, ac принадлежат I.

В этом случае используется обозначение $I \lhd R$. Всегда идеалами будут нулевой $\{0\}$ и само кольцо R — они называются тривиальными. Легко проверить также, что множество $\langle a_1, \ldots, a_s\rangle = \{a_1c_1 + \ldots + a_sc_s :\ c_1, \ldots, c_s \in R\}$ всегда образует идеал в кольце R.

Определение. Подмножество F идеала I коммутативного кольца R с единицей *порождает идеал* I, если всякий элемент из I имеет вид $f_1u_1+f_2u_2+\ldots+f_su_s$ при подходящих $f_1, \ldots, f_s$ из F, $u_1, \ldots, u_s$ из R. Иногда в этой ситуации F называют *базисом идеала* I, хотя однозначности представления элемента идеала через такой базис нет, и используют обозначение $\langle F\rangle = I$. Если множество порождающих F можно выбрать конечным, то идеал I называется *конечно порожденным*.

Очевидно, если $F = \{f_\alpha(x_1, \ldots, x_n) :\ \alpha \in A\}$ и $G = \{g_\beta(x_1, \ldots, x_n) :\ \beta \in B\}$ — два базиса одного идеала, то системы уравнений

$$f_\alpha(x_1, \ldots, x_n) = 0,\ \alpha \in A,$$

и

$$g_\beta(x_1, \ldots, x_n) = 0,\ \beta \in B,$$

равносильны.

Допустим, что мы хотим заменить бесконечную систему полиномиальных уравнений на равносильную конечную. Тогда достаточно установить, что справедлива следующая

Теорема Гильберта о базисе. В алгебре многочленов от конечного числа переменных всякий идеал конечно порожден.

Доказательство. Отметим, что поле K имеет только тривиальные идеалы, которые конечно порождены. Используя индукцию по числу переменных и представление алгебры $K[x_1, \ldots x_n]$ в форме $R[x_n]$, где $R = K[x_1, \ldots, x_{n-1}]$, достаточно доказать, что *если* R *— кольцо, все идеалы которого конечно порождены, то и кольцо* $R[x]$ *такое же.*

Пусть J — идеал в $R[x]$ и пусть I — множество старших коэффициентов всех многочленов из J (полагаем, что старший коэффициент нулевого многочлена равен нулю). Тогда I — идеал в R. В самом деле, если $a,\ b$ из I, то найдутся такие многочлены f и g из J, что

$$f = ax^n + \ldots\ ,\quad g = bx^m + \ldots\ ,$$

где точками обозначены, как обычно, младшие члены для f и g. Можно считать, что $n \geq m$ и что $a \neq b$. Тогда многочлен

$$f - gx^{n-m} = (a - b)x^n + \ldots$$

принадлежит J и $a - b \in I$. Если c из R, то $cf = cax^n + \ldots,\quad ca \in I$.

По предположению идеал I порождается конечным множеством $\{a_1, \ldots, a_s\}$. Тогда существуют принадлежащие J многочлены

$$f_1 = a_1x^{n_1} + \ldots\ ,\ \ldots\ , f_s = a_sx^{n_s} + \ldots\ .$$

Пусть $m = \max\{n_1, \ldots, n_s\}$.

Если $f = ax^k + \ldots$ — элемент идеала J и $k \geq m$, то можно *исключить старший член* f следующим приемом. Поскольку a из I, то найдутся такие $b_1, \ldots, b_s$ из R, что $a = a_1b_1 + \ldots + a_sb_s$. Тогда

$$g = f - f_1b_1x^{k-n_1} - \ldots - f_sb_sx^{k-n_s}$$

является многочленом, содержится в идеале J и *ст.* $g <$ *ст.* f. Если еще *ст.* $g \geq m$, то можно исключить старший член g аналогичным приемом. Продолжая, получим многочлен

$$r = f - f_1u_1 - \ldots - f_su_s,\quad \textit{ст.}\, r < m.$$

Если $r = 0$, то $f = f_1u_1 + \ldots + f_su_s \in \langle f_1, \ldots, f_s\rangle$. Как действовать, если $r \neq 0$?

В этом случае старший коэффициент r содержится в множестве

$$I_k = \{\text{ст.к. } h : \ h \in J, \ \text{ст. } h < k \text{ или } h = 0\},$$

причем $k = \text{ст. } h < m$. Легко проверить, что I_k — идеал в R, и дальнейшее исключение старших членов для r вплоть до нуля возможно тем же приемом с помощью конечного множества многочленов $f_{s+1}, \ldots, f_t$ из J степеней $< m$, старшие коэффициенты которых порождают идеалы $I_{m-1}, \ I_{m-2}, \ldots, \ I_0$. Следовательно, идеал J порождается $f_1, \ldots, f_s, f_{s+1}, \ldots, f_t$.

Теорема доказана.

Следствие 1. Всякая бесконечная система полиномиальных уравнений от конечного числа переменных над полем равносильна своей конечной подсистеме.

Следствие 2. Всякая возрастающая цепочка полиномиальных идеалов выравнивается через конечное число шагов

$$I_k \lhd K[X], \quad I_1 \leq I_2 \leq \ldots \leq I_k \leq \ldots \Longrightarrow \exists N : I_N = I_{N+1} = I_{N+2} = \ldots \ .$$

Доказательство. Легко проверить, что объединение всех идеалов цепочки образует идеал $I = \bigcup I_k$, который порождается, в силу теоремы Гильберта о базисе, конечным числом многочленов $f_1, \ldots, f_s$. Пусть $f_j \in I_{k_j}, \ N = \max\{k_1, \ldots, k_s\}$. Тогда $f_1, \ldots, f_s \in I_N$ и потому $I = \langle f_1, \ldots, f_s \rangle \subseteq I_N$. Обратное включение $I_N \subseteq I$ очевидно, и, следовательно,

$$I_N = I_{N+1} = I_{N+2} = \ldots = I.$$

Упражнение. Докажите, что условие обрыва (выравнивания) любых возрастающих цепочек идеалов в кольце и условие конечной порождаемости любого идеала кольца равносильны.

Кольца с такими свойствами изучались Э.Нетер и впоследствии были названы *нетеровыми.*

УПОРЯДОЧЕНИЕ ОДНОЧЛЕНОВ

Пусть $X = (x_1, x_2, \ldots, x_n)$ — набор переменных или алфавит и

$$X^* = \{x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n} | \ k_1, k_2, \ldots, k_n - \text{ неотрицательные целые } \}$$

— множество всех формальных произведений перестановочных переменных. Относительно естественного умножения X^* образует коммутативную полугруппу с единицей, элементы которой — произведения переменных. Алгебра многочленов $K[X]$ с коэффициентами из поля K может рассматриваться как бесконечномерное векторное пространство с базисом X^*, умножение в котором получилось распространением умножения с базиса на пространство по закону дистрибутивности. Моделируя случай одной переменной, где важную

роль играет выделение старшего члена многочлена, нам надо научиться упорядочивать произведения переменных, причем так, что старший член произведения многочленов — произведение старших членов сомножителей.

Определение. Линейный порядок $>$ на X^* назовем (мультипликативно) *устойчивым*, если

$$u > v \Longrightarrow uw > vw, \quad u \neq 1 \Longrightarrow u > 1$$

для любых $u,\ v,\ w \in X^*$.

Вообще говоря, таких порядков много. Укажем наиболее часто встречающиеся на практике.

Словарный или лексикографический порядок $x_1 > x_2 > \ldots > x_n$ задается правилом

$$x_1^{k_1} \ldots x_n^{k_n} > x_1^{l_1} \ldots x_n^{l_n} \Longleftrightarrow (\exists i:\ k_i > l_i \text{ и } k_j = l_j \text{ при } j < i).$$

Иначе говоря, располагаем буквы в словах (т.е. произведениях переменных) в требуемом алфавитном порядке, а сами слова упорядочиваем почти как в словаре по *первому* встретившемуся различию в буквах при чтении слов слева направо. Конечно, этот порядок линеен и устойчив. Он будет полезен при исключениях неизвестных: если мы добились, что старший член многочлена в этом порядке не содержит переменной x_1, то тогда и все остальные (младшие) члены многочлена не будут содержать переменной x_1, хотя при этом возможно накопление больших показателей при других переменных даже если мы начинали с многочленов малой степени.

Изменяя порядок переменных, можно построить другие словарные порядки типа $x_{i_1} > x_{i_2} > \ldots > x_{i_n}$.

Степенно-словарный порядок устанавливается с приоритетом сравнения полных степеней, т.е. сумм показателей. Для него

$$u = x_1^{k_1} \ldots x_n^{k_n} > v = x_1^{l_1} \ldots x_n^{l_n} \Longleftrightarrow$$
$$\Longleftrightarrow (\sum k_i > \sum l_i \text{ или } \sum k_i = \sum l_i, \text{ но } u > v \text{ в словарном порядке}).$$

Требуемые свойства линейности и устойчивости проверяются просто. Порядков такого типа несколько за счет вариаций словарных порядков. Отметим, что при исключениях относительно степенно-словарных порядков степень не может увеличиться, более того, для многочлена степени k она гарантированно понижается через $\begin{pmatrix} n+k-1 \\ n-1 \end{pmatrix}$ шагов, которое равно количеству всех произведений n переменных полной степени k.

ТЕОРЕМА. Устойчивый порядок на полугруппе X^* нетеров, т. е. всякая убывающая последовательность произведений переменных выравнивается на конечном шаге.

Доказательство. Допустим, что существует бесконечная строго убывающая последовательность произведений переменных

$$u_1 > u_2 > u_3 > \ldots\ .$$

Идеал, порожденный всеми этими произведениями, конечно порожден ввиду теоремы Гильберта о базисе. Можно считать, что он порождается $u_1, \ldots, u_N$. Поэтому

$$u_{N+1} = \sum u_i h_i$$

для некоторых многочленов $h_1, \ldots, h_N$. Поскольку u_{N+1} — произведение переменных, то оно должно появиться как член правой суммы, т. е. $u_{N+1} = u_k v$, где $k \leq N$, а v — некоторое произведение переменных, $v \neq 1$. Ввиду устойчивости порядка $v > 1$ и $u_{N+1} = u_k v > u_k$, что противоречит убыванию последовательности $u_1,\ u_2,\ \ldots$.

Определение. Кольцо многочленов от нескольких переменных, для которого полугруппа произведений переменных снабжена устойчивым линейным порядком, будем называть *упорядоченным*.

Упр. Укажите старшие члены многочлена $x^3y^9 + 5x^4y^7 + 3x^5y^7$ относительно порядков а) словарного $x > y$, б) словарного $y > x$, в) степенно-словарного $x > y$. Покажите, что при *любом* устойчивом упорядочении одночлен $5x^4y^7$ не может быть старшим в этом многочлене.

Упр. Можно ли описать все устойчивые порядки на полугруппе произведений переменных, хотя бы в случае двух переменных? Покажите, что линеен и устойчив порядок

$$x^m y^n > x^k y^l \Leftrightarrow \alpha m + \beta n > \alpha k + \beta l,$$

где $\alpha,\ \beta$ — заранее заданные рационально независимые вещественные строки одинаковой длины, упорядоченные словарно.

ДЕЛЕНИЕ С ОСТАТКОМ

Теперь наша цель — установить для многочленов от нескольких переменных аналог деления с остатком для многочленов от одной переменной.

Фиксируем некоторый устойчивый порядок на полугруппе произведений переменных $x_1, \ldots, x_n$ и пусть f и g — два многочлена, причем $g \neq 0$. Предположим, что старший член v многочлена g делит некоторый одночлен w из f в кольце многочленов: $w = vu$. Тогда переход

$$f \xrightarrow{g} h = f - gu$$

назовем *элементарным делением f на g* (с остатком).

Будем говорить, что многочлен f *сводится* к многочлену r относительно множества многочленов G и кратко обозначать $f \xrightarrow{G} r$, если найдется конечная последовательность элементарных делений с началом f, концом r и делителями g_i из G:

$$f \xrightarrow{g_1} f_1 = f - g_1u_1 \xrightarrow{g_2} f_2 = f - g_1u_1 - g_2u_2 \xrightarrow{g_3} \ldots\ldots$$
$$\ldots \xrightarrow{g_k} f_k = f - g_1u_1 - g_2u_2 - \ldots - g_ku_k = r.$$

При этом многочлен r назовем *несводимым относительно* G или *остатком*, если далее последовательность элементарных делений относительно G продолжить невозможно. Это означает, что любой одночлен из r не делится на старшие члены многочленов из G.

Элементарное деление с остатком называют также элементарной редукцией, вместо сводимости говорят о редуцируемости, остаток называют нередуцируемым многочленом.

Лемма (о представлении многочлена через делители и остаток). Заданная последовательность элементарных делений многочлена f относительно множества многочленов $G = \{g_1, g_2, \ldots,\ g_s\}$, приводящая к остатку r, позволяет *конструктивно* находить такие многочлены $u_1, u_2, \ldots,\ u_s$, что

$$f = r + g_1u_1 + g_2u_2 + \ldots + g_su_s.$$

При этом все слагаемые g_iu_i имеют старшие члены не больше, чем старший член f.

Доказательство очевидно.

Мы видим, что такие определения конечно обобщают обычное деление с остатком для многочленов от одной переменной, где последовательность элементарных делений всегда обрывается на единственном остатке. Убедимся, что для многочленов от нескольких переменных любая последовательность элементарных делений также обязательно обрывается, но — вот беда — остатки могут быть разные!

Пример. Пусть $x,\ y$ — переменные и $x > y$ в словарном порядке. Пусть

$$f = x^2y - y,\ g_1 = xy - x,\ g_2 = x^2 - y.$$

Тогда

$$f \xrightarrow{g_1} (x^2y - y) - (xy - x)x = x^2 - y \xrightarrow{g_2} 0, \quad f = 0 + g_1x + g_2$$

или

$$f \xrightarrow{g_2} (x^2y - y) - (x^2 - y)y = y^2 - y = r \neq 0, \quad f = r + g_10 + g_2y.$$

Теорема. Любая последовательность элементарных делений многочлена f с остатком относительно множества многочленов G в упорядоченной алгебре многочленов обрывается через конечное число шагов.

Доказательство. Допустим противное: последовательность элементарных делений

$$f \longrightarrow f_1 \longrightarrow f_2 \longrightarrow \ldots$$

бесконечна. Старшие произведения этих многочленов образуют монотонно убывающую последовательность, которая по теореме о нетеровости устойчивых порядков на полугруппе произведений переменных выравнивается с номера i_1. Другими словами, начиная с номера i_1, все многочлены f_i имеют одинаковое старшее произведение u_1. Кроме того, с этого номера они обязаны содержать ненулевые вторые члены после старших, ввиду

предполагаемой бесконечности процесса элементарных делений. По той же теореме последовательность вторых членов выравнивается с номера i_2. Соответствующее старшее произведение u_2 таково, что $u_1 > u_2$, поскольку u_1 и u_2 входят в многочлен с номером i_2, u_1 — его старшее произведение. Далее с номера i_2 многочлены обязаны содержать ненулевые третьи члены, последовательность которых выравнивается с номера i_3 и дает произведение переменных u_3, меньшее, чем u_2. Продолжая в том же духе, получим строго убывающую последовательность произведений переменных $u_1 > u_2 > u_3 > \dots$. Но это противоречит теореме о нетеровости устойчивых порядков. Таким образом, наше допущение неверно и любая последовательность элементарных делений обрывается через конечное число шагов. Теорема доказана.

Упр. Представьте многочлен $f = 3x^3 + x^2(y-1) + x(2y^3 + y^2 + y) + 3x$ через делители $g_1 = x^2 + y^2,\ g_2 = xy + y^3 - y^2,\ g_3 = y^5 - 2y^4 + 2y^3$ и остаток при словарном порядке $x > y$.

БАЗИСЫ-ДЕЛИТЕЛИ

Здесь мы разберемся, когда остаток при сводимости относительно множества многочленов получается один и тот же независимо от выбора последовательности элементарных делений.

Определение. Конечное множество G многочленов называется *базисом-делителем* для идеала I упорядоченной алгебры многочленов $K[x_1, \dots, x_n]$, если

$$G \subset I,\ \ \forall f \in I\ \exists g \in G : \textit{ст.чл. } g \text{ делит } \textit{ст.чл. } f.$$

Сразу отметим три основных вопроса относительно базисов-делителей:

1) Насколько полезно это понятие, какие задачи мы можем решить, если знаем базис-делитель для идеала?

2) Всякий ли идеал алгебры многочленов имеет базис-делитель при данном упорядочении?

3) Наше определение не дает возможности проверить за конечное число шагов, что данное множество многочленов является базисом-делителем. Как все-таки проверить, что данное множество многочленов является базисом-делителем? Как построить базис-делитель за конечное число шагов, если идеал задан некоторой системой порождающих?

Здесь мы ответим на второй вопрос и частично затронем остальные.

Теорема 1. Всякий идеал алгебры многочленов от нескольких переменных над полем относительно любого устойчивого порядка имеет базис-делитель.

Доказательство. Пусть I — идеал в алгебре многочленов над полем и пусть J — идеал, порожденный всеми старшими членами многочленов из I. По теореме Гильберта о базисе идеал J конечно порожден и потому J порождается старшими членами конечного множества многочленов $G = \{g_1, \dots, g_s\}$ из I. Покажем, что G — базис-делитель для

идеала I. По построению G содержится в I. Если f из I, то *ст.чл.* f из J и существуют такие многочлены $u_1, \ldots, u_s$, что

$$\textit{ст.чл.}\, f = (\textit{ст.чл.}\, g_1)u_1 + \ldots + (\textit{ст.чл.}\, g_s)u_s.$$

Но тогда *ст.пр.* f обязано содержаться среди приведенных слагаемых в правой части равенства и потому *ст.чл.* g_k делит *ст.чл.* f при некотором k. Теорема доказана.

Следующая теорема, в частности, решает вопрос единственности остатков, дает алгоритм, определяющий вхождение данного многочлена в идеал, если известен его базис-делитель.

Теорема 2. Для идеала I упорядоченной алгебры многочленов $K[X]$ и конечного множества $G = \{g_1, \ldots, g_s\} \subset I$ следующие утверждения равносильны.

1) G — базис-делитель идеала I.

2) Для любого многочлена из $K[X]$ при любом выборе последовательности делений относительно G остатки совпадают, $I = \langle G \rangle$.

3) $f \in I \iff f \xrightarrow{G} 0$.

4) $(f \in I) \iff (\exists u_1, \ldots, u_s \in K[X] : f = g_1u_1 + \ldots + g_su_s,\ \textit{ст.пр.}\, f = \max\{\textit{ст.пр.}\, g_iu_i | i = 1, \ldots, s\})$.

5) $\langle \textit{ст.пр.}\, f \mid f \in I \rangle = \langle \textit{ст.пр.}\, g_1, \ldots, \textit{ст.пр.}\, g_s \rangle$.

Доказательство. 1) $\Rightarrow$ 2). Пусть $G = \{g_1, \ldots, g_s\}$ — базис-делитель и

$$f \xrightarrow{G} r_1 = f - g_1u_1 - \ldots - g_su_s,$$
$$f \xrightarrow{G} r_2 = f - g_1v_1 - \ldots - g_sv_s,$$

где $r_1,\ r_2$ — остатки. Если $r_1 \neq r_2$, то ненулевой многочлен $r_1 - r_2$ несводим относительно G. С другой стороны, $r_1 - r_2 = g_1(v_1 - u_1) + \ldots + g_s(v_s - u_s) \in I$, и потому $r_1 - r_2$ сводим относительно G, если G — базис-делитель. Следовательно, $r_1 = r_2 =: r$. Кроме того,

$$f \in I \iff r \in I \iff r = 0,\ f = g_1u_1 + \ldots + g_su_s \in \langle G \rangle.$$

2) $\Rightarrow$ 3). Если $f \in I = \langle G \rangle$, то $f = g_1h_1 + \ldots + g_sh_s = \sum_i g_i(\sum_j \alpha_{ij}v_{ij}) = \sum_i \sum_j \alpha_{ij}g_iv_{ij}$, где $\alpha_{ij} \in K,\ v_{ij} \in X^*$. Опуская индексы, покажем, что

$$\text{если } f \xrightarrow{G} r,\ \ r \text{ – остаток, то } f - \alpha gv \xrightarrow{G} r$$

для любых $g \in G,\ v \in X^*,\ \alpha \in K$. Возможны следующие случаи.

а) *ст.пр.* (gv) входит в f и соответствующий одночлен из f полностью сокращается в переходе $f \to f - \alpha gv$. Тогда этот переход — элементарное деление с остатком, продолжая которое в конце получим r ввиду единственности остатков.

б) *ст.пр.* (gv) не входит в f. Тогда есть элементарное деление с остатком $f - \alpha gv \to f$, продолжая которое получим в конце снова r.

в) *ст.пр.* (gv) входит в f и соответствующее произведение из f не уничтожается в переходе $f \to f - \alpha gv$. Тогда можно сначала элементарным делением с остатком уничтожить *ст.пр.* (gv) и в f, и в $f - \alpha gv$, перейдя к общему многочлену h, а затем добраться снова до r.

Теперь, после возможно многократного применения этого приема, получим

$$0 = f - \sum_i \sum_j \alpha_{ij} g_i v_{ij} \xrightarrow{G} r.$$

Но тогда $r = 0$.

Если $f \xrightarrow{G} r$, то ввиду леммы о представлении многочлена

$$f - r = g_1 u_1 + g_2 u_2 + \ldots + g_s u_s \in I.$$

Поэтому f и r лежат в одном смежном классе по идеалу I и f из I тогда и только тогда, когда r из I. Если r — ненулевой многочлен, то по свойству базиса-делителя элементарным делением его можно свести ниже. Поэтому если r — остаток, то $r = 0$ и $f \xrightarrow{G} 0$.

3) $\Rightarrow$ 4). Если $f \in I$, то $f \xrightarrow{G} 0$ и по лемме о представлении многочлена через делители и остаток получим требуемое выражение для f. Обратное включение очевидно.

4) $\Rightarrow$ 5). Если $f \in I$, то при подходящих $u_1, \ldots, u_s \in K[X]$ имеем

$$f = g_1 u_1 + \ldots + g_s u_s,\ \textit{ст.пр.}\, f = \max\{\textit{ст.пр.}\, g_i u_i | i = 1, \ldots, s\} \in \langle g_1, \ldots, g_s \rangle$$

.

5) $\Rightarrow$ 1). Если $f \in I$, то *ст.пр.* f = *ст.пр.* $(g_i u_i)$ = (*ст.пр.* g_i)(*ст.пр.* u_i) при некотором i, таким образом, G — базис-делитель для I.

Теорема доказана.

Мы можем теперь *сократить словосочетание* "базис-делитель для идеала относительно порядка" до более краткого "базис-делитель относительно порядка", поскольку соответствующий идеал всегда порождается его базисом-делителем.

Последняя теорема иногда позволяет распознать, будет ли данное множество F многочленов базисом-делителем или нет. Если удалось найти многочлен f, который сводится относительно F к двум разным остаткам, то тогда F не будет базисом-делителем. Наоборот, если удалось доказать, что остаток при любой сводимости относительно F один и тот же, то тогда F — базис-делитель.

Пример 1. Пусть $f_1 = x^3 - 1,\ f_2 = x^2 - 1,\quad f = x^3$ из алгебры $\mathbb{Q}[x]$. Тогда

$$f = x^3 = (x^3 - 1) + 1 \xrightarrow{f_1} 1,$$

$$f = x^3 = (x^2 - 1)x + x \xrightarrow{f_2} x \neq 1.$$

Следовательно, $F = \{f_1, f_2\}$ не является базисом-делителем.

Упражнение. Покажите, что в алгебре многочленов от одной переменной над полем всякий идеал является главным, так как порождается одним элементом — наибольшим общим делителем многочленов, порождающих идеал. В этом случае базис-делитель обязательно включает этот НОД.

Пример 2. Пусть $g_1 = x - p(z),\ g_2 = y - q(z)$. Покажем, что $G = \{g_1, g_2\}$ — базис-делитель относительно словарного порядка $x > y > z$. Очевидно, x и y — старшие члены соответственно g_1 и g_2. Любой процесс сводимости многочлена f относительно G прервется только тогда, когда в очередном остатке отсутствуют вхождения букв x и y, т.е. когда остаток $r(z)$ зависит только от z. При этом

$$f(x, y, z) - r(z) = (x - p(z))u(x, y, z) + (y - q(z))v(x, y, z)$$

для подходящих многочленов u и v. Подставляя в это полиномиальное равенство $x = p(z),\ y = q(z)$, получим, что $r(z) = f(p(z), q(z), z)$, и, следовательно, остаток при любой сводимости один и тот же. Теперь очевидно, что сопоставляя каждому смежному классу $f + I$ единственный содержащийся в нем остаток $r(z)$ при сводимости относительно G, получим изоморфизм фактор-алгебры $K[x, y, z]/I$ и алгебры $K[z]$.

В общем случае, если известен базис-делитель для идеала, то ввиду теоремы 2 мы можем за конечное число шагов распознать равенство смежных классов по идеалу, "вычислять" суммы и произведения смежных классов. Поскольку алгебра многочленов с коэффициентами из поля K является бесконечномерным векторным пространством над K, а идеалы — подпространства, то фактор-алгебра является фактор-пространством. Базисы-делители позволяют отыскать базис фактор-алгебры как векторного пространства, а если она конечна, то составить для нее таблицу умножения, тем самым задав фактор-алгебру полностью. Более сложный пример такого вычисления приведем после того как научимся строить базисы-делители для данного идеала.

Теперь ясно, что базис-делитель — важное понятие при работе с многочленами от нескольких переменных.

ЕДИНСТВЕННОСТЬ НЕСВОДИМЫХ БАЗИСОВ-ДЕЛИТЕЛЕЙ

Из определения базиса-делителя сразу следует, что всякое конечное подмножество из идеала, содержащее его базис-делитель, само будет базисом-делителем. Естественно для данного идеала попытаться найти базис-делитель, минимальный в следующем смысле.

Определение. Базис-делитель G идеала I называется *несводимым*, если всякий многочлен g из G не сводится относительно множества $G - \{g\}$ и *ст.к.* $g = 1$.

Теорема. Всякий ненулевой идеал упорядоченной алгебры многочленов над полем имеет единственный несводимый базис-делитель.

Доказательство. Построим сначала несводимый базис, исходя из некоторого базиса-делителя G. Если $g,\ h$ — различные многочлены из G и *ст.чл.* g делит *ст.чл.* h, то h можно

исключить из базиса: $G-\{h\}$ остается базисом-делителем идеала I. Таким образом, можно считать, что старшие члены многочленов из базиса-делителя попарно не делят друг друга. Если $g \xrightarrow{G-\{g\}} r$ и r — остаток, то старшие члены g и r совпадают, замена g на r снова дает базис-делитель. Такой процесс замен можно продолжить, но он обязательно прервется на несводимом базисе, поскольку иначе можно построить строго убывающую бесконечную последовательность одночленов. Осталось только разделить полученные многочлены на их старшие коэффициенты.

Теперь покажем единственность несводимой базиса. Пусть G и H — две несводимых базиса-делителя для идеала I. Для всякого g из G существует такой h из H, что ($ст.чл.\, h$) делит ($ст.чл.\, g$). В свою очередь, существует такой g' из G, что ($ст.чл.\, g'$) делит ($ст.чл.\, h$). Но тогда ($ст.чл.\, g'$) делит ($ст.чл.\, g$). Ввиду несводимости $g' = g$ и тогда $ст.чл.\, h = ст.чл.\, g$. Если $h \neq g$, то $ст.чл.\,(h-g)$ встречается, с точностью до числового множителя, среди младших членов либо многочлена g, либо h. Поскольку $h - g \in I$, то $ст.чл.\,(h-g)$ обязан делиться на старший член подходящего многочлена из $G-\{g\}$ и на старший член некоторого многочлена из $H-\{h\}$, что противоречит несводимости. Таким образом, $h = g$. Этот процесс сравнения многочленов из G и H можно продолжить без помех и далее. В итоге получим, что $G = H$.

ВЫЧИСЛЕНИЕ БАЗИСОВ-ДЕЛИТЕЛЕЙ

Здесь будет дан ответ на два важных вопроса:

1) Как проверить за конечное число шагов, что данное конечное множество многочленов является базисом-делителем для порожденного им идеала?

2) Как построить за конечное число шагов базис-делитель для идеала, заданного произвольным конечным порождающим множеством многочленов?

Сразу отметим, что последний алгоритм, построенный Бухбергером, включает в себя как алгоритм Евклида отыскания НОД, так и метод приведения к треугольному виду для систем линейных уравнений с помощью исключения неизвестных.

Определение. Пусть $\alpha u,\ \beta v$ — старшие члены многочленов f и g соответственно, где $\alpha,\ \beta$ — старшие коэффициенты, $u,\ v$ — старшие произведения переменных. Пусть w — наименьшее общее кратное $u,\ v$ и пусть $w = uu' = vv'$. Многочлен

$$f \triangle g = \frac{1}{\alpha} f u' - \frac{1}{\beta} g v' = \frac{w}{ст.чл.\, f} f - \frac{w}{ст.чл.\, g} g$$

назовем *срезкой* (пиков) пары многочленов $f,\ g$.[1]

Отметим сразу, что $g \triangle f = -(f \triangle g)$ и что $(\lambda f) \triangle (\mu g) = f \triangle g$ для ненулевых скаляров λ, μ.

[1] Бухбергер называет его S-полиномом от слова сизигия (упряжка) и обозначает $S(f, g)$.

Следующая теорема Бухбергера отвечает на первый вопрос, а следствие из нее — на второй.

Теорема. Пусть задано конечное множество $G = \{g_1, \ldots, g_s\}$ многочленов от переменных $x_1, \ldots, x_n$ над полем K. Тогда G — базис-делитель для $I = \langle G \rangle$ относительно данного упорядочения $K[x_1, \ldots, x_n]$, если и только если срезки всех пар из G сводятся относительно G к нулю:

$$g_i \triangle g_j \xrightarrow{G} 0, \quad i,\ j = 1, \ldots,\ s.$$

Доказательство. Если G — базис-делитель для идеала I, то $g_i \triangle g_j \xrightarrow{G} 0$ для всех $i,\ j$, поскольку $g_i \triangle g_j \in I$.

Пусть теперь $g_i \triangle g_j \xrightarrow{G} 0$ для всех $i,\ j$. Покажем, что G — базис-делитель. Можно считать, что *ст.к.* $g_i = 1$. Пусть $f \in I = \langle G \rangle$. Тогда

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

для некоторых многочленов h_i. Если *ст.пр.* f и "пик" $v_0 = \max\{\text{ст.пр.}\,(g_i h_i) : i = 1, \ldots, s\}$ слагаемых суммы (*) совпадают, то некоторый *ст.чл.* g_k делит *ст.чл.* f, т.е. выполнено требуемое свойство базиса-делителя. Однако в общем случае, точнее, когда $(\text{ст.пр. } f) < v_0$, в выражении для f старшие члены слагаемых могут сократиться при сложении и старший член f будет сформирован из младших членов слагаемых. Покажем, что тогда можно получить представление для f типа (*) с пиком $v_1 < v_0$.

Выделим сначала в сумме (*) все слагаемые с пиком v_0. Перенумерацией добьёмся, чтобы *ст.пр.* $(g_i h_i) = v_0$ только при $i = 1, \ldots, p$, где $p \le s$. Обозначая многоточием младшие члены многочленов, запишем

$$h_i = \alpha_i u_i + \ldots;\ f = \sum_{i=1}^{p} g_i h_i + \ldots = \sum_{i=1}^{p} g_i(\alpha_i u_i + \ldots) + \ldots = \sum_{i=1}^{p} \alpha_i (g_i u_i) + \ldots.$$

Многочлен $\widehat{f} = \sum_{i=1}^{p} \alpha_i (g_i u_i)$ включает сумму всех пиков выражения (*). Если обозначить $f_i = g_i u_i$, то *ст.чл.* $f_i = v_0$ при $i = 1, \ldots, p$. Поскольку *ст.пр.* $f < v_0$, то $\sum_{i=1}^{p} \alpha_i = 0$.

Ясно, что $f_i \triangle f_j = f_i - f_j$. Поэтому

$$\begin{gathered}\widehat{f} = \alpha_1 f_1 + \ldots + \alpha_p f_p = \alpha_1(f_1 - f_2) + (\alpha_1 + \alpha_2)(f_2 - f_3) + \ldots \\ \ldots + (\alpha_1 + \ldots + \alpha_{p-1})(f_{p-1} - f_p) + (\alpha_1 + \ldots + \alpha_{p-1} + \alpha_p) f_p = \\ = \alpha_1(f_1 \triangle f_2) + \ldots + (\alpha_1 + \ldots + \alpha_{p-1})(f_{p-1} \triangle f_p).\end{gathered}$$

Кроме того, обозначая $u_{ij} = \text{НОК}(\text{ст.пр. } g_i, \text{ст.пр. } g_j)$, имеем

$$f_i \triangle f_j = (g_i u_i) \triangle (g_j u_j) = \tfrac{v_0}{\text{ст. чл. } g_i u_i} g_i u_i - \tfrac{v_0}{\text{ст. чл. } g_j u_j} g_j u_j =$$

$$\tfrac{v_0}{\text{ст. чл. } g_i} g_i - \tfrac{v_0}{\text{ст. чл. } g_j} g_j = \tfrac{v_0}{u_{ij}} \left(\tfrac{u_{ij}}{\text{ст. чл. } g_i} g_i - \tfrac{u_{ij}}{\text{ст. чл. } g_j} g_j \right) = \tfrac{v_0}{u_{ij}} g_i \triangle g_j \xrightarrow{G} \tfrac{v_0}{u_{ij}} 0 = 0.$$

По лемме о представлении через делители и остаток найдутся такие многочлены h_{ik}, что

$$f_i - f_{i+1} = \sum_{k=1}^{s} g_k h_{ik},\ \textit{ст.пр.}\,(g_k h_{ik}) \le \textit{ст.пр.}\,(f_i - f_{i+1}) < v_0.$$

Используем это выражение для $f_i - f_{i+1}$ в записи $\widehat{f}$ и далее в записи (*) для f. Тогда получим сумму типа (*) для f, в которой пик v_1 для слагаемых будет меньше, чем v_0. Этот процесс можно продолжить и далее, если $\textit{ст.пр.}\, f < v_1$. Таким образом можно построить строго убывающую последовательность произведений переменных

$$v_0 > v_1 > v_2 > \dots .$$

Поскольку убывающая последовательность одночленов обрывается, то оборвется и этот процесс "срезки пиков". В итоге мы обязательно придем к случаю минимального пика, который уже рассмотрен в начале доказательства. Теорема доказана.

Следствие 1 (алгоритм Бухбергера). Следующий процесс вычислений через конечное число шагов преобразует данное конечное множество F многочленов в базис-делитель G для идеала $I = \langle F \rangle$.

0) Обозначить $G := F$.

1) Заменить многочлен из множества G, полученного на шаге 3 (или 0 в начале алгоритма), на его остаток от деления на множество *остальных* многочленов из G, если это деление возможно; повторить эти замены для других многочленов, если они возможны; иначе сохранить обозначение G и перейти к шагу 2.

2) Вычислить срезку пары многочленов из G и свести срезку относительно G к остатку r; перейти к шагу 3.

3) Если остаток r *ненулевой*, то расширить G, положив, по определению, $G := G \bigcup \{r\}$ и затем перейти к шагу 1. Если остаток нулевой, то вернуться к шагу 2, пока не исчерпаны все пары многочленов из G. В последнем случае перейти к 4).

4) Если *все* срезки пар многочленов из G сводятся относительно G к нулю, то G и есть требуемый базис-делитель.

Процесс оборвется на конечном шаге, т.е. к случаю 4 мы обязательно придем. Действительно, иначе возникнет строго возрастающая цепочка идеалов I_k, порожденных старшими членами многочленов из G после первых k циклов алгоритма:

$$I_0 < I_1 < I_2 < \dots ,$$

что невозможно ввиду следствия 2 из теоремы Гильберта о базисе.

Следствие 2. Пусть K — подполе поля L, $F \subset K[X]$. Тогда идеал I, порожденный F в $L[X]$ относительно некоторого порядка, имеет базис-делитель в $K[X]$.

Действительно, если исходя из F мы будем строить базис-делитель для I по алгоритму Бухбергера, то останемся в $K[X]$.

ПРИМЕРЫ ВЫЧИСЛЕНИЯ БАЗИСОВ-ДЕЛИТЕЛЕЙ

Отметим, что реализация алгоритма Бухбергера вручную обычно затруднительна — здесь может по существу оказать помощь какая-нибудь система компьютерной алгебры, например, Maple. Быстрое разбухание вычислений происходит по нескольким причинам. Во-первых, при элементарных делениях один из одночленов заменяется на сумму возможно *многих* младших одночленов. Во вторых, как только вычислен ненулевой остаток от очередной срезки, приходится находить остатки его срезок со *всеми* ранее полученными многочленами.

Есть несколько способов ускорить вычисления. Желательно, например, в первую очередь вычислять остатки срезок таких пар, для которых НОК старших членов имеет минимальную полную степень. Другие способы рассмотрим позднее.

Пример 1. Для идеала I, порожденного многочленами $g_1 = x^2y + z, g_2 = xz + y$ в кольце $\mathbb{Q}[x,\ y,\ z]$, найдем базис-делитель относительно словарного порядка $x > y > z$.

Пусть старшие члены многочленов подчеркиваются прямой чертой снизу. Тогда

$$g_1 \triangle g_2 = (\underline{x^2y} + z)z - (\underline{xz} + y)xy = z^2 - \underline{xy^2} = g_3.$$

Так как g_3 несводим относительно g_1 и g_2, то вычисляем и сводим относительно $g_1,\ g_2,\ g_3$ срезки новых пар из этого множества:

$$g_1 \triangle g_3 = (x^2y + z)y + (z^2 - xy^2)x = zy + \underline{xz^2} \xrightarrow{g_2} 0,$$

$$g_2 \triangle g_3 = (xz + y)y^2 + (z^2 - xy^2)z = \underline{y^3} + z^3 = g_4.$$

Появился новый ненулевой остаток g_4. Теперь будем вычислять срезки новых пар и сводить их относительно g_1, g_2, g_3, g_4. Имеем

$$g_1 \triangle g_4 = (x^2y + z)y^2 - (y^3 + z^3)x^2 = zy^2 - x^2z^3 \xrightarrow{g_2} zy^2 + xz^2y \xrightarrow{g_2} 0,$$

$$g_2 \triangle g_4 = (xz + y)y^3 - (y^3 + z^3)xz = y^4 - xz^4 \xrightarrow{g_2} y^4 + yz^3 \xrightarrow{g_4} 0,$$

$$g_3 \triangle g_4 = (z^2 - x^2y)y + (y^3 + z^3)x = yz^2 + xz^3 \xrightarrow{g_2} 0.$$

Мы видим, что все срезки сводятся к нулю и по теореме Бухбергера множество многочленов g_1, g_2, g_3, g_4 образует базис-делитель идеала I. Отметим также, что $x^2y + z,\ xz + y,\ xy^2 - z, y^3 + z^3$ — несводимый базис-делитель.

Пример 2. Вычислим теперь базис-делитель для того же идеала, но относительно словарного порядка $z > y > x$. Имеем $g_1 = \underline{z} + yx^2,\ g_2 = \underline{zx} + y$. Тогда

$$g_1 \triangle g_2 = (z + yx^2)x - (zx + y) = \underline{yx^3} - y = g_3,$$

$$g_1 \triangle g_3 = (z + yx^2)yx^3 - (yx^3 - y)z = \underline{zy} + y^2x^5 \xrightarrow{g_1} y^2x^5 - y^2x^2 \xrightarrow{g_3} 0,$$

$$g_2 \triangle g_3 = (zx+y)yx^2 - (yx^3-y)z = \underline{zy} + y^2x^2 \xrightarrow{g_1} 0.$$

Таким образом, идеал I относительно нового порядка имеет базис-делитель из трех многочленов $g_1 = z + yx^2,\ g_2 = zx + y,\ g_3 = yx^3 - y$. Более того, он сводим:

$$g_2 \xrightarrow{g_1} -yx^3 + y \xrightarrow{g_3} 0.$$

Следовательно, $g_1 = z+yx^2,\ g_3 = yx^3-y$ — снова базис-делитель для I, причем, очевидно, несводимый.

Теперь разберемся в структуре фактор-алгебры $A = \mathbb{Q}[x,y,z]/I$. Во-первых,

$$A \simeq \mathbb{Q}[x,y]/\langle yx^3 - y\rangle,$$

поскольку любой многочлен сводится относительно g_1 к многочлену от переменных $x,\ y$, а в любых дальнейших делениях с остатком может участвовать только g_3. Во-вторых, многочлен yx^3-y разлагается в произведение попарно взаимно простых множителей $y,\ x-1,\ x^2+x+1$. Поэтому

$$\mathbb{Q}[x,y]/\langle y(x-1)(x^2+x+1)\rangle \simeq \mathbb{Q}[x,y]/\langle y\rangle \oplus \mathbb{Q}[x,y]/\langle x-1\rangle \oplus \mathbb{Q}[x,y]/\langle x^2+x+1\rangle,$$ [2]

а слагаемые соответственно изоморфны $\mathbb{Q}[x],\ \mathbb{Q}[y],\ \mathbb{Q}(\epsilon)[y]$, где $\epsilon = (-1+i\sqrt{3})/2$.

Упр.1. Базисы-делители могут быть приспособлены для задачи переписывания симметрического многочлена от нескольких переменных через элементарные симметрические, либо через степенные суммы. Разберитесь в этом с помощью следующего примера.

Пусть $f_1 = x+y-\sigma,\ f_2 = xy-\tau, f = (x-y)^2$. Найдите базис-делитель G для $I = \langle f_1,\ f_2\rangle$ относительно порядка $x > y > \sigma > \tau$, а также нормальную форму для f относительно G.

Заметим, что в этом простом примере результат можно предсказать:

$$x+y \equiv \sigma (\mathrm{mod}\ I),\ xy \equiv \tau (\mathrm{mod}\ I) \Longrightarrow (x-y)^2 = (x+y)^2 - 4xy \equiv \sigma^2 - 4\tau (\mathrm{mod}\ I).$$

Тем не менее, отсюда ясен путь автоматического решения аналогичных, но численно более громоздких задач.

Упр. 2. Найти базис-делитель для идеала I алгебры $\mathbb{Q}[x,y]$, порожденного многочленами $f_1 = x^3 + xy + y^2,\ f_2 = x^2 + y^2$ относительно порядков

а) словарного $x > y$,

б) словарного $y > x$,

в) степенно-словарного $x > y$,

г) степенно-словарного $y > x$.

[2] Использовать следующий очевидный факт. Если $I,\ J$ — идеалы в кольце R, то по определению $IJ = \langle ab | a \in I,\ b \in J\rangle$. Отображение $\varphi : R/IJ \to R/I \oplus R/J$, заданное правилом $a + IJ \mapsto (a+I, a+J)$, является гомоморфизмом с ядром $I \cap J$. Если $I \cap J = IJ$, то φ — изоморфное вложение, а если $I + J = R$, то φ — изоморфизм.

Упр. 3. Найти размерность и базис фактор-алгебры $\mathbb{Q}[x,y]/I$ для идеала из упражнения 2, составьте таблицу умножения для этой базы.

Упр. 4. Задача, аналогичная двум предыдущим, если рассматривать $f_1,\ f_2$ как многочлены над полем вычетов $\mathbb{Z}_2$ или $\mathbb{Z}_3$.

Упр. 5. Найти базис-делитель для идеала, порожденного вещественными многочленами $x^2y+z,\ xz+y$ относительно степенно-словарного порядка $x<y<z$.

Упр. 6. Входит ли многочлен $f=3y^3+y^2(x-1)+y(2x^3+x^2+x)$ в идеал из упр.2? Если входит, то найдите его выражение через f_1 и f_2.

ТЕОРЕМА ГИЛЬБЕРТА О КОРНЯХ

Мы снова возвращаемся к решению систем полиномиальных уравнений. Теорема Гильберта о корнях или Nullstellensatz — одна из ключевых в алгебраической геометрии. Она показывает, как выглядят *все следствия* данной системы полиномиальных уравнений, если мы решаем систему в алгебраически замкнутом поле.

Теорема Гильберта о корнях. *Пусть K — поле, L — его алгебраическое замыкание и $f,\ f_1,\ldots,f_s$ — многочлены от переменных $x_1,\ldots,x_n$ над полем K. Допустим, что f обращается в нуль на всех общих корнях многочленов $f_1,\ldots,f_s$ в поле L. Тогда существует целое $p>0$ и такие многочлены $u_1,\ldots,u_s$ из $K[x_1,\ldots,x_n]$, что*

$$f^p=f_1u_1+\ldots+f_su_s.$$

Дадим сначала геометрическую трактовку и обсудим возможное ослабление условий теоремы. Множество общих корней в L^n совокупности многочленов F из $K[x,\ldots,x_n]$ называется *алгебраическим многообразием* и обозначается $Var_L(F)$. Читатель сразу вспомнит, что таковы прямые, плоскости, кривые и поверхности второго порядка, изучаемые в аналитической геометрии. Ясно, что за этим определением скрывается весьма богатое семейство геометрических объектов. С другой стороны, если V — подмножество в L^n, то можно рассматривать "аннулятор" $Ann_K(V)$, состоящий из всех многочленов в $K[x_1,\ldots,x_n]$, обращающихся в нуль на всех точках из V. По определению, аннулятор пустого множества совпадает со всем кольцом многочленов. Очевидно, $Ann_K(V)$ — идеал в $K[X]$. Например, $Var_{\mathbf{R}}(x^2+y^2)=\{(0,0)\},\ Ann_{\mathbf{R}}((0,0))=\langle x,y\rangle$. Теорема Гильберта о корнях утверждает, что для идеала I, порожденного F в $K[X]$,

$$Ann_K(Var_L(I))=\sqrt{I}, \tag{1}$$

где

$$\sqrt{I}=\{f\in K[X]: f^p\in I \text{ для некоторого целого } p>0\}$$

— идеал, который называется *радикалом* идеала I в $K[X]$. Развивая эту идею, можно утверждать, что это соответствие — двойственность между решеткой алгебраических многообразий относительно включения и решеткой радикальных полиномиальных идеалов. С его помощью некоторые геометрические вопросы можно переводить на алгебраический язык и, наоборот, трактовать алгебраические вопросы геометрически.

Отметим, что нельзя ограничиться решениями системы полиномиальных уравнений только в поле K. Действительно, многочлен x обращается в нуль на всех корнях многочлена x^2+y^2 в $\mathbf{R}^2$, но никакая его степень не делится на x^2+y^2. Мы вынуждены увеличить поле, где ищут решения, и теорема Гильберта утверждает, что надо увеличить K до его алгебраического замыкания L, получающегося присоединением к полю K всех корней многочленов от одной переменной с коэффициентами из K. Мы не обосновываем подробно существование алгебраического замыкания[3], сомневающиеся могут далее считать, что L — поле комплексных чисел, а K — его подполе.

Доказательство теоремы Гильберта о корнях разобьем на три этапа. Сначала покажем, что она равносильна своей ослабленной форме, затем докажем ослабленную форму теоремы, не обращая внимание на алгебраичность корней, и наконец займемся этой алгебраичностью.

Теорема Гильберта о корнях (в слабой форме). *Если полиномиальная система уравнений над полем K от конечного набора X переменных не имеет решений в алгебраическом замыкании L поля K, то идеал, порожденный левыми частями уравнений в $K[X]$, совпадает с $K[X]$. В символах*

$$I \lhd K[X],\ Var_L(I) = \emptyset \implies I = K[X]. \tag{2}$$

$(1) \Longrightarrow (2) : Var_L(I) = \emptyset \implies Ann(\emptyset) = K[X] = \sqrt{I} \implies 1 = 1^p \in I,\ I = K[X].$

Доказываем равносильность (1) и (2).

$(2) \Longrightarrow (1)$: Пусть $I = \langle f_1, \ldots, f_s \rangle$ и пусть $f \in Ann_K(Var_L(I))$. Введем дополнительную переменную t. Многочлены

$$f_1, \ldots, f_s, 1 - tf$$

не имеют общих корней в L. Поэтому идеал, порожденный ими, содержит единицу и существуют такие многочлены $h_1, \ldots, h_s, h$ из $K[X,t]$, что

$$f_1(X)h_1(X,t) + \ldots + f_s(X)h_s(X,t) + (1 - tf(X))h(X,t) = 1.$$

Поскольку это полиномиальное тождество, вместо t можно подставить любой элемент из расширения кольца $K[X]$, перестановочный с переменными X и полем K. Подставим

[3]Доказательство можно найти, например, в книге С.Ленг, Алгебра, М., Мир, 1968, стр. 194.

вместо t рациональную функцию $1/f(X)$. Приводя к общему знаменателю полученное равенство, найдем требуемое соотношение

$$f^p = f_1 u_1 + \ldots + f_s u_s.$$

Теперь докажем утверждение (2). Предположим, что $I < K[X]$. Ввиду обрыва возрастающих цепочек идеалов найдется такой максимальный идеал J, что $I \leq J < K[X]$. Тогда фактор-кольцо $R = K[X]/J$ является полем. Если положить $\alpha_i = x_i + J$, то набор $(\alpha_1, \ldots, \alpha_n)$ — общий корень для многочленов идеала I:

$$f_k(\alpha_1, \ldots, \alpha_n) = f_k(x_1, \ldots, x_n) + J = J = 0 \text{ в } K[X]/J = R$$

при всех $k = 1, \ldots, s$. Это будет противоречить предположению $Var_L(I) = \emptyset$, если мы заметим, что $\alpha_1, \ldots, \alpha_n$ *алгебраичны* над полем K, поскольку тогда их можно расположить в L.

Мы добрались до самого трудного места в доказательстве. Если K — несчетное алгебраически замкнутое поле, например, поле комплексных чисел, то доказательство можно завершить легко. Так и поступим, а общий случай разберем позднее.

Итак, предположим дополнительно, что K несчетно. Если α_i трансцендентно над K, то подалгебра $K[\alpha_i]$ поля R изоморфна алгебре многочленов $K[t]$ и потому R содержит ее поле частных, изоморфное полю рациональных дробей $K(t)$. Известно, что базу $K(t)$ как векторного пространства над полем K образуют степени переменной t и простейшие дроби вида $t^k/p^n(t)$, где $p(t)$ — неразложимый многочлен из $K[t]$, $k < ст.\, p(t)$, $k \geq 0$, $n > 0$. В частности, простейшими будут все дроби вида $1/(t - \alpha)$, где $\alpha \in K$. Поскольку множество таких дробей несчетно, то размерность $K(t)$ как векторного пространства над полем K несчетна. Аналогичное утверждение верно и для R, поскольку R содержит подполе, изоморфное $K(t)$. С другой стороны, ясно, что алгебра многочленов $K[X]$ имеет счетную размерность и потому ее фактор-пространство $R = K[X]/I$ имеет не более, чем счетную размерность. Полученное противоречие доказывает теорему Гильберта о корнях для несчетных полей.

Общий случай требует более тонких рассуждений. Приведем их, хотя и они основаны на доказательстве "методом от противного", т.е. неконструктивны. Позднее мы найдем конструктивный вариант доказательства, решая с помощью базисов-делителей прозвольную систему полиномиальных уравнений.

Индукцией по n покажем, что если n-порожденная K-алгебра $R = K[\alpha_1, \ldots, \alpha_n]$ является полем, то элементы $\alpha_1, \ldots, \alpha_n$ алгебраичны над K. При $n = 1$ утверждение очевидно: если α_1 трансцендентен над K, то $K[\alpha_1]$ изоморфно кольцу многочленов, которое полем не является.

Сделаем индукционный переход от $n - 1$ к n. Выделим элемент $\alpha = \alpha_1$ среди элементов $\alpha_1, \ldots, \alpha_n$. Поле R содержит подполе (α) и $K[\alpha_1, \ldots, \alpha_n] = K(\alpha)[\alpha_2, \ldots, \alpha_n]$. По

предположению индукции $\alpha_2, \ldots, \alpha_n$ алгебраичны над (α). Ввиду свойств алгебраических элементов, теперь достаточно показать, что α алгебраичен над K. Всякое α_i при $i \geq 2$ — корень некоторого многочлена с коэффициентами из поля $K(\alpha)$. Домножая его на подходящие элементы кольца $K[\alpha]$, можно считать, что α_i — корень некоторого многочлена с коэффициентами из кольца $K[\alpha]$. Более того, найдется такой общий элемент $a_0(\alpha)$ из $K[\alpha]$, что произведение $a_0(\alpha)\alpha_i$ цело над кольцом $K[\alpha]$, т.е. является корнем многочлена со старшим коэффициентом 1 и остальными коэффициентами из $K[\alpha]$. Поскольку целые элементы над подкольцом сами образуют подкольцо[4], то любой элемент из $K[\alpha_1, \ldots, \alpha_n]$ после домножения на подходящую степень $a_0(\alpha)^q$ становится цел над $K[\alpha]$. В частности, элементы из $K(\alpha)$ тоже становятся целыми над $K[\alpha]$ после домножения на подходящую степень фиксированного элемента $a_0(\alpha)$. Следовательно, *всякий* элемент из поля $K(\alpha)$ должен иметь вид

$$\frac{c(\alpha)}{a_0(\alpha)^q}, \tag{3}$$

где $c(\alpha)$ цел над $K[\alpha]$, $a_0(\alpha)$ — наш фиксированный элемент из $K[\alpha]$, q — целое. Допустим, что α трансцендентен над K. Тогда $K[\alpha]$ изоморфно кольцу многочленов, а $K(\alpha)$ — полю рациональных функций от одной переменной. Легко увидеть, что целые над $K[\alpha]$ элементы из $K(\alpha)$ принадлежат $K[\alpha]$ и потому $c(\alpha)$ принадлежит кольцу $K[\alpha]$. Но тогда из представления (3) для дроби $1/p(\alpha)$ следовало бы, что любой неразложимый многочлен $p(\alpha)$ делит $a_0(\alpha)$ и потому кольцо многочленов $K[\alpha]$ содержит только конечное число неразложимых многочленов, что неверно. Противоречие показывает, что α алгебраичен над K, и теорема доказана.

Упр. Доказать, что всякий максимальный идеал в алгебре $K[x_1, \ldots, x_n]$, где K — алгебраически замкнутое поле, имеет вид $\langle x_1 - \alpha_1, \ldots, x_n - \alpha_n \rangle$. Таким образом, в этом случае существует соответствие между точками аффинного пространства K^n и максимальными идеалами в алгебре многочленов $K[x_1, \ldots, x_n]$.

СИСТЕМЫ С КОНЕЧНЫМ МНОЖЕСТВОМ РЕШЕНИЙ

Пусть дана система полиномиальных уравнений

$$\begin{cases} f_1(x_1, \ldots, x_n) &= 0, \\ \ldots\ldots\ldots &\ldots \\ f_s(x_1, \ldots, x_n) &= 0, \end{cases} \tag{4}$$

[4]Пусть Δ — кольцо, $f, g \in \Delta[x]$, *ст.к.* $f =$ *ст.к.* $g = 1, a = a_1, a_2, \ldots, a_m$ — все корни f, $b = b_1, b_2, \ldots, b_n$ — все корни g в расширении Δ. Тогда $a - b, ab$ — корни многочленов

$$\varphi(x) = \prod_{i,j}(x - (a_i - b_j)), \psi(x) = \prod_{i,j}(x - a_i b_j),$$

каждый из которых после перемножения имеет старший коэффициент 1, а остальные из Δ ввиду симметричности по двум системам корней $a_1, \ldots, a_m$ и $b_1, \ldots, b_n$.

с коэффициентами из поля K. Как узнать, имеет ли она решения хотя бы в некотором расширении поля K? Как найти решения, если их конечное число? Воспользуемся тем, что если $I = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, то система (1) равносильна системе

$$\begin{cases} g_1(x_1, \ldots, x_n) &= 0, \\ \ldots\ldots\ldots & \ldots \\ g_t(x_1, \ldots, x_n) &= 0, \end{cases} \tag{5}$$

над любым расширением поля K.

Теорема 1 (критерий совместности). Система полиномиальных уравнений (4) над полем K не имеет решений в алгебраическом замыкании L поля K, если и только если некоторый (равносильно, любой) базис-делитель для идеала $I = \langle f_1, \ldots, f_s \rangle$ в $K[x_1, \ldots, x_n]$ содержит ненулевое элемент из K.

Доказательство. Если наша система несовместна, то ввиду теоремы Гильберта о корнях в слабой форме идеал I содержит единицу, а его базис-делитель, как следует из определения, обязан включать ненулевое число.

Обратное утверждение следует из равносильности исходной системы и системы уравнений, связанной с базисом-делителем. Последняя несовместна, поскольку она содержит равенство $c = 0$ для ненулевого числа c.

Следствие. Существует алгоритм, определяющий несовместность системы полиномиальных уравнений в алгебраически замкнутом поле.

Достаточно с помощью алгоритма Бухбергера переработать левые части уравнений в базис-делитель.

Определение. Система полиномиальных уравнений (4) над полем K называется *треугольной*, если число уравнений равно числу переменных и многочлен f_i для любого $i = 1, \ldots, n$ имеет вид

$$a_i x_i^{k_i} + \varphi_i(x_i, \ldots, x_n)$$

где $a_i \in K$, $a_i \neq 0$, $k_i > 0$, а φ_i — многочлен над K от переменных $x_i, \ldots, x_n$, причем показатели при переменной x_i в многочлене φ_i меньше, чем k_i. В этом случае систему многочленов $f_1, \ldots, f_n$ будем также называть *треугольной*.

Треугольная система полиномиальных уравнений имеет конечное число решений. Действительно, последнее уравнение связывает только переменную x_n и потому имеет конечное число решений. Если каждое из этих решений подставить в предпоследнее уравнение, связывающее x_{n-1} и x_n, то задача сводится к отысканию корней многочленов от x_{n-1}, и так далее.

Теорема 2. Система полиномиальных уравнений (4) над полем K имеет конечное число решений в алгебраическом замыкании L поля K тогда и только тогда, когда система уравнений (5), связанная с базисом-делителем идеала $I = \langle f_1, \ldots, f_s \rangle$ в $K[X]$ относительно словарного порядка $x_1 > x_2 > \ldots > x_n$ содержит треугольную подсистему.

Доказательство. Пусть

$$\begin{array}{rcl} c_1 & = & (c_{11}, \ldots, c_{1n}) \\ \ldots & & \ldots\ldots\ldots \\ c_N & = & (c_{N1}, \ldots, c_{Nn}) \end{array}$$

— все решения системы (4) в поле L. Тогда многочлен

$$h(x_n) = \prod_{i=1}^{N} (x_n - c_{in})$$

обращается в нуль на всех корнях системы (4). По теореме Гильберта о корнях некоторая его степень входит в идеал, порожденный $f_1, \ldots, f_s$ в $L[X]$, а ее старший член, зависящий только от x_n, делится на старший член подходящего многочлена, скажем, g_n, из базиса-делителя, который можно выбрать в $K[X]$. Но тогда старший член g_n зависит только от x_n, младшие члены g_n тоже зависят только от x_n — иначе они старше старшего члена ввиду свойств принятого порядка. Следовательно, g_n можно считать последним многочленом искомой треугольной подсистемы.

Точно так же, поскольку есть многочлен от переменной x_{n-1}, обращающийся в нуль на всех решениях системы (1), то в базисе-делителе найдется многочлен g_{n-1}, старший член которого зависит только от x_{n-1}, а младшие зависят лишь от x_{n-1} и x_n, причем показатели при x_{n-1} меньше, чем у старшего члена. Можно считать его предпоследним многочленом треугольной подсистемы. Ясно, что эту процедуру можно продолжить, пока не выстроим всю треугольную подсистему.

Обратное утверждение очевидно, так как решения системы являются решениями ее треугольной подсистемы, последняя же имеет конечное число решений. Теорема доказана.

Сейчас мы дадим внутреннюю характеристику идеалов из теоремы 2, не связанную с выходом в алгебраическое замыкание поля K и не использующую теорему Гильберта о корнях.

Теорема 3. Фактор-алгебра $K[X]\ /I$ алгебры многочленов $K[X]$ по идеалу I конечномерна над K тогда и только тогда, когда базис-делитель идеала I относительно словарного порядка содержит треугольную систему многочленов.

Доказательство. Если $K[X]\ /I$ конечномерна, то степени $1,\ x_i,\ x_i^2,\ x_i^3, \ldots$ любой переменной x_i линейно зависимы по модулю идеала I и потому существует ненулевой многочлен $h_i(x_i)$, зависящий только от x_i и принадлежащий идеалу I. Рассуждая далее также, как в доказательстве теоремы 2, построим треугольную подсистему в базисе-делителе идеала I относительно словарного порядка.

Допустим теперь, что идеал I содержит треугольную систему многочленов. Очевидно, базис фактор-алгебры $K[X]\ /I$ образуют произведения переменных, несводимые по

модулю идеала. Но тогда показатели при переменных будут ограничены степенями соответствующих многочленов из треугольной системы. Следовательно, таких произведений конечное число и фактор-алгебра конечномерна. Теорема доказана.

Идеалы из формулировки теоремы 3 называются идеалами *полного ранга*, так как соответствующие им алгебраические многообразия над алгебраически замкнутым полем являются объединениями конечного числа точек.

Упр. Выделить системы с конечным числом комплексных решений и найти эти решения для систем

$$\begin{cases} ab &= c^2 + c, \\ bc &= a^2 + a, \\ ac &= b^2 + b, \end{cases}$$

$$\begin{cases} ab &= c^2 + c, \\ bc &= a^2 - a, \\ ac &= b^2 + b. \end{cases}$$

Упр. Решить систему уравнений

$$\begin{cases} y^2 + (x-4)y + x^2 - 2x + 3 &= 0, \\ y^3 - 5y^2 + (x+7)y + x^3 - x^2 - 5x - 3 &= 0. \end{cases}$$

Упр. Пусть $f(x,y),\ g(x,y)$ — взаимно простые многочлены над полем. Доказать, что система уравнений

$$\begin{cases} f(x,y) = 0 \\ g(x,y) = 0 \end{cases}$$

имеет только конечное число решений.

Упр. Найти критические точки вещественной рациональной функции

$$f(x,y) = \frac{x+y}{x^2+y^2+1}.$$

ИСКЛЮЧЕНИЕ ПЕРЕМЕННЫХ И ПЕРЕСЕЧЕНИЕ ИДЕАЛОВ

Результаты этого параграфа позволяют задавать уравнениями проекции алгебраического многообразия на координатные плоскости и "сумму" алгебраических многообразий, т.е. наименьшее алгебраическое многообразие, содержащее два алгебраических многообразия, заданные уравнениями. Кроме того, мы укажем алгоритм проверки вхождения многочлена в радикал идеала.

Пусть $X = \{x_1, \ldots, x_m\},\ Y = \{y_1, \ldots, y_n\}$ — два набора переменных, $>_x,\ >_y$ — устойчивые линейные порядки на полугруппах $X^*,\ Y^*$ соответственно. Зададим порядок на X^*Y^* по правилу

$$uv > u'v' \Longleftrightarrow (u >_x u' \text{ или } (u = u',\ v >_y v'))$$

для любых $u, u' \in X^*,\ v, v' \in Y^*$. Назовем его порядком с *X-предпочтением* перед Y. Очевидно, что он линеен и устойчив.

Теорема 1. Пусть G — базис-делитель для идеала I в кольце $K[X,Y]$, упорядоченном с X-предпочтением перед Y . Тогда $G \cap K[Y]$ является базисом-делителем для идеала $I \cap K[Y]$ в $K[Y]$ относительно порядка $>_y$.

Доказательство. Ясно, что $G \cap K[Y] \subset I \cap K[Y]$. Пусть теперь $f = f(Y) \in I \cap K[Y]$. Так как G — базис-делитель для I, то найдется такой многочлен $g \in G$, что *ст.чл.* g делит *ст.чл.* f. Поэтому, *ст.чл.* g содержит только Y-переменные. Ввиду свойств порядка, его младшие члены тоже содержат только Y-переменные. Следовательно, $g \in K[Y]$ и по определению $G \cap K[Y]$ — базис-делитель для $I \cap K[Y]$.

Следствие. Над алгебраически замкнутым полем имеется алгоритм для отыскания наименьшего алгебраического многообразия, содержащего проекцию данного алгебраического многообразия на любую координатную плоскость: если $F \subset K[X,Y]$, F конечно и $V = Var_K(F)$, а W — проекция V на Y-плоскость, то

$$Ann_K(W) = \sqrt{\langle G \cap K[Y] \rangle}, \tag{6}$$

где G — базис-делитель для идеала $I = \langle F \rangle$ в $K[X,Y]$ относительно порядка с X-предпочтением перед Y.

Доказательство. Очевидно, многочлены из $G \cap K[Y]$ обращаются в нуль на W. Наоборот, если многочлен f из $K[Y]$ обращается в нуль на W, то он обращается в нуль и на V, поскольку не зависит от переменных X. Ввиду теоремы Гильберта о корнях подходящая степень f попадает в идеал I, порожденный F в $K[X,Y]$, и потому содержится в идеале $I \cap K[Y]$, база которого $G \cap K[Y]$, как получается, задает W и может быть найдена алгоритмически.

Пример. Найдем условие на комплексные коэффициенты $a,\ b$ кубического многочлена $f = x^3 + ax + b$, при которых имеются кратные корни. Как известно, кратные корни будут корнями и производной $f' = 3x^2 + a$ многочлена f. Исключим переменную x из системы уравнений

$$\begin{cases} x^3 + ax + b &= 0, \\ 3x^2 + a &= 0. \end{cases},$$

используя срезки в словарном порядке $x > a > b$. Положим

$$f_2 = 3f - xf' = 2ax + 3b.$$

Общий корень $f,\ f'$ будет корнем и f_2. Следовательно, кратный корень x равен $-3b/2a$. Далее положим $f_3 = 2af' - 3xf_2 = 2a^2 - 9bx,\ f_4 = 9bf_2 + 2af_3 = 4a^3 + 27b^2$. Последнее выражение (со знаком минус) называется *дискриминантом* $\mathrm{Dis}(f)$ нашего кубического многочлена. Итак, $\mathrm{Dis}(f)$ входит в идеал I, порожденный f и f' в кольце $\mathbb{C}[x,a,b]$. Более того, из критерия Бухбергера следует, что $f',\ f_2,\ f_3,\ \mathrm{Dis}(f)$ образуют базис-делитель для

I, а $\mathrm{Dis}(f)$ — базис-делитель для пересечения $I \cap \mathbb{C}[a,b]$. Следовательно, любое полиномиальное соотношение между a и b, при которых f имеет кратный корень, следует из соотношения $\mathrm{Dis}(f) = 0$.

Упр. Нарисуйте в некоторой окрестности нуля трехмерного евклидова пространства "сборку Уитни" — поверхность, заданную в прямоугольной системе координат b, a, x кубическим уравнением $x^3 + ax + b = 0$. Можно рассматривать ее как график функции $b = -x^3 - ax$ и построить поверхность вручную, либо использовать какую-нибудь систему компьютерной алгебры. Фиксация a, b определяет прямую, которая пересечет поверхность 1, 2 или 3 раза в соответствии с количеством вещественных корней кубического уравнения от переменной x. Линия кратных корней $4a^3 + 27b^2 = 0$ отвечает прямым, пересекающим поверхность 2 раза в случае двух корней, один из которых кратности 2, и 1 раз в случае корня кратности 3.

Упр. Аналогичная задача (кратные корни, дискриминант, поверхность) для уравнения $x^2 + px + q = 0$.

Замечание. Если поле K *не замкнуто алгебраически*, то формула (6) может быть неверна. Действительно, пусть $I = \langle (x^2-y)(z^2+1),\ x^2-z^2-1\rangle \lhd \mathbb{R}[x,y,z]$, $V = Var_{\mathbb{R}}(I)$. Тогда V легко нарисовать и увидеть, что $W = pr_{(x,y)}V = \{\text{парабола } y = x^2\}$. Теперь вычислим базис-делитель G для I относительно словарного порядка $z > y > x$, используя алгоритм Бухбергера.

Имеем $f_1 = (z^2+1)(x^2-y)$, $f_2 = z^2 - x^2 + 1$, $f_1 \triangle f_2 = f_1 - f_2(x^2-y) = x^2(x^2-y) = f_3$. Далее легко подсчитать, что

$$f_2 \triangle f_3 \xrightarrow{\{f_2,f_3\}} 0, \quad f_1 \triangle f_3 \xrightarrow{f_3} 0.$$

Следовательно, $G = \{f_1, f_2, f_3\}$ — требуемый базис-делитель для I, $G \cap \mathbb{R}[x,y] = \{x^2(x^2 - y)\}$. Теперь очевидно, что алгебраическое многоообразие $Var_{\mathbb{R}} x^2(x^2-y)$ — объединение параболы W и оси y.

Что изменится в этих вычислениях, если заменить поле вещественных чисел на поле комплексных чисел?

Теорема 2. Пусть $I,\ J$ — идеалы в $K[x_1,\ldots,x_n]$ и λ — новая переменная. Пусть $\langle \lambda I,\ (1-\lambda)J\rangle$ — идеал в $K[\lambda, x_1, \ldots, x_n]$. Тогда

$$I \cap J = \langle \lambda I,\ (1-\lambda)J\rangle \cap K[x_1,\ldots,x_n].$$

Доказательство. Если $f \in I \cap J$, то

$$f = \lambda f + (1-\lambda) f \in \langle \lambda I,\ (1-\lambda)J\rangle \cap K[X].$$

Теперь докажем обратное включение. Пусть $I = \langle f_1, \ldots, f_s\rangle$, $J = \langle f'_1, \ldots, f'_t\rangle$ и f — элемент правой части доказываемого равенства. Тогда

$$f(X) = \sum_{i=1}^{s} \lambda f_i(X) h_i(\lambda, X) + \sum_{j=1}^{t} (1-\lambda) f'_j(X) h'_j(\lambda, X).$$

Так как λ не входит в X, то подставляя $\lambda = 1$, получим

$$f(X) = \sum_{i=1}^{s} f_i(X) h_i(1, X) \in I.$$

А теперь подставим $\lambda = 0$. Тогда получим, что

$$f(X) = \sum_{j=1}^{t} f'_j(X) h'_j(0, X) \in J.$$

Следовательно, $f \in I \cap J$, и теорема доказана.

Следствие 1. Существует алгоритм для отыскания полиномиальных уравнений наименьшего алгебраического многообразия, содержащего два заданных полиномиальными уравнениями алгебраических многообразий.

Действительно, достаточно найти базис-делитель для идеала $\langle \lambda I,\ (1-\lambda)J \rangle$ относительно порядка с λ-предпочтением перед X и взять из нее X-многочлены.

Следствие 2. Существует алгоритм для вычисления наименьшего общего кратного и наибольшего общего делителя двух многочленов от нескольких переменных.

Действительно, существование НОК и НОД следует из единственности разложения на неразложимые множители для многочленов над полем. Кроме того,

$$\langle \text{НОК}(f, g) \rangle = \langle f \rangle \cap \langle g \rangle,\ \text{НОД} = \frac{fg}{\text{НОК}}.$$

Пример. Найдем наибольший общий делитель d и наименьшее общее кратное k рациональных многочленов

$$f = x^2y^2 - y^2 + x^2 - 1,\ g = xy^2 - y^2 - x + 1.$$

Для этого вычислим несводимый базис-делитель G идеала $I = \langle \lambda f,\ (1-\lambda)g \rangle$ в $\mathbb{Q}[x, y]$, используя словарный порядок $\lambda > x > y$. Получим

$$G = \langle x^2y^4 - x^2 - y^4 + 1,\ -\lambda xy^2 + \lambda x + \lambda y^2 - \lambda + xy^2 - x - y^2 + 1,\ 2\lambda x^2 - 2\lambda + x^2y^2 - x^2 - y^2 + 1 \rangle.$$

Следовательно,

$$k = x^2y^4 - x^2 - y^4 + 1.$$

Чтобы вычислить НОД, разделим fg на k, используя алгоритм деления с остатком. Получим

$$d = x - 1.$$

Теорема 3. Пусть $I = \langle f_1, \ldots, f_s \rangle$ — идеал в $K[x_1, \ldots, x_n]$. Тогда $f \in \sqrt{I}$, если и только если $1 \in \langle 1 - \lambda f, f_1, \ldots, f_s \rangle \lhd K[\lambda, x_1, \ldots, x_n]$, где λ — новая переменная.

Доказательство. По теореме Гильберта о корнях $\sqrt{I} = Ann_K(Var_L(I))$, где L — алгебраическое замыкание поля K. Пусть $f \in \sqrt{I}$. Если $(a_0, a_1, \ldots, a_n) \in Var_L(\langle 1 - \lambda f, f_1, \ldots, f_s)\rangle)$, то

$$f_i(a_1, \ldots, a_n) = 0 \text{ при } i = 1, \ldots, s,\ 1 - a_0 f(a_1, \ldots, a_n) = 0.$$

Но тогда $(a_1, \ldots, a_n) \in Var_L(I)$ и, значит, $f(a_1, \ldots, a_n) = 0$ и получается противоречие с последним равенством. Следовательно, $Var_L(\langle 1 - \lambda f,\ f_1, \ldots, f_s\rangle)$ пусто и тогда $1 \in \langle 1 - \lambda f,\ f_1, \ldots, f_s\rangle$.

Наоборот, пусть $1 \in \langle 1 - \lambda f,\ f_1, \ldots, f_s\rangle$. Тогда

$$1 = (1 - \lambda f)h + \sum_{i=1}^{s} f_i h_i$$

для некоторых h, h_i из $K[\lambda, x_1, \ldots, x_n]$ отсюда для любых точек $(a_1, \ldots, a_n) \in Var_L(I)$ имеем

$$1 = (1 - \lambda f(a_1, \ldots, a_n))h(\lambda, a_1, \ldots, a_n).$$

Правая часть — многочлен от λ. Если $f(a_1, \ldots, a_n) \neq 0$, то, полагая $\lambda = 1/f(a_1, \ldots, a_n)$, получим противоречие. Следовательно, $f(a_1, \ldots, a_n) = 0$ и $f \in \sqrt{I}$. Теорема доказана.

Упр. Найти базис-делитель для пересечения $I \cap J$ идеалов

$$I = \langle x^3 + y^3 - 1,\ x - y + 1\rangle, \quad J = \langle xy - 1\rangle.$$

Упр. Пусть $I = \langle xy^2 + 2y^2,\ x^4 - 2x^2 + 1\rangle$ — идеал в кольце $\mathbb{Q}[x, y]$. Проверить, что многочлен $f = y - x^2 + 1$ принадлежит радикалу $\sqrt{I}$. Найти степень f , принадлежащую идеалу I.

СИСТЕМЫ С БЕСКОНЕЧНЫМ МНОЖЕСТВОМ РЕШЕНИЙ

Здесь мы попытаемся решить конструктивно произвольную систему полиномиальных уравнений и оценим трудности на этом пути. Как следствие получится конструктивное доказательство теоремы Гильберта о корнях, независимое от ранее приведенных. Предлагаемый подход обобщает известный метод решения систем линейных уравнений с помощью приведения к треугольному виду (метод Гаусса). Разобьем конструкцию на несколько шагов.

1) Вычисление ранга идеала.

Случай, когда идеал I, порожденный левыми частями уравнений, *полного ранга*, уже разобран.

Мы можем считать, что размерность фактор-алгебры по идеалу бесконечна. Это означает, что все степени некоторой переменной независимы по модулю идеала. Тогда можно

разбить множество переменных на две части, скажем, X и Y так, что $I \cap K[Y] = \{0\}$, причем Y непусто, максимально по включению и по мощности. Мы можем найти такое разбиение конструктивно ввиду результатов предыдущего параграфа. Можно утверждать, что элементы из Y алгебраически независимы по модулю идеала I. Мощность d множества Y называется *размерностью* многообразия нулей идеала I, а число $r = n - d$ — *рангом* идеала I.

2) Переход к простому идеалу с сохранением ранга.

Отметим, что в общем случае максимальные только по включению подмножества Z множества переменных, такие, что $I \cap K[Z] = \{0\}$, могут иметь разную мощность. Причина в том, что соответствующее алгебраическое многообразие может распадаться на неприводимые компоненты разной размерности. Поскольку таких компонент конечное число, то можно сосредоточиться на изучении только одной неприводимой компоненты максимальной размерности. Ее аннулятор — простой идеал J. Мы перейдем от I к J следующим образом. Ввиду обрыва возрастающих цепочек идеалов в алгебре многочленов найдется максимальный идеал J со свойством

$$I \subseteq J, \quad J \cap K[Y] = \{0\}.$$

Тогда J — простой идеал. Действительно, если $fg \in J, \quad f \notin J, \ g \notin J$, то $\langle f, \ J\rangle \cap K[Y] \neq \{0\}, \langle g, \ J\rangle \cap K[Y] \neq \{0\}$. Поэтому $f + u = p \neq 0, \ g + v = q \neq 0$ для некоторых $u, \ v \in J, \quad p, \ q \in K[Y]$. Тогда $pq \in K[Y], pq \neq 0$. С другой стороны, $pq = (f + u)(g + v) = fg + ug + fv + uv \in J$, что противоречит предположению $J \cap K[Y] = \{0\}$. Итак, мы можем заменить идеал I на простой идеал J той же размерности. Сам алгоритм перехода и условия его осуществимости оставим пока в стороне.

3) Переход к локализации.

Очевидно, алгебра $R = K[X, Y]$ содержится в алгебре $S = K(Y)[X]$ многочленов от переменных X с коэффициентами из поля $K(Y)$ рациональных дробей от переменных Y. Обозначим через J^e наименьший идеал в L, содержащий идеал J, а через J^{ec} — его пересечение с R. Покажем, что $J^{ec} = J$. Очевидно, $J^{ec} \supseteq J$. С другой стороны, легко убедиться, что $J^e = \{f/p \mid f \in J, \ p \in K[Y], \ p \neq 0\}$. Поэтому если $f/p = h \in R$, то $f = ph \in J, \ p \notin J, \ J$ прост и тогда $h \in J$.

Теперь докажем, что J^e — идеал полного ранга в алгебре S. Ввиду максимальности Y для всякого $x \in X$ имеем $J \cap K[Y, x] \neq \{0\}$. Поэтому найдется

$$f = p_0 x^k + p_1 x^{k-1} + \ldots + p_k \in J, \ p_i \in K[Y], \ p_0 \neq 0.$$

Тогда

$$f/p_0 = x^k + (p_1/p_0)x^{k-1} + \ldots + (p_k/p_0) \in J^e$$

и степени x линейно зависимы над $K(Y)$ по модулю идеала J^e. Из произвольности x следует конечномерность фактор-алгебры S по идеалу J^e(см. теорему 3 из параграфа о системах с конечным множеством решений).

3) Переход к обобщенно-треугольному базису идеала J.

Поскольку поле $K(Y)$ конструктивно ввиду конструктивности K и идеал J^e полного ранга, то можно построить для него треугольный базис $f_1, \ldots, f_r$ из $K(Y)[X]$, полагая $X = \{x_1, \ldots, x_r\}, Y = \{x_{r+1}, \ldots, x_n\}$ и устанавливая порядок $x_1 > \ldots > x_r$. Умножая на подходящий многочлен из $K[Y]$, можно избавиться от знаменателей коэффициентов этих многочленов и получить другой треугольный базис $g_1, \ldots, g_r$ идеала J^e, принадлежащий R. Но тогда эти многочлены содержатся в $J^{ec} = J$. Ввиду треугольности имеем

$$g_i \in K[x_i, \ldots, x_n], \quad \text{ст.к. } g_i \in K[x_{r+1}, \ldots, x_n], \quad i = 1, \ldots, r.$$

Пусть теперь $h_1, \ldots, h_m$ — некоторый базис идеала J в алгебре R. Так как $J^e \supseteq J$ и $g_1, \ldots, g_r$ — базис J^e, то

$$h_i = \sum v_{ij} g_j$$

при некоторых $v_{ij} \in S = K(Y)[X]$. Пусть f — произведение всех знаменателей коэффициентов из $K(Y)$ многочленов v_{ij} при всех $i,\ j$. Тогда $f \neq 0,\ f \in K[x_{r+1}, \ldots, x_n]$. Покажем, что

$$J = \{g \in R \,|\, fg \in \langle g_1, \ldots, g_r \rangle_R\}.$$

Пусть $g \in J$. Тогда $g = \sum u_i h_i = \sum u_i (\sum v_{ij} g_j)$. Поэтому

$$fg = \sum u_i (f v_{ij} g_j) \in \langle g_1, \ldots, g_r \rangle.$$

Наоборот, если

$$fg \in \langle g_1, \ldots, g_r \rangle \subseteq J^{ec} = J,$$

то ввиду простоты J и алгебраической независимости переменных $Y = \{x_{r+1}, \ldots, x_n\}$ по модулю идеала J получаем, что $g \in J$.

Такую систему многочленов $f, g_1, \ldots, g_r$ назовем обобщенно-треугольным базисом идеала J.

4) Описание множества решений системы.

Покажем, что множество решений системы непусто и, в частности, тем самым получим доказательство ослабленной теоремы Гильберта о корнях. Более того, покажем, что вне подходящего множества меньшей размерности многообразие решений системы над алгебраически замкнутым полем K выглядит как объединение конечного числа кусков, похожих на изогнутые дополнения к гиперповерхностям в аффинных пространствах K^d.

Пусть q_i — старший коэффициент многочлена g_i из обобщенно-треугольного базиса как многочлена из $K[Y][X]$. Тогда q_i из $K[Y]$ и пусть

$$p = f \prod_{i=1}^{r} q_i.$$

Поскольку p — ненулевой многочлен из $K[x_{r+1},\dots,x_n]$ и K бесконечно, то уравнение $p=0$ задает гиперповерхность в пространстве K^d. Покажем, что вне ее множество решений системы устроено хорошо.

Выберем любые $\alpha_{r+1},\dots,\alpha_n$ из K с условием $p(\alpha_{r+1},\dots,\alpha_n)\neq 0$, — таких найдется бесконечно много. Но тогда f и все q_i тоже не обращаются в нуль. Следовательно, система уравнений

$$g_i(x_1,\dots,x_r,\alpha_{r+1},\dots,\alpha_n)=0,\quad i=1,\dots,r,$$

треугольна и имеет конечное число решений $(\alpha_1,\dots,\alpha_r)$, ограниченное функцией от степеней многочленов и числа переменных. Покажем, что $\alpha=(\alpha_1,\dots,\alpha_r,\alpha_{r+1},\dots,\alpha_n)$ — общий корень нашего идеала J.

Если $g\in J$, то $fg\in\langle g_1,\dots,g_r\rangle$ и потому fg обращается в нуль в точке α. Поскольку $f(\alpha)\neq 0$, то $g(\alpha)=0$.

Отметим, что таким способом мы получим *все* общие корни α идеала J, для которых $p(\alpha)\neq 0$, — это следует из вхождения $g_1,\dots,g_r$ в идеал J.

ПОЛИНОМИАЛЬНЫЕ ГОМОМОРФИЗМЫ

Здесь мы научимся находить ядра и образы для гомоморфизмов полиномиальных колец.

Всякий K-гомоморфизм $\varphi: K[y_1,\dots,y_m]\longrightarrow K[x_1,\dots,x_n]$, при котором поле K отображается тождественно, задается отображением

$$\varphi: y_i\longmapsto f_i,\ i=1,\dots,m.$$

Тогда если $h(X)=\sum a_{k_1,\dots,k_m}y_1^{k_1}\cdots y_m^{k_m}$, то $\varphi(h)=\sum a_{k_1,\dots,k_m}f_1^{k_1}\cdots f_m^{k_m}=h(f_1,\dots,f_m)$. Многочлены $f_1,\dots,f_m$ могут быть любыми. Будем для краткости называть такие гомоморфизмы полиномиальными. Напомним, что "образ" и "ядро" гомоморфизма φ — это соответственно множества

$$Im\varphi=\{\varphi(h):\ h\in K[Y]\}\text{ — подкольцо из }K[Y],$$

$$Ker\varphi=\{h\in K[X]:\ \varphi(h)=0\}\text{ — идеал из }K[X].$$

Если $h\in Ker\varphi$, то $h(f_1,\dots,f_n)=0$, т.е. $Ker\varphi$ — "идеал соотношений" между многочленами $f_1,\dots,f_n$. Интересно, например, какие алгебраические зависимости есть между "параболами" и "гиперболами"?

Теорема 1. Пусть $I=\langle y_1-f_1,\dots,y_m-f_m\rangle$ — идеал из $K[x_1,\dots,x_n,y_1,\dots,y_m]$. Тогда $Ker\varphi=I\cap K[y_1,\dots,y_m]$.

Следствие. Базис ядра гомоморфизма $\varphi: K[Y]\longrightarrow K[X]$ можно найти алгоритмически за конечное число шагов.

Доказательство теоремы. Пусть $h \in I \cap K[Y]$. Тогда

$$h(Y) = \sum_{i=1}^{m} (y_i - f_i(x_1, \ldots, x_n))\, u_i(x_1, \ldots, x_n, y_1, \ldots, y_m).$$

Отсюда $h(f_1, \ldots, f_m) = 0,\ h \in Ker\varphi$.

Наоборот, если $h \in Ker\varphi$, то

$$h = \sum c_{k_1,\ldots,k_m} y_1^{k_1} \cdots y_m^{k_m}.$$

Так как $h(f_1, \ldots, f_m) = 0$, то

$$h = h - h(f_1, \ldots, f_m) = \sum c_{k_1,\ldots,k_m} (y_1^{k_1} \cdots y_m^{k_m} - f_1^{k_1} \cdots f_m^{k_m}).$$

Так как $y_i \equiv f_i \pmod I$, то $y_1^{k_1} \cdots y_m^{k_m} \equiv f_1^{k_1} \cdots f_m^{k_m} \pmod I$, и, следовательно,

$$h \in I \cap K[Y].$$

Теорема доказана.

Упр. Найти основные полиномиальные зависимости между уравнением гиперболы $x^2 - y^2 = 1$ и уравнением параболы $y - x^2 = 0$.

Теорема 2. Пусть выполнены условия теоремы 1 и G — базис-делитель для I относительно порядка с X-предпочтением перед Y. Тогда $f \in K[X]$ принадлежит $Im\,\varphi$, если и только если остаток $r = N_G(f)$ многочлена f относительно G принадлежит $K[Y]$. В этом случае $f = \varphi(r) = r(f_1, \ldots, f_m)$.

Следствие. Проблема вхождения многочлена в конечно порожденную подалгебру алгебры многочленов алгоритмически разрешима.

Доказательство теоремы. Если $f \in Im\varphi$, то $f = h(f_1, \ldots, f_m)$, где $h \in K[Y]$. Тогда

$$f(x_1, \ldots, x_n) - h(y_1, \ldots, y_m) = h(f_1, \ldots, f_m) - h(y_1, \ldots, y_m) \in I,$$

как в доказательстве предыдущей теоремы. Следовательно, $f \xrightarrow{G} r$ и $h \xrightarrow{G} r$, где $r = N_G(f) = N_G(h)$. Так как $h \in K[Y]$ и порядок с X-предпочтением, то $r = N_G(h) \in K[Y]$.

Наоборот, если $f \xrightarrow{G} r,\ r \in K[Y]$, то $f - r \in I$, и

$$f(x_1, \ldots, x_n) - r(y_1, \ldots, y_m) = \sum_i (y_i - f_i(x_1, \ldots, x_n))\, u_i(x_1, \ldots, x_m, y_1, \ldots, y_m).$$

Подставим f_i вместо y_i. Тогда

$$f(x_1, \ldots, x_n) - r(f_1, \ldots, f_m) = 0, \quad f = r(f_1, \ldots, f_m) \in Im\,\varphi.$$

Теорема доказана.

В качестве применения покажем как можно конструктивно решать некоторые задачи из теории алгебраических чисел.

Напомним, что элемент α поля L называется *алгебраическим* над подполем K поля L, если α — корень ненулевого многочлена с коэффициентами из поля K. Такой многочлен наименьшей степени со старшим коэффициентом 1 есть только один. Он называется *минимальным* многочленом для элемента α над полем K и обозначается μ_K^α. Минимальный многочлен μ_K^α неразложим над K и делит любой многочлен с коэффициентами из K, для которого α является корнем. Метод базисов-делителей поможет нам найти минимальный многочлен в некоторых случаях.

Теорема. Пусть α алгебраичен над полем K с минимальным многочленом $f(x)$ и пусть β алгебраичен над полем $K(\alpha) = K[\alpha]$ с минимальным многочленом $g(\alpha, y)$, где $g(x, y)$ из $K[x, y]$. Тогда β алгебраичен над K, а его минимальный многочлен над K — многочлен $r(y)$, зависящий только от y, из несводимого базиса-делителя идеала $\langle f,\ g\rangle$ в $K[x,\ y]$ относительно словарного порядка $x > y$.

Доказательство. 1) Покажем сначала алгебраичность β над K. Можно считать, что

$$f(x) = x^k + a_1x^{k-1} + \ldots + a_k,\quad a_i \in K,\quad g(x, y) = y^l + b_1(x)y^{l-1} + \ldots + b_l(x),\quad b_i(x) \in K[x].$$

Тогда f и g принадлежат ядру гомоморфизма $\varphi : K[x, y] \longrightarrow K[\alpha, \beta]$, при котором $x \mapsto \alpha,\ y \mapsto \beta$. Из вида f и g следует, что фактор-алгебра $K[x, y]\ /Ker\varphi$ конечномерна над K. Следовательно, степени $1,\ y,\ y^2,\ y^3, \ldots$ линейно зависимы над K по модулю $Ker\varphi$, и потому существует ненулевой многочлен $h(y)$ из $Ker\varphi$. Для него $h(\beta) = 0$.

2) Имеем

$$r(y) = f(x)u(x, y) + g(x, y)v(x, y).$$

Подставляя $x = \alpha,\ y = \beta$, получим равенство $r(\beta) = 0$. Теперь установим минимальность r. Достаточно показать неразложимость $r(y)$ в $K[y]$. Поскольку при $x = \alpha$ получаем $r(y) = g(\alpha, y)v(\alpha, y)$ и $g(\alpha, y)$ неразложим в $K(\alpha)[y]$, то один из неразложимых делителей $p(y)$ многочлена $r(y)$ делится на $g(\alpha, y)$ в кольце $K(\alpha)[y]$:

$$p(y) = g(\alpha, y)w(\alpha, y).$$

Тогда многочлен $p(y) - g(x, y)w(x, y)$ обращается в нуль при $x = \alpha$. Разлагая его по степеням y, получаем, что все коэффициенты разложения делятся на $f(x)$, откуда

$$p(y) - g(x, y)w(x, y) = f(x)s(x, y),\quad p(y) \in \langle f,\ g\rangle.$$

Но тогда *ст.чл.* p делится на *ст.чл.* r и *ст.* p не меньше *ст.* r. С другой стороны, p делит r . Следовательно, $p = r$ и r неразложим.

Упр. Полагая $\alpha = \sqrt{2}, \beta = \sqrt{2} + i$, покажите, что минимальный многочлен для β над $\mathbb{Q}$ равен $y^4 - 2y^2 + 9$.

ПОЛИНОМИАЛЬНЫЕ ПРЕОБРАЗОВАНИЯ ПРОСТРАНСТВ

Здесь будет установлен критерий полиномиальной обратимости для полиномиального отображения пространства K^n в себя, где K — поле.

Пусть K — поле, $f_1, \ldots, f_n \in K[x_1, \ldots, x_n]$. Отображение $\varphi : K^n \longrightarrow K^n$ по правилу

$$\varphi : (a_1, \ldots, a_n) \longmapsto (f_1(a_1, \ldots, a_n), \ldots, f_n(a_1, \ldots, a_n))$$

называется *полиномиальным.* Отметим, что если поле K бесконечно, то разным наборам многочленов отвечают разные полиномиальные отображения. Для конечного поля это не так — многочлены x и $x^2 + x + 1$ задают одинаковые полиномиальные отображения поля из двух элементов.

Упражнение. Для конечного поля K всякое отображение $\varphi : K^n \longrightarrow K^n$ полиномиально.

Полиномиальное отображение $\varphi : K^n \longrightarrow K^n$ называется *полиномиально обратимым,* если существуют такие многочлены $g_1, \ldots, g_n \in K[x_1, \ldots, x_n]$, что

$$g_i(f_1, \ldots, f_n) = x_i, \quad i = 1, \ldots, n.$$

Дифференцируя последнее равенство по x_j, получим

$$\sum_k \left.\frac{\partial g_i}{\partial x_k}\right|_{\substack{x_1=f_1 \\ \cdots \\ x_n=f_n}} \cdot \frac{\partial f_k}{\partial x_j} = \begin{cases} 0 \text{ при } j \neq i \\ 1 \text{ при } j = i. \end{cases}$$

Отсюда матрица Якоби

$$\left(\frac{\partial f_j}{\partial x_i}\right)$$

имеет полиномиальную обратную

$$\begin{pmatrix} & & \\ \left.\dfrac{\partial g_i}{\partial x_j}\right|_{\substack{x_1=f_1 \\ \cdots \\ x_n=f_n}} & & \\ & & \end{pmatrix}$$

и, следовательно, якобиан

$$\det\left(\frac{\partial f_j}{\partial x_i}\right) = c \in K - \{0\}.$$

Отметим, что обратное утверждение не доказано и не опровергнуто до сих пор. Это и есть знаменитая

Проблема якобиана (Келлер, 1939). Будет ли полиномиальное отображение конечномерного векторного пространства над полем скаляров характеристики нуль в это же пространство полиномиально обратимым, если его якобиан является ненулевым скаляром?

Тем не менее, алгоритмическое решение проблемы полиномиальной обратимости полиномиального отображения можно получить с помощью базисов-делителей.

Теорема. Пусть $I = \langle y_1 - f_1, \ldots, y_n - f_n \rangle \lhd K[X, Y]$. Тогда следующие утверждения равносильны:

1) Отображение пространства K^n в себя по правилу

$$\varphi : (a_1, \ldots, a_n) \longmapsto (f_1(a_1, \ldots, a_n), \ldots, f_n(a_1, \ldots, a_n))$$

полиномиально обратимо.

2) Несводимый базис-делитель для идеала I относительно порядка с X-предпочтением перед Y имеет вид

$$x_1 - g_1, \ldots, x_n - g_n,$$

где $g_1, \ldots, g_n \in K[Y]$.

При этом

$$g_i(f_1, \ldots, f_n) = x_i, \quad i = 1, \ldots, n.$$

Доказательство. Если $x_i - g_i = \sum_j h_{ij}(y_j - f_j)$, то, подставляя в это тождество f_j вместо y_j, получим, что $x_i - g_i(f_1, \ldots, f_n) = 0$, откуда обратным для φ будет отображение K^n, связанное с набором многочленов $g_1, \ldots, g_n$.

Теперь предположим, что φ полиномиально обратимо. Тогда найдутся такие многочлены g_i из $K[Y]$, что

$$g_i(f_1, \ldots, f_n) = x_i, \quad i = 1, \ldots, n.$$

Отсюда

$$x_i - g_i = g_i(f_1, \ldots, f_n) - g_i(y_1, \ldots, y_n) \in I,$$

так как если $a_1 - b_1 \in I, \ldots, a_n - b_n \in I$, то $a_1 \cdots a_n - b_1 \cdots b_n \in I$. Таким образом, множество $G = \{x_1 - g_1, \ldots, x_n - g_n\} \subset I$. Кроме того, ясно, что множество G несводимо относительно порядка с X-предпочтением перед Y и оно будет базисом-делителем, если мы покажем, что всякий ненулевой элемент из I содержит X-переменные, т.е. $I \cap K[Y] = 0$. Пусть $g \in I \cap K[Y]$. Тогда

$$g(Y) = \sum_i (y_i - f_i(X)) h_i(X, Y)$$

при некоторых многочленах h_i. Подстановка f_i вместо y_i дает равенство $g(f_1, \ldots, f_n) = 0$. Если $g \neq 0$, то получается, что многочлены $f_1, \ldots, f_n$ алгебраически зависимы над полем

K. С другой стороны, многочлены $x_1, \ldots, x_n$ алгебраически выражаются (как многочлены с коэффициентами из K) через $f_1, \ldots, f_n$ и, очевидно, алгебраически независимы над K. Это противоречит теореме о замене для *алгебраической* зависимости систем элементов поля, принадлежащей Штейницу и аналогичной известной теореме о замене для *линейных* зависимостей систем векторов из векторного пространства (см., Ван дер Варден, Алгебра, М., Наука, 1976, с. 266). Следовательно, $g = 0$ и теорема доказана.

Упражнение. Обратить полиномиальное отображение $\varphi : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$, если

$$\varphi : x \mapsto x + y + 4x^2 + 4xy + y^2, \quad \varphi : y \mapsto 4x + 3y + 8x^2 + 8xy + 2y^2.$$

ЛИТЕРАТУРА

1. Б. Бухбергер, Базисы Грёбнера. Алгоритмический метод в теории полиномиальных идеалов, в кн. "Компьютерная алгебра. Символьные и алгебраические вычисления" (Ред. Б.Бухбергер, Д.Коллинз, Р.Лоос), М., Мир, 1986, стр. 331–372.

2. Дж. Дэвенпорт, И. Сирэ, Э. Турнье, Компьютерная алгебра. Системы и алгоритмы алгебраических вычислений, М., Мир, 1991.

3. Д. Кокс, Дж. Литтл, Д. О'Ши, Идеалы, многоообразия и алгоритмы: Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры, М., Мир, 2000.

4. W.W. Adams, Ph. Loustaunau, An introduction to Grobner Bases, Amer. Math. Soc., 1994, (Grad. Stud. in Math., Vol. 3).

5. T. Becker, V. Weispfenning, in cooperation with H. Kredel, Grobner Bases: A computation approach to commutative algebra, Springer-Verlag, 1993 (GTM, 141).

6. B. Sturmfels, Algorithms in Invariant Theory, Springer, Wien – N.Y., 1993.

7. Grobner bases and application, ed. B. Buchberger, Fr. Winkler, London Math. Soc. Lecture Note Series, 251, Cambr. Univ. Press, 1998.