Санкт-Петербургский государственный университет

Е.А.Калинина, А.Ю.Утешев

ТЕОРИЯ ИСКЛЮЧЕНИЯ

Учебное пособие

НИИ химии СПбГУ
Санкт–Петербург 2002

ББК 22.174
Д32

Р е ц е н з е н т ы:
докт. физ.-мат. наук, проф. *Е.И.Веремей*
(С.-Петерб. гос. ун-т.),
докт. физ.-мат. наук, проф. *В.Ф.Зайцев*
(Рос. гос. пед. ун-т им. А.И.Герцена)

Печатается по постановлению
Редакционно-издательского совета
факультета прикладной математики — процессов управления
Санкт-Петербургского государственного университета

Калинина Е.А., Утешев А.Ю.
Д32 Теория исключения: Учеб. пособие. — СПб.: Изд-во НИИ химии СПбГУ, 2002. — 72 с.

ISBN 5-7997-0419-3

Пособие посвящено изложению основ теории исключения: (суб)результанты и наибольший общий делитель, дискриминант — все эти понятия трактуются в подходах Сильвестра, Кронекера и Безу. Обсуждается приложение этих понятий к задачам решения системы алгебраических уравнений от двух переменных, поиска максимума полиномиальной функции, построения эквидистанты алгебраической кривой, многомерной интерполяции и преобразования Чирнгауза.

Многочисленные примеры и упражнения поясняют вычислительные аспекты алгоритмов и иллюстрируют их особенности, возникающие при реальной работе. Для удобства читателя приведена сводка функций из системы аналитических вычислений MAPLE.

Уровень изложения ориентирован на студентов младших курсов университетов, обучающихся по специальности прикладная математика.

При работе над изданием авторы пользовались поддержкой
Российского фонда фундаментальных исследований,
грант № 01-01-00716.

ББК 22.174

ISBN 5-7997-0419-3

Введение

Настоящая брошюра представляет исправленное и дополненное переиздание учебного пособия авторов [6]. Целью, которую авторы ставили себе при подготовке первого издания, было методическое обеспечение соответствующего раздела в общем курсе высшей алгебры, читаемом на факультете прикладной математики — процессов управления СПбГУ. Однако отзывы коллег убедили авторов в том, что изложенные в пособии результаты могли бы оказаться полезными и для более широкого круга читателей. Объяснение этому обстоятельству авторы видят в том, что в отечественной литературе по алгебре этот раздел традиционно освещается недостаточно полно — в отличие, например, от таких классических курсов, как [21] или [25].

При подготовке нового издания авторы решили сохранить уровень сложности изложения, ориентированный на восприятие студента первого курса классического университета, обучающегося по специальности *прикладная математика*. Предполагается, что студент владеет аппаратом определителей и его применением к задаче установления совместности системы линейных уравнений, а также базовыми понятиями теории полиномов от одной переменной.

Для более же квалифицированного читателя в настоящем введении приведем описание постановок задач и дадим краткий исторический обзор теории.

Итак, объектом теории исключения является система уравнений

$$f_1(x_1, \dots, x_n) = 0, \dots, f_n(x_1, \dots, x_n) = 0 \ , \tag{1}$$

где $f_1, \dots, f_n$ — полиномы по $x_1, \dots, x_n$. Поиск решения такой системы численными (итерационными) методами сложен и, как правило, эффективен только для случая $n = 1$ переменной. Основной целью теории исключения ставится сведение задачи решения системы (1) к одномерному случаю. Именно, с помощью элементарных преобразований систему (1) *как правило* удается свести к эквивалентной ей (т.е. имеющей тот же набор решений) системе вида

$$\mathcal{X}(x_1) = 0,\ x_2 - \vartheta_2(x_1) = 0, \dots, x_n - \vartheta_n(x_1) = 0 \ . \tag{2}$$

Здесь $\mathcal{X}(x_1)$ — полином, а $\vartheta_2(x_1), \dots, \vartheta_n(x_1)$ — рациональные функции по x_1. Следовательно, в этом случае решение системы (1) сведется к решению уравнения от одной переменной; иными словами, все остальные переменные оказываются **исключенными**. Каждый корень полинома $\mathcal{X}(x_1)$ задает первую компоненту (координату) решения системы (1), а соответствующие ему остальные компоненты выражаются через первую с помощью оставшихся уравнений системы (2). Еще раз подчеркнем то обстоятельство, что все компоненты решения системы (1) могут быть рационально выражены через какую-то одну, например — как в системе (2) — первую.

Техника, позволяющая осуществить приведение системы (1) к виду (2), основана на понятии **результанта**. Формально результант двух полиномов $f(x)$ и $g(x)$ можно определить как полиномиальную функцию коэффициентов $f(x)$ и $g(x)$, обращение которой в нуль является условием необходимым и достаточным для существования общего корня указанных полиномов. Вопрос о существовании такой функции ставился еще Ньютоном; однако первое систематическое исследование этого вопроса было предпринято Безу, изложившим свои результаты в книге [17]. В заслугу Безу может быть поставлено распространение идеи результанта на случай полиномов от нескольких переменных. Последнее позволило ему доказать фундаментальный результат теории: число решений системы (1) *как правило* равно произведению степеней входящих в нее полиномов:

$$\deg\left(\mathcal{X}(x_1)\right) = \deg f_1 \times \ldots \times \deg f_n \ .$$

XIX век стал веком расцвета теории в трудах Пуассона, Абеля, Коши, Лиувилля, Эрмита, Кронекера, Кэли, Сильвестра, Шлэфли и ряда других ученых.

В тридцатые годы XX века теория стала жертвой общей тенденции к аксиоматической формализации математики — тенденции, намеченной еще Гильбертом и впоследствии реализованной Ван-дер-Варденом и Бурбаки. Результатом явилось то, что в учебниках по алгебре для изложения была выбрана хотя и универсальная, логически последовательная, но, вместе с тем, абсолютно неконструктивная методология изложения теории [3], [22]; все богатство, накопленное предыдущим веком, полностью игнорировалось. Последствия не заставили себя ждать: интерес к теории потеряли сначала прикладные математики, а потом и "чистые"; она практически исчезает из университетских учебников или же остается в них незначительными фрагментами[1].

Интерес возродился в восьмидесятые годы. Ряд факторов благоприятствовал этому. Одним из таких факторов стала потребность в абсолютной достоверности результатов, получаемых в ходе вычислений. Другим же фактором явилась необходимость в оценке влияния на решения параметров, входящих в систему (1). Даже если численные методы и могли решить систему (1) при некоторой специализации параметров, то они оказывались малопригодными для задачи исследования динамики решений при вариации этих параметров. Именно для подобных исследований возможность аналитического представления решений или, хотя бы, преобразования системы (1) к эквивалентной, но более простого вида, может оказаться решающей. Известная трудоемкость символьных алгоритмов потребовала достаточного развития вычислительной техники, но после того как это произошло, область науки, известная как "компьютерная алгебра", стала бурно разви-

[1] По меткому выражению одного из авторов, теория *исключения* была фактически *исключена* из алгебры.

ваться. Эта область располагается на стыке математики и информатики; интерес к ней научного сообщества выражается в быстро растущем числе публикаций, из которых укажем только некоторые обзорные монографии и сборники статей [1], [5], [7], [8]. Компьютерная алгебра имеет дело, в основном, с точными числами и алгебраическими выражениями в их символьном представлении. В таких ее системах общего назначения, как REDUCE, MACSYMA, MATHEMATICA, MAPLE, AXIOM, MuPAD алгоритмический базис составляют операции над полиномами и рациональными функциями, поэтому исследования в этой области включают в себя создание, развитие и анализ эффективности методов факторизации, вычисления наибольших общих делителей, отделения (локализации) вещественных корней полиномов, преобразования систем алгебраических уравнений к наиболее простому виду. Поскольку идеологии решения задач двух алгебр — классической и компьютерной — совпали, интерес современных исследователей к разработке научного наследия XIX века значительно возрос.

Интерес к теории исключения был стимулирован еще и потребностью выявить истоки теории базисов Грёбнера, первое конструктивное продвижение которой обеспечили работы Бухбергера в семидесятых годах XX века. Бухбергером был разработан универсальный алгоритм построения базиса идеала, порожденного полиномами $f_1, \ldots, f_n$; при некоторых дополнительных условиях искомый базис удается построить в форме $\widetilde{\mathcal{X}}(x_1), x_2 - \widetilde{\vartheta_2}(x_1), \ldots, x_n - \widetilde{\vartheta_n}(x_1)$ при полиномиальных $\widetilde{\mathcal{X}}, \widetilde{\vartheta_2}, \ldots, \widetilde{\vartheta_n}$. Тем самым обеспечивается возможность сведения системы (1) к виду (2). К сожалению, алгоритм Бухбергера (и многочисленные последующие модификации) оказался своего рода "черным ящиком" — когда для конкретной системы (1) практически невозможно оценить априори время расчета системы (2). В сравнении с методом базисов Грёбнера теория исключения обладает весьма существенным преимуществом, а именно — наглядностью. Представление результанта в виде подходящего определителя оказалось довольно удобным также и с точки зрения оценки влияния вариаций коэффициентов полиномов на решения системы.

Теперь опишем кратко содержание настоящего пособия. В первой его части вводится основополагающее понятие результанта и устанавливаются свойства последнего. Формальное определение основывается на представлении результанта в виде определителя (детерминанта) Сильвестра. Не являясь самым вычислительно оптимальным способом вычисления, этот способ, тем не менее, является наиболее наглядным. Выводятся основные свойства результанта, устанавливается его связь с алгоритмом Евклида вычисления наибольшего общего делителя полиномов, указываются альтернативные детерминантные представления результанта (в форме Кронекера и в форме Безу), обсуждаются его применения для вычисления дискриминанта и преобразования Чирнгауза, для нахождения экстремальных значений полинома и др. Среди этого многообразия выделим два ключевых результата:

1) результант позволяет по коэффициентам полиномов однозначно установить, имеют ли они общий корень;

2) если упомянутый корень единственен, то его можно найти как рациональную функцию коэффициентов полиномов — с помощью миноров результанта.

Именно эти результаты используются во второй части для построения алгоритма исключения переменной в системе двух уравнений. Для такой системы мы приводим также доказательство теоремы Безу о “наиболее вероятном” числе ее решений, а также обсуждаем такие исключительные случаи как, например, неприводимость системы (1) к виду (2). Рассматриваются также приложения теории исключения к различным задачам алгебры, геометрии и теории дифференциальных уравнений.

Обозначения

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ и $\mathbb{Z}$ — множества комплексных, вещественных, рациональных и целых чисел соответственно.

$\lfloor\ \rfloor$ обозначает целую часть числа.

Запись $f(x) \in \mathbb{C}[x]$ означает, что коэффициенты $f(x)$ принадлежат множеству комплексных чисел. Аналогично для множеств $\mathbb{R}$, $\mathbb{Q}$ и $\mathbb{Z}$ и для полиномов нескольких переменных. Запись $f(x) \in \mathbb{A}[x]$ означает, что коэффициенты $f(x)$ принадлежат какому-то конкретному из множеств $\mathbb{C}, \mathbb{R}$ или $\mathbb{Q}$.

$\mathcal{R}(f,g)$ (или $\mathcal{R}_x(f,g)$) — результант полиномов f и g (по определенной переменной).

$\mathsf{НОД}\,(f,g)$ — наибольший общий делитель полиномов.

$\mathcal{D}(f)$ — дискриминант полинома.

$\mathcal{J}(x,y)$ — якобиан полиномов.

$\mathbb{O}$ — нулевая матрица (вектор); иногда также означает, что некоторое место матрицы занято нулевыми элементами.

^{t} — означает транспонирование матрицы.

Знак $\ominus$ означает, что данный параграф (теорему, упражнение и пр.) при первом чтении можно пропустить

Замечание. В §8 вводится определение **элиминанты**; так, полином $\mathcal{X}(x_1)$ из формул (2) будет **элиминантой системы (1) по переменной** x_1 (или **по исключению переменных** $x_2, \ldots, x_n$). Характерное для учебников XIX века, в современных книгах оно не встречается. Аналогичное замечание справедливо и относительно понятия **эквидистанты** из §11.3.

Часть 1. Результант и субрезультанты

1 Результант

1.1 Определение

Пример 1.1. *Найти условие, при котором полиномы*

$$f(x) = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5 \text{ и } g(x) = b_0x^3 + b_1x^2 + b_2x + b_3$$

$(a_0 \neq 0, b_0 \neq 0)$ *из* $\mathbb{A}[x]$ *имеют общий корень.*

Решение. Пусть f и g имеют корень $x = c \in \mathbb{C}$: $f(c) = 0, g(c) = 0$. Тогда

$$\begin{array}{rl}
c^2f(c) = & a_0c^7+a_1c^6+a_2c^5+a_3c^4+a_4c^3+a_5c^2 = 0\ ,\\
cf(c) = & a_0c^6+a_1c^5+a_2c^4+a_3c^3+a_4c^2+a_5c = 0\ ,\\
f(c) = & a_0c^5+a_1c^4+a_2c^3+a_3c^2+a_4c+a_5 = 0\ ,\\
g(c) = & b_0c^3+b_1c^2+b_2c+b_3 = 0\ ,\\
cg(c) = & b_0c^4+b_1c^3+b_2c^2+b_3c = 0\ ,\\
c^2g(c) = & b_0c^5+b_1c^4+b_2c^3+b_3c^2 = 0\ ,\\
c^3g(c) = & b_0c^6+b_1c^5+b_2c^4+b_3c^3 = 0\ ,\\
c^4g(c) = & b_0c^7+b_1c^6+b_2c^5+b_3c^4 = 0\ .
\end{array} \tag{1.1}$$

Запишем эти равенства как систему линейных уравнений

$$\underbrace{\begin{array}{c}3\\5\end{array}\left\{\begin{pmatrix}
a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & & \\
 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & \\
 & & a_0 & a_1 & a_2 & a_3 & a_4 & a_5\\
 & & & & b_0 & b_1 & b_2 & b_3\\
 & & & b_0 & b_1 & b_2 & b_3 & \\
 & & b_0 & b_1 & b_2 & b_3 & & \\
 & b_0 & b_1 & b_2 & b_3 & & & \\
b_0 & b_1 & b_2 & b_3 & & & &
\end{pmatrix}\right.}_{M_{8\times8}}\underbrace{\begin{pmatrix}c^7\\c^6\\c^5\\c^4\\c^3\\c^2\\c\\1\end{pmatrix}}_{X} = \mathbb{O}_{8\times1} \tag{1.2}$$

относительно столбца неизвестных $X = \left[c^7, c^6, c^5, c^4, \ldots, 1\right]^t$ (неуказанные элементы матрицы M считаются равными нулю). Эта система однородная и имеет нетривиальное решение (последняя компонента вектора X равна единице). Следовательно, определитель ее матрицы равен нулю: $\det M{=}0$. Это условие является необходимым для существования общего корня у полиномов f и g. △

Для общего случая полиномов

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \text{ и } g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m$$

из $\mathbb{A}[x]$ ($a_0 \neq 0$, $b_0 \neq 0$) составим квадратную матрицу порядка $m+n$:

$$M = \left(\begin{array}{ccccccccccc} a_0 & a_1 & a_2 & \dots & \dots & a_n & 0 & \dots & 0 & 0 \\ 0 & a_0 & a_1 & \dots & \dots & a_{n-1} & a_n & \dots & 0 & 0 \\ \vdots & & \ddots & & & & & & \ddots & \\ 0 & 0 & \dots & a_0 & \dots & \dots & & \dots & a_{n-1} & a_n \\ 0 & 0 & \dots & & b_0 & b_1 & \dots & \dots & b_{m-1} & b_m \\ 0 & 0 & \dots & b_0 & b_1 & \dots & & \dots & b_m & 0 \\ \vdots & & \iddots & \dots & & & & & & \vdots \\ 0 & b_0 & \dots & \dots & b_m & 0 & \dots & & \dots & 0 \\ b_0 & \dots & \dots & b_m & 0 & \dots & & & & 0 \end{array} \right) \begin{array}{l} \left. \begin{array}{l} \\ \\ \\ \\ \end{array} \right\} m \\ \left. \begin{array}{l} \\ \\ \\ \\ \end{array} \right\} n \end{array} , \qquad (1.3)$$

элементы выше a_n и b_0, и ниже a_0 и b_m все равны нулю.

Определение. Выражение

$$\mathcal{R}(f,g) \stackrel{\text{def}}{=} (-1)^{n(n-1)/2} \det M \qquad (1.4)$$

называется **результантом** полиномов f и g (в форме Сильвестра).

По построению, результант является полиномом относительно коэффициентов $a_0, \dots, a_n, b_0, \dots, b_m$:

$$\mathcal{R}(a_0 x^n + \dots + a_n,\ b_0 x^m + \dots + b_m) \in \mathbb{Z}[a_0, \dots, a_n, b_0, \dots, b_m] \ .$$

Упражнение 1.1. *Доказать равенство*

$$\mathcal{R}(a_0x^2+a_1x+a_2,\ b_0x^2+b_1x+b_2) = (a_0b_2-a_2b_0)^2-(a_0b_1-a_1b_0)(a_1b_2-a_2b_1) \ . \qquad (1.5)$$

Теорема 1.1. *Для того чтобы f и g имели общий корень, необходимо и достаточно выполнение условия $\mathcal{R}(f,g) = 0$.*

Доказательство . Нам осталось показать достаточность. Идею доказательства проиллюстрируем на примере 1.1. Пусть

$$f(x) \equiv a_0(x-\lambda_1) \times \dots \times (x-\lambda_5),\ g(x) \equiv b_0(x-\mu_1)(x-\mu_2)(x-\mu_3) \ .$$

Дополнительно предположим, что все корни $\lambda_1, \dots, \lambda_5$ полинома $f(x)$ различны и все корни μ_1, μ_2, μ_3 полинома $g(x)$ различны.

Домножим матрицу M справа на матрицу

$$V = \left(\begin{array}{cccccc} \mu_1^7 & \mu_2^7 & \mu_3^7 & \lambda_1^7 & \dots & \lambda_5^7 \\ \mu_1^6 & \mu_2^6 & \mu_3^6 & \lambda_1^6 & \dots & \lambda_5^6 \\ \dots & & & & & \dots \\ \mu_1 & \mu_2 & \mu_3 & \lambda_1 & \dots & \lambda_5 \\ 1 & 1 & 1 & 1 & \dots & 1 \end{array} \right)_{8\times 8} \ .$$

Результатом умножения будет следующая матрица:

$$L = \begin{pmatrix} \mu_1^2 f(\mu_1) & \mu_2^2 f(\mu_2) & \mu_3^2 f(\mu_3) & 0 & \dots & 0 \\ \mu_1 f(\mu_1) & \mu_2 f(\mu_2) & \mu_3 f(\mu_3) & 0 & \dots & 0 \\ f(\mu_1) & f(\mu_2) & f(\mu_3) & 0 & \dots & 0 \\ 0 & 0 & 0 & g(\lambda_1) & \dots & g(\lambda_5) \\ 0 & 0 & 0 & \lambda_1 g(\lambda_1) & \dots & \lambda_5 g(\lambda_5) \\ 0 & 0 & 0 & \lambda_1^2 g(\lambda_1) & \dots & \lambda_5^2 g(\lambda_5) \\ 0 & 0 & 0 & \lambda_1^3 g(\lambda_1) & \dots & \lambda_5^3 g(\lambda_5) \\ 0 & 0 & 0 & \lambda_1^4 g(\lambda_1) & \dots & \lambda_5^4 g(\lambda_5) \end{pmatrix} .$$

В получившемся матричном равенстве перейдем к определителям:

$$M \cdot V = L \;\Rightarrow\; \det M \det V = \det L \;. \tag{1.6}$$

Найдем выражения для $\det V$ и для $\det L$. Матрица V представляет собой матрицу Вандермонда (с точностью до перестановки строк). Как известно, ее определитель равен произведению всевозможных разностей, составленных из чисел $\lambda_1, \dots, \lambda_5$, μ_1, μ_2, μ_3:

$$\det V = \left[\prod_{1 \le L < K \le 3} (\mu_K - \mu_L) \right] \left[\prod_{1 \le \ell < k \le 5} (\lambda_k - \lambda_\ell) \right] \left[\prod_{k=1}^{3} \prod_{j=1}^{5} (\mu_k - \lambda_j) \right] \;.$$

Далее, матрица L блочно-диагональная, и

$$\det L = \begin{vmatrix} \mu_1^2 f(\mu_1) & \mu_2^2 f(\mu_2) & \mu_3^2 f(\mu_3) \\ \mu_1 f(\mu_1) & \mu_2 f(\mu_2) & \mu_3 f(\mu_3) \\ f(\mu_1) & f(\mu_2) & f(\mu_3) \end{vmatrix} \cdot \begin{vmatrix} g(\lambda_1) & \dots & g(\lambda_5) \\ \lambda_1 g(\lambda_1) & \dots & \lambda_5 g(\lambda_5) \\ \lambda_1^2 g(\lambda_1) & \dots & \lambda_5^2 g(\lambda_5) \\ \lambda_1^3 g(\lambda_1) & \dots & \lambda_5^3 g(\lambda_5) \\ \lambda_1^4 g(\lambda_1) & \dots & \lambda_5^4 g(\lambda_5) \end{vmatrix} =$$

$$= f(\mu_1) f(\mu_2) f(\mu_3) \begin{vmatrix} \mu_1^2 & \mu_2^2 & \mu_3^2 \\ \mu_1 & \mu_2 & \mu_3 \\ 1 & 1 & 1 \end{vmatrix} g(\lambda_1) \times \dots \times g(\lambda_5) \begin{vmatrix} 1 & \dots & 1 \\ \lambda_1 & \dots & \lambda_5 \\ \lambda_1^2 & \dots & \lambda_5^2 \\ \lambda_1^3 & \dots & \lambda_5^3 \\ \lambda_1^4 & \dots & \lambda_5^4 \end{vmatrix} =$$

(обращаем внимание на то, что определители — снова типа Вандермонда)

$$= - \left[\prod_{1 \le L < K \le 3} (\mu_K - \mu_L) \right] \cdot \left[\prod_{1 \le \ell < k \le 5} (\lambda_k - \lambda_\ell) \right] f(\mu_1) f(\mu_2) f(\mu_3) g(\lambda_1) \times \dots \times g(\lambda_5) \;.$$

Итак, это — величина правой части равенства (1.6), а величина левой, с точностью до знака, равна $\mathcal{R}(f,g) \cdot \det V$. Если $\mathcal{R}(f,g) = 0$, то хотя бы одно из чисел

$$f(\mu_1),\, f(\mu_2),\, f(\mu_3),\, g(\lambda_1), \dots, g(\lambda_5)$$

должно обратиться в нуль (поскольку, по предположению, $\lambda_k \neq \lambda_\ell, \mu_K \neq \mu_L$). $\square$

Замечание. Используя выведенное в ходе доказательства выражение для $\det V$, можем получить из равенства (1.6) явное представление результанта $\mathcal{R}(f,g)$ через корни обоих полиномов. Действительно, сократив[2] общий множитель, получим:

$$\mathcal{R}(f,g) = a_0^m b_0^n \prod_{k=1}^{m} \prod_{j=1}^{n} (\lambda_j - \mu_k) \ , \tag{1.7}$$

где $\lambda_1, \ldots, \lambda_n$ — корни полинома $f(x)$, а $\mu_1, \ldots, \mu_m$ — корни полинома $g(x)$. Таким образом, величина $\mathcal{R}(f,g)$ характеризует расстояние между множествами корней полинома $f(x)$ и полинома $g(x)$. В свою очередь, формулу (1.7) можно переписать в эквивалентных видах:

$$\mathcal{R}(f,g) = a_0^m \prod_{j=1}^{n} g(\lambda_j) = \tag{1.8}$$

$$= (-1)^{mn} b_0^n \prod_{k=1}^{m} f(\mu_k) \ . \tag{1.9}$$

Иногда в литературе равенство (1.8) берут в качестве формального определения результанта. В частном случае $g(x) \equiv const$ из нее следует:

$$\mathcal{R}(f, const) = (const)^n \ . \tag{1.10}$$

Упражнение 1.2. *Доказать, что* $\mathcal{R}(f,g) = (-1)^{nm}\mathcal{R}(g,f)$.

Упражнение 1.3. *Доказать, что* $\mathcal{R}\,(f_1 \cdot f_2,\, g) = \mathcal{R}(f_1,\, g) \cdot \mathcal{R}(f_2,\, g)$.

Пример 1.2. *Доказать, что если* $n \geq m \geq 1$, $A \neq 0$, $C \neq 0$ *и* $\deg(Af(x) + Bg(x)) = \deg(Cf(x) + Dg(x)) = n$, *то*

$$\mathcal{R}(Af(x) + Bg(x), Cf(x) + Dg(x)) = (AD - BC)^n \mathcal{R}\,(f(x), g(x)) \ .$$

Решение. Из определения результанта следует, что

$$\mathcal{R}(Af, Dg) = A^m D^n \mathcal{R}(f,g) \ . \tag{1.11}$$

По условию $\deg(Cf + Dg) = n$. Используя (1.11) и (1.8), получаем

$$\mathcal{R}(f, Cf + Dg) = D^n \mathcal{R}(f,g) \ . \tag{1.12}$$

[2] Что, строго говоря, не всегда допустимо... Тем не менее, мы просим принять на веру, что следующая формула будет верна всегда!

Очевидно, что $Cf + Dg = D(Af + Bg)/B - (AD - BC)f/B$. Применяя результат упражнения 1.2, получаем

$$\mathcal{R}(Af+Bg, Cf+Dg) = \mathcal{R}\left(Af+Bg, \frac{D}{B}(Af+Bg) - \frac{AD-BC}{B}f\right) =$$

$$= \left(-\frac{AD-BC}{B}\right)^n \mathcal{R}(Af+Bg, f) = \left(-\frac{AD-BC}{B}\right)^n (-1)^{n^2} \mathcal{R}(f, Af+Bg) =$$

$$= B^n \left(\frac{AD-BC}{B}\right)^n \mathcal{R}(f,g) = (AD-BC)^n \mathcal{R}(f,g) \ .$$

△

Пример 1.3. *Пусть*

$$f^*(x) \stackrel{\text{def}}{=} x^n f(1/x) = a_n x^n + \ldots + a_0, \ g^*(x) \stackrel{\text{def}}{=} x^m g(1/x) = b_m x^m + \ldots + b_0,$$

и числа a_0, a_n, b_0, b_m отличны от нуля. Доказать, что

$$\mathcal{R}(f^*, g^*) = (-1)^{mn} \mathcal{R}(f,g) \ .$$

Решение. Корнями полинома f^* являются числа $1/\lambda_j$. Используя равенство (1.8) и формулу Виета, получаем

$$\mathcal{R}(f^*, g^*) = a_n^m \prod_{j=1}^n g^*\left(\frac{1}{\lambda_j}\right) = a_n^m \prod_{j=1}^n \left(\frac{1}{\lambda_j}\right)^m \prod_{j=1}^n g(\lambda_j) =$$

$$= (-1)^{mn} a_0^m \prod_{j=1}^n g(\lambda_j) = (-1)^{mn} \mathcal{R}(f,g) \ .$$

△

Упражнение 1.4. *Вычислить результант полиномов:*
а) $3x^2 + x - 2$ *и* $x^2 - 2x - 2$*;*
б) $x^3 - 3x + 6$ *и* $x^3 + x^2 - x - 1$*.*

Упражнение 1.5. *Найти все значения параметра p, при которых полиномы*
а) $x^3 + px + 1$ *и* $x^2 + px + 1$*;*
б) $x^3 + px^2 - 20$ *и* $x^3 + px - 14$
имеют общий корень.

1.2 Результант и алгоритм Евклида

Итак, согласно теореме 1.1, условие $\mathcal{R}(f,g)=0$ равносильно существованию общего корня полиномов $f(x)$ и $g(x)$, или же, иными словами, *нетривиального* наибольшего общего делителя $\mathsf{НОД}\,(f,g)$ этих полиномов. Обратно, условие $\mathcal{R}(f,g)\neq 0$ гарантирует взаимную простоту полиномов $f(x)$ и $g(x)$, т.е. то, что $\mathsf{НОД}\,(f,g)=const\neq 0$. Поскольку конструктивное вычисление $\mathsf{НОД}\,(f,g)$ может быть организовано по алгоритму Евклида, следует ожидать, что в этом алгоритме выражение для $\mathcal{R}(f,g)$ должно явно проявиться на каком-то этапе.

Пример 1.4. *Найти условия взаимной простоты полиномов*

$$f(x)=a_0x^2+a_1x+a_2 \;\; и \;\; g(x)=b_0x^2+b_1x+b_2,\;\; a_0\neq 0, b_0\neq 0 \;\; .$$

Решение. Первым шагом алгоритма Евклида будет деление (с остатком) $f(x)$ на $g(x)$:

$$f(x)=\frac{a_0}{b_0}g(x)+\underbrace{\left(a_1-\frac{a_0b_1}{b_0}\right)x+\left(a_2-\frac{a_0b_2}{b_0}\right)}_{\stackrel{\text{def}}{=}r_1(x)} \;\; .$$

Предположим сначала, что $a_1b_0-a_0b_1\neq 0$. Тогда второй шаг алгоритма Евклида заключается в делении $g(x)$ на $r_1(x)$. После длинных выкладок получим:

$$g(x)=r_1(x)\frac{b_0}{a_1b_0-a_0b_1}\left[b_0x+\left(b_1-b_0\frac{a_2b_0-a_0b_2}{a_1b_0-a_0b_1}\right)\right]+\underbrace{\frac{b_0\mathcal{R}(f,g)}{(a_1b_0-a_0b_1)^2}}_{\stackrel{\text{def}}{=}r_2(x)} \;\; ,$$

где $\mathcal{R}(f,g)$ в точности совпадает с результантом (1.5).

Теперь проанализируем $\mathsf{НОД}\,(f,g)$ в зависимости от величины $\mathcal{R}(f,g)$. Если $\mathcal{R}(f,g)\neq 0$, то очевидно, что на следующем, т.е. третьем, шаге алгоритм Евклида остановится и $\mathsf{НОД}\,(f,g)=r_2(x)=const\neq 0$. В этом случае полиномы $f(x)$ и $g(x)$ взаимно просты. Если же $\mathcal{R}(f,g)=0$, то $\mathsf{НОД}\,(f,g)=r_1(x)$, т.е. $\mathsf{НОД}$ является линейным по x полиномом.

Предположим теперь, что $a_1b_0-a_0b_1=0$. Алгоритм Евклида остановится уже на втором шаге. Полиномы $f(x)$ и $g(x)$ будут взаимно простыми при $a_2b_0-a_0b_2\neq 0$. Одновременное выполнение условий

$$a_1b_0-a_0b_1=0 \quad \text{и} \quad a_2b_0-a_0b_2=0$$

равносильно тому, что коэффициенты полиномов $f(x)$ и $g(x)$ пропорциональны, т.е. $f(x)=Cg(x)$ при некоторой константе C. Тогда $\mathsf{НОД}\,(f,g)$ совпадает с любым из этих полиномов.

Обобщая предшествующие рассуждения, можем выписать условие взаимной простоты $f(x)$ и $g(x)$.

Ответ. $\mathsf{НОД}\,(f,g)=1$ тогда и только тогда, когда $\mathcal{R}(f,g)\neq 0$, где число $\mathcal{R}(f,g)$ определяется формулой (1.5).

Рассмотрим теперь общую схему алгоритма Евклида. Пусть схема последовательного деления имеет вид:

$$\begin{aligned}
f(x) &= g(x)q_1(x)+r_1(x)\ , \quad 0\le \deg r_1(x)<\deg g(x)\ ,\\
g(x) &= r_1(x)q_2(x)+r_2(x)\ , \quad 0\le \deg r_2(x)<\deg r_1(x)\ ,\\
r_1(x) &= r_2(x)q_3(x)+r_3(x)\ , \quad 0\le \deg r_3(x)<\deg r_2(x)\ ,\\
&\dots \qquad \dots\\
r_{k-2}(x) &= r_{k-1}(x)q_k(x)+r_k(x)\ , \quad 0\le \deg r_k(x)<\deg r_{k-1}(x)\ ,\\
r_{k-1}(x) &= r_k(x)q_{k+1}(x)\ ;
\end{aligned}$$

т.е. $r_k(x)=\mathsf{НОД}\,(f(x),g(x))$. Рассмотрим первую строчку схемы. Очевидно, что на корнях полинома $g(x)$ значения $f(x)$ и $r_1(x)$ совпадают: $f(\mu_k)=r_1(\mu_k)$. Тогда, на основании формулы (1.9), имеем

$$\mathcal{R}(f,g)=(-1)^{mn}b_0^n\prod_{k=1}^{m}f(\mu_k)=(-1)^{mn}b_0^n\prod_{k=1}^{m}r_1(\mu_k)=(-1)^{mn}b_0^{n-n_1}\mathcal{R}(g,r_1)\ ,$$

здесь $n_1\stackrel{\text{def}}{=}\deg r_1(x)$. Итак, с точностью до степени старшего коэффициента полинома g, результант полиномов f и g совпадает с результантом полиномов g и r_1. Теперь перейдем ко второй строчке схемы. На основании тех же рассуждений можем утверждать, что $\mathcal{R}(g,r_1)=(-1)^{n_1m}\widetilde{b}_0^{n_1-n_2}\mathcal{R}(r_1,r_2)$, где $n_2\stackrel{\text{def}}{=}\deg r_2(x)$, а $\widetilde{b}_0$ — старший коэффициент полинома $r_1(x)$. Продолжаем процесс далее. На каждом шаге степени остатков понижаются, т.е. вычисление результанта все упрощается. И если предположить, что предпоследний остаток, т.е. $r_{k-1}(x)$, является линейным полиномом, то $r_k(x)$ должен быть константой: $r_k(x)\equiv const$. Согласно формуле (1.10), эта константа совпадает с $\mathcal{R}(r_{k-1},\,r_k)$ и, следовательно, будет обращаться в нуль тогда и только тогда, когда $\mathcal{R}(f,g)=0$. Если взять коэффициенты полиномов f и g *символьными* (буквенными) — как это было сделано в примере 1.4, то результант этих полиномов, рассматриваемый как полином относительно их коэффициентов, будет совпадать с $\mathcal{R}(r_{k-1},\,r_k)$, с точностью до сомножителя, являющегося рациональной функцией коэффициентов. Таким образом, вычисление $\mathcal{R}(f,g)$ может быть произведено с помощью вычисления $\mathsf{НОД}\,(f,g)$ по алгоритму Евклида; именно эта схема вычисления реализована во всех пакетах компьютерной алгебры.

Покажем теперь отношение результанта к еще одной задаче.

Задача. Найти полиномы $u(x)$ и $v(x)$ из $\mathbb{A}[x]$, обеспечивающие справедливость тождества

$$f(x)v(x)+g(x)u(x)\equiv\mathsf{НОД}\,(f,g)\ , \tag{1.13}$$

которое называется **линейным представлением наибольшего общего делителя**.

Теорема 1.2. *Существуют полиномы* $\tilde{u}(x)$ *и* $\tilde{v}(x)$ *из* $\mathbb{A}[x]$ *со степенями* $\deg\tilde{u} \le (\deg f) - 1,\ \deg\tilde{v} \le (\deg g) - 1$, *удовлетворяющие тождеству*

$$\mathcal{R}(f,g) \equiv f(x)\tilde{v}(x) + g(x)\tilde{u}(x)\ . \tag{1.14}$$

Если, вдобавок, полиномы $f(x)$ *и* $g(x)$ *взаимно просты, то полиномы* $\tilde{u}(x)$ *и* $\tilde{v}(x)$ *будут определяться единственным образом.*

Доказательство проведем снова для случая $n = 5$ и $m = 3$. Прибавим к последнему столбцу матрицы M ее первый столбец, домноженный на x^7, второй, домноженный на x^6, и т.д., предпоследний, домноженный на x. Величина определителя не изменится. С другой стороны,

$$\mathcal{R}(f,g) = \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & 0 & x^2f(x) \\ 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & xf(x) \\ 0 & 0 & a_0 & a_1 & a_2 & a_3 & a_4 & f(x) \\ 0 & 0 & 0 & 0 & b_0 & b_1 & b_2 & g(x) \\ 0 & 0 & 0 & b_0 & b_1 & b_2 & b_3 & xg(x) \\ 0 & 0 & b_0 & b_1 & b_2 & b_3 & 0 & x^2g(x) \\ 0 & b_0 & b_1 & b_2 & b_3 & 0 & 0 & x^3g(x) \\ b_0 & b_1 & b_2 & b_3 & 0 & 0 & 0 & x^4g(x) \end{vmatrix}\ .$$

Представим последний столбец определителя в виде суммы двух:

$$[x^2f(x), xf(x), f(x), 0, 0, 0, 0, 0]^t \text{ и } [0, 0, 0, g(x), xg(x), x^2g(x), x^3g(x), x^4g(x)]^t\ ;$$

тогда определитель можно также представить в виде суммы двух слагаемых. Следовательно, полином $\tilde{v}(x)$ (или $\tilde{u}(x)$) равен определителю, получающемуся из результанта заменой в нем последнего столбца на $[x^2, x, 1, 0, 0, 0, 0, 0]^t$ (или соответственно на $[0, 0, 0, 1, x, x^2, x^3, x^4]^t$).

Пусть теперь полиномы $f(x)$ и $g(x)$ взаимно просты. Тогда тождество (1.13) имеет вид

$$f(x)\tilde{v}(x) + g(x)\tilde{u}(x) \equiv 1\ . \tag{1.15}$$

Будем искать полиномы $\tilde{u}(x)$ и $\tilde{v}(x)$, ему удовлетворяющие, методом неопределенных коэффициентов:

$$\tilde{v}(x) \stackrel{\text{def}}{=} v_0x^2 + v_1x + v_2,\ \tilde{u}(x) \stackrel{\text{def}}{=} u_0x^4 + u_1x^3 + u_2x^2 + u_3x + u_4\ .$$

Подставим эти выражения в тождество (1.15)

$$(v_0a_0 + u_0b_0)x^7 + (v_0a_1 + v_1a_0 + u_0b_1 + u_1b_0)x^6 + \ldots + (v_2a_5 + u_4b_3) \equiv 1$$

и приравняем коэффициенты при одинаковых степенях x:

$$\begin{array}{lllllll}
v_0a_0 & & & +u_0b_0 & & & = 0\\
v_0a_1 & +v_1a_0 & & +u_0b_1 & +u_1b_0 & & = 0\\
v_0a_2 & +v_1a_1 & +v_2a_0 & +u_0b_2 & +u_1b_1 & +u_2b_0 & = 0\\
 & & \dots & & & \dots & \dots\\
 & & v_2a_5 & & & +u_4b_3 & = 1
\end{array}$$

Получим систему из 8 линейных уравнений для определения 8 коэффициентов $v_0, v_1, v_2, u_0, u_1, u_2, u_3, u_4$. Определитель этой системы (с точностью до транспонирования и перестановки столбцов) совпадает с результантом. По предположению, $\mathcal{R}(f,g) \neq 0$. Следовательно, система имеет единственное решение, которое может быть определено по формулам Крамера. Легко показать тождественность этого решения тому, что получено в доказательстве первой части теоремы. □

Пример 1.5. *Найти полиномы $\tilde{u}(x)$ и $\tilde{v}(x)$, удовлетворяющие тождеству* (1.14) *для* $f(x) = x^5 - 4\,x - 2,\ g(x) = x^3 - 1$.

Решение. Разложим по последнему столбцу определитель

$$\tilde{v}(x) = \begin{vmatrix}
1 & 0 & 0 & 0 & -4 & -2 & 0 & x^2\\
0 & 1 & 0 & 0 & 0 & -4 & -2 & x\\
0 & 0 & 1 & 0 & 0 & 0 & -4 & 1\\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 1 & 0 & 0 & -1 & 0\\
0 & 0 & 1 & 0 & 0 & -1 & 0 & 0\\
0 & 1 & 0 & 0 & -1 & 0 & 0 & 0\\
1 & 0 & 0 & -1 & 0 & 0 & 0 & 0
\end{vmatrix} = -18\,x^2 + 7\,x - 8\ .$$

Аналогично находим $\tilde{u}(x) = 18\,x^4 - 7\,x^3 + 8\,x^2 + 18\,x - 79$,а $\mathcal{R}(f,g) = 95$. △

Упражнение 1.6. *Найти полиномы $\tilde{u}(x)$ и $\tilde{v}(x)$, удовлетворяющие тождеству* (1.14) *для*

а) $f(x) = x^3 + 3x + 3,\ g(x) = x^2 - x - 2$;

б) $f(x) = x^4,\ g(x) = x^3 - 3x^2 + 4$;

в) $f(x) = x^5 - x^3 + 2x^2 - 2x + 2,\ g(x) = x^4 + 2x^3 + 7x^2 + 2x + 6$.

Упражнение 1.7. *Зная, что полиномы $f(x)$ и $g(x)$ взаимно просты, методом неопределенных коэффициентов подобрать полиномы $\tilde{u}(x)$ и $\tilde{v}(x)$ наименьшей степени, удовлетворяющие тождеству* (1.15) *для*

а) $f(x) = x^5,\ g(x) = (x-2)^3$;

б) $f(x) = x^3 + x^2 - x - 2,\ g(x) = x^3 - 4x^2 + 5x - 2$.

2 Дискриминант

Для того чтобы полином $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbb{A}[x]$ имел кратный корень, необходимо и достаточно, чтобы он имел общий корень со своей производной $f'(x)$. По теореме 1.1, для этого необходимо и достаточно, чтобы $\mathcal{R}(f, f') = 0$. Соответствующий определитель

$$D = \begin{vmatrix}
a_0 & a_1 & \ldots & a_{n-2} & a_{n-1} & a_n & & & \\
 & a_0 & \ldots & a_{n-3} & a_{n-2} & a_{n-1} & a_n & \mathbb{O} & \\
 & & \ddots & & & & \ddots & \ddots & \\
 & & & a_0 & a_1 & \ldots & & a_{n-1} & a_n \\
 & \mathbb{O} & & & na_0 & & \ldots & 2a_{n-2} & a_{n-1} \\
 & & & na_0 & (n-1)a_1 & & \ldots & a_{n-1} & \\
 & & \iddots & \iddots & & & \iddots & & \\
 & na_0 & (n-1)a_1 & \ldots & & a_{n-1} & & \mathbb{O} & \\
na_0 & (n-1)a_1 & \ldots & & a_{n-1} & & & &
\end{vmatrix}$$

будет делиться на a_0 (общий множитель элементов первого столбца).

Определение. Выражение D/a_0 называется **дискриминантом** полинома $f(x)$ и обозначается $\mathcal{D}(f)$:

$$\mathcal{D}(f) \stackrel{\text{def}}{=} D/a_0 = (-1)^{n(n-1)/2}\mathcal{R}(f, f')/a_0 \ . \tag{2.1}$$

По построению, дискриминант является полиномом относительно коэффициентов $a_0, \ldots, a_n$:

$$\mathcal{D}(a_0x^n + \ldots + a_n) \in \mathbb{Z}[a_0, \ldots, a_n] \ ;$$

степень этого полинома равна $2n - 2$, и в своем разложении по степеням $a_0, \ldots, a_n$ он будет содержать слагаемое $(-1)^{n(n-1)/2}n^n a_0^{n-1}a_n^{n-1}$.

Пример 2.1. *Для квадратного трехчлена*

$$\mathcal{D}(a_0x^2 + a_1x + a_2) = \frac{1}{a_0}\begin{vmatrix} a_0 & a_1 & a_2 \\ 0 & 2a_0 & a_1 \\ 2a_0 & a_1 & 0 \end{vmatrix} = a_1^2 - 4\,a_0a_2 \ .$$

Упражнение 2.1. *Доказать, что*

а) $\mathcal{D}(x^3 + p\,x + q) = -108\left(\dfrac{q^2}{4} + \dfrac{p^3}{27}\right)$;

б) $\mathcal{D}(a_0x^3 + a_1x^2 + a_2x + a_3) = a_1^2a_2^2 - 4a_1^3a_3 - 4\,a_0a_2^3 + 18\,a_0a_1a_2a_3 - 27\,a_0^2a_3^2$;

в) $\mathcal{D}(x^4 + p\,x + q) = 6912\left(\dfrac{q^3}{27} - \dfrac{p^4}{256}\right)$.

Следующий результат является очевидным следствием теоремы 1.1.

Теорема 2.1. *Полином $f(x)$ имеет кратный корень тогда и только тогда, когда $\mathcal{D}(f) = 0$.*

Теорема 2.2. *Имеет место равенство*

$$\mathcal{D}(f) = a_0^{2n-2} \prod_{1 \le j < k \le n} (\lambda_k - \lambda_j)^2 \ . \tag{2.2}$$

Здесь $\lambda_1, \ldots, \lambda_n$ — корни $f(x)$.

Доказательство . Воспользуемся равенством (1.8) в применении к случаю $g(x) \equiv f'(x)$:

$$\mathcal{R}(f, f') = a_0^{n-1} \prod_{j=1}^{n} f'(\lambda_j) =$$

$$= a_0^{n-1} \prod_{j=1}^{n} [a_0(\lambda_j - \lambda_1)(\lambda_j - \lambda_2) \ldots (\lambda_j - \lambda_{j-1})(\lambda_j - \lambda_{j+1}) \ldots (\lambda_j - \lambda_n)] \ .$$

Последнее произведение содержит $n(n-1)$ сомножителей, причем наряду с $(\lambda_j - \lambda_k)$ включает и $(\lambda_k - \lambda_j)$. Поменяем у половины сомножителей знаки:

$$\mathcal{R}(f, f') = (-1)^{n(n-1)/2} a_0^{2n-1} \prod_{0 \le j < k \le n} (\lambda_k - \lambda_j)^2 \ .$$

Из (2.1) тогда следует (2.2). □

Таким образом, величина $\mathcal{D}(f)$ характеризует расстояние между корнями полинома $f(x)$.

Теорема 2.3. *Справедлива оценка:*

$$\frac{\sqrt{|\mathcal{D}(f)|}}{(2\rho)^{n(n-1)/2-1}|a_0|^{n-1}} \le \min_{\substack{j,k \in \{1,\ldots,n\} \\ j \ne k}} |\lambda_j - \lambda_k| \le \frac{|\mathcal{D}(f)|^{1/[n(n-1)]}}{|a_0|^{2/n}} \ .$$

Здесь $\rho \stackrel{\text{def}}{=} \max\limits_{j \in \{1,\ldots,n\}} |a_j|$.

Упражнение 2.2. *Доказать, что для вещественности всех корней полинома $f(x) \in \mathbb{R}[x]$ необходимо выполнение условия $\mathcal{D}(f) \ge 0$.*

Упражнение 2.3. *Доказать следующие формулы:*
а) $\mathcal{D}(f \cdot g) = \mathcal{D}(f)\mathcal{D}(g)[\mathcal{R}(f, g)]^2$;
б) $\mathcal{D}(f(x)(x - a)) = \mathcal{D}(f(x))[f(a)]^2$;
в) $\mathcal{D}(f(g(x))) = \mathcal{D}(f(x))^m \prod\limits_{j=1}^{n} \mathcal{D}(g(x) - \lambda_j)$; здесь $a_0 = b_0 = 1$.

Упражнение 2.4. *Пусть $f^* \stackrel{\text{def}}{=} x^n f(1/x) = a_n x^n + \ldots + a_0$ и $a_0 \ne 0$, $a_n \ne 0$. Доказать, что $\mathcal{D}(f) = \mathcal{D}(f^*)$.*

3 Субрезультанты

Рассмотрим снова пример 1.1. Пусть $\mathcal{R}(f,g)=0$. Тогда, по теореме 1.1, существует общий корень полиномов $f(x)$ и $g(x)$. Выразим его через коэффициенты полиномов.

Неизвестное значение $x=c$ этого корня должно удовлетворять равенствам (1.1). Отбросим первое и последнее из них:

$$\begin{aligned}
a_0c^6+a_1c^5+a_2c^4+a_3c^3+a_4c^2+\ a_5c &= 0\ ,\\
a_0c^5+a_1c^4+a_2c^3+a_3c^2+a_4c+a_5 &= 0\ ,\\
b_0c^3+b_1c^2+b_2c+b_3 &= 0\ ,\\
b_0c^4+b_1c^3+b_2c^2+\ b_3c &= 0\ ,\\
b_0c^5+b_1c^4+b_2c^3+\ b_3c^2 &= 0\ ,\\
b_0c^6+b_1c^5+b_2c^4+\ b_3c^3 &= 0\ .
\end{aligned} \tag{3.1}$$

Перепишем в матричном виде

$$\underbrace{\begin{pmatrix}
a_0 & a_1 & a_2 & a_3 & a_4 & a_5\\
0 & a_0 & a_1 & a_2 & a_3 & a_4\\
0 & 0 & 0 & b_0 & b_1 & b_2\\
0 & 0 & b_0 & b_1 & b_2 & b_3\\
0 & b_0 & b_1 & b_2 & b_3 & 0\\
b_0 & b_1 & b_2 & b_3 & 0 & 0
\end{pmatrix}}_{M_1}
\begin{pmatrix} c^6\\ c^5\\ c^4\\ c^3\\ c^2\\ c \end{pmatrix}
=
\begin{pmatrix} 0\\ -a_5\\ -b_3\\ 0\\ 0\\ 0 \end{pmatrix}\ .$$

Пусть $\det M_1\neq 0$. Тогда, по теореме Крамера, существует единственное решение системы (3.1), и корень c представи́м в виде

$$c=-\frac{\overbrace{\begin{vmatrix}
a_0 & a_1 & a_2 & a_3 & a_4 & \\
 & a_0 & a_1 & a_2 & a_3 & a_5\\
 & & & b_0 & b_1 & b_3\\
 & & b_0 & b_1 & b_2 & \\
 & b_0 & b_1 & b_2 & b_3 & \\
b_0 & b_1 & b_2 & b_3 & &
\end{vmatrix}}^{\det M_1^{(1)}}}{\det M_1}\ .$$

Определение. Определитель матрицы M_1, получаемой из матрицы (1.3) вычеркиванием первого и последнего столбцов, первой и последней строк, называется **первым субрезультантом** полиномов f и g; будем обозначать его $\mathcal{R}^{(1)}(f,g)$.

Теорема 3.1. *Для того чтобы $f(x)$ и $g(x)$ имели только один общий корень, необходимо и достаточно, чтобы*

$$\mathcal{R}(f,g)=0,\ \mathcal{R}^{(1)}(f,g)\neq 0\ .$$

Упражнение 3.1. *Пусть* $\mathcal{R}(f,g) = 0$ *и* $x = c$ *— общий корень* $f(x)$ *и* $g(x)$. *Обозначим* $f_1(x) = f(x)/(x-c)$, $g_1(x) = g(x)/(x-c)$. *Доказать равенство*

$$\mathcal{R}^{(1)}(f,g) = \mathcal{R}(f_1, g_1) \ . \tag{3.2}$$

Подсказка. Для случая

$$f(x) = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5,\ g(x) = b_0x^3 + b_1x^2 + b_2x + b_3$$

рассуждения будут следующими. Поскольку $f(x) \equiv (x-c)f_1(x)$, $g(x) \equiv \equiv (x-c)g_1(x)$, то коэффициенты полиномов

$$f_1(x) = a'_0x^4 + a'_1x^3 + a'_2x^2 + a'_3x + a'_4,\ g_1(x) = b'_0x^2 + b'_1x + b'_2$$

можно найти из равенств

$$a_0 = a'_0, a_j = a'_j - a'_{j-1}c,\ (j = 1,2,3,4)\ , a_5 = -a'_4c\ ,$$

$$b_0 = b'_0, b_j = b'_j - b'_{j-1}c,\ (j = 1,2)\ , b_3 = -b'_2c\ .$$

Если из каждого столбца результанта

$$\mathcal{R}(f_1,g_1) = \begin{vmatrix} a'_0 & a'_1 & a'_2 & a'_3 & a'_4 & 0 \\ 0 & a'_0 & a'_1 & a'_2 & a'_3 & a'_4 \\ 0 & 0 & 0 & b'_0 & b'_1 & b'_2 \\ 0 & 0 & b'_0 & b'_1 & b'_2 & 0 \\ 0 & b'_0 & b'_1 & b'_2 & 0 & 0 \\ b'_0 & b'_1 & b'_2 & 0 & 0 & 0 \end{vmatrix}$$

(кроме первого) вычесть предшествующий, домноженный на c, то получим выражение для $\mathcal{R}^{(1)}(f,g)$.

Упражнение 3.2. *Доказать теорему* 3.1.

Следствие 1. *При выполнении условия теоремы* 3.1 *единственный общий корень рационально выражается через коэффициенты полиномов* $f(x)$ *и* $g(x)$*:*

$$c = -\frac{\det M_1^{(1)}}{\mathcal{R}^{(1)}(f,g)}\ . \tag{3.3}$$

Здесь матрица $M_1^{(1)}$ *получается из* $M^{(1)}$ *заменой последнего ее столбца на*

$$[\underbrace{0,\ldots,0}_{m-2}, a_n, b_m, \underbrace{0,\ldots,0}_{n-2}]^t\ .$$

Пример 3.1. *Найти общий корень полиномов*

$$f(x) = x^2 - 4\,x - 5 \quad и \quad g(x) = x^2 - 7\,x + 10\ .$$

Решение. Общий корень $f(x)$ и $g(x)$ существует, поскольку

$$\mathcal{R}(f,g)=\begin{vmatrix} 1 & -4 & -5 & 0\\ 0 & 1 & -4 & -5\\ 0 & 1 & -7 & 10\\ 1 & -7 & 10 & 0 \end{vmatrix}=0\ .$$

Имеем далее:

$$\mathcal{R}^{(1)}(f,g)=\begin{vmatrix} 1 & -4\\ 1 & -7 \end{vmatrix}=-3\neq 0,\ \det M_1^{(1)}=\begin{vmatrix} 1 & -5\\ 1 & 10 \end{vmatrix}=15\ .$$

По формуле (3.3), получаем: $c=-\dfrac{15}{-3}=5.$ $\triangle$

Пусть теперь $\mathcal{R}(f,g)=0, \mathcal{R}^{(1)}(f,g)=0$. Тогда у полиномов $f(x)$ и $g(x)$ имеется, по крайней мере, два общих корня c_1 и c_2.

Оба эти корня должны удовлетворять уравнениям (3.1). Рассмотрим подсистему (субсистему) системы (3.1), вычеркнув первое и последнее уравнения и считая c равным c_1 или c_2 :

$$\begin{cases} a_0c^5+a_1c^4+a_2c^3+a_3c^2+a_4c+a_5 &= 0\ ,\\ b_0c^3+b_1c^2+b_2c+b_3 &= 0\ ,\\ b_0c^4+b_1c^3+b_2c^2+b_3c &= 0\ ,\\ b_0c^5+b_1c^4+b_2c^3+b_3c^2 &= 0\ . \end{cases}$$

Запишем эти уравнения в матричной форме:

$$\underbrace{\begin{pmatrix} a_0 & a_1 & a_2 & a_3\\ 0 & 0 & b_0 & b_1\\ 0 & b_0 & b_1 & b_2\\ b_0 & b_1 & b_2 & b_3 \end{pmatrix}}_{M_2}\begin{pmatrix} c^5\\ c^4\\ c^3\\ c^2 \end{pmatrix}=\begin{pmatrix} -a_4c-a_5\\ -b_2c-b_3\\ -b_3c\\ 0 \end{pmatrix}\ .$$

Пусть $\det M_2\neq 0$. Тогда, по теореме Крамера, существует единственное решение этой системы, и c^2 должно удовлетворять уравнению

$$c^2=\frac{\begin{vmatrix} a_0 & a_1 & a_2 & -a_4c-a_5\\ & & b_0 & -b_2c-b_3\\ & b_0 & b_1 & -b_3c\\ b_0 & b_1 & b_2 & \end{vmatrix}}{\det M_2}\ ,$$

откуда получаем следующее квадратное уравнение, которому должны удовлетворять c_1 и c_2:

$$\begin{vmatrix} a_0 & a_1 & a_2 & a_3\\ 0 & 0 & b_0 & b_1\\ 0 & b_0 & b_1 & b_2\\ b_0 & b_1 & b_2 & b_3 \end{vmatrix}c^2+\begin{vmatrix} a_0 & a_1 & a_2 & a_4\\ 0 & 0 & b_0 & b_2\\ 0 & b_0 & b_1 & b_3\\ b_0 & b_1 & b_2 & 0 \end{vmatrix}c+\begin{vmatrix} a_0 & a_1 & a_2 & a_5\\ 0 & 0 & b_0 & b_3\\ 0 & b_0 & b_1 & 0\\ b_0 & b_1 & b_2 & 0 \end{vmatrix}=0\ . \qquad (3.4)$$

Определение. Определитель матрицы M_2, получаемой из матрицы M вычеркиванием двух первых и двух последних столбцов, двух первых и двух последних строк, называется **вторым субрезультантом** полиномов f и g и обозначается $\mathcal{R}^{(2)}(f,g)$.

Теорема 3.2. *Для того чтобы $f(x)$ и $g(x)$ имели в точности два общих корня, необходимо и достаточно, чтобы выполнялись условия*

$$\mathcal{R}(f,g) = \mathcal{R}^{(1)}(f,g) = 0,\ \mathcal{R}^{(2)}(f,g) \neq 0\ .$$

Упражнение 3.3. *Доказать теорему, используя результат упражнения* 3.1.

Следствие 1. *При условии теоремы* 3.2 *оба корня должны удовлетворять квадратному уравнению*

$$x^2\mathcal{R}^{(2)}(f,g) + x\det M_2^{(1)} + \det M_2^{(2)} = 0\ . \tag{3.5}$$

Здесь матрицы $M_2^{(1)}$ и $M_2^{(2)}$ получаются из M_2 заменой последнего ее столбца на

$$[\underbrace{0,\ldots,0}_{m-4}, a_n, a_{n-1}, b_{m-1}, b_m, \underbrace{0,\ldots,0}_{n-4}]^t \quad и \quad [\underbrace{0,\ldots,0}_{m-3}, a_n, b_m, \underbrace{0,\ldots,0}_{n-3}]^t$$

соответственно. Полином, стоящий в левой части уравнения (3.5)*, является* НОД (f,g).

Определение. Определитель матрицы M_k, получаемой из матрицы M вычеркиванием k первых и k последних столбцов, k первых и k последних строк, называется **k-м субрезультантом** полиномов f и g и обозначается $\mathcal{R}^{(k)}(f,g)$. Для однообразия будем считать нулевым субрезультантом определитель матрицы M: $\mathcal{R}^{(0)}(f,g) \stackrel{\text{def}}{=} \det M = (-1)^{n(n-1)/2}\mathcal{R}(f,g)$.

Пример 3.2.

$$\mathcal{R}^{(3)}(a_0x^5+a_1x^4+a_2x^3+a_3x^2+a_4x+a_5,\ b_0x^3+b_1x^2+b_2x+b_3) =$$

$$= \begin{vmatrix} 0 & b_0 \\ b_0 & b_1 \end{vmatrix} = -\,b_0^2\ .$$

Упражнение 3.4. *Доказать, что при $n > m$*

$$\mathcal{R}^{(k)}(f,g) = (-1)^{(m+n-2k)(m+n-2k-1)/2} b_0^{m+n-2k}$$

для $k = m,\ldots,\lfloor (m+n)/2 \rfloor$.

Обобщая результаты теорем 3.1 и 3.2, приходим к следующему результату.

Теорема 3.3. а) *Для существования d общих корней у $f(x)$ и $g(x)$ (т.е. для того, чтобы $\deg(\mathsf{НОД}\,(f,g)) = d$), необходимо и достаточно, чтобы*

$$\mathcal{R}(f,g) = \mathcal{R}^{(1)}(f,g) = \ldots = \mathcal{R}^{(d-1)}(f,g) = 0,\ \mathcal{R}^{(d)}(f,g) \neq 0\ .$$

б) *В этом случае* $\mathsf{НОД}\,(f,g)$ *можно представить в виде*

$$x^d \mathcal{R}^{(d)}(f,g) + x^{d-1} \det M_d^{(1)} + \ldots + \det M_d^{(d)}\ .$$

Здесь $M_d^{(j)}$ — матрица, получаемая из M_d заменой последнего столбца на столбец

$$[a_{m+n-2d+j-1}, a_{m+n-2d+j-2}, \ldots, a_{n-d+j}, b_{m-d+j}, \\ b_{m-d+j+1}, \ldots, b_{m+n-2d+j-1}]^t$$

(здесь полагаем $a_K = 0$ при $K > n$ и $b_L = 0$ при $L > m$).

в) *Полиномы $v(x)$ и $u(x)$ из $\mathbb{A}[x]$, дающие линейное представление* $\mathsf{НОД}\,(f,g)$ *(см. формулу* (1.13)*), получаются из $\mathcal{R}^{(d)}$ заменой в нем последнего столбца на*

$$\left[x^{m-d-1}, x^{m-d-2}, \ldots, x, 1, 0, 0, \ldots, 0\right]^t \ \text{ и } \ \left[0, 0, \ldots, 0, 0, 1, x, \ldots, x^{n-d-1}\right]^t$$

соответственно. Эти полиномы будут единственными при ограничениях на степени:

$$\deg v \leq m-d-1,\ \deg u \leq n-d-1\ .$$

Упражнение 3.5. *Доказать пункты а) и в) теоремы* 3.3.

Подсказка. Для пункта в) в случае

$$f(x) = a_0x^5 + a_1x^4 + a_2x^3 + a_3x^2 + a_4x + a_5,\ g(x) = b_0x^3 + b_1x^2 + b_2x + b_3$$

и $d = 2$ рассуждения будут следующими. Домножим $\mathcal{R}^{(2)}$ на x^2:

$$x^2\mathcal{R}^{(2)} = x^2 \begin{vmatrix} a_0 & a_1 & a_2 & a_3 \\ 0 & 0 & b_0 & b_1 \\ 0 & b_0 & b_1 & b_2 \\ b_0 & b_1 & b_2 & b_3 \end{vmatrix} = \begin{vmatrix} a_0 & a_1 & a_2 & a_3x^2 \\ 0 & 0 & b_0 & b_1x^2 \\ 0 & b_0 & b_1 & b_2x^2 \\ b_0 & b_1 & b_2 & b_3x^2 \end{vmatrix} =$$

теперь к последнему столбцу прибавим первый, умноженный на x^5, второй, умноженный на x^4, и третий, умноженный на x^3:

$$= \begin{vmatrix} a_0 & a_1 & a_2 & a_0x^5+a_1x^4+a_2x^3+a_3x^2 \\ 0 & 0 & b_0 & b_0x^3+b_1x^2 \\ 0 & b_0 & b_1 & b_0x^4+b_1x^3+b_2x^2 \\ b_0 & b_1 & b_2 & b_0x^5+b_1x^4+b_2x^3+b_3x^2 \end{vmatrix} = \begin{vmatrix} a_0 & a_1 & a_2 & f(x)-(a_4x+a_5) \\ 0 & 0 & b_0 & g(x)-(b_2x+b_3) \\ 0 & b_0 & b_1 & xg(x)-b_3x \\ b_0 & b_1 & b_2 & x^2g(x) \end{vmatrix} =$$

последний столбец представляем в виде линейной комбинации остальных:

$$= f(x)\begin{vmatrix} a_0 & a_1 & a_2 & 1 \\ 0 & 0 & b_0 & 0 \\ 0 & b_0 & b_1 & 0 \\ b_0 & b_1 & b_2 & 0 \end{vmatrix} + g(x)\begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & 0 & b_0 & 1 \\ 0 & b_0 & b_1 & x \\ b_0 & b_1 & b_2 & x^2 \end{vmatrix} - \begin{vmatrix} a_0 & a_1 & a_2 & a_4x+a_5 \\ 0 & 0 & b_0 & b_2x+b_3 \\ 0 & b_0 & b_1 & b_3x \\ b_0 & b_1 & b_2 & 0 \end{vmatrix} .$$

Если перенести последний определитель в левую часть (т.е. к $x^2\mathcal{R}^{(2)}$), то слева получим выражение для $\mathsf{НОД}\,(f,g)$ (см. формулу (3.4)); в правой же части коэффициенты при $f(x)$ и $g(x)$ будут равны соответственно полиномам $v(x)$ и $u(x)$ из тождества (1.13).

Упражнение 3.6. *Найти* $\mathsf{НОД}\,(f,g)$ *для*
а) $f(x)=x^4-x^3-x^2+1,\ g(x)=x^4-2\,x^3+2\,x^2-2\,x+1$;
б) $f(x)=x^3+5\,x^2+5\,x+4,\ g(x)=x^3-x^2-x-2$;
в) $f(x)=x^3-4\,x^2+4\,x-3,\ g(x)=3\,x^4-2\,x^3+4\,x^2-x+2$;
г) $f(x)=2\,x^3+5\,x^2-6\,x-9,\ g(x)=3\,x^3+7\,x^2-11\,x-5$.

Упражнение 3.7. *При каком условии полиномы*

$$a_0x^4+a_1x^3+a_2x^2+a_3x+a_4 \ \text{и}\ b_0x^4+b_1x^3+b_2x^2+b_3x+b_4$$

имеют общий делитель второй степени? Найти его вид.

Упражнение 3.8. *Известно, что кубические уравнения*

$$x^3+a_1x^2+a_2x+a_3=0 \ \text{и}\ x^3+b_1x^2+b_2x+b_3=0$$

имеют два общих корня. Найти квадратное уравнение, которому эти корни удовлетворяют, и определить третий корень каждого из кубических уравнений.

Рассмотрим теперь частный случай $g(x)\equiv f'(x)$. Теорема 3.3 позволяет установить наличие d общих корней у полинома и его производной, т.е. наличие d кратных корней у $f(x)$ — с учетом их кратностей. Двойные корни полинома $f(x)$ оказываются простыми корнями $D(x)=\mathsf{НОД}\,(f,f')$, корни же кратностей больших двух становятся кратными корнями $D(x)$, но кратность их понижается на единицу, и для их поиска можно снова применить теорему 3.3 — теперь уже для поиска $\mathsf{НОД}\,(D,D')$.

Упражнение 3.9. *Имеет ли полином кратные корни? Если да, найти их кратности*
а) $f(x)=x^4-x^3-104x^2+514x-720$;
б) $f(x)=x^4-x^3-30x^2-76x-56$;
в) $f(x)=x^4+x^3-2x^2+4x-24$;
г) $f(x)=x^5+x^4-2x^3-2x^2+x+1$;
д) $f(x)=2x^6+6x^5+6x^4+x^3-3x^2-3x-1$.

Упражнение 3.10. *При каких значениях параметров полиномы имеют*
а) двойной корень: $px^3 + p^2x^2 + x + p$; $x^5 + px^4 + q$;
б) тройной корень: $x^4 + px^3 + 2x + q$;
в) только два различных корня: $x^4 + 4x^3 - 2x^2 + px + q$?

4 Метод Кронекера

Как уже отмечалось в §1.2, вычисление результанта посредством его представления в форме определителя матрицы Сильвестра (1.3) не эффективно — особенно при больших степенях полиномов $f(x)$ и $g(x)$. Однако, использование простоты структуры матрицы (1.3) (в частности, ее **разреженность** — т.е. наличие большого числа нулевых элементов) позволяет уменьшить порядок определителя с $\deg f + \deg g$ до $\max(\deg f, \deg g)$. В настоящем и следующем параграфах мы обсудим детерминантные формы представления результанта, альтернативные форме Сильвестра.

Для полиномов из $\mathbb{A}[x]$:

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \text{ и } g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m$$

($a_0 \neq 0, b_0 \neq 0$) построим сначала формальное разложение дроби $g(x)/f(x)$ в ряд по отрицательным степеням x. Для этого удобно предварительно построить разложение дроби $1/f(x)$:

$$\frac{1}{f(x)} = \frac{d_{n-1}}{x^n} + \frac{d_n}{x^{n+1}} + \ldots + \frac{d_k}{x^{k+1}} + \ldots \tag{4.1}$$

Домножив обе части разложения (4.1) на $f(x)$ и приравняв затем коэффициенты при одинаковых степенях x, получим рекуррентные формулы для определения коффициентов d_k:

$$d_{n-1}{=}1/a_0,\ d_n = -(d_{n-1}a_1)/a_0,\ \ldots$$
$$d_k{=}\begin{cases} -(d_{k-1}a_1 + d_{k-2}a_2 + \ldots + d_{n-1}a_{k-n+1})/a_0, & \text{если } k \leq n \ ; \\ -(d_{k-1}a_1 + d_{k-2}a_2 + \ldots + d_{k-n}a_n)/a_0, & \text{если } k > n \ . \end{cases}$$

Если домножить теперь разложение (4.1) на полином $g(x)$, то получим требуемое разложение

$$\frac{g(x)}{f(x)} = \mathfrak{L}(x) + \frac{c_0}{x} + \frac{c_1}{x^2} + \ldots + \frac{c_k}{x^{k+1}} + \ldots \ , \tag{4.2}$$

где полином

$$\mathfrak{L}(x) \stackrel{\text{def}}{=} \begin{cases} c_{n-m-1}x^{m-n} + c_{n-m}x^{m-n-1} + \ldots + c_{-1}, & \text{если } m \geq n \ ; \\ 0, & \text{если } m < n \end{cases} \tag{4.3}$$

есть частное от деления $g(x)$ на $f(x)$. Коэффициенты c_k определяются через коэффициенты полинома $g(x)$ и разложения (4.1). Так, при $m \geq n$ получаем:

$$c_{n-m-1} = b_0 d_{n-1},\ c_{n-m} = b_0 d_n + b_1 d_{n-1},\ \ldots$$

$$c_k = \begin{cases} d_{k+m}b_0 + d_{k+m-1}b_1 + \ldots + d_{n-1}b_{k+m-n+1}, & \text{если } k < n \ ; \\ d_{k+m}b_0 + d_{k+m-1}b_1 + \ldots + d_k b_m, & \text{если } k \geq n \ . \end{cases} \tag{4.4}$$

В случае $m < n$ имеем $c_k = 0$ для $k < n - m - 1$, а при $k \geq n - m - 1$ справедливы формулы (4.4).

Упражнение 4.1. *Найти формулы, непосредственно выражающие коэффициенты разложения* (4.2) *через коэффициенты полиномов* $f(x)$ *и* $g(x)$.

Подсказка. Домножить обе части разложения (4.2) на $f(x)$ и сравнить коэффициенты при одинаковых степенях x. Так, для $n = 5, m = 3$ получаем

$$0 = c_0 a_0,\ b_0 = c_0 a_1 + c_1 a_0,\ b_1 = c_0 a_2 + c_1 a_1 + c_2 a_0 \ ,$$
$$b_2 = c_0 a_3 + c_1 a_2 + c_2 a_1 + c_3 a_0,\ b_3 = c_0 a_4 + c_1 a_3 + \ldots + c_4 a_0 \ ,$$

$$0 = c_{k-5}a_5 + c_{k-4}a_4 + \ldots + c_k a_0 \qquad (k \geq 5) \ . \tag{4.5}$$

Теорема 4.1. *Доказать, что при условии различности всех корней* $\lambda_1, \ldots, \lambda_n$ *полинома* $f(x)$, *имеет место равенство*

$$c_k = \sum_{j=1}^{n} \frac{\lambda_j^k g(\lambda_j)}{f'(\lambda_j)} \quad (k \geq 0) \ . \tag{4.6}$$

Доказательство . Без ограничения общности можно считать, что $m < n$. Воспользуемся **формулой Лагранжа**:

$$\frac{g(x)}{f(x)} = \sum_{j=1}^{n} \frac{g(\lambda_j)}{f'(\lambda_j)(x - \lambda_j)} \ . \tag{4.7}$$

Заменив здесь каждую дробь $1/(x - \lambda_j)$ ее разложением по степеням $1/x$

$$\frac{1}{x - \lambda_j} = \frac{1}{x}\left(1 + \frac{\lambda_j}{x} + \frac{\lambda_j^2}{x^2} + \ldots\right)$$

и собрав коэффициенты при одинаковых степенях x, получим требуемое выражение для коэффициентов c_k. □

Вычислим величины $c_0, \ldots, c_{2n-2}$ и составим ганкелеву матрицу

$$C = [c_{j+k}]_{j,k=0}^{n-1} = \begin{pmatrix} c_0 & c_1 & c_2 & \ldots & c_{n-1} \\ c_1 & c_2 & c_3 & \ldots & c_n \\ c_2 & c_3 & c_4 & \ldots & c_{n+1} \\ \ldots & & & & \ldots \\ c_{n-1} & c_n & c_{n+1} & \ldots & c_{2n-2} \end{pmatrix} . \qquad (4.8)$$

Обозначим через C_j ее j-й главный минор.

Теорема 4.2 (Кронекер). а) *Справедливо равенство*

$$C_n = \det C = \mathcal{R}(f,g)/a_0^{n+m} .$$

б) *Степень* $\mathsf{НОД}\,(f,g)$ *равна* d *тогда и только тогда, когда*

$$C_n = C_{n-1} = \ldots = C_{n-d+1} = 0,\ C_{n-d} \neq 0 .$$

В этом случае $\mathsf{НОД}\,(f,g)$ *равен определителю, получающемуся из* C_{n-d} *заменой последнего столбца на столбец*

$$\left[\sum_{j=n-d}^{n} c_{j-1} f_j(x), \sum_{j=n-d}^{n} c_j f_j(x), \ldots, \sum_{j=n-d}^{n} c_{j+n-d-2} f_j(x) \right]^t .$$

Здесь $f_k(x) \stackrel{\text{def}}{=} a_0 x^{n-k} + a_1 x^{n-k-1} + \ldots + a_{n-k}$, *а старший коэффициент* $\mathsf{НОД}\,(f,g)$ *равен* $a_0 C_{n-d}$.

в) *Если* $n > m$, *то полиномы* $v(x)$ *и* $u(x)$, *дающие линейное представление* $\mathsf{НОД}\,(f,g)$ *(см. формулу* (1.13)*), получаются из* C_{n-d} *заменой в нем последнего столбца на*

$$\left[0, -P_0(x), \ldots, -P_{n-d-2}(x)\right]^t \quad и \quad \left[1, x, \ldots, x^{n-d-1}\right]^t$$

соответственно. Здесь $P_k(x) \stackrel{\text{def}}{=} c_0 x^k + \ldots + c_k$.

Пример 4.1. *Доказать справедливость следующего соотношения, связывающего* C_{n-k} *и* k*-й субрезультант полиномов* f *и* $g\,(k \leq n)$*:*

$$a_0^{n+m-2k} C_{n-k} = \mathcal{R}^{(k)} . \qquad (4.9)$$

Решение. Докажем (4.9) для случая $n = 5, m = 3, k = 2$. Составим следующее произведение:

$$\begin{pmatrix} 1 & & & & \\ 0 & 1 & & & \\ 0 & 0 & c_0 & c_1 & c_2 \\ 0 & c_0 & c_1 & c_2 & c_3 \\ c_0 & c_1 & c_2 & c_3 & c_4 \end{pmatrix} \cdot \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ & a_0 & a_1 & a_2 & a_3 \\ & & a_0 & a_1 & a_2 \\ & & & a_0 & a_1 \\ & & & & a_0 \end{pmatrix} .$$

Определитель этого произведения равен произведению определителей, т.е. $C_3 a_0^5$. С другой стороны, выполнив умножение с учетом формул (4.5), получаем матрицу

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 \\ & a_0 & a_1 & a_2 & a_3 \\ & & & b_0 & b_1 \\ & & b_0 & b_1 & b_2 \\ & b_0 & b_1 & b_2 & b_3 \end{pmatrix} ,$$

определитель которой равен $a_0 \mathcal{R}^{(2)}$. $\triangle$

Упражнение 4.2. *Доказать справедливость утверждений б) и в) теоремы Кронекера, пользуясь теоремой* 3.3.

Подсказка. Идею доказательства части в) поясним для частного случая $d = 0$, т.е. при $\mathsf{НОД}\,(f, g) \equiv const$. В соответствии с утверждением теоремы, ищем коэффициенты полиномов

$$u(x) \stackrel{\text{def}}{=} u_0 x^{n-1} + \ldots + u_{n-1} \text{ и } v(x) \stackrel{\text{def}}{=} v_0 x^{n-1} + \ldots + v_{n-2} \ ,$$

удовлетворяющих тождеству $v(x)\, f(x) + u(x)\, g(x) \equiv a_0 C_n$. Разделим это тождество на $f(x)$ и разложим обе части в ряды с использованием разложений (4.1) и (4.2):

$$v(x) + u(x) \left(\frac{c_0}{x} + \frac{c_1}{x^2} + \cdots \right) \equiv a_0 C_n \left(\frac{d_{n-1}}{x^n} + \frac{d_n}{x^{n+1}} + \cdots \right) \ .$$

Приравнивая коэффициенты при одинаковых степенях x, получим систему линейных уравнений относительно $u_{n-1}, \ldots, u_0$:

$$\begin{array}{lcl} x^{-1} & : & c_0 u_{n-1} \quad + c_1 u_{n-2} \quad + \ldots + c_{n-1} u_0 = 0 \ , \\ \ldots & & \ldots \qquad\qquad\qquad\qquad\qquad\quad \ldots \\ x^{-n+1} & : & c_{n-2} u_{n-1} + c_{n-1} u_{n-2} + \ldots + c_{2n-3} u_0 = 0 \ , \\ x^{-n} & : & c_{n-1} u_{n-1} + c_n u_{n-2} \quad + \ldots + c_{2n-2} u_0 = C_n \ . \end{array}$$

Решив эту систему по формулам Крамера, получим выражения для коэффициентов $u_0, \ldots, u_{n-1}$; они совпадают с указанными в теореме. Аналогично

$$\begin{array}{lcl} x^{n-2} & : & v_0 \quad + u_0 c_0 \qquad\qquad\qquad\quad = 0 \ , \\ x^{n-3} & : & v_1 \quad + u_0 c_1 \quad + u_1 c_0 \qquad\quad = 0 \ , \\ \ldots & & \ldots \\ 1 & : & v_{n-2} + u_0 c_{n-2} + u_1 c_{n-3} + \ldots + u_{n-2} c_0 = 0 \ . \end{array} \tag{4.10}$$

Используя полученные выше выражения для $u_0, \ldots, u_{n-1}$, можно выписать выражения $v_0, \ldots, v_{n-2}$ в виде определителей и показать затем тождественность получившихся детерминантных представлений тем, что указаны в

пункте в) теоремы. Однако для практических целей удобнее после нахождения $u_0, \ldots, u_{n-1}$ использовать формулы (4.10) напрямую. Заметим, что $v(x)$ равен частному от деления $u(x)g(x)$ на $f(x)$, взятому с противоположным знаком.

Замечание. Для $n \le m$ утверждение пункта в) теоремы обобщается следующим образом: полином $u(x)$ не изменяется, а к полиному $v(x)$ прибавляется $-\mathfrak{L}(x)u(x)$, где $\mathfrak{L}(x)$ – частное от деления $g(x)$ на $f(x)$, которое может быть найдено по формуле (4.3).

Пример 4.2. *Найти*

$$\mathsf{НОД}\,(2\,x^5 + x^4 - x^3 + 4\,x^2 + 2\,x - 2,\ 10\,x^3 + 3\,x^2 - 6\,x + 1)$$

и его линейное представление.

Решение. По формулам (4.4) вычисляем $c_0, \ldots, c_8$:

$$\{c_j\}_{j=0}^{8} = \{0, 5, -1, 0, -10, 2, 0, 20, -4\}\ .$$

Составляем матрицу (4.8)

$$C = \begin{pmatrix} 0 & 5 & -1 & 0 & -10 \\ 5 & -1 & 0 & -10 & 2 \\ -1 & 0 & -10 & 2 & 0 \\ 0 & -10 & 2 & 0 & 20 \\ -10 & 2 & 0 & 20 & -4 \end{pmatrix}$$

и вычисляем ее главные миноры (начиная с последнего): $C_5 = 0$, $C_4 = 0$, $C_3 = 251 \neq 0$. Согласно пункту б) теоремы, $\deg(\mathsf{НОД}\,) = 2$ и

$$\mathsf{НОД}\,(f,g) = \begin{vmatrix} 0 & 5 & -1\cdot f_3(x) + 0\cdot f_4(x) - 10\cdot f_5(x) \\ 5 & -1 & 0\cdot f_3(x) - 10\cdot f_4(x) + 2\cdot f_5(x) \\ -1 & 0 & -10\cdot f_3(x) + 2\cdot f_4(x) + 0\cdot f_5(x) \end{vmatrix}\ ,$$

где $f_3 = 2x^2 + x - 1$, $f_4 = 2x + 1$, $f_5 = 2$. Разложив определитель по последнему столбцу, получаем: $\mathsf{НОД}\,(f,g) = 251(2\,x^2 + x - 1)$. Для нахождения полиномов его линейного представления воспользуемся пунктом в) теоремы.

$$u(x) = \begin{vmatrix} 0 & 5 & 1 \\ 5 & -1 & x \\ -1 & 0 & x^2 \end{vmatrix} = -25\,x^2 - 5\,x - 1\ .$$

В соответствии с теоремой, $\deg(v(x)) = 0$, и $v(x) = 125$. △

Упражнение 4.3. *Найти* $\mathsf{НОД}\,(f,g)$ *и его линейное представление для*
а) $f(x)=9\,x^5+6\,x^4+3\,x^3+3\,x^2+2\,x+1,\ g(x)=3\,x^4+5\,x^3+6\,x^2+3\,x+1;$
б) $f(x)=x^6-5\,x^5+x^4-3\,x^3-5\,x^2+x+1,\ g(x)=x^5-5\,x^4+x^3-4\,x^2+1;$
в) $f(x) = x^4 - 1,\ g(x) = x^3 + \boldsymbol{i}\,;$
г) $f(x) = x^6 - x^5 + 4\,x^4 - 3\,x^3 + 4\,x^2 - x + 1,$
$g(x) = 2\,x^5 - 2\,x^4 + 5\,x^3 - 4\,x^2 + 4\,x - 1.$

Рассмотрим теперь частный случай $g(x) \equiv f'(x)$.
Коэффициенты разложения

$$\frac{f'(x)}{f(x)} = \frac{s_0}{x} + \frac{s_1}{x^2} + \ldots + \frac{s_k}{x^{k+1}} + \ldots \tag{4.11}$$

называются **суммами Ньютона** полинома $f(x)$.

Упражнение 4.4. *Доказать, что* $s_k = \sum_{j=1}^{n} \lambda_j^k$.

Упражнение 4.5. *Доказать справедливость следующих рекуррентных* **формул Ньютона***:*

$$s_0 = n,\ s_1 = -a_1/a_0,\ \ldots$$

$$s_k = \begin{cases} -(a_1 s_{k-1} + a_2 s_{k-2} + \ldots + a_{k-1} s_1 + a_k k)/a_0, & \text{если } k \le n \quad ; \\ -(a_1 s_{k-1} + a_2 s_{k-2} + \ldots + a_n s_{k-n})/a_0, & \text{если } k > n \quad . \end{cases} \tag{4.12}$$

Вычислим величины $s_0, \ldots, s_{2n-2}$ и составим из них — по аналогии с матрицей (4.8) — ганкелеву матрицу

$$S = [s_{j+k}]_{j,k=0}^{n-1} \quad . \tag{4.13}$$

Обозначим через S_j ее j-й главный минор.

Упражнение 4.6. *Доказать, что*

$$S_n = \mathcal{D}(f)/a_0^{2n-2} \quad .$$

Упражнение 4.7. *Доказать справедливость формулы*

$$S_p = \sum v(\lambda_{j_1}, \ldots, \lambda_{j_p})^2 \quad ,$$

где суммирование идет по всем возможным наборам индексов $(j_1, \ldots, j_p)$, $1 \le j_1 < j_2 < \ldots < j_p \le n$, *а*

$$v(\lambda_{j_1}, \ldots, \lambda_{j_p}) \stackrel{\text{def}}{=} \prod_{1 \le K < L \le p} (\lambda_{j_L} - \lambda_{j_K}) \quad . \tag{4.14}$$

Если, вдобавок, предположить, что все корни $f(x)$ *простые, то*

$$S_{n-1} = \frac{\mathcal{D}(f)}{a_0^{2n-4}} \sum_{j=1}^{n} \frac{1}{f'(\lambda_j)^2} \quad .$$

Подсказка. Показать, что $S_p = \det(V_p \cdot V_p^t)$, где

$$V_p = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \lambda_1 & \lambda_2 & \lambda_3 & \dots & \lambda_n \\ \lambda_1^2 & \lambda_2^2 & \lambda_3^2 & \dots & \lambda_n^2 \\ \dots & & & & \dots \\ \lambda_1^{p-1} & \lambda_2^{p-1} & \lambda_3^{p-1} & \dots & \lambda_n^{p-1} \end{pmatrix} ,$$

и воспользоваться теоремой Бине–Коши для вычисления определителя произведения матриц.

Упражнение 4.8. *Доказать, что для вещественности всех корней полинома $f(x) \in \mathbb{R}[x]$ необходимо, чтобы $S_1 \geq 0, \dots, S_n \geq 0$.*

Упражнение 4.9. *Доказать, что при условии отсутствия кратных корней у полинома $f(x)$ справедлива следующая формула:*

$$C_p = \sum v(\lambda_{j_1}, \dots, \lambda_{j_p})^2 \ \frac{g(\lambda_{j_1})}{f'(\lambda_{j_1})} \times \dots \times \frac{g(\lambda_{j_p})}{f'(\lambda_{j_p})} \ ,$$

где суммирование идет по всем возможным наборам индексов $(j_1, \dots, j_p)$, $1 \leq j_1 < j_2 < \dots < j_p \leq n$, а функция v определяется формулой (4.14). *Если, вдобавок, $\mathcal{R}(f, g) \neq 0$, то*

$$C_{n-1} = (-1)^{n(n-1)/2} \frac{\mathcal{R}(f, g)}{a_0^{m+n-2}} \sum_{j=1}^{n} \frac{1}{g(\lambda_j) f'(\lambda_j)} \ .$$

Подсказка. Воспользоваться формулой (4.6) и подсказкой к упражнению 4.7.

5 Метод Безу[3]

Рассмотрим снова полиномы из $\mathbb{A}[x]$:

$$f(x) = a_0 x^n + \dots + a_n \quad \text{и} \quad g(x) = b_0 x^m + \dots + b_m \quad (a_0 \neq 0, b_0 \neq 0) \ .$$

Найдем остатки от деления $x^k g(x)$ на $f(x)$ для $k = 0, \dots, n-1$:

$$g_k(x) \stackrel{\text{def}}{=} b_{k0} x^{n-1} + b_{k1} x^{n-2} + \dots + b_{k,n-1} \ .$$

Коэффициенты $g_k(x)$ могут быть выражены через коэффициенты $g_{k-1}(x)$ по формулам

$$b_{kj} = b_{k-1,j+1} - b_{k-1,0} a_{j+1}/a_0 \quad (j = 0, \dots, n-1) \ . \tag{5.1}$$

[3]Название метода условное, помимо Безу в его разработке принимали участие Эйлер, Коши, Эрмит и Кэли.

Составим матрицу из этих коэффициентов:

$$B = [b_{kj}]_{k,j=0}^{n-1} \tag{5.2}$$

и обозначим через B_j ее j-й главный минор.

Теорема 5.1. а) *Справедливо равенство*

$$B_n \stackrel{\text{def}}{=} \det B = (-1)^{n(n-1)/2}\mathcal{R}(f,g)/a_0^m \ . \tag{5.3}$$

б) *Степень* $\mathsf{НОД}\,(f,g)$ *равна* d *тогда и только тогда, когда*

$$B_n = B_{n-1} = \ldots = B_{n-d+1} = 0,\ B_{n-d} \neq 0 \ .$$

В этом случае $\mathsf{НОД}\,(f,g)$ *равен определителю, получающемуся из* B_{n-d} *заменой в нем последнего столбца на*

$$\left[\sum_{j=n-d-1}^{n-1} b_{0j}x^{n-j-1}\ ,\ \sum_{j=n-d-1}^{n-1} b_{1j}x^{n-j-1},\ \ldots,\ \sum_{j=n-d-1}^{n-1} b_{n-d-1,j}x^{n-j-1}\right]^t \ .$$

Старший коэффициент $\mathsf{НОД}\,(f,g)$ *равен* B_{n-d}.

в) *Если* $n > m$, *то полиномы* $v(x)$ *и* $u(x)$, *дающие линейное представление* $\mathsf{НОД}\,(f,g)$ *(см. формулу* (1.13)*), получаются из* B_{n-d} *заменой в нем последнего столбца на*

$$\left[0, -P_0(x), \ldots, -P_{n-d-2}(x)\right]^t \ \textit{и}\ \left[1, x, \ldots, x^{n-d-1}\right]^t$$

соответственно. Здесь $P_k(x) \stackrel{\text{def}}{=} (b_{00}x^k + b_{1,0}x^{k-1} + \ldots + b_{k,0})/a_0$.

Доказательство пунктов а) и б) следует из теоремы 3.3 и следующего соотношения, связывающего B_{n-k} и k-й субрезультант полиномов f и g:

$$a_0^{m-k}B_{n-k} = \mathcal{R}^{(k)} \quad (k \leq n) \ . \tag{5.4}$$

Установим справедливость соотношения (5.4) для случая $n = 5$, $m = 3$ и $k = 1$. Для элементов первых двух строк матрицы B имеем следующие формулы:

$$\begin{aligned} b_{00} = 0,\ b_{01} = b_{10} = b_0,\ b_{02} &= b_{11} = b_1,\ b_{03} = b_{12} = b_2 \ , \\ b_{04} = b_{13} &= b_3,\ b_{14} = 0 \ ; \end{aligned}$$

элементы остальных строк получаются по формулам (5.1). Тогда справедливо следующее матричное равенство:

$$\begin{pmatrix} 1 & & & & & \\ 0 & 1 & & & & \\ 0 & 0 & 1 & & & \\ 0 & 0 & 0 & 1 & & \\ 0 & -b_{10}/a_0 & 0 & 0 & 1 & \\ -b_{10}/a_0 & -b_{20}/a_0 & 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ & a_0 & a_1 & a_2 & a_3 & a_4 \\ & & b_0 & b_1 & b_2 & \\ & b_0 & b_1 & b_2 & b_3 & \\ b_0 & b_1 & b_2 & b_3 & & \end{pmatrix} =$$

$$= \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ & a_0 & a_1 & a_2 & a_3 & a_4 \\ & & b_{00} & b_{01} & b_{02} & b_{03} \\ & & b_{10} & b_{11} & b_{12} & b_{13} \\ & & b_{20} & b_{21} & b_{22} & b_{23} \\ & & b_{30} & b_{31} & b_{32} & b_{33} \end{pmatrix} .$$

Переходя в этом равенстве к определителям, получаем $\mathcal{R}^{(1)} = a_0^2 B_4$.

Для доказательства справедливости пункта в) теоремы следует воспользоваться результатом соответствующего пункта из теоремы 3.3. Сначала устанавливается справедливость равенств

$$x^k g(x) = P_{k-1}(x) f(x) + g_k(x), \quad (k = 0, \ldots, n-d-1) \text{ при } P_{-1}(x) \equiv 0 \ ,$$

т.е. показывается, что полином $P_{k-1}(x)$ является частным от деления $x^k g(x)$ на $f(x)$. Если теперь домножить k-е равенство на алгебраическое дополнение к элементу определителя B_{n-d}, стоящему в последнем столбце и k-й строке и просуммировать получившиеся произведения, то на основании свойства разложения определителя по столбцу и результата части б) теоремы получим требуемое утверждение. □

Пример 5.1. *Для полиномов*

$$f(x) = x^6 - 5x^5 + x^4 - 3x^3 - 5x^2 + x + 1 \ \textit{и} \ g(x) = x^5 - 5x^4 + x^3 - 4x^2 + 1$$

найти НОД (f, g) *и его линейное представление.*

Решение. Составим матрицу B:

$$B = \begin{pmatrix} 1 & -5 & 1 & -4 & 0 & 1 \\ 0 & 0 & -1 & 5 & 0 & -1 \\ 0 & -1 & 5 & 0 & -1 & 0 \\ -1 & 5 & 0 & -1 & 0 & 0 \\ 0 & 1 & -4 & -5 & 1 & 1 \\ 1 & -4 & -5 & 1 & 1 & 0 \end{pmatrix} .$$

Поскольку $B_6 = B_5 = B_4 = 0, B_3 = -1$, то НОД имеет степень 3. На основании пункта б) теоремы 5.1:

$$\text{НОД}\,(f, g) = \begin{vmatrix} 1 & -5 & 1 \cdot x^3 - 4 \cdot x^2 + 0 \cdot x + 1 \\ 0 & 0 & -1 \cdot x^3 + 5 \cdot x^2 + 0 \cdot x - 1 \\ 0 & -1 & 5 \cdot x^3 + 0 \cdot x^2 - 1 \cdot x + 0 \end{vmatrix} = -x^3 + 5x^2 - 1 \ .$$

Полиномы $u(x)$ и $v(x)$, дающие линейное представление НОД, находим по алгоритму пункта в) теоремы:

$$u(x) = \begin{vmatrix} 1 & -5 & 1 \\ 0 & 0 & x \\ 0 & -1 & x^2 \end{vmatrix} = x, \ v(x) = \begin{vmatrix} 1 & -5 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & -x+5 \end{vmatrix} = -1 \ .$$

△

Из этого примера видим, что степени полиномов $u(x)$ и $v(x)$ могут быть строго меньшими указанных для них границ. $\triangle$

Следующая модификация метода более распространена. Рассмотрим сначала случай $\deg f = \deg g = n$. Возьмем в качестве $g_k(x)$ вместо остатка от деления $x^k g(x)$ на $f(x)$ остаток от деления $(a_0x^k + a_1x^{k-1} + \ldots + a_k)g(x)$ на $f(x)$.

Упражнение 5.1. *Доказать справедливость тождества*

$$g_k(x) \equiv F_k(x)g(x) - G_k(x)f(x) \ , \tag{5.5}$$

где $F_k(x) \stackrel{\text{def}}{=} a_0x^k + a_1x^{k-1} + \ldots + a_k$, $G_k(x) \stackrel{\text{def}}{=} b_0x^k + b_1x^{k-1} + \ldots + b_k$.

Вычислим $g_k(x)$ для $k = 0, \ldots, n-1$:

$$g_k(x) = \mathfrak{b}_{k0}x^{n-1} + \mathfrak{b}_{k1}x^{n-2} + \ldots + \mathfrak{b}_{k,n-1} \ ,$$

составим матрицу $\mathfrak{B}$ из этих коэффициентов

$$\mathfrak{B} = [\mathfrak{b}_{kj}]_{k,j=0}^{n-1} \tag{5.6}$$

и обозначим через $\mathfrak{B}_j$ ее j-й главный минор.

Определение. Матрица $\mathfrak{B}$, определяемая формулой (5.6), называется **безутиантой**[4] полиномов $f(x)$ и $g(x)$.

Замечание. В случае $\deg(g) = m < \deg(f) = n$ безутианта строится для полиномов $f(x)$ и $x^{n-m}g(x)$.

Пример 5.2. *Доказать, что*

$$\mathfrak{b}_{kj} = d_{0,k+j+1} + d_{1,k+j} + \ldots + d_{k,j+1} \ , \tag{5.7}$$

где $d_{ij} = a_ib_j - a_jb_i$, *в предположении, что* $b_j = 0$ *при* $j > m$, $a_k = 0$ *при* $k > n$.

Решение. Для $n = 3$ равенства (5.5) принимают следующий вид:

$$a_0(b_0x^3 + b_1x^2 + b_2x + b_3) - b_0(a_0x^3 + a_2x^2 + a_3x + a_4) =$$
$$= (a_0b_1 - a_1b_0)x^2 + (a_0b_2 - a_2b_0)x + (a_0b_3 - a_3b_0) \ ,$$
$$(a_0x + a_1)(b_0x^3 + b_1x^2 + b_2x + b_3) - (b_0x + b_1)(a_0x^3 + a_2x^2 + a_3x + a_4) =$$
$$= (a_0b_2 - a_2b_0)x^2 + (a_0b_3 - a_3b_0 + a_1b_2 - a_2b_1)x + (a_1b_3 - a_3b_1) \ ,$$
$$(a_0x^2 + a_1x + a_2)(b_0x^3 + b_1x^2 + b_2x + b_3) -$$
$$-(b_0x^2 + b_1x + b_2)(a_0x^3 + a_2x^2 + a_3x + a_4) =$$
$$= (a_0b_3 - a_3b_0)x^2 + (a_1b_3 - a_3b_1)x + (a_2b_3 - a_3b_2) \ .$$

Отсюда легко следуют равенства (5.7). $\triangle$

[4] Иногда под безутиантой понимают $\det \mathfrak{B}$.

Упражнение 5.2. *Показать, что безутианта — симметричная матрица, т.е.* $\mathfrak{b}_{jk} = \mathfrak{b}_{kj}$.

Упражнение 5.3. *Доказать, что величины* $\mathfrak{b}_{jk}$ *могут быть получены как коэффициенты полинома от двух переменных:*

$$\frac{f(x)g(y) - f(y)g(x)}{x - y} = \sum_{j,k=0}^{n-1} \mathfrak{b}_{jk} x^{n-j-1} y^{n-k-1} \ .$$

Теорема 5.2. *Для случая полиномов одинаковой степени* n *безутианта может быть получена в виде:*

$$\mathfrak{B} = \begin{pmatrix} b_1 & b_2 & \dots & b_{n-1} & b_n \\ b_2 & b_3 & \dots & b_n & \\ \dots & & \iddots & & \\ b_{n-1} & b_n & & \mathbb{O} & \\ b_n & & & & \end{pmatrix} \begin{pmatrix} a_0 & a_1 & \dots & a_{n-2} & a_{n-1} \\ & a_0 & a_1 & \dots & a_{n-2} \\ & & \ddots & & \\ & \mathbb{O} & & a_0 & a_1 \\ & & & & a_0 \end{pmatrix} -$$

$$- \begin{pmatrix} a_n & a_{n-1} & \dots & a_2 & a_1 \\ & a_n & & \dots & a_2 \\ & & \ddots & & \\ & \mathbb{O} & & a_n & a_{n-1} \\ & & & & a_n \end{pmatrix} \begin{pmatrix} & & & & b_0 \\ & \mathbb{O} & & b_0 & b_1 \\ & & \iddots & & \\ & b_0 & b_1 & \dots & b_{n-2} \\ b_0 & b_1 & \dots & b_{n-2} & b_{n-1} \end{pmatrix}$$

т.е., фактически, перемножением $n \times n$*-блоков, составляющих матрицу Сильвестра* (1.3)*:*

$$M = \begin{pmatrix} A_0 & A_1 \\ B_0 & B_1 \end{pmatrix}$$

с транспонированием одного из них:

$$\mathfrak{B} = B_1 A_0 - A_1^t B_0 \ . \tag{5.8}$$

Доказательство проводится вычислением элементов матрицы (5.8) и их сравнением с представлением (5.7). Мы же покажем здесь как можно установить справедливость вытекающего из (5.8) детерминантного равенства:

$$\det M = \det(B_1 A_0 - A_1^t B_0) \ .$$

В самом деле, заметим, что матрица A_0 — невырожденная и что B_0 и B_1 — симметричные. Выпишем для определителя блочной матрицы M равенство Шура [14]:

$$\det M = \det A_0 \det(B_1 - B_0 A_0^{-1} A_1) \ .$$

Отсюда:

$$\det M = \det A_0^t \det(B_1 - B_0 A_0^{-1} A_1) = \det(A_0^t B_1 - A_0^t B_0 A_0^{-1} A_1) =$$
$$= \det(A_0^t B_1 - B_0 A_0 A_0^{-1} A_1) = \det(A_0^t B_1 - B_0 A_1) = \det(B_1 A_0 - A_1^t B_0) \ ,$$

если только мы установим, что $A_0^t B_0 = B_0 A_0$. А это проверяется легко. $\square$

Теорема 5.3. *Пусть* $\deg f = \deg g = n$. *Для безутианты, определяемой формулой* (5.6), *справедливы следующие утверждения:*

а) $\mathfrak{B}_n = \det \mathfrak{B} = (-1)^{n(n-1)/2}\mathcal{R}(f,g)$.

б) *Степень* НОД (f,g) *равна* d *тогда и только тогда, когда*

$$\mathfrak{B}_n = \mathfrak{B}_{n-1} = \ldots = \mathfrak{B}_{n-d+1} = 0,\ \mathfrak{B}_{n-d} \neq 0\ .$$

В этом случае НОД (f,g) *равен определителю, получающемуся из* $\mathfrak{B}_{n-d}$ *заменой последнего столбца на столбец*

$$\left[\sum_{j=n-d-1}^{n-1} \mathfrak{b}_{0j}x^{n-j-1}, \sum_{j=n-d-1}^{n-1} \mathfrak{b}_{1j}x^{n-j-1}, \ldots, \sum_{j=n-d-1}^{n-1} \mathfrak{b}_{n-d-1,j}x^{n-j-1}\right]^t\ .$$

Старший коэффициент НОД (f,g) *равен* $\mathfrak{B}_{n-d}$.

в) *Полиномы* $v(x)$ *и* $u(x)$, *дающие линейное представление* НОД (f,g) *(см. формулу* (1.13)*), получаются из* $\mathfrak{B}_{n-d}$ *заменой в нем последнего столбца на*

$$[-b_0, -b_0x - b_1, \ldots, -b_0x^{n-d-1} - b_1x^{n-d-2} - \ldots - b_{n-d-1}]^t \ \ u$$
$$[a_0, a_0x + a_1, \ldots, a_0x^{n-d-1} + a_1x^{n-d-2} + \ldots + a_{n-d-1}]^t$$

соответственно.

Теорема 5.4. *Справедливо соотношение, связывающее главный минор* $\mathfrak{B}_k$ *безутианты с субрезультантом:*

$$\mathfrak{B}_{n-k} = \mathcal{R}^{(k)} \quad (k \leq n)\ . \tag{5.9}$$

Доказательство формулы (5.9) проведем для случая $n = 5, k = 2$. Составим следующее произведение:

$$\begin{pmatrix} 1 & & & & & \\ 0 & 1 & & & & \\ 0 & 0 & 1 & & & \\ 0 & 0 & -b_0 & a_0 & & \\ 0 & -b_0 & -b_1 & a_1 & a_0 & \\ -b_0 & -b_1 & -b_2 & a_2 & a_1 & a_0 \end{pmatrix} \cdot \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ & a_0 & a_1 & a_2 & a_3 & a_4 \\ & & a_0 & a_1 & a_2 & a_3 \\ & & b_0 & b_1 & b_2 & b_3 \\ & b_0 & b_1 & b_2 & b_3 & b_4 \\ b_0 & b_1 & b_2 & b_3 & b_4 & b_5 \end{pmatrix}\ .$$

Определитель этого произведения равен произведению определителей, т.е. $a_0^3\mathcal{R}^{(2)}$. С другой стороны, выполнив перемножение с учетом формул (5.7), получаем матрицу

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & a_5 \\ & a_0 & a_1 & a_2 & a_3 & a_4 \\ & & a_0 & a_1 & a_2 & a_3 \\ & & & \mathfrak{b}_{00} & \mathfrak{b}_{01} & \mathfrak{b}_{02} \\ & & & \mathfrak{b}_{1,0} & \mathfrak{b}_{1,1} & \mathfrak{b}_{1,2} \\ & & & \mathfrak{b}_{2,0} & \mathfrak{b}_{2,1} & \mathfrak{b}_{2,2} \end{pmatrix}\ ,$$

определитель которой равен $a_0^3\mathfrak{B}_3$. $\square$

Упражнение 5.4. *С помощью теоремы* 3.3 *установить справедливость утверждений пунктов б) и в) теоремы* 5.3 .

Упражнение 5.5. *Найти* НОД (f,g) *и его линейное представление для*
а) $f(x)=x^4-x^3-4x^2-x+1,\ g(x)=2x^4-6x^3+3x^2-3x+1$;
б) $f(x)=2x^3-7x^2+11x-6,\ g(x)=x^4-x^3+3x^2-4x+1$.

Упражнение 5.6. *При каком условии полиномы*

$$a_0x^3+a_1x^2+a_2x+a_3 \text{ и } b_0x^4+b_1x^3+b_2x^2+b_3x+b_4$$

имеют НОД *второй степени? Найти этот* НОД .

6 Приложения

6.1 Уничтожение иррациональности в знаменателе

Пусть $f(x),g(x),g_1(x)$ — полиномы из $\mathbb{A}[x]$, и $\lambda_1,\dots,\lambda_n$ — корни $f(x)$.

Задача. Для рациональной дроби $g_1(x)/g(x)$ найти такой полином $G(x)\in\mathbb{A}[x]$, чтобы

$$G(\lambda_1)=g_1(\lambda_1)/g(\lambda_1),\ \dots,\ G(\lambda_n)=g_1(\lambda_n)/g(\lambda_n)\ .$$

Главным образом, нас будет интересовать случай, когда коэффициенты $f(x),g(x)$ и $g_1(x)$ являются рациональными числами, но среди корней $\lambda_1,\dots,\lambda_n$ полинома $f(x)$ имеются иррациональные. Именно в этом случае поставленную задачу и называют задачей об уничтожении иррациональности в знаменателе выражения $g_1(\lambda)/g(\lambda)$. Здесь предполагается, что $\lambda\in\{\lambda_1,\dots,\lambda_n\}$.

Теорема 6.1. *Если* $\mathcal{R}(f,g)\neq 0$, *то всегда существует полином* $G(x)$, *решающий поставленную задачу. При условии* $\deg G<n$ *такой полином определяется единственным образом, и его коэффициенты будут рационально зависеть от коэффициентов* $f(x),g(x)$ *и* $g_1(x)$.

Доказательство . По теореме 1.2, существуют полиномы $\tilde v(x)$ и $\tilde u(x)$, удовлетворяющие тождеству (1.14):

$$\tilde v(x)f(x)+\tilde u(x)g(x)\equiv\mathcal{R}(f,g)\ ,$$

а если их строить согласно алгоритму теоремы, то легко видеть, что их коэффициенты — как и коэффициенты $\mathcal{R}(f,g)$ — принадлежат $\mathbb{A}$. Подставляем в тождество $x=\lambda_j$:

$$\tilde u(\lambda_j)g(\lambda_j)=\mathcal{R}(f,g)\ \Rightarrow\ \frac{1}{g(\lambda_j)}=\frac{\tilde u(\lambda_j)}{\mathcal{R}(f,g)}\ \text{ и }\ \frac{g_1(\lambda_j)}{g(\lambda_j)}=\frac{g_1(\lambda_j)\tilde u(\lambda_j)}{\mathcal{R}(f,g)}\ .$$

Следовательно, в качестве искомого полинома $G(x)$ можно взять полином $g_1(x)\tilde{u}(x)/\mathcal{R}(f,g)$. Легко видеть, что наряду с полиномом $G(x)$ полином $G(x)+q(x)f(x)$, где $q(x)$ — произвольный полином из $\mathbb{A}[x]$, тоже дает решение поставленной задачи. Взяв в качестве $G(x)$ остаток от деления $g_1(x)\tilde{u}(x)$ на $f(x)$ и поделив его на $\mathcal{R}(f,g)$, получим полином с указанным в теореме ограничением на степень. Результант и полином $\tilde{u}(x)$ можно искать с помощью любой из теорем 1.2, 4.2, 5.1, 5.3, а также методом неопределенных коэффициентов. □

Упражнение 6.1. *Доказать единственность полинома $G(x)$ при выполнении условия* $\deg G < n$.

Пример 6.1. *Уничтожить иррациональность в знаменателе выражения*

$$\frac{\lambda}{\lambda^3-1},\ \textit{где } \lambda \textit{ — корень полинома } x^5-4x-2\ .$$

Решение. Из решения примера 1.5 имеем:

$$\tilde{u}(x)=18\,x^4-7\,x^3+8\,x^2+18\,x-79,\ \mathcal{R}(f,g)=95\ .$$

Воспользуемся теперь алгоритмом из доказательства теоремы 6.1:

$$G(x)=(18\,x^5-7\,x^4+8\,x^3+18\,x^2-79\,x)/95\ .$$

Если поделить $G(x)$ на $f(x)$, то остаток от деления

$$G_1(x)=(-7x^4+8x^3+18x^2-7x+36)/95$$

также является решением задачи — причем единственным среди полиномов степеней меньших 5. △

Упражнение 6.2. *Уничтожить иррациональность в знаменателе выражений*

а) $\lambda/(\lambda-1)$, *где* λ *— корень полинома* x^3-2x-2;

б) $1/(\lambda^3+3\lambda^2+3\lambda+2)$, *где* λ *— корень полинома* $x^4+x^3-4\,x^2-3\,x+2$.

6.2 Преобразование Чирнгауза

Задача. Пусть даны два полинома из $\mathbb{A}[x]$:

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n,\ g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_m$$

($a_0\neq 0, b_0\neq 0$); обозначим $\lambda_1,\ldots,\lambda_n$ (неизвестные нам) корни $f(x)$. Построить полином $F(y)$, имеющий корни $g(\lambda_1),\ldots,g(\lambda_n)$. Нахождение этого полинома называется **преобразованием Чирнгауза** $y=g(x)$ полинома $f(x)$.

Теорема 6.2. *Существует единственный нормализованный полином $F(y)$ степени n, решающий задачу. При этом его коэффициенты будут рационально зависеть от коэффициентов $f(x)$ и $g(x)$.*

Доказательство . Требуемый полином

$$F(y) = (y - g(\lambda_1)) \times \ldots \times (y - g(\lambda_n)) \ .$$

По формуле (1.8):

$$F(y) = \mathcal{R}(f(x), y - g(x))/a_0^m$$

(результант вычисляется для полиномов относительно переменной x, а y считается числовым параметром). □

Пример 6.2. *Найти преобразование Чирнгауза $y = x^2 + x - 1$ полинома $f(x) = x^3 - 2x + 3$.*

Решение. Построим полином $F(y)$:

$$\begin{aligned} F(y) &= \mathcal{R}(x^3 - 2x + 3,\ -x^2 - x + (1 + y)) = \\ &= -\begin{vmatrix} 1 & 0 & -2 & 3 & 0 \\ 0 & 1 & 0 & -2 & 3 \\ 0 & 0 & -1 & -1 & 1+y \\ 0 & -1 & -1 & 1+y & 0 \\ -1 & -1 & 1+y & 0 & 0 \end{vmatrix} = y^3 - y^2 + 6y - 4 \ . \end{aligned}$$

△

Пример 6.3. *Для полинома $f(x) = x^3 + a_1x^2 + a_2x + a_3 \in \mathbb{C}[x]$ подобрать преобразование Чирнгауза вида $y = x^2 + b_1x + b_2 \in \mathbb{C}[x]$ так, чтобы получившийся в результате преобразования полином имел вид $F(y) = y^3 + c_3$.*

Решение. Преобразование Чирнгауза при первоначально неопределенных b_1 и b_2 дает[5]:

$$F(y) = y^3 + c_1y^2 + c_2y + c_3$$

при

$$\begin{aligned} c_1 &= -a_1^2 + 2\,a_2 + a_1b_1 - 3\,b_2 \ , \\ c_2 &= -a_1a_2b_1 + a_2b_1^2 - 2\,a_1a_3 + a_2^2 - 4\,a_2b_2 + 3\,a_3b_1 + 2\,a_1^2b_2 - 2\,a_1b_1b_2 + 3\,b_2^2 \ , \\ c_3 &= a_1b_1b_2^2 - a_1^2b_2^2 + a_1a_2b_1b_2 + a_2a_3b_1 - a_3^2 + 2\,a_2b_2^2 + \\ &\quad + a_3b_1^3 - a_2b_1^2b_2 - a_1a_3b_1^2 + 2\,a_1a_3b_2 - b_2^3 - 3\,a_3b_1b_2 - a_2^2b_2 \ . \end{aligned}$$

[5] Для вычислений использовался пакет MAPLE; см. с. 68.

Требуется подобрать b_1 и b_2 так, чтобы коэффициенты c_1 и c_2 обратились в нуль. Получаем систему из двух уравнений относительно b_1 и b_2: первое из них — линейное, второе — квадратное. Эта система разрешима в радикалах:

$$b_1 = \frac{2\,a_1^3 - 7\,a_1a_2 + 9\,a_3 \pm \sqrt{-3\mathcal{D}(f)}}{2(a_1^2 - 3\,a_2)} \ , \tag{6.1}$$

а b_2 выражается через b_1 по формуле

$$b_2 = \frac{a_1b_1 - a_1^2 + 2\,a_2}{3} \ . \tag{6.2}$$

Здесь $\mathcal{D}(f) = -27\,a_3^2 + 18\,a_1a_2a_3 - 4\,a_1^3a_3 + a_1^2a_2^2 - 4\,a_2^3$, т.е. является дискриминантом кубического полинома (см. упражнение 2.1, б)); предполагается также, что $a_1^2 - 3\,a_2 \neq 0$. Итак, преобразование Чирнгауза при указанных значениях параметров b_1 и b_2 дает полином $y^3 + c_3$ (здесь в приведенное выше выражение для c_3 также следует подставить полученные выражения для b_1 и b_2). $\triangle$

Только что решенный пример позволяет ответить на вопрос: *зачем нужно преобразование Чирнгауза*? Именно, это преобразование *иногда* позволяет решать алгебраические уравнения в радикалах. В самом деле, уравнение $y^3 + c_3 = 0$ можно решить в радикалах; если обозначить μ_1, μ_2 и μ_3 его корни, то корни исходного кубического уравнения $x^3 + a_1x^2 + a_2x + a_3 = 0$ получатся как решения квадратных уравнений $\lambda^2 + b_1\lambda + b_2 = \mu_j$ при b_1 и b_2 заданных формулами (6.1) и (6.2).

Упражнение 6.3. *Найти преобразование Чирнгауза, позволяющее решить в радикалах уравнение* $x^3 + a_1x^2 + {}^1\!/_3\,a_1^2x + a_3 = 0$.

Упражнение 6.4. *Считая теперь доказанным факт разрешимости кубического уравнения в радикалах, придумать способ решения в радикалах уравнения* $x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0$ *с помощью преобразования Чирнгауза вида* $y = x^2 + b_1x + b_2$.

⊖ Фактическое построение преобразования возможно любым из методов нахождения результанта. Следующий способ построения преобразования Чирнгауза является развитием метода Безу (см. §5).

Найдем остатки от деления $x^kg(x)$ на $f(x)$ для $k = 0, 1, \ldots, n-1$:

$$g_k(x) \stackrel{\text{def}}{=} b_{k0} + b_{k1}x + \ldots + b_{k,n-2}x^{n-2} + b_{k,n-1}x^{n-1}$$

(мы изменили порядок нумерации коэффициентов по сравнению с §5) и составим матрицу из этих коэффициентов:

$$B = [b_{kj}]_{k,j=0}^{n-1} \ . \tag{6.3}$$

⊖ **Теорема 6.3 (Эрмит).** $F(y) = (-1)^n \det(B - yE) =$

$$= (-1)^n \begin{vmatrix} b_{00}-y & b_{01} & b_{02} & \dots & b_{0,n-1} \\ b_{1,0} & b_{1,1}-y & b_{1,2} & \dots & b_{1,n-1} \\ \dots & & & \dots & \\ b_{n-1,0} & b_{n-1,1} & b_{n-1,2} & \dots & b_{n-1,n-1}-y \end{vmatrix} .$$

Доказательство . Равенства

$$y = g(x),\ xy = g(x)x,\ \dots, x^{n-1}y = g(x)x^{n-1} \ ,$$

при подстановке $x = \lambda_j$ переходят в

$$y = g_0(\lambda_j),\ \lambda_j y = g_1(\lambda_j), \dots, \lambda_j^{n-1} y = g_{n-1}(\lambda_j) \ .$$

Рассмотрим получившиеся уравнения как линейную однородную систему относительно столбца неизвестных $X = [1, \lambda_j, \dots, \lambda_j^{n-1}]^t$. Поскольку эта система имеет нетривиальное решение, то определитель ее матрицы должен обращаться в нуль. □

⊖ **Пример 6.4.** *Решить пример* 6.2 *по методу Эрмита.*

Решение. Имеем $g_0(x) \equiv g(x) = -1 + x + x^2$; $g_1(x) = -3 + x + x^2$; $g_2(x) = -3 - x + x^2$, следовательно

$$F(y) = (-1)^3 \begin{vmatrix} -1-y & 1 & 1 \\ -3 & 1-y & 1 \\ -3 & -1 & 1-y \end{vmatrix} = y^3 - y^2 + 6y - 4 \ .$$

△

Упражнение 6.5. *Найти преобразование Чирнгауза $y = g(x)$ полинома $f(x)$ для*

а) $f(x) = x^3 - x^2 - 2x + 1,\ g(x) = -x^2 + 2$;

б) $f(x) = x^4 + x^3 + x^2 + x + 1,\ g(x) = x^3 + x^2 + x + 1$;

в) $f(x) = x^5 - 1,\ g(x) = x^4 - 1$.

⊖ **Упражнение 6.6.** *Пусть $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$, $a_0 \neq 0$. Доказать, что полином*

$$F(y) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_2 & a_1 & a_0 \\ a_0y & a_n & a_{n-1} & \dots & a_3 & a_2 & a_1 \\ a_1y & a_0y & a_n & \dots & a_4 & a_3 & a_2 \\ \dots & & & & & & \dots \\ a_{n-3}y & a_{n-4}y & a_{n-5}y & \dots & a_n & a_{n-1} & a_{n-2} \\ a_{n-2}y & a_{n-3}y & a_{n-4}y & \dots & a_0y & a_n & a_{n-1} \\ a_{n-1}y & a_{n-2}y & a_{n-3}y & \dots & a_1y & a_0y & a_n \end{vmatrix}$$

представляет преобразование Чирнгауза $y = x^{n+1}$ полинома $f(x)$, т.е. $F(y)$ имеет корнями $(n+1)$-е степени корней полинома $f(x)$.

Пример 6.5. *Пусть $f(x), g(x), g_1(x)$ — полиномы с рациональными коэффициентами. Построить полином $F(y)$, имеющий корни*

$$g_1(\lambda_1)/g(\lambda_1),\ \ldots,\ g_1(\lambda_n)/g(\lambda_n)\ .$$

Решение. Можно воспользоваться результатами §6.1. Построив полином $G(x)$ такой, что $G(\lambda_j) = g_1(\lambda_j)/g(\lambda_j)$ $(j = 1, \ldots, n)$, сведем задачу к уже решенной. Можно действовать и напрямую: полином

$$F(y) = \mathcal{R}(f(x), yg(x) - g_1(x))$$

решает задачу при условии $\mathcal{R}(f(x), g(x)) \neq 0$. △

6.3 Экстремальные значения полинома

Пусть задан полином с вещественными коэффициентами

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

четной степени n. Предположим, что $a_0<0$. Тогда функция $y = f(x)$ достигает максимального значения в одной из своих стационарных точек, т.е. на вещественных корнях уравнения $f'(x) = 0$. Обозначим эти корни $\mu_1, \ldots, \mu_{n-1}$. Тогда $\max f(x)$ находится среди его критических значений, т.е. чисел $f(\mu_1), \ldots, f(\mu_{n-1})$.

Задача. Построить полином $\mathcal{F}(z)$, корнями которого являются критические значения полинома $f(x)$.

Положим

$$\mathcal{F}(z) \stackrel{\text{def}}{=} (-1)^{n-1}\mathcal{D}(f(x) - z)\ . \tag{6.4}$$

Здесь дискриминант вычисляется относительно переменной x, а z считается числовым параметром. На основании определения дискриминанта и формулы (1.8), получаем требуемое свойство полинома $\mathcal{F}$. По построению, $\mathcal{F} \in \mathbb{Z}[a_0, a_1, \ldots, a_n]$.

Пример 6.6. *Для $f(x) = x^4 + px + q$ имеем*

$$\mathcal{F}(z) = 256\,z^3 - 768q\,z^2 + 768q^2\,z + (27\,p^4 - 256\,q^3)\ .$$

Упражнение 6.7. *Доказать, что свободный член $\mathcal{F}(z)$ равен $(-1)^{n-1}\mathcal{D}(f(x))$. Что означает его обращение в нуль с точки зрения математического анализа?*

Упражнение 6.8. *Построить полином $\mathcal{F}(z)$ для*
а) $f(x) = -x^4 - 4\,x^3 + 2\,x^2 + 12\,x$;
б) $f(x) = -x^4 + 4\,x^3 - 4\,x^2$;
в) $f(x) = -x^6 - 10\,x^3 + 12\,x$
и установить, что $\max f(x)$ достигается в двух стационарных точках.

Пример 6.7. *Проверить достоверность утверждения: максимальный вещественный корень $\mathcal{F}(z)$ совпадает с* $\max f(x)$.

Решение. Для $f(x) = -x^6 - 135x^2 - 324x$ полином (6.4) равен

$$46656(z^3 + 1080z^2 + 1603800z - 354294000)(z - 540)^2$$

и имеет максимальный корень равным $z = 540$; однако последний соответствует комплексно-сопряженным корням $\mu_{1,2} = (-3 \pm \boldsymbol{i}\sqrt{15})/2$ производной $f'(x) = -6(x^5 + 45x + 54)$. Максимум достигается на корне $\mu_3 = 1 - \sqrt[3]{10}$ и равен $90(-4 + 5\sqrt[3]{10} - \sqrt[3]{100}) \approx 191.7526154$. $\triangle$

Часть 2. Исключение переменных в системе двух уравнений

7 Общие сведения о полиномах от двух переменных

Рассмотрим полином от двух переменных x и y

$$f(x,y)=\sum_{j+k=0}^{n} a_{jk}x^j y^k = a_{00}+a_{1,0}x+a_{01}y+a_{2,0}x^2+a_{1,1}xy+a_{02}y^2+\ldots+$$

$$+a_{n0}x^n+a_{n-1,1}x^{n-1}y+\ldots+a_{1,n-1}xy^{n-1}+a_{0n}y^n \ , \qquad (7.1)$$

коэффициенты которого всюду в дальнейшем будем предполагать вещественными или рациональными; $f\in\mathbb{A}[x,y]$ теперь означает $f\in\mathbb{R}[x,y]$ или $f\in\mathbb{Q}[x,y]$.

Определение. Если полином $f(x,y)$ содержит только мономы степени k:

$$f(x,y)=a_{k0}x^k+a_{k-1,1}x^{k-1}y+\ldots+a_{1,k-1}xy^{k-1}+a_{0k}y^k$$

то он называется **однородным полиномом** или **формой степени** k. Будем обозначать его $f_k(x,y)$.

Форма $f_k(x,y)$ обладает следующим свойством:

$$f_k(t\cdot x,\,t\cdot y)\equiv t^k f_k(x,y)\ \forall t\in\mathbb{R}\ .$$

Представление (7.1) полинома $f(x,y)$ очевидным образом группируется по формам:

$$f(x,y)=f_0(x,y)+f_1(x,y)+\ldots+f_n(x,y)\ ,$$

где

$$f_0(x,y)\equiv a_{00},\ f_1(x,y)=a_{1,0}x+a_{01}y,\ldots$$

Если $\deg f=n$, то форма $f_n(x,y)$ называется **старшей формой** полинома $f(x,y)$.

Упражнение 7.1. *Сколькими коэффициентами задается полином $n-$й степени?*

Обобщением разложения (7.1) для полинома $f(x,y)$ является разложение по степеням $X=x-x_0$ и $Y=y-y_0$ при произвольных x_0 и y_0. Новое разложение снова может быть представлено в виде суммы форм — теперь уже относительно X и Y:

$$f(x,y)\equiv f(X+x_0,Y+y_0)=F_0(X,Y)+F_1(X,Y)+\ldots+F_n(X,Y)\ . \quad (7.2)$$

Здесь

$$F_0(X,Y) = f(x_0,y_0),\ F_1(X,Y) = \left.\frac{\partial f}{\partial x}\right|_{(x_0,y_0)} X + \left.\frac{\partial f}{\partial y}\right|_{(x_0,y_0)} Y\ ,$$

$$F_2(X,Y) = \left.\frac{\partial^2 f}{\partial x^2}\right|_{(x_0,y_0)} X^2 + 2\left.\frac{\partial^2 f}{\partial x \partial y}\right|_{(x_0,y_0)} X\,Y + \left.\frac{\partial^2 f}{\partial y^2}\right|_{(x_0,y_0)} Y^2\ ,$$

$$F_k(X,Y) = \sum_{j=0}^{k} \mathsf{C}_k^j \left.\frac{\partial^k f}{\partial x^{k-j}\partial y^j}\right|_{(x_0,y_0)} X^{k-j}Y^j \quad (k \geq 1)\ ,$$

где $\mathsf{C}_k^j \stackrel{\text{def}}{=} \dfrac{k!}{j!(k-j)!}$ — биномиальный коэффициент.

Определения. Точка $(x_0,y_0) \in \mathbb{C}^2$ называется **нулем** полинома $f(x,y)$, если $f(x_0,y_0) = 0$. Нуль называется **простым**, если $F_1(X,Y) \not\equiv 0$, и **кратным кратности** $k+1$, если в разложении (7.2) будет

$$F_0(x,y) = 0,\ F_1(X,Y) \equiv 0, \ldots, F_k(X,Y) \equiv 0, F_{k+1}(X,Y) \not\equiv 0\ .$$

Понятно, что для того чтобы точка (x_0,y_0) была кратным нулем $f(x,y)$, необходимо и достаточно, чтобы

$$f(x_0,y_0) = \left.\frac{\partial f}{\partial x}\right|_{(x_0,y_0)} = \left.\frac{\partial f}{\partial y}\right|_{(x_0,y_0)} = 0\ . \tag{7.3}$$

Упражнение 7.2. *Установить кратность нуля* $(1,-1)$ *для полинома* $x^2 + x\,y - x - y$.

Упражнение 7.3. *Доказать, что если* (x_0,y_0) *— нуль полинома* $f(x,y)$ *кратности* k *и при этом* $x_0 \notin \mathbb{R}$ *или* $y_0 \notin \mathbb{R}$, *то* $(\overline{x}_0,\overline{y}_0)$ *— также нуль полинома, причем той же кратности.*

Определение. Нуль (x_0,y_0) полинома $f(x,y)$ будем называть вещественным, если $x_0 \in \mathbb{R}$ и $y_0 \in \mathbb{R}$; в противном случае пару (x_0,y_0) и $(\overline{x}_0,\overline{y}_0)$ будем называть **комплексно-сопряженными** нулями.

Упражнение 7.4. *Доказать, что если* (x_0,y_0) *— нуль формы* $f_k(x,y)$ *при* $k > 0$, *то при любом значении* $t \in \mathbb{C}$ *точка* (tx_0,ty_0) *также будет нулем* $f_k(x,y)$.

Задача. Решить систему двух уравнений

$$f(x,y) = 0,\ g(x,y) = 0\ , \tag{7.4}$$

т.е. найти общие нули полиномов $f(x,y)$ и $g(x,y)$. Нас интересуют все решения (7.4), в том числе и комплексные $(x,y) \in \mathbb{C}^2$.

Геометрический смысл вещественного нуля полинома $f(x,y)$ степени n — точка на **алгебраической кривой** n-го порядка, заданной уравнением $f(x,y)=0$; кривая может состоять из нескольких **ветвей**. Кратный нуль (см. условия (7.3)) определяет **особую точку**; последняя возникает, например, когда ветвь кривой пересекает саму себя. Вещественное решение системы (7.4) очевидно определяет координаты точки пересечения алгебраических кривых n-го и m-го порядков (рис. 1).

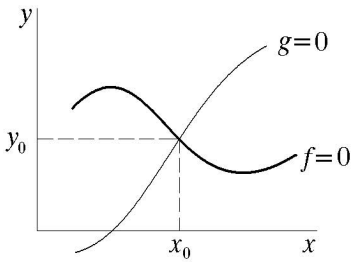

Рис. 1

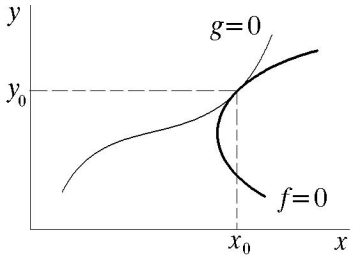

Рис. 2

Частным случаем пересечения кривых является их касание (рис. 2). Для того чтобы точка (x_0,y_0) была точкой касания необходимо, чтобы в ней выполнялись условия:

$$f(x,y)=0,\ g(x,y)=0,\ \frac{\partial f}{\partial x}\Big/\frac{\partial f}{\partial y}=\frac{\partial g}{\partial x}\Big/\frac{\partial g}{\partial y}\ ,$$

где последнее характеризует равенство угловых коэффициентов касательных к алгебраическим кривым $f(x,y)=0$ и $g(x,y)=0$.

Определение. Выражение

$$\mathcal{J}(x,y)=\frac{\partial f}{\partial x}\frac{\partial g}{\partial y}-\frac{\partial g}{\partial x}\frac{\partial f}{\partial y} \tag{7.5}$$

называется **якобианом** полиномов $f(x,y)$ и $g(x,y)$.

Якобиан является двумерным аналогом производной полинома от одной переменной. В частности, обращение его в нуль на некотором решении системы (7.4) означает, что решение — **кратное**. Такое решение при бесконечно-малом возмущении коэффициентов полиномов распадается на несколько простых. Геометрически это означает, что при небольшой деформации этих кривых такая точка неустойчива: она либо распадается на две (или более) точки обычного пересечения, либо порождает пару мнимых.

⊖ **Упражнение 7.5.** *Доказать, что при условии* $a_{n0}\neq 0, a_{0n}\neq 0$ *асимптотами кривой* $f(x,y)=0$ *могут быть лишь прямые вида* $y=Kx+L$, *где*

$$L=-\frac{f_{n-1}(1,K)}{\partial f_n/\partial y\,|_{(1,K)}}\ ,$$

а K — вещественный корень уравнения

$$f_n(1,y) = a_{n0} + a_{n-1,1}y + \ldots + a_{1,n-1}y^{n-1} + a_{0n}y^n = 0 \ ,$$

в предположении, что последнее не имеет кратных корней.

8 Общая схема исключения

Представим $f(x,y)$ и $g(x,y)$ в виде сумм их форм:

$$\begin{aligned} f(x,y) &= f_n(x,y) + f_{n-1}(x,y) + \ldots + f_0(x,y) \ , \\ g(x,y) &= g_m(x,y) + g_{m-1}(x,y) + \ldots + g_0(x,y) \ . \end{aligned}$$

Относительно коэффициентов старших форм

$$\begin{aligned} f_n(x,y) &= a_{n0}x^n + a_{n-1,1}x^{n-1}y + \ldots + a_{0n}y^n \ , \\ g_m(x,y) &= b_{m0}x^m + b_{m-1,1}x^{m-1}y + \ldots + b_{0m}y^m \end{aligned} \tag{8.1}$$

сделаем следующее предположение:

$$a_{n0} \neq 0, a_{0n} \neq 0, b_{m0} \neq 0, b_{0m} \neq 0 \ . \tag{8.2}$$

Пара $(\alpha,\beta) \in \mathbb{C}^2$ будет решением (7.4) тогда и только тогда, когда полиномы $f(\alpha,y)$ и $g(\alpha,y)$ имеют общий корень $y = \beta$, а, следовательно, на основании теоремы 1.1,

$$\mathcal{R}(f(\alpha,y), g(\alpha,y)) = 0 \ . \tag{8.3}$$

Запишем этот результант в форме Сильвестра (см. §1). Для этого разложим $f(\alpha,y)$ и $g(\alpha,y)$ по убывающим степеням y

$$\begin{aligned} f(\alpha,y) &= A_0y^n + A_1(\alpha)y^{n-1} + \ldots + A_n(\alpha) \ , \\ g(\alpha,y) &= B_0y^m + B_1(\alpha)y^{m-1} + \ldots + B_m(\alpha) \end{aligned}$$

(здесь $A_0 = a_{0n} \neq 0, B_0 = b_{0m} \neq 0$ по (8.2), $\deg A_j(\alpha) \leq j$, $\deg B_j(\alpha) \leq j$) и вычислим определитель Сильвестра

$$\left.\begin{matrix} \\ \\ \\ m \\ \\ \\ \\ \\ \\ n \\ \\ \\ \end{matrix}\right\{ \begin{vmatrix} A_0 & A_1(\alpha) & \ldots & & A_n(\alpha) & & \mathbb{O} \\ & A_0 & \ldots & & & A_n(\alpha) & \\ & & \ddots & & & \ldots & \ddots \\ & & & A_0 & A_1(\alpha) & \ldots & A_n(\alpha) \\ & \mathbb{O} & & & B_0 & \ldots & B_m(\alpha) \\ & & & B_0 & B_1(\alpha) & \ldots & \\ & & \iddots & & & \ldots & \iddots \\ & B_0 & B_1(\alpha) & \ldots & & B_m(\alpha) & \\ B_0 & B_1(\alpha) & \ldots & & B_m(\alpha) & & \mathbb{O} \end{vmatrix} = \mathcal{X}(\alpha) \ . \tag{8.4}$$

$\mathcal{X}(\alpha)$ — полином по α. Для выполнения условия (8.3) необходимо и достаточно, чтобы значение α удовлетворяло уравнению $\mathcal{X}(x) = 0$. Если $\{f, g\} \subset \mathbb{A}[x, y]$, то и $\mathcal{X}(x) \in \mathbb{A}[x]$.

Определение. Полином $\mathcal{X}(x)$ — т.е. результант $f(x, y)$ и $g(x, y)$, рассматриваемых как полиномы по переменной y

$$\mathcal{X}(x) \stackrel{\text{def}}{=} \mathcal{R}_y \left(f(x, y), g(x, y)\right) \ ,$$

называется **элиминантой системы** (7.4) по x. Аналогично определяется и вторая элиминанта системы

$$\mathcal{Y}(y) \stackrel{\text{def}}{=} \mathcal{R}_x(f(x, y), g(x, y)) \ .$$

Для простоты, мы не учитывали здесь (и не будем учитывать в последующих примерах) знак $(-1)^{n(n-1)/2}$ в выражениях обеих элиминант.

Теорема 8.1. *Пусть выполнено условие* (8.2). *Если пара* (α, β) *является решением* (7.4), *то необходимо, чтобы* $\mathcal{X}(\alpha) = 0$ *и* $\mathcal{Y}(\beta) = 0$.

Таким образом, решение системы (7.4) сводится к решению одного уравнения от одной переменной: $\mathcal{X}(x) = 0$ (или $\mathcal{Y}(y) = 0$). Говорят, что другая переменная исключена. Поэтому и соответствующий раздел алгебры называется **теорией исключения**.

Пусть теперь $x = \alpha$ — произвольный корень $\mathcal{X}(x)$: $\mathcal{X}(\alpha) = 0$. Тогда выполнено условие (8.3), а значит, $f(\alpha, y)$ и $g(\alpha, y)$ как полиномы от y имеют хотя бы один общий корень β.

Теорема 8.2. *Пусть выполнено условие* (8.2). *Тогда для любого корня* α *элиминанты* $\mathcal{X}(x)$ *существует хотя бы одно значение* $y = \beta$ *такое, что пара* (α, β) *оказывается решением* (7.4).

Пример 8.1. *Решить систему уравнений*

$$\begin{cases} f(x, y) = 4\,x^2 - 7\,xy + y^2 + 13\,x - 2\,y - 3 = 0 \ , \\ g(x, y) = 9\,x^2 - 14\,xy + y^2 + 28\,x - 4\,y - 5 = 0 \ . \end{cases}$$

Решение. Составим элиминанту $\mathcal{X}(x)$:

$$\begin{aligned} f(x, y) &= y^2 + (-7\,x - 2)y + (4\,x^2 + 13\,x - 3) \ , \\ g(x, y) &= y^2 + (-14\,x - 4) + (9\,x^2 + 28\,x - 5) \ , \end{aligned}$$

$$\mathcal{X}(x) = \begin{vmatrix} 1 & -7x - 2 & 4x^2 + 13x - 3 & 0 \\ 0 & 1 & -7x - 2 & 4x^2 + 13x - 3 \\ 0 & 1 & -14x - 4 & 9x^2 + 28x - 5 \\ 1 & -14x - 4 & 9x^2 + 28x - 5 & 0 \end{vmatrix} =$$

$$= 24(x^4 - x^3 - 4x^2 + 4x) \ .$$

Найдем ее корни: $\alpha_1 = 0, \alpha_2 = 1, \alpha_3 = 2, \alpha_4 = -2$.

Итак, найдены x-компоненты решений системы. Как найти их y-компоненты? Можно построить вторую элиминанту $\mathcal{Y}(y)$, отыскать ее корни, составить всевозможные пары из корней $\mathcal{X}(x)$ и $\mathcal{Y}(y)$, подставить их в $f(x,y)$ и $g(x,y)$ и проверить на равенство нулю. Либо же найденный корень $x = \alpha$ подставить в одно из уравнений: $f(\alpha, y) = 0$, решить его относительно y, и каждую полученную таким образом пару подставить в $g(x,y)$; хотя бы одна из них должна удовлетворить уравнению $g(x,y) = 0$. На этих путях нас ожидает следующее препятствие: *как правило*, корни элиминант невозможно установить **точно**; погрешность же вычислений может повлечь ошибку при выявлении истинной пары (α, β).

Хотелось бы минимизировать использование численных методов. Удовлетворить это желание поможет один из результатов первой части. Вспомним, что при $x = \alpha$ полиномы $f(\alpha, y)$ и $g(\alpha, y)$ имеют общий корень, а, следовательно, существует нетривиальный $\mathsf{НОД}\,(f(\alpha,y), g(\alpha,y))$. Степень этого $\mathsf{НОД}$ и его аналитическое выражение через коэффициенты полиномов $f(\alpha, y)$ и $g(\alpha, y)$ можно найти с помощью теории субрезультантов.

Так, если первый субрезультант полиномов $f(\alpha, y)$ и $g(\alpha, y)$ не обращается в нуль: $\mathcal{R}^{(1)}(\alpha) \neq 0$, то $\mathsf{НОД}$ будет первой степени и его выражение[6]:

$$\mathcal{R}^{(1)}(\alpha) y + \det M_1^{(1)}(\alpha) \ . \tag{8.5}$$

Для нашего примера

$$\begin{vmatrix} 1 & -7x-2 \\ 1 & -14x-4 \end{vmatrix} y + \begin{vmatrix} 1 & 4x^2+13x-3 \\ 1 & 9x^2+28x-5 \end{vmatrix} = (-7x-2)y + (5x^2+15x-2) \ ,$$

$\mathcal{R}^{(1)}(x) = -7x - 2 \neq 0$ при $x = 0, 1, 2, -2$. Следовательно, соответствующие этим корням значения y находятся по формуле (3.3):

$$y = -\det M_1^{(1)}(x) / \mathcal{R}^{(1)}(x) \ . \tag{8.6}$$

Ответ. Решения системы: $(1,2)$; $(2,3)$; $(0,-1)$; $(-2,1)$.

Теорема 8.3. *При выполнении условий* (8.2) *и*

$$\mathcal{R}(\mathcal{X}(x), \mathcal{R}^{(1)}(x)) \neq 0 \tag{8.7}$$

система (7.4) *может быть сведена к эквивалентной ей (т.е. имеющей такое же множество решений) системе*

$$\mathcal{X}(x) = 0, \quad \mathcal{R}^{(1)}(x) y + \det M_1^{(1)}(x) = 0 \ . \tag{8.8}$$

Действительно, условие (8.7) эквивалентно тому, что $\mathcal{X}(x)$ и $\mathcal{R}^{(1)}(x)$ не имеют общих корней и, следовательно, $\mathcal{R}^{(1)}(\alpha) \neq 0$.

Что происходит при нарушении условия (8.7)?

[6] См. теорему 3.3.

Пример 8.2. *Решить систему уравнений*

$$\left\{\begin{array}{l} f(x,y) = x^3 - 2x^2y - 4xy^2 + 2y^3 + 6x^2 + 12xy - 16x - 8y = 0 \ , \\ g(x,y) = -3x^3 - 4x^2y - 3xy^2 + 4y^3 + 2x^2 + 24xy - 10y^2 - 12x - 16y + 40 = 0 \ . \end{array}\right.$$

Решение. Найдем элиминанту $\mathcal{X}(x)$, первый субрезультант и определитель матрицы $M_1^{(1)}$:

$$\begin{aligned} \mathcal{X}(x) &= -750x^2(3x^7 + 2x^6 - 120x^5 + 112x^4 + 1136x^3 - 2400x^2 + 256x + 1536) = \\ &= -750\,x^2(x + {}^2\!/_3)(x+4)(x-4)(x+6)(x-2)^3 \ , \\ \mathcal{R}^{(1)}(x) &= -1000\,x(x-2)^2, \ \det M_1^{(1)}(x) = 50\,x(x-2)^2(3\,x^2 + 10x + 32) \ . \end{aligned}$$

На корнях $-{}^2\!/_3$, -4, 4, -6 элиминанты $\mathcal{X}(x)$ формула (8.6) дает истинные значения y-компоненты: ${}^4\!/_3$, 2, 6, 4 соответственно.

Однако на корнях $x = 0$ и $x = 2$ имеем $\mathcal{R}^{(1)}(x) = 0$, и формула (8.6) неприменима — хотя формула (8.8) продолжает оставаться справедливой, обращаясь в тождество вида $0 \equiv 0$. (Попытка использования формулы (8.6) после удаления общего множителя $x(x-2)^2$ оканчивается неудачей: так, пара $(90, {}^8\!/_5)$ не является решением системы.)

По-видимому, при этих значениях α полиномы $f(\alpha, y)$ и $g(\alpha, y)$ имеют более одного общего корня, и для нахождения $\mathsf{НОД}\,(f(\alpha,y), g(\alpha,y))$ воспользуемся вторым субрезультантом:

$$\begin{aligned} &\mathcal{R}^{(2)}(x) = 10(x-2), \ \det M_2^{(1)}(x) \equiv 0 \ , \\ &\det M_2^{(2)}(x) = -10(x^3 + 2x^2 - 4x - 8) = -10(x-2)(x+2)^2 \ . \end{aligned}$$

Для соответствующих y-компонент получаем уравнение

$$\mathcal{R}^{(2)}(\alpha)y^2 + \det M_2^{(1)}(\alpha)y + \det M_2^{(2)}(\alpha) = 0 \ . \tag{8.9}$$

Для нашего примера $(\alpha-2)y^2 - (\alpha-2)(\alpha+2)^2 = 0$, и $\mathcal{R}^{(2)}(\alpha) \neq 0$ при $\alpha = 0$; так что для этого значения x уравнение (8.9) дает два верных значения y-компоненты: $y^2 - 4 = 0$. В самом деле, $(0,2)$ и $(0,-2)$ — решения системы. Более того, уравнение (8.9) остается справедливым и на группе решений, полученной на предыдущем этапе. Однако при $\alpha = 2$ оно обращается в тождество вида $0 \equiv 0$ (не помогает даже удаление общего множителя $(x-2)$: точки $(2,4)$ и $(2,-4)$ решениями системы не являются).

По-видимому, при этом α полиномы $f(\alpha, y)$ и $g(\alpha, y)$ имеют более двух общих корней, и для нахождения $\mathsf{НОД}\,(f(\alpha,y), g(\alpha,y))$ следует воспользоваться третьим субрезультантом. Но он не существует (в матрице M вычеркивать нечего). Это неудивительно — $\mathsf{НОД}\,(f(2,y), g(2,y))$ должен иметь степень не меньшую трех, но сами исходные полиномы $f(2,y)$ и $g(2,y)$ — как раз третьей степени

$$f(2,y) = 2(y^3 - 4y^2 + 4y) = 2\,y(y-2)^2, \ g(2,y) = 4(y^3 - 4y^2 + 4y) = 4\,y(y-2)^2 \ ,$$

и их НОД совпадает с любым из них. Следовательно, третью (и последнюю) группу решений составляют пары $(2,0)$ и $(2,2)$, причем $(2,2)$ оказывается *кратным*, так как якобиан (7.5) обращается на нем в нуль. Такое решение будем считать за два.

Геометрический смысл: абсциссе $x = 0$ соответствуют две ординаты точек пересечения кривых $f(x,y) = 0$ и $g(x,y) = 0$: $y = -2$ и $y = 2$. Абсциссе $x = 2$ также соответствуют два значения y: $y = 0$ и $y = 2$. Оказывается, что в точке $(2,2)$ кривые не пересекаются, но соприкасаются (рис. 3).

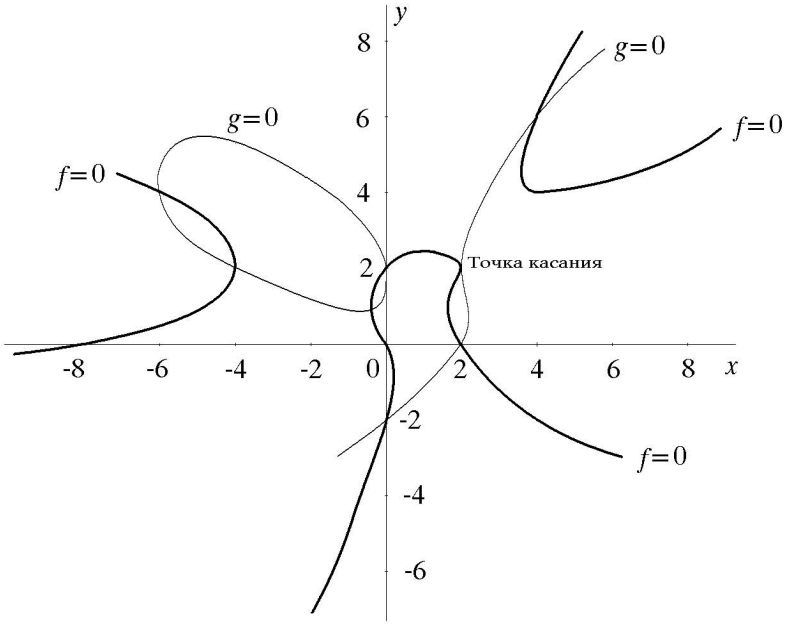

Рис. 3

Ответ. Система имеет 9 решений (с учетом кратностей):

$$(-2/3, 4/3),\ (-4,2),\ (4,6),\ (-6,4),\ (0,2),\ (0,-2),\ (2,0),\ (2,2),\ (2,2)\ .$$

Замечание. В отличие от теоремы 8.3, исходную систему удалось свести к эквивалентной системе, имеющей, однако, бóльшее число уравнений

$$\mathcal{X}(x) = 0;\ \mathcal{R}^{(1)}(x)y + \det M_1^{(1)}(x) = 0\ ;$$
$$\mathcal{R}^{(2)}(x)y^2 + \det M_2^{(1)}(x)y + \det M_2^{(2)}(x) = 0; \ldots \qquad (8.10)$$

Структура системы (8.10): первое уравнение от y не зависит; второе — зависит линейно; третье — квадратично и т.д.

Упражнение 8.1. *Решить системы уравнений*

$$a) \qquad x^2 + y^2 - 3x - y = 0\ ,$$

$$-x^2 - 6xy + y^2 + 7x + 11y - 12 = 0 \ ;$$

б) $5x^2 - 6xy + 5y^2 - 16 = 0 \ ,$
$2x^2 - xy + y^2 - x - y - 4 = 0 \ ;$

в) $11x^2 + 36xy + 30y^2 - 14x - 24y = 0 \ ,$
$10x^2 + 28xy + 19y^2 - 8x - 10y = 0 \ ;$

г) $3x^2 + 4xy - 2y^2 + 6x + 24y - 24 = 0 \ ,$
$8x^2 + 20xy + 11y^2 - 12x - 6y - 8 = 0 \ ;$

д) $2x^2 + 10xy + 13y^2 - 2x - 4y + 1 = 0 \ ,$
$x^2 + 2xy - y^2 - 4x - 8y - 1 = 0 \ ;$

е) $4x^2 - 7xy + y^2 + 28x - 11y + 24 = 0 \ ,$
$9x^2 - 14xy + y^2 + 60x - 20y + 51 = 0 \ ;$

ж) $x^2 + xy + y^2 - 2x - 4y + 3 = 0 \ ,$
$x^3 + y^3 - x^2 + xy - 5y^2 - 5x + 7y - 3 = 0 \ ;$

з) $x^3 - 3xy^2 - 4x^2 + 4y^2 + 6x - 4 = 0 \ ,$
$y^3 - 3x^2y + 8xy - 6y = 0 \ .$

Упражнение 8.2. *Найти приближенные решения систем*

а) $x^2 + y^2 - 6x = 0 \ ,$
$2\,y^3 - 6\,xy^2 + 8\,y^2 + 9\,x - 9\,y = 0 \ ;$

б) $x^2 - 2\,y^2 - 2\,x + 3\,y - 1 = 0 \ ,$
$x^3 + 3\,x^2y - 2\,xy^2 - 4\,y^3 + 12\,x^2 - xy + 4\,y^2 - 2\,x + 3\,y - 11 = 0 \ ;$

в) $2\,x^2 + 3\,y^2 - x + 3\,y - 1 = 0 \ ,$
$x^3 + 3\,x^2y - 5\,xy^2 - 4\,y^3 + 12\,x^2 - xy + 4\,y^2 - 2\,x + 3\,y - 11 = 0$

с точностью до 10^{-3}.

9 Теорема Безу

Каково общее число решений системы (7.4)? На основании теорем 8.1 и 8.2 видим, что оно совпадает с $\deg \mathcal{X}(x)$ (если принимать во внимание все корни последнего, включая невещественные и кратные с учетом кратности).

Теорема 9.1 (Безу). *Пусть выполнено условие* (8.2). *Тогда, как правило*

$$\deg \mathcal{X}(x) = \deg f(x,y) \cdot \deg g(x,y) = nm \ . \tag{9.1}$$

Доказательство приведем для случая $n = 3$ и $m = 2$.

$$f(x,y) = A_0y^3 + A_1(x)y^2 + A_2(x)y + A_3(x)\ ,$$
$$g(x,y) = B_0y^2 + B_1(x)y + B_2(x)\ ,$$

$$\mathcal{X}(x) = \begin{vmatrix} A_0 & A_1(x) & A_2(x) & A_3(x) & \\ & A_0 & A_1(x) & A_2(x) & A_3(x) \\ & & B_0 & B_1(x) & B_2(x) \\ & B_0 & B_1(x) & B_2(x) & \\ B_0 & B_1(x) & B_2(x) & & \end{vmatrix}\ .$$

Здесь

$$A_0 = a_{03}, B_0 = b_{02}; \deg A_j(x) \le j;\ \deg B_j(x) \le j\ \ (j = 1,2,3)\ .$$

Старший моном $\mathcal{X}(x)$ образуется из старших мономов элементов определителя. Выделим их

$$\begin{array}{ll} A_0 = a_{03}; & B_0 = b_{02}\ ; \\ A_1(x) = a_{12}x + \ldots; & B_1(x) = b_{11}x + \ldots\ ; \\ A_2(x) = a_{21}x^2 + \ldots; & B_2(x) = b_{20}x^2 + \ldots\ ; \\ A_3(x) = a_{30}x^3 + \ldots & \end{array}\ .$$

Следовательно,

$$\mathcal{X}(x) = \begin{vmatrix} a_{03} & a_{12}x & a_{21}x^2 & a_{30}x^3 & \\ & a_{03} & a_{12}x & a_{21}x^2 & a_{30}x^3 \\ & & b_{02} & b_{11}x & b_{20}x^2 \\ & b_{02} & b_{11}x & b_{20}x^2 & \\ b_{02} & b_{11}x & b_{20}x^2 & & \end{vmatrix} + \ldots\ ,$$

и нам осталось извлечь степень x из первого определителя. Проделаем это с помощью процедуры, которую можно обобщить на случай произвольных полиномов $f(x,y)$ и $g(x,y)$: домножим вторую и четвертую строки на x, третью — на x^2:

$$= \frac{1}{x^4} \begin{vmatrix} a_{03} & a_{12}x & a_{21}x^2 & a_{30}x^3 & \\ & a_{03}x & a_{12}x^2 & a_{21}x^3 & a_{30}x^4 \\ & & b_{02}x^2 & b_{11}x^3 & b_{20}x^4 \\ & b_{02}x & b_{11}x^2 & b_{20}x^3 & \\ b_{02} & b_{11}x & b_{20}x^2 & & \end{vmatrix} + \ldots$$

Столбцы делятся на $\begin{array}{cccc} \uparrow & \uparrow & \uparrow & \uparrow \\ x & x^2 & x^3 & x^4 \end{array}$

Выносим указанные множители из определителя

$$= \frac{x^{1+2+3+4}}{x^4} \begin{vmatrix} a_{03} & a_{12} & a_{21} & a_{30} & \\ & a_{03} & a_{12} & a_{21} & a_{30} \\ & & b_{02} & b_{11} & b_{20} \\ & b_{02} & b_{11} & b_{20} & \\ b_{02} & b_{11} & b_{20} & & \end{vmatrix} + \ldots =$$

$$= x^6\mathcal{R}(a_{03}y^3 + a_{12}y^2 + a_{21}y + a_{30}, b_{02}y^2 + b_{11}y + b_{20}) + \dots$$

А для произвольных m и n получим

$$\mathcal{X}(x) = \mathcal{A}_0x^{nm} + \mathcal{A}_1x^{nm-1} + \dots + \mathcal{A}_{nm} \tag{9.2}$$

и аналогично

$$\mathcal{Y}(y) = \mathcal{B}_0y^{nm} + \mathcal{B}_1y^{nm-1} + \dots + \mathcal{B}_{nm}$$

при

$$\mathcal{A}_0 \stackrel{\text{def}}{=} \mathcal{R}(f_n(1,y), g_m(1,y)) \text{ и } \mathcal{B}_0 \stackrel{\text{def}}{=} \mathcal{R}(f_n(x,1), g_m(x,1)) \ . \tag{9.3}$$

Упражнение 9.1. *Доказать, что старшие коэффициенты $\mathcal{X}(x)$ и $\mathcal{Y}(y)$ совпадают с точностью до знака.*

Подсказка. Воспользоваться результатом примера 1.3.

Упражнение 9.2. *Доказать, что*

$$\mathcal{A}_{nm} = \mathcal{R}(f(0,y), g(0,y)) \text{ и } \mathcal{B}_{nm} = \mathcal{R}(f(x,0), g(x,0)) \ .$$

Замечание. Итак, мы выяснили смысл выражения "*как правило*" из формулировки теоремы Безу: если число $\mathcal{A}_0$, определяемое формулой (9.3), отлично от нуля. Подчеркнем, что это число зависит только от старших форм (8.1) в разложениях $f(x,y)$ и $g(x,y)$.

Упражнение 9.3. *Установить структуру множества решений системы* (7.4) *при*

$$f(x,y) \stackrel{\text{def}}{=} \prod_{j=1}^{n}(a_jx + b_jy + c_j), \ g(x,y) \stackrel{\text{def}}{=} \prod_{k=1}^{m}(A_kx + B_ky + C_k) \ .$$

При каком условии система имеет бесконечное множество решений?

⊖ Замечание. Упражнения 7.5 и 9.3 позволяют дать следующую геометрическую интерпретацию теоремы Безу. Алгебраические кривые $f(x,y) = 0$ и $g(x,y) = 0$ можно рассматривать как сильно деформированные семейства прямых, причем если в произвольной ограниченной области плоскости деформация еще заметна, то на бесконечности кривые продолжают вести себя "почти как прямые". Теорема Безу утверждает, что число точек пересечения алгебраических кривых остается инвариантным при деформации этих кривых — по крайней мере, до тех пор, пока асимптоты не станут параллельными.

Упражнение 9.4.[6] **Касательной нормалью** *гладкой кривой* K *на плоскости (x,y) назовем прямую, касательную кривой* K *в одной точке и одновременно перпендикулярную ей в другой. Установить максимально возможное число касательных нормалей графика $y = f(x)$, где $f(x) \in \mathbb{R}[x], \deg f > 2$.*

[6] Задача E2886 из журнала American Mathematical Monthly, T.91, №5, 1984.

10 Исключительные случаи теории исключения

Нас будут интересовать случаи, когда либо обращается в нуль числа (9.3), либо нарушаются условия (8.2).

I. Пусть $\mathcal{A}_0 = \mathcal{R}(f_n(1,y), g_m(1,y)) = 0$**.** Возможны следующие случаи:

а) Число решений системы понижается.

Пример 10.1. *Решить систему уравнений*

$$\begin{cases} f(x,y) = x^3 + 3x^2y + 3xy^2 + y^3 - yx - y^2 + x + 2y = 0 \ , \\ g(x,y) = x^2 + 2xy + y^2 - y = 0 \ . \end{cases}$$

Решение. Элиминанты этой системы имеют степени меньшие, чем оценка Безу:

$$\mathcal{X}(x) = x(x+2),\ \mathcal{Y}(y) = y(y-1), \quad \deg \mathcal{X} = \deg \mathcal{Y} = 2 < mn = 6 \ .$$

Действуя согласно алгоритму §8 , получаем систему в виде двух уравнений

$$\mathcal{X}(x) = 0, \quad -2y - x = 0,$$

эквивалентную исходной. Последняя имеет два решения: $(0,0), (-2,1)$. $\triangle$

Теорема 10.1. *Пусть* $\deg(\mathsf{НОД}\,(f_n(1,y), g_m(1,y))) = d$*. Тогда число решений системы уменьшается по крайней мере на* d*.*

Теорема дает лишь достаточное условие понижения степени, как видно из примера 10.1 или 10.2.

Пример 10.2. *Решить систему уравнений*

$$\begin{cases} f(x,y) = x^2 - 4xy + 3y^2 - \dfrac{3}{13}x + \dfrac{45}{13}y + \dfrac{126}{169} = 0 \ , \\ g(x,y) = x^2 - xy - 6y^2 + \dfrac{16}{13}x + \dfrac{42}{13}y + \dfrac{1266}{169} = 0 \ . \end{cases}$$

Решение. Здесь

$$\mathcal{X}(x) = \frac{378}{169}\left(-6\,x^2 + \frac{8701}{13}x + \frac{726}{169}\right) \ ,$$

и хотя $\deg \mathcal{X}$ понижается на 2 по отношению к оценке Безу, при

$$\mathcal{A}_0 = \mathcal{R}(f_n(1,y), g_m(1,y)) = \mathcal{R}(1 - 4y + 3y^2, 1 - y - 6y^2) = 0 \ ,$$

тем не менее, $\mathcal{R}^{(1)}(f_n(1,y), g_m(1,y)) \neq 0$. На понижение степени элиминанты здесь влияют младшие формы разложений $f(x,y)$ и $g(x,y)$.

Ответ. Система имеет 2 решения:

$$\left(\frac{11}{156}(791 \pm 5\sqrt{25033}),\ \frac{1}{156}(2869 \pm 19\sqrt{25033})\right) \ .$$

Заметим, что для этой системы свободные члены в разложениях $f(x,y)$ и $g(x,y)$ не влияют на число решений, но влияют на их вид.

Пример 10.3. *Решить систему уравнений*

$$\begin{cases} f(x,y) = x^2 - 4\,xy + 3\,y^2 - \dfrac{3}{13}x + \dfrac{45}{13}y = 0 \ , \\ g(x,y) = x^2 - xy - 6y^2 + \dfrac{16}{13}x + \dfrac{42}{13}y = 0 \ . \end{cases}$$

Решение. Здесь

$$\mathcal{X}(x) = \frac{81}{169}\left(606x^2 - \frac{4136}{13}x\right) \ .$$

Ответ. Система имеет 2 решения:

$$(0,0),\ \left(\frac{2068}{3939}, -\frac{893}{3939}\right) \ .$$

б) Число решений становится бесконечным.

Пример 10.4. *Решить систему уравнений*

$$\begin{cases} f(x,y) = x^2 - 2xy + y^2 - 1 = 0 \ , \\ g(x,y) = x^2 - y^2 + 2x + 1 = 0 \ . \end{cases}$$

Решение. Здесь $\mathcal{X}(x) \equiv 0,\ \mathcal{Y}(y) \equiv 0$. Алгоритм из §8 дает систему

$$0 = 0,\ (-x)y + (x^2 + x) = 0,\ g(x,y) = 0 \ ,$$

которая имеет бесконечное множество решений: $(\alpha, \alpha+1)$ при любом $\alpha \in \mathbb{C}$ и дополнительно точку $(0,-1)$.

Геометрический смысл: алгебраические кривые $f(x,y)=0$ и $g(x,y)=0$ имеют общую ветвь — прямую $y = x + 1$. $\triangle$

в) Система решений не имеет (несовместна).

Пример 10.5. *Решить систему уравнений*

$$f(x,y) = x^2 - y^2 + 1 = 0,\ g(x,y) = x - y = 0\ .$$

Решение. Здесь $\mathcal{X}(x) \equiv 3 \neq 0$ ни при одном $x \in \mathbb{C}$.
Ответ. Система несовместна.

Рассмотренными примерами исчерпываются все возможные случаи для числа решений системы (7.4): оно либо бесконечно, либо не превосходит mn.

II. Пусть нарушено условие (8.2).

Чисто формально это может привести к невозможности конструкции $\mathcal{X}(x)$ по формуле (8.4): если $a_{0n} = b_{0m} = 0$, то $\mathcal{X}(x) \equiv 0$. В этом случае степени полиномов $f(x,y)$ и $g(x,y)$, рассматриваемых как полиномы от y, становятся меньшими, чем n и m соответственно. Это обстоятельство необходимо учитывать при построении результанта в виде определителя матрицы M, так как ее порядок должен понизиться.

Пример 10.6. *Решить систему уравнений*

$$f(x,y) = xy - 1 = 0,\ g(x,y) = x^2 + 2xy - 1 = 0\ .$$

Решение. Вычисляя $\mathcal{R}_y(f,g)$ как результант полиномов первой степени, запишем:

$$\mathcal{X}(x) = x(x^2+1)\ \Rightarrow\ \alpha_1 = 0, \alpha_{2,3} = \pm\boldsymbol{i}\ .$$

Однако $\alpha_1 = 0$ не соответствует ни одному решению: $f(0,y) = g(0,y) = -1 \neq 0$. Только значения $\alpha_{2,3}$ определяют решения системы: им соответствуют $\beta_{2,3} = \mp\boldsymbol{i}$. В объяснение факта появления "лишнего" корня у элиминанты обратим внимание на то, что при $x = 0$ степени полиномов f и g понижаются, и этот эффект проявляется при построении элиминанты в виде определителя матрицы M. Заметим, что вторая элиминанта $\mathcal{Y}(y) = y^2+1$ не имеет "лишнего" корня.

Ответ. Система имеет 2 решения: $(\pm\boldsymbol{i}\,, \mp\boldsymbol{i}\,)$.

Пример 10.7. *Решить систему уравнений*

$$f(x,y) = xy - 1 = 0,\ g(x,y) = x^2y + x - 2 = 0\ .$$

Решение. Каждая из элиминант этой системы

$$\mathcal{Y}(y) = -2y(y-1),\ \mathcal{X}(x) = 2x(x-1)$$

имеет "лишний" корень, в результате порождается "ложное" решение $(0,0)$. Причина эффекта та же, что и в предыдущем примере. Единственным решением системы будет $(1,1)$. $\triangle$

Для контроля подобных случаев необходимо проверять подозрительные значения переменных, т.е. те из них, которые понижают степени исходных уравнений.

Пример 10.8. *Решить систему уравнений*

$$\left\{\begin{array}{l} f(x,y) = y^2x^2 - xy^2 - 2\,y^2 + yx^3 + 2\,x^2y + 3\,xy + 2\,x - 4\,y + 10 = 0\ , \\ g(x,y) = x^2y - 3\,xy + 2\,y + 2\,x^3 - 6 = 0\ . \end{array}\right.$$

Решение. Раскладываем полиномы системы по степеням y

$$\begin{array}{rcl} f(x,y) & = & (x^2 - x - 2)y^2 + (x^3 + 2\,x^2 + 3\,x - 4)y + 2\,x + 10\ , \\ g(x,y) & = & (x^2 - 3\,x + 2)y + 2\,x^3 - 6 \end{array}$$

и составляем элиминанту по x:

$$\begin{array}{rcl} \mathcal{X}(x) & = & 2\,x^8 - 2\,x^7 - 6\,x^6 + 2\,x^5 - 20\,x^4 + 24\,x^3 + 88\,x^2 - 40\,x - 80 = \\ & = & 2\,(x-2)(x+1)(x^2-2)(x^4+x^2-10)\ . \end{array}$$

Ищем подозрительные корни $\mathcal{X}(x)$:

$$\mathsf{НОД}\ \big(\mathcal{X}(x), (x^2 - x - 2)\big) = x^2 - x - 2 = (x-2)(x+1)\ .$$

Итак, при $x = -1$ и $x = 2$ степень полинома $f(x,y)$ по y понижается. Поскольку $f(-1,y) = -6\,y + 8$, $g(-1,y) = 6\,y - 8$, то корню $x = -1$ соответствует решение системы $(-1,\,4/3)$. Что же касается корня $x = 2$, то здесь ситуация иная: $f(2,y) = 18\,y + 14$, $g(2,y) = 10$ и система несовместна.

Ответ. Решения системы:

$$(-1,\,4/3);\ (\pm\sqrt{2}, \mp\sqrt{2});$$

$$\left(\pm 1/2\sqrt{-2 + 2\sqrt{41}};\, 3/4\sqrt{41} + 9/4 \pm 1/4\sqrt{242 + 38\sqrt{41}}\right)\ ;$$

$$\left(\pm 1/2\,\boldsymbol{i}\ \sqrt{2 + 2\sqrt{41}},\ -3/4\,\sqrt{41} + 9/4 \pm \boldsymbol{i}\ 1/4\sqrt{-242 + 38\sqrt{41}}\right)\ .$$

Упражнение 10.1. *Решить системы уравнений*

а) $\begin{array}{l} x^2 + y^2 - 9 = 0\ , \\ x^2 + y^2 + 2x - y - 3 = 0\ ; \end{array}$

б) $\begin{array}{l} 2x^2 - 3xy + y^2 + 4x - 4 = 0\ , \\ -x^2 + y^2 - 2x - 3y + 5 = 0\ ; \end{array}$

в) $5x^2 - 5y^2 - 3x + 9y = 0\ ,$

$$5x^3+5y^3-15x^2-13xy-y^2=0\ ;$$

г) $$3x^3+9x^2y+9xy^2+3y^3+2x^2-4xy+2y^2-5=0\ ,$$
$$4x^3+12x^2y+12xy^2+4y^3-x^2+2xy-y^2-3=0\ ;$$

д) $$x^3+2x^2y+2xy^2-4xy+y^2-4=0\ ,$$
$$x^2+2yx+2y^2-5y+2=0\ ;$$

е) $$xy-1=0\ ,$$
$$x^3+x^2y+x-3=0\ .$$

11 Замечания

11.1 Об эквивалентных системах

В §8 мы строили системы, эквивалентные исходной системе (7.4). Эти эквивалентные системы имели специальный вид (8.10): первое уравнение зависело только от x, второе зависело от y линейно, возможное третье — квадратично, и т.д. Нас теперь интересует вопрос о единственности системы такого вида, эквивалентной исходной.

Обратимся к примеру 8.1. Эквивалентная система была найдена в следующем виде:

$$\mathcal{X}(x)/24=x^4-x^3-4x^2+4x=0,\ (-7x-2)y+(5x^2+15x-2)=0\ ,$$

и поскольку выполнено условие (8.7), то можно воспользоваться формулой (8.6) для получения y-компоненты:

$$y=\frac{5x^2+15x-2}{7x+2}\ . \tag{11.1}$$

Воспользуемся теперь результатами §6.1. По теореме 6.1, на корнях $\mathcal{X}(x)$ дробь (11.1) будет принимать такие же значения, что и некоторый полином $G(x)$, при этом $G(x)$ можно подобрать степени меньшей $\deg\mathcal{X}$. Построим такой полином по алгоритму теоремы 6.1:

$$\mathcal{R}(x^4-x^3-4\,x^2+4\,x,\ 7\,x+2)=-3456\ ,$$

$$\tilde{u}(x)=\begin{vmatrix} 1 & -1 & -4 & 4 & 0\\ 0 & 0 & 0 & 7 & 1\\ 0 & 0 & 7 & 2 & x\\ 0 & 7 & 2 & 0 & x^2\\ 7 & 2 & 0 & 0 & x^3 \end{vmatrix}=-343\,x^3+441\,x^2+1246\,x-1728\ .$$

Остаток от деления $\tilde{u}(x)(5x^2+15x-2)$ на $x^4-x^3-4x^2+4x$ равен

$$2016x^3-2592x^2-9792x+3456$$

и $G(x)$ отличается от него только на множитель $-1/3456$. Итак, еще одной системой, эквивалентной исходной, будет

$$x^4-x^3-4x^2+4x=0,\ y+(7x^3-9x^2-34x+12)/12=0\ .$$

Теорема 11.1. *При выполнении условия* (8.7) *существует полиномиальная система уравнений вида*

$$\mathcal{X}(x)=0,\ y-G(x)=0\quad(\deg G(x)<\deg\mathcal{X})\ , \tag{11.2}$$

эквивалентная исходной системе (7.4).

Замечание. Условие (8.7) будет выполнено, если $\mathcal{X}(x)$ не имеет кратных корней, т.е.

$$\mathcal{D}(\mathcal{X})\neq 0\ \Rightarrow\ \mathcal{R}(\mathcal{X}(x),\mathcal{R}^{(1)}(x))\neq 0$$

(обратное, вообще говоря, неверно). При этом условии все решения системы различны и имеют различные x-компоненты.

11.2 О проблеме двумерной интерполяции

Задача. Построить полином $f(x,y)\in\mathbb{C}[x,y]$ по его значениям на конечном наборе точек: $f(x_1,y_1)=z_1,\dots,f(x_N,y_N)=z_N$.

Задача аналогична одномерной, однако ее решение в двумерном случае имеет одну особенность. Известно, что коэффициенты полинома $f(x)\in\in\mathbb{C}[x]$ степени не выше, чем n, однозначно восстанавливаются по значениям этого полинома в произвольном наборе из $(n+1)$-й точки (узлах интерполяции) $x_1,\dots,x_{n+1}\,(x_j\neq x_k)$. Полином $f(x,y)$ третьей степени определяется своими 10 коэффициентами (см. упражнение 7.1). По аналогии с одномерным случаем, можно было бы ожидать, что задание этого полинома его значениями в 9 произвольных узлах всегда позволит установить его коэффициенты, причем бесконечным числом способов. Эти ожидания, однако, опровергаются примером.

Пример 11.1. *Построить полином $f(x,y)$ третьей степени такой, что*

$$f(0,0)=0, f(1,1)=z_2, f(-2,1)=z_3, f(3,2)=z_4, f(6,5)=z_5, f(-3,-7)=z_6\ ,$$

$$f(2,-4)=z_7, f(-2,-1/2)=z_8, f\left(\frac{82110385798}{32539385899},\frac{36830918404}{32539385899}\right)=z_9\ .$$

Решение. В каноническом представлении полинома $f(x,y)$ имеется 10 коэффициентов, которые мы считаем неопределенными и ищем из заданных условий. Разрешая получающуюся систему из 9 линейных уравнений относительно этих коэффициентов, мы приходим к ответу: матрица системы имеет ранг 7, т.е., согласно теореме Кронекера–Капелли, сама система будет совместной только при дополнительном условии "связи" величин $z_2, \ldots, z_9$. Именно, последние должны удовлетворять определенному линейному соотношению

$$p_2 z_2 + \ldots + p_9 z_9 = 0$$

при целых $p_2, \ldots, p_9$ (мы не указываем эти числа ввиду их громоздкости). Таким образом, в общем случае поставленная задача неразрешима (например, она не имеет решения при $z_2 = \ldots = z_9 = 1$).

При $z_2, \ldots, z_9$, удовлетворяющих упомянутому уравнению "связи", поставленная задача имеет решение. Однако, оно неединственно в силу все той же теоремы Кронекера–Капелли, поскольку число совместных линейных уравнений меньше числа определяемых ими коэффициентов.

Как удалось подобрать узлы настолько "неудачные" для задачи интерполяции? Как раз с помощью теории исключения. Эти узлы были взяты как точки пересечения двух кривых третьего порядка (кубик)

$$241\,x^3 - 1659\,x^2 y - 6043\,xy^2 + 6300\,y^3 + 1633\,x^2 - 6592\,xy + 23100\,y^2 + 11886\,x - 28866\,y = 0$$

и

$$3814\,x^3 - 3814\,x^2 y + 4493\,xy^2 - 4112\,y^3 - 2040\,x^2 + 4195\,xy - 15550\,y^2 - 25984\,x + 38998\,y = 0\ .$$

Согласно теореме 9.1 (Безу), две такие кривые пересекаются в 9 точках[8]. Система из 9 линейных уравнений для определения 10 коэффициентов интерполяционного полинома при $z_2 = \ldots = z_9 = 0$ становится однородной. Поскольку она имеет 2 линейно независимых набора решений, то ранг ее матрицы должен быть не выше 8. Если мы "сдвинем" хоть одно из значений z_j из нуля, то *почти наверняка* соответствующая неоднородная система станет несовместной, а задача интерполяции — неразрешимой. $\triangle$

11.3 Об эквидистанте

Определение. Рассмотрим гладкую кривую K, в каждой ее точке A проведем перпендикуляр и возьмем на этом перпендикуляре точки, находящиеся на некотором фиксированном расстоянии h от точки A. Полученные точки формируют две кривые, каждую из которых назовем **эквидистантой** кривой K и будем обозначать K_{+h} и K_{-h}.

[8] Сложность заключалась лишь в необходимости подобрать коэффициенты этих кубик так, чтобы все точки пересечения оказались с рациональными координатами.

Эквидистанты имеют очевидный физический смысл. Если предположить, что каждая точка кривой является источником излучения, то эквидистанта представляет собой волновой фронт[9].

Задача. Построить уравнение эквидистант графика $y = f(x)$, где $f(x) \in \mathbb{R}[x]$.

Теорема 11.2. *Эквидистанты* K_h *и* K_{-h} *задаются уравнением*

$$\Phi(x,y) = 0, \text{ где } \Phi(x,y) \stackrel{\text{def}}{=} \mathcal{D}_X \left([X-x]^2 + [f(X)-y]^2 - h^2 \right) .$$

Здесь дискриминант берется по переменной X*, в то время как остальные переменные считаются параметрами.*

Доказательство . Пусть точка (x,y) эквидистанты находится на расстоянии h от ближайшей к ней точки $(X, Y = f(X))$ кривой K. Тангенс угла наклона касательной к графику $Y = f(X)$ равен $f'(X)$. Следовательно, по определению эквидистанты, вектор $(X-x, Y-y)$ должен быть перпендикулярен направляющему вектору касательной. Таким образом, получаем систему из трех уравнений

$$(x-X)^2 + (y-Y)^2 = h^2, \; Y = f(X), \; (x-X) + f'(X)(y-Y) = 0 .$$

Среднее из этих условий позволяет исключить переменную Y из первого и третьего уравнения:

$$(x-X)^2 + (y-f(X))^2 - h^2 = 0, \; (x-X) + f'(X)(y-f(X)) = 0 .$$

Теперь для исключения переменной X мы должны были бы составить элиминанту по переменной X. Очевидно, однако, что второе уравнение является (с точностью до множителя) производной первого по X. □

Пример 11.2. *Найти уравнение эквидистант параболы* $y = x^2$*.*

Решение. После вычисления дискриминанта, отбросим общий множитель его коэффициентов и сгруппируем по степеням h:

$$\begin{aligned}
\Phi(x,y) &= \mathcal{D}_X \left(X^4 + (1-2y)X^2 - 2\,xX + x^2 + y^2 - h^2 \right) = \\
&= (16\,y^2 + 16\,x^2 - 8\,y + 1)(y - x^2)^2 + \\
&+ \left[8(-4\,y^2 - 8\,yx^2 - y + 1 - 8\,x^4)(y - x^2) - (4\,x^2 + 1)^3 \right] h^2 + \\
&+ 8\,(2\,y^2 + 4\,y + 6\,x^2 - 1)h^4 - 16\,h^6 \; .
\end{aligned}$$

Уравнение $\Phi(x,y) = 0$ и дает искомые эквидистанты K_h и K_{-h} для параболы $y = x^2$. На рис. 4 показаны эквидистанты параболы для $h = 1$

[9] В предположении изотропности физической среды, из которой состоит плоскость.

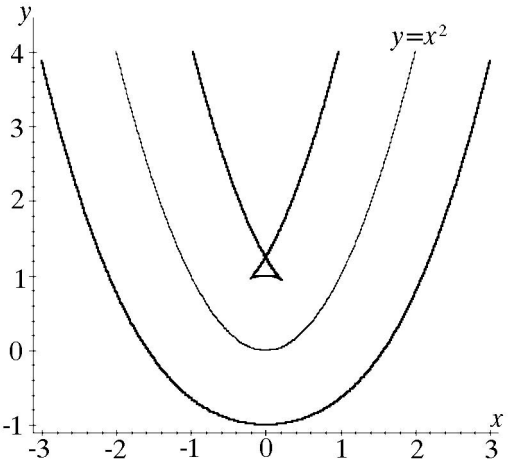

Рис. 4

(чтобы не загромождать график, мы сдвинули координатные оси на несколько единиц). △

Упражнение 11.1. *Рассмотрим снова гладкую кривую* K*, которую теперь — в отличие от только что рассмотренной задачи об эквидистанте — будем считать не источником излучения, а зеркалом.* **Кривой зеркального изображения** *назовем геометрическое место точек, являющихся зеркальными изображениями источника излучения* (x_0, y_0) *относительно касательных к точкам кривой* K*. Доказать, что в случае, когда кривая* K *задана уравнением* $y = f(x)$ *при* $f(x) \in \mathbb{R}[x], \deg f > 1$*, кривая зеркального изображения определяется уравнением* $\Phi(x, y) = 0$*, где*

$$\Phi(x,y) \stackrel{\text{def}}{=} \mathcal{D}_X \left(2X(x-x_0) + 2f(X)(y-y_0) - (x^2 - x_0^2) - (y^2 - y_0^2)\right) \ .$$

Построить это уравнение для $(x_0, y_0) = (0, 0)$*,* $f(x) = x^2 + 1$*.*

12 Заключение

> "Если в задаче меньше трех переменных, это не задача;
> если больше восьми — она неразрешима".
>
> А.Блох. Закон Мерфи. 2003 г.

Настоящее пособие следует рассматривать исключительно только как введение в теорию исключения: фактически, мы наметили только методологию постановок задач и их решений.

Мы укажем здесь несколько направлений, которые мы **не затронули** в настоящем пособии.

В теории исключения наиболее трудной является методология перехода от случая двух переменных к случаю трех переменных. Лежащая "на виду" идея последовательного исключения переменных в системе

$$f_1(x,y,z)=0,\ f_2(x,y,z)=0,\ f_3(x,y,z)=0\ , \tag{12.1}$$

например, по схеме

$$(12.1)\ \Rightarrow\ \left\{\begin{array}{rcl} g_{12}(x,y)\stackrel{\rm def}{=}\mathcal{R}_z(f_1,f_2) &=& 0\\ g_{13}(x,y)\stackrel{\rm def}{=}\mathcal{R}_z(f_1,f_3) &=& 0\end{array}\right.\ \Rightarrow\ h(x)\stackrel{\rm def}{=}\mathcal{R}_y(g_{12},g_{13})=0 \tag{12.2}$$

срабатывает лишь частично: полином $h(x)$ может обладать "посторонними" корнями, т.е. такими, которые не являются компонентами решений исходной системы.

Пример 12.1. *Решить систему уравнений*

$$\left\{\begin{array}{rcl} f_1(x,y,z) &=& x^2-3\,x+y+z+2=0\ ,\\ f_2(x,y,z) &=& x^2+xz+y-1=0\ ,\\ f_3(x,y,z) &=& x^2-x+y-z-2=0\ .\end{array}\right.$$

Решение. Усилим приведенную выше схему составлением всевозможных перекрестных элиминант:

$$\left\{\begin{array}{rcl} g_{12}(y,z) &\stackrel{\rm def}{=}& \mathcal{R}_x(f_1,f_2)=(3+z)^2(y+z)\ ,\\ g_{23}(y,z) &\stackrel{\rm def}{=}& \mathcal{R}_x(f_2,f_3)=(1+z)^2(-z+y)\ ,\\ g_{13}(y,z) &\stackrel{\rm def}{=}& \mathcal{R}_x(f_1,f_3)=4\,y+8\,z+4\,z^2\ ;\end{array}\right.$$

$$\left\{\begin{array}{rcl} h_3(z) &\stackrel{\rm def}{=}& \mathcal{R}_y(g_{13},g_{23})=4\,z(z+1)^2(3+z)\ ,\\ h_1(z) &\stackrel{\rm def}{=}& \mathcal{R}_y(g_{12},g_{13})=4\,z(z+1)(3+z)^2\ ,\\ h_2(z) &\stackrel{\rm def}{=}& \mathcal{R}_y(g_{12},g_{23})=-2\,z(z+1)^2(3+z)^2\ .\end{array}\right.$$

Последние полиномы имеют общий корень $z=0$; однако, легко установить, что при $z=0$ исходная система несовместна.

Ответ. Система имеет два решения: $(1,1,-1),\ (-1,-3,-3)$.

Для оценки возможного числа "посторонних" решений произвольной системы (12.1) воспользуемся трехмерным аналогом теоремы Безу. Именно, утверждается, что число решений системы *как правило* равно произведению степеней входящих в нее уравнений: если $n_j\stackrel{\rm def}{=}\deg f_j$, то это число равно $n_1n_2n_3$. На основании же теоремы 9.1 степень полинома $h(x)$ из схемы (12.2) окажется *как правило* равной $n_1^2n_2n_3$. Итак, если использовать для решения системы схему (12.2), то следует ожидать появления $(n_1^2-n_1)n_2n_3$ "посторонних" корней (при $n_1>1$); проблема их отсеивания представляет отдельную задачу, требующую применения численных методов ...

Итак, добиться успеха "с наскока" не удается и надо приступать к планомерной осаде. Ключевым моментом является понятие двумерного результанта, т.е. полиномиальной функции коэффициентов полиномов $f_1(x,y), f_2(x,y)$ и $g(x,y)$, обращение которой в нуль гарантирует существование общего нуля данных полиномов. Такую функцию можно определить в развитие любого из методов построения результанта, изложенных в первой части, как то: Сильвестра, Кронекера или Безу. Именно, метод Сильвестра развивается в книге [20], метод Кронекера — в статье [24], а Безу — в статье [18]. Обладая конструктивным методом нахождения результанта трех полиномов от двух переменных, мы сможем построить процедуру исключения в системе из трех алгебраических уравнений от переменных x, y и z, аналогичную изложенной в §8 для двумерного случая.

Пример 12.2. *Решить систему уравнений*

$$\left\{\begin{array}{rcl} z^2+zy+y^2-2xz-4yx+3x^2+z+2y-x-2 &=& 0,\\ 2z^2-zy+y^2-xz-yx-6x^2+2z-y+x+2 &=& 0,\\ z^2-2zy-y^2-2xz+2yx+3x^2+2z+3y-3x-1 &=& 0. \end{array}\right.$$

Решение. По методу Безу [18] составляем матрицу $B=[b_{jk}(x)]_{j,k=1}^{4}$, где $b_{jk}(x)\in\mathbb{Q}[x]$. Имеем: $\det B=$

$$=\frac{-1}{49}(869814\,x^7-1156692\,x^6-399400\,x^5+1116418\,x^4-404610\,x^3-93852\,x^2+56816\,x+11506).$$

Корни этого полинома (элиминанты) задают x-компоненты решений системы. Соответствующие им y- и z-компоненты получаются по формулам:

$$\begin{array}{rcl} y &=& \dfrac{6831x^5-18141x^4+1848x^3+16725x^2-5155x-2108}{2277x^4-8581x^3+13522x^2-2995x-2043}\ ,\\ z &=& -\dfrac{13601x^4-34161x^3+17378x^2+1519x-517}{2277x^4-8581x^3+13522x^2-2995x-2043}\ . \end{array}$$

Ответ. Решения системы с точностью до 10^{-5}:

$$(1,0,1)\ ;\ (-0.94428,\,-0.15702,\,-2.42809)\ ;\ (0.74136,\,0.18176,\,-0.97093)\ ;$$

$$(-0.21498\ \pm\ \boldsymbol{i}\ 0.05478,\ 0.67565\ \pm\ \boldsymbol{i}\ 0.33638,-0.21886\ \mp\ \boldsymbol{i}\ 0.65557)\ ;$$

$$(0.48135\ \pm\ \boldsymbol{i}\ 0.39011,\,1.28693\ \mp\ \boldsymbol{i}\ 0.30635,\,0.56791\ \pm\ \boldsymbol{i}\ 1.09756)\ .$$

Мы не указали в настоящем пособии связи задачи исключения переменных с задачей локализации решений алгебраического уравнения или системы уравнений. Дело в том, что каждый метод построения результанта $\mathcal{R}(f,g)$ может быть развит до метода отделения решений алгебраического уравнения [13], [24]. Например, в той же идеологии решается задача установления точного числа вещественных корней полинома $f(x)\in\mathbb{R}[x]$ (см.,

к примеру, упражнение 2.2), а также числа тех из них, что удовлетворяют алгебраическому неравенству $g(x) > 0$.

Мы не указали также связи теории исключения с теорией базисов Грёбнера [7], [8], хотя квалифицированный читатель безусловно заметит, что полиномы системы (11.2) образуют базис Грёбнера радикального нульмерного идеала $\mathcal{I}(f(x,y), g(x,y))$ относительно лексикографического упорядочения $y \succ x$.

Мы не упомянули об аналогии задач преобразования алгебраических уравнений и задач преобразования линейных дифференциальных и разностных уравнений.

Пример 12.3. *Найти условие, при котором два дифференциальных уравнения*

$$\begin{array}{rl} & y''(x) + a_1(x)y'(x) + a_2(x)y(x) + a_3(x) = 0 \\ u & y''(x) + b_1(x)y'(x) + b_2(x)y(x) + b_3(x) = 0 \end{array} \tag{12.3}$$

имеют общее решение.

Решение. Воспользуемся приемом из примера 1.1. Предположим, что существует общее решение этих уравнений: $y = \varphi(x)$; тогда эта функция должна обращать оба уравнения в тождества:

$$\begin{array}{c} \varphi'' + a_1\varphi' + a_2\varphi + a_3 \equiv 0 \ , \\ \varphi'' + b_1\varphi' + b_2\varphi + b_3 \equiv 0 \ . \end{array}$$

Продифференцируем[10] каждое из этих тождеств по x:

$$\begin{array}{c} \varphi''' + a_1\varphi'' + (a_1' + a_2)\varphi' + a_2'\varphi + a_3' \equiv 0 \ , \\ \varphi''' + b_1\varphi'' + (b_1' + b_2)\varphi' + b_2'\varphi + b_3' \equiv 0 \ ; \end{array}$$

и еще один раз:

$$\begin{array}{c} \varphi^{(4)} + a_1\varphi''' + (2a_1' + a_2)\varphi'' + (a_1'' + 2a_2')\varphi' + a_2''\varphi + a_3'' \equiv 0 \ , \\ \varphi^{(4)} + b_1\varphi''' + (2b_1' + b_2)\varphi'' + (b_1'' + 2b_2')\varphi' + b_2''\varphi + b_3'' \equiv 0 \ . \end{array}$$

Теперь объединяем получившиеся тождества в систему, рассматриваемую относительно столбца неизвестных $\left[\varphi^{(4)}(x), \varphi'''(x), \varphi''(x), \varphi'(x), \varphi(x), 1\right]$. Эта система однородна и имеет нетривиальное решение. Следовательно, определитель ее матрицы равен нулю.

[10] Всюду в дальнейшем предполагается, что свойства коэффициентов уравнений обеспечивают выполнимость операций.

Ответ. Для существования общего решения уравнений (12.3) необходимо выполнение условия:

$$\begin{vmatrix} 1 & a_1(x) & 2a_1'(x)+a_2(x) & a_1''(x)+2a_2'(x) & a_2''(x) & a_3''(x) \\ 0 & 1 & a_1(x) & a_1'(x)+a_2(x) & a_2'(x) & a_3'(x) \\ 0 & 0 & 1 & a_1(x) & a_2(x) & a_3(x) \\ 0 & 0 & 1 & b_1(x) & b_2(x) & b_3(x) \\ 0 & 1 & b_1(x) & b_1'(x)+b_2(x) & b_2'(x) & b_3'(x) \\ 1 & b_1(x) & 2b_1'(x)+b_2(x) & b_1''(x)+2b_2'(x) & b_2''(x) & b_3''(x) \end{vmatrix} \equiv 0 \ .$$

Определитель, стоящий в левой части тождества, называется **дифференциальным результантом**.

Монография с изложением затронутого в этом параграфе материала в несколько раз превысит объем настоящего пособия. Авторы имеют намерение подвигнуться на такой труд, но им хотелось бы получить предварительное подтверждение его востребованности... Поэтому авторы с благодарностью воспримут конструктивные предложения и критические замечания, которые просят отправлять им по адресу электронной почты

Alexei.Uteshev@pobox.spbu.ru

или же почты обычной

198504, С.-Петербург, Петродворец,
Университетский пр.35, СПбГУ, факультет ПМ—ПУ.

Приложение.
Полезные функции пакета MAPLE V R6.

Функция **resultant**(f, g, x), где
f, g — полиномы от x;
x — переменная;
возвращает результант полиномов f и g, построенный относительно переменной x.

Функция **discrim**(f, x), где
f — полином от x;
x — переменная;
возвращает дискриминант полинома $f(x)$.

Функция **gcd**(f, g, a, b), где
f, g — полиномы от нескольких переменных над $\mathbb{Q}$;
a, b — необязательные аргументы;
возвращает наибольший общий делитель полиномов f и g.

Необязательные аргументы используются для возврата:
a — $f/\text{НОД}(f, g)$;
b — $g/\text{НОД}(f, g)$.

Специальные функции, упомянутые ниже, являются библиотечными функциями пакета **linalg**. Для их использования нужно выполнять операцию импорта в одной из следующих форм:

with(linalg) — предварительное подключение всего пакета;
linalg[функция](аргументы) — вызов отдельной функции без подключения всего пакета;
with(linalg,функция1,функция2,...) — предварительное подключение функций;
with(linalg,[функция1,функция2,...]) — то же самое в другой форме.

Функция **sylvester**(f, g, x), где
f, g — полиномы от x;
x — переменная;
возвращает матрицу результанта в форме Сильвестра[11] полиномов f и g, построенную относительно переменной x. При этом если степень f по x равна n, а степень g по x равна m, то размерность полученной матрицы будет равна $(n + m)$.

Функция **bezout**(f, g, x), где
f, g — полиномы от x;
x — переменная;
возвращает матрицу Безу[12] полиномов f и g, построенную относительно

[11] См. с. 9.
[12] См. с. 34; по неизвестной причине, разработчики пакета изменили на противоположный порядок формирования столбцов матрицы, в результате чего последняя потеряла свойство симметричности.

переменной x. При этом если степень f по x равна n, а степень g по x равна m, то размерность полученной матрицы будет равна $\max(n, m)$.

Функция **jacobian**(F, X), где

F — вектор или список выражений, состоящий из элементов $f_i(X)$;

X — вектор или список переменных, состоящий из элементов x_j;

возвращает матрицу Якоби[13] выражений F относительно переменных X. При этом элемент j-й строки и k-го столбца этой матрицы равен $\partial f_j / \partial x_k$.

[13] Не якобиан!

Литература

[1] Акритас А. Основы компьютерной алгебры с приложениями. М.Мир,1994

[2] Бохер М. Введение в высшую алгебру. М.-Л. ГТТИ, 1933

[3] Ван-дер-Варден Б.Л. Современная алгебра.Т.2. ОГИЗ, ГИТТЛ, 1947

[4] Джури Э. Инноры и устойчивость динамических систем. М.Наука, 1979

[5] Дэвенпорт Дж., Сирэ И., Турнье Э. Компьютерная алгебра. М.Мир, 1991

[6] Калинина Е.А., Утешев А.Ю. Теория исключения. СПб, СПбГУ, 1997

[7] Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. М.Мир, 2000

[8] Компьютерная алгебра. Символьные и алгебраические вычисления. Под ред. Бухбергер Б.,Коллинз Дж., Лоос Р. М.Мир, 1986

[9] Курош А.Г. Курс высшей алгебры. -М.Наука, 1975

[10] Окунев Л.Я. Высшая алгебра. -М.Учпедгиз, 1958

[11] Окунев Л.Я. Сборник задач по высшей алгебре. -М.Просвещение, 1964

[12] Серре И.А. Курс высшей алгебры. М.-СПб., Вольф, Б.г. (1896?)

[13] Утешев А.Ю., Черкасов Т.М. Локализация решений систем алгебраических уравнений и неравенств. Метод Эрмита.//*ДАН России.* 1996. Т.347. №4. С.451–453

[14] Фаддеев Д.К. Лекции по алгебре. -М.Наука, 1984

[15] Фаддеев Д.К.,Соминский И.С. Сборник задач по высшей алгебре. -М.Наука, 1968

[16] Чезаро Э. Элементарный учебник алгебраического анализа и исчисления бесконечно малых. М.-Л., ОНТИ, 1936

[17] Bézout É. Théorie générale des Équations Algébriques. P.-D. Pierres, Paris. 1779

[18] Bikker P., Uteshev A.Yu. On the Bézout Construction of the Resultant. // *J.Symbolic Computation.* 1999. Т.28. №1. С. 45–88.

[19] Laurent H. L'Élimination, в журнале *Scientia, Phys.-Mathématique.* Т.7. Gauthier–Villars, Paris. 1900

[20] Macaulay F.S. The Algebraic Theory of Modular Systems. Cambridge University Press, Cambridge. 1916

[21] Netto E. Vorlesungen über Algebra. Teubner, Leipzig, T.1. 1896, T.2. 1900

[22] Perron O. Algebra. De Gruyter, Berlin–Leipzig. T. 1. 1932

[23] Pták V. Explicit Expressions for Bezoutians. // *Linear Algebra and its Applications.* T.59. C. 43–54. 1984

[24] Uteshev A.Yu., Cherkasov T.M. The Search for the Maximum of a Polynomial. // *J.Symbolic Computation.* T.25. №5. C. 587–618. 1998

[25] Weber H. Lehrbuch der Algebra. Vieweg, Braunschweig. T.1. 1898

ОГЛАВЛЕНИЕ

Елизавета Александровна Калинина
Алексей Юрьевич Утешев

ТЕОРИЯ ИСКЛЮЧЕНИЯ

Учебное пособие
ЛР №040815 от 22.05.1997

Подписано в печать с оригинала-макета 08.06.2002.
Формат 60x90/16. Печ. л. 4,5. Тираж 150 экз. Заказ №2510

Отпечатано в отделе оперативной полиграфии НИИХ СПбГУ.
198504, С.-Петербург, Старый Петергоф, Университетский пр., 2