В. В. Прасолов

Многочлены

Издание третье,
исправленное

МЦНМО
2003

УДК 512.62
П70
ББК 22.144

Прасолов В. В.

П70 Многочлены. — 3-е изд, исправленное. — М.: МЦНМО, 2003. — 336 с.: ил.

ISBN 5-94057-077-1

В книге изложены основные результаты исследований по теории многочленов, как классические, так и современные. Большое внимание уделено 17-й проблеме Гильберта о представлении неотрицательных многочленов суммами квадратов рациональных функций и ее обобщениям. Теория Галуа обсуждается прежде всего с точки зрения теории многочленов, а не с точки зрения общей теории расширения полей.

Для студентов, аспирантов, научных работников — математиков и физиков.

ББК 22.144

ISBN 5-94057-077-1

Оглавление

Предисловие к первому изданию

Теория многочленов составляет существенную часть университетских курсов алгебры и анализа. Тем не менее, книг, целиком посвященных теории многочленов, чрезвычайно мало.

В этой книге изложены основные результаты исследований по теории многочленов, как классические, так и современные. Большое внимание уделено 17-й проблеме Гильберта о представлении неотрицательных многочленов суммами квадратов рациональных функций и ее обобщениям. Теория Галуа обсуждается прежде всего с точки зрения теории многочленов, а не с точки зрения общей теории полей и их расширений.

В книгу не вошли два важных результата из теории многочленов, изложение которых занимает весьма много места: решение уравнений пятой степени с помощью тэта-функций и классификация коммутирующих многочленов. Эти результаты подробно изложены в двух недавно вышедших книгах, в написании которых я принимал непосредственное участие: [ПрС] и [ПрШ].

Во время работы над этой книгой я получал финансовую поддержку от Российского фонда фундаментальных исследований согласно проекту №98–00–555.

Май 1999 г. *В. Прасолов*

Глава 1
Корни многочленов

1. Неравенства для корней

1.1. Основная теорема алгебры

В те давние времена, когда алгебра была скудна теоремами, следующее утверждение получило название *основной теоремы алгебры*: «*Многочлен степени n с комплексными коэффициентами имеет ровно n корней (с учетом их кратностей)*». Впервые это утверждение сформулировал Альбер де Жирар в 1629 г., но он даже не пытался его доказывать. Первым осознал необходимость доказательства основной теоремы алгебры Даламбер, но его доказательство (1746) не было признано убедительным. Свои доказательства предложили Эйлер (1749), Фонсене (1759) и Лагранж (1771), но и эти доказательства были небезупречны.

Первым удовлетворительное доказательство основной теоремы алгебры получил Гаусс, который привел три разных доказательства (1799, 1815 и 1816), а в 1845 г. опубликовал еще и уточненную версию своего первого доказательства.

Обзор различных доказательств основной теоремы алгебры можно найти в [ТУ]. Мы ограничимся одним доказательством. Оно использует следующую теорему Руше, которая имеет и самостоятельный интерес.

Теорема 1.1 (Руше). Пусть f и g — многочлены и γ — замкнутая несамопересекающаяся кривая на комплексной плоскости. Тогда если

$$\bigl|f(z)-g(z)\bigr| < \bigl|f(z)\bigr| + \bigl|g(z)\bigr| \tag{1}$$

при всех $z \in \gamma$, то внутри кривой γ расположено одинаковое количество корней многочленов f и g (с учетом их кратностей).

Доказательство. Рассмотрим на комплексной плоскости векторные поля $v(z) = f(z)$ и $w(z) = g(z)$. Из условия (1) следует, что ни в какой точке кривой γ векторы v и w не являются противоположно направленными.

Напомним, что *индексом* кривой γ относительно векторного поля v называют количество оборотов вектора $v(z)$ при полном обходе точки z вдоль кривой γ. (Для более подробного знакомства со свойствами индекса мы советуем обратиться к главе 6 книги [Пр1].) Рассмотрим векторное поле $v_t = tv + (1-t)w$. При этом $v_0 = w$ и $v_1 = v$. Ясно также, что

в любой точке $z \in \gamma$ вектор $v_t(z)$ ненулевой. Это означает, что для кривой γ определен индекс $\operatorname{ind}(t)$ относительно векторного поля v_t. Целое число $\operatorname{ind}(t)$ непрерывно зависит от t, поэтому $\operatorname{ind}(t) = \text{const}$. В частности, индексы кривой γ относительно векторных полей v и w совпадают.

Несложно показать, что индекс кривой γ относительно векторного поля v равен сумме индексов *особых* точек, в которых $v(z) = 0$. (Индекс особой точки z_0 определяется как индекс кривой $|z - z_0| = \varepsilon$, где ε достаточно мало.) Для векторного поля $v(z) = f(z)$ индекс особой точки z_0 равен кратности корня z_0 многочлена f. Таким образом, из совпадения индексов кривой γ относительно векторных полей $v(z) = f(z)$ и $w(z) = g(z)$ следует, что внутри кривой γ расположено одинаковое количество корней многочленов f и g. □

С помощью теоремы Руше можно не только доказать основную теорему алгебры, но и получить оценку для модуля любого корня многочлена f.

Теорема 1.2. Пусть $f(z) = z^n + a_1 z^{n-1} + \ldots + a_n$, где $a_i \in \mathbb{C}$. Тогда внутри круга $|z| = 1 + \max\limits_i |a_i|$ расположено ровно n корней многочлена f (с учетом их кратностей).

Доказательство. Пусть $a = \max\limits_i |a_i|$. Многочлен $g(z) = z^n$ имеет внутри рассматриваемого круга корень 0 кратности n. Поэтому достаточно проверить, что если $|z| = 1 + a$, то $\bigl|f(z) - g(z)\bigr| < \bigl|f(z)\bigr| + \bigl|g(z)\bigr|$. Мы даже докажем, что $\bigl|f(z) - g(z)\bigr| < \bigl|g(z)\bigr|$, т. е.

$$|a_1 z^{n-1} + \ldots + a_n| < |z|^n.$$

Ясно, что если $|z| = 1 + a$, то

$$|a_1 z^{n-1} + \ldots + a_n| \leqslant a\bigl(|z|^{n-1} + \ldots + 1\bigr) = a\frac{|z|^n - 1}{|z| - 1} = |z|^n - 1 < |z|^n. \quad \square$$

1.2. Теорема Коши

Здесь мы обсудим теорему Коши о корнях многочленов, а также ее следствия и обобщения.

Теорема 1.3 (Коши). Пусть $f(x) = x^n - b_1 x^{n-1} - \ldots - b_n$, где все числа b_i неотрицательны, причем хотя бы одно из них отлично от нуля. Тогда многочлен f имеет единственный (некратный) положительный корень p, а модули всех остальных корней не превосходят p.

Доказательство. Положим

$$F(x) = -\frac{f(x)}{x^n} = \frac{b_1}{x} + \ldots + \frac{b_n}{x^n} - 1.$$

Если $x \neq 0$, то уравнение $f(x) = 0$ эквивалентно уравнению $F(x) = 0$. При возрастании x от 0 до $+\infty$ функция $F(x)$ строго убывает от $+\infty$ до -1. Поэтому при $x > 0$ функция F обращается в нуль ровно в одной точке p. При этом

$$-\frac{f'(p)}{p^n} = F'(p) = -\frac{b_1}{p^2} - \ldots - \frac{nb_n}{p^{n+1}} < 0.$$

Следовательно, p — некратный корень многочлена f.

Остается доказать, что если x_0 — корень многочлена f, то $q = |x_0| \leqslant p$. Предположим, что $q > p$. Тогда из монотонности функции F следует, что $F(q) < 0$, т. е. $f(q) > 0$. С другой стороны, из равенства $x_0^n = b_1 x_0^{n-1} + \ldots + b_n$ следует, что $q^n \leqslant b_1 q^{n-1} + \ldots + b_n$, т. е. $f(q) \leqslant 0$. Приходим к противоречию. □

Замечание. Теорема Коши непосредственно связана с теоремой Перрона–Фробениуса о неотрицательных матрицах (по этому поводу см. [Wi]).

У многочлена $x^{2n} - x^n - 1$ имеется n корней, модули которых равны модулю положительного корня этого многочлена. Поэтому в теореме Коши утверждение о том, что модули корней не превосходят p, вообще говоря, нельзя заменить на утверждение о том, что модули корней строго меньше p. Но, как показал Островский, в достаточно общей ситуации это можно сделать.

Теорема 1.4 (Островский). Пусть $f(x) = x^n - b_1 x^{n-1} - \ldots - b_n$, где все числа b_i неотрицательны, причем хотя бы одно из них отлично от нуля. Тогда если наибольший общий делитель номеров положительных коэффициентов b_i равен 1, то многочлен f имеет единственный положительный корень p, а модули всех остальных корней строго меньше p.

Доказательство. Пусть положительны только коэффициенты b_{k_1}, $b_{k_2}, \ldots, b_{k_m}$ $(k_1 < k_2 < \ldots < k_m)$. Наибольший общий делитель чисел $k_1, \ldots, k_m$ равен 1, поэтому найдутся такие целые числа $s_1, \ldots, s_m$, что $s_1 k_1 + \ldots + s_m k_m = 1$. Снова рассмотрим функцию

$$F(x) = \frac{b_{k_1}}{x^{k_1}} + \ldots + \frac{b_{k_m}}{x^{k_m}} - 1.$$

Уравнение $F(x) = 0$ имеет единственное положительное решение p. Пусть x — любой другой (ненулевой) корень многочлена f. Положим $q = |x|$. Тогда

$$1 = \frac{b_{k_1}}{x^{k_1}} + \ldots + \frac{b_{k_m}}{x^{k_m}} \leqslant \left|\frac{b_{k_1}}{x^{k_1}}\right| + \ldots + \left|\frac{b_{k_m}}{x^{k_m}}\right| = \frac{b_{k_1}}{q^{k_1}} + \ldots + \frac{b_{k_m}}{q^{k_m}},$$

т. е. $F(q) \geqslant 0$. При этом равенство $F(q) = 0$ возможно лишь в том случае, когда

$$b_{k_i}/x^{k_i} = \left|b_{k_i}/x^{k_i}\right| > 0$$

при всех i. Но в таком случае

$$\frac{b_{k_1}^{s_1} \cdot \ldots \cdot b_{k_m}^{s_m}}{x} = \left(\frac{b_{k_1}}{x^{k_1}}\right)^{s_1} \cdot \ldots \cdot \left(\frac{b_{k_m}}{x^{k_m}}\right)^{s_m} > 0,$$

т. е. $x > 0$. Это противоречит тому, что $x \neq p$, а p — единственный положительный корень уравнения $F(x) = 0$. Таким образом, $F(q) > 0$. Поэтому из монотонности функции $F(x)$ при положительных x следует, что $q < p$. □

Из теоремы Коши–Островского можно вывести следующую оценку для модуля корней многочлена с положительными коэффициентами.

Теорема 1.5. а) (Энестрём–Какейа) Если все коэффициенты многочлена $g(x) = a_0 x^{n-1} + \ldots + a_{n-1}$ положительны, то для любого корня ξ этого многочлена справедлива оценка

$$\min_{1 \leqslant i \leqslant n-1} \{a_i/a_{i-1}\} = \delta \leqslant |\xi| \leqslant \gamma = \max_{1 \leqslant i \leqslant n-1} \{a_i/a_{i-1}\}.$$

б) (Островский) Пусть $a_k/a_{k-1} < \gamma$ при $k = k_1, \ldots, k_m$. Тогда если наибольший общий делитель чисел $n, k_1, \ldots, k_m$ равен 1, то $|\xi| < \gamma$.

Доказательство. Рассмотрим многочлен

$$(x-\gamma)g(x) = a_0x^n - (\gamma a_0 - a_1)x^{n-1} - \ldots - (\gamma a_{n-2} - a_{n-1})x - \gamma a_{n-1}.$$

По определению $\gamma \geqslant a_i/a_{i-1}$, т. е. $\gamma a_{i-1} - a_i \geqslant 0$. Поэтому по теореме Коши γ — единственный положительный корень многочлена $(x-\gamma)g(x)$, а модули всех остальных корней этого многочлена не превосходят γ.

Если ξ — корень многочлена g, то $\eta = \xi^{-1}$ — корень многочлена $a_{n-1}y^{n-1} + \ldots + a_0$. Поэтому

$$|\xi|^{-1} = |\eta| = \max_{1\leqslant i\leqslant n-1}\{a_{i-1}/a_i\} = \left(\min_{1\leqslant i\leqslant n-1}\{a_i/a_{i-1}\}\right)^{-1},$$

т. е.

$$|\xi| \geqslant \delta = \min_{1\leqslant i\leqslant n-1}\{a_i/a_{i-1}\}.$$

Когда выполнено условие б), корень γ многочлена $(x-\gamma)g(x)$ строго больше модулей всех остальных корней этого многочлена. □

Замечание. Теорема Энестрёма–Какейа тоже связана с теоремой Перрона–Фробениуса: см. [AnSV].

Существенное обобщение теоремы Энестрёма–Какейа получено в статье [GG]. При этом отброшено требование вещественности коэффициентов и ослаблено требование их монотонного возрастания. Но формулировка этой теоремы весьма громоздка, поэтому она здесь не приведена.

1.3. Теорема Лагерра

Пусть $z_1, \ldots, z_n \in \mathbb{C}$ — точки, которым приписаны единичные массы. Тогда точку $\zeta = (z_1 + \ldots + z_n)/n$ называют *центром масс* точек $z_1, \ldots, z_n$. Это понятие можно обобщить следующим образом. Сделаем дробно-линейное преобразование w, переводящее точку z_0 в ∞, т. е. $w(z) = \dfrac{a}{z-z_0} + b$. Найдем центр масс образов точек $z_1, \ldots, z_n$, а затем сделаем обратное преобразование w^{-1}. Несложные вычисления показывают, что результат не зависит от a и b, а именно, мы получаем точку

$$\zeta_{z_0} = z_0 + n\left(\frac{1}{z_1-z_0} + \ldots + \frac{1}{z_n-z_0}\right)^{-1} \tag{1}$$

— *центр масс точек* $z_1, \ldots, z_n$ *относительно точки* z_0.

Центр масс точек $z_1, \ldots, z_n$ лежит внутри их выпуклой оболочки. Это утверждение легко переносится на случай центра масс относительно точки z_0. Нужно лишь прямые, соединяющие точки z_i и z_j, заменить окружностями, проходящими через точки z_i, z_j и z_0. Точка z_0, соответствующая точке ∞, лежит при этом вне выпуклой оболочки.

Теорема 1.6. Пусть $f(z) = (z - z_1) \cdot \ldots \cdot (z - z_n)$. Тогда центр масс корней многочлена f относительно произвольной точки z задается формулой

$$\zeta_z = z - nf(z)/f'(z).$$

Доказательство. Ясно, что $f'(z)/f(z) = (z-z_1)^{-1}+\ldots+(z-z_n)^{-1}$. Требуемое утверждение непосредственно следует из формулы (1). □

Теорема 1.7 (Лагерр). Пусть $f(z)$ — многочлен степени n и x — его некратный корень. Тогда центром масс всех остальных корней многочлена относительно точки x служит точка

$$X = x - 2(n-1)f'(x)/f''(x).$$

Доказательство. Пусть $f(z) = (z - x)F(z)$. Тогда $f'(z) = F(z) + (z - x)F'(z)$ и $f''(z) = 2F'(z) + (z - x)F''(z)$. Поэтому $f'(x) = F(x)$ и $f''(x) = 2F'(x)$. Применим предыдущую теорему к многочлену F степени $n - 1$ и к точке $z = x$. В результате получим требуемое. □

Теорема 1.8 (Лагерр). Пусть $f(z)$ — многочлен степени n и

$$X(z) = z - 2(n-1)f'(z)/f''(z).$$

Предположим, что окружность (или прямая) C проходит через некратный корень z_1 многочлена f, а все остальные корни многочлена f принадлежат одной из двух областей, на которые C делит плоскость. Тогда $X(z_1)$ принадлежит той же самой области.

Доказательство. В случае обычного центра масс окружности C соответствует прямая, по одну сторону от которой лежат все корни многочлена, кроме z_1. Их центр масс лежит по ту же самую сторону от этой прямой. □

Следствие. Пусть z_1 — один из некратных корней многочлена f с максимальным модулем. Тогда $\bigl|X(z_1)\bigr| \leqslant |z_1|$, т. е.

$$\bigl|z_1 - 2(n-1)f'(z_1)/f''(z_1)\bigr| \leqslant |z_1|.$$

Доказательство. Все корни f лежат в круге $\{z \in \mathbb{C} \,\big|\, |z| \leqslant |z_1|\}$, поэтому точка $X(z_1)$ тоже лежит в этом круге. □

Теорема 1.9. Пусть f — многочлен с вещественными коэффициентами, а $\zeta_z = z - nf(z)/f'(z)$. Все корни многочлена f вещественны тогда и только тогда, когда при всех $z \in \mathbb{C} \setminus \mathbb{R}$ выполняется неравенство $\operatorname{Im} z \cdot \operatorname{Im} \zeta_z < 0$.

Доказательство. Предположим сначала, что все корни многочлена f вещественны. Пусть $\operatorname{Im} z = a > 0$. Прямая, состоящая из точек с мнимой частью ε, где $0 < \varepsilon < a$, отделяет точку z от всех корней многочлена f (они лежат на вещественной оси). Поэтому $\operatorname{Im} \zeta_z \leqslant \varepsilon$. При $\varepsilon \to 0$ получаем $\operatorname{Im} \zeta_z \leqslant 0$. Легко проверить, что равенство $\operatorname{Im} \zeta_z = 0$ невозможно. В самом деле, пусть $\zeta_z \in \mathbb{R}$. Рассмотрим окружность, проходящую через точку z и касающуюся вещественной оси в точке ζ_z. Слегка пошевелив эту окружность, можно построить окружность, по одну сторону от которой лежат точки z и ζ_z, а по другую — все корни многочлена f. В случае $\operatorname{Im} z = a < 0$ рассуждения аналогичны.

Предположим теперь, что $\operatorname{Im} z \cdot \operatorname{Im} \zeta_z < 0$ при всех $z \in \mathbb{C} \setminus \mathbb{R}$. Пусть z_1 — такой корень многочлена f, что $\operatorname{Im}(z_1) \neq 0$. Тогда $\lim\limits_{z \to z_1} \zeta_z = z_1$, поэтому $\operatorname{Im} z_1 \cdot \operatorname{Im} \zeta_{z_1} > 0$. □

Изложение теории Лагерра основано на статье [Gr]; см. также [ПС].

1.4. Аполярные многочлены

Пусть $f(z)$ — многочлен степени n, ζ — фиксированное число или ∞. Функцию

$$A_\zeta f(z) = \begin{cases} (\zeta - z)f'(z) + nf(z) & \text{при } \zeta \neq \infty; \\ f'(z) & \text{при } \zeta = \infty \end{cases}$$

называют *производной* многочлена $f(z)$ относительно точки ζ. Легко проверить, что если $f(z) = \sum\limits_{k=0}^{n} \binom{n}{k} a_k z^k$, то $\frac{1}{n} f'(z) = \sum\limits_{k=0}^{n-1} \binom{n-1}{k} a_{k+1} z^k$,

а значит,

$$\frac{1}{n}A_\zeta f(z) = \sum_{k=0}^{n-1} \binom{n-1}{k}(a_k + a_{k+1}\zeta)z^k. \qquad (1)$$

Пусть $f(z) = \sum\limits_{k=0}^{n} \binom{n}{k} a_k z^k$ — многочлен с корнями $z_1, \ldots, z_n$, а $g(z) = \sum\limits_{k=0}^{n} \binom{n}{k} b_k z^k$ — многочлен с корнями $\zeta_1, \ldots, \zeta_n$. Из формулы (1) следует, что

$$\frac{1}{n!}A_{\zeta_1} A_{\zeta_2} \ldots A_{\zeta_n} f(z) = a_0 + a_1\sigma_1 + a_2\sigma_2 + \ldots + a_n\sigma_n,$$

где

$$\sigma_1 = \zeta_1 + \zeta_2 + \ldots + \zeta_n = -\binom{n}{1}\frac{b_{n-1}}{b_n},$$

$$\sigma_2 = \zeta_1\zeta_2 + \ldots + \zeta_{n-1}\zeta_n = \binom{n}{2}\frac{b_{n-2}}{b_n},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_n = \zeta_1 \cdot \ldots \cdot \zeta_n = (-1)^n \frac{b_0}{b_n}.$$

Таким образом, равенство $A_{\zeta_1} A_{\zeta_2} \ldots A_{\zeta_n} f(z) = 0$ эквивалентно равенству

$$a_0 b_n - \binom{n}{1} a_1 b_{n-1} + \binom{n}{2} a_2 b_{n-2} + \ldots + (-1)^n a_n b_0 = 0. \qquad (2)$$

Многочлены f и g, коэффициенты которых связаны соотношением (2), называют *аполярными*.

Будем называть *круговой областью* внутреннюю или внешнюю часть круга или полуплоскости.

Теорема 1.10 (J. H. Grace, 1902). Пусть f и g — аполярные многочлены. Тогда если все корни многочлена f лежат в круговой области K, то по крайней мере один корень многочлена g тоже лежит в K.

Доказательство. Нам потребуется следующее вспомогательное утверждение.

Лемма 1.1. Пусть все корни $z_1, \ldots, z_n$ многочлена $f(z)$ лежат внутри круговой области K, а точка ζ лежит вне K. Тогда все корни многочлена $A_\zeta f(z)$ лежат внутри K.

Доказательство. Прежде всего заметим, что если w_i — корень многочлена $A_\zeta f(z)$, то ζ — центр масс корней многочлена $f(z)$ относительно точки w_i (определение центра масс относительно точки см. на с. 13). В самом деле, если $\zeta \neq \infty$, то равенство $A_\zeta f(w_i) = 0$ можно записать в виде

$$(\zeta - w_i)f'(w_i) + nf(w_i) = 0, \quad \text{т. е.} \quad \zeta = w_i - nf(w_i)/f'(w_i).$$

Если же $\zeta = \infty$, то $f'(w_i) = A_\zeta f(w_i) = 0$, поэтому

$$\sum_{j=1}^{n} \frac{1}{z_j - w_i} = \frac{f'(w_i)}{f(w_i)} = 0.$$

Следовательно, центр масс точек $z_1, \ldots, z_n$ относительно точки w_i находится в точке $w_i + \left(\sum \dfrac{1}{z_j - w_i}\right)^{-1} = \infty$.

Теперь уже ясно, что точка w_i не может лежать вне K. В самом деле, если бы точка w_i лежала вне K, то центр масс точек $z_1, \ldots, z_n$ относительно точки w_i лежал бы внутри K, а это противоречит тому, что точка ζ лежит вне K. □

С помощью леммы 1.1 утверждение теоремы доказывается следующим образом. Предположим, что все корни $\zeta_1, \ldots, \zeta_n$ многочлена g лежат вне K. Рассмотрим многочлен $A_{\zeta_2} \ldots A_{\zeta_n} f(z)$. Его степень равна 1, т. е. он имеет вид $c(z-k)$. Из леммы следует, что $k \in K$. Условие аполярности многочленов f и g означает, что $A_{\zeta_1}(z-k) = 0$. С другой стороны, непосредственное вычисление производной показывает, что $A_{\zeta_1}(z-k) = \zeta_1 - k$. Поэтому $k = \zeta_1 \notin K$. Приходим к противоречию. □

Для каждого многочлена f имеется целое семейство аполярных ему многочленов. Подобрав подходящим образом аполярный многочлен, с помощью теоремы Грэйса можно доказать, что у многочлена f есть корень в данной круговой области. Для тех же целей иногда бывает удобно воспользоваться и непосредственно леммой 1.1.

Пример 1. У многочлена

$$f(z) = 1 - z + cz^n, \quad \text{где} \quad c \in \mathbb{C},$$

есть корень в круге $|z - 1| \leqslant 1$.

Доказательство. Многочлены $f(z) = 1 + \binom{n}{1}\frac{-1}{n}z + cz^n$ и $g(z) = z^n + \binom{n}{1}b_{n-1}z^{n-1} + \ldots + b_0$ аполярны, если

$$1 - n\left(\frac{-1}{n}\right)b_{n-1} + cb_0 = 0, \quad \text{т. е.} \quad 1 + b_{n-1} + cb_0 = 0.$$

Пусть $\zeta_k = 1 - \exp(2\pi ik/n)$, $k = 1, \ldots, n$. Тогда $g(z) = \prod(z - \zeta_k) = z^n + \binom{n}{1}b_{n-1}z^{n-1} + \ldots + b_0$, где $b_{n-1} = -\frac{1}{n}\sum\zeta_k = -1$ и $b_0 = \pm\prod\zeta_k = 0$. Поэтому многочлены $f(z)$ и $g(z)$ аполярны. А так как все корни многочлена g лежат в круге $|z - 1| \leqslant 1$, то по крайней мере один из корней многочлена f лежит в этом круге. □

Пример 2. У многочлена $1 - z + c_1z^{n_1} + \ldots + c_kz^{n_k}$, где $1 < n_1 < n_2 < \ldots < n_k$, есть по крайней мере один корень в круге

$$|z| \leqslant \left(\left(1 - \frac{1}{n_1}\right) \cdot \ldots \cdot \left(1 - \frac{1}{n_k}\right)\right)^{-1}.$$

Доказательство. Начнем с многочлена $f(z) = 1 - z + c_1z^{n_1}$. Предположим, что все его корни лежат в области $|z| > \frac{n_1}{n_1 - 1}$. Тогда согласно лемме 1.1 корни многочлена $A_0f(z) = n_1 - (n_1 - 1)z$ тоже лежат в области $|z| > \frac{n_1}{n_1 - 1}$. Но корень многочлена $A_0f(z)$ равен $\frac{n_1}{n_1 - 1}$. Приходим к противоречию.

Для многочлена $f(z) = 1 - z + c_1z^{n_1} + \ldots + c_kz^{n_k}$ доказательство проведем индукцией по k. Рассмотрим многочлен

$$A_0f(z) = n_k - (n_k - 1)z + c_1(n_k - n_1)z^{n_1} + \ldots + c_{k-1}(n_k - n_{k-1})z^{n_{k-1}}.$$

Заменим в этом многочлене z на $\frac{n_k}{n_k - 1}w$. По предположению индукции корни полученного многочлена лежат в круге

$$|w| \leqslant \frac{n_1}{n_1 - 1} \cdot \frac{n_2}{n_2 - 1} \cdot \ldots \cdot \frac{n_{k-1}}{n_{k-1} - 1},$$

поэтому корни многочлена $A_0f(z)$ лежат в круге

$$|z| \leqslant \frac{n_1}{n_1 - 1} \cdot \frac{n_2}{n_2 - 1} \cdot \ldots \cdot \frac{n_k}{n_k - 1}.$$

Следовательно, предположение о том, что все корни многочлена $f(z)$ лежат вне этого круга, приводит к противоречию. □

Пусть $f(z) = \sum_{i=1}^{n} \binom{n}{i} a_i z^i$ и $g(z) = \sum_{i=1}^{n} \binom{n}{i} b_i z^i$. Многочлен $h(z) = \sum_{i=1}^{n} \binom{n}{i} a_i b_i z^i$ называют *композицией* многочленов f и g.

Теорема 1.11 (Сегё). Пусть f и g — многочлены степени n, причем все корни многочлена f лежат в круговой области K. Тогда любой корень композиции h многочленов f и g имеет вид $-\zeta_i k$, где ζ_i — некоторый корень многочлена g, а $k \in K$.

Доказательство. Пусть γ — какой-то корень многочлена h, т. е. $\sum_{i=1}^{n} \binom{n}{i} a_i b_i \gamma^i = 0$. Тогда многочлены $f(z)$ и $G(z) = z^n g(-\gamma z^{-1})$ аполярны. Поэтому согласно теореме Грэйса один из корней многочлена $G(z)$ лежит в K. Пусть, например, $g(-\gamma k^{-1}) = 0$, где $k \in K$. Тогда $-\gamma k^{-1} = \zeta_i$, где ζ_i — корень многочлена g. □

Для многочленов, степени которых не обязательно равны, имеется следующий аналог теоремы Грэйса.

Теорема 1.12 [Az]. Пусть $f(z) = \sum_{i=1}^{n} \binom{n}{i} a_i z^i$ и $g(z) = \sum_{i=1}^{m} \binom{m}{i} b_i z^i$ — многочлены степени n и m, причем $m \leqslant n$. Предположим, что их коэффициенты связаны соотношением

$$\binom{m}{0} a_0 b_m - \binom{m}{1} a_1 b_{m-1} + \ldots + (-1)^m \binom{m}{m} a_m b_0 = 0. \tag{3}$$

Тогда справедливы следующие утверждения:

а) если все корни многочлена $g(z)$ лежат в круге $|z| \leqslant r$, то по крайней мере один корень многочлена $f(z)$ тоже лежит в этом круге;

б) если все корни многочлена $f(z)$ лежат вне круга $|z| \leqslant r$, то по крайней мере один корень многочлена $g(z)$ тоже лежит вне этого круга.

Доказательство [Ru]. а) Соотношение (3) инвариантно относительно замены z на rz в многочленах f и g, поэтому можно считать, что $r = 1$. Предположим, что все корни многочлена $f(z)$ лежат в области $|z| > 1$. Тогда все корни многочлена $z^n f(1/z)$ лежат в области $|z| < 1$.

Поэтому из теоремы Гаусса–Люка (теорема 2.1 на с. 22) следует, что все корни многочлена

$$f_1(z) = D^{(n-m)}\bigl(z^n f(1/z)\bigr) = n(n-1)\cdot\ldots\cdot(m+1)\sum_{i=0}^{m}\binom{m}{i}a_i z^{m-i}$$

лежат в области $|z| < 1$. Следовательно, все корни многочлена

$$f_2(z) = z^m\sum_{i=0}^{m}\binom{m}{i}a_i(1/z)^{m-i} = \sum_{i=0}^{m}\binom{m}{i}a_i z^i$$

лежат в области $|z| > 1$.

Соотношение (3) означает, что многочлены f_2 и g аполярны. Все корни многочлена f_2 лежат в круговой области $|z| > 1$, поэтому согласно теореме Грэйса по крайней мере один корень многочлена g тоже лежит в этой области. Приходим к противоречию.

б) Все корни многочлена f_2 лежат в области $|z| \geqslant 1$, поэтому по крайней мере один корень многочлена g тоже лежит в этой области. □

1.5. Проблема Рауса–Гурвица

Во многих задачах об устойчивости возникает потребность выяснить, все ли корни многочлена лежат в левой полуплоскости (т. е. вещественные части корней отрицательны). Такие многочлены называют *устойчивыми*. Проблема Рауса–Гурвица заключается в том, чтобы непосредственно по коэффициентам многочлена выяснить, устойчив он или нет. Известно много разных решений проблемы Рауса–Гурвица (см., например, [По2]). Мы ограничимся одним простым критерием, приведенным в [Str].

Прежде всего заметим, что достаточно рассмотреть случай многочлена с вещественными коэффициентами. В самом деле, если $p(z) = \sum a_n z^n$ — многочлен с комплексными коэффициентами, то можно рассмотреть многочлен

$$p^*(z) = p(z)\overline{p(\overline{z})} = \Bigl(\sum a_n z^n\Bigr)\Bigl(\sum \overline{a_n} z^n\Bigr).$$

Ясно, что вещественные части корней у многочлена $\overline{p(\overline{z})}$ такие же, как и у многочлена $p(z)$. Кроме того, выражения коэффициентов многочлена $p^*(z)$ симметричны относительно a_n и $\overline{a_n}$. Это означает, что коэффициенты многочлена p^* переходят в себя при сопряжении, т. е. они вещественны.

Теорема 1.13. Пусть $p(z) = z^n + a_1 z^{n-1} + \ldots + a_n$ — многочлен с вещественными коэффициентами, $q(z) = z^m + b_1 z^{m-1} + \ldots + b_m$, где $m = n(n-1)/2$, — многочлен, корнями которого служат все суммы пар корней многочлена p. Многочлен p устойчив тогда и только тогда, когда все коэффициенты многочленов p и q положительны.

Доказательство. Пусть многочлен p устойчив. Отрицательному корню α соответствует множитель $z - \alpha$ с положительными коэффициентами. Паре сопряженных корней $\alpha \pm i\beta$ с отрицательной вещественной частью соответствует множитель

$$(z - \alpha - i\beta)(z - \alpha + i\beta) = z^2 - 2\alpha z + \alpha^2 + \beta^2$$

с положительными коэффициентами. Таким образом, все коэффициенты многочлена p положительны.

Комплексные корни многочлена q распадаются на пары сопряженных корней, поэтому коэффициенты многочлена q вещественные. Кроме того, вещественные части всех корней многочлена q отрицательны. Те же самые рассуждения, что и для многочлена p, показывают, что все коэффициенты многочлена q положительны.

Пусть теперь все коэффициенты многочленов p и q положительны. В таком случае все вещественные корни многочленов p и q отрицательны. Поэтому если α — вещественный корень многочлена p, то $\alpha < 0$, а если $\alpha \pm i\beta$ — пара комплексных сопряженных корней многочлена p, то $2\alpha = (\alpha + i\beta) + (\alpha - i\beta)$ — корень многочлена q, а значит, $2\alpha < 0$. □

2. Корни многочлена и его производной

2.1. Теорема Гаусса–Люка

В 1836 г. Гаусс показал, что все корни производной многочлена P, отличные от кратных корней самого многочлена P, являются положениями равновесия для поля сил, которое создается одинаковыми частицами, расположенными в корнях многочлена P (в корне кратности r расположено r частиц); каждая частица создает силу притяжения, обратно пропорциональную расстоянию до этой частицы. Из этой теоремы Гаусса легко вывести приводимую ниже теорему 2.1, но сам Гаусс об этом не упоминает. Первым сформулировал и доказал теорему 2.1 французский инженер Люка (F. Lucas) в 1874 г. Поэтому теорему 2.1 часто называют *теоремой Гаусса–Люка*.

Теорема 2.1 (Гаусс–Люка). Корни производной многочлена P принадлежат выпуклой оболочке корней самого многочлена P.

Доказательство. Пусть $P(z) = (z - z_1) \cdot \ldots \cdot (z - z_n)$. Легко проверить, что

$$\frac{P'(z)}{P(z)} = \frac{1}{z - z_1} + \ldots + \frac{1}{z - z_n}. \tag{1}$$

Предположим, что $P'(w) = 0$, $P(w) \neq 0$ и w не принадлежит выпуклой оболочке точек $z_1, \ldots, z_n$. Тогда через точку w можно провести прямую, не пересекающую выпуклой оболочки точек $z_1, \ldots, z_n$. Поэтому векторы $w - z_1, \ldots, w - z_n$ лежат в одной полуплоскости, заданной этой прямой. Следовательно, в одной полуплоскости лежат и векторы $\frac{1}{w-z_1}, \ldots$ $\ldots, \frac{1}{w-z_n}$, поскольку $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$. Следовательно, $\frac{P'(w)}{P(w)} = \frac{1}{w - z_1} + \ldots$ $\ldots + \frac{1}{w - z_n} \neq 0$. Получено противоречие. Поэтому w принадлежит выпуклой оболочке корней многочлена P. □

Соотношение (1) позволяет доказать следующее свойство корней производной многочлена с вещественными корнями.

Теорема 2.2 [An]. Пусть $P(z) = (z - x_1) \cdot \ldots \cdot (z - x_n)$, где $x_1 < \ldots$ $\ldots < x_n$. Тогда если некоторый корень x_i заменяется на $x_i' \in (x_i, x_{i+1})$, то все корни производной многочлена P увеличиваются.

Доказательство. Пусть $z_1 < z_2 < \ldots < z_{n-1}$ — корни производной многочлена с корнями $x_1, \ldots, x_n$, а $z_1' < z_2' < \ldots < z_{n-1}'$ — корни производной многочлена с корнями $x_1, \ldots, x_i', \ldots, x_n$. Для корней z_k и z_k' соотношение (1) принимает вид

$$\sum_{i=1}^{n} \frac{1}{z_k - x_i} = 0, \quad \sum_{i=1}^{n} \frac{1}{z_k' - x_i'} = 0. \tag{2}$$

Предположим, что теорема неверна, т. е. $z_k' < z_k$ для некоторого k. Тогда $z_k' - x_i' < z_k - x_i$. При этом числа $z_k' - x_i'$ и $z_k - x_i$ одного знака. В самом деле, $z_j < x_i$, $z_j' < x_i'$ при $j \leqslant i - 1$ и $z_j > x_i$, $z_j' > x_i'$ при $j \geqslant i$. Следовательно, $\frac{1}{z_k - x_i} < \frac{1}{z_k' - x_i'}$ при всех $i = 1, \ldots, n$. Но в таком случае соотношения (2) не могут выполняться одновременно. □

2.2. Корни производной и фокусы эллипса

Корни производной кубического многочлена имеют следующую интересную геометрическую интерпретацию.

Теорема 2.3 (ван ден Берг, [B]). Пусть корни кубического многочлена расположены в вершинах треугольника ABC на комплексной плоскости. Тогда корни производной этого многочлена расположены в фокусах эллипса, касающегося сторон треугольника ABC в их серединах.

Первое доказательство. Прежде всего заметим, что если $Q(z) = P(z - z_0)$, то $Q'(z) = P'(z - z_0)$, поэтому началом координат можно считать любую точку.

Любое аффинное преобразование плоскости можно представить в виде композиции движения, гомотетии и преобразования, имеющего в некоторой прямоугольной системе координат вид $(x, y) \mapsto (x, y\cos\alpha)$. Поэтому можно считать, что треугольник ABC получен преобразованием

$$z \mapsto \frac{z+\overline{z}}{2} + \frac{z-\overline{z}}{2}\cos\alpha = z\cos^2\frac{\alpha}{2} + \overline{z}\sin^2\frac{\alpha}{2} \tag{1}$$

из правильного треугольника с вершинами w, εw и $\varepsilon^2 w$, где $|w| = 1$ и $\varepsilon = \exp(2\pi i/3)$. Тогда полуоси a и b рассматриваемого эллипса равны $\frac{1}{2}$ и $\frac{\cos\alpha}{2}$, а расстояние между его фокусами F_1 и F_2 равно $\sqrt{a^2 - b^2} = \frac{1}{2}\sin\alpha$. Точки F_1 и F_2 переходят в точки $(\pm 1, 0)$ при растяжении с коэффициентом

$$\left(\frac{1}{2}\sin\alpha\right)^{-1} = \left(\sin\frac{\alpha}{2}\cos\frac{\alpha}{2}\right)^{-1}.$$

В результате преобразования (1) и этого растяжения получаем преобразование

$$z \mapsto z\operatorname{ctg}\frac{\alpha}{2} + \overline{z}\operatorname{tg}\frac{\alpha}{2}.$$

Положим $a = w\operatorname{ctg}\frac{\alpha}{2}$. Тогда многочлен с корнями A, B и C имеет вид

$$P(x) = \left(x - a - \frac{1}{a}\right)\left(x - a\varepsilon - \frac{1}{a\varepsilon}\right)\left(x - a\varepsilon^2 - \frac{1}{a\varepsilon^2}\right).$$

Легко проверить, что $P'(x) = 3x^2 + 3\varepsilon + 3\overline{\varepsilon} = 3x^2 - 3$, поэтому корни многочлена P' равны ± 1. □

Второе доказательство [Sho]. Пусть $\varepsilon = \exp(2\pi i/3)$, а z_0, z_1, z_2 — корни рассматриваемого многочлена. Выберем числа $\zeta_0, \zeta_1, \zeta_2$ так, что

$$z_0 = \zeta_0 + \zeta_1 + \zeta_2, \quad z_1 = \zeta_0 + \zeta_1\varepsilon + \zeta_2\varepsilon^2, \quad z_2 = \zeta_0 + \zeta_1\varepsilon^2 + \zeta_2\varepsilon, \qquad (2)$$

т. е.

$$3\zeta_0 = z_0 + z_1 + z_2, \quad 3\zeta_1 = z_0 + z_1\varepsilon^2 + z_2\varepsilon, \quad 3\zeta_2 = z_0 + z_1\varepsilon + z_2\varepsilon^2.$$

В дальнейшем будем предполагать, что $z_0 + z_1 + z_2 = 0$, т. е. $\zeta_0 = 0$.

Легко проверить, что кривая $\zeta_1 e^{i\varphi} + \zeta_2 e^{-i\varphi}$, где $0 \leqslant \varphi \leqslant 2\pi$, представляет собой эллипс, полуоси которого направлены по биссектрисам внешних и внутренних углов угла $\zeta_1 O \zeta_2$ (O — начало координат), причем длины полуосей равны $|\zeta_1| + |\zeta_2|$ и $\big||\zeta_1| - |\zeta_2|\big|$. В самом деле, рассматриваемая кривая является образом единичной окружности при отображении $z \mapsto \zeta_1 z + \zeta_2 \overline{z}$. Кроме того, если $\zeta_1 = |\zeta_1|e^{i\alpha}$ и $\zeta_2 = |\zeta_2|e^{i\beta}$, то

$$\zeta_1 e^{i\varphi} + \zeta_2 e^{-i\varphi} = |\zeta_1| e^{i(\varphi+\alpha)} + |\zeta_2| e^{i(\beta-\varphi)}.$$

Модуль этого выражения максимален при $\varphi = \dfrac{\alpha+\beta}{2} + k\pi$ и минимален при $\varphi = \dfrac{\alpha+\beta}{2} + \dfrac{\pi}{2} + k\pi$. Эти значения φ как раз и соответствуют направлениям указанных биссектрис.

Фокусы f_1 и f_2 эллипса $\zeta_1 e^{i\varphi} + \zeta_2 e^{-i\varphi}$ лежат на прямой, соответствующей углу $\varphi = \dfrac{\alpha+\beta}{2}$, т. е. отношение $\dfrac{f_1 f_2}{\zeta_1\zeta_2}$ является положительным числом. Кроме того, квадрат расстояния от фокуса до центра эллипса равен разности квадратов полуосей, т. е. он равен

$$\big(|\zeta_1| + |\zeta_2|\big)^2 - \big(|\zeta_1| - |\zeta_2|\big)^2 = 4|\zeta_1\zeta_2|.$$

Таким образом, $f_1 f_2 = 4\zeta_1\zeta_2$.

Соотношения (2) при $\zeta_0 = 0$ показывают, что вершины z_0, z_1, z_2 рассматриваемого треугольника лежат на эллипсе $\zeta_1 e^{i\varphi} + \zeta_2 e^{-i\varphi}$ а середины его сторон лежат на эллипсе $\dfrac{1}{2}\big(\zeta_1 e^{i\varphi} + \zeta_2 e^{-i\varphi}\big)$. Середина хорды первого эллипса может лежать на втором эллипсе лишь в том случае, когда эта хорда касается эллипса. Таким образом, требуется доказать, что фокусы эллипса $\dfrac{1}{2}\big(\zeta_1 e^{i\varphi} + \zeta_2 e^{-i\varphi}\big)$ совпадают с корнями производной многочлена $(z - z_0)(z - z_1)(z - z_2)$. Фокусы эллипса удовлетворяют уравнению $z^2 - \zeta_1\zeta_2 = 0$, а корни производной удовлетворяют уравнению

$$3z^2 + z_0 z_1 + z_0 z_2 + z_1 z_2 = 0, \quad \text{т. е.} \quad 3(z^2 - \zeta_1\zeta_2) = 0. \qquad \square$$

2.3. Локализация корней производной

2.3.1. Круги Йенсена

Пусть f — многочлен с вещественными коэффициентами. Для каждой пары сопряженных корней z и $\overline{z}$ этого многочлена рассмотрим отрезок с концами z и $\overline{z}$ и построим на этом отрезке как на диаметре круг; такие круги называют *кругами Йенсена* многочлена f.

Теорема 2.4 (Йенсен). Любой невещественный корень производной многочлена f лежит внутри или на границе одного из кругов Йенсена.

Доказательство. Пусть $z_1, \ldots, z_n$ — корни многочлена f. Тогда

$$\frac{f'(z)}{f(z)} = \sum_{j=1}^{n} \frac{1}{z - z_j}. \tag{1}$$

Прежде всего покажем, что если точка z лежит вне круга Йенсена с диаметром $z_p z_q$, то

$$\operatorname{sgn}\operatorname{Im}\left(\frac{1}{z - z_p} + \frac{1}{z - z_q}\right) = -\operatorname{sgn}\operatorname{Im} z. \tag{2}$$

В самом деле,

$$\frac{1}{z - a - bi} + \frac{1}{z - a + bi} = \frac{2(z-a)\bigl((\overline{z}-a)^2 + b^2\bigr)}{\bigl|(z-a)^2 + b^2\bigr|^2}$$

и

$$\operatorname{Im}\bigl((\overline{z}-a)|z-a|^2 + (z-a)b^2\bigr) = \bigl(b^2 - |z-a|^2\bigr)\operatorname{Im} z.$$

Покажем теперь, что если $z \notin \mathbb{R}$ и $z_j = a \in \mathbb{R}$, то

$$\operatorname{sgn}\operatorname{Im}\left(\frac{1}{z - z_j}\right) = -\operatorname{sgn}\operatorname{Im} z. \tag{3}$$

В самом деле,

$$\frac{1}{z-a} - \frac{1}{\overline{z}-a} = \frac{\overline{z}-z}{|z-a|^2} = \frac{-2\operatorname{Im} z}{|z-a|^2}.$$

Из формул (1), (2) и (3) следует, что если точка $z \notin \mathbb{R}$ расположена вне всех кругов Йенсена, то

$$\operatorname{sgn}\operatorname{Im}\frac{f'(z)}{f(z)} = -\operatorname{sgn}\operatorname{Im} z \neq 0.$$

Поэтому $f'(z) \neq 0$, т. е. z — не корень производной. □

Для количества корней производной, вещественная часть которых принадлежит данному отрезку, можно доказать следующую оценку, уточняющую теорему Йенсена.

Теорема 2.5 (Уолш). Пусть $I = [\alpha, \beta]$, K — объединение I и кругов Йенсена, пересекающих I. Тогда если K содержит k корней многочлена $f(z)$, то количество корней многочлена $f'(z)$, лежащих в K, заключено между $k-1$ и $k+1$.

Доказательство. Пусть C — граница наименьшего прямоугольника, стороны которого параллельны осям координат и который содержит K. Рассмотрим ограничение на C отображения $z \mapsto e^{i\varphi}$, где $\varphi = \arg\bigl(f'(z)/f(z)\bigr)$. Из формул (1), (2) и (3) следует, что образ части C, лежащей в верхней полуплоскости, расположен на полуокружности $|z| = 1$, $\operatorname{Im} z \leqslant 0$, а образ части C, лежащей в нижней полуплоскости, расположен на полуокружности $|z| = 1$, $\operatorname{Im} z \geqslant 0$. Поэтому количество оборотов образа кривой C вокруг начала координат равно 0 или ± 1. Это означает, что индексы кривой C относительно векторных полей $f(z)$ и $f'(z)$ совпадают или отличаются на ± 1, т. е. количества нулей функций f и f', заключенных внутри кривой C, совпадают или отличаются на ± 1. □

2.3.2. Теорема Уолша

Теорема 2.6 (Уолш). Пусть корни многочленов f_1 и f_2 лежат в кругах K_1 и K_2, радиусы которых равны r_1 и r_2, а центры находятся в точках c_1 и c_2. Тогда все корни производной многочлена $f = f_1 f_2$ лежат либо в K_1, либо в K_2, либо в круге K радиуса $\dfrac{n_2 r_1 + n_1 r_2}{n_1 + n_2}$ с центром в точке $\dfrac{n_2 c_1 + n_1 c_2}{n_1 + n_2}$, где $n_1 = \deg f_1$ и $n_2 = \deg f_2$.

Доказательство. Пусть z — корень производной многочлена f, лежащий вне K_1 и K_2. Тогда $f_1'(z) f_2(z) + f_1(z) f_2'(z) = 0$, причем $f_1(z), f_2(z), f_1'(z), f_2'(z) \neq 0$.

Рассмотрим точки ζ_1 и ζ_2 — центры масс корней многочленов f_1 и f_2 относительно точки z. Согласно теореме 1.6 на с. 14

$$\zeta_1 = z - n_1 \frac{f_1(z)}{f_1'(z)}, \quad \zeta_2 = z - n_2 \frac{f_2(z)}{f_2'(z)}.$$

Поэтому

$$n_2\zeta_1 + n_1\zeta_2 = (n_1+n_2)z - n_1n_2\left(\frac{f_1(z)}{f_1'(z)} + \frac{f_2(z)}{f_2'(z)}\right) = (n_1+n_2)z,$$

т. е. $z = \dfrac{n_2\zeta_1 + n_1\zeta_2}{n_1+n_2}$. А так как все корни многочлена f_i лежат в K_i, то $\zeta_i \in K_i$. Остается заметить, что если точки ζ_1 и ζ_2 с массами n_1 и n_2 лежат в кругах K_1 и K_2, то их центр масс z лежит в круге K. □

2.3.3. Теорема Грэйса–Хивуда

Теорема 2.7 (J. H. Grace, 1902, P. J. Heawood, 1907). Если z_1 и z_2 — различные корни многочлена f степени n, то в круге $|z-c| \leqslant r$, где $c = (z_1+z_2)/2$ и $r = \bigl(|z_1-z_2|/2\bigr)\operatorname{ctg}(\pi/n)$, находится по крайней мере один корень многочлена f'.

Доказательство. Пусть $f'(z) = \sum\limits_{k=0}^{n-1}\binom{n-1}{k}a_kz^k$. Тогда

$$0 = f(z_2) - f(z_1) = \int\limits_{z_1}^{z_2} f'(z)\,dz = \sum_{k=0}^{n-1}(-1)^k\binom{n-1}{k}a_kb_{n-1-k},$$

где коэффициенты $b_0,\ldots,b_{n-1}$ зависят только от z_1 и z_2, а от коэффициентов $a_0,\ldots,a_{n-1}$ они не зависят. Таким образом, по данным z_1 и z_2 можно построить многочлен $g(z) = \sum\limits_{k=0}^{n-1}\binom{n-1}{k}b_kz^k$, аполярный многочлену $f'(z)$.

Чтобы получить явное выражение для многочлена g, положим $a_k = (-1)^kx^{n-1-k}$, т. е. рассмотрим многочлен $h(z) = (x-z)^{n-1}$. В таком случае

$$g(x) = \sum_{k=0}^{n-1}\binom{n-1}{k}x^{n-1-k}b_{n-1-k} = \int\limits_{z_1}^{z_2}(x-1)^{n-1}dz = \frac{(x-z_1)^n - (x-z_2)^n}{n}.$$

Корни многочлена g имеют вид $\zeta_k = \dfrac{z_1+z_2}{2} + i\dfrac{z_1-z_2}{2}\operatorname{ctg}\dfrac{k\pi}{n}$, (для $k = 1,2,\ldots,n-1$). Все они лежат на границе рассматриваемого круга $|z-c| \leqslant r$. Поэтому согласно теореме 1.10 на с. 16 в круге $|z-c| \leqslant r$ находится по крайней мере один корень многочлена f'. □

Другие теоремы о локализации корней производной приведены в статье [Ma2].

2.4. Гипотеза Сендова–Илиева

В 1962 г. болгарский математик Б. Сендов высказал следующую гипотезу, которую часто приписывают другому болгарскому математику, Л. Илиеву: «*Пусть $P(z)$ — многочлен, все корни которого лежат в круге $|z| \leqslant 1$. Тогда если z_0 — один из корней многочлена $P(z)$, то в круге $|z - z_0| \leqslant 1$ есть по крайней мере один корень многочлена $P'(z)$*». (Предполагается, что $\deg P \geqslant 2$.)

Гипотеза Сендова–Илиева доказана для всех многочленов степени не выше 5 и для некоторых специальных многочленов (см., например, [Scm]).

Мы ограничимся доказательством гипотезы Сендова–Илиева для многочленов вида

$$P(z) = (z - z_0)^{n_0}(z - z_1)^{n_1}(z - z_2)^{n_2}.$$

Это доказательство приведено в [CS].

Случай, когда $n = n_0 + n_1 + n_2 \geqslant 4$, разбирается достаточно просто. В этом случае нужно доказать, что если $|z_i| \leqslant 1$ при $i = 0, 1, 2$, то многочлен

$$P'(z) = n(z - z_0)^{n_0 - 1}(z - z_1)^{n_1 - 1}(z - z_2)^{n_2 - 1}(z - w_1)(z - w_2) \qquad (1)$$

имеет корень, лежащий в круге $|z - z_0| \leqslant 1$. Если $n_0 > 1$, то таким корнем будет z_0. Поэтому будем считать, что $n_0 = 1$. Запишем $P(z)$ в виде $P(z) = (z - z_0)Q(z)$. Ясно, что

$$P'(z_0) = Q(z_0) = (z_0 - z_1)^{n_1}(z_0 - z_2)^{n_2}. \qquad (2)$$

Из (1) и (2) следует, что

$$n(z_0 - w_1)(z_0 - w_2) = (z_0 - z_1)(z_0 - z_2). \qquad (3)$$

Учитывая, что $|z_0 - z_1| \leqslant |z_0| + |z_1| = 2$ и $|z_0 - z_2| \leqslant 2$, получаем

$$|z_0 - w_1| \cdot |z_0 - w_2| \leqslant 4/n \leqslant 1,$$

поэтому $|z_0 - w_1| \leqslant 1$ или $|z_0 - w_2| \leqslant 1$.

Остается рассмотреть случай, когда $n_0 = n_1 = n_2 = 1$. Для этого нам потребуется следующее вспомогательное утверждение, которое мы сформулируем в более общем виде, чем это нужно для наших целей.

Лемма. Пусть $P(z)$ — многочлен степени n, где $n \geqslant 2$. Тогда если

$$\bigl|P''(z_0)\bigr| \geqslant (n-1)\bigl|P'(z_0)\bigr|,$$

то по крайней мере один из корней многочлена P' лежит в круге $|z - z_0| \leqslant 1$.

Доказательство. Пусть $w_1, w_2, \ldots, w_{n-1}$ — корни многочлена P'. Можно считать, что старший коэффициент многочлена P равен 1. В таком случае $P'(z) = n\prod\limits_{j=1}^{n-1}(z - w_j)$. Если $P'(z) \neq 0$, то можно взять логарифм от обеих частей и продифференцировать их. В результате получим

$$\frac{P''(z)}{P'(z)} = \sum_{j=1}^{n-1}\frac{1}{z - w_j}.$$

По условию z_0 — некратный корень многочлена P, т. е. $P'(z_0) \neq 0$. Предположим, что $|z_0 - w_j| > 1$ при $j = 1, \ldots, n-1$. Тогда из неравенства $\bigl|P''(z_0)\bigr| \geqslant (n-1)\bigl|P'(z_0)\bigr|$ следует, что

$$n - 1 \leqslant \left|\frac{P''(z_0)}{P'(z_0)}\right| \leqslant \sum_{j=1}^{n-1}\frac{1}{|z_0 - w_j|} < n - 1.$$

Приходим к противоречию. □

Займемся теперь непосредственно многочленом

$$P(z) = (z - z_0)(z - z_1)(z - z_2) = (z - z_0)Q(z).$$

Ясно, что

$$\frac{P''(z_0)}{P'(z_0)} = 2\frac{Q'(z_0)}{Q(z_0)} = 2\left(\frac{1}{z_0 - z_1} + \frac{1}{z_0 - z_2}\right) = \frac{2(2z_0 - z_1 - z_2)}{(z_0 - z_1)(z_0 - z_2)}.$$

Рассмотрим треугольник ABC с вершинами $A = z_0$, $B = z_1$, $C = z_2$. Ясно, что $|z_0 - z_1| = c$, $|z_0 - z_2| = b$ и $|2z_0 - z_1 - z_2| = 2m_a$, где m_a — длина медианы. Согласно лемме если $4m_a \geqslant 2bc$, то гипотеза Сендова–Илиева верна. По условию $b \leqslant 2$ и $c \leqslant 2$, поэтому неравенство $2m_a \geqslant bc$ выполняется как при $m_a \geqslant b$, так и при $m_a \geqslant c$. Остается рассмотреть случай, когда $m_a < b$ и $m_a < c$.

Соотношение (3) показывает, что гипотеза Сендова–Илиева верна, если $bc \leqslant 3$. Поэтому можно считать, что $bc > 3$. В таком случае

$$b^2 + c^2 = (b-c)^2 + 2bc > 6,$$

а значит, $b^2 + c^2 - a^2 > 6 - 4 > 0$, т. е. $\angle A < 90°$. Из неравенств $b > m_a$ и $c > m_a$ следует, что $\angle C < 90°$ и $\angle B < 90°$, поэтому треугольник ABC остроугольный. Пусть R — радиус его описанной окружности, h_a — высота, опущенная из вершины A. Тогда $c/h_a = \sin B = 2R/b$, т. е. $bc = 2Rh_a \leqslant 2Rm_a$. Чтобы получить требуемое неравенство $bc \leqslant 2m_a$, остается доказать, что $R \leqslant 1$. Остроугольный треугольник ABC расположен внутри единичной окружности $|z| = 1$. Если описанная окружность S треугольника ABC лежит внутри единичной окружности, то неравенство $R \leqslant 1$ очевидно. Пусть теперь окружность S и единичная окружность имеют общую хорду. Из остроугольности треугольника ABC следует, что эта хорда видна из вершин треугольника под острым углом φ. Эта же хорда видна из точек единичной окружности под углами ψ и $180° - \psi$, где $\psi \leqslant 90°$. При этом $\psi \leqslant \varphi$. Из неравенств $\psi \leqslant \varphi < 90° \leqslant 180° - \psi$ следует, что $R \leqslant 1$.

2.5. Многочлены, у которых совпадают корни их самих и их производных

В статье [Chu] утверждалось, что если P и Q — многочлены со старшим коэффициентом 1, причем множества корней многочленов P и Q совпадают и множества корней многочленов P' и Q' тоже совпадают, то $P^m = Q^n$ для некоторых натуральных m и n. Затем в доказательстве этого утверждения были обнаружены пробелы и вскоре в [Roi] был построен контрпример. Конструкция этого контрпримера весьма сложная. Заинтересованному читателю мы советуем обратиться непосредственно к статье [Roi].

По поводу свойств многочленов, у которых совпадают корни их самих и их производных, см. также [DS].

3. Результант и дискриминант

3.1. Результант

Рассмотрим многочлены $f(x) = \sum\limits_{i=0}^{n} a_i x^{n-i}$ и $g(x) = \sum\limits_{i=0}^{m} b_i x^{m-i}$, где $a_0 \neq 0$ и $b_0 \neq 0$. Над алгебраически замкнутым полем многочлены f и g

имеют общий делитель тогда и только тогда, когда они имеют общий корень. Если же поле не алгебраически замкнуто, то общий делитель может быть многочленом, не имеющим корней.

Наличие у f и g общего делителя эквивалентно тому, что существуют такие многочлены p и q, что $fq = gp$, причем $\deg p \leqslant n-1$ и $\deg q \leqslant m-1$. Пусть $q = u_0x^{m-1} + \ldots + u_{m-1}$ и $p = v_0x^{n-1} + \ldots + v_{n-1}$. Равенство $fq = gp$ можно записать в виде системы уравнений

$$\begin{aligned} a_0u_0 &= b_0v_0, \\ a_1u_0 + a_0u_1 &= b_1v_0 + b_0v_1, \\ a_2u_0 + a_1u_1 + a_0u_2 &= b_2v_0 + b_1v_1 + b_0v_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Многочлены f и g имеют общий корень тогда и только тогда, когда эта система имеет ненулевое решение $(u_0, u_1, \ldots, v_0, v_1, \ldots)$. Если, например, $m = 3$ и $n = 2$, то определитель этой системы уравнений имеет вид

$$\begin{vmatrix} a_0 & 0 & 0 & -b_0 & 0 \\ a_1 & a_0 & 0 & -b_1 & -b_0 \\ a_2 & a_1 & a_0 & -b_2 & -b_1 \\ 0 & a_2 & a_1 & -b_3 & -b_2 \\ 0 & 0 & a_2 & 0 & -b_3 \end{vmatrix} = \pm \begin{vmatrix} a_0 & a_1 & a_2 & 0 & 0 \\ 0 & a_0 & a_1 & a_2 & 0 \\ 0 & 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & b_3 & 0 \\ 0 & b_0 & b_1 & b_2 & b_3 \end{vmatrix} = \pm \det S(f,g).$$

Матрицу $S(f,g)$ называют *матрицей Сильвестра* многочленов f и g. Определитель матрицы $S(f,g)$ называют *результантом* многочленов f и g; результант многочленов f и g обозначают $R(f,g)$. Ясно, что $R(f,g)$ — однородный многочлен степени m по переменным a_i и степени n по переменным b_j. Многочлены f и g имеют общий делитель тогда и только тогда, когда определитель рассматриваемой системы равен нулю, т. е. $R(f,g) = 0$.

Результант имеет много разных приложений. Например, если заданы полиномиальные соотношения $P(x,z) = 0$ и $Q(y,z) = 0$, то с помощью результанта можно получить полиномиальное соотношение $R(x,y) = 0$. В самом деле, рассмотрим данные полиномы $P(x,z)$ и $Q(y,z)$ как полиномы от z, считая x и y постоянными. Тогда результант $R(x,y)$ этих полиномов дает требуемое соотношение $R(x,y) = 0$.

Результант позволяет также сводить решение системы алгебраических уравнений к нахождению корней многочленов. В самом деле, пусть $P(x_0,y_0) = 0$ и $Q(x_0,y_0) = 0$. Рассмотрим $P(x,y)$ и $Q(x,y)$ как многочлены от y. При $x = x_0$ они имеют общий корень y_0. Следовательно, их результант $R(x)$ равен нулю при $x = x_0$.

Теорема 3.1. Пусть x_i — корни многочлена f, а y_j — корни многочлена g. Тогда

$$R(f,g) = a_0^m b_0^n \prod (x_i - y_j) = a_0^m \prod g(x_i) = b_0^n \prod f(y_j).$$

Доказательство. Так как $f(x) = a_0(x - x_1) \cdot \ldots \cdot (x - x_n)$, то $a_k = \pm a_0 \sigma_k(x_1, \ldots, x_n)$, где σ_k — элементарная симметрическая функция. Аналогично $b_k = \pm b_0 \sigma_k(y_1, \ldots, y_m)$. Результант является однородным многочленом степени m по переменным a_i и степени n по переменным b_j, поэтому

$$R(f,g) = a_0^m b_0^n P(x_1, \ldots, x_n, y_1, \ldots, y_m),$$

где P — симметрический многочлен от $x_1, \ldots, x_n$ и $y_1, \ldots, y_m$, обращающийся в нуль при $x_i = y_j$. Формула

$$x_i^k = (x_i - y_j)x_i^{k-1} + y_j x_i^{k-1}$$

показывает, что

$$P(x_1, \ldots, y_m) = (x_i - y_j)Q(x_1, \ldots, y_m) + r(x_1, \ldots, \widehat{x}_i, \ldots, y_m).$$

Подставив в это равенство $x_i = y_j$, получим, что r — нулевой многочлен. Аналогичные рассуждения показывают, что многочлен P делится на $S = a_0^m b_0^n \prod (x_i - y_j)$.

Так как $g(x) = b_0 \prod\limits_{j=1}^{m} (x - y_j)$, то $\prod\limits_{i=1}^{n} g(x_i) = b_0^n \prod\limits_{i,j} (x_i - y_j)$, а значит,

$$S = a_0^m \prod_{i=1}^{n} g(x_i) = a_0^m \prod_{i=1}^{n} (b_0 x_i^m + b_1 x_i^{m-1} + \ldots + b_m)$$

— однородный многочлен степени n по переменным $b_0, \ldots, b_m$. Для переменных $a_0, \ldots, a_n$ рассуждения аналогичны. Ясно также, что симметрический многочлен $a_0^m \prod\limits_{i=1}^{n} (b_0 x_i^m + b_1 x_i^{m-1} + \ldots + b_m)$ является многочленом от $a_0, \ldots, a_n, b_0, \ldots, b_m$. Следовательно, $R(f,g) = R(a_0, \ldots, b_m) = \lambda S$, где λ — некоторое число. С другой стороны, коэффициент при $\prod x_i^m$ у многочленов $a_0^m b_0^n P(x_1, \ldots, y_m)$ и S равен $a_0^m b_0^n$, поэтому $\lambda = 1$. □

Следствие 1. $R(g,f) = (-1)^{\deg f \deg g} R(f,g)$.

Следствие 2. Если $f = gq + r$, то

$$R(f,g) = b_0^{\deg f - \deg r} R(r,g),$$

где b_0 — старший коэффициент многочлена g.

Доказательство. Пусть y_j — корни многочлена g. Тогда $f(y_j) = r(y_j)$. Остается воспользоваться тем, что $R(f,g) = b_0^{\deg f} \prod f(y_j)$ и $R(r,g) = b_0^{\deg r} \prod f(y_j)$. □

Следствие 3. $R(f,gh) = R(f,g)R(f,h)$.

Доказательство. Пусть x_i — корни многочлена f, а a_0 — его старший коэффициент. Тогда

$$\begin{aligned} R(f,gh) &= a_0^{\deg g + \deg h} \prod g(x_i)h(x_i), \\ R(f,g) &= a_0^{\deg g} \prod g(x_i), \\ R(f,h) &= a_0^{\deg h} \prod h(x_i). \end{aligned}$$ □

Теорема 3.2. Пусть $f(x) = \sum\limits_{i=0}^{n} a_i x^{n-i}$ и $g(x) = \sum\limits_{i=0}^{m} b_i x^{m-i}$. Тогда существуют многочлены φ и ψ с целыми коэффициентами от переменных $x, a_0, \ldots, a_n, b_0, \ldots, b_m$, для которых выполняется равенство

$$\varphi(x,a,b)f(x) + \psi(x,a,b)g(x) = R(f,g).$$

Доказательство. Пусть $c_0, \ldots, c_{n+m-1}$ — столбцы матрицы Сильвестра $S(f,g)$ и $y_k = x^{m+n-k-1}$. Тогда $y_0c_0 + \ldots + y_{n+m-1}c_{n+m-1} = c$, где c — столбец $\bigl(x^{m-1}f(x), \ldots, f(x), x^{n-1}g(x), \ldots, g(x)\bigr)$. Рассмотрим это равенство как систему линейных уравнений относительно $y_0, \ldots, y_{n+m-1}$ и воспользуемся правилом Крамера, чтобы найти y_{n+m-1}. В результате получим

$$y_{n+m-1} \det(c_0, \ldots, c_{n+m-1}) = \det(c_0, \ldots, c_{n+m-2}, c). \qquad (1)$$

Остается заметить, что $y_{n+m-1} = 1$, $\det(c_0, \ldots, c_{n+m-1}) = R(f,g)$, а определитель, стоящий в правой части равенства (1), можно представить в требуемом виде. □

3.2. Дискриминант

Пусть $x_1, \ldots, x_n$ — корни многочлена $f(x) = a_0x^n + \ldots + a_n$, причем $a_0 \neq 0$. Величину $D(f) = a_0^{2n-2} \prod\limits_{i<j} (x_i - x_j)^2$ называют *дискриминантом* многочлена f.

Теорема 3.3. $R(f, f') = \pm a_0 D(f)$.

Доказательство. По теореме 3.1 $R(f, f') = a_0^{n-1} \prod\limits_i f'(x_i)$, где x_i — корни многочлена f. Легко проверить, что $f'(x_i) = a_0 \prod\limits_{j \neq i} (x_j - x_i)$. Поэтому

$$R(f, f') = a_0^{2n-1} \prod_{j \neq i} (x_j - x_i) = \pm a_0^{2n-1} \prod_{i<j} (x_j - x_i)^2. \qquad \square$$

Замечание. Несложно показать, что

$$R(f, f') = -R(f', f) = (-1)^{n(n-1)/2} a_0 D(f).$$

Следствие. Дискриминант является многочленом с целыми коэффициентами от коэффициентов многочлена f.

Теорема 3.4. Пусть f, g и h — многочлены со старшим коэффициентом 1. Тогда

$$D(fg) = D(f)D(g)R^2(f, g),$$
$$D(fgh) = D(f)D(g)D(h)R^2(f, g)R^2(g, h)R^2(h, f).$$

Доказательство. Пусть $x_1, \ldots, x_n$ — корни многочлена f, а $y_1, \ldots, y_m$ — корни многочлена g. Тогда

$$D(fg) = \prod (x_i - x_j)^2 \prod (y_i - y_j)^2 \prod (x_i - y_j)^2 = D(f)D(g)R^2(f, g).$$

Вторая формула доказывается аналогично. $\square$

Теорема 3.5. Пусть f — вещественный многочлен степени n, не имеющий вещественных корней. Тогда $\operatorname{sgn} D(f) = (-1)^{n/2}$.

Доказательство. Воспользовавшись разложением

$$f(x) = a_0(x - x_1) \cdot \ldots \cdot (x - x_n),$$

легко проверить, что

$$D\big((x-a)f(x)\big) = D\big(f(x)\big)\big(f(a)\big)^2.$$

Пусть a и $\overline{a}$ — пара сопряженных корней многочлена f, т. е. $f(x) = (x-a)(x-\overline{a})g(x)$. Тогда

$$D\big(f(x)\big) = D\big(g(x)\big)(a-\overline{a})^2\big(f(a)f(\overline{a})\big)^2.$$

Ясно, что $\operatorname{sgn}(a-\overline{a})^2 = -1$ и $\big(f(a)f(\overline{a})\big)^2 = \big|f(a)\big|^4 > 0$. Поэтому $\operatorname{sgn} D(f) = -\operatorname{sgn} D(g)$. Требуемое утверждение теперь легко доказывается индукцией по n. □

Теорема 3.6. Пусть $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами. Тогда его дискриминант $D(f)$ имеет вид $4k$ или $4k+1$, где k — целое число.

Доказательство. Пусть $x_1, \ldots, x_n$ — корни многочлена f. Тогда $D(f) = \delta^2(f)$, где $\delta(f) = \prod\limits_{i<j}(x_i - x_j)$. Рассмотрим вспомогательную величину $\delta_1(f) = \prod\limits_{i<j}(x_i + x_j)$. Ясно, что $\delta_1(f)$ — симметрическая функция от корней многочлена f, поэтому $\delta_1(f)$ — целое число. Кроме того,

$$\delta_1^2(f) - \delta^2(f) = \prod_{i<j}\big((x_i-x_j)^2 + 4x_ix_j\big) - \prod_{i<j}(x_i-x_j)^2 = 4U(x_1, \ldots, x_n),$$

где U — симметрический многочлен от $x_1, \ldots, x_n$ с целыми коэффициентами. Поэтому $D(f) = \delta_1^2(f) + 4k_1$, где k_1 — целое число. Ясно также, что $\delta_1^2(f) = 4k_2$ или $4k_2 + 1$. □

3.3. Вычисление некоторых результантов и дискриминантов

В этом параграфе мы приведем некоторые примеры вычисления результантов и дискриминантов.

Пример 3.1. $D(x^n + a) = (-1)^{n(n-1)/2}n^n a^{n-1}$.

Доказательство. Воспользуемся тем, что

$$D(f) = (-1)^{n(n-1)/2} R(f, f') = (-1)^{n(n-1)/2} \prod_{i=1}^{n} f'(x_i),$$

где $x_1, \ldots, x_n$ — корни многочлена f. В нашем случае $f'(x) = nx^{n-1}$ и $\prod x_i = (-1)^n a$, а значит, $\prod x_i^{n-1} = (-1)^{n(n-1)} a^{n-1} = a^{n-1}$. □

Пример 3.2. $D(x^{n-1} + x^{n-2} + \ldots + 1) = (-1)^{(n-1)(n-2)/2} n^{n-2}$.

Доказательство. Рассматриваемый многочлен $\varphi(x) = x^{n-1} + \ldots + 1$ удовлетворяет соотношению $(x-1)\varphi(x) = x^n - 1$. Поэтому

$$D(\varphi)\big(\varphi(1)\big)^2 = D\big((x-1)\varphi(x)\big) = D(x^n - 1) = (-1)^{(n-1)(n-2)/2} n^n.$$

Остается заметить, что $\varphi(1) = n$. □

Пример 3.3. Пусть $f_n(x) = 1 + x + \dfrac{x^2}{2!} + \ldots + \dfrac{x^n}{n!}$. Тогда

$$D(n! f_n) = (-1)^{n(n-1)/2} (n!)^n.$$

Доказательство. Коэффициент при старшем члене многочлена $g(x) = n! f_n(x)$ равен 1, поэтому

$$D(g) = (-1)^{n(n-1)/2} R(g, g') = (-1)^{n(n-1)/2} \prod_{i=1}^{n} g'(\alpha_i),$$

где $\alpha_1, \ldots, \alpha_n$ — корни многочлена f_n.

Ясно, что $g'(\alpha_i) = n! f_n'(\alpha_i) = n! f_{n-1}(\alpha_i) = n! \left(f_n(\alpha_i) - \dfrac{\alpha_i^n}{n!} \right) = -\alpha_i^n$. Поэтому

$$D(g) = (-1)^{n(n-1)/2} \prod_{i=1}^{n} (-\alpha_i^n).$$

Остается заметить, что $\prod \alpha_i = (-1)^n g(0) = (-1)^n n!$. □

Пример 3.4. Пусть $d = (r, s)$, $r_1 = r/d$ и $s_1 = s/d$. Тогда

$$R(x^r - a, x^s - b) = (-1)^s \big(a^{s_1} - b^{r_1}\big)^d.$$

Доказательство. Соотношение $R(g,f) = (-1)^{\deg f \deg g} R(f,g)$ показывает, что если требуемое утверждение верно для пары (r,s), то оно верно и для пары (s,r). В самом деле, $(-1)^{rs+d+r} = (-1)^s$. Таким образом, можно считать, что $r \geqslant s$.

При $s = 0$ утверждение очевидно. Если $s > 0$, то, поделив $x^r - a$ на $x^s - b$, получим остаток $bx^{r-s} - a$. Поэтому

$$\begin{aligned} R(x^r - a, x^s - b) &= R(bx^{r-s} - a, x^s - b) = \\ &= R(b, x^s - b) R\big(x^{r-s} - a/b, x^s - b\big) = \\ &= b^s R\big(x^{r-s} - a/b, x^s - b\big). \end{aligned}$$

Легко видеть, что если $R(x^{r-s} - a/b, x^s - b) = (-1)^s\big((a/b)^{s_1} - b^{r_1 - s_1}\big)$, то $R(x^r - a, x^s - b) = (-1)^s\big(a^{s_1} - b^{r_1}\big)^d$. Остается применить индукцию по $r + s$. □

Пример 3.5. Пусть $n > k > 0$, $d = (n,k)$, $n_1 = n/d$ и $k_1 = k/d$. Тогда

$$\begin{aligned} &D(x^n + ax^k + b) = \\ &\quad = (-1)^{n(n-1)/2} b^{k-1} \Big(n^{n_1} b^{n_1 - k_1} + (-1)^{n_1+1} (n-k)^{n_1 - k_1} k^{k_1} a^{n_1}\Big)^d. \end{aligned}$$

Доказательство [Sw]. Из формулы $D(f) = (-1)^{n(n-1)/2} R(f, f')$ получаем

$$\begin{aligned} D(x^n + ax^k + b) &= (-1)^{n(n-1)/2} R(x^n + ax^k + b, nx^{n-1} + kax^{k-1}) = \\ &= (-1)^{n(n-1)/2} n^n R(x^n + ax^k + b, x^{n-1} + n^{-1} kax^{k-1}). \end{aligned}$$

Воспользовавшись тем, что

$$R(f, x^m g) = R(f, x^m) R(f,g) = \big(f(0)\big)^m R(f,g),$$

получим

$$D(x^n + ax^k + b) = (-1)^{n(n-1)/2} n^n b^{k-1} R(x^n + ax^k + b, x^{n-k} + n^{-1} ka).$$

Остаток от деления многочлена $x^n + ax^k + b$ на $x^{n-k} + n^{-1}ka$ равен $a(1 - n^{-1}k)x^k + b$, поэтому

$$R(x^n + ax^k + b, x^{n-k} + n^{-1}ka) = R\big(a(1 - n^{-1}k)x^k + b, x^{n-k} + n^{-1}ka\big).$$

Результант пары двучленов вычислен в предыдущем примере. □

4. Разделение корней

Здесь мы обсудим различные теоремы, позволяющие вычислить или хотя бы оценить сверху количество вещественных корней многочлена, расположенных на интервале (a, b). Формулировки таких теорем часто используют понятие *числа перемен знака* в последовательности a_0, $a_1, \ldots, a_n$, где $a_0 a_n \neq 0$. Это число определяется следующим образом. Все нулевые члены рассматриваемой последовательности исключаются, а для оставшихся ненулевых членов вычисляется количество пар соседних членов разного знака.

4.1. Теорема Фурье–Бюдана

Теорема 4.1 (Фурье–Бюдан). Пусть $N(x)$ — число перемен знака в последовательности $f(x), f'(x), \ldots, f^{(n)}(x)$, где f — многочлен степени n. Тогда число корней многочлена f (с учетом их кратности), заключенных между a и b, где $f(a) \neq 0$, $f(b) \neq 0$ и $a < b$, не превосходит $N(a) - N(b)$, причем число корней может отличаться от $N(a) - N(b)$ лишь на четное число.

Доказательство. Пусть точка x движется по отрезку $[a, b]$ от a к b. Число $N(x)$ изменяется лишь в том случае, когда x проходит через корень многочлена $f^{(m)}$ при некотором $m \leqslant n$.

Рассмотрим сначала случай, когда точка x проходит через r-кратный корень x_0 многочлена $f(x)$. В окрестности точки x_0 многочлены $f(x), f'(x), \ldots, f^{(r)}(x)$ ведут себя приблизительно как $(x - x_0)^r g(x_0)$, $(x-x_0)^{r-1} r g(x_0), \ldots, r! g(x_0)$. Таким образом, при $x < x_0$ в этой последовательности происходит r перемен знака, а при $x > x_0$ в этой последовательности перемен знака не происходит (имеется в виду, что точка x достаточно близка к x_0).

Предположим теперь, что точка x проходит через r-кратный корень x_0 многочлена $f^{(m)}$, не являющийся корнем многочлена $f^{(m-1)}$ (при этом x_0 может как быть корнем f, так и не быть корнем f). Требуется доказать, что при проходе через x_0 число перемен знака в последовательности $f^{(m-1)}(x), f^{(m)}(x), \ldots, f^{(m+r)}(x)$ изменяется на неотрицательное четное число. В окрестности точки x_0 эти многочлены ведут себя приблизительно как $F(x_0), (x-x_0)^r G(x_0), (x-x_0)^{r-1} r G(x_0), \ldots, r! G(x_0)$. Если исключить $F(x_0)$, то в оставшейся последовательности при $x < x_0$ происходит ровно r перемен знака, а при $x > x_0$ перемен знака не происходит. Что же касается первых двух членов, $F(x_0)$ и $(x - x_0)^r G(x_0)$,

то в случае четного r число перемен знака при $x < x_0$ и при $x > x_0$ одно и то же, а в случае нечетного r число перемен знака при $x < x_0$ на 1 больше или меньше, чем при $x > x_0$ (в зависимости от того, имеют ли $F(x_0)$ и $G(x_0)$ один и тот же знак или разные знаки). Итак, при четном r изменение числа перемен знака равно r, а при нечетном r изменение числа перемен знака равно $r \pm 1$. В обоих случаях это изменение четно и неотрицательно. □

Следствие 1 (Правило Декарта). Количество положительных корней многочлена $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ не превосходит числа перемен знака в последовательности $a_0, a_1, \ldots, a_n$.

Доказательство. Так как $f^{(r)}(0) = r!a_{n-r}$, то $N(0)$ совпадает с числом перемен знака в последовательности коэффициентов многочлена f. Ясно также, что $N(+\infty) = 0$. □

Замечание. Якоби показал, что правило Декарта можно использовать и для оценки количества корней, заключенных между α и β. Для этого нужно сделать замену $y = \dfrac{x-\alpha}{\beta-x}$, т. е. $x = \dfrac{\alpha+\beta y}{1+y}$, и рассмотреть многочлен

$$(1+y)^n f\left(\frac{\alpha+\beta y}{1+y}\right) = b_0y^n + b_1y^{n-1} + \ldots + b_n.$$

Правило Декарта, примененное к этому многочлену, дает оценку количества корней, заключенных между α и β. В самом деле, когда x изменяется от α до β, y изменяется от 0 до ∞.

Следствие 2 (de Gua). Если в многочлене отсутствуют $2m$ последовательных членов (т. е. коэффициенты при этих членах равны нулю), то у этого многочлена не менее $2m$ мнимых корней, а если отсутствуют $2m+1$ последовательных членов, то в случае, когда их заключают члены разного знака, многочлен имеет не менее $2m$ мнимых корней, а в случае, когда их заключают члены одного знака, многочлен имеет не менее $2m+2$ мнимых корней.

В некоторых случаях сравнение перемен знаков в двух последовательностях позволяет получить более точную оценку числа корней, чем та оценка, которую дает теорема Фурье–Бюдана. Теорема такого рода

была впервые сформулирована еще Ньютоном, но доказал ее лишь Сильвестр в 1871 г. Заменим последовательность $f(x), f'(x), \ldots, f^{(n)}(x)$ на последовательность $f_0(x), f_1(x), \ldots, f_n(x)$, где

$$f_i(x) = \frac{(n-i)!}{n!} f^{(i)}(x), \tag{1}$$

и рассмотрим еще одну последовательность $F_0(x), F_1(x), \ldots, F_n(x)$, где $F_0(x) = F(x)$, $F_n(x) = f_n^2(x)$ и

$$F_i(x) = f_i^2(x) - f_{i-1}(x) f_{i+1}(x), \quad i = 1, \ldots, n-1. \tag{2}$$

Будем учитывать только те пары $f_i(x), f_{i+1}(x)$, для которых $\operatorname{sgn} F_i(x) = \operatorname{sgn} F_{i+1}(x)$. Пусть $N_+(x)$ — количество пар, для которых $\operatorname{sgn} f_i(x) = \operatorname{sgn} f_{i+1}(x)$, а $N_-(x)$ — количество тех пар, для которых $\operatorname{sgn} f_i(x) = -\operatorname{sgn} f_{i+1}(x)$.

Теорема 4.2 (Ньютон–Сильвестр). Пусть f — многочлен степени n без кратных корней. Тогда число корней многочлена f, заключенных между a и b, где $a < b$ и $f(a)f(b) \neq 0$, не превосходит как $N_+(b) - N_+(a)$, так и $N_-(a) - N_-(b)$.

Доказательство. Рассмотрим сначала случай, когда для многочлена f выполняются следующие условия:

1) никакие два последовательных многочлена f_i не имеют общих корней;

2) никакие два последовательных многочлена F_i не имеют общих корней;

3) корни многочленов f_i и F_i отличны от a и b.

В таком случае из формулы (2) следует, что у многочленов f_i и F_i нет общих корней.

Из формул (1) и (2) легко получить, что

$$f_i' = (n-i) f_{i+1}, \tag{3}$$

$$f_i F_i' = (n-i-1)(F_i f_{i+1} + F_{i+1} f_i). \tag{4}$$

Пусть точка x движется от a к b. Числа $N_\pm(x)$ изменяются лишь в том случае, когда точка x проходит либо через корень многочлена f_i, либо через корень многочлена F_i. Разберем отдельно три случая.

Случай 1: *прохождение через корень x_0 многочлена $f_0 = f$*. Если $f_0(x_0) = 0$, то

$$F_1(x_0) = f_1^2(x_0) - f_0(x_0) f_2(x_0) = f_1^2(x_0) > 0.$$

Поэтому при прохождении через x_0 в последовательности $F_0(x) = 1$, $F_1(x)$ перемен знака не происходит.

Из формулы (3) следует, что $\operatorname{sgn} f'(x) = \operatorname{sgn} f_1(x)$. Поэтому если $f_1(x_0) > 0$, то $f_0(x_0 - \varepsilon) < 0$ и $f_0(x_0 + \varepsilon) > 0$, а если $f_1(x_0) < 0$, то $f_0(x_0 - \varepsilon) > 0$ и $f_0(x_0 + \varepsilon) < 0$. В обоих случаях $f_0(x_0 - \varepsilon) f_1(x_0 - \varepsilon) < 0$ и $f_0(x_0 + \varepsilon) f_1(x_0 + \varepsilon) > 0$. Таким образом, при прохождении через x_0 величина N_+ увеличивается на 1, а величина N_- уменьшается на 1. (Речь идет только о вкладе в $N_\pm$ пары f_0, f_1.)

Случай 2: *прохождение через корень x_0 многочлена f_i, где $i \geqslant 1$*. В этом случае изменение знаков происходит в последовательности f_{i-1}, f_i, f_{i+1}. Возможные варианты знаков рассматриваемых многочленов при $x = x_0 \pm \varepsilon$ сильно ограничиваются следующими соотношениями:

1) согласно формуле (3) $\operatorname{sgn} f_{i+1} = \operatorname{sgn} f_i'$;

2) согласно формуле (2) $\operatorname{sgn} F_i(x_0) = \operatorname{sgn}\bigl(f_i^2(x_0) - f_{i-1}(x_0) f_{i+1}(x_0)\bigr) = -\operatorname{sgn}\bigl(f_{i-1}(x_0) f_{i+1}(x_0)\bigr)$;

3) $\operatorname{sgn} F_{i\pm1} = \operatorname{sgn} f_{i\pm1}^2 = 1$.

Если $F_i(x_0) < 0$, то в парах F_{i-1}, F_i и F_i, F_{i+1} происходят смены знака, а по условию мы такие пары не рассматриваем. Если же $F_i(x_0) > 0$, то $f_{i-1}(x_0) f_{i+1}(x_0) < 0$. Знаки полностью определяются знаком $f_{i+1}(x_0)$. При обоих знаках сначала пары $f_{i-1}(x_0 - \varepsilon), f_i(x_0 - \varepsilon)$ и $f_i(x_0 - \varepsilon), f_{i+1}(x_0 - \varepsilon)$ дают, соответственно, вклады в N_+ и в N_-, а затем пары $f_{i-1}(x_0 + \varepsilon), f_i(x_0 + \varepsilon)$ и $f_i(x_0 + \varepsilon), f_{i+1}(x_0 + \varepsilon)$ дают, наоборот, вклады в N_- и в N_+. Таким образом, их общий вклад как в N_+, так и в N_- не изменяется.

Случай 3: *прохождение через корень x_0 многочлена F_i*. В этом случае для знаков многочленов выполняются следующие соотношения:

1) $f_{i-1}(x_0) f_{i+1}(x_0) = f_i^2(x_0) - F_i(x_0) = f_i^2(x_0) > 0$;

2) $\operatorname{sgn} f_i' = \operatorname{sgn} f_{i+1}$;

3) из формулы (4) следует, что $\operatorname{sgn} F_i' = \operatorname{sgn} f_{i-1} f_{i+1} F_{i+1}$.

Несложный перебор возможных вариантов показывает, что либо N_+ и N_- не изменяются, либо N_+ увеличивается на 2, либо N_- уменьшается на 2.

Остается объяснить, как можно избавиться от наложенных на многочлен f условий 1)–3). Если какие-то из этих условий не выполняются, то после малого шевеления коэффициентов многочлена f эти условия будут выполняться. Но корни многочлена f некратные, поэтому при

малом шевелении коэффициентов количество корней многочлена f, лежащих строго внутри отрезка $[a, b]$, не изменяется. □

Замечание. Для многочлена f с кратными корнями можно применить чуть более тонкие рассуждения. А именно, рассматривать не произвольные малые шевеления, а лишь те, при которых вещественный корень кратности r распадается на r различных вещественных корней. Чтобы получить такое малое шевеление, удобнее изменять не коэффициенты многочлена, а его корни.

4.2. Теорема Штурма

Рассмотрим многочлены $f(x)$ и $f_1(x) = f'(x)$. Будем искать наибольший общий делитель многочленов f и f_1 по алгоритму Евклида:

$$\begin{aligned} f &= q_1 f_1 - f_2, \\ f_1 &= q_2 f_2 - f_3, \\ &\dots\dots\dots\dots\dots\dots \\ f_{n-2} &= q_{n-1} f_{n-1} - f_n, \\ f_{n-1} &= q_n f_n. \end{aligned}$$

Последовательность $f, f_1, \dots, f_{n-1}, f_n$ называют *последовательностью Штурма* многочлена f.

Теорема 4.3 (Штурм). Пусть $w(x)$ — число перемен знака в последовательности $f(x), f_1(x), \dots, f_n(x)$. Тогда количество корней многочлена f (без учета их кратности), заключенных между a и b, где $f(a) \neq \neq 0$, $f(b) \neq 0$ и $a < b$, в точности равно $w(a) - w(b)$.

Доказательство. Рассмотрим сначала случай, когда многочлен f не имеет кратных корней (т. е. многочлены f и f' не имеют общих корней). В таком случае f_n — некоторая ненулевая константа.

Проверим сначала, что если мы проходим через один из корней многочленов $f_1, \dots, f_{n-1}$, то число перемен знака не изменяется. В рассматриваемом случае соседние многочлены не имеют общих корней, т. е. если $f_r(\alpha) = 0$, то $f_{r\pm1}(\alpha) \neq 0$. Кроме того, из равенства $f_{r-1} = q_{r-1} f_r - -f_{r+1}$ следует, что $f_{r-1}(\alpha) = -f_{r+1}(\alpha)$. Но в таком случае число перемен знака в последовательности $f_{r-1}(\alpha), \varepsilon, f_{r+1}(\alpha)$ равно 2 как при $\varepsilon > 0$, так и при $\varepsilon < 0$.

Будем двигаться от a к b. Если мы проходим через корень x_0 многочлена f, то сначала числа $f(x)$ и $f'(x)$ будут разного знака, а потом эти числа будут одного знака. Таким образом, количество перемен знака в последовательности Штурма уменьшается на 1. Все остальные перемены знака, как уже было показано, при прохождении через точку x_0 сохраняются.

Рассмотрим теперь случай, когда многочлен f имеет корень x_0 кратности m. В таком случае f и f_1 имеют общий делитель $(x-x_0)^{m-1}$, поэтому многочлены $f_1,\dots,f_r$ делятся на $(x-x_0)^{m-1}$. Поделив $f, f_1, \dots$ $\dots, f_r$ на $(x-x_0)^{m-1}$, получим последовательность Штурма $\varphi, \varphi_1, \dots, \varphi_r$ для многочлена $\varphi(x) = f(x)/(x-x_0)^{m-1}$. Многочлен φ имеет некратный корень x_0, поэтому при прохождении через x_0 число перемен знака в последовательности $\varphi, \varphi_1, \dots, \varphi_r$ увеличивается на 1. Но при фиксированном x последовательность $f, f_1, \dots, f_r$ получается из последовательности $\varphi, \varphi_1, \dots, \varphi_r$ умножением на константу, поэтому число перемен знака в этих последовательностях одно и то же. □

4.3. Теорема Сильвестра

Вычисление последовательности Штурма весьма трудоемко. Сильвестр предложил следующий более элегантный метод вычисления количества вещественных корней многочлена.

Пусть f — вещественный многочлен степени n с некратными корнями $\alpha_1, \dots, \alpha_n$. Положим $s_k = \alpha_1^k + \dots + \alpha_n^k$. (Для вычисления s_k, разумеется, не нужно знать корни многочлена, потому что s_k, как симметрическая функция, выражается через коэффициенты многочлена.)

Теорема 4.4 (Сильвестр). а) Количество вещественных корней многочлена f равно сигнатуре квадратичной формы, заданной матрицей

$$\begin{pmatrix} s_0 & s_1 & \dots & s_{n-1} \\ s_1 & s_2 & \dots & s_n \\ \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & \dots & s_{2n} \end{pmatrix}.$$

б) Все корни многочлена f положительны тогда и только тогда, когда положительно определена матрица

$$\begin{pmatrix} s_1 & s_2 & \dots & s_n \\ s_2 & s_3 & \dots & s_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ s_n & s_{n+1} & \dots & s_{2n+1} \end{pmatrix}.$$

Доказательство (Эрмит). Пусть ρ — вещественный параметр. Рассмотрим квадратичную форму

$$F(x_1, \ldots, x_n) = \frac{y_1^2}{\alpha_1 + \rho} + \ldots + \frac{y_n^2}{\alpha_n + \rho}, \qquad (1)$$

где $y_r = x_1 + \alpha_r x_2 + \ldots + \alpha_r^{n-1} x_n$. Коэффициенты многочлена F являются симметрическими функциями от корней многочлена f, поэтому они вещественны. Это, в частности, означает, что форму F можно представить в виде

$$h_1^2 + \ldots + h_p^2 - h_{p+1}^2 - \ldots - h_n^2,$$

где $h_1, \ldots, h_n$ — линейные формы от $x_1, \ldots, x_n$ с действительными коэффициентами.

Действительному корню α_r соответствует слагаемое

$$\frac{y_r^2}{\alpha_r + \rho} = \frac{(x_1 + \alpha_r x_2 + \ldots + \alpha_r^{n-1} x_n)^2}{\alpha_r + \rho}.$$

Это слагаемое можно представить в виде $\pm h_r^2$, где знак плюс берется при $\alpha_r + \rho > 0$, а знак минус берется при $\alpha_r + \rho < 0$.

Пара сопряженных корней α_r и α_s дает вклад

$$F_{r,s} = (\alpha_r + \rho)^{-1} y_r^2 + (\alpha_r + \rho)^{-1} y_s^2.$$

Пусть $y_r = u + iv$ и $(\alpha_r + \rho)^{-1} y = \lambda + i\mu$, где u, v, λ, μ — вещественные числа. Тогда $y_s = u - iv$ и $(\alpha_s + \rho)^{-1} y = \lambda - i\mu$. Поэтому

$$F_{r,s} = 2\lambda(u^2 - v^2) - 4\mu uv.$$

При $u = 0$ и при $v = 0$ форма $F_{r,s}$ принимает значения разного знака, поэтому она приводится к виду $u_1^2 - v_1^2$.

В итоге получаем, что все корни многочлена f вещественны и удовлетворяют неравенству $\alpha_r > -\rho$ в том и только в том случае, когда форма (1) положительно определена. Элементы матрицы этой формы имеют вид

$$a_{ij} = \frac{\alpha_1^{i+j-2}}{\alpha_1 + \rho} + \ldots + \frac{\alpha_n^{i+j-2}}{\alpha_n + \rho}.$$

Утверждения а) и б) получаются при $\rho = +\infty$ и при $\rho = 0$ соответственно. □

Квадратичная форма, появляющаяся в теореме Сильвестра, имеет весьма интересную интерпретацию. Эта интерпретация позволит нам получить другое доказательство теоремы Сильвестра, причем даже для многочленов с кратными корнями.

Рассмотрим линейное пространство $V = \mathbb{R}[x]/(f)$, состоящее из многочленов, рассматриваемых по модулю многочлена $f \in \mathbb{R}[x]$. Будем считать, что старший коэффициент многочлена f равен 1 и $\deg f = n$. Многочлены $1, x, \ldots, x^{n-1}$ образуют базис пространства V. Каждому элементу $a \in V$ можно сопоставить линейное отображение $V \to V$, заданное формулой $v \mapsto av$ (элементы пространства V — многочлены; их можно перемножать). Пусть $\mathrm{tr}(a)$ — след этого отображения. Рассмотрим симметрическую билинейную форму $\varphi(v, w) = \mathrm{tr}(vw)$.

Теорема 4.5. а) Пусть $f(x) = (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n) \in \mathbb{R}[x]$ и $s_k = \alpha_1^k + \ldots + \alpha_n^k$. Тогда матрица формы φ относительно базиса $1, x, \ldots, x^{n-1}$ имеет вид

$$\begin{pmatrix} s_0 & s_1 & \ldots & s_{n-1} \\ s_1 & s_2 & \ldots & s_n \\ \vdots & \vdots & \ddots & \vdots \\ s_{n-1} & s_n & \ldots & s_{2n} \end{pmatrix}.$$

б) Сигнатура формы φ равна количеству различных вещественных корней многочлена f.

Доказательство. а) Разложим многочлен f над полем $\mathbb{C}$ на взаимно простые линейные множители: $f = f_1^{m_1} \cdot \ldots \cdot f_r^{m_r}$. Согласно китайской теореме об остатках (лемма на с. 84) отображение

$$h \pmod f \mapsto \bigl(h \pmod{f_1^{m_1}}, \ldots, h \pmod{f_r^{m_r}}\bigr)$$

задает канонический изоморфизм

$$\mathbb{C}[x]/(f) \cong \mathbb{C}[x]/(f_1^{m_1}) \times \ldots \times \mathbb{C}[x]/(f_r^{m_r}).$$

В этом разложении множители взаимно ортогональны относительно формы φ. Действительно, пусть многочлены h_i и h_j относятся к множителям с различными номерами i и j, т. е. $h_i \equiv 0 \pmod{f/f_i^{m_i}}$ и $h_j \equiv 0 \pmod{f/f_j^{m_j}}$. Тогда $h_i h_j \equiv 0 \pmod f$, поэтому отображение $v \mapsto h_i h_j v$ нулевое, а значит, его след равен нулю. Таким образом, $\varphi = \varphi_1 + \ldots + \varphi_r$, где φ_i — ограничение формы φ на пространство $\mathbb{C}[x]/(f_i^{m_i}) = \mathbb{C}[x]/(x - \alpha_i)^{m_i}$. Остается проверить, что $\varphi_i(1, x^k) = m_i \alpha_i^k$.

Матрица формы φ_i легко вычисляется в базисе $1, x{-}\alpha_i, \ldots, (x{-}\alpha_i)^{m_i - 1}$. Действительно, в этом базисе отображение $v \mapsto (x - \alpha_i)^k v$ представляется треугольной матрицей; след этой матрицы равен m_i при $k = 0$ и равен 0 при $k > 0$. Воспользовавшись тем, что

$$0 = \varphi_i(1, x - \alpha_i) = \varphi_i(1, x) - \alpha_i \varphi_i(1, 1) = \varphi_i(1, x) - m_i \alpha_i,$$

получим $\varphi_i(1, x) = m_i\alpha_i$. Затем с помощью равенства $\varphi_i\bigl(1, (x-\alpha_i)^k\bigr) = 0$ индукцией по k получаем $\varphi_i(1, x^k) = m_i\alpha_i^k$.

б) При вычислении сигнатуры нужно оставаться в поле $\mathbb{R}$, поэтому мы разложим многочлен f над полем $\mathbb{R}$ на взаимно простые линейные или квадратичные множители: $f = f_1^{m_1} \cdot \ldots \cdot f_r^{m_r}$. Снова рассмотрим разложение

$$\mathbb{R}[x]/(f) \cong \mathbb{R}[x]/(f_1^{m_1}) \times \ldots \times \mathbb{R}[x]/(f_r^{m_r}).$$

Нам достаточно проверить, что сигнатура ограничения формы φ на $\mathbb{R}[x]/(f_i^{m_i})$ равна 1, если $\deg f_i = 1$, и равна 0, если f_i — неприводимый над $\mathbb{R}$ многочлен степени 2. Как мы уже выясняли, в базисе $1, x-\alpha_i$, $(x-\alpha_i)^{m_i-1}$ форма φ_i записывается матрицей $\begin{pmatrix} m_i & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 0 \end{pmatrix}$. Поэтому если $\deg f_i = 1$, то сигнатура формы φ_i равна 1.

Если f_i — неприводимый над $\mathbb{R}$ многочлен степени 2, то $\mathbb{R}[x]/(f_i^{m_i}) \cong \mathbb{R}[x]/(x^2+1)^{m_i}$; здесь имеется в виду изоморфизм над $\mathbb{R}$. Таким образом, достаточно вычислить сигнатуру формы φ на $\mathbb{R}[x]/(x^2+1)^m$. Матрицу формы φ удобно вычислять в базисе $1, x^2, x^2+1, x(x^2+1)$, $(x^2+1)^2, \ldots, x(x^2+1)^{m-1}, (x^2+1)^{m-1}$. В этом базисе операторы умножения на x и на x^2 представляются матрицами

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & \ldots \\ -1 & 0 & 1 & 0 & 0 & \ldots \\ 0 & 0 & 0 & 1 & 0 & \ldots \\ 0 & 0 & -1 & 0 & 1 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix} \quad \text{и} \quad \begin{pmatrix} -1 & 0 & 1 & 0 & 0 & \ldots \\ 0 & -1 & 0 & 1 & 0 & \ldots \\ 0 & 0 & -1 & 0 & 1 & \ldots \\ 0 & 0 & 0 & -1 & 0 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Поэтому след оператора умножения на x равен 0, а след оператора умножения на x^2 равен $-2m$. Операторы умножения на $x^a(x^2+1)^k$, где $a = 0, 1, 2$ и $k \geqslant 1$, представляются диагональными матрицами с нулевыми диагоналями; такие операторы имеют нулевой след. В итоге получаем, что матрица формы φ имеет вид

$$\begin{pmatrix} 2m & 0 & 0 & \ldots & 0 \\ 0 & -2m & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & 0 \\ 0 & 0 & 0 & \ldots & 0 \end{pmatrix}.$$

Сигнатура такой формы равны нулю. □

4.4. Разделение комплексных корней

Теорема Штурма позволяет алгоритмически указать набор отрезков, которые содержат все вещественные корни вещественного многочлена, причем каждый отрезок содержит ровно один корень. Кронекер в серии работ (1869–1878) разработал теорию, позволяющую алгоритмически указать набор кругов, которые содержат все комплексные корни комплексного многочлена, причем каждый круг содержит ровно один корень. Точнее говоря, Кронекер показал, что количество комплексных корней, заключенных внутри данного круга, можно вычислить с помощью теоремы Штурма.

Пусть $z = x + iy$. Представим многочлен $P(z)$ в виде $P(z) = \varphi(x, y) + i\psi(x, y)$. Мы будем предполагать, что у многочлена P нет кратных корней, т. е. если $P(z) = 0$, то $P'(z) \neq 0$.

Корню многочлена P соответствует точка пересечения кривых $\varphi = 0$ и $\psi = 0$. Поэтому количество корней многочлена P, лежащих внутри замкнутой несамопересекающейся кривой γ, равно числу точек пересечения кривых $\varphi = 0$ и $\psi = 0$, лежащих внутри γ. Это число можно вычислить следующим образом. Будем обходить кривую γ в положительном направлении, т. е. против часовой стрелки, и каждой точке пересечения кривых γ и $\varphi = 0$ будем сопоставлять число $\varepsilon_i = \pm 1$ по следующему правилу: $\varepsilon_i = 1$, если из области $\varphi\psi > 0$ попадаем в область $\varphi\psi < 0$; $\varepsilon_i = -1$, если из области $\varphi\psi < 0$ попадаем в область $\varphi\psi > 0$.

В случае общего положения количество точек пересечения кривых γ и $\varphi = 0$ четно (при каждом прохождении через точку пересечения функция φ меняет знак), поэтому $\sum \varepsilon_i = 2k$, где k — целое число.

Теорема 4.6 (Кронекер). а) Число k равно количеству точек пересечения кривых $\varphi = 0$ и $\psi = 0$, лежащих внутри кривой γ.

б) Если γ — окружность данного радиуса с данным центром, то для заданного многочлена P число k вычисляется алгоритмически.

Доказательство. а) Ясно, что $dP(z) = (\varphi_x + i\psi_x)dx + (\psi_y - i\varphi_y)i\,dy$, поэтому $\varphi_x + i\psi_x = P'(z) = \psi_y - i\varphi_y$, а значит, $\psi_y = \varphi_x$ и $\psi_x = -\varphi_y$ (соотношения Коши–Римана). Таким образом,

$$\begin{vmatrix} \varphi_x & \varphi_y \\ \psi_x & \psi_y \end{vmatrix} = \begin{vmatrix} \varphi_x & \varphi_y \\ \varphi_y & -\varphi_x \end{vmatrix} = \varphi_x^2 + \varphi_y^2 > 0.$$

Это означает, что поворот от вектора $\operatorname{grad}\varphi = (\varphi_x, \varphi_y)$ к вектору $\operatorname{grad}\psi = (\psi_x, \psi_y)$ происходит против часовой стрелки. Геометрически

это означает, что области $\varphi\psi > 0$ и $\varphi\psi < 0$ расположены так, как показано на рис. 1.

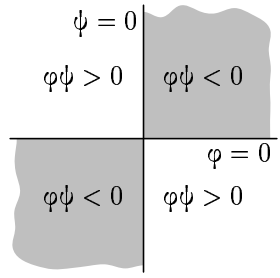

Рис. 1

Будем стягивать кривую γ в точку. При переходе через точку пересечения кривых $\varphi = 0$ и $\psi = 0$ число k уменьшается на 1 (рис. 2), а при перестройке, изображенной на рис. 3, число k не изменяется. Ясно также, что когда кривая γ станет достаточно малой, то она не будет пересекаться с кривыми $\varphi = 0$ и $\psi = 0$, а в таком случае число k будет равно 0.

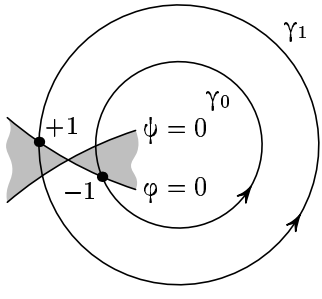

Рис. 2

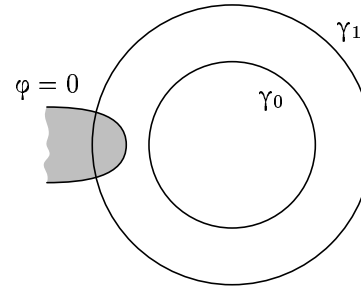

Рис. 3

б) Окружность радиуса r с центром (a, b) можно следующим образом параметризовать вещественным параметром t:

$$x = a + r\frac{1-t^2}{1+t^2}, \quad y = b + r\frac{2t}{1+t^2}.$$

Подставив эти выражения в $\varphi(x, y)$, получим многочлен $\Phi(t)$ с вещественными коэффициентами. Вещественные корни этого многочлена соответствуют точкам пересечения кривых γ и $\varphi = 0$. По теореме Штурма

для каждого корня можно найти отрезок, его содержащий. Вычислив знаки функции $\varphi\psi$ в концах этого отрезка, можно найти соответствующее ε_i. □

5. Ряд Лагранжа и оценки корней многочлена

5.1. Ряд Лагранжа–Бюрмана

Напомним, что если $f(z) = \sum\limits_{n=-\infty}^{\infty} c_n(z-a)^n$, то

$$\frac{1}{2\pi i}\int\limits_{\gamma} f(z)\,dz = c_{-1},$$

где γ — кривая, охватывающая точку a. Этим свойством мы воспользуемся для того, чтобы получить разложение функции $f(z)$ в ряд по степеням $\varphi(z) - b$, где $b = \varphi(a)$. При этом в окрестности точки a функция $\varphi(z)$ должна быть обратима, т. е. $\varphi'(a) \neq 0$. В таком случае

$$\frac{f'(z)\varphi'(a)}{\varphi(z)-\varphi(a)} = \frac{f'(z)\varphi'(a)}{\varphi'(a)(z-a)+\ldots} = \frac{f'(a)}{z-a} + \ldots,$$

поэтому

$$\frac{1}{2\pi i}\int\limits_{\gamma} \frac{f'(z)\varphi'(a)}{\varphi(z)-\varphi(a)}\,dz = f'(a).$$

Проинтегрировав это равенство, получим

$$f(z) - f(a) = \int\limits_a^z f'(\zeta)\,d\zeta = \frac{1}{2\pi i}\int\limits_a^z\int\limits_{\gamma} \frac{f'(w)\varphi'(\zeta)}{\varphi(w)-\varphi(\zeta)}\,dw\,d\zeta.$$

Преобразуем полученное выражение, выделяя члены $\varphi(z) - b$, где $b = \varphi(a)$:

$$\frac{f'(w)\varphi'(\zeta)}{\varphi(w)-\varphi(\zeta)} = \frac{f'(w)\varphi'(\zeta)}{\varphi(w)-b}\cdot\frac{\varphi(w)-b}{\varphi(w)-\varphi(\zeta)},$$
$$\frac{\varphi(w)-b}{\varphi(w)-\varphi(\zeta)} = \left(1 - \frac{\varphi(\zeta)-b}{\varphi(w)-b}\right)^{-1} = \sum_{m=0}^{\infty}\left(\frac{\varphi(\zeta)-b}{\varphi(w)-b}\right)^m.$$

Изменив порядок интегрирования, получим

$$f(z)-f(a)=\frac{1}{2\pi i}\int\limits_{\gamma}\left(\int\limits_{a}^{z}\frac{f'(w)\varphi'(\zeta)}{\varphi(w)-b}\sum_{m=0}^{\infty}\left(\frac{\varphi(\zeta)-b}{\varphi(w)-b}\right)^{m}d\zeta\right)dw.$$

При вычислении интеграла по ζ рассмотрим лишь множители, зависящие от ζ:

$$\int\limits_{a}^{z}\varphi'(z)\big(\varphi(\zeta)-b\big)^{m}d\zeta=\int\limits_{\varphi(a)}^{\varphi(z)}\big(\varphi(\zeta)-b\big)^{m}d\varphi(\zeta)=\frac{\big(\varphi(\zeta)-b\big)^{m+1}}{m+1}$$

(мы учли, что $\varphi(a)-b=0$).

Таким образом,

$$f(z)-f(a)=\sum_{m=0}^{\infty}\frac{\big(\varphi(\zeta)-b\big)^{m+1}}{m+1}\frac{1}{2\pi i}\int\limits_{\gamma}\frac{f'(w)\,dw}{\big(\varphi(\zeta)-b\big)^{m+1}}.$$

Рассмотрим такую функцию $\psi(w)$, для которой выполняется равенство $\dfrac{1}{\varphi(w)-b}=\dfrac{\psi(w)}{w-a}$, т. е.

$$\psi(w)=\frac{w-a}{\varphi(w)-b}. \tag{1}$$

Для такой функции $\psi(w)$ получаем

$$\frac{1}{2\pi i}\int\limits_{\gamma}\frac{f'(w)\,dw}{\big(\varphi(w)-b\big)^{m+1}}=\frac{1}{2\pi i}\int\limits_{\gamma}\frac{f'(w)\big(\psi(w)\big)^{m+1}dw}{(w-a)^{m+1}}=$$

$$=\frac{1}{m!}\cdot\frac{d^m}{dw^m}\Big(f'(w)\big(\psi(w)\big)^{m+1}\Big)_{w=a}.$$

В самом деле,

$$f'(w)\big(\psi(w)\big)^{m+1}=\sum_{k=0}^{\infty}c_k(w-a)^k,$$

где

$$c_k=\frac{1}{k!}\cdot\frac{d^k}{dw^k}\Big(f'(w)\big(\psi(w)\big)^{k+1}\Big)_{w=a}.$$

А интересующий нас интеграл равен коэффициенту при $(w-a)^{-1}$ ряда $\sum\limits_{k=0}^{\infty} c_k(w-a)^{k-m-1}$, т. е. он равен c_m.

В итоге получаем следующее разложение $f(z)$ по степеням $\varphi(z)-b$:

$$f(z)-f(a)=\sum_{n=1}^{\infty}\frac{\bigl(\varphi(z)-b\bigr)^n}{n!}\cdot\frac{d^{n-1}}{dw^{n-1}}\Bigl(f'(w)\bigl(\psi(w)\bigr)^n\Bigr)_{w=a}, \tag{2}$$

где $\psi(w)$ определяется формулой (1), т. е. $\psi(w)=\dfrac{w-a}{\varphi(w)-b}$. Ряд (2) называют *рядом Бюрмана*. Бюрман получил его в 1799 г., обобщая ряд, полученный Лагранжем в 1770 г. *Ряд Лагранжа* получается из ряда Бюрмана при $\varphi(z)=\dfrac{z-a}{h(z)}$, где $h(z)$ — некоторая функция. В этом случае $b=\varphi(a)=0$ и

$$\psi(z)=\frac{z-a}{\varphi(z)-b}=h(z).$$

Следовательно,

$$f(z)=f(a)+\sum_{n=0}^{\infty}\frac{s^n}{n!}\cdot\frac{d^{n-1}}{da^{n-1}}\Bigl(f'(a)\bigl(h(a)\bigr)^n\Bigr),$$

где $s=\varphi(z)$. В частности,

$$z=a+\sum_{n=0}^{\infty}\frac{s^n}{n!}\cdot\frac{d^{n-1}}{da^{n-1}}\bigl(h(a)\bigr)^n. \tag{3}$$

Таким образом, в том случае, когда ряд (3) сходится, он позволяет вычислить корень уравнения $z=a+s\,h(z)$.

Пример. Пусть $h(z)=z^{-1}$. В этом случае ряд (3) имеет вид

$$z=a+\sum_{n=1}^{\infty}\frac{(-1)^{n-1}(2n-2)!}{n!\,(n-1)!\,a^{2n-1}}\,s^n. \tag{4}$$

Ряд (4) сходится при $|s|<|a|^2/4$. Рассматриваемое уравнение $z=a+s/z$ имеет два корня, а именно,

$$\frac{a}{2}\left(1+\sqrt{1+4s^2/a^2}\right),\quad \frac{a}{2}\left(1-\sqrt{1+4s^2/a^2}\right).$$

Ряд (4) представляет только первый из этих корней.

5.2. Ряд Лагранжа и оценки корней

Ряд Лагранжа позволяет в некоторых случаях получить оценки корней многочлена. Рассмотрим, например, многочлен

$$f(z) = a_0 + a_1(z-c) + a_2(z-c)^2 + \ldots + a_k(z-c)^k.$$

Уравнение $f(z) = 0$ можно записать в виде $z = c + s\,h(z)$, где $s = -1/a_1$, $h(z) = a_0 + a_2(z-c)^2 + a_3(z-c)^3 + \ldots + a_k(z-c)^k$. Ряд Лагранжа для этого уравнения имеет вид

$$z = c + \sum_{n=1}^{\infty} \frac{s^n}{n!} \cdot \frac{d^{n-1}}{dz^{n-1}} \left(h^n(z)\right)_{z=c}.$$

В нашем случае

$$h^n(z) = \sum_{\nu_0+\nu_2+\ldots+\nu_k=n} a_0^{\nu_0} a_2^{\nu_2} \cdot \ldots \cdot a_k^{\nu_k} \frac{n!}{\nu_0!\,\nu_2! \cdot \ldots \cdot \nu_k!} (z-c)^{2\nu_2+\ldots+k\nu_k},$$

поэтому

$$\frac{d^{n-1}}{dz^{n-1}} \left(h^n(z)\right)_{z=c} = \sum \frac{(n-1)!}{\nu_0!\,\nu_2! \cdot \ldots \cdot \nu_k!} a_0^{\nu_0} a_2^{\nu_2} \cdot \ldots \cdot a_k^{\nu_k}, \qquad (1)$$

где суммирование ведется по наборам $\{\nu_0, \nu_2, \ldots, \nu_k\}$, удовлетворяющим соотношениям

$$\nu_0 + \nu_2 + \ldots + \nu_k = n, \quad 2\nu_2 + \ldots + k\nu_k = n - 1.$$

Эти соотношения эквивалентны соотношениям

$$n - 1 = 2\nu_2 + \ldots + k\nu_k, \quad \nu_0 = \nu_2 + 2\nu_3 + \ldots + (k-1)\nu_k + 1.$$

Учитывая, что $s = -1/a_1$, получаем

$$z = c - \frac{a_0}{a_1} \sum \frac{(2\nu_2 + \ldots + k\nu_k)!}{\nu_0!\,\nu_2! \cdot \ldots \cdot \nu_k!} \left(\frac{a_0 a_2}{(-a_1)^2}\right)^{\nu_2} \cdot \ldots \cdot \left(\frac{a_0^{k-1} a_k}{(-a_1)^k}\right)^{\nu_k}, \qquad (2)$$

где $\nu_0 = \nu_2 + 2\nu_3 + \ldots + (k-1)\nu_k + 1$.

Если ряд (2) сходится, то определяемое этим рядом число z является одним из корней уравнения $f(z) = 0$.

Теорема 5.1 [Be]. Пусть $|a_0| + |a_2| + \ldots + |a_k| < |a_1|$. Тогда ряд (2) сходится и для корня z, определяемого этим рядом, выполняется неравенство

$$|z - c| \leqslant -\ln\left(1 - \frac{1}{|a_1|}\big(|a_0| + |a_2| + \ldots + |a_k|\big)\right).$$

Доказательство. Из формулы (1) следует, что

$$\left|\frac{1}{n!} \cdot \frac{d^{n-1}}{dz^{n-1}}\big(h^n(z)\big)_{z=c}\right| \leqslant \frac{1}{n}\big(|a_0| + |a_2| + \ldots + |a_k|\big)^n.$$

Поэтому

$$|z - c| \leqslant \sum_{n=1}^{\infty} \frac{|a_1|^{-n}}{n}\big(|a_0| + |a_2| + \ldots + |a_k|\big)^n =$$

$$= -\ln\left(1 - \frac{1}{|a_1|}\big(|a_0| + |a_2| + \ldots + |a_k|\big)\right). \quad \square$$

Задачи к главе 1

1.1. Доказать, что многочлен $f(x)$ делится на $f'(x)$ тогда и только тогда, когда $f(x) = a_0(x - x_0)^n$.

1.2. Доказать, что многочлен

$$a_0 + a_1 x^{m_1} + a_2 x^{m_2} + \ldots + a_n x^{m_n}$$

имеет не более n положительных корней.

1.3 (Ньютон). Доказать, что если все корни многочлена

$$P(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$$

с вещественными коэффициентами вещественны и попарно различны, то

$$a_i^2 > \frac{n - i + 1}{n - 1} \cdot \frac{i + 1}{i} a_{i-1} a_{i+1}, \quad i = 1, 2, \ldots, n - 1.$$

1.4. Доказать, что многочлен

$$a_1 x^{m_1} + a_2 x^{m_2} + \ldots + a_n x^{m_n}$$

не имеет корней кратности более $n - 1$, отличных от нуля.

1.5. Найти число вещественных корней следующих многочленов:

а) $1 + x + \dfrac{x^2}{2} + \ldots + \dfrac{x^n}{n}$;

б) $nx^n - x^{n-1} - \ldots - 1$.

1.6. Пусть $0 = m_0 < m_1 < \ldots < m_n$ и $m_i \equiv i \pmod 2$. Доказать, что многочлен

$$a_0 + a_1 x^{m_1} + a_2 x^{m_2} + \ldots + a_n x^{m_n}$$

имеет не более n вещественных корней.

1.7. Пусть x_0 — корень многочлена $x^n + a_1 x^{n-1} + \ldots + a_n$. Доказать, что для любого $\varepsilon > 0$ существует такое $\delta > 0$, что если $|a_i - a_i'| < \delta$, $i = 1, \ldots, n$, то у многочлена $x^n + a_1' x^{n-1} + \ldots + a_n'$ есть корень x_0', для которого $|x_0 - x_0'| < \varepsilon$.

1.8. Пусть числа $a_1, \ldots, a_n$ попарно различны, а числа $b_1, \ldots, b_n$ положительны. Доказать, что в таком случае все корни уравнения

$$\sum \frac{b_k}{x - a_k} = x - c, \quad c \in \mathbb{R},$$

вещественны.

1.9. Найти все корни уравнения

$$\frac{(x^2 - x + 1)^3}{x^2(x-1)^2} = \frac{(a^2 - a + 1)^3}{a^2(a-1)^2}.$$

1.10. Найти число корней многочлена $x^n + x^m - 1$, абсолютные величины которых меньше 1.

1.11. Пусть $f(z) = z^n + a_1 z^{n-1} + \ldots + a_n$, где $a_1, \ldots, a_n \in \mathbb{C}$. Доказать, что любой корень z многочлена f удовлетворяет неравенствам $-\beta \leqslant \operatorname{Re} z \leqslant \alpha$, где α — единственный положительный корень многочлена

$$x^n + (\operatorname{Re} a_1)x^{n-1} - |a_2|x^{n-2} - \ldots - |a_n|,$$

а β — единственный положительный корень многочлена

$$x^n - (\operatorname{Re} a_1)x^{n-1} - |a_2|x^{n-2} - \ldots - |a_n|.$$

1.12 [Su]. Пусть $f(z)$ — многочлен степени n с комплексными коэффициентами. Доказать, что многочлен $F = f \cdot f' \cdot f'' \cdot \ldots \cdot f^{(n-1)}$ имеет по крайней мере $n + 1$ различных корней.

Решения задач

1.3. Положим $Q(y) = y^n P(y^{-1})$. Корни многочлена $Q(y)$ тоже вещественны и попарно различны, поэтому корни квадратного трехчлена

$$Q^{(n-2)}(y) = \\ = (n-2)\cdot(n-3)\cdot\ldots\cdot 4\cdot 3\left(n(n-1)a_n y^2 + 2(n-1)a_{n-1}y + 2a_{n-2}\right)$$

вещественны и различны. Следовательно,

$$(n-1)^2 a_{n-1}^2 > 2n(n-1)a_n a_{n-2}.$$

При $i = n-1$ требуемое неравенство доказано.

Рассмотрим теперь многочлен

$$P^{(n-i-1)}(x) = b_0 x^{i+1} + b_1 x^i + \ldots + b_{i+1}x^2 + b_i x + b_{i-1}.$$

Применив к нему уже доказанное неравенство, получим

$$b_i^2 > \frac{2(i+1)}{i} b_{i-1} b_{i+1}.$$

А так как

$$b_{i+1} = (n-i+1)\cdot\ldots\cdot 4\cdot 3\, a_{i+1},$$
$$b_i = (n-i)\cdot\ldots\cdot 3\cdot 2\, a_i,$$
$$b_{i-1} = (n-i-1)\cdot\ldots\cdot 2\cdot 1\, a_{i-1},$$

то

$$\left(2(n-i)a_i\right)^2 > \frac{2(i+1)}{i} 2(n-i+1)(n-i)a_{i-1}a_{i+1}.$$

После сокращения получаем требуемое неравенство.

1.11. При возрастании x от 0 до $+\infty$ функция $x^n \pm \operatorname{Re} a_1$ монотонно возрастает, а функция $|a_2|/x + |a_3|/x^2 + \ldots + |a_n|/x^{n-1}$ монотонно убывает. Поэтому у каждого из рассматриваемых многочленов положительный корень единствен.

Предположим, что $f(z) = 0$ и $\operatorname{Re} z > \alpha$. Тогда

$$\alpha + \operatorname{Re} a_1 < \operatorname{Re}(z + a_1) \leqslant |z + a_1| = |a_2/z + a_3/z^2 + \ldots + a_n/z^{n-1}| \leqslant \\ \leqslant |a_2|/|z| + \ldots + |a_n|/|z|^{n-1} < |a_2|/\alpha + \ldots + |a_n|/\alpha^{n-1}$$

(последнее неравенство следует из того, что $|z| \geqslant \operatorname{Re} z > \alpha$). С другой стороны, по условию $\alpha + \operatorname{Re} a_1 = |a_2|/\alpha + \ldots + |a_n|/\alpha^{n-1}$. Приходим к противоречию.

Оценка снизу для $\operatorname{Re} z$ получается как оценка сверху для вещественной части корня многочлена $(-1)^n f(-z)$.

1.12. Пусть $z_1, \ldots, z_m$ — различные корни многочлена F, $\mu_j(r)$ — кратность z_j как корня многочлена $f^{(r)}$, где $r = 0, 1, \ldots, n-1$. Рассмотрим симметрические функции

$$s_k(r) = \sum_{j=1}^{k} \mu_j(r) z_j^k, \tag{1}$$

т. е. $s_k(r)$ — сумма k-х степеней корней многочлена $f^{(r)}$. Элементарные симметрические функции от корней многочлена $f^{(r)}$ будем обозначать $\sigma_k(r)$; при $k > n - r$ полагаем $\sigma_k(r) = 0$.

Легко проверить, что если $f(z) = \sum\limits_{k=0}^{n} (-1)^k a_k z^{n-k}$, то

$$f^{(r)}(z) = \sum_{k=0}^{n-r} (-1)^k a_k \frac{(n-k)!}{(n-k-r)!} z^{n-k-r},$$

поэтому

$$\sigma_k(r) = \frac{a_k}{a_0} \cdot \frac{(n-k)!(n-r)!}{n!(n-k-r)!} = \frac{a_k}{a_0} \cdot \frac{(n-k)!}{n!} \cdot (n-r) \cdot \ldots \cdot (n-k-r+1).$$

Таким образом, $\sigma_k(r)$ — многочлен степени k от переменной r, причем $\sigma_k(n) = 0$.

На с. 93 для $k \geqslant 1$ доказано тождество

$$s_k = \begin{vmatrix} \sigma_1 & 1 & 0 & \ldots & 0 \\ 2\sigma_2 & \sigma_1 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k\sigma_k & \sigma_{k-1} & \sigma_{k-2} & \ldots & \sigma_1 \end{vmatrix}.$$

Из этого тождества, в частности, следует, что $s_k(r)$, где $k > 0$, можно представить в виде линейной комбинации членов $\sigma_{k_1}(r) \ldots \sigma_{k_p}(r)$, где $k_1 + \ldots + k_p = k$; коэффициенты этой линейной комбинации не зависят от r. Следовательно, если $k \geqslant 1$, то $s_k(r)$ — многочлен степени не выше k от переменной r. Ясно также, что $s_0(r) = \sum\limits_{j=1}^{m} \mu_j(r) = n - r$ и $s_k(n) = 0$ при всех $k \geqslant 0$.

Рассмотрим соотношение (1) при $k = 0, 1, \ldots, m-1$ как систему линейных уравнений относительно неизвестных $\mu_j(r)$, $j = 1, \ldots, m$. По условию числа $z_1, \ldots, z_m$ попарно различны, поэтому определитель рассматриваемой системы уравнений не равен нулю (этот определитель

является определителем Вандермонда). Решив эту систему линейных уравнений по правилу Крамера, получим представление $\mu_j(r)$ в виде линейной комбинации членов $s_k(r)$, $k = 0, \ldots, m-1$, причем в этой линейной комбинации коэффициенты не зависят от r. Следовательно, $\mu_j(r)$ — многочлен степени $d_j \leqslant m-1$ от переменной r. При этом $\mu_j(n) = 0$, так как $s_k(n) = 0$ при всех k.

Предположим, что количество различных корней многочлена F строго меньше $n+1$, т. е. $m < n+1$. Тогда $d_j \leqslant m-1 < n$, т. е. $\mu_j(r)$ — многочлен от переменной r степени не выше $n-1$. В таком случае $\Delta^1\mu_j(r) = \mu_j(r+1) - \mu_j(r)$ — многочлен степени не выше $n-2$, $\Delta^2\mu_j(r) = \Delta^1\mu_j(r+1) - \Delta^1\mu_j(r)$ — многочлен степени не выше $n-3$, ..., $\Delta^{n-1}\mu_j(r)$ — константа и $\Delta^n\mu_j(r)$ — тождественный нуль. В частности,

$$\Delta^n\mu_j(0) = \sum_{r=0}^{n}(-1)^r\binom{n}{r}\mu_j(r) = 0.$$

Чтобы прийти к противоречию, достаточно показать, что $\Delta^n\mu_1(0) \neq 0$.

Рассмотрим выпуклую оболочку корней многочлена f. По теореме Гаусса–Люка (теорема 2.1 на с. 22) она совпадает с выпуклой оболочкой точек $z_1, \ldots, z_m$. Можно считать, что z_1 — вершина выпуклой оболочки корней многочлена f. Тогда точка z_1 лежит вне выпуклой оболочки точек $z_2, \ldots, z_m$. Пусть $\mu = \mu_1(0)$ — кратность z_1 как корня многочлена f. Тогда при $0 \leqslant r \leqslant \mu - 1$ число z_1 будет корнем кратности $\mu - r$ многочлена $f^{(r)}$, а $f^{(\mu)}(z_1) \neq 0$. Выпуклая оболочка корней многочлена $f^{(\mu)}$ не содержит z_1, поэтому $f^{(r)}(z_1) \neq 0$ при $r \geqslant \mu$. Таким образом,

$$\mu_1(r) = \begin{cases} \mu - r & \text{при } 0 \leqslant r \leqslant \mu - 1; \\ 0 & \text{при } r \geqslant \mu. \end{cases}$$

Ясно также, что $\mu \leqslant n-1$, поскольку у f есть по крайней мере один корень, отличный от z_1. Поэтому

$$\Delta^2\mu_1(r) = \begin{cases} 0 & \text{при } 0 \leqslant r \leqslant n-1,\ r \neq \mu - 1; \\ 1 & \text{при } r = \mu - 1. \end{cases}$$

Следовательно, при $n > 2$ получаем

$$\Delta^n\mu_1(0) = \Delta^{n-2}\bigl(\Delta^2\mu_1\bigr)(0) = \sum_{r=0}^{n-2}(-1)^r\binom{n-2}{r}\Delta^2\mu_1(r) = (-1)^{\mu-1}\binom{n-2}{\mu-1},$$

а при $n = 2$ получаем $\mu = 1$ и $\Delta^2\mu_1(0) = 1$. В обоих случаях $\Delta^n\mu_1(0) \neq 0$, что и требовалось.

Глава 2
Неприводимые многочлены

6. Основные свойства неприводимых многочленов

6.1. Разложение многочленов на неприводимые множители

Пусть f и g — многочлены с коэффициентами из поля k. Говорят, что многочлен f *делится* на многочлен g, если $f = gh$, где h — некоторый многочлен (с коэффициентами из поля k).

Многочлен d называют *общим делителем* многочленов f и g, если f и g делятся на d. Общий делитель d многочленов f и g называют *наибольшим общим делителем* многочленов f и g, если он делится на любой общий делитель многочленов f и g. Ясно, что наибольший общий делитель определен однозначно с точностью до умножения на ненулевой элемент поля k.

Наибольший общий делитель $d = (f, g)$ многочленов f и g можно найти с помощью следующего *алгоритма Евклида*. Для определенности будем считать, что $\deg f \geqslant \deg g$. Пусть r_1 — остаток от деления f на g, r_2 — остаток от деления g на r_1, ..., r_{k+1} — остаток от деления r_{k-1} на r_k. Степени многочленов r_i строго убывают, поэтому для некоторого n получим $r_{n+1} = 0$, т. е. r_{n-1} делится на r_n. При этом f и g делятся на r_n, так как на r_n делятся многочлены $r_{n-1}, r_{n-2}, \ldots$ Кроме того, если f и g делятся на некоторый многочлен h, то r_n делится на h, так как на h делятся многочлены $r_1, r_2, \ldots$ Таким образом, $r_n = (f, g)$.

Непосредственно из алгоритма Евклида вытекают важные следствия, которые мы сформулируем в виде отдельной теоремы.

Теорема 6.1. а) Если d — наибольший общий делитель многочленов f и g, то найдутся такие многочлены a и b, что $d = af + bg$.

б) Пусть f и g многочлены над полем $k \subset K$. Тогда если у многочленов f и g есть нетривиальный общий делитель над полем K, то у них есть нетривиальный общий делитель и над полем k.

Многочлен f с коэффициентами из кольца k называют *приводимым* над k, если $f = gh$, где g и h — многочлены положительной степени с коэффициентами из кольца k. В противном случае многочлен f называют *неприводимым* над k.

Пусть $f = f_1 \cdot \ldots \cdot f_s$ — некоторое разложение многочлена f над полем k на множители $f_1, \ldots, f_s$, являющиеся многочленами над полем k. От разложения на множители с произвольными коэффициентами можно перейти к разложению со старшим коэффициентом 1. В самом деле, если $f_i(x) = a_i x^i + \ldots$ — многочлен над полем k, то $g_i = a_i^{-1} f_i$ — тоже многочлен над полем k, причем его старший коэффициент равен 1. Поэтому разложение $f = f_1 \cdot \ldots \cdot f_s$ можно заменить на разложение $f = a g_1 \cdot \ldots \cdot \ldots \cdot g_s$, где $a = a_1 \cdot \ldots \cdot a_s$. Мы не будем различать два разложения такого вида, отличающиеся лишь порядком множителей.

Кольцо многочленов от переменной x с коэффициентами в коммутативном кольце R будем обозначать $R[x]$.

Теорема 6.2. Пусть k — поле. Тогда у многочлена $f \in k[x]$ есть разложение на неприводимые множители, причем это разложение единственно.

Доказательство. Существование разложения легко доказывается индукцией по $n = \deg f$. Прежде всего отметим, что для неприводимого многочлена f требуемое разложение состоит из самого многочлена f. При $n = 1$ многочлен f неприводим. Пусть разложение существует для любого многочлена степени меньше n и f — многочлен степени n. Можно считать, что многочлен f приводим, т. е. $f = gh$, где $\deg g < n$ и $\deg h < n$. Но тогда разложения для g и h существуют по предположению индукции.

Докажем теперь единственность разложения. Пусть $a g_1 \cdot \ldots \cdot g_s = b h_1 \cdot \ldots \cdot h_t$, где $a, b \in k$ и $g_1, \ldots, g_s, h_1, \ldots, h_t$ — неприводимые многочлены над k со старшим коэффициентом 1. Ясно, что в таком случае $a = b$. Многочлен $g_1 \ldots g_s$ делится на неприводимый многочлен h_1. Это означает, что один из многочленов $g_1, \ldots, g_s$ делится на h_1. Чтобы убедиться в этом, достаточно доказать следующее вспомогательное утверждение.

Лемма. Если многочлен qr делится на неприводимый многочлен p, то один из многочленов q и r делится на p.

Доказательство. Пусть многочлен q не делится на p. Тогда $(p, q) = 1$, т. е. существуют такие многочлены a и b, что $ap + bq = 1$. Умножив обе части этого равенства на r, получим $apr + bqr = r$. Многочлены pr и qr делятся на p, поэтому r делится на p. □

Пусть для определенности g_1 делится на h_1. Учитывая, что g_1 и h_1 — неприводимые многочлены со старшим коэффициентом 1, получаем $g_1 = h_1$. Сократим обе части равенства $g_1 \cdot \ldots \cdot g_s = h_1 \cdot \ldots \cdot h_t$ на $g_1 = h_1$.

После нескольких таких операций получим $s = t$ и $g_1 = h_{i_1}, \ldots, g_s = h_{i_s}$, где $\{i_1, \ldots, i_s\} = \{1, \ldots, s\}$. □

Для кольца целых чисел $\mathbb{Z}$ неприводимость многочленов определяется точно так же, как и в случае поля, т. е. многочлен $f \in \mathbb{Z}[x]$ неприводим над $\mathbb{Z}$, если его нельзя представить в виде произведения многочленов положительной степени с целыми коэффициентами. Но в случае кольца не всегда можно поделить коэффициенты многочлена на старший коэффициент; можно лишь поделить коэффициенты на наибольший общий делитель всех коэффициентов. Это приводит к следующему определению. Пусть $f(x) = \sum a_i x^i$, где $a_i \in \mathbb{Z}$. Наибольший общий делитель коэффициентов $a_0, \ldots, a_n$ называют *содержанием* многочлена f. Содержание многочлена f обозначают $\operatorname{cont}(f)$. Ясно, что $f(x) = \operatorname{cont}(f)g(x)$, где g — многочлен над $\mathbb{Z}$ с содержанием 1.

Лемма (Гаусс). $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$.

Доказательство. Достаточно рассмотреть случай, когда $\operatorname{cont}(f) = \operatorname{cont}(g) = 1$. В самом деле, коэффициенты многочленов f и g можно разделить на $\operatorname{cont}(f)$ и $\operatorname{cont}(g)$, соответственно.

Пусть $f(x) = \sum a_i x^i$, $g(x) = \sum b_i x^i$, $fg(x) = \sum c_i x^i$. Предположим, что $\operatorname{cont}(fg) = d > 1$ и p — простой делитель числа d. Тогда все коэффициенты многочлена fg делятся на p, а у многочленов f и g есть коэффициенты, не делящиеся на p. Пусть a_r — первый коэффициент многочлена f, не делящийся на p, b_s — первый коэффициент многочлена g, не делящийся на p. Тогда

$$c_{r+s} = a_r b_s + a_{r+1}b_{s-1} + a_{r+2}b_{s-2} + \ldots + a_{r-1}b_{s+1} + a_{r-2}b_{s+2} + \ldots \equiv$$
$$\equiv a_r b_s \not\equiv 0 \pmod{p},$$

так как

$$b_{s-1} \equiv b_{s-2} \equiv \ldots \equiv b_0 \equiv 0 \pmod{p}, \quad a_{r-1} \equiv a_{r-2} \equiv \ldots \equiv a_0 \equiv 0 \pmod{p}.$$

Получено противоречие. □

Следствие. Многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$ тогда и только тогда, когда он неприводим над $\mathbb{Q}$.

Доказательство. Пусть $f \in \mathbb{Z}[x]$ и $f = gh$, где $g, h \in \mathbb{Q}[x]$. Можно считать, что $\operatorname{cont}(f) = 1$. Выберем для многочлена g натуральное число m так, что $mg \in \mathbb{Z}[x]$. Пусть $n = \operatorname{cont}(mg)$. Тогда рациональное число $r = m/n$ таково, что $rg \in \mathbb{Z}[x]$ и $\operatorname{cont}(rg) = 1$. Аналогично выберем положительное рациональное число s для многочлена h. Покажем,

что в таком случае $rs = 1$, т. е. разложение $f = (rg)(sh)$ является разложением над $\mathbb{Z}$. Действительно, согласно лемме Гаусса $\operatorname{cont}(rg)\operatorname{cont}(sh) = \operatorname{cont}(rsgh)$, т. е. $1 = \operatorname{cont}(rsf)$. Учитывая, что $\operatorname{cont}(f) = 1$, получаем $rs = 1$. □

Для вычисления разложения многочлена $f \in \mathbb{Z}[x]$ на неприводимые множители Кронекер предложил следующий алгоритм (*алгоритм Кронекера*). Пусть $\deg f = n$ и $r = [n/2]$. Если многочлен $f(x)$ приводим, то у него есть делитель $g(x)$ степени не выше r. Чтобы найти этот делитель $g(x)$, рассмотрим числа $c_j = f(j)$, $j = 0, 1, \ldots, r$. Если $c_j = 0$, то $x - j$ — делитель многочлена $f(x)$. Если же $c_j \neq 0$, то $g(j)$ — делитель числа c_j. Каждому набору $d_0, \ldots, d_r$ делителей чисел $c_0, \ldots, c_r$ соответствует ровно один многочлен $g(x)$ степени не выше r, для которого $g(j) = d_j$, $j = 0, 1, \ldots, r$. А именно,

$$g(x) = \sum_{j=0}^{r} d_j g_j(x), \qquad g_j(x) = \prod_{\substack{0 \leqslant k \leqslant r, \\ k \neq j}} \left(\frac{x-k}{j-k}\right).$$

Для каждого такого многочлена $g(x)$ нужно проверить, будут ли его коэффициенты целыми числами и будет ли он делителем многочлена $f(x)$.

Другие, более эффективные алгоритмы разложения многочленов на неприводимые множители приведены ниже (см. с. 85–87 и 313–323).

6.2. Признак Эйзенштейна

Одним из наиболее известных признаков неприводимости многочленов является следующий *признак Эйзенштейна*.

Теорема 6.3 (признак Эйзенштейна). Пусть $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ — многочлен с целыми коэффициентами, причем для некоторого простого числа p коэффициент a_n не делится на p, коэффициенты $a_0, \ldots, a_{n-1}$ делятся на p, но коэффициент a_0 не делится на p^2. Тогда f — неприводимый многочлен.

Доказательство. Предположим, что

$$f = gh = \left(\sum b_k x^k\right)\left(\sum c_l x^l\right),$$

причем g и h — многочлены положительной степени с целыми коэффициентами. Число $b_0 c_0 = a_0$ делится на p, поэтому одно из чисел b_0 и c_0

делится на p. Пусть, для определенности, b_0 делится на p. Тогда c_0 не делится на p, так как $a_0 = b_0c_0$ не делится на p^2. Если все числа b_i делятся на p, то a_n делится на p. Поэтому b_i не делится на p при некотором i, где $0 < i \leqslant \deg g < n$; можно считать, что i — наименьший номер числа b_i, не делящегося на p. С одной стороны, по условию число a_i делится на p. С другой стороны, $a_i = b_ic_0 + b_{i-1}c_1 + \ldots + b_0c_i$, причем все числа $b_{i-1}c_1, \ldots, b_0c_i$ делятся на p, а число b_ic_0 не делится на p. Получено противоречие. □

Пример 6.1. Пусть p — простое число, а число q не делится на p. Тогда многочлен $x^m - pq$ неприводим над $\mathbb{Z}$.

Пример 6.2. Если p — простое число, то многочлен $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$ неприводим.

В самом деле, к многочлену

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1}x^{p-2} + \ldots + \binom{p}{p-1}$$

можно применить признак Эйзенштейна.

Пример 6.3. Для любого натурального n многочлен

$$f(x) = 1 + x + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!}$$

неприводим.

Доказательство. Требуется доказать, что многочлен

$$n!f(x) = x^n + nx^{n-1} + n(n-1)x^{n-2} + \ldots + n!$$

неприводим над $\mathbb{Z}$. Для этого достаточно найти такое простое число p, что $n!$ делится на p, но не делится на p^2, т. е. $p \leqslant n < 2p$.

Пусть $n = 2m$ или $n = 2m + 1$. Согласно постулату Бертрана существует такое простое число p, что $m < p \leqslant 2m$ (доказательство постулата Бертрана см., например, в [Ч]). При $n = 2m$ неравенства $p \leqslant n < 2p$ очевидны. При $n = 2m + 1$ получаем неравенства $p \leqslant n - 1$ и $n - 1 < 2p$. Но в этом случае число $n - 1$ четно, поэтому из неравенства $n - 1 < 2p$ следует неравенство $n < 2p$. Ясно также, что $p \leqslant n - 1 < n$. □

6.3. Неприводимость по модулю p

Пусть $\mathbb{F}_p$ — поле вычетов по модулю p. Многочлен с целыми коэффициентами можно рассматривать и как многочлен с коэффициентами из поля $\mathbb{F}_p$. При этом неприводимый над $\mathbb{Z}$ многочлен может оказаться приводимым над полем $\mathbb{F}_p$ при всех p. Построение соответствующего примера основано на следующей теореме.

Теорема 6.4. Многочлен $P(x) = x^4+ax^2+b^2$, где $a, b \in \mathbb{Z}$, приводим над полем $\mathbb{F}_p$ при всех простых p.

Доказательство. При $p = 2$ имеется всего 4 многочлена указанного вида, а именно, x^4, $x^4 + x^2 = x^2(x^2 + 1)$, $x^4 + 1 = (x + 1)^4$, $x^4 + x^2 + 1 = (x^2 + x + 1)^2$. Все эти многочлены приводимы.

Пусть p — нечетное простое число. Тогда можно выбрать целое число s так, что $a \equiv 2s \pmod p$. В таком случае

$$\begin{aligned} P(x) = x^4 + ax^2 + b^2 &\equiv (x^2 + s)^2 - (s^2 - b^2) \equiv \\ &\equiv (x^2 + b)^2 - (2b - 2s)x^2 \equiv \\ &\equiv (x^2 - b)^2 - (-2b - 2s)x^2 \pmod p. \end{aligned}$$

Поэтому достаточно доказать, что одно из чисел $s^2 - b^2$, $2b - 2s$, $-2b - 2s$ является квадратичным вычетом по модулю p.

Напомним основные сведения из теории квадратичных вычетов. При отображении $x \mapsto x^2$ элементы x и $-x$ переходят в один и тот же элемент. Поэтому образ множества ненулевых элементов поля $\mathbb{F}_p$ при этом отображении состоит из $(p - 1)/2$ элементов. С другой стороны, если $x = y^2$, то $x^{(p-1)/2} = y^{p-1} = 1$, т. е. все $(p - 1)/2$ элементов образа удовлетворяют уравнению $x^{(p-1)/2} = 1$, которое не может иметь более $(p - 1)/2$ решений. Элементы, не лежащие в образе отображения $x \mapsto x^2$ удовлетворяют уравнению $x^{(p-1)/2} = -1$. Поэтому если два целых числа не являются квадратами по модулю p, то их произведение является квадратом по модулю p.

Предположим, что $2b - 2s$ и $-2b - 2s$ не являются квадратами по модулю p. Тогда их произведение $4(s^2 - b^2)$ — квадрат по модулю p, а значит, $s^2 - b^2$ тоже квадрат по модулю p. □

Пример 1. Многочлен $x^4 + 1$ неприводим над $\mathbb{Z}$, но приводим по модулю p при всех простых p.

Доказательство. Достаточно доказать, что многочлен x^4+1 неприводим над $\mathbb{Z}$. Корни этого многочлена имеют вид $(\pm 1 \pm i)/2$. В любой многочлен с вещественными коэффициентами невещественные корни могут входить лишь парами (комплексно сопряженными). Поэтому единственными нетривиальными вещественными делителями многочлена x^4+1 являются многочлены $x^2 \pm \sqrt{2}x+1$ с корнями $(1\pm i)/2$ и $(-1\pm i)/2$. Оба эти многочлена не лежат в $\mathbb{Z}[x]$. □

Пример 2. Пусть $c \in \mathbb{N}$ и $\sqrt{c} \notin \mathbb{Q}$. Тогда многочлен $P(x) = x^4 + 2(1-c)x^2 + (1+c)^2$ неприводим над $\mathbb{Z}$, но приводим по модулю любого простого числа p.

Доказательство. Достаточно доказать, что многочлен $P(x)$ неприводим над $\mathbb{Z}$. Легко проверить, что корни многочлена P равны $\pm\sqrt{-1+c \pm 2i\sqrt{c}} = \pm i \pm \sqrt{c}$. Объединяя комплексно сопряженные корни в пары, получим многочлены $x^2 \pm 2\sqrt{c}x + 1 + c$. Эти многочлены не лежат в $\mathbb{Z}[x]$. □

7. Признаки неприводимости

7.1. Признак Дюма

Пусть p — фиксированное простое число, $f(x) = \sum\limits_{i=0}^{n} A_i x^i$ — многочлен с целыми коэффициентами, причем $A_0 A_n \neq 0$. Запишем ненулевые коэффициенты многочлена f в виде $A_i = a_i p^{\alpha_i}$, где a_i — целое число, не делящееся на p. Каждому ненулевому коэффициенту $a_i p^{\alpha_i}$ сопоставим точку на плоскости с координатами (i, α_i). По этим точкам можно построить диаграмму Ньютона многочлена f (соответствующую простому числу p). Делается это следующим образом. Пусть $P_0 = (0, \alpha_0)$ и $P_1 = (i_1, \alpha_{i_1})$, где i_1 — наибольшее целое число, для которого ниже прямой P_0P_1 нет данных точек. Пусть, далее, $P_2 = (i_2, \alpha_{i_2})$, где i_2 — наибольшее целое число, для которого ниже прямой P_1P_2 нет данных точек и т. д. (рис. 4). Самый последний отрезок имеет вид $P_{r-1}P_r$, где $P_r = (n, \alpha_n)$. Если звенья ломаной $P_0 \ldots P_r$ проходят через точки с целочисленными координатами, то все эти точки мы тоже считаем вершинами ломаной. При этом к вершинам $P_0, \ldots, P_r$ добавляется еще $s \geqslant 0$ вершин. Полученную в результате ломаную $Q_0 \ldots Q_{r+s}$ называют *диаграммой Ньютона* (здесь $Q_0 = P_0$ и $Q_{r+s} = P_r$). Отрезки P_lP_{l+1}

и Q_iQ_{i+1} будем называть, соответственно, *сторонами* и *звеньями* диаграммы Ньютона, а векторы $\overrightarrow{Q_iQ_{i+1}}$ будем называть *векторами звеньев* диаграммы Ньютона.

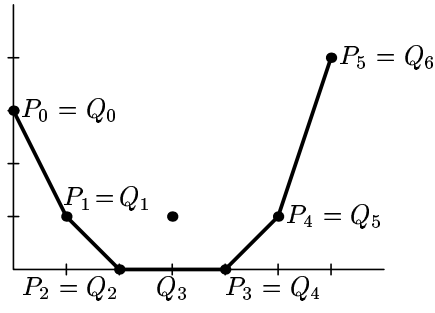

Рис. 4

Рассмотрим систему векторов звеньев диаграммы Ньютона, взяв каждый вектор с учетом его кратности, т. е. столько раз, сколько он входит в число векторов звеньев.

Теорема 7.1 (Дюма, [Dum]). Пусть $f = gh$, где f, g и h — многочлены с целыми коэффициентами. Тогда система векторов звеньев для многочлена f представляет собой объединение систем векторов звеньев для g и h. (Простое число p для всех многочленов берется одно и то же.)

Доказательство [W]. Пусть $f(x) = \sum\limits_{i=0}^{n} a_i p^{\alpha_i} x^i$, $g(x) = \sum\limits_{j=0}^{m} b_j p^{\beta_j} x^j$ и $h(x) = \sum\limits_{k=0}^{n-m} c_k p^{\gamma_k} x^k$ (числа a_i, b_j, c_k не делятся на p). Возьмем некоторую сторону P_lP_{l+1} диаграммы Ньютона многочлена f (сторона P_lP_{l+1} может состоять из нескольких звеньев диаграммы Ньютона). Пусть точки P_l и P_{l+1} имеют соответственно координаты (i_-, α_{i_-}) и (i_+, α_{i_+}). Наклон стороны P_lP_{l+1} равен

$$M = \frac{\alpha_{i_+} - \alpha_{i_-}}{i_+ - i_-}.$$

Пусть $\alpha_{i_+} - \alpha_{i_-} = At$ и $i_+ - i_- = It$, где $t > 0$ — наибольший общий делитель чисел $\alpha_{i_+} - \alpha_{i_-}$ и $i_+ - i_-$. Тогда $M = A/I$, причем $(A, I) = 1$.

Рассматриваемая сторона P_lP_{l+1} диаграммы Ньютона лежит на прямой $I\alpha - Ai = F$, где $F = I\alpha_{i_+} - Ai_+ = I\alpha_{i_-} - Ai_-$. По условию все точки (i, α_i), $i = 0, 1, \ldots, n$, лежат не ниже этой прямой, т. е. $I\alpha_i - Ai \geqslant F$,

причем это неравенство строгое при $i < i_-$ и при $i > i_+$. Будем называть число $I\alpha_i - Ai$ *весом* монома $ap^\alpha x^i$, где $(a,p) = 1$. Числа i_- и i_+ однозначно определяются как наименьший и наибольший показатели степени x мономов многочлена f с минимальным весом.

Для многочлена g рассмотрим величину

$$G = \min_{j=0,\dots,m} \{I\beta_j - Aj\}$$

и определим j_- и j_+ как наименьший и наибольший индексы, для которых

$$G = I\beta_{j_-} - Aj_- = I\beta_{j_+} - Aj_+.$$

Аналогично для многочлена h рассмотрим величину

$$H = \min_{k=0,\dots,n-m} \{I\gamma_k - Ak\}$$

и определим k_- и k_+ как наименьший и наибольший индексы, для которых

$$H = I\gamma_{k_-} - Ak_- = I\gamma_{k_+} - Ak_+.$$

Ясно, что

$$a_{j_-+k_-}p^{\alpha_{j_-+k_-}} = \sum_{j+k=j_-+k_-} (b_jp^{\beta_j}x^j)(c_kp^{\gamma_k}x^k).$$

Вес произведения двух членов равен сумме их весов, поэтому вес слагаемого с $j = j_-$ и $k = k_-$ равен $G + H$. Веса всех остальных слагаемых строго больше $G + H$, так как для них $j < j_-$ или $k < k_-$. В самом деле, пусть, например, $j < j_-$. Тогда вес члена $b_jp^{\beta_j}x^j$ строго больше G, а вес члена $c_kp^{\gamma_k}x^k$ не меньше H.

Вес члена $(b_jp^{\beta_j}x^j)(c_kp^{\gamma_k}x^k)$ при $j + k = \text{const}$ монотонно возрастает с возрастанием $\beta_j + \gamma_k$, поскольку $I > 0$. В рассматриваемом случае $j + k = j_- + k_-$, поэтому сумма $\beta_j + \gamma_k$ строго минимальна при $j = j_-$ и $k = k_-$. Следовательно, вес члена $a_{j_-+k_-}p^{\alpha_{j_-+k_-}}$ равен $G + H$. Ясно также, что при $i < j_- + k_-$ вес члена $a_ip^{\alpha_i}x^i$ строго больше $G + H$, а при $i \geqslant j_- + k_-$ вес члена $a_ip^{\alpha_i}x^i$ не меньше $G + H$. Следовательно, $G + H = F$ и $j_- + k_- = i_-$. Аналогично доказывается, что $j_+ + k_+ = i_+$. Таким образом,

$$i_+ - i_- = (j_+ - j_-) + (k_+ - k_-). \tag{1}$$

В частности, одно из чисел $j_+ - j_-$ и $k_+ - k_-$ отлично от нуля.

Если оба числа $j_+ - j_-$ и $k_+ - k_-$ отличны от нуля, то отрезок с концами (j_-, β_{j_-}) и (j_+, β_{j_+}) является стороной диаграммы Ньютона многочлена g, а отрезок с концами (k_-, γ_{k_-}) и (k_+, γ_{k_+}) является стороной диаграммы Ньютона многочлена h. Наклон сторон в обоих случаях равен $M = A/I$, так как

$$\frac{\beta_{j_+} - \beta_{j_-}}{j_+ - j_-} = \frac{A}{I} = \frac{\gamma_{k_+} - \gamma_{k_-}}{k_+ - k_-}.$$

Соотношение (1) показывает, что сумма длин сторон с наклоном M диаграмм Ньютона многочленов g и h равна длине стороны (с тем же самым наклоном M) диаграммы Ньютона многочлена f.

Если же одно из чисел $j_+ - j_-$ и $k_+ - k_-$ равно нулю, то у диаграммы Ньютона одного из многочленов g и h есть сторона с наклоном M, причем ее длина равна длине стороны диаграммы Ньютона многочлена f, а у диаграммы Ньютона другого многочлена сторон с наклоном M нет.

Итак, вектор стороны с наклоном M диаграммы Ньютона многочлена f равен сумме векторов сторон с тем же наклоном M диаграмм Ньютона многочленов g и h. Соотношение (1) показывает, что если у одной из диаграмм Ньютона многочленов g и h есть сторона с некоторым наклоном M, то у диаграммы Ньютона многочлена f тоже должна быть сторона с таким наклоном. □

Следствие (Признак Дюма). Если для некоторого простого числа p диаграмма Ньютона многочлена f состоит ровно из одного звена (т. е. состоит из отрезка, внутри которого нет точек с целочисленными координатами), то многочлен f неприводим.

Приведем теперь три примера применения теоремы Дюма для доказательства неприводимости многочленов.

Пример 7.1 (Признак Эйзенштейна). Пусть $f = a_0 + a_1 x + \ldots + a_n x^n$ — многочлен с целыми коэффициентами, причем для некоторого простого числа p коэффициент a_n не делится на p, коэффициенты $a_0, \ldots, a_{n-1}$ делятся на p и коэффициент a_0 не делится на p^2. Тогда f — неприводимый многочлен.

Доказательство. Диаграмма Ньютона многочлена f состоит из одного отрезка с концами $(0, 1)$ и $(n, 0)$; внутри этого отрезка нет точек с целочисленными координатами. □

Пример 7.2. Пусть p — простое число, $(c,p)=1$ и $(m,n)=1$. Тогда многочлен x^n+cp^m неприводим.

Доказательство. Диаграмма Ньютона рассматриваемого многочлена представляет собой отрезок с концами $(0,m)$ и $(n,0)$. Из условия $(m,n)=1$ следует, что внутри этого отрезка нет точек с целочисленными координатами. □

Пример 7.3. Пусть p — простое число. Тогда если у многочлена $f(x)=x^n+px+bp^2$, где $(b,p)=1$, нет целых корней, то этот многочлен неприводим.

Доказательство. Диаграмма Ньютона многочлена f состоит из отрезка с концами $(0,2)$ и $(1,1)$ и отрезка с концами $(1,1)$ и $(n,0)$. Внутри этих отрезков нет точек с целочисленными координатами, поэтому нетривиальное разложение многочлена f над $\mathbb{Z}$ может состоять лишь из линейного множителя и множителя степени $n-1$. □

7.2. Многочлены с доминирующим коэффициентом

В некоторых ситуациях можно утверждать, что многочлен, у которого есть достаточно большой коэффициент, обязательно будет неприводимым. Среди признаков такого рода наиболее известен следующий *признак Перрона*.

Теорема 7.2 [Pe]. Пусть $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$ — многочлен с целыми коэффициентами, причем $a_n\neq 0$.

а) Если $|a_1|>1+|a_2|+\ldots+|a_n|$, то многочлен f неприводим.

б) Если $|a_1|\geqslant 1+|a_2|+\ldots+|a_n|$ и $f(\pm 1)\neq 0$, то многочлен f неприводим.

Доказательство. а) Проверим сначала, что все корни многочлена f, за исключением ровно одного корня, лежат строго внутри единичного круга $|z|\leqslant 1$. Ясно, что требуемым свойством обладает многочлен $g(x)=x^n+a_1x^{n-1}$, поэтому согласно теореме Руше (см. с. 9) достаточно доказать, что при $|z|=1$ выполняется неравенство $\bigl|f(z)-g(z)\bigr|<\bigl|f(z)\bigr|+\bigl|g(z)\bigr|$. Но при $|z|=1$, с одной стороны,

$$\bigl|f(z)-g(z)\bigr|=|a_2z^{n-2}+\ldots+a_n|\leqslant|a_2|+\ldots+|a_n|<|a_1|-1, \qquad (1)$$

а с другой стороны,

$$\big|f(z)\big| + \big|g(z)\big| \geqslant \big|g(z)\big| = |z^n + a_1 z^{n-1}| = |z + a_1| \geqslant |a_1| - 1. \qquad (2)$$

Предположим, что многочлен f можно представить в виде произведения многочленов f_1 и f_2 положительной степени с целыми коэффициентами. Произведение корней каждого из многочленов f_1 и f_2 — целое число, не равное нулю, поэтому у каждого из этих многочленов есть корень, модуль которого не меньше 1. Но у многочлена f есть лишь один такой корень. Приходим к противоречию.

б) В случае $|a_1| = 1 + |a_2| + \ldots + |a_n|$ неравенство (1) становится нестрогим. Но при условии $f(\pm 1) \neq 0$ становится строгим неравенство (2). В самом деле, при $|z| = 1$ равенство

$$\big|f(z)\big| + \big|g(z)\big| = |a_1| - 1$$

возможно лишь в том случае, когда одновременно выполняются равенства $\big|f(z)\big| = 0$ и $|z + a_1| = |a_1| - 1$. Последнее равенство может выполняться лишь в том случае, когда $z \in \mathbb{R}$. А так как $|z| = 1$, то $z = \pm 1$. □

Теорема 7.3 [Br]. Пусть $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$ — натуральные числа, причем $n \geqslant 2$. Тогда многочлен $p(x) = x^n - a_1 x^{n-1} - a_2 x^{n-2} - \ldots - a_n$ неприводим.

Доказательство. Рассмотрим многочлен $f(x) = (x-1)p(x)$. Ясно, что

$$f(x) = x^{n+1} - b_1 x^n + b_2 x^{n-1} + \ldots + b_{n+1},$$

где $b_1 = a_1 + 1, b_2 = a_1 - a_2, \ldots, b_n = a_{n-1} - a_n, b_{n+1} = a_n$. Числа $b_1, \ldots, b_{n+1}$ натуральные и $b_1 = 1 + b_2 + \ldots + b_{n+1}$. Таким образом, многочлен $f(x)$ удовлетворяет одному из условий теоремы 7.2 (б). Но он не удовлетворяет второму условию $f(\pm 1) \neq 0$. Поэтому придется провести чуть более тонкие рассуждения. Покажем сначала, что при всех достаточно малых $\varepsilon > 0$ на окружности $|z| = 1 + \varepsilon$ многочлен $h(z) = b_1 z^n - b_2 z^{n-1} - \ldots - b_{n+1}$ по модулю строго больше многочлена $z^{n+1} = f(z) + h(z)$. В самом деле, если $|z| = 1 + \varepsilon$, то

$$\begin{aligned}\big|h(z)\big| - |z^{n+1}| &\geqslant b_1(1+\varepsilon)^n - b_2(1+\varepsilon)^{n-1} - \ldots - b_{n+1} - (1+\varepsilon)^{n+1} = \\ &= \varepsilon\big(nb_1 - (n-1)b_2 - \ldots - 2b_{n-1} - b_n - (n+1)\big) + \ldots = \\ &= \varepsilon\big(b_2 + 2b_3 + \ldots + (n-1)b_n + nb_{n+1} - 1\big) + \ldots\end{aligned}$$

Коэффициент при ε положителен, поэтому при достаточно малых $\varepsilon > 0$ выполняется неравенство $|h(z)| - |z^{n+1}| > 0$. В таком случае

$$|f(z) + h(z)| = |z^{n+1}| < |h(z)| \leqslant |f(z)| + |h(z)|,$$

поэтому согласно теореме Руше многочлен $f(z)$ имеет внутри круга $|z| \leqslant 1 + \varepsilon$ столько же корней, сколько и многочлен $h(z)$. Но все корни многочлена $h(z)$ лежат строго внутри единичного круга $|z| \leqslant 1$. В самом деле, если $|z| \geqslant 1$, то

$$\begin{aligned} |h(z)| &\geqslant b_1|z|^n - b_2|z|^{n-1} - \ldots - b_{n+1} \geqslant \\ &\geqslant |z|^n(b_1 - b_2 - \ldots - b_{n+1}) = |z|^n > 0. \end{aligned}$$

Устремив ε к нулю, получим, что внутри и на границе единичного круга расположено ровно n корней многочлена $f(x) = (x-1)p(x)$. Поэтому ровно $n-1$ корней многочлена $p(x)$ лежит внутри единичного круга и лишь один из его корней лежит вне единичного круга. Следовательно, многочлен p неприводим. □

Признак неприводимости, аналогичный признаку Перрона, но с условием не на коэффициент при x^{n-1}, а на свободный член (младший коэффициент), тоже справедлив, но лишь в том случае, когда свободный член — простое число.

Теорема 7.4 [Os]. Пусть $f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x \pm p$ — многочлен с целыми коэффициентами, причем p — простое число.

а) Если $p > 1 + |a_1| + \ldots + |a_{n-1}|$, то многочлен f неприводим.

б) Если $p \geqslant 1 + |a_1| + \ldots + |a_{n-1}|$ и среди корней многочлена f нет корней из единицы, то многочлен f неприводим.

Доказательство. Предположим, что $f(x) = g(x)h(x)$, где g и h — многочлены положительной степени с целыми коэффициентами. Произведение младших коэффициентов многочленов g и h равно $\pm p$. А так как число p простое, один из этих младших коэффициентов равен ± 1. Поэтому произведение абсолютных величин корней одного из многочленов g и h равно 1. У этого многочлена должен быть такой корень α, что $|\alpha| \leqslant 1$. При этом α должен быть также и корнем многочлена f. Из равенства $f(\alpha) = 0$ следует, что

$$p = |\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha| \leqslant 1 + |a_1| + \ldots + |a_{n-1}|.$$

В случае а) приходим к противоречию.

В случае б), т. е. в том случае, когда среди корней многочлена f нет корней из единицы, выполняется неравенство $|\alpha| < 1$, поэтому

$$p < 1 + |a_1| + \ldots + |a_{n-1}|.$$

Снова приходим к противоречию. □

7.3. Неприводимость многочленов, принимающих малые значения

Теорема 7.5 (Пойа). Пусть f — многочлен степени n с целыми коэффициентами и $m = \left[\frac{n+1}{2}\right]$. Предположим, что для попарно различных целых чисел $a_1, \ldots, a_n$ выполняются неравенства $\left|f(a_i)\right| < 2^{-m}m!$ и при этом числа $a_1, \ldots, a_n$ не являются корнями многочлена f. Тогда многочлен f неприводим.

Доказательство. Нам потребуется следующее вспомогательное утверждение.

Лемма (Пойа). Пусть g — многочлен степени k с целыми коэффициентами, $d_0 < d_1 < \ldots < d_k$ — целые числа. Тогда $\left|g(d_i)\right| \geqslant k!2^{-k}$ для некоторого i.

Доказательство. Рассмотрим многочлен

$$G(x) = (x - d_0) \cdot \ldots \cdot (x - d_k) \sum_{i=0}^{k} \frac{g(d_i)}{x - d_i} \prod_{j \neq i} \frac{1}{d_i - d_j}.$$

Легко проверить, что $G(d_i) = g(d_i)$ при $i = 0, \ldots, k$ и $\deg G \leqslant k$. Поэтому $G(x) = g(x)$.

Старший коэффициент многочлена G равен

$$\sum_{i=0}^{k} g(d_i) \prod_{j \neq i} \frac{1}{d_i - d_j}.$$

По условию он является ненулевым целым числом, поэтому его абсолютная величина не меньше 1. Следовательно, одно из чисел $\left|g(d_i)\right|$

не меньше

$$\left|\sum_{i=0}^{k}\prod_{j\neq i}\frac{1}{|d_i-d_j|}\right|^{-1}\geqslant\left|\sum_{i=0}^{k}\prod_{j\neq i}\frac{1}{|i-j|}\right|^{-1}=$$

$$=\left(\sum_{i=0}^{k}\frac{1}{i!(k-i)!}\right)^{-1}=k!\left(\sum_{i=0}^{k}\binom{k}{i}\right)^{-1}=k!2^{-k}.\quad\square$$

Предположим, что $f=gh$, где g и h — многочлены с целыми коэффициентами. Можно считать, что $\deg h\leqslant\deg g=k$. Тогда $m\leqslant k<n$. Ясно, что $g(a_i)\neq 0$ и $g(a_i)$ делит $f(a_i)$. Поэтому

$$\bigl|g(a_i)\bigr|\leqslant\bigl|f(a_i)\bigr|<2^{-m}m!.$$

С другой стороны, согласно лемме Пойа для одного из чисел a_i выполняется неравенство $\bigl|g(a_i)\bigr|\geqslant 2^{-k}k!$ (мы применяем лемму Пойа к $d_i=a_{i-1}$). Остается заметить, что если $k\geqslant m$, то $2^{-k}k!\geqslant 2^{-m}m!$. В самом деле, если $m=k+r$, то

$$\frac{m!}{k!}=(k+1)\cdot(k+2)\cdot\ldots\cdot(k+r)\leqslant 2^r=\frac{2^m}{2^k}.\quad\square$$

Пример. Многочлен $(x-1)\cdot(x-2)\cdot\ldots\cdot(x-n)+1$ неприводим.

Другие признаки неприводимости многочленов, принимающих малые значения, приведены в [Tv].

8. Неприводимость трехчленов и четырехчленов

8.1. Неприводимость многочленов $x^n\pm x^m\pm x^p\pm 1$

Пусть $f(x)=x^n+\varepsilon_1x^m+\varepsilon_2x^p+\varepsilon_3$, где $n>m>p\geqslant 1$ и $\varepsilon_i=\pm 1$. Выясним, следуя [Lj], в каком случае многочлен f неприводим. Ясно, что многочлен f неприводим тогда и только тогда, когда неприводим многочлен

$$x^nf(x^{-1})=1+\varepsilon_1x^{n-m}+\varepsilon_2x^{n-p}+\varepsilon_3x^n,$$

поэтому достаточно рассмотреть случай, когда $m+p \geqslant n$. В самом деле, если $m+p<n$, то $(n-m)+(n-p)>n$. Из дальнейшего рассмотрения можно также исключить тривиальный случай $f(x)=(x^m+\varepsilon_2)(x^p+\varepsilon_1)$, т. е. $n=m+p$ и $\varepsilon_3=\varepsilon_1\varepsilon_2$.

Будем называть многочлен $\varphi(x)$ степени s *возвратным*, если $\varphi(x)=\pm x^s\varphi(x^{-1})$.

Лемма 8.1. Пусть $f(x)=\varphi(x)\psi(x)$, где $\varphi(x)$ и $\psi(x)$ — многочлены положительной степени с целыми коэффициентами и со старшими коэффициентами 1. Тогда по крайней мере один из многочленов $\varphi(x)$ и $\psi(x)$ возвратен.

Доказательство. Пусть $r=\deg\varphi$ и $s=n-r=\deg\psi$. Рассмотрим многочлены

$$f_1(x)=x^r\varphi(x^{-1})\psi(x)=\sum_{i=0}^{n}c_ix^{n-i},$$

$$f_2(x)=x^s\psi(x^{-1})\varphi(x)=x^nf_1(x^{-1})=\sum_{i=0}^{n}c_{n-i}x^{n-i}.$$

Ясно, что

$$f_1(x)f_2(x)=x^nf(x^{-1})=(x^n+\varepsilon_1x^m+\varepsilon_2x^p+\varepsilon_3)(\varepsilon_3x^n+\varepsilon_2x^{n-p}+\varepsilon_1x^{n-m}+1).$$

Сравнение коэффициентов при x^{2n} показывает, что $c_0c_n=\varepsilon_3$, поэтому $c_0=\pm1$ и $c_n=\pm1$. Сравнение коэффициентов при x^n показывает, что

$$c_0^2+c_1^2+\ldots+c_{n-1}^2+c_n^2=1+\varepsilon_1^2+\varepsilon_2^2+\varepsilon_3^2=4,$$

т. е. $c_1^2+\ldots+c_{n-1}^2=2$. Итак, $c_0=\pm1$, $c_n=\pm1$, $c_\alpha=\pm1$ и $c_\beta=\pm1$ для некоторых $1\leqslant\alpha<\beta\leqslant n-1$; все остальные коэффициенты c_i равны нулю. Поэтому $f_1(x)f_2(x)$ можно записать в двух видах:

$$c_0c_nx^{2n}+c_\alpha c_nx^{2n-\alpha}+c_\beta c_nx^{2n-\beta}+c_0c_\alpha x^{n+\alpha}+ \\ +c_0c_\beta x^{n+\beta}+c_\alpha c_\beta x^{n+\beta-\alpha}+4x^n+\ldots \quad (1)$$

и

$$\varepsilon_3x^{2n}+\varepsilon_2x^{2n-p}+\varepsilon_1x^{2n-m}+\varepsilon_1\varepsilon_3x^{n+m}+\varepsilon_2\varepsilon_3x^{n+p}+ \\ +\varepsilon_1\varepsilon_2x^{n+m-p}+4x^n+\ldots \quad (2)$$

Чтобы сравнить (1) и (2), упорядочим мономы в порядке возрастания степеней, учитывая лишь три старших монома. Для (1) получаем четыре варианта:

$$\begin{aligned}
\beta \leqslant n/2 &\ :\ 2n > 2n-\alpha > 2n-\beta,\\
\beta > n/2,\ \alpha \leqslant n-\beta &\ :\ 2n > 2n-\alpha \geqslant n+\beta,\\
\beta > n/2,\ n/2 \geqslant \alpha > n-\beta &\ :\ 2n > n+\beta > 2n-\alpha,\\
\beta > n/2,\ \alpha > n/2 &\ :\ 2n > n+\beta > n+\alpha.
\end{aligned}$$

Для (2) получаем два варианта:

$$\begin{aligned}
n \geqslant 2m &\ :\ 2n > 2n-p > 2n-m,\\
2m > n \geqslant n+p &\ :\ 2n > 2n-p > n+m.
\end{aligned}$$

Сравнивая три старших монома в (1) и (2), для пары (α,β) получаем четыре возможных варианта:

$$(\alpha,\beta) = (p,m),\ (p,n-m),\ (m,n-p) \text{ или } (n-m,n-p).$$

Если $(\alpha,\beta) = (p,m)$, то сравнение (1) и (2) показывает, что

$$c_0c_n = \varepsilon_3, \quad c_pc_n = \varepsilon_2, \quad c_mc_n = \varepsilon_1,$$

поэтому

$$f_1(x) = c_n(\varepsilon_3x^n + \varepsilon_2x^{n-p} + \varepsilon_1x^{n-m} + 1) = c_nx^nf(x^{-1}).$$

Следовательно, $\psi(x) = c_nx^s\psi(x^{-1})$.

Если $(\alpha,\beta) = (n-m,n-p)$, то аналогично получаем

$$c_0c_n = \varepsilon_3, \quad c_0c_{n-m} = \varepsilon_1, \quad c_0c_{n-p} = \varepsilon_2,$$

поэтому

$$f_1(x) = c_0(x^n + \varepsilon_1x^m + \varepsilon_2x^p + \varepsilon_3) = c_0f(x).$$

Следовательно, $\varphi(x) = c_0x^r\varphi(x^{-1})$.

Если $(\alpha,\beta) = (p,n-m)$, то в (1) встречаются мономы степеней

$$2n,\ 2n-p,\ n+m,\ n+p,\ 2n-m,\ 2n-m-p,\ n,$$

а в (2) встречаются мономы степеней

$$2n,\ 2n-p,\ 2n-m,\ n+m,\ n+p,\ n+m-p,\ n.$$

Поэтому число $2n-m-p$ равно одному из трех чисел $n+m, n+p$, $n+m-p$. Равенства $2n-m-p=n+m$ и $2n-m-p=n+p$ противоречат предположению о том, что $n \leqslant m+p$. Поэтому $2n-m-p=n+m-p$, т. е. $n=2m$. Следовательно, $(\alpha,\beta)=(p,m)$.

Если $(\alpha,\beta)=(m,n-p)$, то аналогично получаем $n=2m$, т. е. $(\alpha,\beta)=(n-m,n-p)$. □

Лемма 8.2. Пусть λ и λ^{-1} — корни многочлена $f(x)$. Тогда выполняется одна из трех пар условий:

(I) $\lambda^n=-\varepsilon_3$ и $\lambda^{m-p}=-\varepsilon_1\varepsilon_2$,

(II) $\lambda^m=-\varepsilon_1\varepsilon_3$ и $\lambda^{n-p}=-\varepsilon_2$,

(III) $\lambda^p=-\varepsilon_2\varepsilon_3$ и $\lambda^{n-m}=-\varepsilon_1$.

Доказательство. Условия $f(\lambda)=0$ и $f(\lambda^{-1})=0$ можно записать в виде

$$\lambda^n+\varepsilon_1\lambda^m+\varepsilon_2\lambda^p+\varepsilon_3=0, \quad \lambda^n+\varepsilon_2\varepsilon_3\lambda^{n-p}+\varepsilon_1\varepsilon_3\lambda^{n-m}+\varepsilon_3=0.$$

Вычитая одно равенство из другого, получим

$$\varepsilon_2\varepsilon_3\lambda^{n-p}+\varepsilon_1\varepsilon_3\lambda^{n-m}-\varepsilon_1\lambda^m-\varepsilon_2\lambda^p=0,$$

т. е.

$$(\varepsilon_2\lambda^{m-p}+\varepsilon_1)(\varepsilon_3\lambda^{n-m}-\varepsilon_1\varepsilon_2\lambda^p)=0.$$

Поэтому либо $\lambda^p=-\varepsilon_1\varepsilon_2\lambda^m$, либо $\lambda^p=\varepsilon_1\varepsilon_2\varepsilon_3\lambda^{n-m}$. Подставив эти значения λ^p в соотношение $f(\lambda)=0$, получим, соответственно, либо $\lambda^n=-\varepsilon_3$, либо

$$(\lambda^m+\varepsilon_1\varepsilon_2)(\lambda^{n-m}-\varepsilon_1)=0.$$ □

С помощью лемм 8.1 и 8.2 легко доказать следующие две теоремы, которые, в свою очередь, приводят к полному описанию неприводимых многочленов вида $x^n+\varepsilon_1x^m+\varepsilon_2x^p+\varepsilon_3$. В обеих теоремах (как и в леммах 8.1 и 8.2) предполагается, что $n \leqslant m+p$ и $f(x) \neq (x^m+\varepsilon_2)(x^p+\varepsilon_1)$.

Теорема 8.1. а) Если у многочлена $f(x)$ нет корней, являющихся корнями из единицы, то многочлен $f(x)$ неприводим.

б) Если у многочлена $f(x)$ есть ровно q корней, являющихся корнями из единицы, то многочлен $f(x)$ можно представить в виде произведения

двух многочленов с целыми коэффициентами, один из которых имеет степень q и все данные q корней из единицы являются его корнями, а другой многочлен неприводим.

Доказательство. Пусть $f(x) = \varphi(x)\psi(x)$, где $\varphi, \psi \in \mathbb{Z}[x]$. Согласно лемме 8.1 можно считать, что если λ — корень многочлена φ, то λ^{-1} тоже корень многочлена φ. В таком случае, как следует из леммы 8.2, λ — корень из единицы. Если не все корни многочлена f являются корнями из единицы, то либо многочлен ψ неприводим над $\mathbb{Z}$, либо $\psi = \psi_1\psi_2$, где $\psi_1, \psi_2 \in \mathbb{Z}[x]$ и все корни многочлена ψ_1 являются корнями из единицы, а у многочлена ψ_2 есть корень, не являющийся корнем из единицы. В таком случае все корни многочлена $\varphi\psi_1$ являются корнями из единицы. Продолжая аналогичные рассуждения для многочлена ψ_2, получим требуемое разложение многочлена f. □

Остается выяснить, в каких случаях у многочлена f есть корни, являющиеся корнями из единицы. Ответ на этот вопрос дает следующая теорема.

Теорема 8.2. Пусть d — наибольший общий делитель чисел n, m, p. Положим

$$n_1 = n/d,\ m_1 = m/d,\ p_1 = p/d,$$
$$d_1 = (n_1, m_1 - p_1),\ d_2 = (m_1, n_1 - p_1),\ d_3 = (p_1, n_1 - m_1).$$

Тогда любой корень из единицы, являющийся одновременно корнем многочлена f, удовлетворяет одному из уравнений

$$x^{dd_1} = \pm 1, \quad x^{dd_2} = \pm 1, \quad x^{dd_3} = \pm 1,$$

причем он является некратным корнем многочлена f.

Доказательство. Пусть λ — корень из единицы, являющийся корнем многочлена f. Тогда λ^{-1} — тоже корень многочлена f. Лемма 8.2 дает три варианта условий на λ. Рассмотрим, например, вариант (I): $\lambda^n = -\varepsilon_3$ и $\lambda^{m-p} = -\varepsilon_1\varepsilon_2$. Ясно, что $(n, m-p) = dd_1$, поэтому существуют такие целые числа u и v, что $dd_1 = nu + (m-p)v$. Следовательно, $\lambda^{dd_1} = (\lambda^n)^u(\lambda^{m-p})^v = \pm 1$, так как $\lambda^n = -\varepsilon_3 = \pm 1$ и $\lambda^{m-p} = -\varepsilon_1\varepsilon_3 = \pm 1$. Варианты (II) и (III) рассматриваются аналогично.

Остается доказать, что λ — некратный корень многочлена f, т. е. $\lambda f'(\lambda) = n\lambda^n + \varepsilon_1 m\lambda^m + \varepsilon_2 p\lambda^p \neq 0$. Подставляя соотношения (I), (II)

и (III) в равенство $n\lambda^n + \varepsilon_1 m\lambda^m + \varepsilon_2 p\lambda^p = 0$, получим, соответственно, $\varepsilon_2\lambda^p(p-m) = n\varepsilon_3$, $\varepsilon_2\lambda^p(p-n) = m\varepsilon_3$, $\varepsilon_1\lambda^m(m-n) = p\varepsilon_2\varepsilon_3$. Равенство $|\lambda| = 1$ в первом случае выполняться не может, а во втором и в третьем случае это равенство означает, что $n = m + p$. При условии $n = m + p$ соотношения (II) принимают вид $\lambda^m = -\varepsilon_1\varepsilon_3$ и $\lambda^m = -\varepsilon_2$, а соотношения (III) принимают вид $\lambda^p = -\varepsilon_2\varepsilon_3$ и $\lambda^p = -\varepsilon_1$. В обоих случаях $\varepsilon_3 = \varepsilon_1\varepsilon_2$, что соответствует многочлену $f(x) = (x^m + \varepsilon_2)(x^p + \varepsilon_1)$, исключенному из рассмотрения. □

8.2. Неприводимость некоторых триномов

Воспользовавшись результатами, полученными в предыдущем параграфе, несложно выяснить, какие из триномов вида $x^n \pm x^m \pm 1$ неприводимы.

Теорема 8.3 [Lj]. Пусть $n \geqslant 2m$, $d = (n, m)$, $n_1 = n/d$ и $m_1 = m/d$. Тогда многочлен

$$g(x) = x^n + \varepsilon x^m + \varepsilon', \quad \text{где } \varepsilon = \pm 1 \text{ и } \varepsilon' = \pm 1,$$

неприводим, за исключением трех случаев, в которых $n_1 + m_1 \equiv 0 \pmod 3$:

а) n_1 и m_1 нечетны и $\varepsilon = 1$;

б) n_1 четно и $\varepsilon' = 1$;

в) m_1 четно и $\varepsilon' = \varepsilon$.

Во всех этих случаях $g(x)$ является произведением некоторого неприводимого многочлена на $x^{2d} + \varepsilon^m\varepsilon'^n x^d + 1$.

Доказательство. Случай, когда $n = 2m$ и $\varepsilon' = 1$, очевиден. Поэтому будем считать, что либо $n = 2m$ и $\varepsilon' = -1$, либо $n > 2m$. В таком случае к многочлену

$$(x^n + \varepsilon x^m + \varepsilon')(x^n - \varepsilon') = x^{2n} + \varepsilon x^{n+m} - \varepsilon\varepsilon' x^m - 1$$

можно применить теоремы 8.1 и 8.2, поскольку $2n > n + m > m$ и если $2n = (n + m) + m$, т. е. $n = 2m$, то $\varepsilon_3 \neq \varepsilon_1\varepsilon_2$. В обозначениях теоремы 8.2 имеем:

$$(2n, n + m, m) = (n, m) = d,\ d_1 = (2n_1, n_1) = n_1,\ d_3 = (m_1, n_1 - m_1) = 1$$

и $d_2 = (n_1 + m_1, 2n_1 - m_1) = (n_1 + m_1, 3n_1)$. Таким образом, $d_2 = 1$, если $n_1 + m_1 \not\equiv 0 \pmod 3$ и $d_2 = 3$, если $n_1 + m_1 \equiv 0 \pmod 3$.

Согласно теореме 8.2 корни из единицы, являющиеся одновременно корнями многочлена g, удовлетворяют одному из уравнений $x^{dd_1} = \pm 1$, $x^{dd_2} = \pm 1$, $x^{dd_3} = \pm 1$. Первое уравнение имеет вид $x^n = \pm 1$, а третье $x^d = \pm 1$. Если $x^n = \pm 1$, то $g(x) = \pm 1 + \varepsilon x^m \pm 1 \neq 0$, а если $x^d = \pm 1$, то $g(x) = \pm 1 \pm 1 \pm 1 \neq 0$. Остается рассмотреть случай, когда $d_2 = 3$. В лемме 8.2 случай (I) приводит к соотношениям $\lambda^{2n} = \pm 1$ и $\lambda^n = \pm 1$, а случай (III) приводит к соотношениям $\lambda^m = \pm 1$ и $\lambda^{n-m} = \pm 1$. В обоих случаях получаем $\lambda^n = \pm 1$, поэтому $g(\lambda) \neq 0$. Случай (II) приводит к соотношениям $\lambda^{n+m} = \varepsilon$, $\lambda^{2n-m} = \varepsilon\varepsilon'$, т. е. $\lambda^{3n} = \varepsilon'$, $\lambda^{3m} = \varepsilon\varepsilon'$. Таким образом, $(\lambda^{3d})^{n_1} = \varepsilon'$ и $(\lambda^{3d})^{m_1} = \varepsilon\varepsilon'$, где $(n_1, m_1) = 1$ и $n_1 + m_1 \equiv 0 \pmod 3$. Из условия $(n_1, m_1) = 1$ следует, что $n_1 u + m_1 v = 1$ для некоторых целых чисел u и v. Поэтому

$$\lambda^{3d} = \lambda^{3dn_1u+3dm_1v} = (\varepsilon')^u(\varepsilon\varepsilon')^v = \pm 1.$$

Если числа n_1 и m_1 нечетны, то $\lambda^{3d} = \varepsilon' = \varepsilon\varepsilon'$, поэтому $\varepsilon = 1$ и $\lambda^{3d} = \varepsilon'$.

Если число n_1 четно, то $\varepsilon' = 1$.

Если число m_1 четно, то $\varepsilon\varepsilon' = 1$. □

Согласно признаку Перрона (теорема 7.2 на с. 68) трином $x^n \pm ax^{n-1} \pm 1$, где $a \geqslant 3$ — целое число, неприводим. При $a = 2$ этот трином неприводим, если у него нет корней, равных ± 1. Все эти утверждения верны и для тринома $x^n \pm ax \pm 1$.

Неприводимость триномов $x^n \pm 2x^m \pm 1$ исследована в [Sc1].

В заключение приведем формулировки двух теорем о неприводимости триномов.

Теорема 8.4 [MS]. Пусть многочлен $x^n \pm px^m \pm 1$, где $n > m$ и p — простое число, приводим. Тогда $n/(n, m) \leqslant 4^{p^2}$.

Теорема 8.5 [Ra]. а) Многочлен $x^5 + x + n$ раскладывается в произведение неприводимых квадратного и кубического многочленов тогда и только тогда, когда $n = \pm 1$ или $n = \pm 6$.

б) Многочлен $x^5 - x + n$ раскладывается в произведение неприводимых квадратного и кубического многочленов тогда и только тогда, когда $n = \pm 15$, $n = \pm 22\,440$ или $n = \pm 2\,759\,640$.

9. Теорема неприводимости Гильберта

Пусть $f(t, x) \in \mathbb{Q}[t, x]$ — многочлен от двух переменных. Многочлен f называют *приводимым*, если $f = gh$, где $g, h \in \mathbb{Q}[t, x]$ — многочлены положительной степени.

Теорема 9.1 (Гильберт, [Hi3]). Если $f(t,x)$ — неприводимый многочлен над $\mathbb{Q}$, то существует бесконечно много рациональных чисел t_0, для которых многочлен $f(t_0,x)$ неприводим над $\mathbb{Q}$.

Мы приведем доказательство теоремы Гильберта, принадлежащее Дёрге [Dö], воспользовавшись теми изложениями этого доказательства, которые приведены в [Л2] и в [Sr]. Более современное доказательство можно найти в [Fr].

Начнем с того, что установим связь между приводимостью многочлена $f(t_0,x)$ и наличием на определенной алгебраической кривой точки с рациональными координатами (t_0,y_0). Пусть $f(t,x)\in\mathbb{Q}[t,x]$ — неприводимый многочлен. Запишем его в виде $f(t,x)=a_n(t)x^n+\ldots+a_0(t)$, где $a_i(t)\in\mathbb{Q}[t]$. Многочлену $f(t,x)$ можно сопоставить многочлен $F(x)=$ $=a_n(t)x^n+\ldots+a_0(t)$ с коэффициентами из поля $k=\mathbb{Q}(t)$. Пусть $\overline{k}$ — алгебраическое замыкание поля k. Тогда

$$F(x)=a_n(t)\cdot(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_n),$$

где $\alpha_1,\ldots,\alpha_n\in\overline{k}$ — корни неприводимого над $k=\mathbb{Q}(t)$ многочлена $F(x)=f(t,x)$. В случае, когда $a_n(t_0)\neq 0$, им можно сопоставить корни $\alpha_1',\ldots,\alpha_n'\in\overline{\mathbb{Q}}$ многочлена $f(t_0,x)$.

Предположим, что многочлен $f(t_0,x)$ приводим над $\mathbb{Q}$. После перенумерации корней можно считать, что $f(t_0,x)=a_n(t_0)g_0(x)h_0(x)$, где

$$g_0(x)=(x-\alpha_1')\cdot\ldots\cdot(x-\alpha_s')\in\mathbb{Q}[x],$$
$$h_0(x)=(x-\alpha_{s+1}')\cdot\ldots\cdot(x-\alpha_n')\in\mathbb{Q}[x].$$

Положим $g(x)=(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_s)$ и $h(x)=(x-\alpha_{s+1})\cdot\ldots\cdot(x-\alpha_n)$. Тогда $F(x)=a_n(t)g(x)h(x)$, где $g(x)$, $h(x)\in\overline{k}[x]$. По условию многочлен $F(x)$ неприводим над $k[x]$, поэтому у многочлена $g(x)$ есть некоторый коэффициент y, лежащий в $\overline{k}\setminus k$. Напомним, что $k=\mathbb{Q}(t)$, поэтому элемент y алгебраичен над $\mathbb{Q}(t)$, т. е.

$$b_m(t)y^m+b_{m-1}(t)y^{m-1}+\ldots+b_0(t)=0,\quad\text{где}\quad b_i(t)\in\mathbb{Q}(t).$$

В результате получаем некоторую алгебраическую кривую C (с рациональными коэффициентами) на плоскости (t,y). При этом коэффициенту y многочлена g соответствует коэффициент $y_0\in\mathbb{Q}$ многочлена g_0, который удовлетворяет соотношению

$$b_m(t_0)y_0^m+b_{m-1}(t_0)y_0^{m-1}+\ldots+b_0(t_0)=0,$$

т. е. на кривой C есть рациональная точка (t_0,y_0).

Итак, рассмотрим все многочлены вида $(x-\alpha_{i_1})\cdot\ldots\cdot(x-\alpha_{i_k})$, где $1\leqslant k\leqslant n-1$, и у каждого из этих многочленов выберем коэффициент, не лежащий в $\mathbb{Q}[t]$. Эти коэффициентам мы сопоставим плоские алгебраические кривые $C_1,\ldots,C_M$ с рациональными коэффициентами. При этом если точка $t_0\in\mathbb{Q}$ такова, что ни на одной из кривых $C_1,\ldots,C_M$ нет рациональных точек вида (t_0,y_0), то многочлен $f(t_0,x)$ неприводим.

Займемся теперь исследованием рациональных точек плоской алгебраической кривой C, заданной уравнением

$$b_m(t)y^m+b_{m-1}(t)y^{m-1}+\ldots+b_0(t)=0,\quad\text{где}\quad b_i(t)\in\mathbb{Z}(t).$$

Прежде всего сделаем замену переменных $\widetilde{y}=b_m(t)y$. В результате получим кривую

$$\widetilde{y}^m+b_{m-1}(t)\widetilde{y}^{m-1}+b_{m-2}(t)b_m(t)\widetilde{y}^{m-2}+\ldots+b_0(t)\big(b_m(t)\big)^{m-1}=0.$$

Если $(t_0,\widetilde{y}_0)$ — рациональная точка этой кривой и $t_0\in\mathbb{Z}$, то $\widetilde{y}_0\in\mathbb{Z}$. В дальнейшем ограничимся рассмотрением целочисленных точек кривой.

Итак, можно считать, что $b_m(t)=1$, т. е. кривая задана уравнением

$$y^m+b_{m-1}(t)y^{m-1}+\ldots+b_0(t)=0,\quad\text{где}\quad b_i(t)\in\mathbb{Z}(t).$$

Покажем, что в окрестности точки $t=\infty$ алгебраическая функция $y(t)$ имеет разложение вида $y(t)=a(t^{1/k})^n+\ldots+b+c(t^{1/k})^{-1}+\ldots$, где $t^{1/k}$ — одна из ветвей корня степени k из t (для определенности выберем ту ветвь, для которой $t^{1/k}>0$ при $t>0$). Отображение $(y,t)\mapsto t$ задает разветвленное накрытие $M^2\to\mathbb{C}P^1$, где M^2 — риманова поверхность алгебраической функции $y(t)$. Нас интересуют ветви этого разветвленного накрытия над точкой ∞. Возьмем одну из ветвей и рассмотрим ее пересечение с прообразом окрестности точки ∞. Ограничение разветвленного накрытия на это множество имеет вид $z\mapsto z^k$. Это означает, что функция $y(z)$ однозначна и $z^k=t$. Ясно также, что точка $z=\infty$ не является существенно особой точкой функции $y(z)$.

Нас интересует случай, когда существует бесконечная возрастающая последовательность натуральных чисел t_i, для которых $y(t_i)$ — вещественное (и даже целое) число. Покажем, что в таком случае все коэффициенты разложения $y(t)$ вещественны. Предположим, что не все эти коэффициенты вещественны. Пусть $\xi t^{s/k}$ — член самой старшей степени s/k с невещественным ξ. Тогда при вещественных t члены более высокой степени никак не влияют на мнимую часть суммы ряда, а при

$t \to +\infty$ члены меньшей степени малы по сравнению с $\xi t^{s/k}$ и не могут уничтожить его мнимую часть.

Остается сделать последний шаг — доказать, что числа $t_i \in \mathbb{N}$, для которых $y(t_i) \in \mathbb{Z}$, образуют множество нулевой плотности. Это легко выводится из следующего утверждения.

Теорема 9.2. Пусть $\varphi(t) = a(t^{1/k})^n + \ldots + b + c(t^{1/k})^{-1} + \ldots$ — функция вещественного переменного, представленная вещественным рядом, сходящимся при $t \geqslant R$. Предположим, что $\varphi(t)$ — не многочлен. Тогда существуют такие константы $C > 0$ и $\varepsilon \in (0,1)$, что количество натуральных чисел $t \leqslant N$, для которых $\varphi(t) \in \mathbb{Z}$, не превосходит CN^{ε}.

Доказательство. Прежде всего заметим, что в разложении производной порядка m функции $\varphi(t) = a(t^{1/k})^n + \ldots$ нет членов вида t^{ν}, где $\nu > (n/k) - m$. Поэтому можно выбрать целое число $m \geqslant 1$ так, что $\varphi^{(m)}(t) \sim ct^{-\mu}$ при $t \to \infty$, причём $\mu > 0$ и $c \neq 0$ (последнее свойство обеспечивается тем, что φ — не многочлен).

Лемма. Существуют такие положительные константы c_1 и α, что если T достаточно велико, то отрезок $[T, T + c_1 T^{\alpha}]$ содержит не более m натуральных чисел t, для которых $\varphi(t) \in \mathbb{Z}$.

Доказательство. Пусть $t_1 < \ldots < t_{m+1}$. Рассмотрим интерполяционный многочлен Лагранжа

$$f(t) = \sum_{i=1}^{m+1} \varphi(t_i) \frac{(t-t_1)\cdot\ldots\cdot(t-t_{i-1})(t-t_{i+1})\cdot\ldots\cdot(t-t_{m+1})}{(t_i-t_1)\cdot\ldots\cdot(t_i-t_{i-1})(t_i-t_{i+1})\cdot\ldots\cdot(t_i-t_{m+1})}.$$

Функция $\varphi - f$ обращается в нуль в точках $t_1, \ldots, t_{m+1}$, поэтому согласно теореме Ролля на отрезке $[t_1, t_{m+1}]$ есть такая точка ξ, что

$$\varphi^{(m)}(\xi) = f^{(m)}(\xi) = m! \sum_{i=1}^{m+1} \frac{\varphi(t_i)}{(t_i-t_1)\cdot\ldots\cdot(t_i-t_{i-1})(t_i-t_{i+1})\cdot\ldots\cdot(t_i-t_{m+1})}.$$

Таким образом, $\varphi^{(m)}(\xi)$ — рациональное число, знаменатель которого не превосходит $\prod\limits_{1 \leqslant i < j \leqslant m+1} (t_j - t_i) < (t_{m+1} - t_1)^{m(m+1)/2}$. С другой стороны, если t_1 достаточно велико, то $0 < \left|\varphi^{(m)}(\xi)\right| \leqslant c_2 t_1^{-\mu}$.

Положим $\Delta T = t_{m+1} - t_1$. Тогда $\left|f^{(m)}(\xi)\right| \geqslant \Delta T^{-m(m+1)/2}$, поэтому $c_2 t_1^{-\mu} \geqslant \Delta T^{-m(m+1)/2}$, т. е. $\Delta T > c_1 T^{\alpha}$, где $\alpha = 2\mu/m(m+1)$ и $c_1 = c_2^{-2/m(m+1)}$. □

Выберем ε так, что $1-\alpha\varepsilon=\varepsilon$, т. е. $\varepsilon=\dfrac{1}{1+\alpha}$ (при этом $0<\varepsilon<1$). Разобьем отрезок $[1,N]$ на отрезки $[1,N^\varepsilon]$ и $[N^\varepsilon,N]$. Согласно лемме любой отрезок длины $c_1(N^\varepsilon)^\alpha$, принадлежащий $[N^\varepsilon,N]$, содержит не более m натуральных чисел t, для которых $\varphi(t)\in\mathbb{Z}$. Поэтому общее количество таких натуральных чисел t на отрезке $[1,N]$ не превосходит

$$N^\varepsilon+n\frac{N-N^\varepsilon}{c_1N^{\alpha\varepsilon}}<N^\varepsilon+\frac{m}{c_1}N^{1-\alpha\varepsilon}=N^\varepsilon+\frac{m}{c_1}N^\varepsilon.$$

Таким образом, в качестве C можно взять $1+\dfrac{m}{c_1}$. □

Пусть $B(N)$ — количество натуральных чисел $t\leqslant N$, для которых $\varphi(t)\in\mathbb{Z}$. Тогда $\lim\limits_{N\to\infty}\left(CN^\varepsilon/N\right)=\lim\limits_{N\to\infty}\left(C/N^{1-\varepsilon}\right)=0$. Это, в частности, означает, что существует бесконечно много натуральных чисел t, для которых $\varphi(t)\notin\mathbb{Z}$.

10. Алгоритмы разложения на неприводимые множители

10.1. Алгоритм Берлекэмпа

В наиболее эффективных алгоритмах разложения многочлена с целыми коэффициентами на неприводимые множители используется разложение этого многочлена над полем $\mathbb{F}_p$ для некоторого простого p. Поэтому мы сначала обсудим один из алгоритмов разложения многочленов по модулю p, предложенный Берлекэмпом [Ber1].

Пусть f — многочлен с коэффициентами из поля $\mathbb{F}_p$. Можно считать, что его старший коэффициент равен 1. Прежде чем применять алгоритм Берлекэмпа, нужно избавиться от кратных неприводимых множителей многочлена f. Делается это следующим образом. Пусть $f=f_1^{n_1}\cdot\ldots\cdot f_k^{n_k}$, где $f_1,\ldots,f_k$ — попарно различные неприводимые многочлены со старшими коэффициентами 1. Легко проверить, что

$$d=(f,f')=\prod_{p\nmid n_i}f_i^{n_i-1}\prod_{p\mid n_i}f_i^{n_i},\quad\text{т. е.}\quad\frac{f}{d}=\prod_{p\nmid n_i}f_i.$$

Многочлен f разлагается в произведение многочленов d и f/d, причем в разложении многочлена f/d нет кратных неприводимых множителей.

Если $\deg d < \deg f$, то к многочлену d можно применить такую же операцию. Если же $0 < \deg d = \deg f$, то $d = \prod\limits_{p|n_i} f_i^{n_i} = g^p$. Ясно, что $\deg g < \deg f$ и по разложению многочлена g можно восстановить разложение многочлена d.

Алгоритм Берлекэмпа основан на следующей теореме.

Теорема 10.1. Пусть $f \in \mathbb{F}_p[x]$ — многочлен положительной степени n с старшим коэффициентом 1.

а) Если многочлен $h \in \mathbb{F}_p[x]$ удовлетворяет соотношению $h^p \equiv h \pmod f$, т. е. $h^p - h$ делится на f, то

$$f(x) = \prod_{a \in \mathbb{F}_p} \bigl(f(x), h(x) - a\bigr).$$

б) Пусть $f = f_1 \cdot \ldots \cdot f_k$, где $f_1, \ldots, f_k$ — попарно различные неприводимые многочлены со старшим коэффициентом 1. В таком случае многочлен h удовлетворяет соотношению $h^p \equiv h \pmod f$ тогда и только тогда, когда $h(x) \equiv a_i \pmod{f_i}$, где $a_i \in \mathbb{F}_p$. При этом каждому набору $(a_1, \ldots, a_k)$ соответствует ровно один многочлен h, степень которого меньше степени многочлена f.

Доказательство. а) Положим $F(x) = \prod\limits_{a \in \mathbb{F}_p} \bigl(f(x), h(x) - a\bigr)$. Многочлены $h(x) - a$ при различных a взаимно просты, поэтому многочлены $\bigl(f(x), h(x) - a\bigr)$ являются взаимно простыми делителями многочлена $f(x)$. Следовательно, многочлен $f(x)$ делится на их произведение $F(x)$. С другой стороны, в поле $\mathbb{F}_p$ справедливо полиномиальное тождество $\prod\limits_{a \in \mathbb{F}_p} (y - a) = y^p - y$, поэтому многочлен

$$\prod_{a \in \mathbb{F}_p} \bigl(h(x) - a\bigr) = \bigl(h(x)\bigr)^p - h(x)$$

делится на $f(x)$, а значит, многочлен $F(x)$ делится на $f(x)$. Итак, многочлены f и F делятся друг на друга, а их старшие коэффициенты равны 1, поэтому $F = f$.

б) Если $h(x) \equiv a_i \pmod{f_i}$, то $\bigl(h(x)\bigr)^p \equiv a_i^p \equiv a_i \equiv h(x) \pmod{f_i}$, а значит, $\bigl(h(x)\bigr)^p \equiv h(x) \pmod{f_1 \cdot \ldots \cdot f_k}$. Наоборот, если многочлен $\bigl(h(x)\bigr)^p - h(x) = \prod\limits_{a \in \mathbb{F}_p} \bigl(h(x) - a\bigr)$ делится на f, то он делится на все многочлены $f_1, \ldots, f_k$. Ясно также, что если неприводимый многочлен f_i

делит произведение попарно взаимно простых множителей $h(x) - a$, то он делит один из этих множителей, т. е. $h(x) \equiv a_i \pmod{f_i}$.

Существование и единственность многочлена h с заданным набором $(a_1, \ldots, a_k)$ очевидным образом вытекает из следующего утверждения (*китайская теорема об остатках для многочленов*).

Лемма. Пусть $f_1, \ldots, f_k$ — взаимно простые неприводимые многочлены над полем F, $g_1, \ldots, g_k$ — произвольные многочлены над тем же полем. Тогда существует такой многочлен h, что $h(x) \equiv g_i \pmod{f_i}$, причем этот многочлен определен однозначно по модулю многочлена $f = f_1 \cdot \ldots \cdot f_k$.

Доказательство. Многочлены f_i и $F_i = f/f_i$ взаимно просты, поэтому существуют такие многочлены a_i и b_i, что $a_i f_i + b_i F_i = 1$. При этом $b_i F_i \equiv 1 \pmod{f_i}$ и $b_i F_i \equiv 0 \pmod{f_j}$ при $j \neq i$.

Положим $h = \sum g_i b_i F_i$. Тогда $h \equiv g_i b_i F_i \pmod{f_i} \equiv g_i \pmod{f_i}$. Существование требуемого многочлена h доказано.

Единственность требуемого многочлена следует из того, что если многочлены $h_1 - g_i$ и $h_2 - g_i$ делятся на f_i, то многочлен $h_1 - h_2$ делится на $f_1 \cdot \ldots \cdot f_k = f$. □ □

Соотношение $\big(h(x)\big)^p \equiv h(x) \pmod{f}$ эквивалентно системе линейных уравнений над полем $\mathbb{F}_p$. В самом деле, пусть $h(x) = t_0 + t_1 x + \ldots + t_{n-1} x^{n-1}$ (напомним, что $\deg h < \deg f = n$). Тогда $h(x)^p = h(x^p) = t_0 + t_1 x^p + \ldots + t_{n-1} x^{p(n-1)}$. Для каждого монома x^{pj}, $j = 0, 1, \ldots, n-1$, найдем его остаток от деления на многочлен f:

$$x^{pj} \equiv \sum_{i=0}^{n-1} q_{ij} x^i \pmod{f}.$$

В результате получим систему линейных уравнений

$$\sum_{i=0}^{n-1} t_j q_{ij} = t_i, \quad i = 1, \ldots, n-1.$$

Размерность пространства решений этой системы равна k, где k — количество неприводимых множителей многочлена f. Ясно, что $q_{00} = 1$ и $q_{i0} = 0$ при $i > 0$. Поэтому система имеет тривиальное решение $t_0 = c$, $t_1 = \ldots = t_{n-1} = 0$; это решение соответствует многочлену h нулевой степени.

Пусть $h_1 = 1, h_2, \ldots, h_k$ — базис пространства решений. Если $k = 1$, то многочлен f неприводим. Если же $k > 1$, то находим наибольшие общие делители многочленов $f(x)$ и $h_2(x) - a$ для всех $a \in \mathbb{F}_p$. В результате получим набор делителей $g_1, \ldots, g_s$ многочлена f. Если $s < k$, то для каждого g_i вычислим $\bigl(g_i, h_3(x) - a\bigr)$, и т. д. до тех пор, пока не получим все k делителей.

Легко проверить, что в конце концов мы обязательно получим все k делителей. В самом деле, пусть f_1 и f_2 — разные неприводимые делители многочлена f. Рассмотрим набор $(a_1, a_2, \ldots, a_k)$, где $a_1 \neq a_2$. Ему соответствует многочлен h, для которого $h(x) \equiv a_1 \pmod{f_1}$ и $h(x) \equiv a_2 \pmod{f_2}$. Поэтому для некоторого базисного многочлена h_i должны выполняться сравнения $h_i(x) \equiv a_{1i} \pmod{f_1}$ и $h_i(x) \equiv a_{2i} \pmod{f_2}$, где $a_{1i} \neq a_{2i}$. Такой многочлен h_i разъединит множители f_1 и f_2.

Замечание. Используя идею алгоритма разложения Кантора–Цассенхауза [CZ], можно существенно увеличить эффективность алгоритма Берлекэмпа. А именно, вместо многочленов $h_i(x) - a = h_i(x) - ah_1(x)$ можно брать многочлены $H(x) = a_1h_1(x) + \ldots + a_kh_k(x)$, где $a_1, \ldots, a_k$ — случайный набор элементов $\mathbb{F}_p$, и вычислять наибольшие общие делители многочленов f и $H^{(p-1)/2} - 1$. Если многочлен f приводим и $p \geqslant 3$, то с вероятностью не менее $4/9$ мы при этом сразу же получим нетривиальное разложение.

10.2. Факторизация с помощью леммы Гензеля

На с. 61 приведен алгоритм Кронекера разложения многочлена с целыми коэффициентами на неприводимые множители, но этот алгоритм требует слишком больших вычислений. Известны и гораздо более эффективные алгоритмы. Наибольший теоретический интерес представляет алгоритм Ленстры–Ленстры–Ловаса, который мы обсудим в Дополнении (см. с. 313). Но на практике он нередко оказывается более медленным, чем алгоритм факторизации, который мы сейчас опишем.

Пусть f — многочлен с целыми коэффициентами. Если $\operatorname{cont}(f) \neq 1$, то, поделив f на $\operatorname{cont}(f)$, мы получим многочлен с содержанием 1. Пусть $f = f_1^{n_1} \cdot \ldots \cdot f_k^{n_k}$ — разложение многочлена f над $\mathbb{Z}$ на неприводимые множители. Тогда $f' = f_1^{n_1-1} \cdot \ldots \cdot f_k^{n_k-1} g$, где $g \in \mathbb{Z}[x]$. Поэтому над $\mathbb{Z}$ наибольший общий делитель многочленов f и f' тоже равен $f_1^{n_1-1} \cdot \ldots \cdot f_k^{n_k-1}$, как и над $\mathbb{Q}$. Таким образом, над $\mathbb{Z}$ многочлен f можно поделить на (f, f') и получить многочлен без кратных корней. В дальнейшем будем считать, что $\operatorname{cont}(f) = 1$ и многочлены f и f' взаимно просты.

Существуют многочлены $u,\ v \in \mathbb{Q}[x]$, для которых $uf + vf' = 1$, поэтому существуют многочлены $\overline{u}, \overline{v} \in \mathbb{Z}[x]$, для которых $\overline{u}f + \overline{v}f' = n$, $n \in \mathbb{N}$. Если простое число p взаимно просто с n, то над полем $\mathbb{F}_p$ наибольший общий делитель многочленов f и f' равен 1. Будем последовательно вычислять (f, f') над $\mathbb{F}_p$ для $p = 2, 3, 5, \ldots$ до тех пор, пока не окажется, что $(f, f') = 1$ и при этом старший коэффициент многочлена f взаимно прост с p. Это простое число p мы фиксируем и в дальнейшем будем иметь дело именно с ним.

По модулю p у многочлена f нет кратных неприводимых множителей, поэтому к нему можно применить алгоритм Берлекэмпа и получить разложение $f \equiv af_1 \cdot \ldots \cdot f_k \pmod{p}$, где $f_1, \ldots, f_k \in \mathbb{Z}[x]$ — многочлены со старшим коэффициентом 1, a — старший коэффициент многочлена f и $\deg f = \deg f_1 + \ldots + \deg f_k$. Приводимая ниже лемма Гензеля позволяет по этому разложению построить разложение многочлена f по модулю p^m.

Достаточно рассмотреть следующую ситуацию: $f \equiv f_1 f_2 \pmod{p^m}$, где $f, f_1, f_2 \in \mathbb{Z}[x]$, $\deg f = \deg f_1 + \deg f_2$, старший коэффициент многочлена f_1 равен 1, старший коэффициент многочлена f взаимно прост с p и многочлены f_1 и f_2 взаимно просты по модулю p. Последнее условие означает, что существуют многочлены $u, v \in \mathbb{Z}[x]$, для которых $uf_1 + vf_2 \equiv 1 \pmod{p}$. Если u', v' — другие такие многочлены, то $u' \equiv u + wf_2 \pmod{p}$ и $v' \equiv v - wf_1 \pmod{p}$, где $w \in \mathbb{Z}[x]$. Поэтому условие $\deg u < \deg f_2$, $\deg v < \deg f_1$ однозначно задает многочлены u и v по модулю p.

Продолжением Гензеля разложения $f \equiv f_1 f_2 \pmod{p^m}$ будем называть разложение $f \equiv \overline{f}_1 \overline{f}_2 \pmod{p^{m+1}}$ где для многочленов $\overline{f}_1$ и $\overline{f}_2$ выполняются те же самые условия, что и для многочленов f_1 и f_2, и при этом $\overline{f}_i \equiv f_i \pmod{p^m}$ и $\deg \overline{f}_i = \deg f_i$.

Лемма (Гензель). Если $m \geqslant 1$, то для любого разложения $f \equiv f_1 f_2 \pmod{p^m}$, удовлетворяющего указанным выше условиям, существует его продолжение Гензеля $f \equiv \overline{f}_1 \overline{f}_2 \pmod{p^{m+1}}$ и при этом многочлены $\overline{f}_1$ и $\overline{f}_2$ определены однозначно по модулю p^{m+1}.

Доказательство. Мы ищем такие многочлены $\overline{f}_1,\ \overline{f}_2 \in \mathbb{Z}[x]$, что $\overline{f}_i = f_i + p^m g_i$, $\deg \overline{f}_i = \deg f_i$, старший коэффициент $\overline{f}_1$ равен 1 и при этом выполняется сравнение $f \equiv \overline{f}_1 \overline{f}_2 \pmod{p^{m+1}}$ т. е.

$$f_1 f_2 + p^m (g_2 f_1 + g_1 f_2) + p^{2m} g_1 g_2 \equiv f \pmod{p^{m+1}}.$$

Ясно, что $p^{2m} g_1 g_2 \equiv 0 \pmod{p^{m+1}}$, поэтому мы приходим к сравнению

$$g_2 f_1 + g_1 f_2 \equiv d \pmod{p}, \tag{1}$$

где $d = p^{-m}(f - f_1 f_2) \in \mathbb{Z}[x]$. Решения сравнения (1) можно получить с помощью многочленов u и v, для которых $uf_1 + vf_2 \equiv 1 \pmod{p}$. А именно, $g_1 \equiv dv + wf_1 \pmod{p}$ и $g_2 \equiv du - wf_2 \pmod{p}$, где $w \in \mathbb{Z}[x]$ — произвольный многочлен. Из того, что $\overline{f}_1 = f_1 + p^m g_1$ и старшие коэффициенты многочленов f_1 и $\overline{f}_1$ равны 1, следует, что $\deg g_1 < \deg f_1$. Поэтому при заданном v многочлен g_1 по модулю p определен однозначно. В таком случае многочлен g_2 по модулю p тоже определен однозначно. Следовательно, многочлены $\overline{f}_1$ и $\overline{f}_2$ определены однозначно по модулю p^{m+1}. □

Замечание. Процесс вычисления разложения многочлена по модулю p^m, где m велико, можно существенно ускорить, если рассматривать поднятия разложений по модулю q до разложений по модулю qr, где $r = (p, q)$. Подробности см. в [Coh].

Чтобы получить разложение многочлена $f \in \mathbb{Z}[x]$ на неприводимые множители, можно поступить следующим образом. (Мы предполагаем, что $\operatorname{cont}(f) = 1$ и у многочлена f нет кратных корней.) С помощью неравенства Миньотта (теорема 17.6 на с. 171) получим оценку M для коэффициентов делителей многочлена f, степень которых не превосходит $\frac{1}{2}\deg f$. Затем выберем m так, что $p^m > 2aM$, где $a > 0$ — старший коэффициент многочлена f. После этого с помощью алгоритма Берлекэмпа и леммы Гензеля построим разложение $f \equiv a \cdot f_1 \cdot \ldots \cdot f_k \pmod{p^m}$, где $f_1, \ldots, f_k \in \mathbb{Z}[x]$ — многочлены со старшим коэффициентом 1.

Пусть $g(x) = a_1 x^l + \ldots \in \mathbb{Z}[x]$ — делитель многочлена f. Тогда $a_2 = a/a_1 \in \mathbb{N}$ и многочлен $a_2 g$ по модулю p имеет вид $a \cdot f_{i_1} \cdot \ldots \cdot f_{i_d}$. Условие $p^m > 2aM$ показывает, что многочлен $a_2 g$ однозначно восстанавливается по многочлену $a \cdot f_1 \cdot \ldots \cdot f_k \pmod{p^m}$. В самом деле, коэффициенты многочлена $a_2 g$ заключены строго между $\pm\frac{1}{2}p^m$, поэтому они однозначно восстанавливаются по своим остаткам от деления на p^m.

Задачи к главе 2

2.1. Пусть $f \in \mathbb{Z}[x]$ — многочлен с корнями $\alpha_1, \ldots, \alpha_n$ и $M = \max\limits_i |\alpha_i|$. Доказать, что если $f(x_0)$ — простое число для некоторого целого x_0, причем $|x_0| > M + 1$, то многочлен f неприводим.

2.2. Пусть p — простое число. Доказать, что многочлен $x^p - x - a$, где a — натуральное число, не делящееся на p, неприводим.

2.3. Пусть для многочлена $f \in \mathbb{Z}[x]$ существует такое целое число n, что:

1) все корни многочлена f лежат в полуплоскости $\operatorname{Re} z < n - \frac{1}{2}$;

2) $f(n-1) \neq 0$;

3) $f(n)$ — простое число.

Доказать, что многочлен f неприводим.

2.4 [Kl]. а) Пусть $f(x) = f_n x^n + \ldots + f_0 \in \mathbb{Z}[x]$, причем $|f_0| > 1$. Пусть, далее, $\{c_1, \ldots, c_r\}$ — все делители числа $|f_0|$. Предположим, что в n различных целых точках $a_1, \ldots, a_n$ многочлен f принимает простые значения $p_1, \ldots, p_n$ и при этом $|a_i| > 2$ и a_i не делит $c_j \pm 1$, где $i = 1, \ldots, n$ и $j = 1, \ldots, r$. Доказать, что многочлен f неприводим.

б) Пусть целые числа $a_1, \ldots, a_n, r$ и s таковы, что $|a_k| > 2$, числа $q = (-1)^n a_1 \cdot \ldots \cdot a_n + s$ и $p_k = r a_k + s$, где $k = 1, \ldots, n$, простые и при этом a_k не делит $q \pm 1$. Доказать, что многочлен $f(x) = (x - a_1) \cdot \ldots \cdot \ldots \cdot (x - a_n) + rx + s$ неприводим.

2.5. Пусть $f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + p a_n$ — многочлен с целыми коэффициентами, причем p — простое число. Доказать, что если $p > \sum\limits_{i=0}^{n-1} |a_n|^{n-1-i} |a_i|$, то многочлен f неприводим.

2.6. Пусть $a_1, \ldots, a_n$ — попарно различные целые числа.

а) Доказать, что многочлен $(x-a_1)\cdot(x-a_2)\cdot\ldots\cdot(x-a_n)-1$ неприводим.

б) Доказать, что многочлен $(x-a_1)\cdot(x-a_2)\cdot\ldots\cdot(x-a_n)+1$ неприводим за исключением следующих случаев:

$$(x-a)(x-a-2)+1 = (x-a-1)^2;$$

$$(x-a)(x-a-1)(x-a-2)(x-a-3)+1 = \big((x-a-1)(x-a-2)-1\big)^2.$$

в) Доказать, что многочлен $(x-a_1)^2 \cdot (x-a_2)^2 \cdot \ldots \cdot (x-a_n)^2 + 1$ неприводим.

2.7. Доказать, что любой многочлен с целыми коэффициентами можно представить в виде суммы двух неприводимых многочленов.

2.8. а) Пусть $f(x)$ — многочлен с целыми коэффициентами, принимающий значение $+1$ более чем для трех целых x. Доказать, что $f(n) \neq -1$ при $n \in \mathbb{Z}$.

б) Пусть $a, b \in \mathbb{Z}$ и многочлен ax^2+bx+1 неприводим. Доказать, что если $n \geqslant 7$ и $a_1, \ldots, a_n$ — попарно различные целые числа, то многочлен $a\big(\varphi(x)\big)^2 + b\varphi(x) + 1$, где $\varphi(x) = (x-a_1)\cdot(x-a_2)\cdot\ldots\cdot(x-a_n)$, неприводим.

2.9. Пусть $F(x_1, \ldots, x_n) \in \mathbb{Z}[x_1, \ldots, x_n]$ и $f(x) = F(x, \ldots, x)$. Доказать, что если многочлен f неприводим, то многочлен F тоже неприводим.

2.10. Пусть $p > 3$ — простое число, $n < 2p$. Доказать, что многочлен $x^{2p} + px^n - 1$ неприводим.

2.11. Пусть $p > 3$ — простое число $a_1 + \ldots + a_p = 2p$, $n < 2p$. Доказать, что многочлен $x_1^{a_1} \cdot \ldots \cdot x_p^{a_p} + x_1^n + \ldots + x_p^n - 1$ неприводим.

2.12. Пусть f — неприводимый многочлен с целыми коэффициентами, D — его дискриминант, p — простое число. Предположим, что многочлен f по модулю p разлагается на k неприводимых множителей. Доказать, что $D^{(p-1)/2} \equiv (-1)^{n-k} \pmod{p}$.

Решения задач

2.1. Предположим, что $f(x) = g(x)h(x)$, где $g, h \in \mathbb{Z}[x]$ и $\deg g \geqslant 1$, $\deg h \geqslant 1$. Число $f(x_0) = p$ простое, поэтому можно считать, что $g(x_0) = \pm 1$ и $h(x_0) = \pm p$. С другой стороны, корни $\beta_1, \ldots, \beta_k$ многочлена g являются корнями многочлена f, поэтому $|\beta_i| \leqslant M$, а значит,

$$\big|g(x_0)\big| = |a_0| \prod |x_0 - \beta_i|,$$

где $|a_0| \geqslant 1$ и $|x_0 - \beta_i| \geqslant |x_0| - |\beta_i| > (M+1) - M = 1$. Следовательно, $\big|g(x_0)\big| > 1$. Получено противоречие.

2.2. Предположим, что многочлен $x^p - x - a$ приводим над $\mathbb{Z}$. Тогда он приводим и как многочлен над $\mathbb{Z}_p$, т. е. над $\mathbb{Z}_p$ имеет место равенство $x^p - x - a = g(x)h(x)$, где $1 \leqslant \deg g \leqslant p-1$ и многочлен g неприводим. Если $b \in \mathbb{Z}_p$, то $g(x-b)h(x-b) = (x-b)^p - (x-b) - a = x^p - x - a$. Таким образом, многочлен $x^p - x - a$ делится на p многочленов $g_i(x) = g(x-i)$, $i = 0, 1, \ldots, p-1$. Если $\deg g \leqslant p-1$, то эти многочлены попарно различны, поскольку $(x-i)^k - (x-j)^k = (j-i)kx^{k-1} + \ldots$ Поэтому $p = \deg(x^p - x - a) \geqslant p \deg g$. Следовательно, $\deg g = 1$. Но если a не делится на p, то многочлен $x^p - x - a$ не имеет корней в $\mathbb{Z}_p$, поскольку $b^p - b = 0$ для любого $b \in \mathbb{Z}_p$.

2.3. Предположим, что $f(x) = g(x)h(x)$, где $g, h \in \mathbb{Z}[x]$ и $\deg g \geqslant 1$, $\deg h \geqslant 1$. Число $f(n) = p$ простое, поэтому можно считать, что $g(n) = \pm 1$ и $h(n) = \pm p$. С другой стороны, если $g(\beta_i) = 0$, то $f(\beta_i) = 0$, поэтому $\operatorname{Re}\beta_i < n - \frac{1}{2}$, т. е. $\operatorname{Re}\left(n - \frac{1}{2} - \beta_i\right) > 0$. Это означает, что если $t > 0$, то $\left|n - \frac{1}{2} - \beta_i - t\right| < \left|n - \frac{1}{2} - \beta_i + t\right|$, поэтому $\left|g\left(n - \frac{1}{2} - t\right)\right| < \left|g\left(n - \frac{1}{2} + t\right)\right|$. Из условия $f(n-1) \neq 0$ следует, что $|g(n-1)| \geqslant 1$. Таким образом, $|g(n)| = \left|g\left(n - \frac{1}{2} + \frac{1}{2}\right)\right| > \left|g\left(n - \frac{1}{2} - \frac{1}{2}\right)\right| = |g(n-1)| \geqslant 1$. Приходим к противоречию.

2.4. а) Предположим, что $f = f_1 f_2$, где $f_1, f_2 \in \mathbb{Z}[x]$. Пусть $f_1(0) = b_1$ и $f_2(0) = c_1$. Для определенности можно считать, что $|b_1| \leqslant |c_1|$.

Случай 1: $|b_1| = 1$. В этом случае $|c_1| = |f_0| > 1$. Из условия $f(a_k) = p_k$, где p_k — простое число, следует, что либо $f_1(a_k) = \pm p_k$ и $f_2(a_k) = \pm 1$, либо $f_1(a_k) = \pm 1$ и $f_2(a_k) = \pm p_k$. Предположим сначала, что $f_2(a_k) = \pm 1$. Тогда $f_2(a_k) - f_2(0) = -(c_1 \pm 1)$. С другой стороны, $f_2(a_k) - f_2(0)$ делится на a_k. Приходим к противоречию. Остается предположить, что $f_1(a_k) = \pm 1 = \pm b_1 = \pm f_1(0)$. Если $f_1(a_k) = -f_1(0)$, то $f_1(a_k) - f_1(0) = 2f_1(a_k) = \pm 2$. С другой стороны, $f_1(a_k) - f_1(0)$ делится на a_k, поэтому $|a_k| \leqslant 2$, что противоречит условию. Таким образом, $f_1(a_k) = f_1(a_0) = b_1$ при $k = 1, \ldots, n$. Учитывая, что степень многочлена f_1 строго меньше n, получаем $f_1(x) = b_1$ при всех x.

Случай 2: $|b_1| > 1$. В этом случае b_1 и c_1 играют одинаковые роли, поскольку $|c_1| \geqslant |b_1| > 1$. Пусть для определенности $f_1(a_k) = \pm p_k$ и $f_2(a_k) = \pm 1$. Тогда $f_2(a_k) - f_2(0) = -(c_1 \pm 1)$ делится на a_k, что противоречит условию.

б) Очевидным образом следует из а).

2.5. Как и при доказательстве теоремы 7.4, получаем, что произведение абсолютных величин корней одного из многочленов g и h не превосходит $|a_n|$. Чтобы прийти к противоречию, достаточно показать, что для любого корня α многочлена f выполняется неравенство $|\alpha| > |a_n|$. Предположим, что $f(\alpha) = 0$ и $|\alpha| \leqslant |a_n|$. Тогда

$$|pa_n| = |\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha| \leqslant |a_n| \sum_{i=0}^{n-1} |a_n|^{n-1-i}|a_i| < p|a_n|,$$

чего не может быть.

Глава 3
Многочлены специального вида

11. Симметрические многочлены

11.1. Примеры симметрических многочленов

Многочлен $f(x_1, \ldots, x_n)$ называют *симметрическим*, если для любой подстановки $\sigma \in S_n$ выполняется равенство

$$f\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right) = f(x_1, \ldots, x_n).$$

Основным примером симметрических многочленов служат *элементарные* симметрические многочлены

$$\sigma_k(x_1, \ldots, x_n) = \sum_{i_1 < \ldots < i_k} x_{i_1} \cdot \ldots \cdot x_{i_k},$$

где $1 \leqslant k \leqslant n$; удобно считать, что $\sigma_0 = 1$ и $\sigma_k(x_1, \ldots, x_n) = 0$ при $k > n$.

Элементарные симметрические многочлены можно задавать с помощью *производящей функции*

$$\sigma(t) = \sum_{k=0}^{\infty} \sigma_k t^k = \prod_{i=1}^{n} (1 + t x_i).$$

Если x_1, $\ldots$, x_n — корни многочлена $x^n + a_1 x^{n-1} + \ldots + a_n$, то $\sigma_k(x_1, \ldots, x_n) = (-1)^k a_k$.

Другим примером симметрических многочленов служат *полные однородные* симметрические многочлены

$$p_k(x_1, \ldots, x_n) = \sum_{i_1 + \ldots + i_n = k} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}.$$

Им соответствует производящая функция

$$p(t) = \sum_{k=0}^{\infty} p_k t^k = \prod_{i=1}^{n} (1 - t x_i)^{-1}.$$

Важным примером симметрических многочленов служат также *степенные суммы*

$$s_k(x_1, \ldots, x_n) = x_1^k + \ldots + x_n^k.$$

Им соответствует производящая функция

$$s(t) = \sum_{k=0}^{\infty} s_k t^{k-1} = \sum_{i=1}^{n} x_i (1 - t x_i)^{-1}.$$

Иногда используются *мономиальные* симметрические многочлены

$$m_{i_1 \ldots i_n}(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} x_{\sigma(1)}^{i_1} \cdot \ldots \cdot x_{\sigma(n)}^{i_n}.$$

Производящие функции $\sigma(t)$ и $p(t)$ связаны соотношением $\sigma(t)p(-t) = 1$. Приравнивая коэффициенты при t^n, $n \geqslant 1$, в левой и правой части, получаем

$$\sum_{r=0}^{n} (-1)^r \sigma_r p_{n-r} = 0. \tag{1}$$

Производящая функция $s(t)$ выражается через $p(t)$ и $\sigma(t)$ следующим образом:

$$s(t) = \frac{d}{dt} \ln p(t) = \frac{p'(t)}{p(t)}, \quad \text{т. е.} \quad s(t)p(t) = p'(t);$$

$$s(-t) = -\frac{d}{dt} \ln \sigma(t) = -\frac{\sigma'(t)}{\sigma(t)}, \quad \text{т. е.} \quad s(-t)\sigma(t) = -\sigma'(t).$$

Приравнивая коэффициенты при t^{n+1}, получаем

$$n p_n = \sum_{r=1}^{n} s_r p_{n-r}, \tag{2}$$

$$n \sigma_n = \sum_{r=1}^{n} (-1)^{r-1} s_r \sigma_{n-r}. \tag{3}$$

Соотношения (3) называют *формулами Ньютона.*

Запишем соотношения (1) для $n = 1, \ldots, k$. При фиксированных $\sigma_1, \ldots, \sigma_k$ эти соотношения можно рассматривать как систему линейных

уравнений для $p_1, \ldots, p_k$, а при фиксированных $p_1, \ldots, p_k$ — как систему уравнений для $\sigma_1, \ldots, \sigma_k$. Решая эти системы, находим

$$\sigma_k = \begin{vmatrix} p_1 & 1 & 0 & \ldots & 0 \\ p_2 & p_1 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ p_{k-1} & p_{k-2} & p_{k-3} & \ldots & 1 \\ p_k & p_{k-1} & p_{k-2} & \ldots & p_1 \end{vmatrix}, \quad p_k = \begin{vmatrix} \sigma_1 & 1 & 0 & \ldots & 0 \\ \sigma_2 & \sigma_1 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma_{k-1} & \sigma_{k-2} & \sigma_{k-3} & \ldots & 1 \\ \sigma_k & \sigma_{k-1} & \sigma_{k-2} & \ldots & \sigma_1 \end{vmatrix}.$$

Аналогично с помощью соотношений (2) получаем

$$s_k = (-1)^{k-1} \begin{vmatrix} p_1 & 1 & 0 & \ldots & 0 \\ 2p_2 & p_1 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ kp_k & p_{k-1} & p_{k-2} & \ldots & p_1 \end{vmatrix},$$

$$p_k = \frac{1}{k!} \begin{vmatrix} s_1 & -1 & 0 & \ldots & 0 \\ s_2 & s_1 & -2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-1} & s_{k-2} & s_{k-3} & \ldots & -k+1 \\ s_k & s_{k-1} & s_{k-2} & \ldots & s_1 \end{vmatrix}.$$

С помощью соотношений (3) получаем

$$s_k = \begin{vmatrix} \sigma_1 & 1 & 0 & \ldots & 0 \\ 2\sigma_2 & \sigma_1 & 1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ k\sigma_k & \sigma_{k-1} & \sigma_{k-2} & \ldots & \sigma_1 \end{vmatrix}, \quad \sigma_k = \frac{1}{k!} \begin{vmatrix} s_1 & 1 & 0 & \ldots & 0 \\ s_2 & s_1 & 2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{k-1} & s_{k-2} & s_{k-3} & \ldots & k-1 \\ s_k & s_{k-1} & s_{k-2} & \ldots & s_1 \end{vmatrix}.$$

11.2. Основная теорема о симметрических многочленах

Элементарные симметрические многочлены алгебраически независимы и образуют базис кольца симметрических многочленов. Более точная формулировка этого утверждения выглядит следующим образом.

Теорема 11.1. Пусть $f(x_1, \ldots, x_n)$ — симметрический многочлен. Тогда существует такой многочлен $g(y_1, \ldots, y_n)$, что $f(x_1, \ldots, x_n) = g(\sigma_1, \ldots, \sigma_n)$. При этом многочлен g единствен.

Доказательство. Достаточно рассмотреть случай, когда f — однородный многочлен. Будем говорить, что моном $x_1^{\lambda_1} \cdot \ldots \cdot x_n^{\lambda_n}$ имеет более высокий порядок, чем моном $x_1^{\mu_1} \cdot \ldots \cdot x_n^{\mu_n}$, если $\lambda_1 = \mu_1, \ldots$

$\ldots$, $\lambda_k = \mu_k$ и $\lambda_{k+1} > \mu_{k+1}$ (возможно, $k = 0$). Пусть $ax_1^{\lambda_1} \cdot \ldots \cdot x_n^{\lambda_n}$ — старший моном многочлена f. Тогда $\lambda_1 \geqslant \ldots \geqslant \lambda_n$. Рассмотрим симметрический многочлен

$$f_1 = f - a\sigma_1^{\lambda_1-\lambda_2} \cdot \sigma_2^{\lambda_2-\lambda_3} \cdot \ldots \cdot \sigma_n^{\lambda_n}. \qquad (1)$$

Старший член монома $\sigma_1^{\lambda_1-\lambda_2} \cdot \ldots \cdot \sigma_n^{\lambda_n}$ равен

$$x_1^{\lambda_1-\lambda_2}(x_1x_2)^{\lambda_2-\lambda_3} \cdot \ldots \cdot (x_1 \cdot \ldots \cdot x_n)^{\lambda_n} = x_1^{\lambda_1} \cdot x_2^{\lambda_2} \cdot \ldots \cdot x_n^{\lambda_n},$$

поэтому порядок старшего монома многочлена f_1 строго ниже порядка старшего монома многочлена f. Применим к многочлену f_1 снова операцию (1) и т. д. Ясно, что после конечного числа таких операций придем к нулевому многочлену.

Докажем теперь единственность представления $f(x_1, \ldots, x_n) = g(\sigma_1, \ldots, \sigma_n)$. Достаточно проверить, что если

$$g(y_1, \ldots, y_n) = \sum a_{i_1 \ldots i_n} y_1^{i_1} \cdot \ldots \cdot y_n^{i_n}$$

— ненулевой многочлен, то после подстановки $y_1 = \sigma_1 = x_1 + \ldots + x_n, \ldots, y_n = \sigma_n = x_1 \cdot \ldots \cdot x_n$ этот многочлен останется ненулевым. Ограничимся рассмотрением старших мономов

$$a_{i_1 \ldots i_n} x_1^{i_1+\ldots+i_n} x_2^{i_2+\ldots+i_n} \cdot \ldots \cdot x_n^{i_n},$$

получающихся в результате подстановки. Ясно, что самый старший среди этих мономов ни с чем сократиться не может. □

Из доказательства теоремы 11.1 видно, что если $f(x_1, \ldots, x_n)$ — симметрический многочлен с целыми коэффициентами, то $f(x_1, \ldots, x_n) = g(\sigma_1, \ldots, \sigma_n)$, где g — тоже многочлен с целыми коэффициентами. Детерминантное выражение σ_k через $p_1, \ldots, p_k$ показывает, что для полных однородных многочленов справедливо аналогичное утверждение. Что же касается степенных сумм, то для них выражение вида $f(x_1, \ldots, x_n) = g(s_1, \ldots, s_n)$ тоже существует, но при этом коэффициенты многочлена g не обязательно целые. Например,

$$x_1x_2 = \frac{(x_1 + x_2)^2 - (x_1^2 + x_2^2)}{2} = \frac{s_1^2 - s_2}{2}.$$

Из основной теоремы о симметрических многочленах следует, что если $x_1, \ldots, x_n$ — корни многочлена $x^n + a_1x^{n-1} + \ldots + a_n$, то величина

$$D = \prod_{i<j}(x_i - x_j)^2,$$

представляющая собой симметрический многочлен от $x_1, \ldots, x_n$, полиномиально выражается через $a_1, \ldots, a_n$. Эту величину называют *дискриминантом* многочлена.

Назовем многочлен $f(x_1, \ldots, x_n)$ *кососимметрическим*, если

$$f(\ldots, x_i, \ldots, x_j, \ldots) = -f(\ldots, x_j, \ldots, x_i, \ldots),$$

т. е. при транспозиции любых двух переменных x_i и x_j многочлен меняет знак. Примером кососимметрического многочлена служит $\Delta = \prod_{i<j}(x_i - x_j)$. Ясно, что $\Delta^2 = D$.

Теорема 11.2. Любой кососимметрический многочлен $f(x_1, \ldots, x_n)$ можно представить в виде

$$\Delta(x_1, \ldots, x_n) g(x_1, \ldots, x_n),$$

где g — симметрический многочлен.

Доказательство. Достаточно проверить, что f делится на Δ. В самом деле, если f/Δ — многочлен, то этот многочлен по очевидным причинам симметрический. Покажем, например, что f делится на $x_1 - x_2$. Сделаем замену $x_1 = u + v$, $x_2 = u - v$. В результате получим

$$f(x_1, x_2, x_3, \ldots, x_n) = f_1(u, v, x_3, \ldots, x_n).$$

Если $x_1 = x_2$, то $u = 0$. Поэтому $f_1(0, v, x_3, \ldots, x_n) = 0$. Это означает, что многочлен f_1 делится на u, т. е. многочлен f делится на $x_1 - x_2$. Аналогично доказывается, что f делится на $x_i - x_j$ при всех $i < j$. □

11.3. Неравенства Мюрхеда

Пусть $\lambda = (\lambda_1, \ldots, \lambda_n)$ — *разбиение*, т. е. упорядоченный набор целых неотрицательных чисел $\lambda_1 \geqslant \lambda_2 \geqslant \ldots \geqslant \lambda_n \geqslant 0$. Положим $|\lambda| = \lambda_1 + \ldots + \lambda_n$. Будем считать, что $\lambda \geqslant \mu$, если $\lambda_1 + \ldots + \lambda_k \geqslant \mu_1 + \ldots + \mu_k$ при $k = 1, 2, \ldots, n$.

Каждому набору λ можно сопоставить однородный симметрический многочлен

$$M_\lambda(x_1, \ldots, x_n) = \frac{1}{n!} \sum_{\sigma \in S_n} x_1^{\lambda_{\sigma(1)}} \cdot \ldots \cdot x_n^{\lambda_{\sigma(n)}}. \qquad (1)$$

Степень этого многочлена равна $|\lambda|$.

Пример 1. Если $\lambda = (1, \ldots, 1)$, то $M_\lambda(x_1, \ldots, x_n) = x_1 \cdot \ldots \cdot x_n$.

В самом деле, сумма (1) в этом случае состоит из $n!$ слагаемых $x_1 \cdot \ldots \cdot x_n$.

Пример 2. Если $\lambda = (n, 0, \ldots, 0)$, то $M_\lambda(x_1, \ldots, x_n) = (x_1^n + \ldots + x_n^n)/n$.

В самом деле, сумма (1) в этом случае состоит из $(n-1)!$ слагаемых x_1^n, $(n-1)!$ слагаемых x_2^n и т. д.

При положительных $x_1, \ldots, x_n$ выполняется неравенство

$$\frac{x_1^n + \ldots + x_n^n}{n} \geqslant x_1 \cdot \ldots \cdot x_n$$

(неравенство между средним арифметическим и средним геометрическим). Следующее утверждение является обобщением этого неравенства.

Теорема 11.3 (Мюрхед, [Mu]). Неравенство

$$M_\lambda(x) \geqslant M_\mu(x) \tag{2}$$

выполняется при всех $x = (x_1, \ldots, x_n)$ с положительными $x_1, \ldots, x_n$ в том и только том случае, когда $|\lambda| = |\mu|$ и $\lambda \geqslant \mu$. При этом равенство достигается лишь в том случае, когда $\lambda = \mu$ и $x_1 = \ldots = x_n$.

Доказательство. Предположим сначала, что неравенство (2) выполняется при всех $x > 0$. Пусть $x_1 = \ldots = x_k = a$ и $x_{k+1} = \ldots = x_n = 1$. Тогда

$$1 \leqslant \lim_{a \to \infty} M_\lambda(x)/M_\mu(x) = \lim_{a \to \infty} \left(a^{\lambda_1 + \ldots + \lambda_k}/a^{\mu_1 + \ldots + \mu_k}\right).$$

Следовательно, $\lambda_1 + \ldots + \lambda_k \geqslant \mu_1 + \ldots + \mu_k$.

При $k = n$, положив $x_1 = \ldots = x_n = a$, получаем равенство

$$M_\lambda(x)/M_\mu(x) = a^{\lambda_1 + \ldots + \lambda_k}/a^{\mu_1 + \ldots + \mu_k}.$$

При $a > 1$, как и ранее, получим $|\lambda| \geqslant |\mu|$. А при $0 < a < 1$ получим $|\lambda| \leqslant |\mu|$.

Доказательство утверждения в обратную сторону более сложно. Оно использует следующее преобразование R_{ij}. Пусть $\mu_i \geqslant \mu_j > 0$, где $i < j$. Положим $R_{ij}\mu = \mu'$, где $\mu'_i = \mu_i + 1$, $\mu'_j = \mu_j - 1$ и $\mu'_k = \mu_k$ при $k \neq i, j$. Легко проверить, что $\mu' > \mu$ и $|\mu'| = |\mu|$.

Лемма 1. Если $\lambda = R_{ij}\mu$, то $M_\lambda(x) \geqslant M_\mu(x)$, причем равенство достигается лишь в том случае, когда $x_1 = \ldots = x_n$. (Предполагается, что числа $x_1, \ldots, x_n$ положительны.)

Доказательство. Для каждой пары индексов p, q, где $1 \leqslant p < q \leqslant n$, в $M_\lambda(x) - M_\mu(x)$ входит слагаемое вида

$$A \cdot \left(x_p^{\lambda_i} x_q^{\lambda_j} + x_q^{\lambda_i} x_p^{\lambda_j} - x_p^{\mu_i} x_q^{\mu_j} - x_q^{\mu_i} x_p^{\mu_j}\right), \tag{3}$$

где A — некоторое положительное число. Обозначим для наглядности $x_p = a$, $x_q = b$, $\mu_i = \alpha$, $\mu_j = \beta$. Напомним, что $\lambda_i = \alpha + 1$, $\lambda_j = \beta - 1$ и $\alpha \geqslant \beta$. Выражение (3), деленное на A, равно

$$a^{\alpha+1}b^{\beta-1} + a^{\beta-1}b^{\alpha+1} - a^\alpha b^\beta - a^\beta b^\alpha = (ab)^{\beta-1}(a-b)(a^{\alpha+1-\beta} - b^{\alpha+1-\beta}) \geqslant 0,$$

причем равенство возможно лишь в том случае, когда $a = b$. Поэтому $M_\lambda(x) - M_\mu(x) \geqslant 0$, причем если среди чисел $x_1, \ldots, x_n$ есть хотя бы два различных, то неравенство строгое. □

Лемма 2. Если $\lambda \geqslant \mu$ и $|\lambda| = |\mu|$, но $\lambda \neq \mu$, то λ можно получить из μ с помощью конечного числа преобразований R_{ij}.

Доказательство. Пусть i — наименьший индекс, для которого $\lambda_i \neq \mu_i$. Тогда из условия $\lambda \geqslant \mu$ следует, что $\lambda_i > \mu_i$. Равенство $|\lambda| = |\mu|$, означает, что $\sum(\lambda_k - \mu_k) = 0$, поэтому $\lambda_j < \mu_j$ для некоторого индекса j. Ясно, что $i < j$ и $\mu_j > 0$. Поэтому к μ можно применить преобразование R_{ij}. В результате получим последовательность ν, для которой $\nu_i = \mu_i + 1$, $\nu_j = \mu_j - 1$ и $\nu_k = \mu_k$ при $k \neq i, j$. Учитывая, что $\lambda_i > \mu_i$ и $\lambda_j < \mu_j$, получаем

$$|\lambda_i - \mu_i| = |\lambda_i - \nu_i| + 1, \quad |\lambda_j - \mu_j| = |\lambda_j - \nu_j| + 1.$$

Таким образом,

$$\sum |\lambda_k - \nu_k| = \sum |\lambda_k - \mu_k| - 2,$$

т. е. с помощью преобразования R_{ij} нам удалось уменьшить на 2 величину $\sum |\lambda_k - \mu_k|$. Поэтому с помощью некоторого числа преобразований R_{ij} эту величину можно сделать равной нулю. □

Из лемм 1 и 2 неравенство Мюрхеда следует очевидным образом. □

11.4. Функции Шура

Рассмотрим бесконечную матрицу

$$P = \begin{pmatrix} p_0 & p_1 & p_2 & \dots \\ 0 & p_0 & p_1 & \dots \\ 0 & 0 & p_0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix},$$

где $p_i = p_i(x_1, \dots, x_n)$ — полный однородный многочлен степени n; элемент a_{ij} матрицы P равен p_{j-i}. *Функцией Шура*, или *S-функцией*, соответствующей разбиению λ, называют минор матрицы P, образованный строками $0, 1, \dots, n-1$ и столбцами $\lambda_1, \lambda_2+1, \dots, \lambda_n+n-1$. Эту симметрическую функцию от переменных $x_1, \dots, x_n$ обозначают s_λ. В виде определителя функция s_λ записывается следующим образом:

$$s_\lambda = |p_{\lambda_i+i-j}|_1^n.$$

Косой функцией Шура $s_{\lambda,\mu}$, соответствующей паре разбиений λ и μ, называют минор матрицы P, образованный строками μ_1, μ_2+1, ..., μ_n+n-1 и столбцами λ_1, λ_2+1, ..., λ_n+n-1. Ясно, что при этом $s_\lambda = s_{\lambda,0}$. Разбиение μ называют *подразбиением* разбиения λ, если $\lambda_i \geqslant \mu_i$ при $i = 1, \dots, n$. Можно доказать, что если μ не является подразбиением λ, то $s_{\lambda,\mu} = 0$.

Первоначально функции Шура (еще до Шура) были введены Якоби как отношения кососимметрических функций определенного вида. Пусть $\alpha = (\alpha_1, \dots, \alpha_n)$ — некоторое разбиение, a_α — антисимметризация одночлена $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$, т. е.

$$a_\alpha = \sum_{\omega \in S_n} (-1)^\omega \omega(x^\alpha),$$

где $(-1)^\omega$ — знак подстановки ω и $\omega(x^\alpha) = x_{\omega(1)}^{\alpha_1} \cdot \ldots \cdot x_{\omega(n)}^{\alpha_n}$. Легко проверить, что многочлен $a_\alpha(x_1, \dots, x_n)$ равен определителю $|x_i^{\alpha_j}|_1^n$; в частности, этот многочлен кососимметрический. Поэтому если $\alpha_i = \alpha_{i+1}$ для некоторого i, то $a_\alpha = 0$. Таким образом, можно считать, что $\alpha = \lambda + \delta$, где $\delta = (n-1, n-2, \dots, 1, 0)$.

Теорема 11.4 (тождество Якоби–Труди). Пусть $\delta = (n-1, \dots, 1, 0)$. Тогда $s_\lambda = a_{\lambda+\delta}/a_\delta$, т. е. $|p_{\lambda_i+i-j}|_1^n = |x_i^{\lambda_j+n-j}|_1^n / |x_i^{n-j}|_1^n$.

ДОКАЗАТЕЛЬСТВО. Пусть $\alpha = (\alpha_1, \ldots, \alpha_n)$ — некоторое разбиение. Рассмотрим матрицы $A_\alpha = \|x_j^{\alpha_i}\|_1^n$ и $H_\alpha = \|p_{\alpha_i - n + j}\|_1^n$. Рассмотрим также матрицу $M = \left\|(-1)^{n-i}\sigma_{n-i}(\widehat{x}_j)\right\|_1^n$, где $\widehat{x}_j = (x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$. Покажем, что эти три матрицы связаны соотношением

$$H_\alpha M = A_\alpha. \tag{1}$$

Пусть $\sigma^{(j)}(t) = \sum\limits_{k=0}^{n-1} \sigma_k(\widehat{x}_j)t^k = \prod\limits_{l \neq j}(1 + x_l t)$ и $p(t) = \sum\limits_{k=0}^{\infty} p_k t^k = \prod\limits_{l=1}^{n}(1 - x_l t)^{-1}$. Тогда

$$p(t)\sigma^{(j)}(-t) = (1 - x_j t)^{-1}.$$

Сравнивая коэффициенты при t^{α_i} в обеих частях этого равенства, получаем

$$\sum_{l=1}^{n} p_{\alpha_i - n + l}(-1)^{n-l}\sigma_{n-l}(\widehat{x}_j) = x_j^{\alpha_i}.$$

Это и есть требуемое соотношение (1).

Из (1), в частности, следует, что

$$\det H_\alpha \det M = \det A_\alpha. \tag{2}$$

Чтобы вычислить $\det M$, положим $\alpha = \delta = (n-1, \ldots, 1, 0)$. В таком случае матрица H_α имеет вид $\|p_{j-i}\|_i^n$. Эта матрица треугольная с элементами $p_0 = 1$ на диагонали. Поэтому $\det H_\delta = 1$, а значит, $\det M = \det A_\delta = a_\delta$. А так как $\det H_\alpha = s_{\alpha - \delta}$, то при $\alpha = \lambda + \delta$ равенство (2) принимает вид $s_\lambda a_\delta = a_{\lambda+\delta}$, т. е. $s_\lambda = a_{\lambda+\delta}/a_\delta$. □

12. Целозначные многочлены

12.1. Базис целозначных многочленов

Многочлен $p(x)$ называют *целозначным*, если он принимает целые значения при всех целых x.

Индукцией по k можно доказать, что многочлен

$$\binom{x}{k} = \frac{x \cdot (x-1) \cdot \ldots \cdot (x-k+1)}{k!}$$

целозначный. В самом деле, при $k = 1$ это очевидно. Предположим теперь, что многочлен $\binom{x}{k}$ целозначный. Легко проверить, что

$$\binom{x+1}{k+1} - \binom{x}{k+1} = \binom{x}{k}.$$

Следовательно, при всех целых m, n разность $\binom{m}{k+1} - \binom{n}{k+1}$ является целым числом. Остается заметить, что $\binom{0}{k+1} = 0$.

В некотором смысле целозначные многочлены исчерпываются многочленами $\binom{x}{k}$, причем требование $p(n) \in \mathbb{Z}$ при всех $n \in \mathbb{Z}$ можно существенно ослабить. А именно, справедливо следующее утверждение.

Теорема 12.1. Пусть p_k — многочлен степени k, принимающий целые значения при $x = n, n+1, \ldots, n+k$ для некоторого целого числа n. Тогда

$$p_k(x) = c_0\binom{x}{k} + c_1\binom{x}{k-1} + c_2\binom{x}{k-2} + \ldots + c_k,$$

где $c_0, c_1, \ldots, c_k$ — целые числа.

Доказательство. Многочлены

$$\binom{x}{0} = 1, \quad \binom{x}{1} = x, \quad \binom{x}{2} = \frac{x^2}{2} - \frac{x}{2}, \quad \ldots, \quad \binom{x}{k} = \frac{x^k}{k!} + \ldots$$

образуют базис в пространстве многочленов степени не выше k, поэтому

$$p_k(x) = c_0\binom{x}{k} + c_1\binom{x}{k-1} + \ldots + c_k,$$

где $c_0, c_1, \ldots, c_k$ — некоторые числа. Нужно лишь доказать, что эти числа целые.

Докажем это индукцией по k. При $k = 0$ многочлен $p_0(x) = c_0$ принимает целое значение при $x = n$, поэтому число c_0 целое. Предположим теперь, что требуемое утверждение доказано для многочленов степени не выше k. Пусть многочлен

$$p_{k+1}(x) = c_0\binom{x}{k+1} + \ldots + c_{k+1}$$

принимает целые значения при $x = n, n+1, \ldots, n+k+1$. Рассмотрим многочлен

$$\Delta p_{k+1}(x) = p_{k+1}(x+1) - p_{k+1}(x) = c_0\binom{x}{k} + c_1\binom{x}{k-1} + \ldots + c_k.$$

Он принимает целые значения при $x = n, n+1, \ldots, n+k$. Поэтому числа $c_0, c_1, \ldots, c_k$ целые, а значит, число

$$c_{k+1} = p_{k+1}(n) - c_0\binom{n}{k+1} - c_1\binom{n}{k} - \ldots - c_k\binom{n}{1}$$

тоже целое. □

Теорема 12.2. Пусть $R(x)$ — рациональная функция, принимающая целые значения при всех целых x. Тогда $R(x)$ — целозначный многочлен.

Доказательство. Рациональную функцию $R(x)$ можно записать в виде $R(x) = f(x)/g(x)$, где f и g — многочлены. Поделив f на g с остатком, получим

$$R(x) = p_k(x) + r(x),$$

где p_k — многочлен степени k, а $r(x) \to 0$ при $x \to \infty$. Таким образом, при больших n значения $p_k(n)$ мало отличаются от целых чисел. Покажем, что $p_k(x)$ — целозначный многочлен. Это делается почти так же, как и при доказательстве теоремы 12.1.

Запишем многочлен $p_k(x)$ в виде

$$p_k(x) = c_0\binom{x}{k} + \ldots + c_k.$$

При $k = 0$ число c_0 должно сколь угодно мало отличаться от целого числа, поэтому $c_0 \in \mathbb{Z}$. Многочлен

$$\Delta p_k(x) = p_k(x+1) - p_k(x) = c_0\binom{x}{k-1} + \ldots + c_{k-1}.$$

при больших целых x тоже принимает почти целые значения, а его степень равна $k-1$. Применив к нему предположение индукции, получим, что числа $c_0, c_1, \ldots, c_{k-1}$ целые. Ясно также, что число

$$c_k = p_k(n) - c_0\binom{n}{k} - \ldots - c_{k-1}\binom{n}{1}$$

тоже целое.

Остается доказать, что $r(x) = 0$. Как мы уже знаем, $r(n) \in \mathbb{Z}$ при $n \in \mathbb{Z}$ и $r(n) \to 0$ при $n \to \infty$. Следовательно, $r(n) = 0$ при всех достаточно больших целых n. Но любая рациональная функция, имеющая бесконечно много нулей, тождественно равна нулю. □

Следствие. Пусть $f(x)$ и $g(x)$ — многочлены с целыми коэффициентами, причем $f(n)$ делится на $g(n)$ при всех целых n. Тогда

$$f(x) = \left(\sum_{k=0}^{m} c_k\binom{x}{k}\right) g(x),$$

где $c_0, \ldots, c_m$ — целые числа.

Пойа [Pó] показал, что если целая аналитическая функция $f(z)$ принимает целочисленные значения при целых или натуральных значениях переменной z и при этом возрастает не слишком быстро, то $f(z)$ — целозначный многочлен. Точнее говоря, справедливы следующие утверждения:

1) если $f(\mathbb{N}) \subset \mathbb{Z}$ и $|f(z)| < Ce^{k|z|}$, где $k < \ln 2$, то f — целозначный многочлен (доказательство этого утверждения можно найти также на сс. 161–162 книги [Ге2]);

2) если $f(\mathbb{Z}) \subset \mathbb{Z}$ и $|f(z)| < Ce^{k|z|}$, где $k < \ln\left(\frac{3+\sqrt{5}}{2}\right)$, то f — целозначный многочлен.

Примеры функций 2^z и $\frac{1}{\sqrt{5}}\left(\left(\frac{3+\sqrt{5}}{2}\right)^z - \left(\frac{3-\sqrt{5}}{2}\right)^z\right)$ показывают, что обе оценки неулучшаемы.

12.2. Целозначные многочлены от многих переменных

Базисные целозначные многочлены от n переменных устроены аналогично базисным целозначным многочленам от одной переменной.

Теорема 12.3 ([Ost]). Многочлен $p_{d_1\dots d_n}(x_1,\dots,x_n)$, где d_i — степень по переменной x_i, принимает целые значения при $x_1 = a_1, a_1+1, \dots$ $\dots, a_1+d_1, \dots, x_n = a_n, a_n+1, \dots, a_n+d_n$ тогда и только тогда, когда

$$p_{d_1\dots d_n}(x_1,\dots,x_n) = \sum c_{k_1\dots k_n}\binom{x_1}{k_1}\dots\binom{x_n}{k_n},$$

где $c_{k_1\dots k_n}$ — целые числа. В частности, такой многочлен принимает целые значения при всех целых $x_1,\dots,x_n$.

Доказательство. Проведем рассуждения при $n = 2$ (общий случай аналогичен). При фиксированном $x_1 \in \{a_1,\dots,a_1+d_1\}$ многочлен $p_{d_1d_2}(x_1,x_2)$ принимает целые значения при $x_2 = a_2,\dots,a_2+d_2$. Поэтому согласно теореме 12.1 при $x_1 = a_1,\dots,a_1+d_1$ выполняется равенство

$$p_{d_1d_2}(x_1,x_2) = \sum_{k_2=0}^{d_2} c_{k_2}(x_1)\binom{x_2}{k_2}, \tag{1}$$

где $c_{k_2}(a_1),\dots,c_{k_2}(a_1+d_1)$ — целые числа. Если же рассматривать равенство (1) как соотношение для многочленов от переменных x_1 и x_2, то ясно, что $c_{k_2}(x_1)$ — однозначно определенный многочлен. Как мы уже

выяснили, этот многочлен (степени не выше d_1) принимает целые значения при $x_1 = a_1, \ldots, a_1 + d_1$. что и требовалось. □

12.3. q-аналог целозначных полиномов

Биномиальным коэффициентом Гаусса, или *q-биномиальным коэффициентом,* называют величину

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdot\ldots\cdot(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdot\ldots\cdot(q-1)}.$$

При $q \to 1$ биномиальный коэффициент Гаусса переходит в обычный биномиальный коэффициент $\binom{n}{k}$. Биномиальный коэффициент Гаусса является одним из многочисленных q-аналогов элементарных и специальных функций (см., например, [Ки] и [ГР]).

Тождество $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ имеет q-аналог вида

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k \end{bmatrix}_q + \begin{bmatrix} n \\ k-1 \end{bmatrix}_q q^{n-k+1}. \tag{1}$$

Для доказательства равенства (1) достаточно заметить, что после сокращения общих частей числителей и знаменателей это равенство принимает вид

$$\frac{q^{n+1}-1}{(q^k-1)(q^{n-k+1}-1)} = \frac{1}{q^k-1} + \frac{q^{n-k+1}}{q^{n-k+1}-1}.$$

В дальнейшем будем считать, что q, n и k — целые числа, причем $q \geqslant 2$ и $1 \leqslant k \leqslant n$. В таком случае индукция по n на основе формулы (1) показывает, что $\begin{bmatrix} n \\ k \end{bmatrix}_q$ — целое число.

Рассмотрим многочлены $f_0, f_1, f_2, \ldots$, где $f_0 = 1$ и

$$f_k(x) = q^{-k(k-1)/2}\frac{(x-1)(x-q)\cdot\ldots\cdot(x-q^{k-1})}{(q-1)(q^2-1)\cdot\ldots\cdot(q^k-1)}$$

при $k \geqslant 1$. Легко проверить, что

$$f_k(q^n) = 0 \quad \text{при} \quad n = 0,\ 1,\ \ldots,\ k-1 \quad \text{и} \quad f_k(q^k) = 1. \tag{2}$$

Кроме того, $f_k(q^n) = \begin{bmatrix} n \\ k \end{bmatrix}_q$ при $n \geqslant k$. В частности, при всех натуральных n число $f_k(q^n)$ целое.

Теорема 12.4. Многочлен $p_k(x)$ степени k принимает целые значения при $x = 1, q, q^2, \ldots, q^k$ тогда и только тогда, когда

$$p_k(x) = c_k f_k(x) + c_{k-1} f_{k-1}(x) + \ldots + c_1 f_1(x) + c_0, \tag{3}$$

где $c_0, c_1, \ldots, c_k$ — целые числа. В частности, такой многочлен принимает целые значения при всех $x = q^n$ $(n \in \mathbb{N})$.

Доказательство. Многочлены $f_0, f_1, \ldots, f_k$ образуют базис линейного пространства многочленов степени не выше k, поэтому равенство (3) выполняется при некоторых $c_0, c_1, \ldots, c_k \in \mathbb{C}$. Нужно лишь проверить, что $c_0, \ldots, c_k \in \mathbb{Z}$. Формулы (2) показывают, что

$$\begin{aligned}
p_k(1) &= c_0, \\
p_k(q) &= c_1 + c_0, \\
p_k(q^2) &= c_2 + c_1 f_1(q^2) + c_0, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
p_k(q^k) &= c_k + c_{k-1} f_{k-1}(q^k) + \ldots + c_1 f_1(q^k) + c_0.
\end{aligned}$$

Поэтому последовательно получаем

$$c_0 \in \mathbb{Z} \Rightarrow c_1 \in \mathbb{Z} \Rightarrow \ldots \Rightarrow c_k \in \mathbb{Z}. \qquad \square$$

Если целая аналитическая функция принимает целые значения в точках $1, q, q^2, \ldots$ и при этом растет не слишком быстро, то эта функция — многочлен. Точную формулировку и доказательство этого утверждения можно найти в книге [Ге2], с. 186–188.

13. Круговые многочлены

13.1. Основные свойства круговых многочленов

Многочлен $\Phi_n(x) = \prod (x - \varepsilon_k)$, где $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ — примитивные корни степени n из единицы, называют *круговым многочленом*, или *многочленом деления круга* порядка n. Например, $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, $\Phi_4(x) = x^2 + 1$.

При $n > 2$ в число первообразных корней (из единицы) степени n не входит ± 1. В таком случае первообразные корни разбиваются на пары комплексно сопряженных чисел. Поэтому при $n > 2$ степень многочлена Φ_n четна.

Непосредственно из определения кругового многочлена видно, что

$$\prod_{d|n} \Phi_d(x) = x^n - 1.$$

Теорема 13.1. Пусть $n > 1$ — нечетное число. Тогда

$$\Phi_{2n}(x) = \Phi_n(-x).$$

Доказательство. Если $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ — первообразные корни степени n, то $-\varepsilon_1, \ldots, -\varepsilon_{\varphi(n)}$ — первообразные корни степени $2n$. Таким образом,

$$\Phi_n(-x) = (-x - \varepsilon_1) \cdot \ldots \cdot (-x - \varepsilon_{\varphi(n)}),$$
$$\Phi_{2n}(x) = (x + \varepsilon_1) \cdot \ldots \cdot (x + \varepsilon_{\varphi(n)}).$$

Остается заметить, что степень многочлена Φ_n четна. □

13.2. Формула обращения Мёбиуса

Соотношение

$$\prod_{d|n} \Phi_d(x) = x^n - 1$$

позволяет получить явное выражение для $\Phi_n(x)$ через $x^d - 1$, где d пробегает делители n. Для этого имеется достаточно общая конструкция, основанная на *функции Мёбиуса*

$$\mu(n) = \begin{cases} 1 & \text{при } n = 1; \\ (-1)^k & \text{при } n = p_1 \ldots p_k; \\ 0 & \text{при } n = p^2 m. \end{cases}$$

Теорема 13.2 (Мёбиус). Если $F(n) = \sum\limits_{d|n} f(d)$, то

$$f(n) = \sum_{d|n} \mu(d) F(n/d) = \sum_{d|n} \mu(n/d) F(d).$$

Доказательство. Прежде всего проверим, что при всех $n > 1$ выполняется соотношение $\sum\limits_{d|n} \mu(d) = 0$. Пусть $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Тогда

$$\sum_{d|n} \mu(d) = \sum_{d|p_1 \ldots p_k} \mu(d) = 1 - \binom{k}{1} + \binom{k}{2} + \ldots + (-1)^k = (1-1)^k = 0.$$

Ясно, что

$$\sum_{ab=n} F(a)\mu(b) = \sum_{d_1 d_2 b=n} f(d_1)\mu(b) = \sum_{d_1|n} \left(f(d_1) \sum_{d_2 b=n/d_1} \mu(b) \right).$$

Пусть $n/d_1 = m$. Тогда

$$\sum_{d_2 b=m} \mu(b) = \sum_{b|m} \mu(b) = \begin{cases} 1 & \text{при } n = d_1; \\ 0 & \text{при } n \neq d_1. \end{cases}$$

Поэтому

$$\sum_{d_1|n} \left(f(d_1) \sum_{d_2 b=n/d_1} \mu(b) \right) = f(n). \qquad \square$$

Следствие. Если $F(n) = \prod\limits_{d|n} f(d)$, то

$$f(n) = \prod_{d|n} F(n/d)^{\mu(d)} = \prod_{d|n} F(d)^{\mu(n/d)}.$$

Для круговых многочленов формула обращения Мёбиуса дает выражение

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}.$$

Теорема 13.3. Коэффициенты многочлена $\Phi_n(x)$ — целые числа.

Доказательство. Сгруппируем в произведении $\prod_{d|n}(x^d - 1)^{\mu(n/d)}$ отдельно множители с $\mu = 1$ и множители с $\mu = -1$. В результате получим $\Phi_n(x) = P(x)/Q(x)$, где P и Q — многочлены с целыми коэффициентами и со старшим коэффициентом 1. Алгоритм деления многочленов показывает, что Φ_n — многочлен с рациональными коэффициентами. Поэтому существует такое целое m, что многочлен $m\Phi_n$ имеет целые коэффициенты, причем их наибольший общий делитель равен 1. Согласно лемме Гаусса наибольший общий делитель коэффициентов многочлена $mP = (m\Phi_n)Q$ равен произведению наибольших общих делителей коэффициентов многочленов $m\Phi_n$ и Q, т. е. он равен 1. С другой стороны, наибольший общий делитель коэффициентов многочлена mP равен m. Поэтому $m = \pm 1$, т. е. коэффициенты многочлена Φ_n — целые числа. $\square$

13.3. Неприводимость круговых многочленов

В предыдущем параграфе мы показали, что коэффициенты многочлена $\Phi_n(x)$ — целые числа.

Теорема 13.4. Многочлен Φ_n неприводим над $\mathbb{Z}$.

Доказательство. Предположим, что $\Phi_n = fg$, где f и g — многочлены с целыми коэффициентами. Пусть ε — корень многочлена Φ_n. Можно считать, что $f(\varepsilon) = 0$ и многочлен f неприводим. Пусть p — простое число, взаимно простое с n. Тогда ε^p — корень многочлена Φ_n. Мы хотим доказать, что ε^p — корень многочлена f. Предположим, что ε^p не является корнем многочлена f. Тогда можно считать, что $\Phi_n = fgh$, где f и g — неприводимые многочлены со старшим коэффициентом 1 и $f(\varepsilon) = 0$, $g(\varepsilon^p) = 0$.

Многочлен $x^n - 1$ и неприводимый многочлен $f(x)$ имеют общий корень ε, поэтому $x^n - 1$ делится на $f(x)$. Аналогично $x^n - 1$ делится на $g(x)$. А так как многочлены f и g взаимно просты, то $x^n - 1$ делится на их произведение. Следовательно, дискриминант D многочлена $x^n - 1$ делится на результант $R(f, g)$ (см. теорему 3.4 на с. 34). Легко проверить, что $D = \pm n^n$ (см. пример 3.1 на с. 35). Чтобы прийти к противоречию, достаточно показать, что $R(f, g)$ делится на p.

Лемма. Если p — простое число и $f(x)$ — многочлен с целыми коэффициентами, то $\bigl(f(x)\bigr)^p \equiv f(x^p) \pmod p$.

Доказательство. Пусть $f(x) = a_n x^n + \ldots + a_1 x + a_0$. Тогда

$$\bigl(f(x)\bigr)^p = \sum_{k_0+\ldots+k_n=p} \frac{p!}{k_0! \cdot \ldots \cdot k_n!} (a_n x^n)^{k_n} \cdot \ldots \cdot (a_0)^{k_0}.$$

Число $p!/(k_0! \cdot \ldots \cdot k_n!)$ не делится на p лишь в том случае, когда одно из чисел $k_0, \ldots, k_n$ равно p. Следовательно,

$$\bigl(f(x)\bigr)^p \equiv (a_n x)^p + \ldots + (a_0)^p \pmod p.$$

Воспользовавшись тем, что $a^p \equiv a \pmod p$ при всех a, получим требуемое. □

Пусть $y_1 = \varepsilon^p$, y_2, $\ldots$, y_k — корни многочлена g. Согласно лемме $f(\varepsilon^p) \equiv \bigl(f(\varepsilon)\bigr)^p \equiv 0 \pmod p$, т. е. $f(y_1) = p\psi(y_1)$, где ψ — многочлен с

целыми коэффициентами. Многочлен $f-p\psi$ и неприводимый многочлен g имеют общий корень y_1, поэтому $f-p\psi$ делится на g, а значит, $f(y_i)-p\psi(y_i)=0$ при всех i. Следовательно,

$$R(f,g)=\pm f(y_1)\cdot\ldots\cdot f(y_k)=\pm p^k\psi(y_1)\cdot\ldots\cdot\psi(y_k).$$

Выражение $\psi(y_1)\cdot\ldots\cdot\psi(y_k)$ представляет собой симметрический многочлен с целыми коэффициентами от корней многочлена g. Таким образом, это выражение — целое число, т. е. $R(f,g)$ делится на p^k.

Итак, если Φ_n делится на неприводимый многочлен f и ε — корень f, то для любого простого числа p, взаимно простого с n, число ε^p тоже будет корнем многочлена f. Теперь уже легко показать, что все корни многочлена Φ_n являются корнями многочлена f, т. е. $f=\pm\Phi_n$. В самом деле, любой корень ω многочлена Φ_n имеет вид ε^m, где $(m,n)=1$. Запишем m в виде $m=p_1\cdot\ldots\cdot p_s$, где $p_1,\ldots,p_s$ — простые числа, среди которых могут быть совпадающие. Из условия $(m,n)=1$ следует, что $(p_i,n)=1$ при всех i. Поэтому $\varepsilon^{p_1},\varepsilon^{p_1p_2},\ldots,\varepsilon^{p_1\cdots p_s}=\omega$ — корни многочлена f. □

13.4. Выражение Φ_{mn} через Φ_n

Круговой многочлен $\Phi_{mn}(x)$ во многих случаях можно выразить через $\Phi_n(x)$. Мы ограничимся случаем, когда $m=p$ — простое число.

Теорема 13.5. Пусть p — простое число. Тогда

$$\Phi_{pn}(x)=\begin{cases}\Phi_n(x^p) & \text{при } (n,p)=p;\\ \Phi_n(x^p)/\Phi_n(x) & \text{при } (n,p)=1.\end{cases}$$

Доказательство. Рассмотрим сначала случай, когда n делится на p. Если ε — примитивный корень степени pn, то $\omega=\varepsilon^p$ — примитивный корень степени n. При этом корню ω соответствуют корни $\varepsilon_1,\ldots,\varepsilon_p$ так, что $(x-\varepsilon_1)\cdot\ldots\cdot(x-\varepsilon_p)=x^p-\omega$. Следовательно,

$$\Phi_{pn}(x)=\prod_{\varepsilon}(x-\varepsilon)=\prod_{\omega=\varepsilon^p}(x^p-\omega)=\Phi_n(x^p).$$

Рассмотрим теперь случай, когда n не делится на p. В этом случае делители pn состоят из делителей n и их произведений на p. Поэтому

$$\Phi_{pn}(x)=\prod_{d\mid pn}(x^d-1)^{\mu(pn/d)}=\prod_{d\mid n}(x^d-1)^{\mu(pn/d)}\prod_{d\mid n}(x^{dp}-1)^{\mu(n/d)}.$$

А так как $\mu(pn/d) = -\mu(n/d)$, то

$$\Phi_{pn}(x) = \prod_{d|n}(x^d-1)^{-\mu(n/d)}\prod_{d|n}(x^{dp}-1)^{\mu(n/d)} = \big(\Phi_n(x)\big)^{-1}\Phi_n(x^p). \quad \square$$

Воспользовавшись теоремой 13.5, можно вычислить $\Phi_n(\pm 1)$. Начнем с вычисления $\Phi_n(1)$. Если n делится на p, то согласно теореме 13.5 $\Phi_n(1) = \Phi_{n/p}(1)$. Таким образом, если $n = p_1^{\alpha_1}\cdot\ldots\cdot p_k^{\alpha_k}$ и $m = p_1\cdot\ldots\cdot p_k$, то $\Phi_n(1) = \Phi_m(1)$. Остается вычислить $\Phi_m(1)$. Если $m = p$ — простое число, то $\Phi_p(1) = p$. Если же $m = p_1\cdot\ldots\cdot p_k$, где $k > 1$, то положим $p = p_1$ и $n = m/p$. Согласно теореме 13.5 $\Phi_m(1) = \Phi_n(1)/\Phi_n(1) = 1$.

Итак, если $n > 1$, то

$$\Phi_n(1) = \begin{cases} p & \text{при } n = p^\lambda; \\ 1 & \text{при } n \neq p^\lambda. \end{cases}$$

Вычислим теперь $\Phi_n(-1)$. Возможны следующие варианты.

1) $n > 1$ — нечетное число. Тогда $\Phi_n(-1) = \Phi_{2n}(1) = 1$.

2) $n = 2^k$. Тогда $\Phi_n(x) = (x^n-1)/(x^{n/2}-1) = (x^{n/2}+1)$. Поэтому $\Phi_n(-1) = 0$ при $n = 2$ и $\Phi_n(-1) = 2$ при $n = 2^k$, где $k > 1$.

3) $n = 2m$, где $m > 1$ — нечетное число. В этом случае $\Phi_n(-1) = \Phi_m(1)$. Таким образом, $\Phi_n(-1) = p$, если $m = p^\alpha$, и $\Phi_n(-1) = p$, если в m входит более одного простого делителя.

4) $n = 2^k m$, где $k > 1$ и $m > 1$ — нечетное число. Пусть $m = p_1^{\alpha_1}\cdot\ldots\cdot p_t^{\alpha_t}$. Тогда $\Phi_n(x) = \Phi_{2r}(x^s)$, где $r = p_1\cdot\ldots\cdot p_t$ и $s = 2^{k-1}p_1^{\alpha_1-1}\cdot\ldots\cdot p_t^{\alpha_t-1}$. Поэтому $\Phi_n(-1) = \Phi_{2r}(1) = 1$.

13.5. Дискриминант кругового многочлена

Представим круговой многочлен $\Phi_n(x)$ в виде

$$\Phi_n(x) = \prod_{d|n}(x^d-1)^{\mu(n/d)} = (x^n-1)\prod_{d|n,\,d\neq n}(x^d-1)^{\mu(n/d)}.$$

Если ε — корень многочлена Φ_n, то

$$\Phi_n'(\varepsilon) = n\varepsilon^{n-1}\prod_{d|n,\,d\neq n}(\varepsilon^d-1)^{\mu(n/d)}.$$

Поэтому модуль дискриминанта многочлена Φ_n равен

$$\prod_{\varepsilon}|\Phi_n'(\varepsilon)| = n^{\varphi(n)}\prod_{d|n,\,d\neq n}\prod_{\varepsilon}|1-\varepsilon^d|^{\mu(n/d)}.$$

Ясно, что ε^d — примитивный корень степени n/d, т. е.

$$\prod_{\varepsilon}(1-\varepsilon^d) = \bigl(\Phi_{n/d}(1)\bigr)^{\varphi(n)/\varphi(n/d)},$$

поскольку отношение $\deg\Phi_n$ к $\deg\Phi_{n/d}$ равно $\varphi(n)/\varphi(n/d)$.

Значение многочлена $\Phi_{n/d}(x)$ при $x=1$ может быть отлично от 1 лишь в том случае, когда $n/d = p^\lambda$. С другой стороны, $\mu(n/d)\neq 0$ лишь в том случае, когда n/d не делится на квадрат простого числа. Поэтому остаются лишь те значения d, для которых n/d — простое число. Итак,

$$\prod_{\varepsilon}|\Phi_n'(\varepsilon)| = n^{\varphi(n)}\left(\prod_{p|n}p^{\frac{\varphi(n)}{p-1}}\right)^{-1}.$$

Остается определить знак дискриминанта многочлена Φ_n. Воспользуемся для этого тем, что у многочлена Φ_n нет вещественных корней, а его степень равна $\varphi(n)$. В таком случае знак дискриминанта должен быть равен $(-1)^{\varphi(n)/2}$ (см. теорему 3.5 на с. 34).

13.6. Результант пары круговых многочленов

Начнем с того, что вычислим результант $R(\Phi_n, x^m-1)$. Многочлен x^m-1 делится на $\Phi_1 = x-1$, поэтому $R(\Phi_1, x^m-1)=0$. Предположим, что $n\geqslant 2$. Пусть $d=(n,m)$, $n_1 = n/d$, $\xi_1,\xi_2,\ldots$ — первообразные корни степени n, $\eta_1,\eta_2,\ldots$ — первообразные корни степени n_1. Тогда

$$R(\Phi_n, x^m-1) = \prod(\xi_i^m-1) = \prod(1-\xi_i^m) =$$
$$= \Bigl(\prod(1-\eta_i)\Bigr)^{\varphi(n)/\varphi(n_1)} = \bigl(\Phi_{n_1}(1)\bigr)^{\varphi(n)/\varphi(n_1)}.$$

Если $n_1=1$, т. е. если m делится на n, то $\Phi_{n_1}(1)=0$, поэтому $R(\Phi_n, x^m-1)=0$. Если же $n_1\neq 1$, то $\Phi_{n_1}(1)=p$ при $n_1=p^\lambda$ и $\Phi_{n_1}(1)=1$ при $n_1\neq p^\lambda$.

Переходя к вычислению $R(\Phi_n, \Phi_m)$, заметим, что это — целое число, являющееся делителем как числа $R(\Phi_n, x^m - 1)$, так и числа $R(\Phi_m, x^n - 1)$. В самом деле, $x^m - 1 = \Phi_m(x)f(x)$, где $f(x)$ — многочлен с целыми коэффициентами, поэтому

$$R(\Phi_n, x^m - 1) = R(\Phi_n, \Phi_m f) = R(\Phi_n, \Phi_m)R(\Phi_n, f).$$

Кроме того, если $n > m > 1$, то

$$R(\Phi_m, \Phi_n) = (-1)^{\varphi(m)\varphi(n)}R(\Phi_n, \Phi_m) = R(\Phi_n, \Phi_m)$$

и $R(\Phi_m, \Phi_n) > 0$. Последнее свойство можно доказать, например, так. Ясно, что

$$0 \neq R(\Phi_n, x^m - 1) = \prod_{d|m} R(\Phi_n, \Phi_d),$$

поэтому

$$R(\Phi_n, \Phi_m) = \prod_{d|m} R(\Phi_n, x^d - 1)^{\mu(m/d)} > 0.$$

Если m не делится на n и n не делится на m, то числа m/d и n/d, где $d = (m, n)$, не равны 1 и взаимно просты. Поэтому числа $R(\Phi_n, x^m - 1)$ и $R(\Phi_m, x^n - 1)$ взаимно просты, а значит, $R(\Phi_n, \Phi_m) = 1$.

Пусть теперь для определенности m делится на n. Если $m = n$, то $R(\Phi_n, \Phi_m) = 0$. Если $m/n \neq p^\lambda$, то $R(\Phi_m, x^n - 1) = 1$, поэтому $R(\Phi_n, \Phi_m) = 1$. Остается рассмотреть случай $m/n = p^\lambda$. Ясно, что

$$R(\Phi_n, \Phi_m) = \prod_{\delta|n} R(\Phi_m, x^\delta - 1)^{\mu(n/\delta)}.$$

В правой части все множители равны 1, за исключением тех, для которых $m/\delta = p^a$.

Если $(n, p) = 1$, то неединичный множитель возникает лишь при $\delta = n$. В этом случае

$$R(\Phi_n, \Phi_m) = R(\Phi_m, x^n - 1) = p^{\varphi(m)/\varphi(m/n)} = p^{\varphi(n)}.$$

Если n делится на p, то неединичные множители возникают лишь при $\delta = n$ и при $\delta = n/p$. В этом случае

$$R(\Phi_n, \Phi_m) = \frac{R(\Phi_m, x^n - 1)}{R(\Phi_m, x^{n/p} - 1)} = p^a,$$

где

$$a=\frac{\varphi(m)}{\varphi(m/n)}-\frac{\varphi(m)}{\varphi(mp/n)}=\varphi(m)\left(\frac{1}{p^{\lambda-1}(p-1)}-\frac{1}{p^{\lambda}(p-1)}\right)=\frac{\varphi(m)}{p^{\lambda}}=\varphi(n).$$

Итак, если $m\geqslant n$, то

$$R(\Phi_n,\Phi_m)=\begin{cases}0 & \text{при } m=n;\\ p^{\varphi(n)} & \text{при } m=np^{\lambda};\\ 1 & \text{в остальных случаях.}\end{cases}$$

13.7. Коэффициенты круговых многочленов

Примеры многочленов $\Phi_n(x)$ при малых n показывают, что их коэффициенты равны 0 и ±1. Но в работе [Suz] доказано, что любое целое число служит коэффициентом некоторого кругового многочлена. Это доказательство основано на следующем вспомогательном утверждении.

Лемма. Для любого натурального $t\geqslant 3$ существуют такие простые числа $p_1<p_2<\ldots<p_t$, что $p_1+p_2>p_t$.

Доказательство. Фиксируем $t\geqslant 3$. Предположим, что для любого набора простых чисел $p_1<p_2<\ldots<p_t$ выполняется неравенство $p_1+p_2\leqslant p_t$. В таком случае $2p_1<p_t$, поэтому между 2^{k-1} и 2^k заключено менее t простых чисел. Это означает, что $\pi(2^k)<kt$ (здесь $\pi(s)$ — количество простых чисел между 1 и s).

Согласно теореме Чебышева (см. [ГНШ], [Дэ] или [Ч]) $\pi(x)>cx/\ln x$, где c — положительная константа. Поэтому $c2^k/\ln 2^k<kt$, т. е. $c2^k<k^2t\ln 2$. При достаточно больших k это неравенство выполняться не будет. □

Пусть $t\geqslant 3$ — нечетное целое число. Выберем простые числа $p_1<p_2<\ldots<p_t$ так, что $p_1+p_2>p_t$. Положим $p=p_t$. Рассмотрим многочлен $\Phi_n(x)$ по модулю x^{p+1}. При нечетном t

$$\Phi_{p_1\ldots p_t}=\frac{(x^{p_1}-1)\cdot\ldots\cdot(x^{p_t}-1)}{x-1}\cdot\frac{\prod(x^{p_ip_jp_k}-1)}{\prod(x^{p_ip_j}-1)}\cdot\ldots$$

Но $x^{p_ip_j}\equiv 0\pmod{x^{p+1}}$, $x^{p_ip_jp_k}\equiv 0\pmod{x^{p+1}}$ и т. д. Поэтому

$$\Phi_{p_1\ldots p_t}\equiv\pm\frac{(1-x^{p_1})\cdot\ldots\cdot(1-x^{p_t})}{1-x}\pmod{x^{p+1}}.$$

Равенство $\Phi_{p_1\dots p_t}(0) = 1$ позволяет выбрать знак плюс. Из неравенства $p_i + p_j \geqslant p_1 + p_2 > p_t = p$ следует, что

$$(1 - x^{p_1}) \cdot \ldots \cdot (1 - x^{p_t}) \equiv (1 - x^{p_1} - \ldots - x^{p_t}) \pmod{x^{p+1}}.$$

Ясно также, что $(1 - x)^{-1} \equiv (1 + x + \ldots + x^p) \pmod{x^{p+1}}$. Поэтому

$$\Phi_{p_1\dots p_t} \equiv (1 + x + \ldots + x^p)(1 - x^{p_1} - \ldots - x^{p_t}) \pmod{x^{p+1}}.$$

Среди мономов $x^{p_i}, x^{p_i+1}, \ldots, x^{p_i+p}$ моном x^p встречается при всех i, а мономы x^{p-1} и x^{p-2} встречаются при всех $i \neq t$. Поэтому коэффициент при x^p у многочлена $\Phi_{p_1\dots p_t}$ равен $-t+1$, а коэффициент при x^{p-2} равен $-(t-1)+1 = -t+2$.

Когда t пробегает все нечетные числа начиная с 3, числа $-t+1$ и $-t+2$ пробегают все отрицательные числа.

Чтобы получить в качестве коэффициентов круговых многочленов все положительные числа, рассмотрим многочлен $\Phi_{2p_1\dots p_t}$, где $p_1 \geqslant 3$ и $p_1 + p_2 > p_t$. Число $n = p_1 \cdot \ldots \cdot p_t$ нечетно, поэтому $\Phi_{2n}(x) = \Phi_n(-x)$. Это означает, что у многочленов Φ_{2n} и Φ_n коэффициенты как при x^p, так и при x^{p-2} отличаются знаком, т. е. у многочлена $\Phi_{2p_1\dots p_t}$ коэффициенты при x^p и x^{p-2} равны $t-1$ и $t-2$, соответственно.

13.8. Теорема Веддерберна

Одним из наиболее интересных приложений круговых многочленов является доказательство теоремы Веддерберна о коммутативности конечного тела. Такое доказательство предложил Витт [Wt].

Телом называют кольцо, в котором уравнения $ax = b$ и $xa = b$ однозначно разрешимы при всех $a \neq 0$.

Теорема 13.6 (Веддерберн). Конечное ассоциативное тело R коммутативно, т. е. является полем.

Доказательство. Пусть e_1 и e_2 — решения уравнений $ax = a$ и $xa = a$, соответственно. Тогда $ae_1a = a^2 = ae_2a$, поэтому $ae_1 = ae_2$ и $e_1 = e_2 = e$. Покажем, что $be = b$ для любого b. В самом деле, пусть $xa = b$. Тогда $be = xae = xa = b$. Аналогично $eb = b$.

Таким образом, тело R содержит единицу 1. Рассмотрим поле F_p, порожденное элементом $1 \in R$. Тело R является линейным пространством над полем F_p. Пусть r — размерность этого пространства. Тогда R состоит из p^r элементов. Пусть Z — центр тела R, т. е. множество тех

элементов R, которые коммутируют со всеми элементами R. Ясно, что Z — поле, содержащее F_p. Поэтому Z состоит из $q = p^s$ элементов. Тело R является также и линейным пространством над полем Z. Если размерность R над Z равна t, то R состоит из q^t элементов. Таким образом, $p^r = q^t = p^{st}$. Мы хотим доказать, что $R = Z$, т. е. $t = 1$.

Для любого элемента $x \in R$ рассмотрим его нормализатор $N_x = \{y \in R \mid xy = yx\}$. Ясно, что N_x — подтело в R, содержащее Z. С одной стороны, тело N_x является линейным пространством над полем Z, поэтому N_x состоит из q^d элементов. С другой стороны, тело R является линейным пространством над телом N_x, поэтому $q^t = (q^d)^k = q^{dk}$, т. е. $d \mid t$.

В мультипликативной группе R^* для каждого элемента x рассмотрим его орбиту $O_x = \{yxy^{-1} \mid y \in R^*\}$. Ясно, что O_x состоит из

$$|O_x| = |R^*|/|N_x^*| = (q^t - 1)/(q^d - 1)$$

элементов. Орбиты разных элементов либо совпадают, либо не пересекаются, поэтому R^* разбивается на орбиты, причем орбита любого элемента Z^* состоит из одного элемента. Следовательно,

$$q^t - 1 = q - 1 + \sum (q^t - 1)/(q^d - 1), \tag{1}$$

где суммирование ведется по некоторым делителям d числа t. При этом $d < t$ (равенство $d = t$ соответствует тому, что $x \in Z^*$; такие элементы выделены в качестве первого слагаемого).

С помощью кругового многочлена $\Phi_t(x)$ мы покажем, что равенство (1) возможно лишь при $t = 1$. Многочлен $x^t - 1$ делится нацело на $\Phi_t(x)$. Более того, если $d \mid t$ и $d < t$, то многочлен $(x^t - 1)/(x^d - 1)$ тоже делится нацело на $\Phi_t(x)$, так как в этом случае многочлены $x^d - 1$ и $\Phi_t(x)$ не имеют общих корней. В частности, числа $q^t - 1$ и $(q^t - 1)/(q^d - 1)$ делятся на $\Phi_t(q)$. Соотношение (1) показывает, что тогда $q - 1$ делится на $\Phi_t(q)$. С другой стороны, $|\Phi_t(q)| = \prod |q - \varepsilon_i| > q - 1$, так как $|\varepsilon_i| = 1$ и $\varepsilon_i \neq 1$. □

13.9. Многочлены, неприводимые по модулю p

С помощью формулы обращения Мёбиуса можно получить выражение для числа неприводимых многочленов степени n со старшим коэффициентом 1 над полем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Докажем сначала следующее утверждение.

Теорема 13.7. Пусть $F_d(x)$ — произведение всех неприводимых многочленов степени d со старшим коэффициентом 1 над полем $\mathbb{F}_p$. Тогда

$$x^{p^n} - x = \prod_{d|n} F_d(x).$$

Доказательство. Многочлен $x^{p^n} - x$ взаимно прост со своей производной $p^n x^{p^n-1} - 1 = -1$, поэтому у него нет кратных корней. Таким образом, достаточно доказать, что если $f(x)$ — неприводимый многочлен степени d со старшим коэффициентом 1, то $f(x)$ делит $x^{p^n} - x$ тогда и только тогда, когда d делит n.

Пусть α — корень многочлена f и $K = \mathbb{F}_p(\alpha)$ — расширение степени d поля $\mathbb{F}_p$. Оно состоит из p^d элементов и все его элементы удовлетворяют уравнению $x^{p^d} - x = 0$. В самом деле, мультипликативная группа поля $\mathbb{F}_p$ имеет порядок $p^d - 1$, поэтому любой ненулевой элемент $x \in \mathbb{F}_p$ удовлетворяет уравнению $x^{p^d-1} = 1$.

Лемма. а) Над произвольным полем многочлен $x^n - 1$ делит $x^m - 1$ тогда и только тогда, когда n делит m.

б) Если $a \geqslant 2$ — натуральное число, то $a^n - 1$ делит $a^m - 1$ тогда и только тогда, когда n делит m.

Доказательство. а) Пусть $m = qn + r$, где $0 \leqslant r < n$. Тогда

$$\frac{x^m - 1}{x^n - 1} = x^r \frac{x^{qn} - 1}{x^n - 1} + \frac{x^r - 1}{x^n - 1}.$$

Многочлен $x^{qn} - 1$ делится на $x^n - 1$. Поэтому $x^m - 1$ делится на $x^n - 1$ тогда и только тогда, когда $x^r - 1$ делится на $x^n - 1$. Но $r < n$, поэтому $x^r - 1$ делится на $x^n - 1$ лишь при $r = 0$.

б) Доказывается аналогично. □

Предположим сначала, что d делит n. Тогда $p^d - 1$ делит $p^n - 1$, а значит, $x^{p^d} - x$ делит $x^{p^n} - x$. Корень α неприводимого многочлена $f(x)$ является также и корнем уравнения $x^{p^d} = x$, поэтому $f(x)$ делит $x^{p^d} - x$.

Предположим теперь, что $f(x)$ делит $x^{p^n} - x$. Тогда $\alpha^{p^n} - \alpha = 0$. Если $b_1\alpha^{d-1} + b_2\alpha^{d-2} + \ldots + b_d$ — произвольный элемент поля K, то

$$(b_1\alpha^{d-1} + \ldots + b_d)^p = b_1(\alpha^{p^n})^{d-1} + \ldots + b_d = b_1\alpha^{d-1} + \ldots + b_d.$$

Поэтому любой элемент поля K удовлетворяет уравнению $x^{p^n} = x$, т. е. $x^{p^n} - x$ делится на $x^{p^d} - x$. Следовательно, n делится на d. □

Пусть N_d — число неприводимых многочленов степени d со старшим коэффициентом 1 над полем $\mathbb{F}_p$. Тогда степень многочлена F_d равна dN_d, поэтому

$$p^n = \sum_{d|n} dN_d.$$

Применив формулу обращения Мёбиуса, получим

$$N_n = \frac{1}{n} \sum_{d|n} \mu(n/d) p^d.$$

В частности, $N_n \neq 0$, так как сумма $\sum_{d|n} \mu(n/d) p^d$ имеет вид $p^{d_1} \pm \pm p^{d_2} \pm \ldots \pm p^{d_k}$, где числа d_i попарно различны.

14. Многочлены Чебышева

14.1. Определение и основные свойства

Многочлены Чебышева $T_n(x)$ являются одним из наиболее замечательных семейств многочленов. Они часто встречаются во многих областях математики, от теории аппроксимации до теории чисел и топологии трехмерных многообразий. Мы обсудим некоторые наиболее простые, но весьма важные свойства многочленов Чебышева.

Определение многочленов Чебышева основано на том, что $\cos n\varphi$ полиномиально выражается через $\cos\varphi$, т. е. существует такой многочлен $T_n(x)$, что $T_n(x) = \cos n\varphi$ при $x = \cos\varphi$. В самом деле, формула

$$\cos(n+1)\varphi + \cos(n-1)\varphi = 2\cos\varphi\cos n\varphi$$

показывает, что многочлены $T_n(x)$, определенные рекуррентным соотношением

$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$$

и начальными условиями $T_0(x) = 1$ и $T_1(x) = x$, обладают нужным свойством. Эти многочлены $T_n(x)$ называют *многочленами Чебышева.*

Непосредственно из того, что $T_n(x) = \cos n\varphi$ при $x = \cos\varphi$, следует, что $|T_n(x)| \leqslant 1$ при $x \leqslant 1$. А из рекуррентного соотношения следует, что $T_n(x) = 2^{n-1}x^n + a_1x^{n-1} + \ldots + a_n$, где $a_1, \ldots, a_n$ — целые числа.

Наиболее важное свойство многочленов Чебышева было обнаружено самим Чебышевым. Оно заключается в следующем.

Теорема 14.1. Пусть $P_n(x) = x^n + \ldots$ — многочлен степени n со старшим коэффициентом 1, причем $|P_n(x)| \leqslant \frac{1}{2^{n-1}}$ при $|x| \leqslant 1$. Тогда $P_n(x) = \frac{1}{2^{n-1}}T_n(x)$. (Иными словами, многочлен $\frac{1}{2^{n-1}}T_n(x)$ — наименее уклоняющийся от нуля на интервале $[-1, 1]$ многочлен степени n со старшим коэффициентом 1.)

Доказательство. Мы воспользуемся лишь одним свойством многочлена $T_n(x) = 2^{n-1}x^n + \ldots$, а именно тем, что $T_n\bigl(\cos(k\pi/n)\bigr) = \cos k\pi = (-1)^k$ при $k = 0, 1, \ldots, n$. Рассмотрим многочлен $Q(x) = \frac{1}{2^{n-1}}T_n(x) - P_n(x)$. Его степень не превосходит $n-1$, поскольку старшие члены многочленов $\frac{1}{2^{n-1}}T_n(x)$ и $P_n(x)$ равны. Из того, что $|P_n(x)| \leqslant \frac{1}{2^{n-1}}$ при $|x| \leqslant 1$, следует, что в точке $x_k = \cos(k\pi/n)$ знак числа $Q(x_k)$ совпадает со знаком числа $T_n(x_k)$. Таким образом, в концах каждого отрезка $[x_{k+1}, x_k]$ многочлен $Q(x)$ принимает значения разного знака, поэтому у многочлена $Q(x)$ на этом отрезке есть корень. Чуть более аккуратные рассуждения нужны в том случае, когда $Q(x_k) = 0$. В этом случае либо x_k — двукратный корень, либо внутри одного из отрезков $[x_{k+1}, x_k]$ и $[x_k, x_{k-1}]$ есть еще один корень. Это следует из того, что в точках x_{k+1} и x_{k-1} многочлен $Q(x)$ принимает значения одного знака (рис. 5).

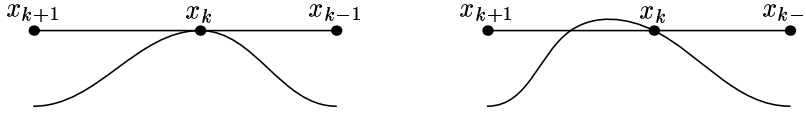

Рис. 5

Количество отрезков $[x_{k+1}, x_k]$ равно n, поэтому многочлен $Q(x)$ имеет по крайней мере n корней. Для многочлена степени не более $n-1$ это означает, что он тождественно равен нулю, т. е. $P_n(x) = \frac{1}{2^{n-1}}T_n(x)$. □

Если $z = \cos\varphi + i\sin\varphi$, то $z + z^{-1} = 2\cos\varphi$ и $z^n + z^{-n} = 2\cos n\varphi$.

Поэтому $T_n\left(\dfrac{z+z^{-1}}{2}\right) = \dfrac{z^n+z^{-n}}{2}$. Воспользовавшись этим свойством, можно доказать следующее утверждение.

Теорема 14.2. Пусть $m = [n/2]$. Тогда

$$T_n(x) = \sum_{j=0}^{m} \binom{n}{2j} x^{n-2j}(x^2-1)^j.$$

Доказательство. Пусть $x = (z+z^{-1})/2$ и $y = (z-z^{-1})/2$. Тогда $y^2 = x^2 - 1$ и

$$z^n + z^{-n} = (x+y)^n + (x-y)^n = \sum_{i=0}^{n} \binom{n}{i}\bigl(1+(-1)^i\bigr)x^{n-i}y^i =$$
$$= 2\sum_{j=0}^{m} \binom{n}{2j} x^{n-2j}y^{2j} = 2\sum_{j=0}^{m} \binom{n}{2j} x^{n-2j}(x^2-1)^j.$$

Остается заметить, что $T_n(x) = \dfrac{z^n+z^{-n}}{2}$. □

Следствие. Пусть p — нечетное простое число. Тогда

$$T_p(x) \equiv T_1(x) \pmod{p}.$$

Доказательство. Запишем p в виде $p = 2m+1$. Тогда

$$T_p(x) = \sum_{j=0}^{m} \binom{p}{2j} x^{p-2j}(x^2-1)^j.$$

Если $j > 0$, то $\binom{p}{2j}$ делится на p. Поэтому

$$T_p(x) \equiv x^p \pmod{p} \equiv x \pmod{p} = T_1(x).$$ □

Для пары многочленов P и Q можно определить их *композицию* $P \circ Q(x) = P\bigl(Q(x)\bigr)$. Многочлены P и Q называют *коммутирующими*, если $P \circ Q = Q \circ P$, т. е. $P\bigl(Q(x)\bigr) = Q\bigl(P(x)\bigr)$.

Теорема 14.3. Многочлены $T_n(x)$ и $T_m(x)$ коммутирующие.

Доказательство. Пусть $x = \cos\varphi$. Тогда $T_n(x) = \cos(n\varphi) = y$ и $T_m(y) = \cos m(n\varphi)$, поэтому $T_m\bigl(T_n(x)\bigr) = \cos mn\varphi$. Аналогично $T_n\bigl(T_m(x)\bigr) = \cos mn\varphi$. Таким образом, равенство $T_n\bigl(T_m(x)\bigr) = T_m\bigl(T_n(x)\bigr)$ выполняется при $|x| < 1$, а значит, это равенство выполняется при всех x. □

Многочлены Чебышева являются единственным нетривиальным примером коммутирующих многочленов. Дело в том, что справедлива следующая теорема классификации пар коммутирующих многочленов. Пусть $l(x) = ax + b$, где $a, b \in \mathbb{C}$ и $a \neq 0$. Будем говорить, что пара многочленов $l \circ f \circ l^{-1}$ и $l \circ g \circ l^{-1}$ *эквивалентна* паре многочленов f и g.

Теорема 14.4 (Ритт). Пусть f и g — коммутирующие многочлены. Тогда пара многочленов f и g эквивалентна одной из следующих пар:

(1) x^m и εx^n, где $\varepsilon^{m-1} = 1$;

(2) $\pm T_m(x)$ и $\pm T_n(x)$, где T_m и T_n — многочлены Чебышева;

(3) $\varepsilon_1 Q^{(k)}(x)$ и $\varepsilon_2 Q^{(l)}(x)$, где $\varepsilon_1^q = \varepsilon_2^q = 1$, $Q(x) = xP(x^q)$, $Q^{(1)} = Q$, $Q^{(2)} = Q \circ Q$, $Q^{(3)} = Q \circ Q \circ Q$, ...

Эта теорема была доказана в 1922 г. американским математиком Риттом; все известные ее доказательства весьма сложные. Современное изложение доказательства теоремы Ритта приведено в [ПрШ].

В некоторых случаях вместо многочлена $T_n(x)$ удобно рассматривать многочлен $P_n(x) = 2T_n(x/2)$ со старшим коэффициентом 1. Многочлены $P_n(x)$ удовлетворяют рекуррентному соотношению $P_{n+1}(x) = xP_n(x) - P_{n-1}(x)$, поэтому $P_n(x)$ — многочлен с целыми коэффициентами.

Если $z = \cos\varphi + i\sin\varphi = e^{i\varphi}$, то $z + z^{-1} = 2\cos\varphi$ и $z^n + z^{-n} = 2\cos n\varphi$. Поэтому $P(z + z^{-1}) = 2T_n(\cos\varphi) = 2\cos n\varphi = z^n + z^{-n}$, т. е. многочлен $P_n(x)$ соответствует полиномиальному выражению величины $z^n + z^{-n}$ через $z + z^{-1}$.

С помощью многочленов P_n можно доказать следующее утверждение.

Теорема 14.5. Если оба числа α и $\cos(\alpha\pi)$ рациональны, то число $2\cos(\alpha\pi)$ целое, т. е. $\cos(\alpha\pi) = 0, \pm 1/2$ или ± 1.

ДОКАЗАТЕЛЬСТВО. Пусть $\alpha = m/n$ — несократимая дробь. Положим $x_0 = 2\cos t$, где $t = \alpha\pi$. Тогда $P_n(x_0) = 2\cos(nt) = 2\cos(n\alpha\pi) = 2\cos(m\pi) = \pm 2$. Поэтому x_0 — корень многочлена $P_n(x) \mp 2 = x^n + b_1 x^{n-1} + \ldots + b_n$ с целыми коэффициентами. Пусть $x_0 = 2\cos(\alpha\pi) = p/q$ — несократимая дробь. Тогда $p^n + b_1 p^{n-1} q + \ldots + b_n q^n = 0$, а значит, p^n делится на q. Но числа p и q взаимно простые, поэтому $q = \pm 1$, т. е. $2\cos(\alpha\pi)$ — целое число. □

Производные многочленов Чебышева удобно вычислять, опираясь непосредственно на соотношение $T_n(x) = \cos n\varphi$, где $x = \cos\varphi$. Например,

$$T_n'(x) = \frac{d\cos n\varphi}{d\varphi}\left(\frac{d\cos\varphi}{d\varphi}\right)^{-1} = \frac{n\sin n\varphi}{\sin\varphi},$$

$$T_n''(x) = \frac{d}{d\varphi}\left(\frac{n\sin n\varphi}{\sin\varphi}\right)\frac{-1}{\sin\varphi} = \frac{n\cos\varphi\sin n\varphi - n^2\cos n\varphi\sin\varphi}{\sin^3\varphi}.$$

Из этих формул следует, что

$$(1-x^2)T_n'(x) = n\big(T_{n-1}(x) - xT_n(x)\big),$$

$$(1-x^2)\big(T_n'(x)\big)^2 = n^2\big(1 - T_n(x)\big)^2,$$

$$(1-x^2)T_n''(x) - xT_n'(x) + n^2 T_n(x) = 0.$$

Тождество $(1-x^2)\big(T_n'(x)\big)^2 = n^2\big(1 - T_n(x)\big)^2$, можно переписать в виде

$$1 = T_n^2(x) - (1-x^2)\mathcal{U}_n^2(x), \tag{1}$$

где $\mathcal{U}_n(x) = \dfrac{\sin n\varphi}{\sin\varphi}$ и $x = \cos\varphi$. Легко проверить, что $\mathcal{U}_n$ — многочлен с целыми коэффициентами. Действительно, индукция по n показывает, что

$$\sin nx = p_n(\cos x)\,\sin x, \quad \cos nx = q_n(\cos x),$$

где p_n и q_n — многочлены с целыми коэффициентами.

Тождество (1) можно использовать для получения решений *уравнения Пелля*

$$x^2 - dy^2 = 1.$$

В самом деле, если (x_1, y_1) — натуральное решение этого уравнения, то

$$1 = T_n^2(x_1) - \frac{(1-x_1^2)}{y_1^2}\left(y_1\mathcal{U}_n(x_1)\right)^2 =$$

$$= T_n^2(x_1) - d\left(y_1\mathcal{U}_n(x_1)\right)^2,$$

поэтому $\bigl(T_n(x_1), y_1\mathcal{U}_n(x_1)\bigr)$ — тоже натуральное решение этого уравнения.

Замечание. Можно доказать, что если (x_1, y_1) — наименьшее натуральное решение уравнения Пелля, то все его натуральные решения имеют вид $\bigl(T_n(x_1), y_1\mathcal{U}_n(x_1)\bigr)$.

14.2. Ортогональные многочлены

Многочлены $f_k(x)$, $k = 0, 1, \ldots$, называют *ортогональными* многочленами на отрезке $[a, b]$ с весовой функцией $w(x) \geqslant 0$, если $\deg f_k = k$ и

$$\int_a^b f_m(x) f_n(x) w(x)\, dx = 0$$

при $m \neq n$.

В пространстве V^{n+1} многочленов степени не более n можно задать скалярное произведение формулой

$$(f, g) = \int_a^b f(x) g(x) w(x)\, dx.$$

Ортогональные многочлены $f_0, f_1, \ldots, f_n$ образуют ортогональный базис в пространстве V^{n+1} с таким скалярным произведением.

Если задан отрезок $[a, b]$ и весовая функция $w(x)$, то ортогональные многочлены определены однозначно с точностью до пропорциональности. В самом деле, они получаются в результате ортогонализации базиса $1, x, x^2, \ldots$

Наиболее известны следующие ортогональные многочлены:

a	b	$w(x)$	Название
-1	1	1	многочлены Лежандра
-1	1	$(1-x^2)^{\lambda-1/2}$	многочлены Гегенбауэра
-1	1	$(1-x)^{\alpha}(1+x)^{\beta}$	многочлены Якоби
$-\infty$	∞	$\exp(-x^2)$	многочлены Эрмита
0	∞	$x^{\alpha}e^{-x}$	многочлены Лагерра

Теорема 14.6. Многочлены Чебышева образуют ортогональную систему многочленов на отрезке $[-1, 1]$ с весовой функцией $w(x) = \dfrac{1}{\sqrt{1-x^2}}$.

Доказательство. Сделав замену $x = \cos\varphi$, получим

$$\int_{-1}^{1} T_n(x)T_m(x)\frac{dx}{\sqrt{1-x^2}} = \int_0^{\pi} \cos n\varphi \cos m\varphi \, d\varphi = \int_0^{\pi} \frac{\cos(m+n)\varphi + \cos(m-n)\varphi}{2} d\varphi.$$

Остается заметить, что

$$\int_0^{\pi} \cos k\varphi \, d\varphi = 0 \qquad \text{при } k \neq 0. \qquad \square$$

Следствие. Если $P_n(x)$ — многочлен степени n и

$$\int_{-1}^{1} P_n(x)\frac{x^k dx}{\sqrt{1-x^2}} = 0$$

при $k = 0, 1, \ldots, n-1$, то $P_n(x) = \lambda T_n(x)$, где λ — некоторое число.

Доказательство. В пространстве V^{n+1} со скалярным произведением

$$(f, g) = \int_{-1}^{1} f(x)g(x)\frac{dx}{\sqrt{1-x^2}}$$

ортогональное дополнение к подпространству, порожденному многочленами $1, x, x^2, \ldots, x^{n-1}$, порождено многочленом Чебышева $T_n(x)$. $\square$

Следствие теоремы 14.6 бывает полезно при доказательстве того, что некоторый многочлен является многочленом Чебышева. Например, с его помощью можно доказать следующее утверждение.

Теорема 14.7. Многочлены Чебышева можно вычислять по формуле

$$T_n(x) = \frac{(-1)^n\sqrt{1-x^2}}{1\cdot 3\cdot 5\cdot \ldots \cdot (2n-1)}\frac{d^n}{dx^n}(1-x^2)^{n-1/2}.$$

Доказательство. Индукцией по m легко доказать, что при $m \leqslant n$

$$\frac{d^m}{dx^m}(1-x^2)^{n-1/2} = P_m(x)(1-x^2)^{n-m-1/2},$$

где $P_m(x)$ — многочлен степени m, причем $P_0(x) = 1$, $P_1(x) = -(2n-1)x$ и $P_{m+1} = 1 - x^2 - (2n-2m-1)xP_m(x)$ при $m \geqslant 1$. Следовательно,

$$\sqrt{1-x^2}\,\frac{d^n}{dx^n}(1-x^2)^{n-1/2} = P_n(x)$$

— многочлен степени n.

Проверим, что $P_n(x) = \lambda T_n(x)$, т. е.

$$\int_{-1}^{1} x^k \frac{d^n}{dx^n}(1-x^2)^{n-1/2}dx = 0$$

при $k = 0, 1, \ldots, n-1$. Интегрируя по частям, получаем

$$\int_{-1}^{1} x^k \frac{d^n}{dx^n}(1-x^2)^{n-1/2}dx =$$

$$= x^k P_{n-1}(x)(1-x^2)^{1/2}\Big|_{-1}^{1} - \int_{-1}^{1} kx^{k-1}\frac{d^{n-1}}{dx^{n-1}}(1-x^2)^{n-1/2}dx.$$

Первое слагаемое равно нулю, так как $1 - x^2 = 0$ при $x = \pm 1$. Затем интегрируем по частям второе слагаемое и т. д. Чтобы в конце концов получить нуль, нужно проинтегрировать по частям $k+1$ раз. При этом на последнем шаге возникнет дифференциал $\dfrac{d^{n-k-1}}{dx^{n-k-1}}$. Это означает, что число $n-k-1$ должно быть неотрицательно, т. е. $k \leqslant n-1$.

Остается проверить, что $\lambda = (-1)^n 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)$. Для этого можно вычислить $P_n(1)$. Дело в том, что при $x = 1$ рекуррентное соотношение

$$P_{m+1}(x) = 1 - x^2 - (2n-2m-1)xP_m(x)$$

принимает вид

$$P_{m+1}(1) = -(2n-2m-1)P_m(1).$$

Таким образом, $P_n(1) = (-1)^n 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1)$. Ясно также, что $T_n(1) = 1$. □

14.3. Неравенства для многочленов Чебышева

Многочлены Чебышева мало уклоняются от нуля на отрезке $[-1,1]$. Это компенсируется тем, что они и их производные быстро возрастают вне этого отрезка. Точнее говоря, справедливо следующее утверждение.

Теорема 14.8. [Ro] Пусть многочлен $p(x) = a_0 + a_1 x + \ldots + a_n x^n$, где $a_i \in \mathbb{C}$, таков, что $|p(x)| \leqslant 1$ при $-1 \leqslant x \leqslant 1$. Тогда $|p^{(k)}(x)| \leqslant |T_n^{(k)}(x)|$ при $|x| \geqslant 1$, $x \in \mathbb{R}$.

Доказательство. Мы воспользуемся лишь тем, что $|p(x_i)| \leqslant 1$ при $x_i = \cos(n-i)\pi/n$, $i = 0, 1, \ldots, n$. Многочлен $p(x)$ полностью определяется этими значениями $p(x_i)$. В самом деле,

$$p(x) = \sum_{i=0}^{n} \frac{p(x_i)}{g_i(x_i)} g_i(x), \tag{1}$$

где $g_i(x) = \prod\limits_{j \neq i} (x - x_j)$. Дифференцируя k раз соотношение (1), получим

$$p^{(k)}(x) = \sum_{i=0}^{n} \frac{p(x_i)}{g_i(x_i)} g_i^{(k)}(x).$$

А так как $|p(x_i)| \leqslant 1$, то

$$|p^{(k)}(x)| \leqslant \sum_{i=0}^{n} \left| \frac{g_i^{(k)}(x)}{g_i(x_i)} \right|. \tag{2}$$

Многочлен $T_n(x)$ в точке x_i принимает значение $\cos(n-i)\pi = (-1)^{n-i}$. Поэтому

$$|T_n^{(k)}(x)| = \left| \sum_{i=0}^{n} \frac{(-1)^{n-i}}{g_i(x_i)} g_i^{(k)}(x) \right|.$$

Ясно также, что $\operatorname{sgn} g_i(x_i) = (-1)^{n-i}$. Кроме того, при $|x| \geqslant 1$ знак числа $g_i^{(k)}(x)$ не зависит от i. В самом деле, все корни многочлена $g_i(x)$ принадлежат отрезку $[-1,1]$, поэтому все корни многочлена $g_i^{(k)}(x)$ тоже принадлежат этому отрезку. Следовательно, $\operatorname{sgn} g_i^{(k)}(x) = 1$ при $x \geqslant 1$ и $\operatorname{sgn} g_i^{(k)}(x) = (-1)^{n-k}$ при $x \leqslant 1$.

В итоге при $|x| \geqslant 1$ получаем

$$\left|T_n^{(k)}(x)\right| = \left|\sum_{i=0}^{n} \frac{g_i^{(k)}(x)}{g_i(x_i)}\right|.$$

В таком случае из неравенства (2) следует, что $\left|p^{(k)}(x)\right| \leqslant \left|T_n^{(k)}(x)\right|$. □

Из теоремы 14.8 можно извлечь много полезных следствий. Сформулируем их в виде отдельных теорем.

Теорема 14.9. Пусть многочлен $p(x) = a_0 + a_1x + \ldots + a_nx^n$, где $a_i \in \mathbb{C}$, таков, что $\left|p(x)\right| \leqslant 1$ при $-1 \leqslant x \leqslant 1$. Тогда $|a_n| \leqslant 2^{n-1}$.

Доказательство. Напомним, что $T_n(x) = b_0 + b_1x + \ldots + b_nx^n$, где $b_n = 2^{n-1}$. Поэтому, применив теорему 14.8 при $k = n$, получим $|a_n| \leqslant |b_n| = 2^{n-1}$. □

Теорема 14.10. При $x \leqslant -1$ и при $x \geqslant 1$ выполняется неравенство

$$\left|T_{n-1}^{(k)}(x)\right| \leqslant \left|T_n^{(k)}(x)\right|.$$

Доказательство. Для многочлена $p(x) = T_{n-1}(x)$ выполняется условие теоремы 14.8, поэтому $|T_{n-1}^{(k)}(x)| = |p(x)| \leqslant |T_n^{(k)}(x)|$. □

Теорема 14.11 [As]. При $x, y \geqslant 1$ выполняется неравенство

$$T_n(xy) \leqslant T_n(x)T_n(y).$$

Доказательство. Фиксируем $y \geqslant 1$ и рассмотрим многочлен $p(x) = T_n(xy)/T_n(y)$. Проверим, что этот многочлен удовлетворяет условию теоремы 14.8, т. е. $\left|p(x)\right| = \left|T_n(xy)\right|/T_n(y) \leqslant 1$ при $-1 \leqslant x \leqslant 1$. При вещественном s функция $\left|T_n(s)\right|$ зависит только от $|s|$, причем если $|s| \geqslant 1$, то $\left|T_n(s)\right|$ монотонно возрастает с возрастанием $|s|$. Ясно также, что $\left|T_n(s)\right| \leqslant 1 \leqslant T_n(y)$ при $|s| \leqslant 1$. Следовательно, если $y \geqslant 1$ и $-1 \leqslant x \leqslant 1$, то $\left|T_n(xy)\right| \leqslant T_n(y)$.

Согласно теореме 14.8 при $x \geqslant 1$ выполняется неравенство $\left|p(x)\right| \leqslant T_n(x)$, т. е. $T_n(xy) \leqslant T_n(x)T_n(y)$. □

14.4. Производящая функция

Для последовательности функций $a_n(x)$ можно рассмотреть ряд $\sum\limits_{n=0}^{\infty} a_n(x)z^n = F(x,z)$. Если радиус сходимости этого ряда положителен, то функцию $F(x,z)$ называют *производящей функцией* последовательности $a_n(x)$.

Теорема 14.12. При $-1 < x < 1$ и $|z| < 1$ выполняются следующие равенства:

(а) $$2\sum_{n=1}^{\infty} \frac{T_n(x)}{n} z^n = -\ln(1-2xz+z^2);$$

(б) $$1 + 2\sum_{n=1}^{\infty} T_n(x)z^n = \frac{1-z^2}{1-2xz+z^2}.$$

Доказательство. а) Пусть $x = \cos\varphi$. Тогда

$$1 - 2xz + z^2 = (1 - e^{i\varphi}z)(1 - e^{-i\varphi}z),$$

поэтому $\ln(1-2xz+z^2) = \ln(1-e^{i\varphi}z) + \ln(1-e^{-i\varphi}z)$. Ясно также, что

$$-\ln(1-e^{\pm i\varphi}z) = \sum_{n=1}^{\infty} \frac{e^{\pm in\varphi}}{n} z^n$$

при $|z| < 1$. Следовательно,

$$-\ln(1-2xz+z^2) = \sum_{n=1}^{\infty} \frac{2\cos n\varphi}{n} z^n = 2\sum_{n=1}^{\infty} \frac{T_n(x)}{n} z^n.$$

б) Продифференцировав по z обе части равенства (а), получим

$$2\sum_{n=1}^{\infty} T_n(x)z^{n-1} = \frac{2x-2z}{1-2xz+z^2}$$

Следовательно,

$$1 + 2\sum_{n=1}^{\infty} T_n(x)z^n = 1 + \frac{z(2x-2z)}{1-2xz+z^2} = \frac{1-z^2}{1-2xz+z^2}. \qquad \square$$

С помощью теоремы 14.12 можно получить следующее явное выражение для многочлена Чебышева.

Теорема 14.13. Пусть $n \geqslant 1$ и $m = [n/2]$. Тогда

$$T_n(x) = \frac{1}{2}\sum_{k=0}^{m}(-1)^k \frac{n}{n-k}\binom{n-k}{k}(2x)^{n-2k}.$$

Доказательство. Согласно теореме 14.12 (а)

$$2\sum_{n=1}^{\infty}\frac{T_n(x)}{n}z^n = -\ln(1-2xz+z^2) = \sum_{p=1}^{\infty}\frac{(2xz-z^2)^p}{p} =$$

$$= \sum_{p=1}^{\infty}\sum_{k=0}^{p}(-1)^k\frac{1}{p}\binom{p}{k}z^{p+k}(2x)^{p-k}.$$

Поэтому

$$T_n(x) = \frac{1}{2}\sum_{p+k=n}(-1)^k\frac{n}{p}\binom{p}{k}(2x)^{p-k}$$

$$= \frac{1}{2}\sum_{k=0}^{M}(-1)^k\frac{n}{n-k}\binom{n-k}{k}(2x)^{n-2k}.$$

Суммирование ведется до тех пор, пока $n-2k \geqslant 0$, поэтому $M = [n/2] = m$. □

Более удобная явная формула получается для многочлена $P_n(x) = 2T_n(x/2)$, а именно:

$$P_n(x) = \sum_{k=0}^{m}(-1)^k\frac{n}{n-k}\binom{n-k}{k}x^{n-2k}, \tag{1}$$

где $m = [n/2]$.

Напомним, что многочлен $P_n(x)$ соответствует полиномиальному выражению величины $z^n + z^{-n}$ через $z + z^{-1}$ (это следует из того, что $z^n + z^{-n} = 2\cos n\varphi$ и $z + z^{-1} = 2\cos\varphi$ при $z = e^{i\varphi}$).

Легко проверить, что при $n = 2m+1$ выполняется равенство

$$(z+z^{-1})^n = \sum_{k=0}^{m}\binom{n}{k}(z^{n-2k}+z^{2k-n}),$$

а при $n = 2m$ выполняется равенство

$$(z + z^{-1})^n = \sum_{k=0}^{m-1} \binom{n}{k}(z^{n-2k} + z^{2k-n}) + \binom{n}{m}.$$

Таким образом, если $P_0(x) = 1$, а при $n \geqslant 1$ многочлены $P_n(x)$ задаются формулой (1), то выполняется соотношение

$$x^n = \sum_{k=0}^{m} \binom{n}{k} P_{n-2k}(x), \tag{2}$$

где $m = [n/2]$.

Соотношения (1) и (2) можно записать следующим образом. Пусть $a_n = x^n$ и $b_n = P_n(x)$, где x — некоторое фиксированное число. Тогда

$$a_n = \sum_{k=0}^{m} \binom{n}{k} b_{n-2k}, \quad b_n = \sum_{k=0}^{m} (-1)^k \frac{n}{n-k} \binom{n-k}{k} a_{n-2k} \tag{3}$$

(при $n = 0$ второе соотношение выглядит как $b_0 = a_0$). Покажем, что соотношения (3) эквивалентны не только для указанных последовательностей, но и для произвольных последовательностей. Прежде всего заметим, что первое соотношение имеет вид $a_n = b_n + \sum \beta_{n-i} b_{n-i}$, а второе соотношение имеет вид $b_n = a_n + \sum \alpha_{n-i} a_{n-i}$, поэтому каждое соотношение однозначно определяет как последовательность a_n по последовательности b_n, так и последовательность b_n по последовательности a_n. Ясно также, что для последовательностей $a_n = \sum \lambda_i x_i^n$, $b_n = \sum \lambda_i P_n(x_i)$, где λ_i и x_i — фиксированные наборы чисел, соотношения (3) эквивалентны, потому что они эквивалентны для последовательностей $a_n = x_i^n$, $b_n = P_n(x_i)$. Остается проверить, что для любой последовательности $a_0, a_1, \ldots, a_n$ можно подобрать такие числа $\lambda_0, \ldots, \lambda_n$ и $x_0, \ldots, x_n$, что $a_l = \sum_{i=0}^{n} \lambda_i x_i^l$ при $l = 0, 1, \ldots, n$. Выберем произвольные попарно различные числа $x_0, \ldots, x_n$. Тогда для чисел $\lambda_0, \ldots, \lambda_n$ получим систему линейных уравнений с определителем

$$\begin{vmatrix} 1 & \ldots & 1 \\ x_0 & \ldots & x_n \\ \ldots & \ldots & \ldots \\ x_0^n & \ldots & x_n^n \end{vmatrix} \neq 0.$$

Эта система уравнений имеет решение при любых $a_0, \ldots, a_n$.

Соотношения (3) позволяют получать нетривиальные тождества с биномиальными коэффициентами. Положим, например, $b_n = 1$ при всех n. Тогда

$$a_{2m+1} = \sum_{k=0}^{m} \binom{2m}{k} = 2^{2m},$$
$$a_{2m} = \sum_{k=0}^{m} \binom{2m+1}{k} = \frac{1}{2}\left(2^{2m} + \binom{2m}{m}\right);$$

эти тождества легко получаются из разложений $(1+1)^{2m+1}$ и $(1+1)^{2m}$ по биному Ньютона. В таком случае соотношение

$$b_n = \sum_{k=0}^{m} (-1)^k \frac{n}{n-k} \binom{n-k}{k} a_{n-2k}$$

принимает вид

$$1 = \sum_{k=0}^{m} (-1)^k \frac{2m+1}{2m+1-k} \binom{2m+1-k}{k} 2^{2m},$$
$$2 = \sum_{k=0}^{m} (-1)^k \frac{2m}{2m-k} \binom{2m-k}{k} \frac{1}{2}\left(2^{2m-2k} + \binom{2m-2k}{m-k}\right).$$

15. Многочлены Бернулли

15.1. Определения многочленов Бернулли

Рассмотрим функцию $g(z,t) = \dfrac{te^{tz}}{e^t - 1}$. При $t = 2k\pi i$ знаменатель обращается в нуль, поэтому при таких t функция $g(z,t)$ может иметь особенности. Но при $t = 0$, как легко убедиться, функция g регулярна. Поэтому функцию $g(z,t)$ можно разложить в ряд

$$g(z,t) = \sum_{n=0}^{\infty} \frac{t^n}{n!} B_n(z),$$

сходящийся при $|t| < 2\pi$.

Как мы сейчас увидим, $B_n(z)$ — многочлен степени n. Многочлены $B_n(z)$ называют *многочленами Бернулли*, а числа $B_n = B_n(0)$ называют *числами Бернулли*.

Ряд для функции $g(z,t)$ представляет собой произведение рядов

$$g(0,t)=\sum_{n=0}^{\infty}\frac{t^n}{n!}B_n \quad \text{и} \quad e^{tz}=\sum_{n=0}^{\infty}\frac{t^n z^n}{n!}.$$

Поэтому

$$\frac{B_n(z)}{n!}=\sum_{k=0}^{\infty}\frac{B_{n-k}z^k}{k!\,(n-k)!},$$

т. е.

$$B_n(z)=\sum_{k=0}^{\infty}\binom{n}{k}B_{n-k}z^k.$$

Формально это равенство можно записать в виде $B_n(z)=(B+z)^n$, где под B^{n-k} будет подразумеваться B_{n-k}.

Одно из важнейших свойств многочленов Бернулли заключается в том, что

$$B_n(z+1)-B_n(z)=nz^{n-1}. \tag{1}$$

Для доказательства формулы (1) достаточно заметить, что

$$\sum_{n=0}^{\infty}\bigl(B_n(z+1)-B_n(z)\bigr)\frac{t^n}{n!}=g(t,z+1)-g(t,z)=$$

$$=\frac{te^{t(z+1)}}{e^t-1}-\frac{te^{tz}}{e^t-1}=te^{tz}=\sum_{n=0}^{\infty}\frac{t^{n+1}z^n}{n!}.$$

Сложим равенства (1) для $z=0,1,\ldots,m-1$. В результате получим

$$\sum_{k=0}^{m-1}k^{n-1}=\frac{1}{n}\bigl(B_n(m)-B_n(0)\bigr). \tag{2}$$

Это, в частности, означает, что сумма $1+2^{n-1}+\ldots+(m-1)^{n-1}$ представляет собой многочлен степени n от m. Именно это свойство было обнаружено Я. Бернулли [Bern]. А производящая функция $\dfrac{te^{tz}}{e^t-1}=$ $=\sum\limits_{n=0}^{\infty}\dfrac{t^n}{n!}B_n(z)$ была предложена Эйлером в 1738 г.

При вычислении многочленов Бернулли удобно пользоваться рекуррентными соотношениями

$$\sum_{r=0}^{n-1}\binom{n}{r}B_r(z)=nz^{n-1}, \quad n\geqslant 2. \tag{3}$$

Эти соотношения можно доказать следующим образом:

$$\sum_{n=0}^{\infty}\frac{t^n}{n!}B_n(z+1)=\frac{te^{tz}}{e^t-1}e^z=\left(\sum_{r=0}^{\infty}\frac{t^r}{r!}B_r(z)\right)\left(\sum_{s=0}^{\infty}\frac{z^s}{s!}\right),$$

поэтому $B_n(z+1)=\sum\limits_{r=0}^{n}\binom{n}{r}B_r(z)=B_n(z)+\sum\limits_{r=0}^{n-1}\binom{n}{r}B_r(z)$. Остается воспользоваться соотношением (1).

При $z=0$ соотношения (3) превращаются в рекуррентные соотношения для чисел Бернулли

$$\sum_{r=0}^{n-1}\binom{n}{r}B_r=0,\quad n\geqslant 2. \tag{4}$$

Легко проверить, что $B_0=1$, Поэтому из соотношений (4) последовательно получаем

$$B_1=-\frac{1}{2},\quad B_2=\frac{1}{6},\quad B_3=0,\quad B_4=-\frac{1}{30},\quad B_5=0,\quad \ldots$$

Несложно показать, что $B_{2k+1}=0$ при $k\geqslant 1$. В самом деле,

$$\frac{t}{e^t-1}=1-\frac{t}{2}+\sum_{n=2}^{\infty}\frac{t^n}{n!}B_n,$$

поэтому достаточно проверить, что функция

$$\frac{t}{e^t-1}+\frac{t}{2}=t\frac{e^t+1}{e^t-1}$$

четна. В четности этой функции легко убедиться.

В 1832 г. Аппель показал, что многочлены Бернулли связаны соотношением

$$B'_{n+1}(z)=(n+1)B_n(z).$$

Чтобы доказать это соотношение, продифференцируем по z обе части равенства

$$\sum_{n=0}^{\infty}\frac{t^n}{n!}B_n(z)=\frac{te^{tz}}{e^t-1}.$$

В результате получим

$$\sum_{n=0}^{\infty}\frac{t^n}{n!}B'_n(z)=\frac{t^2e^{tz}}{e^t-1}=\sum_{n=0}^{\infty}\frac{t^{n+1}}{n!}B_n(z).$$

Приравнивая коэффициенты при t^{n+1}, получаем требуемое.

15.2. Теоремы дополнения, сложения аргументов и умножения

Многочлены Бернулли обладают следующими свойствами:

$B_n(1-z) = (-1)^n B_n(z)$ (*теорема дополнения*);

$B_n(x+y) = \sum\limits_{s=0}^{n} \binom{n}{s} B_s(x) y^{n-s}$ (*теорема сложения аргументов*);

$\frac{1}{m} \sum\limits_{k=0}^{m-1} B_n\left(z + \frac{k}{m}\right) = m^{-n} B_n(mz)$ (*теорема умножения*).

Все эти теоремы легко выводятся из соотношения

$$\sum_{n=0}^{\infty} \frac{t^n}{n!} B_n(z) = \frac{te^{tz}}{e^t - 1}.$$

Для доказательства теоремы дополнения достаточно заметить, что

$$\sum_{n=0}^{\infty} \frac{t^n}{n!} B_n(1-z) = \frac{te^{t(1-z)}}{e^t - 1} = \frac{-te^{-tz}}{e^{-t} - 1} = \sum_{n=0}^{\infty} \frac{(-t)^n}{n!} B_n(z).$$

Теорема сложения аргументов доказывается следующим образом:

$$\sum_{n=0}^{\infty} \frac{t^n}{n!} B_n(x+y) = \frac{te^{tx}e^{ty}}{e^t - 1} = \left(\sum_{s=0}^{\infty} \frac{t^s}{s!} B_s(x)\right) \left(\sum_{r=0}^{\infty} \frac{t^r y^r}{r!}\right) =$$

$$= \sum_{r,\, s=0}^{\infty} \frac{t^{r+s}}{r!s!} B_s(x) y^r = \sum_{n=0}^{\infty} \sum_{s=0}^{n} \frac{t^n}{n!} \binom{n}{s} B_s(x) y^{n-s}.$$

Для доказательства теоремы умножения мы воспользуемся тождеством

$$\frac{1}{e^t - 1} = \frac{1 + e^t + \ldots + e^{(m-1)t}}{e^{mt} - 1}.$$

Из этого тождества следует, что

$$\sum_{n=0}^{\infty} \frac{t^n}{n!} B_n(mz) = \frac{te^{mtz}}{e^t - 1} = \frac{1}{m} \frac{e^{mtz} mt(1 + e^t + \ldots + e^{(m-1)t})}{e^{mt} - 1} =$$

$$= \frac{1}{m} \sum_{k=0}^{m-1} \frac{e^{(z+k/m)mt} mt}{e^{mt} - 1} = \frac{1}{m} \sum_{k=0}^{m-1} \sum_{n=0}^{\infty} \frac{m^n t^n}{n!} B_n\left(z + \frac{k}{m}\right).$$

Теорема умножения показывает, что многочлен Бернулли $B_n(x)$ является решением функционального уравнения

$$\frac{1}{m}\sum_{k=0}^{m-1} f\left(x+\frac{k}{m}\right) = m^{-n} f(mx). \tag{1}$$

Теорема 15.1 [Le]. При фиксированных m, $n>1$ существует единственный многочлен степени n со старшим коэффициентом 1, удовлетворяющий функциональному уравнению (1).

Доказательство. Существование требуемого многочлена можно доказать и непосредственно, но мы не будем этого делать, а просто воспользуемся уже известным нам фактом, что многочлены Бернулли удовлетворяют функциональному уравнению (1).

Пусть $p(x) = x^n + \ldots$ и $q(x) = x^n + \ldots$ — два разных многочлена, удовлетворяющих функциональному уравнению (1). Их разность $\Delta(x) = a_0 x^d + \ldots$, где $a_0 \neq 0$ и $d < n$, тоже удовлетворяет уравнению (1). Сравнение коэффициентов при x^d в левой и правой части равенства

$$\frac{1}{m}\sum_{k=0}^{m-1} \Delta\left(x+\frac{k}{m}\right) = m^{-n}\Delta(mx)$$

показывает, что $a_0 = m^{d-n}a_0$. Это противоречит условию $m>1$ и предположению о том, что $a_0 \neq 0$ и $d<n$. □

Сделав замену переменных, функциональное уравнение (1) можно привести к виду

$$f(x) = m^{s-1}\sum_{k=0}^{m-1} f\left(\frac{x+k}{m}\right), \tag{2}$$

где $s=n$. В случае натурального s непрерывные функции $f:(0,1)\to\mathbb{C}$, удовлетворяющие уравнению (1), исследовал Кубер [Ku]. В общем случае, т. е. при $s\in\mathbb{C}$, пространство таких функций двумерно, причем в нем можно выбрать базис f_{even}, f_{odd} так, что

$$f_{\text{even}}(x) = f_{\text{even}}(1-x) \quad \text{и} \quad f_{\text{odd}}(x) = -f_{\text{odd}}(1-x).$$

О разных свойствах решений уравнения (2) Джон Милнор написал большую интересную статью [Mi].

15.3. Формула Эйлера

Пусть $s \in \mathbb{C}$, $\operatorname{Re} s > 1$. Тогда ряд $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ сходится. Функция $\zeta(s) = \sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ допускает аналитическое продолжение на всю комплексную плоскость. При этом в точке $s = 1$ она имеет простой полюс, а в остальных точках регулярна.

При целых s ряд $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ рассматривал еще Эйлер. Но рассматривать $\zeta(s)$ как функцию комплексного переменного первым начал Риман, и именно он обнаружил наиболее глубокие ее свойства и наиболее важные ее приложения. В связи с этим функцию $\zeta(s)$ называют *дзета-функцией Римана*.

Теорема 15.2 (Эйлер). Если k — натуральное число, то

$$\zeta(2k) = \frac{(-1)^{k+1} B_{2k} 2^{2k-1} \pi^{2k}}{(2k)!}.$$

Доказательство. Воспользуемся разложением функции $\sin z$ в бесконечное произведение: $\sin z = z \prod\limits_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2\pi^2}\right)$. Продифференцировав логарифмы обеих частей этого равенства, получим

$$\frac{\cos z}{\sin z} = \frac{1}{z} + \sum_{n=1}^{\infty} \frac{2z}{z^2 - n^2\pi^2},$$

т. е.

$$z\frac{\cos z}{\sin z} = 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \left(\frac{z}{n\pi}\right)^{2k}. \tag{1}$$

С другой стороны, подставив $t = 2iz$ в равенство

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + \sum_{m=2}^{\infty} B_m \frac{t^m}{m!},$$

получим

$$z\frac{\cos z}{\sin z} = iz\frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = 1 + \sum_{m=2}^{\infty} B_m \frac{(2iz)^m}{m!}. \tag{2}$$

Сравнение коэффициентов при z^{2k} в (1) и (2) дает требуемое равенство. □

Из формулы Эйлера для $\zeta(2k)$ видно, что число $\zeta(2k)$ трансцендентное, потому что число π трансцендентное. Что же касается чисел $\zeta(2k+1)$, то для них нет столь удобной формулы. В частности, лишь в 1978 г. Апери (R. Apéry) доказал иррациональность числа $\zeta(3)$. Наиболее простое из известных мне доказательств иррациональности числа $\zeta(3)$ приведено в [Beu].

15.4. Теорема Фаульгабера–Якоби

Суммированием степенного ряда $1^m+2^m+3^m+\ldots$ математики интересовались задолго до Бернулли. В 1617 г. немецкий математик Иоганн Фаульгабер (1580–1635) опубликовал книгу, в которой привел суммы таких рядов для $m \leqslant 11$. Затем в 1631 г. в книге [Fa] он продолжил свои вычисления до $m = 17$.

Суммированием степенных рядов занимался и Пьер Ферма. В 1636 г. он писал Мерсенну: «...Мы не хотели здесь на этом останавливаться, однако построили решение, возможно, простейшей во всей арифметике задачи, благодаря которой не только *можем найти сумму квадратов или кубов любой прогрессии*, но и *вообще сумму всех степеней до бесконечности благодаря самому общему методу*; квадрато-квадратов, квадрато-кубов и т. д.» Многие историки математики склонны верить, что Ферма действительно получил решение этой задачи почти за сто лет до Бернулли.

Фаульгабер в своей книге [Fa] отметил, что все суммы $\sum n^k$ полиномиально выражаются через первые две суммы $\sum n$ и $\sum n^2$. Двести лет спустя, в 1834 г., Якоби переоткрыл теорему Фаульгабера. Известно, что у Якоби была упомянутая книга Фаульгабера, но не известно, читал он ее или нет.

Введем для удобства многочлены

$$S_{n-1}(m) = \frac{1}{n}\bigl(B_n(m) - B_n(0)\bigr).$$

Формула (2) на с. 130 показывает, что

$$S_n(m) = 1^n + 2^n + \ldots + (m-1)^n.$$

Теорема 15.3 (Фаульгабер–Якоби). Пусть $U = S_1(x)$ и $V = S_2(x)$. Тогда при $k \geqslant 1$ существуют такие многочлены P_k и Q_k с рациональными коэффициентами, что $S_{2k+1}(x) = U^2 P_k(U)$ и $S_{2k}(x) = V Q_k(U)$.

Доказательство. Чтобы получить выражение для S_{2k+1}, воспользуемся равенством

$$\big(n(n-1)\big)^r = \sum_{x=1}^{n-1}(x^r(x+1)^r - x^r(x-1)^r) = \\ = 2\left(\tbinom{r}{1}\sum x^{2r-1} + \tbinom{r}{3}\sum x^{2r-3} + \tbinom{r}{5}\sum x^{2r-5} + \dots\right), \quad (1)$$

т. е.

$$\big(n(n-1)\big)^{i+1} = \sum \tbinom{i+1}{2(i-j)+1} S_{2j+1}(n).$$

Эти равенства для можно записать в матричном виде:

$$\begin{pmatrix} n^2(n-1)^2 \\ n^3(n-1)^3 \\ n^4(n-1)^4 \\ \vdots \end{pmatrix} = 2\begin{pmatrix} 2 & 0 & 0 & \dots \\ 1 & 3 & 0 & \dots \\ 0 & 4 & 4 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}\begin{pmatrix} S_3(n) \\ S_5(n) \\ S_7(n) \\ \vdots \end{pmatrix}.$$

В полученной бесконечной матрице все главные миноры конечного порядка невырожденные, поэтому

$$\begin{pmatrix} S_3(n) \\ S_5(n) \\ S_7(n) \\ \vdots \end{pmatrix} = \frac{1}{2}\|a_{ij}\|^{-1}\begin{pmatrix} n^2(n-1)^2 \\ n^3(n-1)^3 \\ n^4(n-1)^4 \\ \vdots \end{pmatrix}, \quad \text{где} \quad a_{ij} = \tbinom{i+1}{2(i-j)+1}.$$

Эта формула показывает, что $S_{2k+1}(n)$ выражается через $n(n-1) = 2U(n)$ и делится на $\big(n(n-1)\big)^2$.

Чтобы получить выражение для S_{2k}, воспользуемся равенством

$$n^{r+1}(n-1)^r = \sum_{x=1}^{n-1}(x^r(x+1)^{r+1} - (x-1)^r x^{r+1}) = \\ = \sum x^{2r}\left(\tbinom{r+1}{1} + \tbinom{r}{1}\right) + \sum x^{2r-1}\left(\tbinom{r+1}{2} - \tbinom{r}{2}\right) + \\ + \sum x^{2r-2}\left(\tbinom{r+1}{3} + \tbinom{r}{3}\right) + \sum x^{2r-3}\left(\tbinom{r+1}{4} - \tbinom{r}{4}\right) + \dots = \\ = \left(\tbinom{r+1}{1} + \tbinom{r}{1}\right)\sum x^{2r} + \left(\tbinom{r+1}{3} + \tbinom{r}{3}\right)\sum x^{2r-2} + \dots \\ \dots + \tbinom{r}{1}\sum x^{2r-1} + \tbinom{r}{3}\sum x^{2r-3} + \dots$$

Суммы нечетных степеней можно уничтожить с помощью (1). В результате получим

$$n^{r+1}(n-1)^r = \frac{n^r(n-1)^r}{2} + \left(\binom{r+1}{1} + \binom{r}{1}\right)\sum x^{2r} + \\ + \left(\binom{r+1}{3} + \binom{r}{3}\right)\sum x^{2r-2} + \dots,$$

т. е.

$$n^i(n-1)^i\left(\frac{2n-1}{2}\right) = \sum\left(\binom{i+1}{2(i-j)+1} + \binom{i}{2(i-j)+1}\right)S_{2j}(n).$$

Теперь аналогично предыдущему случаю получаем

$$\begin{pmatrix} S_2(n) \\ S_4(n) \\ S_6(n) \\ \vdots \end{pmatrix} = \frac{2n-1}{2}\|b_{ij}\|^{-1}\begin{pmatrix} n(n-1) \\ n^2(n-1)^2 \\ n^3(n-1)^3 \\ \vdots \end{pmatrix},$$

где $b_{ij} = \binom{i+1}{2(i-j)+1} + \binom{i}{2(i-j)+1}$.

Простые вычисления показывают, что $S_2(n) = \frac{2n-1}{2}\cdot\frac{n(n-1)}{3}$. Поэтому многочлены $S_4(n)$, $S_6(n)$, ... делятся на $S_2(n)$, причем $S_{2k}(n)/S_2(n)$ является многочленом от $n(n-1) = 2U(n)$. □

15.5. Арифметические свойства чисел и многочленов Бернулли

В этом параграфе мы докажем некоторые теоремы о знаменателях значений многочленов Бернулли в рациональных точках. Наибольший интерес при этом представляют значения в точке 0, т. е. числа Бернулли.

При формулировке утверждений о знаменателях рациональных чисел бывает удобно пользоваться понятием p-целого числа. Если p — простое число, то рациональное число r называют *p-целым*, если p не входит в знаменатель числа r, т. е. знаменатель t несократимой дроби $s/t = r$ не делится на p.

Для рационального числа r запись $r \equiv 0 \pmod p$ будет означать, что числитель s несократимой дроби $s/t = r$ делится на p. Легко проверить, что если $r_1 \equiv r_2 \equiv 0 \pmod p$, то $r_1 r_2 \equiv 0 \pmod p$ и $r_1 \pm r_2 \equiv 0 \pmod p$. Кроме того, если число r_1 является p-целым и $r_2 \equiv 0 \pmod p$, то $r_1 r_2 \equiv \equiv 0 \pmod p$.

Теорема 15.4 (Куммер). Пусть p — простое число. Если натуральное число n не делится на $p-1$, то число B_n/n является p-целым и

$$\frac{B_{n+p-1}}{n+p-1} - \frac{B_n}{n} \equiv 0 \pmod{p}.$$

Доказательство. Мультипликативная группа поля $\mathbb{Z}/p\mathbb{Z}$ циклическая, поэтому у нее есть образующая. Это означает, что существует натуральное число a, заключенное между 1 и p, для которого $a^k \not\equiv \not\equiv 1 \pmod{p}$ при $k = 1, \ldots, p-2$. Рассмотрим функцию

$$A(t) = \frac{at}{e^{at}-1} - \frac{t}{e^t-1} = \sum_{k=1}^{\infty}(a^k-1)B_k\frac{t^k}{k!} =$$
$$= t\sum_{k=1}^{\infty}(a^k-1)\frac{B_k}{k}\frac{t^{k-1}}{(k-1)!} = t\sum_{k=1}^{\infty}A_k\frac{t^{k-1}}{(k-1)!},$$

где $A_{k-1} = (a^k-1)\dfrac{B_k}{k}$.

Достаточно доказать, что все числа A_k являются p-целыми и

$$A_{k+p-1} - A_k \equiv 0 \pmod{p}.$$

В самом деле, если n не делится на $p-1$, то $a^n \not\equiv 1 \pmod{p}$, поэтому равенство $\dfrac{B_n}{n} = \dfrac{A_{n-1}}{a^n-1}$ показывает, что число B_n/n тоже будет p-целым. А так как $a^{p-1} \equiv 1 \pmod{p}$, то

$$A_{k+p-1} - A_k = (a^{n+p-1}-1)\frac{B_{n+p-1}}{n+p-1} - (a^n-1)\frac{B_n}{n} \equiv$$
$$\equiv \left(\frac{B_{n+p-1}}{n+p-1} - \frac{B_n}{n}\right)(a^n-1) \pmod{p}.$$

Воспользуемся равенством

$$\sum_{k=1}^{\infty}A_k\frac{t^{k-1}}{(k-1)!} = \frac{a}{e^{at}-1} - \frac{1}{e^t-1}.$$

Положим $u = e^t - 1$. Тогда

$$\frac{a}{e^{at}-1} - \frac{1}{e^t-1} = \frac{a}{(1+u)^a-1} - \frac{1}{u} = \frac{a}{au+\sum b_s u^s} - \frac{1}{u} =$$
$$= \frac{1}{u}\left(\frac{1}{1+\sum(b_s/a)u^{s-1}} - 1\right) = \sum_{r=0}^{\infty}c_r u^r.$$

Все числа c_r являются p-целыми, потому что таковы все числа b_s/a. Таким образом,

$$\sum_{k=1}^{\infty} A_k \frac{t^{k-1}}{(k-1)!} = \sum_{r=0}^{\infty} c_r (e^t - 1)^r,$$

где все коэффициенты c_r являются p-целыми.

Функцию $(e^t-1)^r$ можно представить в виде линейной комбинации с целыми коэффициентами функций e^{mt}, $m = 0, 1, \ldots, r$. В свою очередь,

$$e^{mt} = \sum_{l=0}^{\infty} m^l \frac{t^l}{l!}.$$

Поэтому A_k можно представить в виде линейной комбинации с p-целыми коэффициентами чисел m^{k-1}. Равенство $c_r(e^t-1)^r = c_r t^r + \ldots$ показывает, что эта линейная комбинация состоит из конечного числа слагаемых.

Сумма и произведение p-целых чисел является p-целым числом, поэтому A_k — p-целое число. Ясно также, что

$$m^{(k-1)+(p-1)} - m^{k-1} = m^{k-1}(m^{p-1} - 1) \equiv 0 \pmod{p}.$$

Поэтому число $A_{k+p-1} - A_k$ представляет собой линейную комбинацию с p-целыми коэффициентами рациональных чисел, у которых числители делятся на p. Это означает, что

$$A_{k+p-1} - A_k \equiv 0 \pmod{p}. \qquad \square$$

Теорема 15.5 (фон Штаудт). Пусть n — четное число, p — простое число. Тогда если n не делится на $p-1$, то B_n — p-целое число, а если n делится на $p-1$, то $pB_n \equiv -1 \pmod{p}$.

Доказательство. Согласно предыдущей теореме, если p — простое число и n не делится на $p-1$, то p не входит в знаменатель B_n. Поэтому остается рассмотреть случай, когда n делится на $p-1$.

Перемножим равенства $\sum\limits_{k=0}^{\infty} B_k \frac{t^k}{k!} = \frac{t}{e^t-1}$ и $\sum\limits_{n=0}^{\infty} \frac{p^n t^{n-1}}{n!} = \frac{e^{pt}-1}{t}$. В результате получим

$$\sum_{n,k=0}^{\infty} \frac{p^n B_k t^{n+k-1}}{n!\,k!} = \sum_{r=0}^{p-1} e^{rt} = \sum_{r=0}^{p-1} \sum_{s=0}^{\infty} \frac{r^s t^s}{s!}.$$

Сравнение коэффициентов при t^n в левой и правой части показывает, что

$$\sum_{k=0}^{n+1} \frac{p^{n+1-k}B_k}{(n+1-k)!\,k!} = \sum_{r=1}^{p-1} \frac{r^n}{n!}.$$

Учитывая, что $B_{n+1} = B_{n-1} = 0$, получаем

$$pB_n = -\sum_{k=0}^{n-2} pB_k \frac{p^{n-k}}{n+1-k} + \sum_{r=1}^{p-1} r^n.$$

Ясно, что при $n-k \geqslant 2$ число $p^{n-k}/(n-k+1)$ является p-целым, поэтому индукция по n показывает, что числа $pB_2, \ldots, pB_n$ являются p-целыми. (База индукции: $pB_0 = p$, $pB_1 = -p/2$.)

При $n-k \geqslant 2$ число $p^{n-k}/(n-k+1)$ не только является p-целым, но и его числитель (после возможных сокращений) делится на p, т.е.

$$p^{n-k}/(n-k+1) \equiv 0 \pmod{p}.$$

Следовательно,

$$pB_n \equiv \sum_{r=1}^{p-1} r^n \pmod{p}.$$

В рассматриваемом случае n делится на $p-1$, поэтому $r^n \equiv 1 \pmod{p}$ при $r = 1, 2, \ldots, p-1$. В итоге получаем

$$pB_n \equiv -1 \pmod{p}. \qquad \square$$

Положим $\widetilde{B}_n(t) = B_n(t) - B_n(0)$. Напомним, что в таком случае

$$\widetilde{B}_n(m) = n\bigl(1^{n-1} + 2^{n-1} + \ldots + (m-1)^{n-1}\bigr)$$

при всех натуральных m.

Теорема 15.6 (Алмквист–Мойрман). При всех натуральных h, k и n число $k^n\widetilde{B}_n(h/k)$ целое.

Доказательство [Sur]. Теорему сложения аргументов

$$B_n(x+y) = \sum_{s=0}^{n} B_s(x)y^{n-s}$$

можно записать в виде

$$\widetilde{B}_n(x+y)=\sum_{s=0}^{n}\widetilde{B}_s(x)y^{n-s}+\widetilde{B}_n(y).$$

Поэтому требуемое утверждение достаточно доказать для $h=1$.

Обозначим для краткости $k^n\widetilde{B}_n(h/k)=a_n$. Ясно, что $B_0(z)=B_0$. Поэтому

$$\sum_{n=1}^{\infty}\frac{t^n}{n!}\widetilde{B}_n(z)=\sum_{n=0}^{\infty}\frac{t^n}{n!}B_n(z)-\sum_{n=0}^{\infty}\frac{t^n}{n!}B_n(0)=\frac{te^{tz}}{e^t-1}-\frac{t}{e^t-1}=\frac{t(e^{tz}-1)}{e^t-1}.$$

Положим $z=1/k$ и сделаем замену $x=kt$. В результате получим

$$\sum_{n=1}^{\infty}\frac{a_nx^n}{n!}=\frac{kx(e^x-1)}{e^{kx}-1}.$$

Запишем это соотношение в двух видах:

$$\sum_{n=1}^{\infty}\frac{a_nx^n}{n!}(e^{kx}-1)=kx(e^x-1),$$

$$\sum_{n=1}^{\infty}\frac{a_nx^n}{n!}(1+e^x+\ldots+e^{(k-1)x})=kx.$$

Воспользуемся разложениями $e^{kx}-1=\sum\limits_{r=1}^{\infty}\dfrac{k^rx^r}{r!}$ и $e^x-1=\sum\limits_{s=1}^{\infty}\dfrac{x^s}{s!}$. Сравнивая коэффициенты при x^n в левой и правой части, в первом случае при всех $n\geqslant 1$ получаем

$$\sum_{l=1}^{n-1}\binom{n+1}{l}a_rk^{n-l}=(n+1)(1-a_n). \tag{2}$$

Во втором случае получаем $a_1=1$, а при $n\geqslant 2$ получаем

$$\sum_{l=1}^{n-1}\binom{n}{l}a_rs_{n-l}=-ka_n, \tag{3}$$

где $s_0=k$ и $s_m=1^m+2^m+\ldots+(k-1)^m$.

Целочисленность a_n мы докажем по индукции с помощью соотношений (2) и (3). Для этого нам понадобится следующее вспомогательное утверждение.

Лемма. Пусть p — простое число, $2 \leqslant l \leqslant r$ и $(p, s) = 1$. Тогда $\binom{sp^r}{l}$ делится на p^{r-l+1}.

Доказательство. Запишем l в виде $l = tp^a$, где $(t, p) = 1$. Ясно, что $a \leqslant l - 1$ (равенство возможно лишь в случае $l = p = 2$). Легко проверить, что $\binom{m}{n} = \frac{m}{n}\binom{m-1}{n-1}$. Поэтому

$$\binom{sp^r}{l} = \binom{sp^r}{tp^a} = \frac{s}{t}\,p^{r-a}\binom{sp^r-1}{tp^a-1} = \frac{s}{t}\,p^{r-a}\,N,$$

где N — целое число, а числа s и t взаимно просты с p. Следовательно, число $\binom{sp^r}{l}$ делится на p^{r-a}. В свою очередь, p^{r-a} делится на p^{r-l+1}, так как $a \leqslant l - 1$. □

Из наших обозначений уже давно исчезло k, поэтому напомним, что $a_n = k^n \widetilde{B}_n(h/k)$. Рассмотрим сначала случай, когда k — простое число. Предположим, что $a_1, \ldots, a_{n-1}$ — целые числа. Тогда из соотношений (2) и (3) следует, что $(n+1)a_n$ и ka_n — целые числа. Если $n+1$ не делится на k, то a_n — целое число. Пусть теперь $n+1 = sk^r$, где $r \geqslant 1$ и $(k, s) = 1$. Чтобы убедиться в целочисленности a_n, достаточно доказать, что число $(n+1)a_n = sk^r a_n$ делится на k^r. Формула (2) показывает, что для этого, в свою очередь, достаточно доказать, что при $l = 1, 2, \ldots, sk^r - 2$ числа $\binom{n+1}{l}k^{n-l}$ делятся на k^r. При $l \leqslant n - r = sk^r - 1 - r$ это очевидно. Если же $sk^r - r \leqslant l \leqslant sk^r - 2$, то рассмотрим число $l' = sk^r - l$ и применим к нему лемму. В результате получим, что число $\binom{sk^r}{l} = \binom{sk^r}{l'}$ делится на $k^{r-l'+1}$, а значит, число $\binom{n+1}{l}k^{n-l}$ делится на $k^{n-l+r-l'+1} = k^r$, что и требовалось.

Случай $k = p_1^{a_1} \cdot \ldots \cdot p_m^{a_m}$, где $p_1, \ldots, p_m$ — различные простые числа, не требует существенно новых рассуждений. Предположим, что числа $a_1, \ldots, a_{n-1}$ целые. Тогда из соотношений (2) и (3) следует, что числа $(n+1)a_n$ и ka_n целые. Запишем $n+1$ в виде $n+1 = p_1^{b_1} \cdot \ldots \cdot p_m^{b_m} s$, где $(s, p_i) = 1$. Если $b_i \geqslant 1$, то те же самые рассуждения, что и в предыдущем случае, показывают, что $(n+1)a_n$ делится на p^{b_i}. Положим $s_i = (n+1)p_i^{-b_i}$. Тогда $(s_i, p_i) = 1$ и все числа $s_i a_n$ целые. Это означает, что в знаменатель рационального числа a_n не входят простые множители $p_1, \ldots, p_m$. С другой стороны, число ka_n целое, поэтому в знаменатель числа a_n могут входить только простые множители числа k. □

Задачи к главе 3

Симметрические многочлены

3.1. Пусть $\sigma_1, \ldots, \sigma_n$ — элементарные симметрические функции, а числа $a_1, \ldots, a_n \in \mathbb{C}$ удовлетворяют системе уравнений

$$\sigma_k(a_1, \ldots, a_n) = \sigma_k(a_k, \ldots, a_k).$$

Доказать, что $a_1 = \ldots = a_n$.

В задачах 3.2–3.4 мы будем считать, что $x = (x_1, \ldots, x_n)$ и $y = (y_1, \ldots, y_n)$, где все числа $x_1, \ldots, x_n, y_1, \ldots, y_n$ положительны. Сумма $x + y$ определяется покомпонентно.

3.2 [ML]. Доказать, что при $r = 2, \ldots, n$ для элементарных симметрических функций σ_i выполняются неравенства

$$\frac{\sigma_r(x+y)}{\sigma_{r-1}(x+y)} \geqslant \frac{\sigma_r(x)}{\sigma_{r-1}(x)} + \frac{\sigma_r(y)}{\sigma_{r-1}(y)}.$$

3.3 [ML]. Доказать, что при $r = 1, 2, \ldots, n$ выполняется неравенство

$$\sqrt[r]{\sigma_r(x+y)} \geqslant \sqrt[r]{\sigma_r(x)} + \sqrt[r]{\sigma_r(y)}.$$

3.4 [Wh]. Фиксируем k и определим функции $T_r(x)$ соотношением

$$\sum_{r=0}^{\infty} T_r(x) t^r = \begin{cases} \prod\limits_{i=0}^{n} (1 + x_i t)^k & \text{при } k > 0, \\ \prod\limits_{i=0}^{n} (1 - x_i t)^k & \text{при } k < 0. \end{cases}$$

(В частности, если $k = 1$, то $T_r(x) = \sigma_r(x)$ — элементарный симметрический многочлен, а если $k = -1$, то $T_r(x) = p_r(x)$ — полный однородный многочлен.)

а) Доказать, что если $k > 0$, то $\sqrt[r]{T_r(x+y)} \geqslant \sqrt[r]{T_r(x)} + \sqrt[r]{T_r(y)}$.

б) Доказать, что если $k < 0$, то $\sqrt[r]{T_r(x+y)} \leqslant \sqrt[r]{T_r(x)} + \sqrt[r]{T_r(y)}$.

Целозначные многочлены

3.5. Доказать, что если многочлен $f(x)$ степени n принимает целые значения при $x = 0, 1, 4, 9, \ldots, n^2$, то он принимает целые значения при всех $x = m^2$, $m \in \mathbb{N}$.

3.6. Пусть m и n — натуральные числа. Доказать, что следующие условия эквивалентны:

(а) существуют такие целые числа $a_0, \ldots, a_n$, что

$$\text{НОД}(a_0, \ldots, a_n, m) = 1$$

и значения многочлена $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ при всех $x \in \mathbb{Z}$ делятся на m;

(б) $n!/m \in \mathbb{Z}$.

Многочлены Чебышева

3.7. Доказать, что при $n \geqslant 2$ дискриминант многочлена Чебышева T_n равен $2^{(n-1)^2} n^2$.

3.8. а) Доказать, что если число $n \geqslant 3$ нечетно, то многочлен Чебышева T_n приводим.

б) Доказать, что если $n \neq 2^k$, то многочлен T_n приводим.

в) Доказать, что если число $n \geqslant 3$ нечетно, то многочлен $T_n(x)/x$ неприводим тогда и только тогда, когда число n простое.

3.9. Пусть $u(x)$ и $v(x)$ — многочлены с действительными коэффициентами, причем $\sqrt{1-u^2} = v\sqrt{1-x^2}$. Доказать, что тогда:

а) $u'(x) = \pm n v(x)$, где $n = \deg u$;

б) $u(x) = \pm T_n(x)$.

3.10. а) Доказать, что функция $y = T_n(x)$ удовлетворяет дифференциальному уравнению

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

и любое полиномиальное решение этого дифференциального уравнения имеет вид cT_n, где c — некоторая константа.

б) Доказать, что функция $y = T_n(x)$ удовлетворяет дифференциальному уравнению

$$(1-x^2)(y')^2 = n^2(1-y^2),$$

причем это уравнение имеет только два решения, а именно, $y = \pm T_n(x)$.

3.11. Пусть $\Delta_n(x)$ — определитель матрицы порядка n с диагональными элементами $(x, \ldots, x)$, наддиагональными элементами $\left(1, \frac{1}{2}, \ldots, \frac{1}{2}\right)$ и поддиагональными элементами $\left(\frac{1}{2}, \ldots, \frac{1}{2}\right)$; остальные элементы матрицы нулевые, т. е. $a_{ij} = 0$ при $|i-j| > 1$. Доказать, что $T_n(x) = 2^{n-1}\Delta_n(x)$.

3.12 [Da]. Напомним, что матрицу (a_{ij}) называют циркулянтной, если $a_{ij} = b_i - b_j$, где $b_k = b_l$ при $k \equiv l \pmod{n}$. Пусть $\Delta_n(x)$ — определитель циркулянтной матрицы с $b_0 = 1$, $b_1 = -2x$, $b_2 = 1$. Доказать, что

$$\Delta_n(x) = 2\bigl(1 - T_n(x)\bigr).$$

Решения задач

3.2. При $r = 2$ требуемое неравенство следует из тождества

$$\frac{\sigma_2(x+y)}{\sigma_1(x+y)} - \frac{\sigma_2(x)}{\sigma_1(x)} - \frac{\sigma_2(y)}{\sigma_1(y)} = \frac{\sum\limits_{i=1}^{n}\left(x_i\sum\limits_{j=1}^{n} y_j - y_i\sum\limits_{j=1}^{n} x_j\right)^2}{2\sigma_1(x)\sigma_1(y)\sigma_1(x+y)}.$$

Предположим теперь, что $r > 2$ и требуемое неравенство уже доказано для $r-1$. Рассмотрим систему чисел $\widehat{x}_i = (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Легко проверить, что

$$\sum_{i=1}^{n} x_i\sigma_{r-1}(\widehat{x}_i) = r\sigma_r(x), \tag{1}$$

$$x_i\sigma_{r-1}(\widehat{x}_i) + \sigma_r(\widehat{x}_i) = \sigma_r(x). \tag{2}$$

Запишем равенства (2) для $i = 1, \ldots, n$ и просуммируем их. В результате получим

$$\sum_{i=1}^{n} x_i\sigma_{r-1}(\widehat{x}_i) + \sum_{i=1}^{n} \sigma_r(\widehat{x}_i) = n\sigma_r(x).$$

Вычтя из этого равенства тождество (1), получим

$$\sum_{i=1}^{n} \sigma_r(\widehat{x}_i) = (n-r)\sigma_r(x). \tag{3}$$

Ясно также, что

$$\sigma_r(x) - \sigma_r(\widehat{x}_i) = x_i\sigma_{r-1}(\widehat{x}_i) = x_i\sigma_{r-1}(x) - x_i^2\sigma_{r-2}(\widehat{x}_i).$$

Суммируя эти равенства при $i = 1, \ldots, n$ и учитывая соотношение (3), получаем

$$r\sigma_r(x) = \sum_{i=1}^{n} x_i\sigma_{r-1}(x) - \sum_{i=1}^{n} x_i^2\sigma_{r-2}(\widehat{x}_i),$$

т. е.

$$\frac{\sigma_r(x)}{\sigma_{r-1}(x)} = \frac{1}{r}\left(\sum_{i=1}^{n} x_i - \sum_{i=1}^{n} \frac{x_i^2 \sigma_{r-2}(\widehat{x}_i)}{\sigma_{r-1}(x)}\right) =$$

$$= \frac{1}{r}\left(\sum_{i=1}^{n} x_i - \sum_{i=1}^{n} \frac{x_i^2}{x_i + \sigma_{r-1}(\widehat{x}_i)/\sigma_{r-2}(\widehat{x}_i)}\right).$$

Запишем аналогичные тождества для y и $x+y$. Требуемое неравенство следует из того, что если x_i, y_i, a_i, b_i, c_i — положительные числа, причем $c_i \geqslant a_i + b_i$, то

$$\frac{x_i^2}{x_i+a_i} + \frac{y_i^2}{y_i+a_i} - \frac{(x_i+y_i)^2}{x_i+y_i+c_i} \geqslant \frac{x_i^2}{x_i+a_i} + \frac{y_i^2}{y_i+a_i} - \frac{(x_i+y_i)^2}{x_i+y_i+a_i+b_i} =$$

$$= \frac{(a_i x_i - b_i y_i)^2}{(x_i+a_i)(y_i+b_i)(x_i+y_i+a_i+b_i)} \geqslant 0.$$

3.3. Мы воспользуемся задачей 3.2 и следующим вспомогательным утверждением.

Лемма. Если $a_1, \ldots, a_r, b_1, \ldots, b_r$ — неотрицательные числа, то

$$\sqrt[r]{(a_1+b_1)\cdot\ldots\cdot(a_r+b_r)} \geqslant \sqrt[r]{a_1\cdot\ldots\cdot a_r} + \sqrt[r]{b_1\cdot\ldots\cdot b_r}.$$

Доказательство. Пусть

$$R(z) = \bigl\{(z_1, \ldots, z_r) \in \mathbb{R}^r \mid z_1\cdot\ldots\cdot z_r = 1,\ z_i > 0\bigr\}.$$

Согласно неравенству между средним арифметическим и средним геометрическим

$$\sqrt[r]{a_1\cdot\ldots\cdot a_r} = \min_{R(z)} \frac{a_1 z_1 + \ldots + a_r z_r}{r}.$$

Поэтому

$$\sqrt[r]{(a_1+b_1)\cdot\ldots\cdot(a_r+b_r)} = \min_{R(z)} \frac{(a_1+b_1)z_1 + \ldots + (a_r+b_r)z_r}{r} \geqslant$$

$$\geqslant \min_{R(z)} \frac{a_1 z_1 + \ldots + a_r z_r}{r} + \min_{R(z)} \frac{b_1 z_1 + \ldots + b_r z_r}{r} \geqslant$$

$$\geqslant \sqrt[r]{a_1\cdot\ldots\cdot a_r} + \sqrt[r]{b_1\cdot\ldots\cdot b_r}. \quad \square$$

Представим $\sigma_r(x+y)$ в виде произведения

$$\frac{\sigma_r(x+y)}{\sigma_{r-1}(x+y)} \cdot \frac{\sigma_{r-1}(x+y)}{\sigma_{r-2}(x+y)} \cdot \ldots \cdot \frac{\sigma_1(x+y)}{1}.$$

Согласно задаче 3.2

$$\frac{\sigma_k(x+y)}{\sigma_{k-1}(x+y)} \geqslant \frac{\sigma_k(x)}{\sigma_{k-1}(x)} + \frac{\sigma_k(y)}{\sigma_{k-1}(y)}.$$

Воспользовавшись теперь леммой, получим

$$\sqrt[r]{\sigma_r(x+y)} \geqslant \sqrt[r]{\frac{\sigma_r(x)}{\sigma_{r-1}(x)} \cdot \frac{\sigma_{r-1}(x)}{\sigma_{r-2}(x)} \cdot \ldots \cdot \frac{\sigma_1(x)}{1}} + \\ + \sqrt[r]{\frac{\sigma_r(y)}{\sigma_{r-1}(y)} \cdot \frac{\sigma_{r-1}(y)}{\sigma_{r-2}(y)} \cdot \ldots \cdot \frac{\sigma_1(y)}{1}} = \sqrt[r]{\sigma_r(x)} + \sqrt[r]{\sigma_r(y)}.$$

3.4. Мы рассмотрим лишь случай $k < 0$, включающий полные однородные многочлены. Пусть $l = -k > 0$. В таком случае для гамма-функции имеется интегральное представление

$$\Gamma(l) = \int_0^\infty e^{-t} t^{l-1}\, dt.$$

При $a > 0$ можно сделать замену $t = as$ и получить

$$\Gamma(l) = a^l \int_0^\infty e^{-as} s^{l-1}\, ds,$$

т. е.

$$a^k = a^{-l} = \frac{1}{\Gamma(l)} \int_0^\infty e^{-as} s^{l-1}\, ds.$$

Положим $a_i = 1 - x_i t$. При малых $|t|$ число a_i положительно, поэтому

$$\prod_{i=1}^n (1 - x_i t)^k = \left(\frac{1}{\Gamma(l)}\right)^n \int_0^\infty \ldots \int_0^\infty f(s_1, \ldots, s_n)\, ds_1 \ldots ds_n,$$

где

$$f(s_1,\dots,s_n)=e^{-s_1-\dots-s_n}e^{t(x_1s_1+\dots+x_ns_n)}(s_1\cdot\ldots\cdot s_n)^{l-1}.$$

Учитывая, что

$$e^{t(x_1s_1+\dots+x_ns_n)}=\sum_{r=0}^{\infty}\frac{t^r(x_1s_1+\ldots+x_ns_n)^r}{r!},$$

получаем

$$T_r(x)=\frac{1}{r!}\left(\frac{1}{\Gamma(l)}\right)^n\int_0^\infty\!\!\dots\!\int_0^\infty(x_1s_1+\ldots+x_ns_n)^r\varphi(s_1,\dots,s_n)\,ds_1\dots ds_n,$$

где $\varphi(s_1,\dots,s_n)=e^{-s_1-\dots-s_n}(s_1\cdot\ldots\cdot s_n)^{l-1}$. Требуемое неравенство следует теперь из неравенства Минковского

$$\left(\int_a^b\big(g(x)+h(x)\big)^r\,dx\right)^{1/r}\leqslant\left(\int_a^b g^r(x)\,dx\right)^{1/r}+\left(\int_a^b h^r(x)\,dx\right)^{1/r},$$

где функции g и h неотрицательны на $[a,b]$.

3.11. Несложные вычисления показывают, что $T_n(x)=2^{n-1}\Delta_n(x)$ при $n=1$ и $n=2$. При $n\geqslant 2$, раскладывая определитель $\Delta_n(x)$ по последней строке, получаем соотношение

$$\Delta_{n+1}(x)=x\Delta_n(x)-\frac{1}{4}\Delta_{n-1}(x).$$

Это соотношение соответствует рекуррентному соотношению

$$T_{n+1}(x)=2xT_n(x)-T_{n-1}(x).$$

3.12. Пусть $\varepsilon_1,\dots,\varepsilon_n$ — различные корни степени n из 1, $f(t)=c_0+$ $+c_1t+\ldots+c_nt^n$. Тогда определитель циркулянтной матрицы с элементами $a_{ij}=c_{i-j}$ равен $f(\varepsilon_1)\cdot f(\varepsilon_2)\cdot\ldots\cdot f(\varepsilon_n)$. В самом деле, например, при $n=3$ получаем

$$\begin{pmatrix}1&1&1\\1&\varepsilon_1&\varepsilon_1^2\\1&\varepsilon_2&\varepsilon_2^2\end{pmatrix}\begin{pmatrix}c_0&c_2&c_1\\c_1&c_0&c_2\\c_2&c_1&c_0\end{pmatrix}=\begin{pmatrix}f(1)&f(1)&f(1)\\f(1)&\varepsilon_1f(\varepsilon_1)&\varepsilon_1^2f(\varepsilon_1)\\f(1)&\varepsilon_2f(\varepsilon_2)&\varepsilon_2^2f(\varepsilon_2)\end{pmatrix}=$$

$$=f(\varepsilon_1)\cdot f(\varepsilon_2)\cdot\ldots\cdot f(\varepsilon_n)\begin{pmatrix}1&1&1\\1&\varepsilon_1&\varepsilon_1^2\\1&\varepsilon_2&\varepsilon_2^2\end{pmatrix}.$$

А так как определитель матрицы $\begin{pmatrix} 1 & 1 & 1 \\ 1 & \varepsilon_1 & \varepsilon_1^2 \\ 1 & \varepsilon_2 & \varepsilon_2^2 \end{pmatrix}$ не равен нулю, на него можно сократить. В результате получим требуемое равенство. При $n > 3$ рассуждения аналогичны.

В нашем случае $f(t) = 1 - 2xt + t^2$, поэтому

$$\Delta_n(x) = \prod_{k=1}^{n}(1 - 2x\varepsilon_k + \varepsilon_k^2).$$

Таким образом, требуется доказать, что

$$2(1 - \cos n\varphi) = \prod_{k=1}^{n}(1 - 2\varepsilon_k \cos\varphi + \varepsilon_k^2).$$

Докажем сначала, что

$$2(1 - \cos n\varphi) = 2^n \prod_{k=1}^{n}\left(1 - \cos\left(\varphi + \frac{2k\pi}{n}\right)\right).$$

Это равенство следует из того, что

$$x^{2n} - 2x^n \cos n\varphi + 1 = \left(x^n - \exp(in\varphi)\right)\left(x^n - \exp(-in\varphi)\right) =$$
$$= \prod_{k=1}^{n}\left(x - \exp i\left(\varphi + \frac{2k\pi}{n}\right)\right)\prod_{k=1}^{n}\left(x - \exp i\left(-\varphi - \frac{2k\pi}{n}\right)\right) =$$
$$= \prod_{k=1}^{n}\left(x^2 - 2x\cos\left(\varphi + \frac{2k\pi}{n}\right) + 1\right).$$

В самом деле, при $x = 1$ получаем требуемое равенство.

Докажем теперь, что

$$2^n \prod_{k=1}^{n}\left(1 - \cos\left(\varphi + \frac{2k\pi}{n}\right)\right) = \prod_{k=1}^{n}(1 - 2\cos\varphi\,\varepsilon_k + \varepsilon_k^2),$$

где $\varepsilon_k = \exp(2k\pi i/n)$. Ясно, что

$$(x - \varepsilon_k)(x - \varepsilon_{-k}) = x^2 - 2x\cos(2k\pi/n) + 1.$$

Поэтому $\varepsilon_k^2 + 1 = 2\varepsilon_k \cos(2k\pi/n)$, а значит,

$$\prod_{k=1}^{n}(1 - 2\cos\varphi\,\varepsilon_k + \varepsilon_k^2) = \prod_{k=1}^{n} 2\varepsilon_k\,(\cos(2k\pi/n) - \cos\varphi) =$$
$$= 2^{2n}\left(\prod_{k=1}^{n}\varepsilon_k\right)\prod_{k=1}^{n}\sin\left(\frac{\varphi}{2} + \frac{k\pi}{n}\right)\sin\left(\frac{\varphi}{2} - \frac{k\pi}{n}\right).$$

Остается заметить, что последнее выражение равно

$$2^{2n}\prod_{k=1}^{n}\sin^2\left(\frac{\varphi}{2} + \frac{k\pi}{n}\right) = 2^n\prod_{k=1}^{n}\left(1 - \cos\left(\varphi + \frac{2k\pi}{n}\right)\right).$$

В самом деле, $\prod\varepsilon_k = (-1)^{n+1}$, так как $x^n - 1 = \prod(x - \varepsilon_k)$. Ясно также, что при $k = 1, \ldots, n-1$

$$\sin\left(\frac{\varphi}{2} + \frac{k\pi}{n}\right) = -\sin\left(\frac{\varphi}{2} - \frac{(n-k)\pi}{n}\right),$$

а при $k = n$

$$\sin\left(\frac{\varphi}{2} + \frac{k\pi}{n}\right) = \sin\left(\frac{\varphi}{2} - \frac{k\pi}{n}\right).$$

Глава 4
Некоторые свойства многочленов

16. Многочлены с предписанными значениями

16.1. Интерполяционный многочлен Лагранжа

Пусть $x_1, \ldots, x_{n+1}$ — попарно различные точки комплексной плоскости $\mathbb{C}$. Тогда существует ровно один многочлен $P(x)$ степени не выше n, принимающий в точке x_i заданное значение a_i. Действительно, единственность многочлена P следует из того, что разность двух таких многочленов обращается в нуль в точках $x_1, \ldots, x_{n+1}$ и имеет при этом степень не выше n. Ясно также, что следующий многочлен обладает всеми требуемыми свойствами:

$$P(x) = \sum_{k=1}^{n+1} a_k \frac{(x-x_1)\cdot\ldots\cdot(x-x_{k-1})\cdot(x-x_{k+1})\cdot\ldots\cdot(x-x_{n+1})}{(x_k-x_1)\cdot\ldots(x_k-x_{k-1})\cdot(x_k-x_{k+1})\cdot\ldots\cdot(x_k-x_{n+1})} =$$

$$= \sum_{k=1}^{n+1} a_k \frac{\omega(x)}{(x-x_k)\omega'(x_k)},$$

где $\omega(x) = (x-x_1)\cdot\ldots\cdot(x-x_{n+1})$.

Многочлен $P(x)$ называют при этом *интерполяционным многочленом Лагранжа*, а точки $x_1, \ldots, x_{n+1}$ называют *узлами интерполяции*. Если $a_k = f(x_k)$, где f — некоторая функция, то многочлен P называют интерполяционным многочленом Лагранжа для функции f.

Теорема 16.1. Пусть $f \in C^{n+1}\bigl([a,b]\bigr)$ и P — интерполяционный многочлен Лагранжа для функции f с узлами интерполяции $x_1, \ldots, x_{n+1} \in [a,b]$. Тогда

$$\max_{a\leqslant x\leqslant b}\bigl|P(x)-f(x)\bigr| \leqslant \frac{M}{(n+1)!}\max_{a\leqslant x\leqslant b}\bigl|\omega(x)\bigr|,$$

где $M = \max\limits_{a\leqslant x\leqslant b}\bigl|f^{(n+1)}(x)\bigr|$ и $\omega(x) = (x-x_1)\cdot\ldots\cdot(x-x_{n+1})$.

ДОКАЗАТЕЛЬСТВО. Достаточно проверить, что для любой точки $x_0 \in [a,b]$ найдется такая точка $\xi \in [a,b]$, что

$$f(x_0) - P(x_0) = \frac{f^{(n+1)}(\xi)}{(n+1)!}\omega(x_0).$$

При $x_0 = x_i$, $1 \leqslant i \leqslant n$, это равенство очевидно, поэтому будем считать, что $x_0 \neq x_i$. Рассмотрим функцию

$$u(x) = f(x) - P(x) - \lambda\omega(x),$$

где λ — некоторая константа. Поскольку $\omega(x_0) \neq 0$, эту константу можно выбрать так, что $u(x_0) = 0$. Ясно также, что $u(x_1) = \ldots\ldots = u(x_{n+1}) = 0$. Функция $u(x)$ имеет по крайней мере $n+2$ нулей на отрезке $[a,b]$, поэтому функция $u'(x)$ имеет по крайней мере $n+1$ нуль на этом отрезке, а функция $u^{(k)}(x)$ имеет по крайней мере $n+2-k$ нулей. При $k = n+1$ получаем, что функция $u^{(n+1)}(x) = f^{(n+1)}(x) - (n+1)!\lambda$ обращается в нуль в некоторой точке $\xi \in [a,b]$. Это означает, что $\lambda = f^{(n+1)}(\xi)/(n+1)!$, т. е.

$$f(x_0) - P(x_0) = \frac{f^{(n+1)}(\xi)}{(n+1)!}\omega(x_0). \qquad \square$$

Для фиксированного отрезка $[a,b]$ и для фиксированной степени n оценка, даваемая теоремой 16.1, оптимальна в том случае, когда $\omega(x)$ — многочлен степени n со старшим коэффициентом 1, наименее отклоняющийся от нуля на отрезке $[a,b]$. Например, если $[a,b] = [-1,1]$, то $\omega(x) = \frac{1}{2^n}T_{n+1}(x)$, где $T_{n+1}(x)$ — многочлен Чебышева. Напомним, что $T_{n+1}(x) = \cos\bigl((n+1)\arccos x\bigr)$ при $x \leqslant 1$. Корни многочлена T_{n+1} имеют вид

$$x_k = \cos\frac{(2k-1)\pi}{2(n+1)}, \quad k = 1, \ldots, n+1.$$

Для таких узлов интерполяционный многочлен имеет вид

$$P(x) = \frac{1}{n+1}\sum_{k=1}^{n+1} f(x_k)(-1)^{k-1}\sqrt{1-x_k^2}\,\frac{T_{n+1}(x)}{x-x_k}.$$

Действительно, если $\omega(x) = \frac{1}{2^n}T_{n+1}(x)$, то

$$\frac{\omega(x)}{(x-x_k)\omega'(x)} = \frac{T_{n+1}(x)}{(x-x_k)T'_{n+1}(x)},$$

поэтому требуется доказать, что

$$T'_{n+1}(x_k) = \frac{(n+1)(-1)^{k-1}}{\sqrt{1-x_k^2}}.$$

Учитывая, что $T_{n+1}(x) = \cos(n+1)\varphi$, где $x = \cos\varphi$, получаем

$$T'_{n+1}(x_k) = \frac{(n+1)\sin(n+1)\varphi}{\sin\varphi}.$$

Если $\cos\varphi = x_k$, то $\sin\varphi = \sqrt{1-x_k^2}$ и $\sin(n+1)\varphi = (-1)^{k-1}$.

Помимо чебышевских узлов интерполяции часто используются узлы, равномерно распределенные на отрезке или на окружности. Для узлов

$$x_k = \exp\left(\frac{2\pi i k}{n+1}\right), \quad k = 1, \ldots, n+1$$

интерполяционный многочлен имеет вид

$$P(x) = \frac{1}{n+1}\sum_{k=1}^{n+1} x_k f(x_k)\frac{x^n-1}{x-x_k}.$$

Для доказательства этой формулы достаточно заметить, что

$$\frac{d}{dx}(x^{n+1}-1)\bigg|_{x=x_k} = (n+1)x_k^n = (n+1)x_k^{-1}.$$

Интерполяционный многочлен для узлов $x_k = a + (k-1)h$, $k = 1, \ldots, n+1$, можно записать в виде

$$P(x) = f(a) + \frac{\Delta f(a)}{h}(x-a) + \frac{\Delta^2 f(a)}{h^2}\frac{(x-a)(x-a-h)}{2!} + \ldots$$
$$\ldots + \frac{\Delta^n f(a)}{h^n}\frac{(x-a)(x-a-h)\cdot\ldots\cdot\big(x-a-(n-1)h\big)}{n!},$$

где $\Delta f(x) = f(x+h) - f(x)$, $\Delta^{k+1} f(x) = \Delta\big(\Delta^k f(x)\big) = \sum\limits_{j=0}^{k}(-1)^{k-j}\binom{k}{j} f(x+jh)$.

Многочлен $P(x)$ называют при этом *интерполяционным многочленом Ньютона*. Легко проверить, что $P(x_k) = f(x_k)$. Действительно, $P(a) = f(a)$, $P(a+h) = f(a) + \Delta f(a)$, $P(a+2h) = f(a) + 2\Delta f(a) + \Delta^2 f(a)$, $\ldots$, $P(a+mh) = \sum\limits_{j=0}^{m}\binom{m}{j}\Delta^j f(a) = f(a+mh)$. Последнее равенство следует из того, что $\Delta^k f(x+h) = \Delta^{k+1} f(x) + \Delta^k f(x)$.

16.2. Интерполяционный многочлен Эрмита

Пусть $x_1, \ldots, x_n$ — попарно различные точки комплексной плоскости $\mathbb{C}$, $\alpha_1, \ldots, \alpha_n$ — натуральные числа, сумма которых равна $m+1$. Предположим, что в каждой точке x_i заданы числа $y_i^{(0)}, y_i^{(1)}, \ldots, y_i^{(\alpha_i-1)}$. Тогда существует единственный многочлен $H_m(x)$ степени не выше m, для которого выполняются равенства

$$H_m(x_i) = y_i^{(0)}, H_m'(x_i) = y_i^{(1)}, \ldots, H_m^{(\alpha_i-1)}(x_i) = y_i^{(\alpha_i-1)},$$

$i = 1, \ldots, n$. Иными словами, в точке x_i многочлен H_m имеет заданные значения производных до порядка $\alpha_i - 1$ включительно. Такой многочлен H_m называют *интерполяционным многочленом Эрмита.*

Единственность интерполяционного многочлена Эрмита достаточно очевидна. Действительно, если $G(x)$ — разность двух интерполяционных многочленов Эрмита, то $\deg G \leqslant m$ и $G(x)$ делится на $(x-x_1)^{\alpha_1} \cdot \ldots \cdot (x-x_n)^{\alpha_n}$.

Пусть $\Omega(x) = (x-x_1)^{\alpha_1} \cdot \ldots \cdot (x-x_n)^{\alpha_n}$. Чтобы построить интерполяционный многочлен Эрмита, достаточно указать многочлены $\varphi_{ik}(x)$ ($i = 1, \ldots, n$ и $k = 0, 1, \ldots, \alpha_i - 1$), обладающие следующими свойствами:

1) $\deg \varphi_{ik} \leqslant m$;

2) $\varphi_{ik}(x)$ делится на многочлен $\Omega(x)/(x-x_i)^{\alpha_i}$, т. е. $\varphi_{ik}(x)$ делится на $(x-x_j)^{\alpha_j}$ при $j \neq i$;

3) разложение $\varphi_{ik}(x)$ по степеням $(x-x_i)$ начинается с $\frac{1}{k!}(x-x_i)^k + (x-x_i)^{\alpha_i}$.

Действительно, $\varphi_{ik}^{(0)}(x_j) = \ldots = \varphi_{ik}^{(\alpha_i-1)}(x_j) = 0$ при $j \neq i$, $\varphi_{ik}^{(k)}(x_i) = 1$ и $\varphi_{ik}^{(l)}(x_i) = 0$ при $0 \leqslant l \leqslant \alpha_i - 1$, $l \neq k$. Поэтому можно положить

$$H_m(x) = \sum_{i=1}^{n} \sum_{k=0}^{\alpha_i-1} y_i^{(k)} \varphi_{ik}(x).$$

Функция $\frac{1}{k!} \frac{(x-x_i)^{\alpha_i}}{\Omega(x)}$ регулярна в точке x_i, поэтому в окрестности точки x_i ее можно разложить в ряд Тэйлора:

$$\frac{1}{k!} \frac{(x-x_i)^{\alpha_i}}{\Omega(x)} = \sum_{s=0}^{\infty} a_{iks}(x-x_i)^s = l_{ik}(x) + \sum_{s=\alpha_i-k}^{\infty} a_{iks}(x-x_i)^s.$$

Здесь $l_{ik}(x)$ — многочлен степени не выше $\alpha_i - k - 1$, являющийся начальной частью ряда Тэйлора. Несложно проверить, что многочлен

$$\varphi_{ik}(x) = \frac{\Omega}{(x-x_i)^{\alpha_i}}\left(l_{ik}(x)(x-x_i)^k\right)$$

обладает всеми требуемыми свойствами. Свойства 1 и 2 очевидны, а свойство 3 доказывается следующим образом:

$$\varphi_{ik}(x) = \frac{l_{ik}(x)(x-x_i)^k}{k!l_{ik}(x) + a(x-x_i)^{\alpha_i-k} + \ldots} = \frac{(x-x_i)^k}{k!}\left(1 + b(x-x_i)^{\alpha_i-k} + \ldots\right).$$

Записывая в явном виде начальный участок ряда Тэйлора $l_{ik}(x)$, получаем

$$H_m(x) = \sum_{i=1}^{n}\sum_{k=0}^{\alpha_i-1}\sum_{s=0}^{\alpha_i-k-1} y_i^{(k)}\frac{1}{k!}\frac{1}{s!}\left(\frac{(x-x_i)^{\alpha_i}}{\Omega(x)}\right)^{(s)}_{x=x_i}\frac{\Omega(x)}{(x-x_i)^{\alpha_i-k-s}}.$$

16.3. Многочлен с предписанными значениями в нулях производной

В 1956 г. в заметке [Anr] было анонсировано утверждение, что для любых n комплексных чисел $a_1, \ldots, a_n$ существует многочлен степени $n+1$ со старшим коэффициентом 1, принимающий значения $a_1, \ldots, a_n$ в нулях своей производной. Но доказано это утверждение было лишь через 9 лет Рене Томом [Th]. Мы приведем доказательство, предложенное Яном Мысильским [My].

Теорема 16.2. Для любых заданных чисел $a_1, \ldots, a_n \in \mathbb{C}$ существуют такие числа $b_1, \ldots, b_n \in \mathbb{C}$ и такой многочлен $P(x) = x^{n+1} + p_1x^n + \ldots + p_nx$, что $P(b_i) = a_i$ и $P'(b_i) = 0$ для $i = 1, \ldots, n$, причем если в последовательности $b_1, \ldots, b_n$ число β встречается k раз, то $P(x) - P(\beta)$ делится на $(x-\beta)^{k+1}$.

Доказательство. Для $b = (b_1, \ldots, b_n) \in \mathbb{C}^n$ положим

$$P_b(x) = (n+1)\int_0^x \prod_{i=1}^{n}(t-b_i)dt.$$

Ясно, что $P_b(0) = 0$ и $P_b(x)$ — многочлен степени $n+1$ со старшим коэффициентом 1. Кроме того,

$$P_b'(x) = (n+1)(x-b_1)\cdot\ldots\cdot(x-b_n),$$

поэтому $P_b'(b_i) = 0$. Если число β встречается k раз в последовательности $b_1,\ldots,b_n$, то $P_b'(\beta) = \ldots = P_b^{(k)}(\beta) = 0$. Отметим, что любое число β является корнем многочлена $P_b(x) - P_b(\beta)$ и $\big(P_b(x) - P_b(\beta)\big)' = P_b'(x)$. Поэтому $P_b(x) - P_b(\beta)$ делится на $(x-\beta)^{k+1}$.

Остается доказать, что отображение $\varphi : \mathbb{C}^n \to \mathbb{C}^n$, заданное формулой $\varphi(b) = \big(P_b(b_1),\ldots,P_b(b_n)\big)$, сюръективно. Прежде всего покажем, что φ — локальный гомеоморфизм в любой точке $b = (b_1,\ldots,b_n)$, для которой $b_i \neq b_j$ при $i \neq j$ и $b_1\cdot\ldots\cdot b_n \neq 0$. Для этого достаточно проверить, что $\det\left(\dfrac{\partial P_b(b_i)}{\partial b_j}\right) \neq 0$. Предположим, что $\det\left(\dfrac{\partial P_b(b_i)}{\partial b_j}\right) = 0$. Тогда существуют такие числа $c_1,\ldots,c_n$, не все равные нулю, что

$$\sum_{j=1}^{n} c_j \frac{\partial P_b(b_i)}{\partial b_j} = 0 \quad \text{при} \quad i = 1,\ldots,n. \tag{1}$$

Легко проверить, что

$$\frac{\partial P_b(b_i)}{\partial b_j} = -(n+1)\int_0^{b_i} \prod_{s\neq j}(t-b_s)\,dt$$

(при $i = j$ появляется еще дополнительное слагаемое $(n+1)\prod\limits_{s=1}^{n}(b_i - b_s)$, но оно равно нулю). Поэтому равенство (1) можно записать в виде

$$F(x) = \int_0^x \sum_{j=1}^{n} c_j \prod_{s\neq j}(t-b_s)\,dt = 0 \quad \text{при} \quad x = b_1,\ldots,b_n.$$

Подынтегральное выражение представляет собой многочлен от t степени не выше n, принимающий значение $c_j\prod\limits_{s\neq j}(t-b_s)$ при $t = b_j$. По условию $\prod\limits_{s\neq j}(t-b_s) \neq 0$ и $c_j \neq 0$ для некоторого j. Следовательно, $F(x)$ — ненулевой многочлен степени не выше $n+1$. С другой стороны, $F(x) = 0$ при $x = 0, b_1,\ldots,b_n$. Получено противоречие.

Отображение $\varphi : \mathbb{C}^n \to \mathbb{C}^n$ индуцирует отображение $\widetilde{\varphi} : \mathbb{C}P^n \to \mathbb{C}P^n$, заданное формулой

$$\widetilde{\varphi}\big((b_0 : \ldots : b_n)\big) = \big(b_0^{n+1} : P_b(b_1) : \ldots : P_b(b_n)\big).$$

Дело в том, что $\varphi(\lambda b) = \lambda^{n+1}\varphi(b)$ и $\varphi^{-1}(0) = 0$. Первое свойство доказывается с помощью замены переменных $\tau = \lambda t$:

$$\int_0^b \prod_{i=1}^n (t - b_i)\,dt = \int_0^{\lambda b} \prod_{i=1}^n (\lambda^{-1}\tau - b_i)\lambda^{-1}\,d\tau = \lambda^{-n-1} \int_0^{\lambda b} \prod_{i=1}^n (\tau - \lambda b_i)\,d\tau.$$

Второе свойство доказывается следующим образом. Пусть $\varphi(b_1, \ldots, b_n) = (0, \ldots, 0)$. Предположим, что последовательность $b_1, \ldots, b_n$ состоит из k_1 чисел $\beta_1, \ldots, k_m$ чисел β_m ($\beta_i \neq \beta_j$ при $i \neq j$). Тогда многочлен $P_b(x) = P_b(x) - P_b(\beta_i)$ имеет степень $n = k_1 + \ldots + k_m$ и делится на x и на $(x - \beta_1)^{k_1+1} \cdot \ldots \cdot (x - \beta_m)^{k_m+1}$. Это возможно лишь в том случае, когда $b_1 = \ldots = b_n = 0$.

Пусть Δ — множество точек $(b_0 : b_1 : \ldots : b_n) \in \mathbb{C}P^n$, координаты которых удовлетворяют одному из следующих уравнений:

$$b_i = 0 \quad (i = 0, \ldots, n); \qquad b_i = b_j \quad (1 \leqslant i < j \leqslant n).$$

Ограничение отображения $\widetilde{\varphi}$ на $\mathbb{C}P^n \setminus \Delta$ является локальным гомеоморфизмом. Кроме того, $\widetilde{\varphi}(\Delta) \subset \Delta$. Действительно, если $b_0 = 0$, то

$$\widetilde{\varphi}\big((b_0 : b_1 : \ldots : b_n)\big) = \big(0 : P_b(b_1) : \ldots\big);$$

если $b_i = 0$ при $i \geqslant 1$, то $P_b(b_i) = 0$, а если $b_i = b_j$ при $1 \leqslant i < j \leqslant n$, то $P_b(b_i) = P_b(b_j)$.

Образ $\mathbb{C}P^n$ при отображении $\widetilde{\varphi}$ — компактное множество; в частности, оно замкнуто. Образ $\mathbb{C}P^n \setminus \Delta$ при отображении $\widetilde{\varphi}$ — открытое множество, граница которого принадлежит $\widetilde{\varphi}(\Delta) \subset \Delta$. Множество Δ не разбивает $\mathbb{C}P^n$, поскольку оно имеет вещественную коразмерность 2. Следовательно, $\widetilde{\varphi}(\mathbb{C}P^n \setminus \Delta) \supset \mathbb{C}P^n \setminus \Delta$ и замыкание множества $\widetilde{\varphi}(\mathbb{C}P^n \setminus \Delta)$ совпадает с $\mathbb{C}P^n$. □

Замечание. Неверно, что $\widetilde{\varphi}(\mathbb{C}P^n \setminus \Delta) \subset \mathbb{C}P^n \setminus \Delta$. Например, $\varphi(1, 2, 3) = (-9, -8, -9)$.

17. Высота многочлена и другие нормы

17.1. Лемма Гаусса

Пусть K — поле, $x \mapsto |x|_v \in \mathbb{R}$ — некоторая функция на K. Эту функцию называют *абсолютным значением,* если выполняются следующие условия:

(1) $|x|_v \geqslant 0$, причем $|x|_v = 0 \Leftrightarrow x = 0$;

(2) $|xy|_v = |x|_v|y|_v$;

(3) $|x+y|_v \leqslant |x|_v + |y|_v$.

Если же вместо условия (3) выполняется более сильное условие $|x+y|_v \leqslant \max\{|x|_v, |y|_v\}$, то абсолютное значение называют *неархимедовым.*

Для поля рациональных чисел $\mathbb{Q}$ имеется естественное абсолютное значение $|x|_v = |x|$ — модуль (абсолютная величина) числа x. Но есть еще и так называемые *p-адические абсолютные значения*, которые определяются для каждого простого числа p следующим образом. Запишем рациональное число x в виде $x = p^r m/n$, где m и n — целые числа, не делящиеся на p. Положим $|x|_p = p^{-r}$. Легко проверить, что это абсолютное значение неархимедово. В самом деле, пусть $x = p^r m_1/n_1$ и $y = p^s m_2/n_2$, причем $r \leqslant s$. Тогда $\max\{|x|_p, |y|_p\} = p^{-r}$ и

$$x + y = p^r \frac{m_1 n_2 + p^{s-r} m_2 n_1}{n_1 n_2}.$$

Поэтому $|x+y|_p \leqslant p^{-r}$ (строгое неравенство возможно лишь в том случае, когда $s = r$).

Высотой многочлена $f(x) = \sum a_i x^i$ относительно данного абсолютного значения $|\cdot|_v$ называют величину $H(f) = \max\limits_i |a_i|_v$. Нас будут интересовать оценки высоты произведения многочленов через высоты множителей. Наиболее простая оценка получается в том случае, когда абсолютное значение неархимедово.

Лемма (Гаусс). Пусть $H(f)$ — высота многочлена f относительно неархимедова абсолютного значения $|\cdot|$. Тогда $H(fg) = H(f)H(g)$.

Доказательство. Пусть $f(x) = a_n x^n + \ldots + a_0$ и $g(x) = b_m x^m + \ldots + b_0$. Рассмотрим те из коэффициентов $a_n, \ldots, a_0$, для которых абсолютное значение максимально (их может быть несколько), а затем выберем среди них коэффициент a_r с наибольшим номером r. Аналогично выберем максимальный коэффициент b_s с наибольшим номером s.

Ясно, что $fg(x) = c_{n+m}x^{n+m} + \ldots + c_0$, где $c_k = \sum\limits_{i+j=k} a_i b_j$. Учитывая, что $|\cdot|$ — неархимедово абсолютное значение, получаем

$$|c_k| \leqslant \max_{i+j=k} \{|a_i| \cdot |b_j|\}.$$

Поэтому

$$\begin{gathered} |c_k| < |a_r| \cdot |b_s| \quad \text{при} \quad k > r+s, \\ c_{r+s} = a_r b_s (1+\alpha), \quad \text{где} \quad |\alpha| < 1, \\ |c_k| \leqslant |a_r| \cdot |b_s| \quad \text{при} \quad k < r+s \end{gathered}$$

Для неархимедова абсолютного значения из условия $|\alpha| < 1$ следует, что $|1+\alpha| = 1$. В самом деле, $|1+\alpha| \leqslant \max\{1, |\alpha|\} = 1$ и $1 = |1+\alpha-\alpha| \leqslant \leqslant \max\{|1+\alpha|, |\alpha|\}$, поэтому $1 \leqslant |1+\alpha|$.

Таким образом, $|c_{r+s}| = |a_r| \cdot |b_s|$, а абсолютные величины всех остальных коэффициентов c_k не превосходят $|a_r| \cdot |b_s|$. Поэтому $H(fg) = = |c_{r+s}| = |a_r| \cdot |b_s| = H(f)H(g)$. □

Гаусс, разумеется, формулировал и доказывал свою лемму на более простом языке. А именно, он доказывал, что *наибольший общий делитель коэффициентов произведения многочленов f и g равен произведению наибольшего общего делителя коэффициентов многочлена f и наибольшего общего делителя коэффициентов многочлена g.* К такой формулировке можно перейти следующим образом. Для p-адического абсолютного значения $H(f) = p^{-r}$, где r — наибольшая степень числа p, на которую делятся коэффициенты многочлена f. Равенство $H(fg) = = H(f)H(g)$ означает, что если в наибольшие общие делители коэффициентов многочленов f и g простое число p входит в степенях r и s соответственно, то в наибольший общий делитель коэффициентов многочлена fg оно входит в степени $r+s$.

Для многочлена $f(x_1, \ldots, x_n) = \sum a_{i_1 \ldots i_n} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$ от n переменных высота определяется аналогично: $H(f) = \max |a_{i_1 \ldots i_n}|$. Для доказательства леммы Гаусса в случае многочленов от n переменных можно воспользоваться так называемой *подстановкой Кронекера.* Пусть $d = \deg f + \deg g + 1$. Сопоставим многочлену $h(x_1, \ldots, x_n) = = \sum c_{k_1 \ldots k_n} x^{k_1} \cdot \ldots \cdot x^{k_n}$ многочлен

$$\bigl(S_d h\bigr)(y) = h\bigl(y, y^d, \ldots, y^{d^{n-1}}\bigr) = \sum c_{k_1 \ldots k_n} x^{k_1 + d k_2 + d^2 k_3 + \ldots + d^{n-1} k_n}.$$

Если $\deg h < d$, то наборы ненулевых коэффициентов у многочленов h и $S_d h$ одни и те же, поэтому $H(h) = H(S_d h)$. Кроме того, $S_d(fg) = S_d(f)S_d(g)$. Таким образом, лемма Гаусса для многочленов от n переменных следует из леммы Гаусса для одной переменной.

17.2. Многочлены от одной переменной

В случае архимедовых нормирований высота $H(f) = \max|a_i|$ уже не будет обладать свойством $H(fg) = H(f)H(g)$. Но как раз в случае обычного модуля (абсолютной величины) оценка высоты многочлена наиболее интересна. Такие оценки нужны для теории трансцендентных чисел. Оценки высоты многочлена были получены А. О. Гельфондом [Ге1] при решении *седьмой проблемы Гильберта*: «*Если число* $a \neq 0, 1$ *алгебраическое, а число* b *иррациональное алгебраическое, то число* a^b *трансцендентное.*» Впоследствии упрощенное доказательство оценок Гельфонда получил К. Малер [М1], [М2].

Для оценки высоты многочлена $f(x) = a_d(x-\alpha_1)\cdot\ldots\cdot(x-\alpha_d)$ Малер использовал величину

$$M(f) = |a_d| \prod_{i=1}^{d} \max\{1, |\alpha_i|\},$$

которую теперь называют *мерой Малера* многочлена f. Ясно, что $M(fg) = M(f)M(g)$. Поэтому оценка сверху и снизу для $M(f)$ через $H(f)$ дает возможность получить оценку для $H(fg)$ через $H(f)$ и $H(g)$.

Теорема 17.1. Пусть $\deg f = d$. Тогда

$$\frac{M(f)}{\sqrt{d+1}} \leqslant H(f) \leqslant 2^{d-1} M(f).$$

Доказательство. Начнем с более простого неравенства $H(f) \leqslant 2^{d-1}M(f)$. Ясно, что

$$|a_d| \cdot |\alpha_{i_1}\alpha_{i_2}\cdot\ldots\cdot\alpha_{i_k}| \leqslant \prod_{i=1}^{d} \max\{1, |\alpha_i|\} = M(f).$$

Поэтому

$$|a_k| \leqslant \binom{d}{k} M(f). \tag{1}$$

Опираясь на формулу $\binom{d+1}{k} = \binom{d}{k-1} + \binom{d}{k}$, индукцией по d легко доказать, что $\binom{d}{k} \leqslant 2^{d-1}$ при $d \geqslant 1$. Вместе с формулой (1) это доказывает требуемое неравенство.

Доказательство неравенства $M(f) \leqslant \sqrt{d+1}\,H(f)$ опирается на формулу Йенсена.

Лемма (Формула Йенсена). Если функция $f(z)$ голоморфна в круге $|z| \leqslant 1$ и имеет внутри этого круга нули $z_1, \ldots, z_n$ (с учетом кратностей), то

$$\frac{1}{2\pi}\int_0^{2\pi} \ln\bigl|f(e^{i\varphi})\bigr|\,d\varphi = \ln\bigl|f(0)\bigr| - \sum_{k=1}^{n} \ln|z_k|.$$

Доказательство. Рассмотрим вспомогательную функцию

$$f_1(z) = \frac{f(z)}{w_1(z)\cdot\ldots\cdot w_n(z)},$$

где $w_k(z) = \dfrac{z - z_k}{1 - z\overline{z}_k}$. Легко проверить, что w_k конформно отображает единичный круг в самого себя. В самом деле, если $|z| = 1$, то $\bigl|w_k(z)\bigr|^2 = 1$; кроме того, $w_k(z_k) = 0$. У функции f_1 нет нулей внутри единичного круга, потому что нули $z_1, \ldots, z_n$ ее числителя $f(z)$ сокращаются с нулями ее знаменателя $w_1(z)\cdot\ldots\cdot w_n(z)$. Поэтому согласно теореме о среднем для гармонической функции $\ln\bigl|f_1(z)\bigr| = \operatorname{Re}\bigl(\ln f_1(z)\bigr)$ получаем

$$\frac{1}{2\pi}\int_0^{2\pi} \ln\bigl|f_1(e^{i\varphi})\bigr|\,d\varphi = \ln\bigl|f_1(0)\bigr|.$$

Но $\bigl|f_1(e^{i\varphi})\bigr| = \bigl|f(e^{i\varphi})\bigr|$, а $\ln\bigl|f_1(0)\bigr| = \ln\bigl|f(0)\bigr| - \sum\limits_{k=1}^{n} \ln|z_k|$. □

Следствие. Пусть f — многочлен. Тогда

$$M(f) = \exp\int_0^1 \ln\bigl|f(e^{2\pi i t})\bigr|\,dt. \tag{2}$$

Доказательство. Обе части требуемого равенства мультипликативны относительно f. Поэтому достаточно рассмотреть случай $f(x) = x - \alpha$. При $|\alpha| \geqslant 1$ у функции f нет нулей внутри единичного круга, а при $|\alpha| < 1$ внутри единичного круга у нее есть нуль α. Поэтому согласно формуле Йенсена

$$\int_0^1 \ln\bigl|f(e^{2\pi it})\bigr|\,dt = \frac{1}{2\pi}\int_0^{2\pi} \ln\bigl|f(e^{i\varphi})\bigr|\,d\varphi = \\ = \ln\bigl|f(0)\bigr| - \varepsilon \ln|\alpha| = (1-\varepsilon)\ln|\alpha|,$$

где $\varepsilon = 0$ при $|\alpha| \geqslant 1$ и $\varepsilon = 1$ при $|\alpha| < 1$.

С другой стороны, $M(f) = \max\{1, |\alpha|\} = |\alpha|^{1-\varepsilon}$. □

Вооружившись формулой (2), можно приступить к доказательству неравенства $M(f) \leqslant \sqrt{d+1}\,H(f)$. Ясно, что

$$\int_0^1 \Bigl|\sum a_k e^{2k\pi it}\Bigr|^2 dt = \int_0^1 \sum a_k \overline{a}_l e^{2(k-l)\pi it}\,dt = \sum |a_k|^2.$$

Кроме того, из выпуклости функции exp следует, что для любой функции $u(t)$ выполняется неравенство

$$\exp\int_0^1 u(t)\,dt \leqslant \int_0^1 \exp u(t)\,dt.$$

При $u(t) = 2\ln\bigl|f(e^{2\pi it})\bigr|$ получаем

$$M(f) = \exp\int_0^1 \frac{u(t)\,dt}{2} = \left(\exp\int_0^1 u(t)\,dt\right)^{1/2} \leqslant \\ \leqslant \left(\int_0^1 \exp u(t)\,dt\right)^{1/2} = \left(\int_0^1 \bigl|f(e^{2\pi it})\bigr|^2 dt\right)^{1/2} = \\ = \Bigl(\sum |a_k|^2\Bigr)^{1/2} \leqslant \sqrt{d+1}\,\max|a_k| = \sqrt{d+1}\,H(f).$$ □

С помощью теоремы 17.1 можно получить следующие оценки для $H(fg)$ через $H(f)$ и $H(g)$.

Теорема 17.2. Пусть $d_1 = \deg f$ и $d_2 = \deg g$, причем $d_1 \leqslant d_2$. Тогда

$$\left(2^{d_1+d_2-2}\sqrt{d_1+d_2+1}\right)^{-1} H(f)H(g) \leqslant H(fg) \leqslant (1+d_1)H(f)H(g).$$

Доказательство. Неравенство $H(fg) \leqslant (1+d_1)H(f)H(g)$ доказывается непосредственно, без использования формулы Йенсена. Пусть $f(x) = \sum a_i x^i$, $g(x) = \sum b_j x^j$, $fg(x) = \sum c_k x^k$. Тогда

$$|c_k| = |a_0 b_k + a_1 b_{k-1} + \ldots + a_{d_1} b_{k-d_1}| \leqslant$$
$$\leqslant (1+d_1)\max|a_i| \max|b_j| = (1+d_1)H(f)H(g).$$

Для доказательства неравенства

$$H(f)H(g) \leqslant 2^{d_1+d_2-2}\sqrt{d_1+d_2-1}\,H(fg)$$

воспользуемся теоремой 17.1. Согласно этой теореме

$$H(f) \leqslant 2^{d_1-1}M(f), \quad H(g) \leqslant 2^{d_2-1}M(g) \quad \text{и} \quad \sqrt{d_1+d_2+1}\,M(fg) \leqslant H(fg).$$

Остается заметить, что $M(f)M(g) = M(fg)$. □

С помощью меры Малера $M(f)$ можно получить оценки и для *длины* $L(f) = \sum\limits_{k=0}^{d} |a_k|$ многочлена f. В самом деле, с одной стороны, из неравенства (1) на с. 160 следует, что

$$L(f) = \sum_{k=0}^{d} |a_k| \leqslant M(f) \sum_{k=0}^{d} \binom{d}{k} = 2^d M(f). \tag{3}$$

С другой стороны,

$$\left|f(e^{2\pi i t})\right| = \left|\sum a_k e^{2\pi i t}\right| \leqslant \sum |a_k| = L(f).$$

Поэтому

$$M(f) \leqslant \exp \int_0^1 \ln L(f)\,dt = L(f). \tag{4}$$

Комбинируя неравенства (3) и (4), получаем

$$L(f)L(g) \leqslant 2^{d_1} M(f) 2^{d_2} M(g) \leqslant 2^{d_1+d_2} L(fg).$$

Оценка сверху для $L(fg)$ имеет вид

$$L(fg) \leqslant L(f)L(g).$$

Это неравенство следует непосредственно из определения длины многочлена:

$$L(fg) \leqslant \sum_{i,j} |a_i| \cdot |b_j| = \Big(\sum_i |a_i|\Big)\Big(\sum_j |b_j|\Big) = L(f)L(g).$$

17.3. Максимум модуля и неравенство Бернштейна

Первоначально для оценки высоты многочлена Гельфонд использовал величину $\max\limits_{|z|=1}\big|f(z)\big|$. Он доказал следующее утверждение.

Теорема 17.3. Пусть $d_1 = \deg f$, $d_2 = \deg g$ и $d = d_1 + d_2$. Тогда

$$\max_{|z|=1}\big|f(z)\big| \cdot \max_{|z|=1}\big|g(z)\big| < 2^{2d} \max_{|z|=1}\big|fg(z)\big|.$$

Доказательство. Можно считать, что

$$\max_{|z|=1}\big|f(z)\big| = \max_{|z|=1}\big|g(z)\big| = 1.$$

Предположим, что $\max\limits_{|z|=1}\big|fg(z)\big| \leqslant 2^{-2d}$. В таком случае при $k = 0, 1, \ldots, d$ одно из чисел $\big|f(\varepsilon_k)\big|$ и $\big|g(\varepsilon_k)\big|$, где $\varepsilon_k = \exp\left(\dfrac{2\pi i k}{d+1}\right)$, не превосходит 2^{-d}. Поэтому либо неравенство $\big|f(\varepsilon_k)\big| \leqslant 2^{-d}$ выполняется при $d_1 + 1$ значениях индекса k, либо неравенство $\big|g(\varepsilon_k)\big| \leqslant 2^{-d}$ выполняется при $d_2 + 1$ значениях индекса k. Пусть для определенности

$$\{\varepsilon_0, \ldots, \varepsilon_d\} = \{\alpha_0, \ldots, \alpha_{d_1}\} \cup \{\beta_1 \ldots, \beta_{d_2}\}$$

и $\big|f(\alpha_l)\big| \leqslant 2^{-d}$ при $l = 0, 1, \ldots, d_1$.

Согласно интерполяционной формуле Лагранжа

$$f(z) = \sum_{l=0}^{d_1} f(\alpha_l) \frac{(z-\alpha_0)\cdot\ldots\cdot(z-\alpha_{l-1})(z-\alpha_{l+1})\cdot\ldots\cdot(z-\alpha_{d_1})}{(\alpha_l-\alpha_0)\cdot\ldots\cdot(\alpha_l-\alpha_{l-1})(\alpha_l-\alpha_{l+1})\cdot\ldots\cdot(\alpha_l-\alpha_{d_1})}.$$

Умножим числитель и знаменатель l-го слагаемого на $(\alpha_l - \beta_1) \cdot \ldots \cdot \ldots \cdot (\alpha_l - \beta_{d_2})$. В результате знаменатель станет равным

$$\lim_{x\to\alpha_l} \frac{(x-\varepsilon_0)(x-\varepsilon_1)\cdot\ldots\cdot(x-\varepsilon_d)}{x-\alpha_l} = \lim_{x\to\alpha_l} \frac{x^{d+1}-1}{x-\alpha_l}.$$

Так как α_l — корень многочлена $x^{d+1}-1$, последнее выражение равно производной функции $x^{d+1}-1$ в точке α_l, т. е. оно равно $(d+1)\alpha_l^d$.

В случае, когда $|z|=1$, полученный числитель состоит из d сомножителей, модуль каждого из которых не превосходит 2. Поэтому если $|z|=1$, то

$$\big|f(z)\big| \leqslant (d_1+1)2^{-d}\frac{2^d}{d+1} = \frac{d_1+1}{d+1} < 1,$$

что противоречит предположению о том, что $\max\limits_{|z|=1}\big|f(z)\big| = 1$. □

Замечание. Для многочленов с коэффициентами из поля $F=\mathbb{C}$ или $\mathbb{R}$ более точные оценки вида

$$\max_{|z|=1}\big|f_1(z)\big|\cdot\ldots\cdot\max_{|z|=1}\big|f_m(z)\big| \leqslant C_F(m,n)\max_{|z|=1}\big|f(z)\big|,$$

где $f = f_1\cdot\ldots\cdot f_m$, $n=\deg f$, $C_F(m,n)$ — константа, получены в статье [Bo]. А именно, пусть $I(\theta) = \int\limits_0^\theta \ln\big(2\cos(t/2)\big)\,dt$. Тогда

$$C_{\mathbb{C}}(m,n) = \left(\exp\left(\frac{m}{\pi}I\Big(\frac{m}{\pi}\Big)\right)\right)^n$$

и $C_{\mathbb{R}}(m,n) = C_{\mathbb{C}}(2,n)$. Обе оценки точные.

Для нормы $\|f\| = \max\limits_{|z|=1}\big|f(z)\big|$ выполняется также следующее неравенство.

Теорема 17.4 (Бернштейн). Пусть $\deg f = n$. Тогда $\|f'\| \leqslant n\|f\|$.

Доказательство [O]. Нам потребуется следующее вспомогательное утверждение.

Лемма. Пусть $\deg f \leqslant n$ и $z_1,\ldots,z_n$ — корни многочлена z^n+1. Тогда

$$tf'(t) = \frac{n}{2}f(t) + \frac{1}{n}\sum_{k=1}^{n} f(tz_k)\frac{2z_k}{(z_k-1)^2}.$$

ДОКАЗАТЕЛЬСТВО. Положим $g_t(z) = \dfrac{f(tz) - f(t)}{z - 1}$. Легко проверить, что $g_t(1) = tf'(t)$ и g_t — многочлен от z степени не выше $n - 1$. Интерполяционная формула Лагранжа с узлами $z_1, \ldots, z_n$ показывает, что

$$g_t(z) = \sum_{k=1}^{n} g_t(z_k) \frac{z^n + 1}{(z - z_k) n z_k^{n-1}} = \frac{1}{n} \sum_{k=1}^{n} g_t(z_k) \frac{z^n + 1}{z_k - z} z_k$$

(мы воспользовались тем, что $z_k^{n-1} = -1/z_k$).

При $z = 1$ получаем

$$tf'(t) = \frac{1}{n} \sum_{k=1}^{n} g_t(z_k) \frac{2z_k}{(z_k - 1)^2} = \frac{1}{n} \sum_{k=1}^{n} \frac{f(tz_k) - f(t)}{(z_k - 1)^2} =$$
$$= \frac{1}{n} \sum_{k=1}^{n} f(tz_k) \frac{2z_k}{(z_k - 1)^2} - \frac{f(t)}{n} \sum_{k=1}^{n} \frac{2z_k}{(z_k - 1)^2}.$$

Чтобы вычислить сумму $\sum\limits_{k=1}^{n} \dfrac{2z_k}{(z_k - 1)^2}$, положим $f(t) = t^n$. Тогда $f(tz_k) = = -t_n$, поэтому

$$nt^n = -\frac{2t^n}{n} \sum_{k=1}^{n} \frac{2z_k}{(z_k - 1)^2},$$

т. е.

$$\sum_{k=1}^{n} \frac{2z_k}{(z_k - 1)^2} = -\frac{n^2}{2}. \tag{1}$$

□

Пусть $|t| = 1$. Тогда

$$\left|f'(t)\right| \leqslant \left(\frac{n}{2} f(t) + \frac{1}{n} \sum_{k=1}^{n} \left| \frac{2z_k}{(z_k - 1)^2} \right| \right) \|f\|.$$

Покажем, что $2z_k/(z_k - 1)^2$ — вещественное отрицательное число. В самом деле, $z_k = e^{i\varphi} \neq 1$, поэтому

$$\frac{2z_k}{(z_k - 1)^2} = \frac{2e^{i\varphi}}{(e^{i\varphi} - 1)^2} = \frac{2}{e^{i\varphi} - 2 + e^{-i\varphi}} = \frac{1}{\cos\varphi - 1} < 0.$$

В таком случае из равенства (1) следует, что

$$\frac{1}{n} \sum_{k=1}^{n} \left| \frac{2z_k}{(z_k - 1)^2} \right| = -\frac{1}{n} \sum_{k=1}^{n} \frac{2z_k}{(z_k - 1)^2} = \frac{n}{2}.$$

□

17.4. Многочлены от многих переменных

Для многочлена $F(x_1,\dots,x_n)=\sum a_{k_1\dots k_n}x_1^{k_1}\cdot\ldots\cdot x_n^{k_n}$ от n переменных оценку высоты $H(F)=\max|a_{k_1\dots k_n}|$ тоже удобно производить с помощью меры Малера, как это сделано в [M2].

Меру Малера многочлена от одной переменной можно определить двумя эквивалентными способами:

$$M(f)=|a_d|\prod_{i=1}^{d}\max\{1,|\alpha_i|\},$$

$$M(f)=\exp\int_0^1\ln\bigl|f(e^{2\pi it})\bigr|\,dt.$$

Для многочленов от n переменных пригоден лишь второй из этих способов:

$$M(F)=\exp\int_0^1\left(\ldots\int_0^1\ln\bigl|F(e^{2\pi it_1},\dots,e^{2\pi it_n})\bigr|\,dt_1\ldots\right)dt_n.$$

Напомним, что для многочленов от одной переменной на с. 160 было доказано неравенство

$$|a_k|\leqslant\tbinom{d}{k}M(f).$$

С помощью этого неравенства можно доказать следующее неравенство для многочленов от n переменных:

$$|a_{k_1\dots k_n}|\leqslant\tbinom{d_1}{k_1}\cdot\ldots\cdot\tbinom{d_n}{k_n}M(F),\qquad(1)$$

где $d_1,\dots,d_n$ — степени многочлена F по переменным $x_1,\dots,x_n$. В самом деле, запишем многочлен F в виде

$$F(x_1,\dots,x_n)=\sum_{k_1=1}^{d_1}F_{k_1}(x_2,\dots,x_n)x_1^{k_1}.$$

Для фиксированных $x_2=\alpha_2$, …, $x_n=\alpha_n$ получим

$$\bigl|F_{k_1}(\alpha_2,\dots,\alpha_n)\bigr|\leqslant\tbinom{d_1}{k_1}M(g),$$

где $g(x)=F(x,\alpha_2,\dots,\alpha_n)$.

Положим $x = e^{2\pi i t_1}, \alpha_2 = e^{2\pi i t_2}, \ldots, \alpha_n = e^{2\pi i t_n}$, а затем возьмем логарифмы обеих частей полученного равенства:

$$\ln\bigl|F_{k_1}(e^{2\pi i t_2}, \ldots, e^{2\pi i t_n})\bigr| \leqslant \ln \tbinom{d_1}{k_1} + \int_0^1 \ln\bigl|F(e^{2\pi i t_1}, \ldots, e^{2\pi i t_n})\bigr|\, dt_1.$$

Проинтегрируем обе части этого равенства по $t_2, \ldots, t_n$ от 0 до 1, а после этого возьмем экспоненту. В результате получим $M(F_{k_1}) \leqslant \binom{d_1}{k_1} M(F)$.

Запишем теперь многочлен $F_{k_1}(x_2, \ldots, x_n)$ в виде

$$F_{k_1}(x_2, \ldots, x_n) = \sum_{k_2=1}^{d_2} F_{k_1 k_2}(x_3, \ldots, x_n) x_2^{k_2}.$$

Аналогично доказывается, что

$$M(F_{k_1 k_2}) \leqslant \tbinom{d_2}{k_2} M(F_{k_1}) \leqslant \tbinom{d_1}{k_1}\tbinom{d_2}{k_2} M(F)$$

и т. д. Ясно также, что $M(a_{k_1 \ldots k_n}) = a_{k_1 \ldots k_n}$.

Как мы уже говорили, индукцией по d легко доказать, что $\binom{d}{k} \leqslant 2^{d-1}$ при $d \geqslant 1$. Поэтому из неравенства (1) следует, что если $d_1 > 0, \ldots, d_n > 0$, то

$$H(F) \leqslant 2^{d_1 + d_2 + \ldots + d_n - n} M(F). \tag{2}$$

Если же многочлен $F(x_1, \ldots, x_n)$ зависит в действительности лишь от $\nu(F)$ переменных, а остальные $n - \nu(F)$ переменных входят в него в нулевой степени, то вместо (2) получаем более грубую оценку

$$H(F) \leqslant 2^{d_1 + d_2 + \ldots + d_n - \nu(F)} M(F). \tag{3}$$

Противоположная оценка для $H(F)$ доказывается точно так же, как это делалось на с. 162 для многочленов от одной переменной. Эта оценка имеет вид

$$M(F) \leqslant \sqrt{d_1 + 1} \cdot \ldots \cdot \sqrt{d_n + 1}\, H(F). \tag{4}$$

Пусть $F_1, \ldots, F_s$ — многочлены от переменных $x_1, \ldots, x_n$; $d_{l1}, \ldots, d_{ln}$ — степени многочлена $F(l)$ по этим переменным; $\nu(F_l)$ — количество переменных, от которых F_l действительно зависит (т. е. количество индексов j, для которых $d_{lj} > 0$). Тогда согласно формуле (3)

$$\prod_{l=1}^{s} H(F_l) \leqslant \prod_{l=1}^{s} 2^{d_{l1} + d_{l2} + \ldots + d_{ln} - \nu(F_l)} M(F_l) \leqslant 2^{d_1 + d_2 + \ldots + d_n - \nu(F)} M(F).$$

Воспользовавшись теперь формулой (4), получим

$$H(F_1)\cdot\ldots\cdot H(F_s)\leqslant 2^{d_1+d_2+\ldots+d_n-n}\sqrt{d_1+1}\cdot\ldots\cdot\sqrt{d_n+1}\,H(F);$$

при этом имеется в виду, что $\nu(F)=n$, т. е. многочлен F действительно зависит от всех переменных $x_1,\ldots,x_n$.

Противоположная оценка

$$H(F)\leqslant 2^{d_1+d_2+\ldots+d_n}H(F_1)\cdot\ldots\cdot H(F_s)$$

доказывается без использования меры Малера. Дело в том, что у многочлена F_l количество ненулевых коэффициентов не превосходит

$$(1+d_{l1})\cdot\ldots\cdot(1+d_{ln})\leqslant 2^{d_{l1}+d_{l2}+\ldots+d_{ln}}.$$

Поэтому любой коэффициент многочлена F представляет собой сумму не более чем $2^{d_1+d_2+\ldots+d_n}$ произведений коэффициентов многочленов $F_1,\ldots,F_s$.

С помощью меры Малера можно получить и оценки для так называемой *длины* многочлена

$$L(F)=\sum|a_{k_1\ldots k_n}|.$$

Просуммировав неравенства (1), получим

$$L(F)\leqslant 2^{d_1+d_2+\ldots+d_n}M(F). \tag{5}$$

Для многочлена $F(x_1,\ldots,x_n)=(1+x_1)^{d_1}\cdot\ldots\cdot(1+x_n)^{d_n}$ неравенство (5) превращается в равенство.

Противоположная оценка для $L(F)$ получается просто: из очевидного неравенства

$$\left|F(e^{2\pi it_1},\ldots,e^{2\pi it_n})\right|\leqslant L(F)$$

следует, что

$$M(F)\leqslant L(F). \tag{6}$$

Для многочлена $F(x_1,\ldots,x_n)=x_1^{d_1}\cdot\ldots\cdot x_n^{d_n}$ неравенство (6) превращается в равенство.

Из неравенства (5) следует, что

$$\prod_{l=1}^{s}L(F_l)\leqslant\prod_{l=1}^{s}\left(2^{d_{l1}+d_{l2}+\ldots+d_{ln}}M(F_l)\right)=2^{d_1+d_2+\ldots+d_n}M(F).$$

Учитывая неравенство (6), получаем

$$L(F_1)\cdot\ldots\cdot L(F_s)\leqslant 2^{d_1+d_2+\ldots+d_n}L(F_1\cdot\ldots\cdot F_s).$$

Противоположная оценка

$$L(F_1\cdot\ldots\cdot F_s)\leqslant L(F_1)\cdot\ldots\cdot L(F_s)$$

очевидна.

17.5. Неравенство для пары взаимно простых многочленов

Пусть $f(x)$ и $g(x)$ взаимно простые многочлены над $\mathbb{C}$. Тогда

$$m(x)=\max\bigl\{|f(x)|,|g(x)|\bigr\}>0$$

и $m(x)\to\infty$ при $x\to\infty$. Поэтому величина

$$E(f,g)=\min_x m(x)$$

положительна. В теории трансцендентных чисел бывают нужны оценки снизу для $E(f,g)$. Способ, позволяющий получить точную оценку, предложил Н. И. Фельдман. Мы изложим этот способ, следуя статье Малера [М3].

Теорема 17.5. Пусть $\alpha_1,\ldots,\alpha_m$ — корни многочлена f, $\beta_1,\ldots,\beta_n$ — корни многочлена g. Тогда

$$E(f,g)\geqslant\min_{i,j}\left(2^{-m}|f(\beta_i)|,\,2^{-n}|g(\alpha_j)|\right). \tag{1}$$

Доказательство. Фиксируем произвольное число $x\in\mathbb{C}$ и рассмотрим $\alpha=\min\limits_j|x-\alpha_j|$ и $\beta=\min\limits_i|x-\beta_i|$. При этом $\alpha=|x-\alpha_k|$ и $\beta=|x-\beta_l|$ для некоторых k и l. Из взаимной простоты многочленов f и g следует, что одно из чисел α и β положительно.

Можно считать, что $\alpha\leqslant\beta$. Рассмотрим сначала случай, когда $\alpha>0$. Покажем, что в этом случае для любого i выполняется неравенство

$$|x-\beta_i|\geqslant\frac{|\alpha_k-\beta_i|}{2}. \tag{2}$$

В самом деле, если $|\alpha_k - \beta_i| < 2\alpha$, то

$$|x - \beta_i| \geqslant \beta \geqslant \alpha > \frac{|\alpha_k - \beta_i|}{2}.$$

А если $|\alpha_k - \beta_i| \geqslant 2\alpha = 2|x - \alpha_k|$, то

$$|x - \beta_i| = \big|(x - \alpha_k) + (\alpha_k - \beta_i)\big| \geqslant |x - \alpha_k| + |\alpha_k - \beta_i| \geqslant \frac{|\alpha_k - \beta_i|}{2}.$$

Пусть $g(x) = b_0(x - \beta_1) \cdot \ldots \cdot (x - \beta_n)$. Из неравенства (2) следует, что

$$\big|g(x)\big| = \big|b_0(x - \beta_1) \cdot \ldots \cdot (x - \beta_n)\big| \geqslant 2^{-n}\left|b_0 \prod_{i=1}^{n}(\alpha_k - \beta_i)\right| = 2^{-n}\big|g(\alpha_k)\big|.$$

В случае, когда $\alpha = 0$, т.е. $x = \alpha_k$, неравенство $\big|g(x)\big| \geqslant 2^{-n}\big|g(\alpha_k)\big|$ выполняется очевидным образом.

Итак, если $\alpha \leqslant \beta$, то $\big|g(x)\big| \geqslant 2^{-n}\big|g(\alpha_k)\big|$. Аналогично доказывается, что если $\alpha \geqslant \beta$, то $\big|f(x)\big| \geqslant 2^{-m}\big|f(\beta_l)\big|$. Поэтому в любом случае

$$m(x) \geqslant \min_{l,k}\big\{2^{-m}\big|f(\beta_l)\big|,\, 2^{-n}\big|g(\alpha_k)\big|\big\}. \qquad \square$$

Замечание. Если $f(x) = (x - 1)^m$ и $g(x) = (x + 1)^n$, то неравенство (1) превращается в равенство. Таким образом, оценка (1) точная.

17.6. Неравенство Миньотта

В этой главе мы уже много занимались неравенствами, позволяющими оценить коэффициенты множителей данного многочлена. Оценку такого рода дает также следующая теорема, доказанная Миньоттом [Mi].

Теорема 17.6. Пусть $f(x) = a_0 + a_1x + \ldots + a_mx^m$ и $g(x) = b_0 + b_1x + \ldots + b_nx^n$ — многочлены с целочисленными коэффициентами. Тогда если f делится нацело на g, то

$$|b_j| \leqslant \binom{n-1}{j}\|f\| + \binom{n-1}{j-1}|a_m|,$$

где $\|f\| = \sqrt{a_0^2 + \ldots + a_m^2}$.

Доказательство. Рассмотрим наряду с многочленом $f(x) = a_m \prod(x - \alpha_i)$ и многочлен

$$\widehat{f}(x) = a_m \prod_{|\alpha_i| \geqslant 1} (x - \alpha_i) \prod_{|\alpha_i| < 1} (\overline{\alpha}_i x - 1).$$

Докажем сначала, что $\|\widehat{f}\| = \|f\|$, где $\|\widehat{f}\|$ — корень из суммы квадратов модулей коэффициентов многочлена $\widehat{f}(x)$.

Для этого достаточно доказать следующее утверждение.

Лемма 17.1. Пусть $h(x) = c_0 + c_1 x + \ldots + c_k x^k$, $h_1(x) = (x - \alpha)h(x)$ и $h_2(x) = (\overline{\alpha}x - 1)h(x)$. Тогда $\|h_1\| = \|h_2\|$.

Доказательство. Ясно, что

$$\begin{aligned}
\|h_1\|^2 &= \sum |c_{i-1} - \alpha c_i|^2 = \\
&= \sum \left(|c_{i-1}|^2 + |\alpha c_i|^2 - 2\,\mathrm{Re}(\alpha c_1 \overline{c_{i-1}})\right) = \\
&= \sum \left(|\alpha c_{i-1}|^2 + |c_i|^2 - 2\,\mathrm{Re}(\alpha c_1 \overline{c_{i-1}})\right) = \\
&= \sum |\alpha c_{i-1} - c_i|^2 = \|h_2\|^2.
\end{aligned}$$

□

У многочлена $\widehat{f}$ коэффициент при старшем члене x^m равен $a_m \prod\limits_{|\alpha_i|<1} \overline{\alpha}_i$, а коэффициент при младшем члене равен $\pm a_m \prod\limits_{|\alpha_i|>1} \overline{\alpha}_i$ (произведение, в которое не входит ни одного множителя, считается равным 1). Положим

$$M(f) = \prod_{|\alpha_i|>1} \alpha_i, \quad m(f) = \prod_{|\alpha_i|<1} \alpha_i.$$

Тогда $\|\widehat{f}(x)\|^2 = \|f(x)\|^2 \geqslant |a_m|^2 \left(M(f)^2 + m(f)^2\right)$. Следовательно,

$$M(f) \leqslant \|f(x)\|/|a_m|. \tag{1}$$

Кроме того,

$$|a_j| = |a_m| \cdot \left|\sum \alpha_{i_1} \cdot \ldots \cdot \alpha_{i_{m-j}}\right| \leqslant |a_m| \sum \beta_{i_1} \cdot \ldots \cdot \beta_{i_{m-j}}, \tag{2}$$

где $\beta_i = \max\{1, |\alpha_i|\}$. Ясно, что $\prod \beta_i = M(f)$.

Теперь нам потребуется еще одно вспомогательное утверждение.

Лемма 17.2. Пусть $x_1 \geqslant 1, \ldots, x_m \geqslant 1$ и $x_1 \cdot \ldots \cdot x_m = M$. Тогда

$$\sum_{i_1 < \ldots < i_k} x_{i_1} \cdot \ldots \cdot x_{i_k} \leqslant \binom{m-1}{k-1} M + \binom{m-1}{k}.$$

Доказательство. Можно считать, что $x_1 \leqslant x_2 \leqslant \ldots \leqslant x_m$. Заменим пару $\{x_{m-1}, x_m\}$ на $\{1, x_{m-1}x_m\}$. При этом рассматриваемая сумма увеличится на $\sigma(x_{m-1} - 1)(x_m - 1)$, где σ — сумма произведений $x_{i_1} \cdot \ldots \cdot x_{i_{k-1}}$, $1 \leqslant i_1 < \ldots < i_{k-1} \leqslant m-2$. Таким образом, если $x_{m-1} > 1$, то рассматриваемая сумма строго увеличивается. Поэтому она будет минимальна в том случае, когда $x_1 = \ldots = x_{m-1} = 1$, $x_m = M$. В этом случае сумма состоит из $\binom{m-1}{k-1}$ членов, равных M, и $\binom{m-1}{k}$ членов, равных 1. □

Применив лемму 17.2 к набору $\beta_1, \ldots, \beta_m$, получим

$$\sum \beta_{i_1} \cdot \ldots \cdot \beta_{i_{m-j}} \leqslant \binom{m-1}{m-j-1} M(f) + \binom{m-1}{m-j}.$$

Если теперь учесть, что $\binom{m-1}{m-j-1} = \binom{m-1}{j}$ и $\binom{m-1}{m-j} = \binom{m-1}{j-1}$, то неравенство (2) можно будет записать в виде

$$|a_j| \leqslant |a_m| \left(\binom{m-1}{j} M(f) + \binom{m-1}{j-1} \right).$$

Аналогично доказывается, что

$$|b_j| \leqslant |b_n| \left(\binom{n-1}{j} M(g) + \binom{n-1}{j-1} \right). \tag{3}$$

Все корни многочлена g являются корнями многочлена f, поэтому $M(g) \leqslant M(f)$. Кроме того, $|b_n| \leqslant |a_m|$, так как по условию многочлен g делит многочлен f. Учитывая эти неравенства и неравенство (1), неравенство (3) можно привести к требуемому виду

$$|b_j| \leqslant \binom{n-1}{j} \|f\| + \binom{n-1}{j-1} |a_m|. \qquad \square$$

Следствие. Если f, g и f/g — многочлены с целыми коэффициентами, то

$$\|g\| \leqslant \binom{2n}{n}^{1/2} \|f\|, \quad \text{где} \quad n = \deg g.$$

Доказательство. Ясно, что $|a_n| \leqslant \|f\|$, поэтому

$$|b_j| \leqslant \left(\binom{n-1}{j} + \binom{n-1}{j-1}\right)\|f\| = \binom{n}{j}\|f\|.$$

Следовательно, $\|g\|^2 \leqslant \sum\limits_{j=0}^{n} \binom{n}{j}^2 \|f\|^2$. Остается проверить комбинаторное тождество $\sum\limits_{j=0}^{n} \binom{n}{j}^2 = \binom{2n}{n}$. Для этого достаточно сравнить коэффициенты при t^n в обеих частях равенства $(1+t)^n(1+t)^n = (1+t)^{2n}$. □

18. Уравнения для многочленов

18.1. Диофантовы уравнения для многочленов

18.1.1. Теорема Мэйсона и ее следствия

При доказательстве неразрешимости многих диофантовых уравнений для многочленов весьма эффективным оказывается следующее утверждение.

Теорема 18.1 (Mason). Пусть $a(x)$, $b(x)$ и $c(x)$ — попарно взаимно простые многочлены, связанные соотношением $a+b+c=0$. Тогда степень каждого из этих многочленов не превосходит $n_0(abc)-1$, где n_0 — количество различных корней многочлена.

Доказательство [La]. Положим $f = a/c$ и $g = b/c$. Тогда f и g — рациональные функции, связанные соотношением $f+g+1=0$. Продифференцировав это равенство, получим $f' = -g'$. Поэтому

$$\frac{b}{a} = \frac{g}{f} = -\frac{f'/f}{g'/g}.$$

Рациональные функции f и g имеют специальный вид $\prod(x-\rho_i)^{r_i}$, $r_i \in \mathbb{Z}$. Для функции $R(x) = \prod(x-\rho_i)^{r_i}$ выполняется равенство

$$\frac{R'}{R} = \sum \frac{r_i}{x-\rho_i}.$$

Пусть $a(x) = \prod(x-\alpha_i)^{a_i}$, $b(x) = \prod(x-\beta_j)^{b_j}$, $c(x) = \prod(x-\gamma_k)^{c_k}$.

Тогда

$$f'/f = \sum \frac{a_i}{x-\alpha_i} - \sum \frac{c_k}{x-\gamma_k},$$

$$g'/g = \sum \frac{b_j}{x-\beta_j} - \sum \frac{c_k}{x-\gamma_k}.$$

Поэтому после умножения на многочлен

$$N_0 = \prod (x-\alpha_i)(x-\beta_j)(x-\gamma_k)$$

степени $n_0(abc)$ рациональные функции f'/f и g'/g становятся многочленами степени не выше $n_0(abc)-1$. Таким образом, из взаимной простоты многочленов $a(x)$ и $b(x)$ и из равенства

$$\frac{b}{a} = -\frac{N_0 f/f'}{N_0 g/g'}$$

следует, что степень каждого из многочленов $a(x)$ и $b(x)$ не превосходит $n_0(abc)-1$. Для многочлена $c(x)$ доказательство аналогично. □

Из теоремы 18.1 можно извлечь интересные следствия, которые мы сформулируем как теоремы 18.2–18.4.

Теорема 18.2 (Дэвенпорт). Пусть f и g — взаимно простые многочлены ненулевой степени. Тогда

$$\deg(f^3 - g^2) \geqslant \frac{1}{2}\deg f + 1.$$

Доказательство. Если $\deg f^3 \neq \deg g^2$, то

$$\deg(f^3 - g^2) \geqslant \deg f^3 = 3\deg f \geqslant \frac{1}{2}\deg f + 1.$$

Поэтому можно считать, что $\deg f^3 = \deg g^2 = 6k$.

Рассмотрим многочлены $F = f^3$, $G = g^2$ и $H = F - G = f^3 - g^2$. Ясно, что $\deg H \leqslant 6k$. Согласно теореме 18.1

$$\max\{\deg F, \deg G, \deg H\} \leqslant n_0(FGH) - 1 \leqslant \deg f + \deg g + \deg H - 1,$$

т. е.

$$6k \leqslant 2k + 3k + \deg H - 1.$$

Таким образом, $\deg H \geqslant k + 1 = \frac{1}{2}\deg f + 1$. □

Замечание. Для многочленов

$$f(t) = t^2 + 2,$$
$$g(t) = t^3 + 3t$$

неравенство Дэвенпорта обращается в равенство.

Теорема 18.3. Пусть f, g и h — взаимно простые многочлены, причем хотя бы один из них — не константа. Тогда равенство

$$f^n + g^n = h^n$$

не может выполняться при $n \geqslant 3$.

Доказательство. Согласно теореме 18.1 степень каждого из многочленов f^n, g^n и h^n не превосходит

$$\deg f + \deg g + \deg h - 1.$$

Сложив эти три неравенства, получим

$$n(\deg f + \deg g + \deg h) \leqslant 3(\deg f + \deg g + \deg h - 1).$$

Следовательно, $n < 3$. □

Диофантово уравнение $f^\alpha + g^\beta = h^\gamma$ для многочленов f, g, h имеет очевидное решение, если одно из чисел α, β, γ равно 1. Поэтому будем считать, что $\alpha, \beta, \gamma \geqslant 2$.

Теорема 18.4. Пусть α, β, γ — натуральные числа, причем $2 \leqslant \alpha \leqslant \beta \leqslant \gamma$. Тогда уравнение

$$f^\alpha + g^\beta = h^\gamma$$

имеет взаимно простые решения лишь для следующих наборов (α, β, γ): $(2, 2, \gamma)$, $(2, 3, 3)$, $(2, 3, 4)$ и $(2, 3, 5)$.

Доказательство. Пусть a, b и c — степени многочленов f, g и h. Тогда согласно теореме 18.1

$$\alpha a \leqslant a + b + c - 1, \tag{1}$$
$$\beta b \leqslant a + b + c - 1, \tag{2}$$
$$\gamma c \leqslant a + b + c - 1. \tag{3}$$

Следовательно,

$$\alpha(a+b+c) \leqslant \alpha a + \beta b + \gamma c \leqslant 3(a+b+c) - 3,$$

а значит, $\alpha < 3$. По условию $\alpha \geqslant 2$, поэтому $\alpha = 2$. При $\alpha = 2$ неравенство (1) принимает вид

$$a \leqslant b + c - 1. \tag{4}$$

Сложив неравенства (4), (2) и (3), получим

$$\beta b + \gamma c \leqslant 3(b+c) + a - 3.$$

Учитывая, что $\beta \leqslant \gamma$, и еще раз применяя неравенство (4), получаем

$$\beta(b+c) \leqslant 4(b+c) - 4,$$

а значит, $\beta \leqslant 4$, т. е. $\beta = 2$ или 3.

Остается доказать, что если $\beta = 3$, то $\gamma \leqslant 5$. При $\beta = 3$ неравенство (2) принимает вид

$$2b \leqslant a + c - 1. \tag{5}$$

Сложив неравенства (4) и (5), получим

$$b \leqslant 2c - 2.$$

В таком случае из неравенства (4) следует, что

$$a \leqslant 3c - 3.$$

Из двух последних неравенств и неравенства (3) следует, что

$$\gamma c \leqslant 6c - 6,$$

поэтому $\gamma \leqslant 5$.

Многочлены, удовлетворяющие соотношению $f^\alpha + g^\beta = h^\gamma$, тесно связаны с правильными многогранниками. Подробно эта связь описана в книге Феликса Клейна [Кл]; там же указан способ построения этих многочленов. Мы приведем лишь конечный результат.

Случай $\alpha = \beta = 2$, $\gamma = n$ связан с вырожденным правильным многогранником — плоским n-угольником. Требуемое соотношение имеет вид

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

Случай $\alpha = 2$, $\beta = 3$, $\gamma = 3$ связан с правильным тетраэдром. Соотношение имеет вид

$$12i\sqrt{3}\,(x^5 - x)^2 + (x^4 - 2i\sqrt{3}\,x^2 + 1)^3 = (x^4 + 2i\sqrt{3}\,x^2 + 1)^3.$$

Случай $\alpha = 2$, $\beta = 3$, $\gamma = 4$ связан с кубом и правильным октаэдром. Соотношение имеет вид

$$(x^{12} - 33x^8 - 33x^4 + 1)^2 + 108(x^5 - x)^4 = (x^8 + 14x^4 + 1)^3.$$

Случай $\alpha = 2$, $\beta = 3$, $\gamma = 5$ связан с додекаэдром и икосаэдром. Соотношение имеет вид $T^2 + h^3 = 1728f^5$, где

$$\begin{aligned} T &= x^{30} + 1 + 522(x^{25} - x^5) - 10005(x^{20} + x^{10}), \\ H &= -(x^{20} + 1) + 228(x^{15} - x^5) - 494x^{10}, \\ f &= x(x^{10} + 11x^5 - 1). \end{aligned}$$

□

Теорему 18.4 доказал Г. Шварц [Shw]. Решение диофантова уравнения более общего вида $f^\alpha + g^\beta = l^\mu h^\gamma$ приведено в работе [Ev].

Теорема 18.5 [N]. Пусть $x(t)$, $y(t)$ — рациональные функции и m, $n \geqslant 2$. Тогда уравнение

$$x^n - y^m = 1$$

имеет решение лишь при $m = n = 2$.

Доказательство. Представим x и y в виде $x = f/g$ и $y = h/k$, где f и g — взаимно простые многочлены и h и k тоже взаимно простые многочлены. Тогда рассматриваемое уравнение запишется в виде

$$f^m k^n - h^n g^m = g^m k^n. \tag{6}$$

Из взаимной простоты многочленов f и g следует, что если $g(\alpha) = 0$, то $f(\alpha) = 0$. В таком случае из соотношения (6) следует, что $k(\alpha) = 0$. Аналогично, если $k(\alpha) = 0$, то $g(\alpha) = 0$. Поэтому $g(t) = \prod(t - \alpha_i)^{a_i}$ и $k(t) = \prod(t - \alpha_i)^{b_i}$, где a_i, $b_i \geqslant 1$.

Кратность α_i как корня многочленов $f^m k^n$, $h^n g^m$ и $g^m k^n$ равна nb_i, ma_i и $nb_i + ma_i$, соответственно. Если $nb_i \neq ma_i$, то кратность корня α_i многочлена $f^m k^n - h^n g^m$ строго меньше $nb_i + ma_i$. Поэтому $nb_i = ma_i$, т. е. $k^n = g^m$.

Уравнение (6) после сокращения на $k^n = g^m$ принимает вид

$$f^m - h^n = g^m.$$

Согласно теореме 18.4 возможны лишь два варианта: $m = n = 2$ и $\{m, n\} = \{2, 3\}$. Но во втором случае $k^n = g^m = l^6$, где l — некоторый многочлен, а уравнение $f^3 - h^2 = l^6$ решений не имеет. □

18.1.2. Проблема Варинга для многочленов

Классическая проблема Варинга заключается в том, чтобы для данного натурального числа n найти минимальное число $k = k(n)$, для которого любое натуральное число m можно представить в виде $m = m_1^n + \ldots + m_k^n$, где $m_1, \ldots, m_k$ — целые неотрицательные числа. Известно много разных обобщений этой проблемы для многочленов. Мы будем подразумевать под *проблемой Варинга для многочленов* следующую задачу: для данного натурального числа n найти минимальное число $k = k(n)$, для которого любой многочлен $g \in \mathbb{C}[x]$ можно представить в виде $g = f_1^n + \ldots + f_k^n$, где $f_i \in \mathbb{C}[x]$.

При решении проблемы Варинга достаточно ограничиться случаем $g(x) = x$. Действительно, если $x = f_1^n(x) + \ldots + f_k^n(x)$ и $h(x)$ — произвольный многочлен, то $h(x) = f_1^n\big(h(x)\big) + \ldots + f_k^n\big(h(x)\big)$.

Тождество $\left(x + \frac{1}{4}\right)^2 - \left(x - \frac{1}{4}\right)^2 = x$ показывает, что $k(2) = 2$.

Теорема 18.6 [NM]. Если $n \geqslant 3$, то: а) $k(n) \geqslant 3$; б) $k(n) \leqslant n < k^2(n) - k(n)$.

Доказательство. а) Предположим, что $x = f_1^n(x) + f_2^n(x) = \prod\limits_{r=1}^{n} (f_1 + \varepsilon^r f_2)$, где ε — примитивный корень степени n из единицы. Все множители $f_1 + \varepsilon^r f_2$, кроме одного, являются константами. При $n \geqslant 3$ таких множителей по крайней мере два. Поэтому $f_1 + af_2 = \alpha$ и $f_1 + bf_2 = \beta$, где $a \neq b$ и $a, b, \alpha, \beta \in \mathbb{C}$. Следовательно, $f_1, f_2 \in \mathbb{C}$, чего не может быть.

б) Для многочлена $f(x)$ положим $\Delta f(x) = f(x+1) - f(x)$ и $\Delta^p f = \Delta(\Delta^{p-1} f)$ при $p \geqslant 2$. Легко проверить, что $\deg(\Delta f) = \deg f - 1$. Поэтому $\deg \Delta^{n-1}(x^n) = 1$, т. е. $\Delta^{n-1}(x^n) = ax + b$. С другой стороны, непосредственно из определения видно, что

$$\Delta^{n-1}(x^n) = (x + n - 1)^n + c_1(x + n - 2)^n + \ldots + c_{n-1}x^n.$$

В самом деле, например,

$$\Delta^2(x^3) = \big((x+2)^3 - (x+1)^3\big) - \big((x+1)^3 - x^3\big).$$

Сделав замену $x_1 = ax + b$, получим представление $x_1 = f_1^n(x_1) + \ldots + f_n^n(x_1)$; это представление показывает, что $k(n) \leqslant n$.

Займемся теперь доказательством неравенства $n < k^2(n) - k(n)$. Рассмотрим представление $x = f_1^n(x) + \ldots + f_k^n(x)$, $f_i \in \mathbb{C}[x]$, для которого число k минимально.

Напомним, что вронскиан $W(g_1, \ldots, g_k)$ функций $g_1(x), \ldots, g_k(x)$ равен определителю матрицы $\begin{pmatrix} g_1(x) & \ldots & g_k(x) \\ g_1'(x) & \ldots & g_k'(x) \\ \vdots & \ddots & \vdots \\ g_1^{(k-1)}(x) & \ldots & g_k^{(k-1)}(x) \end{pmatrix}$. Рассмотрим два вронскиана $W_1 = W(f_1^n, f_2^n, \ldots, f_k^n)$ и $W_2 = W(x, f_2^n, \ldots, f_k^n)$. По условию $x = f_1^n + \ldots + f_k^n$, поэтому первый столбец вронскиана W_2 получается из первого столбца вронскиана W_1 добавлением линейной комбинации других столбцов W_1. Следовательно, $W_1 = W_2$.

Если функции $g_1, g_2, \ldots, g_k$ линейно зависимы, то их вронскиан $W(g_1, \ldots, g_k)$ тождественно равен нулю. Обратное утверждение неверно. Например, если $g_1(x) = x^2$, а $g_2(x) = x|x|$, то

$$W(g_1, g_2) = \begin{vmatrix} x^2 & x|x| \\ 2x & 2|x| \end{vmatrix} = 0,$$

но функции g_1 и g_2 линейно независимы. Можно доказать, что если вронскиан $W(g_1, \ldots, g_k)$ тождественно равен нулю при $x \in (a, b)$, то существует интервал $(\alpha, \beta) \subset (a, b)$, на котором функции $g_1, \ldots, g_k$ линейно зависимы (простое доказательство этого утверждения приведено в [Kru]). В частности, для полиномиальных функций $g_1, \ldots, g_k$ из того, что вронскиан $W(g_1, \ldots, g_k)$ тождественно равен нулю, следует, что эти функции линейно зависимы.

Из минимальности представления $x = f_1^n(x) + \ldots + f_k^n(x)$ следует, что функции $f_1^n, \ldots, f_k^n$ линейно независимы, поэтому $W(f_1^n, f_2^n, \ldots, f_k^n)$ — ненулевой многочлен.

Производная порядка r функции f_i^n делится на f_i^{n-r}, поэтому i-й столбец вронскиана делится на f_i^{n-k+1}, а значит, многочлен $W(f_1^n, \ldots, f_k^n)$ делится на $\prod\limits_{i=1}^{k} f_i^{n-k+1}$. В частности,

$$\deg W(f_1^n, \ldots, f_k^n) \geqslant (n-k+1) \sum_{i=1}^{k} \deg f_i. \qquad (1)$$

С другой стороны,

$$\deg W(f_1^n, \ldots, f_k^n) \leqslant n \sum_{i=2}^{k} \deg f_i - \frac{k(k-1)}{2} + 1. \qquad (2)$$

Чтобы доказать это, напомним, что $W(f_1^n, \ldots, f_k^n) = W(x, f_2^n, \ldots, f_k^n)$. Если мы домножим j-ю строку определителя $W(x, f_2^n, \ldots, f_k^n)$ на x^{j-1}, то в результате получим определитель матрицы, у которой все ненулевые элементы i-го столбца (при $i \geqslant 2$) имеет степень $n \deg f_i$. Поэтому

$$\deg W(f_1^n, \ldots, f_k^n) \leqslant 1 + n \sum_{i=2}^{k} \deg f_i - 1 - 2 - \ldots - (k-1) =$$

$$= n \sum_{i=2}^{k} \deg f_i - \frac{k(k-1)}{2} + 1.$$

Сравнивая (1) и (2), получаем

$$(n-k+1) \sum_{i=1}^{k} \deg f_i \leqslant n \sum_{i=2}^{k} \deg f_i - \frac{k(k-1)}{2} + 1,$$

т. е.

$$n \deg f_1 \leqslant (k-1) \sum_{i=1}^{k} \deg f_i - \frac{k(k-1)}{2} + 1.$$

Можно считать, что f_1 — многочлен наибольшей степени. Тогда

$$n \deg f_1 \leqslant k(k-1) \deg f_1 - \frac{k(k-1)}{2} + 1 < k(k-1) \deg f_1;$$

последнее неравенство следует из того, что $1 - k(k-1)/2 < 0$ при $k \geqslant 3$. После сокращения на $\deg f_1$ получаем $n < k(k-1)$. □

18.2. Функциональные уравнения для многочленов

18.2.1. Функциональные уравнения, задающие многочлены

Для многочлена f степени $n+1$ выполняется равенство

$$f(x) = f(y) + (x-y)f'(y) + \ldots + (x-y)^{n+1} \frac{f^{(n+1)}(y)}{(n+1)!}.$$

При этом $f^{(n+1)}$ — константа, а значит,

$$(x-y)^{n+1}\frac{f^{(n+1)}(y)}{(n+1)!} = \\ = (x-y)^n\left(\frac{-yf^{(n+1)}(y)}{(n+1)!}-c\right)+(x-y)^n\left(\frac{xf^{(n+1)}(x)}{(n+1)!}+c\right).$$

Таким образом, у функционального уравнения

$$f(x)=\sum_{k=0}^{n}(x-y)^k g_k(y)+(x-y)^n h(x) \tag{1}$$

есть решение следующего вида:

(а) f — многочлен степени не выше $n+1$;
(б) $g_k(y)=f^{(k)}(y)/k!$ при $k=0,1,\ldots,n-1$;
(в) $g_n(y)=f^{(n)}(y)/n!-yf^{(n+1)}(y)/(n+1)!-c$;
(г) $h(x)=xf^{(n+1)}(x)/(n+1)!+c$.

Теорема 18.7 [СК]. Пусть $f,g_0,\ldots,g_n,h:\mathbb{R}\to\mathbb{R}$ — произвольные функции, которые при всех $x,y\in\mathbb{R}$, $x\neq y$, удовлетворяют уравнению (1). Тогда эти функции имеют указанный выше вид (а)–(г).

Доказательство. При $y=0$ и $y=1$ уравнение (1) принимает вид

$$f(x)=\sum_{k=0}^{n}c_kx^k+x^nh(x),\quad x\neq 0, \tag{2}$$

$$f(x)=\sum_{k=0}^{n}d_kx^k+(x-1)^nh(x),\quad x\neq 1. \tag{3}$$

Следовательно,

$$h(x)=\frac{\sum\limits_{k=0}^{n}(d_k-c_k)x^k}{x^n-(x-1)^n}.$$

Это равенство выполняется при $x\neq 0,1$, а при n четном нужно еще исключить и $x=1/2$.

Фиксировав $y=2$ и $y=4$, аналогичным образом получим равенство

$$h(x)=\frac{\sum\limits_{k=0}^{n}(f_k-e_k)x^k}{(x-2)^n-(x-4)^n},$$

которое выполняется при $x\neq 2,3,4$.

В итоге получаем $h \in C^\infty(\mathbb{R})$, но тогда из (2) и (3) следует, что $f \in C^\infty(\mathbb{R})$.

Продифференцировав n раз по x равенство (1), получим

$$f^{(n)}(x) = n!g_n(y) + \frac{d^n}{dx^n}\big((x-y)^n h(x)\big).$$

При фиксированном x из этого равенства следует, что $g_n(y)$ — полином. Теперь можно продифференцировать равенство (1) по x не n, а $n-1$ раз, и аналогичным образом получить, что $g_{n-1}(y)$ — полином и т. д. В частности, $g_0, \ldots, g_n \in C^\infty(\mathbb{R})$.

Продифференцируем равенство (1) по y и положим $y = 0$. В результате получим

$$0 = -\sum_{k=0}^{n} kx^{k-1} g_k(0) + \sum_{k=0}^{n} kx^k g_k'(0) - nx^{n-1}h(x).$$

Из этого равенства следует, что $x^{n-1}h(x)$ — полином степени не выше n. А если равенство (1) продифференцировать n раз по y и положить $y = 0$, то можно показать, что $h(x)$ — полином (тоже степени не выше n). Но если $h(x)$ — полином, а $x^{n-1}h(x)$ — полином степени не выше n, то $h(x) = ax + b$.

Так как $h(x) = ax + b$ и $f \in C^\infty(\mathbb{R})$, то из (2) следует, что $f(x)$ — полином степени не выше $n+1$. Поэтому

$$f(x+y) = \sum_{k=0}^{n+1} \frac{f^{(k)}(y)}{k!} x^k.$$

С другой стороны, заменив x на $x+y$, соотношение (1) можно записать в виде

$$f(x+y) = \sum_{k=0}^{n} x^k g_k(y) + x^n(ax + ay + b).$$

Это означает, что

$$g_k(y) = \frac{f^{(k)}(y)}{k!} \quad \text{при} \quad k = 0, 1, \ldots, n-1,$$

$$g_n(y) = \frac{f^{(n)}(y)}{n!} - ay - b \quad \text{и} \quad \frac{f^{(n+1)}(y)}{(n+1)!} = a. \qquad \square$$

Следствие 1. Пусть $f \in C^n(\mathbb{R})$ и при всех $x, y \in \mathbb{R}$, $x \neq y$, выполняется равенство

$$\frac{f(x) - \sum\limits_{k=0}^{n-1} \frac{(x-y)^k}{k!} f^{(k)}(y)}{(x-y)^n} = \frac{f^{(n)}(x) + f^{(n)}(y)}{(n+1)!}.$$

Тогда f — полином степени не выше n.

Следствие 2 [Н]. Если при всех $x, y \in \mathbb{R}$, $x \neq y$, выполняется равенство

$$\frac{f(x) - g(y)}{x - y} = \frac{\varphi(x) + \varphi(y)}{2}, \tag{4}$$

то f — полином степени не выше 2, $g = f$ и $\varphi = f'$.

К функциональному уравнению (4) сводится также функциональное уравнение

$$\frac{f(x) - g(y)}{x - y} = \varphi\left(\frac{x+y}{2}\right). \tag{5}$$

Дело в том, что если равенство (5) выполняется при всех $x, y \in \mathbb{R}$, $x \neq y$, то

$$\varphi\left(\frac{x+y}{2}\right) = \frac{\varphi(x) + \varphi(y)}{2}.$$

Чтобы доказать это, заменим в (5) x на $x+y$, а y на $x-y$. В результате получим

$$\frac{f(x+y) - g(x-y)}{2y} = \varphi(x)$$

при всех $x, y \in \mathbb{R}$, $y \neq 0$. Заменив теперь y на $-y$, получим

$$\frac{f(x-y) - g(x+y)}{-2y} = \varphi(x).$$

Следовательно,

$$f(u+v+y) - g(u+v-y) = 2y\varphi(u+v),$$
$$f(u-v+y) - g(u-v-y) = 2y\varphi(u-v)$$

и

$$f(u+v+y)-g(u-v-y)=2(v+y)\varphi(u),$$
$$f(u-v+y)-g(u+v-y)=-2(v-y)\varphi(u).$$

Поэтому

$$\varphi(u+v)+\varphi(u-v)=2\varphi(u).$$

Положив $u+v=x$, $u-v=y$, получим требуемое равенство

$$\varphi(x)+\varphi(y)=2\varphi\left(\frac{x+y}{2}\right).$$

18.2.2. Полиномиальные решения уравнения $f(\alpha x+\beta)=f(x)$

При $\alpha=\pm1$ полиномиальные решения уравнения $f(\alpha x+\beta)=f(x)$ находятся легко. Если $\alpha=1$ и $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$, где $a_0\neq0$, то получаем тождество

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n=a_0(x+\beta)^n+a_1(x+\beta)^{n-1}+\ldots+a_n.$$

Такое тождество возможно лишь в том случае, когда $a_1=a_1+a_0n\beta$, т. е. $\beta=0$.

Если $\alpha=-1$, то уравнение $f(-x+\beta)=f(x)$ после замены $g(x)=f(x+\beta/2)$ сводится к уравнению $g(x)=g(-x)$, решениями которого служат полиномы вида

$$a_0x^{2n}+a_2x^{2n-2}+\ldots+a_{2n}.$$

При произвольном α сравнение коэффициентов при старшем члене многочлена $f(x)=a_0x^n+\ldots$ показывает, что $\alpha^n=1$. Таким образом, при $\alpha\neq\pm1$ получаем $n\geqslant3$.

Теорема 18.8 [Oz]. Пусть многочлен f степени $n\geqslant3$ удовлетворяет соотношению $f(\alpha x+\beta)=f(x)$, где $\alpha\neq\pm1$ и $\alpha^n=1$. Тогда

$$f(x)=a_0\left(x+\frac{\beta}{\alpha-1}\right)^n+c.$$

Доказательство. Достаточно рассмотреть многочлены вида $f(x)=x^n+a_1x^{n-1}+\ldots+a_n$. Требуется доказать, что $a_j=\binom{n}{j}\frac{\beta^j}{(\alpha-1)^j}$ при $j=1,\ldots,n-1$. Доказательство проведем индукцией по j.

Сравнение коэффициентов при x^{n-j} для многочленов $f(x)$ и $f(\alpha x+\beta)$ показывает, что

$$(1-\alpha^{n-j})a_j = \sum_{s=0}^{j-1} a_s \binom{n-s}{j-s} \alpha^{n-j}\beta^{j-s}. \tag{1}$$

При $j=1$ получаем $(1-\alpha^{n-1})a_1 = \binom{n}{1}\alpha^{n-1}\beta$. По условию $\alpha^n = 1$, поэтому

$$a_1 = \binom{n}{1}\frac{\alpha^{-1}\beta}{1-\alpha^{-1}} = \binom{n}{1}\frac{\beta}{\alpha-1}.$$

База индукции доказана.

Для доказательства шага индукции (т. е. перехода от $j=k$ к $j=k+1$) мы снова воспользуемся соотношением (1) и условием $\alpha^n = 1$. По предположению индукции $a_s = \binom{n}{s}\frac{\beta^s}{(\alpha-1)^s}$ при $s = 1, \ldots, k$. Поэтому

$$(1-\alpha^{n-k-1})a_{k+1} = \binom{n}{k+1}\alpha^{n-k-1}\beta^k + \sum_{s=1}^{k}\binom{n}{s}\binom{n-s}{k+1-s}\frac{\alpha^{n-k+1}\beta^{k+1}}{(\alpha-1)^s}.$$

Легко проверить, что $\binom{n}{s}\binom{n-s}{k+1-s} = \binom{n}{k+1}\binom{k+1}{s}$. Поэтому

$$(1-\alpha^{n-k-1})a_{k+1} = \\ = \binom{n}{k+1}\alpha^{n-k-1}\beta^{k+1}\left[1+\binom{k+1}{1}\frac{1}{\alpha-1}+\ldots+\binom{k+1}{k}\frac{1}{(\alpha-1)^k}\right].$$

Ясно также, что выражение в квадратных скобках равно

$$\left(1+\frac{1}{\alpha-1}\right)^{k+1} - \left(\frac{1}{\alpha-1}\right)^{k+1} = \frac{\alpha^{k+1}-1}{(\alpha-1)^{k+1}}.$$

Следовательно,

$$a_{k+1} = \frac{1}{1-\alpha^{n-k-1}}\binom{n}{k+1}\beta^{k+1}\frac{\alpha^n-\alpha^{n-k-1}}{(\alpha-1)^{k+1}}.$$

Учитывая, что $\alpha^n = 1$, получаем

$$a_{k+1} = \binom{n}{k+1}\frac{\beta^{k+1}}{(\alpha-1)^{k+1}}. \qquad \square$$

19. Преобразования многочленов

19.1. Преобразование Чирнгауза

В 1683 г. в лейпцигском журнале «Acta eruditorum» Э.В. фон Чирнгауз (1651–1708) опубликовал способ преобразования алгебраических уравнений, который, как ему казалось, позволял решить в радикалах уравнение любой степени. Лейбниц сразу же опроверг заявление Чирнгауза о всемогуществе его преобразования. Дело в том, что при решении уравнений 5-й степени с помощью преобразования Чирнгауза приходится решать уравнение 24-й степени. Несмотря на это, преобразование Чирнгауза имеет важные приложения. Например, с его помощью любое уравнение пятой степени без кратных корней можно привести к виду $y^5 + 5y = a$, решая при этом лишь уравнения второй и третьей степени.

Преобразование Чирнгауза уравнения $x^n + c_1x^{n-1} + \ldots + c_n = 0$ заключается в следующем. Пусть $x_1, \ldots, x_n$ — корни этого уравнения. Рассмотрим рациональную функцию φ, которая не обращается в бесконечность в точках $x_1, \ldots, x_n$. Положим $y_i = \varphi(x_i)$ и найдем уравнение

$$y^n + q_1y^{n-1} + \ldots + q_n = 0$$

корнями которого являются $y_1, \ldots, y_n$. Далее мы покажем, что если это уравнение не имеет кратных корней, то x_i можно выразить через y_i. Выбирая подходящим образом функцию φ, можно добиться того, чтобы коэффициенты $q_1, \ldots, q_{n-1}$ стали равны нулю. Но для этого потребуется решить уравнение степени $(n-1)!$; именно на это обстоятельство указал Лейбниц.

Не теряя общности, в качестве рациональной функции φ можно взять многочлен степени не более $n-1$. Дело в том, что справедливо следующее утверждение.

Теорема 19.1. Пусть $x_1, \ldots, x_n$ — корни многочлена f степени n и $\varphi = P/Q$, где P и Q — многочлены, причем $Q(x_i) \neq 0$, $i = 1, \ldots, n$. Тогда существует многочлен g степени не более $n-1$, значения которого в точках $x_1, \ldots, x_n$ совпадают со значениями функции φ в этих точках.

Доказательство. По условию многочлены f и Q не имеют общих корней, поэтому они взаимно просты. Следовательно, существуют многочлены a и b, для которых $af + bQ = 1$. Так как $f(x_i) = 0$, то $b(x_i) = 1/Q(x_i)$. Поэтому $\varphi(x_i) = P(x_i)/Q(x_i) = P(x_i)\,b(x_i)$ Таким образом, в качестве требуемого многочлена g можно взять остаток от деления многочлена Pb на многочлен f. □

В дальнейшем будем считать, что к уравнению

$$f(x) = x^n + c_1 x^{n-1} + \ldots + c_n$$

применяется преобразование

$$y = g(x) = p_0 + p_1(x) + \ldots + p_{n-1} x^{n-1}.$$

Покажем, как в этом случае можно вычислить коэффициенты многочлена $y^n + q_1 y^{n-1} + \ldots + q_n$ с корнями $y_i = g(x_i)$, $i = 1, \ldots, n$.

Чтобы избежать громоздких обозначений, ограничимся случаем $n = 3$. Если $x^3 = -c_1 x^2 - c_2 x - c_3$, то

$$yx = p_0 x + p_1 x^2 + p_2(-c_1 x^2 - c_2 x - c_3) = p_0' + p_1' x + p_2' x^2.$$

Аналогично $yx^2 = p_0'' + p_1'' x + p_2'' x^2$, причем p_i'' — линейные функции параметров p_i. Таким образом, если x_i — корень многочлена f и $y_i = g(x_i)$, то система уравнений

$$\begin{cases} (p_0 - y) z_0 + p_1 z_1 + p_2 z = 0, \\ p_0' z_0 + (p_1' - y) z_1 + p_2' z = 0, \\ p_0'' z_0 + p_1'' z_1 + (p_2'' - y) z = 0 \end{cases} \tag{1}$$

имеет ненулевое решение $(z_0, z_1, z_2) = (1, x_i, x_i^2)$. Положим

$$A = \begin{pmatrix} p_0 & p_1 & p_2 \\ p_0' & p_1' & p_2' \\ p_0'' & p_1'' & p_2'' \end{pmatrix}.$$

Тогда $\det(A - yI) = 0$ для $y_i = g(x_i)$. В том случае, когда многочлен $\det(A - yI)$ не имеет кратных корней, он совпадает с искомым многочленом $y^n + q_1 y^{n-1} + \ldots + q_n$. Так как элементы матрицы A линейно зависят от параметров p_i, то коэффициент q_k является многочленом степени k от параметров p_i.

В том случае, когда многочлен $y^n + q_1 y^{n-1} + \ldots + q_n$ не имеет кратных корней, матрица A не имеет кратных собственных значений. Поэтому каждому собственному значению матрицы A соответствует единственное с точностью до пропорциональности решение системы (1). Это означает, что по корню y_i преобразованного многочлена однозначно восстанавливается корень x_i исходного многочлена, причем x_i рационально выражается через y_i.

Преобразование Чирнгауза позволяет решить в радикалах уравнения третьей и четвертой степени. Кубическое уравнение можно привести к виду

$$y^3 + q_3 = 0,$$

решив систему из линейного уравнения $q_1 = 0$ и уравнения второй степени $q_2 = 0$, зависящих от параметров p_0, p_1, p_2. Для этого нужно решить квадратное уравнение.

Уравнение четвертой степени можно привести к виду

$$y^4 + q_2 y^2 + q_4 = 0.$$

Для этого нужно решить систему из линейного уравнения $q_1 = 0$ и уравнения третьей степени $q_3 = 0$, что сводится к решению кубического уравнения.

19.2. Уравнение пятой степени в форме Бринга

Уравнение пятой степени можно привести к виду

$$y^5 + q_4 y + q_5 = 0,$$

решив систему уравнений $q_1 = q_2 = q_3 = 0$. Для этого нужно решить уравнение шестой степени. Более тонкий анализ, проведенный в 1789 г. шведским математиком Брингом, показывает, что в данном случае вместо уравнения шестой степени достаточно решить уравнения второй и третьей степени, поступив следующим образом. Чтобы удовлетворить условию $q_1 = 0$, выразим один из параметров $p_0, \ldots, p_4$ как линейную функцию остальных параметров. Тогда коэффициент q_2 будет представлять собой квадратичную форму относительно четырех из параметров p_i. Эту квадратичную форму можно привести к виду

$$u_1^2 + u_2^2 - v_1^2 - v_2^2,$$

где u_j и v_j — линейные функции от p_i (для этого понадобится извлекать квадратные корни). Чтобы удовлетворить равенству $q_2 = 0$, достаточно решить систему линейных уравнений $u_1 = v_1$, $u_2 = v_2$. После этого остается два параметра, причем относительно них уравнение q_3 представляет уравнение третьей степени. В итоге получаем уравнение вида $y^5 + q_4 y + q_5 = 0$. В том случае, когда $q_4 \neq 0$, с помощью линейной замены это уравнение можно привести к виду $y^5 + 5y = a$.

Аналогичным образом уравнение

$$x^n + c_1 x^{n-1} + \ldots + c_n = 0, \quad n \geqslant 5, \tag{1}$$

с помощью преобразования $y = p_0 + p_1 x + p_2 x^2 + p_3 x^3 + p_4 x^4$ можно привести к виду

$$y^n + q_4 y^{n-4} + q_5 y^{n-5} + \ldots + q_n = 0.$$

При этом понадобится решать лишь уравнения второй и третьей степени.

Кроме того, вместо системы уравнений $q_1 = q_2 = q_3 = 0$ можно решить систему $q_1 = q_2 = q_4 = 0$, т. е. на последнем шаге вместо кубического уравнения $q_3 = 0$ решить уравнение четвертой степени $q_4 = 0$. Тогда уравнение (1) будет приведено к виду

$$y^n + q_3 y^{n-3} + q_5 y^{n-5} + \ldots + q_n = 0.$$

Используя такие преобразования и замену $x \mapsto x^{-1}$, уравнение пятой степени можно привести к любому из следующих видов: $x^5 + px + q = 0$, $x^5 + px^2 + q = 0$, $x^5 + px^3 + q = 0$, $x^5 + px^4 + q = 0$.

19.3. Представление многочленов в виде сумм степеней линейных функций

Задача о представлении многочлена в виде суммы степеней линейных функций наиболее проста в случае квадратного трехчлена $x^2 + 2ax + b$. Эта задача такова: квадратный трехчлен требуется представить в виде $\lambda_1(x + \alpha_1)^2 + \ldots + \lambda_m(x + \alpha_m)^2$; при этом нужно также выяснить каким минимальным количеством базисных линейных функций $x + \alpha_1, \ldots, x + \alpha_m$ можно обойтись. Есть два варианта этой задачи:

1) базисные функции одни и те же для всех квадратных трехчленов;

2) базисные функции для каждого квадратного трехчлена выбираются свои.

В первом случае минимальное m равно 3. В качестве базисных функций можно взять любые три различные функции $x + \alpha_1$, $x + \alpha_2$, $x + \alpha_3$. Действительно, система уравнений для $\lambda_1, \lambda_2, \lambda_3$ имеет вид

$$\begin{aligned} \lambda_1 + \lambda_2 + \lambda_3 &= 1, \\ \alpha_1\lambda_1 + \alpha_2\lambda_2 + \alpha_3\lambda_3 &= a, \\ \alpha_1^2\lambda_1 + \alpha_2^2\lambda_2 + \alpha_3^2\lambda_3 &= b. \end{aligned}$$

Она всегда имеет решение, так как ее определителем служит ненулевой определитель Вандермонда. Ясно также, что двумя функциями $x+\alpha_1$ и $x+\alpha_2$ нельзя обойтись: $\lambda_3=0$ лишь в том случае, когда a, b, α_1 и α_2 связаны соотношением $a(\alpha_1+\alpha_2)=b+\alpha_1\alpha_2$.

Во втором случае минимальное m равно 2. Требуемое представление имеет, например, вид

$$x^2+2ax+b=\frac{1}{2}\left(x+a+\sqrt{b-a^2}\right)^2+\frac{1}{2}\left(x+a-\sqrt{b-a^2}\right)^2.$$

Для многочленов степени n задача о выборе универсальных базисных функций $x+\alpha_1,\ldots,x+\alpha_m$ решается точно так же, как и при $n=2$. Сформулируем ответ в виде теоремы (ее доказательство при $n>2$ такое же, как и при $n=2$).

Теорема 19.2. а) Если $\alpha_1,\ldots,\alpha_{n+1}$ — попарно различные числа, то любой многочлен степени n можно представить в виде

$$\lambda_1(x+\alpha_1)^n+\ldots+\lambda_{n+1}(x+\alpha_{n+1})^n.$$

б) Если числа $\alpha_1,\ldots,\alpha_m$ таковы, что любой многочлен степени n можно представить в виде

$$\lambda_1(x+\alpha_1)^n+\ldots+\lambda_m(x+\alpha_m)^n,$$

то $m\geqslant n+1$.

Набор универсальных базисных линейных форм несложно указать и для многочленов степени n от m переменных. Для удобства вместо многочлена $f(x_1,\ldots,x_m)$ степени n будем рассматривать однородный многочлен

$$F(x_0,x_1,\ldots,x_m)=x_0^n f\left(\frac{x_1}{x_0},\ldots,\frac{x_m}{x_0}\right).$$

Теорема 19.3 [Ss]. Пусть $\alpha_0,\ldots,\alpha_n$ — попарно различные числа, $Z_j=x_0+\alpha_s x_1+\alpha_t x_2+\ldots+\alpha_u x_m$, где $\alpha_s,\alpha_t,\ldots,\alpha_u\in\{\alpha_0,\ldots,\alpha_n\}$. Тогда формы $(Z_j)^n$ порождают линейное пространство всех однородных многочленов степени n от $m+1$ переменных.

Замечание. Количество форм $(Z_j)^n$ равно $(n+1)^m$, а размерность пространства однородных многочленов степени n от $m+1$ переменных равна $\binom{m+n}{n}$.

Доказательство. Рассмотрим для простоты случай $m = 2$. В этом случае многочлен

$$p(x, y, z) = \sum_{0 \leqslant i+j \leqslant n} a_{ij} x^{n-i-j} y^i z^j$$

требуется представить в виде

$$p(x, y, z) = \sum_{s,t=1}^{n+1} \lambda_{st} (x + \alpha_s y + \alpha_t z)^n = \sum_{s,t=1}^{n+1} \lambda_{st} \sum_{0 \leqslant i+j \leqslant n} c_{nij} \alpha_s^i \alpha_t^j x^{n-i-j} y^i z^j,$$

где $c_{nij} = \dfrac{n!}{i!j!(n-i-j)!}$. Получаем систему уравнений

$$a_{ij} = c_{nij} \sum_{s,t=1}^{n+1} \lambda_{st} \alpha_s^i \alpha_t^j, \quad 0 \leqslant i + j \leqslant n.$$

Дополним эту систему уравнениями

$$\sum_{s,t=1}^{n+1} \lambda_{st} \alpha_s^i \alpha_t^j = 0 \quad \text{при} \quad i + j > n, \quad 1 \leqslant i, j \leqslant n.$$

В результате получим систему линейных уравнений с матрицей $V \otimes V$, где $V = \|\alpha_i^j\|_0^n$ — матрица Вандермонда. Для произвольных матриц A и B с помощью приведения их к жордановой нормальной форме легко доказывается, что $\det(A \otimes B) = (\det A)^b (\det B)^a$, где a — размер матрицы A, b — размер матрицы B. Поэтому $\det(V \otimes V) = (\det V)^{(n+1)^2} \neq 0$.

Для произвольного m аналогично получаем систему линейных уравнений с определителем $\det(V \otimes \ldots \otimes V) = (\det V)^{(n+1)^m}$. □

В том случае, когда для каждого многочлена выбираются свои базисные линейные функции, задача существенно усложняется. Добавление слагаемого $b_k(x + \beta_k)^n$ увеличивает число варьируемых параметров на 2. Точное совпадении числа параметров, которыми задается многочлен степени n, и числа параметров в выражении $b_1(x + \beta_1)^n + \ldots$ $\ldots + b_k(x + \beta_k)^n$ возможно лишь в том случае, когда n нечетно. При этом $k = (n+1)/2$. Оказывается, что в случае общего положения многочлен нечетной степени n действительно можно представить в виде суммы $(n + 1)/2$ слагаемых вида $b(x + \beta)^n$. Но в некоторых вырожденных случаях могут оказаться необходимыми и дополнительные слагаемые.

Пример. Многочлен x^3+x^2 нельзя представить в виде $b_1(x+\beta_1)^3+$ $+b_2(x+\beta_2)^3$.

Доказательство. Ясно, что $\beta_1 \neq \beta_2$ и $\beta_1\beta_2 \neq 0$. В таком случае из условий $b_1\beta_1^2+b_2\beta_2^2=0$ и $b_1\beta_1^3+b_2\beta_2^3=0$ следует, что $b_1=b_2=0$. Приходим к противоречию. □

Уточним теперь, что в рассматриваемой ситуации означает «многочлен общего положения». Ограничимся при этом случаем $n=5$ (для остальных нечетных n рассуждения аналогичны). Запишем многочлен $f(x)$ степени 5 в виде

$$a_5x^5+5a_4x^4+10a_3x^3+10a_2x^2+5a_1x+a_0.$$

Пусть

$$\begin{vmatrix} 1 & z & z^3 & z^3 \\ a_0 & a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_5 \end{vmatrix} = p_3z^3+p_2z^2+p_1z+p_0=p(z).$$

Будем говорить, что $f(x)$ — многочлен общего положения, если $p(z)$ — многочлен, имеющий ровно 3 различных корня (в частности, $p_3\neq 0$).

Теорема 19.4 (Сильвестр). Многочлен общего положения нечетной степени n можно представить в виде суммы

$$b_1(x+\beta_1)^n+\ldots+b_k(x+\beta_k)^n,$$

где $k=(n+1)/2$.

Доказательство. В случае $n=5$ требуется решить систему уравнений

$$b_1\beta_1^r+b_1\beta_2^r+b_1\beta_3^r=a_r, \qquad (1)$$

$r=0,1,\ldots,5$. Выберем в качестве β_1,β_2 и β_3 корни уравнения $p(z)=0$. По условию эти три числа различны, поэтому из системы уравнений (1) для $r=0,1,2$ однозначно находятся b_1,b_2 и b_3. Остается доказать, что для полученных значений b_i и β_i выполняются уравнения (1) при $r=3,4,5$.

Из определения многочлена $p(z)$ следует, что для любых чисел x_0,x_1,x_2,x_3 выполняется равенство

$$\begin{vmatrix} x_0 & x_1 & x_2 & x_3 \\ a_0 & a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_5 \end{vmatrix} = p_3x_3+p_2x_2+p_1x_1+p_0x_0.$$

Кроме того, если строку (x_0, x_1, x_2, x_3) заменить на $(a_i, a_{i+1}, a_{i+2}, a_{i+3})$, где $i = 0, 1, 2$, то определитель обратится в нуль. Для $i = 0$ получаем

$$p_3 a_3 + p_2 a_2 + p_1 a_1 + p_0 a_0 = 0,$$

т. е.

$$\begin{aligned} -p_3 a_3 &= p_0 \sum b_i + p_1 \sum b_i \beta_i + p_2 \sum b_i \beta_i^2 = \\ &= \sum b_i (p + 0 + p_1 \beta_i + p_2 \beta_i^2) = -\sum b_i p_3 \beta_i^3. \end{aligned}$$

Учитывая, что $p_3 \neq 0$, получаем соотношение (1) для $r = 3$. Беря $i = 1$ и 2, аналогично получаем соотношения (1) для $r = 4$ и 5. □

20. Алгебраические числа

20.1. Определение и основные свойства

Число $\alpha \in \mathbb{C}$ называют *алгебраическим*, если оно является корнем неприводимого многочлена с рациональными коэффициентами. Если старший коэффициент равен 1, а все остальные коэффициенты — целые числа, то число α называют *целым алгебраическим*. Каждому алгебраическому числу α соответствует единственный неприводимый многочлен f со старшим коэффициентом 1. Корни этого многочлена называют числами, *сопряженными* с α.

Назовем многочлен *унитарным*, если его старший коэффициент равен 1. Несложно показать, что если α — корень произвольного (т. е. не обязательно неприводимого) унитарного многочлена с целыми коэффициентами, то α — целое алгебраическое число. Иными словами, если унитарный многочлен с целочисленными коэффициентами представлен в виде произведения двух унитарных многочленов с рациональными коэффициентами, то все эти рациональные коэффициенты — целые числа. Это утверждение — одна из возможных формулировок леммы Гаусса (лемма 6.1 на с. 60).

Теорема 20.1. Пусть α и β — алгебраические числа, $\varphi(x, y)$ — произвольный многочлен с рациональными коэффициентами. Тогда $\varphi(\alpha, \beta)$ — алгебраическое число.

Доказательство. Пусть $\{\alpha_1, \ldots, \alpha_n\}$ и $\{\beta_1, \ldots, \beta_m\}$ — наборы чисел, сопряженных с α и β соответственно. Рассмотрим многочлен

$$F(t) = \prod_{i=1}^{n} \prod_{j=1}^{m} \bigl(t - \varphi(\alpha_i, \beta_j)\bigr).$$

Коэффициенты этого многочлена являются симметрическими функциями от $\alpha_1, \ldots, \alpha_n$ и $\beta_1, \ldots, \beta_m$. Поэтому они являются рациональными числами. □

Замечание. Аналогично можно доказать, что если α и β — целые алгебраические числа, а $\varphi(x, y)$ — многочлен с целыми коэффициентами, то $\varphi(\alpha, \beta)$ — целое алгебраическое число.

В частности, если α и β — алгебраические числа (целые алгебраические числа), то $\alpha\beta$ и $\alpha \pm \beta$ тоже алгебраические числа (целые алгебраические числа). Кроме того, если $\alpha \neq 0$ — алгебраическое число, то α^{-1} тоже алгебраическое число. В самом деле, если α — корень многочлена $\sum a_k x^k$ степени n, то α^{-1} — корень многочлена $\sum a_k x^{n-k}$. Но если α — целое алгебраическое число, то число α^{-1} не обязательно целое алгебраическое. Таким образом, алгебраические числа образуют поле, а целые алгебраические числа образуют кольцо.

Теорема 20.2. Пусть α и β — алгебраические числа, связанные соотношением $\varphi(\alpha, \beta) = 0$, где φ — многочлен с рациональными коэффициентами. Тогда для любого числа α_i, сопряженного с α, найдется число β_j, сопряженное с β, для которого $\varphi(\alpha_i, \beta_j) = 0$.

Доказательство. Пусть $\{\alpha_1, \ldots, \alpha_n\}$ и $\{\beta_1, \ldots, \beta_m\}$ — наборы чисел, сопряженных с α и β соответственно. Рассмотрим многочлен

$$f(x) = \prod_{j=1}^{m} \varphi(x, \beta_j).$$

Коэффициенты этого многочлена рациональны и $f(\alpha) = 0$. Поэтому $f(x)$ делится на $\prod(x - \alpha_i)$, а значит, $f(\alpha_i) = 0$, т. е. $\varphi(\alpha_i, \beta_j) = 0$ для некоторого j. □

Теорема 20.3. Пусть α — корень многочлена

$$f(x) = x^n + \beta_{n-1}x^{n-1} + \ldots + \beta_0,$$

где $\beta_0, \ldots, \beta_{n-1}$ — целые алгебраические числа. Тогда α — целое алгебраическое число.

Доказательство. Рассмотрим многочлен

$$F(x) = \prod_{i,\ldots,l} (x^n + \beta_{n-1,i}x^{n-1} + \ldots + \beta_{0,l}),$$

где $\{\beta_{n-1,i}\}, \ldots, \{\beta_{0,l}\}$ — все числа, сопряженные с $\beta_{n-1}, \ldots, \beta_0$ соответственно. Легко проверить, что коэффициенты многочлена F — целые числа. Ясно также, что α — корень многочлена F. □

Алгебраическое число α называют *вполне вещественным*, если все сопряженные с ним числа вещественны. Иными словами, все корни неприводимого многочлена с корнем α вещественны.

Пример. Число $\alpha = 2\cos(k\pi/n)$ вполне вещественно.

В самом деле, $\alpha = \varepsilon + \varepsilon^{-1}$, где $\varepsilon = \exp(k\pi/n)$. Пусть число α_1 сопряжено с α. Из теоремы 20.2 следует, что $\alpha_1 = \varepsilon_1 + \varepsilon_1^{-1}$, где число ε_1 сопряжено с ε. Число ε удовлетворяет уравнению $x^n - 1 = 0$, поэтому ε_1 тоже будет корнем этого уравнения, а значит, $\varepsilon_1 = \exp(l\pi/n)$. В таком случае $\alpha_1 = 2\cos(l\pi/n) \in \mathbb{R}$.

20.2. Теорема Кронекера

В 1857 г. Кронекер [Kr] доказал следующее утверждение.

Теорема 20.4 (Кронекер). а) Пусть $\alpha \neq 0$ — целое алгебраическое число. Тогда если α — не корень из единицы, то абсолютная величина одного из чисел, сопряженных с α, строго больше 1.

б) Пусть β — вполне вещественное целое алгебраическое число. Тогда если $\beta \neq 2\cos r\pi$, $r \in \mathbb{Q}$, то абсолютная величина одного из чисел, сопряженных с β, строго больше 2.

Доказательство. а) Пусть $\{\alpha_1, \ldots, \alpha_n\}$ — набор чисел, сопряженных с α. Предположим, что $|\alpha_i| \leqslant 1$, $i = 1, \ldots, n$. Рассмотрим многочлен

$$f_k(x) = (x - \alpha_1^k) \cdot \ldots \cdot (x - \alpha_n^k) = x^n + a_{k,n-1}x^{n-1} + \ldots + a_{k,0}.$$

Из того, что α — целое алгебраическое число, следует, что $a_{k,n-1}, \ldots$ $\ldots, a_{k,0} \in \mathbb{Z}$. А из условия $|\alpha_i| \leqslant 1$, $i = 1, \ldots, n$ следует, что $|a_{k,s}| \leqslant \binom{n}{s}$. Таким образом, коэффициенты многочленов $f_1, f_2 \ldots$ принимают конечное число значений, поэтому среди многочленов $f_1, f_2 \ldots$ будет лишь конечное число различных многочленов. Но тогда множество корней этих многочленов конечно, а все числа $\alpha, \alpha^2, \alpha^3, \ldots$ входят в это множество. Следовательно, $\alpha^p = \alpha^q$, где $p, q \in \mathbb{N}$ и $p \neq q$. А так как $\alpha \neq 0$, то $\alpha^{p-q} = 1$.

б) Пусть $\{\beta_1, \ldots, \beta_n\}$ — набор чисел, сопряженных с β. По условию все они вещественные. Предположим, что $|\beta_i| \leqslant 2$, $i = 1, \ldots, n$. В таком случае модули всех чисел, сопряженных с

$$\alpha = \frac{\beta}{2} + \sqrt{\frac{\beta^2}{4} - 1},$$

будут равны 1. В самом деле, числа α и β связаны соотношением $\alpha^2 - -\beta\alpha + 1 = 0$, поэтому согласно теореме 20.2 любое число α_j, сопряженное с α, является корнем многочлена вида $\alpha_j^2 - \beta_i\alpha_j + 1 = 0$. Так как $|\beta_i| \leqslant 2$, то $\beta_i^2/4 \leqslant 1$, а значит,

$$|\alpha_j|^2 = \left(\frac{\beta_i^2}{2}\right) + 1 - \left(\frac{\beta_i^2}{2}\right) = 1.$$

Согласно теореме 20.3 число α целое алгебраическое. Поэтому к нему можно применить утверждение а). В результате получим, что $\alpha = e^{r\pi i}$, где $r \in \mathbb{Q}$. Поэтому

$$\beta = \alpha + \alpha^{-1} = \alpha + \overline{\alpha} = 2\cos r\pi,$$

что и требовалось. □

Приведем один интересный пример использования теоремы Кронекера.

Теорема 20.5 (Минковский). Пусть A — квадратная матрица с целочисленными элементами. Предположим, что все элементы матрицы $A - I$, где I — единичная матрица, делятся на некоторое натуральное число $n \geqslant 2$, но при этом $A \neq I$. Тогда:

а) если $n > 2$, то $A^m \neq I$ при всех натуральных m;

б) если $n = 2$ и при этом $A^2 \neq I$, то $A^m \neq I$ при всех натуральных m.

Доказательство. По условию $A = I + nB$, где B — матрица с целочисленными элементами. В частности, все собственные значения матрицы B являются целыми алгебраическими числами. Собственные значения α матрицы A и собственные значения β матрицы B связаны соотношением $\alpha = 1 + n\beta$.

Предположим, что $A^m = I$. Тогда $\alpha^m = 1$, а значит, $|\alpha| = 1$. Поэтому

$$|\beta| = \frac{|\alpha - 1|}{n} \leqslant \frac{2}{n} \leqslant 1. \tag{1}$$

Неравенство (1) строгое, за исключением лишь того случая, когда $n = 2$ и $|\alpha - 1| = 2$, т. е. $\alpha = -1$.

При $n > 2$ неравенство (1) строгое. В таком случае целое алгебраическое число β и все сопряженные с ним числа по модулю строго меньше 1. Следовательно, $\beta = 0$, а значит, $\alpha = 1$.

Равенство $A^m = I$ может выполняться лишь в том случае, когда все жордановы клетки матрицы A имеют размер 1×1. Если при этом все собственные значения матрицы A равны 1, то $A = I$.

Рассмотрим теперь случай $n = 2$. В этом случае $\alpha = \pm 1$. Следовательно, жорданова форма матрицы A представляет собой диагональную матрицу с элементами ± 1 на диагонали. Поэтому $A^2 = I$, что противоречит условию. □

Элементарные, но весьма громоздкие оценки позволяют доказать следующее уточнение теоремы Кронекера.

Теорема 20.6 [ScZ]. а) Пусть $\alpha \neq 0$ — целое алгебраическое число, причем α — не корень из единицы. Пусть, далее, $\{\alpha_1, \ldots, \alpha_n\}$ — набор сопряженных с ним чисел. Тогда если среди чисел $\alpha_1, \ldots, \alpha_n$ содержится $2s$ невещественных, то

$$\max_{1 \leqslant i \leqslant n} |\alpha_i| > 1 + 4^{-s-2}.$$

б) Пусть β — вполне вещественное целое алгебраическое число, причем $\beta \neq 2\cos r\pi$, $r \in \mathbb{Q}$. Пусть, далее, $\{\beta_1, \ldots, \beta_n\}$ — набор сопряженных с ним чисел. Тогда

$$\max_{1 \leqslant i \leqslant n} |\beta_i| > 2 + 4^{-2n-3}.$$

20.3. Теорема Лиувилля

Эйлер высказывал предположение, что не все числа являются алгебраическими, но доказать это ему не удалось. Впервые существование *трансцендентных* (т. е. не алгебраических) чисел доказал Лиувилль в 1844 г. А в 1874 г. Кантор показал, что трансцендентных чисел в некотором смысле даже больше, чем алгебраических. А именно, алгебраические числа образуют счетное множество, тогда как множество всех действительных (или комплексных) чисел несчетно.

Доказательство Лиувилля основано на достаточно простом, но важном замечании: иррациональное алгебраическое число не допускает слишком хорошего приближения рациональными числами. Точнее говоря, справедливо следующее утверждение.

Теорема 20.7 (Лиувилль). Пусть α — корень неприводимого многочлена $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, где $n \geqslant 2$. Тогда существует такое число $c > 0$ (зависящее только от α), что

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^n} \tag{1}$$

для любого целого p и натурального q.

Доказательство. Если $\left|\alpha - \frac{p}{q}\right| \geqslant 1$, то неравенство (1) выполняется при $c = 1$. Поэтому будем считать, что $\left|\alpha - \frac{p}{q}\right| < 1$. Запишем многочлен $f(x)$ в виде $f(x) = a_n \prod\limits_{i=1}^{n} (x - \alpha_i)$, где $\alpha_1 = \alpha$. Тогда

$$\left|f\left(\frac{p}{q}\right)\right| = |a_n| \cdot \left|\alpha - \frac{p}{q}\right| \cdot \prod_{i=2}^{n} \left|\frac{p}{q} - \alpha_i\right| \leqslant$$

$$\leqslant |a_n| \cdot \left|\alpha - \frac{p}{q}\right| \cdot \prod_{i=2}^{n} \left(|\alpha| + 1 + |\alpha_i|\right) = c_1 \left|\alpha - \frac{p}{q}\right|,$$

где c_1 — положительное число, зависящее только от $|a_n|$ и α.

Будем считать, что $a_0, \ldots, a_n$ — целые числа, взаимно простые в совокупности. Тогда число $|a_n|$ полностью определяется числом α. Кроме того, число

$$q^n f(p/q) = a_n p^n + a_{n-1} p^{n-1} + \ldots + a_0 q^n$$

целое, поэтому $|q^n f(p/q)| \geqslant 1$. Следовательно,

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{1}{c_1}\left|f\left(\frac{p}{q}\right)\right| \geqslant \frac{1}{c_1 q^n} = \frac{c}{q^n},$$

где $c = c_1^{-1}$. □

Теорема 20.8 (Лиувилль). Число $\alpha = \sum\limits_{k=0}^{\infty} 2^{-k!}$ трансцендентное.

Доказательство. Для каждого натурального n рассмотрим число $\alpha = \sum\limits_{k=0}^{n} 2^{-k!} = p/q$, где p — целое число и $q = 2^{n!}$. При этом

$$\left|\alpha - \frac{p}{q}\right| = \frac{1}{2^{(n+1)!}}\left(1 + \frac{1}{2^{n+2}} + \frac{1}{2^{(n+2)(n+3)}} + \ldots\right) < \frac{2}{2^{(n+1)!}} = \frac{2}{q^{n+1}}.$$

Предположим, что α — алгебраическое число степени N. Тогда согласно теореме 20.7

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{c}{q^N},$$

а значит, $2q^{-n-1} > cq^{-N}$, т. е. $c < 2q^{N-n-1} = 2 \cdot 2^{n!(N-n-1)}$. Но $\lim\limits_{n\to\infty} 2^{n!(N-n-1)} = 0$. Приходим к противоречию. □

Неравенство (1) можно записать в виде

$$|q\alpha - p| > c/q^{n-1}.$$

Положим $P(x) = qx - p$. Тогда

$$\bigl|P(\alpha)\bigr| > c/H^{n-1}, \tag{2}$$

где $H = \max\bigl\{|p|, |q|\bigr\}$ — высота многочлена P. Неравенство, аналогичное неравенству (2), выполняется и для многочлена P произвольной степени.

Теорема 20.9. Пусть α — алгебраическое число степени n. Тогда существует такое число $c > 0$ (зависящее лишь от α), что для любого многочлена P степени k с целыми коэффициентами либо выполняется равенство $P(\alpha) = 0$, либо выполняется неравенство

$$\bigl|P(\alpha)\bigr| > c^k/H^{n-1},$$

где H — высота многочлена P (т. е. наибольший из модулей коэффициентов многочлена P).

Доказательство. Пусть $P(x) = a_k x^k + \ldots + a_1 x + a_0$, где $a_i \in \mathbb{Z}$, и $P(\alpha) \neq 0$. Для некоторого натурального r число $\beta = r\alpha$ целое алгебраическое. Зададим многочлен Q соотношением $Q(rx) = r^k P(x)$. Ясно, что $Q(y) = r^k P(y/r) = a_k y^k + r a_{k-1} y^{k-1} + \ldots + r^k a_0$ — многочлен с целыми коэффициентами. Поэтому произведение $Q(\beta_1) \cdot \ldots \cdot Q(\beta_n)$, где $\beta_1, \ldots, \beta_n$ — все числа, сопряженные с β, является целым числом, отличным от нуля. Следовательно, $\bigl|Q(\beta)\bigr| \cdot \bigl|Q(\beta_2) \cdot \ldots \cdot Q(\beta_n)\bigr| \geqslant 1$, т. е.

$$r^{kn} \bigl|P(\alpha)\bigr| \cdot \bigl|P(\alpha_2) \cdot \ldots \cdot P(\alpha_n)\bigr| \geqslant 1. \tag{3}$$

С другой стороны,

$$\bigl|P(\alpha_i)\bigr| \leqslant H\bigl(1 + |\alpha_i| + \ldots + |\alpha_i|^k\bigr) \leqslant H\bigl(1 + |\alpha_i|\bigr)^k. \tag{4}$$

Пусть $h(\alpha) = \max\bigl\{|\alpha_1|, \ldots, |\alpha_n|\bigr\}$. Тогда из неравенств (3) и (4) следует, что

$$\bigl|P(\alpha)\bigr| \cdot H^{n-1} \Bigl(r^n \bigl(1 + h(\alpha)\bigr)^{n-1}\Bigr)^k \geqslant 1.$$

Положив $c = r^{-n}\bigl(1 + h(\alpha)\bigr)^{1-n}$, получаем требуемое неравенство. □

При $n = 2$ теорема Лиувилля неулучшаема в том смысле, что неравенство

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

имеет бесконечно много решений. Но при $n > 3$ оценку (1) последовательно улучшали Туэ, Зигель, Дайсон, Гельфонд, Шнейдер, Рот и др. Например, Рот [Rth] доказал следующее утверждение.

Теорема 20.10 (Рот). Пусть α — иррациональное алгебраическое число, а положительное число δ сколь угодно мало. Тогда неравенство

$$|\alpha - p/q| < q^{-2-\delta}$$

выполняется лишь для конечного числа пар q, p, где число q натуральное, а число p целое.

Доказательство теоремы Рота можно найти, например, в книге [K1].

Задачи к главе 4

4.1. Пусть $z_1, \ldots, z_n$ — вершины правильного n-угольника, z_0 — его центр. Доказать, что если P — многочлен степени не выше $n-1$, то $\frac{1}{n}\sum_{k=1}^{n} P(z_k) = P(z_0)$.

4.2. Пусть многочлен $P(x, y)$ таков, что $P(x, y) = P(x+1, y+1)$. Доказать, что этот многочлен имеет вид $P(x, y) = \sum a_k (x-y)^k$.

4.3. Пусть $f(x)$ — многочлен степени n без кратных корней, $x_1, \ldots, x_n$ — его корни. Доказать, что:

а) $\sum_{i=1}^{n} \frac{x_i^k}{f'(x_i)} = 0$ при $k = 0, 1, \ldots, n-2$; б) $\sum_{i=1}^{n} \frac{x_i^{n-1}}{f'(x_i)} = 1$.

4.4. Пусть $P(z)$ — многочлен степени n, причем $\max\limits_{|z|=1} |P(z)| \leqslant 1$. Доказать, что если $P(\alpha) = 0$, то $\max\limits_{|z|=1} \left|\frac{P(z)}{z-\alpha}\right| \leqslant \frac{n+1}{2}$ и $\max\limits_{|z|\leqslant 1} \left|\frac{P(z)}{z-\alpha}\right| \leqslant \frac{n}{1+|\alpha|}$.

4.5. Пусть $d = x^2 + ax + b \in \mathbb{Z}[x]$.

а) Доказать, что уравнение $p^2 - dq^2 = 1$ имеет нетривиальные решения $p, q \in \mathbb{Z}[x]$ в точности в следующих случаях:

(1) a нечетно и $4b = a^2 - 1$;

(2) a четно и $b = (a/2)^2 \pm 1$ или $b = (a/2)^2 \pm 2$.

б) Доказать, что уравнение $p^2 - dq^2 = -1$ имеет нетривиальные решения $p, q \in \mathbb{Z}[x]$ тогда и только тогда, когда a четно и $b = (a/2)^2 + 1$.

4.6. Доказать, что существует единственный с точностью до умножения на -1 многочлен $f(x)$ степени n, для которого функция $(x+1)\big(f(x)\big)^2 - 1$ нечетна.

4.7. Пусть $P_n(x)$ многочлен степени n над полем $\mathbb{C}$. Доказать, что при $n = 4$, 6 и 8 почти все многочлены $P_n(x)$ можно представить в следующем виде:

$$P_4 = u^4 + v^4 + \lambda u^2 v^2;$$
$$P_6 = u^6 + v^6 + w^6 + \lambda uvw(u-v)(v-w)(w-u);$$
$$P_8 = u^8 + v^8 + w^8 + z^8 \lambda u^2 v^2 w^2 z^2$$

(здесь u, v, w, z — линейные функции, λ — число).

4.8. Пусть числа $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ таковы, что для всех натуральных m число $\sum \alpha_i^m$ целое. Доказать, что все коэффициенты многочлена $\prod(x - \alpha_i)$ целые.

Глава 5
Теория Галуа

21. Теорема Лагранжа и резольвента Галуа

21.1. Теорема Лагранжа

Пусть K — поле характеристики 0 и φ — рациональная функция от переменных $x_1, \ldots, x_n$ над полем K. Функции φ можно сопоставить группу G_φ, состоящую из тех элементов σ группы S_n, которые оставляют φ без изменения, т. е.

$$\varphi(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \varphi(x_1, \ldots, x_n).$$

Например, если функция φ симметрическая, то $G_\varphi = S_n$, а если $\varphi = \sum a_i x_i$, где числа $a_1, \ldots, a_n$ попарно различны, то G_φ содержит только тождественную подстановку.

Теорема 21.1 (Лагранж). Пусть $\varphi, \psi \in K(x_1, \ldots, x_n)$, причем $G_\varphi \subset G_\psi$. Тогда $\psi = R(\varphi)$, где R — рациональная функция, коэффициентами которой служат симметрические функции от $x_1, \ldots, x_n$.

Первое доказательство. Разобьем группу G_ψ на смежные классы $h_1 G_\varphi = G_\varphi, h_2 G_\varphi, \ldots, h_k G_\varphi$. Каждому смежному классу $h_i G_\varphi$ соответствует функция φ_i — образ φ под действием данного смежного класса. При этом $\varphi_i \neq \varphi_j$ при $i \neq j$.

Функция ψ инвариантна относительно действия G_φ, поэтому смежному классу $h_i G_\varphi$ однозначно соответствует некоторая функция ψ_i (при $G_\varphi \neq G_\psi$ среди этих функций будут совпадающие).

Функция $\sum\limits_{i=1}^{k} \dfrac{\psi_i}{t - \varphi_i}$ инвариантна относительно действия всех подстановок группы S_n. Поэтому

$$\sum_{i=1}^{k} \frac{\psi_i}{t - \varphi_i} = \frac{F(t)}{\Omega(t)},$$

где $\Omega(t) = (t - \varphi_1) \cdot \ldots \cdot (t - \varphi_k)$ и $F(t)$ — многочлены от t, коэффициенты которых являются симметрическими функциями от $x_1, \ldots, x_n$. Из условия $\varphi_i \neq \varphi_j$ при $i \neq j$ следует, что $\Omega'(\varphi) \neq 0$.

Ясно, что

$$\lim_{t\to\varphi_i}\frac{\Omega(t)}{t-\varphi_i}=\lim_{t\to\varphi_i}\frac{\Omega(t)-\Omega(\varphi_i)}{t-\varphi_i}=\Omega'(\varphi_i).$$

Таким образом,

$$\lim_{t\to\varphi_i}\frac{\Omega(t)}{\Omega'(t)(t-\varphi_i)}=\begin{cases}0 & \text{при } \varphi_i\neq\varphi;\\ 1 & \text{при } \varphi_i=\varphi.\end{cases}$$

Поэтому

$$\frac{F(\varphi)}{\Omega'(\varphi)}=\sum_{i=1}^{k}\psi_i\frac{\Omega(\varphi)}{\Omega'(\varphi)(\varphi-\varphi_i)}=\psi. \qquad \square$$

Второе доказательство. Построим функции $\varphi_1=\varphi,\dots,\varphi_k$ и $\psi_1=\psi,\dots,\psi_k$, как и в первом доказательстве. Ясно, что

$$\sum\varphi_i^s\psi_i=T_s \tag{1}$$

— симметрическая функция от $x_1,\dots,x_n$. Рассмотрим равенства (1) при $s=0,\dots,k-1$ как систему линейных уравнений относительно $\psi_1,\dots,\psi_k$. Решая эту систему, получим $\psi_1=D_1/\Delta$, где

$$\Delta=\begin{vmatrix}1 & \dots & 1\\ \varphi_1 & \dots & \varphi_k\\ \vdots & \ddots & \vdots\\ \varphi_1^{k-1} & \dots & \varphi_k^{k-1}\end{vmatrix}\quad\text{и}\quad D_1=\begin{vmatrix}T_0 & 1 & \dots & 1\\ T_1 & \varphi_2 & \dots & \varphi_k\\ \vdots & \vdots & \ddots & \vdots\\ T_{k-1} & \varphi_2^{k-1} & \dots & \varphi_k^{k-1}\end{vmatrix}.$$

Запишем полученное равенство в виде $\psi_1=D_1\Delta/\Delta^2$. Ясно, что Δ^2 — симметрическая функция. При перестановке любой пары функций $\varphi_2,\dots,\varphi_k$ оба определителя D_1 и Δ меняют знак, поэтому $D_1\Delta$ — симметрическая функция от $\varphi_2,\dots,\varphi_k$. Следовательно, $D_1\Delta=S_0+{}+\varphi_1S_1+\dots+\varphi_1^{k-1}S_{k-1}$, где $S_0,\dots,S_{k-1}$ — симметрические многочлены от $\varphi_2,\dots,\varphi_k$. Поэтому $S_0,\dots,S_{k-1}$ выражаются через

$$\begin{aligned}\sigma_1'&=\varphi_2+\dots+\varphi_k,\\ \sigma_2'&=\varphi_2\varphi_3+\dots,\\ &\dots\dots\dots\dots\\ \sigma_{k-1}'&=\varphi_2\cdot\ldots\cdot\varphi_k.\end{aligned}$$

Но, как легко проверить,

$$\begin{aligned}
\sigma_1' &= \sigma_1 - \varphi_1,\\
\sigma_2' &= \sigma_2 - \varphi_1\sigma_1 + \varphi_1^2,\\
\sigma_3' &= \sigma_3 - \varphi_1\sigma_2 + \varphi_1^2\sigma_1 - \varphi_1^3,\\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

где $\sigma_1, \sigma_2, \ldots$ — элементарные симметрические функции от $\varphi_1, \ldots, \varphi_k$. Поэтому $\sigma_1', \ldots, \sigma_{k-1}'$ выражаются через $\sigma_1, \ldots, \sigma_{k-1}$ и φ_1. Таким образом, $D_1\Delta$ — многочлен от $\varphi_1 = \varphi$, коэффициентами которого служат симметрические функции от $x_1, \ldots, x_n$. □

Из теоремы Лагранжа можно извлечь многочисленные следствия. Пусть φ и ψ — рациональные функции от переменных $x_1, \ldots, x_n$. Если $\psi = R(\varphi)$, где R — рациональная функция, коэффициентами которой служат симметрические функции от $x_1, \ldots, x_n$, то будем для краткости говорить, что ψ *рационально выражается* через φ.

Следствие 1. Любая рациональная функция от переменных $x_1, \ldots, x_n$ рационально выражается через $a_1x_1 + \ldots + a_nx_n$, где $a_1, \ldots, a_n$ — попарно различные числа.

Следствие 2. Если $G_\varphi = G_\psi$, то функции φ и ψ рационально выражаются друг через друга.

Следствие 3. Если рациональная функция r инвариантна относительно всех подстановок, сохраняющих функции $r_1, \ldots, r_n$, то r рационально выражается через $r_1, \ldots, r_n$.

Доказательство. Можно считать, что функции $r_1, \ldots, r_n$ линейно независимы. Пусть $\varphi = a_1r_1 + \ldots + a_nr_n$, где $a_1, \ldots, a_n$ — попарно различные числа. Тогда любая подстановка, сохраняющая φ, должна сохранять и все функции $r_1, \ldots, r_n$. Поэтому r сохраняется при всех подстановках, сохраняющих φ. Следовательно, r рационально выражается через $\varphi = a_1r_1 + \ldots + a_nr_n$. □

Следствие 4. Пусть многочлен $f(x_1, \ldots, x_n)$ при всевозможных подстановках переменных принимает лишь два различных значения. Тогда

$$f = S_1 + \Delta S_2,$$

где S_1 и S_2 — симметрические функции, а $\Delta = \prod\limits_{i<j}(x_i - x_j)$.

Доказательство. Если f — не симметрическая функция, то подстановки, сохраняющие f, образуют в S_n подгруппу индекса 2. Поэтому достаточно доказать, что в S_n есть лишь одна подгруппа индекса 2, а именно, знакопеременная группа A_n. Пусть $G \subset S_n$ — подгруппа индекса 2 и $h \in S_n \setminus G$. Тогда S_n разбивается на непересекающиеся множества G и $hG = Gh$. Поэтому $hGh^{-1} = G$ и если $h_1, h_2 \in S_n \setminus G$, то $h_1h_2 \in G$. Если бы группа G содержала некоторую транспозицию (ij), то она содержала бы и любую другую транспозицию (pq). В самом деле, (pq) получается из (ij) при сопряжении любой подстановкой, переводящей i в p и j в q. Таким образом, все транспозиции лежат в $S_n \setminus G$, а значит, их попарные произведения лежат в G. Итак, в G лежат все произведения четного числа транспозиций, а значит, $G \supset A_n$. Но $|G| = |A_n|$, поэтому $G = A_n$. □

В теореме Лагранжа речь идет о рациональных функциях от переменных $x_1, \ldots, x_n$. Переход от алгебраически независимых $x_1, \ldots, x_n$ к конкретным значениям этих переменных требует определенной деликатности. Дело в том, что подстановки, сохраняющие значение функции $\varphi(x_1, \ldots, x_n)$ при заданных $x_1, \ldots, x_n$, могут не образовывать группу. Пусть, например, $x_k = \exp(2\pi ik/7)$, $k = 1, \ldots, 6$. Рассмотрим функцию $f(x_1, \ldots, x_6) = x_1x_6$. Пусть $\sigma = (12)(56)$ и $\tau = (16)(23)$. Подстановки σ и τ переводят f в $\sigma f = x_2x_5 = 1$ и $\tau f = x_6x_1 = 1$, соответственно, т. е. σ и τ сохраняют f. Но τ переводит $\sigma f = x_2x_5$ в $\tau\sigma f = x_3x_5 \neq 1$.

Чтобы избежать подобных неприятностей, Галуа предложил рассматривать не все подстановки корней уравнения, а лишь те, которые сохраняют все рациональные соотношения между ними. Точнее говоря, пусть $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ — многочлен с коэффициентами из поля K и $\alpha_1, \ldots, \alpha_n$ — его корни. Будем рассматривать такие подстановки σ, что для любой рациональной функции $r \in K(x_1, \ldots, x_n)$ из равенства $r(\alpha_1, \ldots, \alpha_n) = 0$ следует равенство $r(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$. На современном языке это означает, что подстановка σ соответствует автоморфизму поля $K(\alpha_1, \ldots, \alpha_n)$, сохраняющему основное поле K. Группу всех таких подстановок называют *группой Галуа* многочлена f. (Эта группа, разумеется, зависит от поля K.)

В рассмотренном выше примере подстановки σ и τ не входят в группу Галуа многочлена $x^6 + x^5 + \ldots + x + 1$, корнями которого являются $x_1, \ldots, x_6$. В самом деле, подстановки σ и τ не сохраняют, например, соотношения $x_2 = x_1^2$ и $x_6 = x_1^6$.

Для любой рациональной функции от корней $\alpha_1, \ldots, \alpha_n$ многочлена f можно рассмотреть те подстановки из группы Галуа, которые сохраня-

ют ее значение. Ясно, что эти подстановки теперь уже образуют группу. В самом деле, пусть σ и τ — подстановки из группы Галуа многочлена f, а $r(x_1, \ldots, x_n)$ — такая рациональная функция, что

$$r(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = r(\alpha_1, \ldots, \alpha_n), \tag{2}$$

$$r(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) = r(\alpha_1, \ldots, \alpha_n). \tag{3}$$

Подстановки σ и τ можно применять к любым рациональным соотношениям между корнями $\alpha_1, \ldots, \alpha_n$, поэтому, применив τ к соотношению (2), получим

$$r(\alpha_{\tau\sigma(1)}, \ldots, \alpha_{\tau\sigma(n)}) = r(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}).$$

Теперь из соотношения (3) следует, что подстановка $\tau\sigma$ тоже сохраняет значение функции r.

21.2. Резольвента Галуа

Пусть $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ — многочлен над полем K нулевой характеристики и $\alpha_1, \ldots, \alpha_n$ — его корни. Предположим, что у многочлена f нет кратных корней, т. е. числа $\alpha_1, \ldots, \alpha_n$. попарно различны. Рассмотрим рациональную функцию

$$\psi(x_1, \ldots, x_n) = m_1x_1 + \ldots + m_nx_n,$$

где $m_1, \ldots, m_n$ — некоторые целые числа. Покажем, что числа $m_1, \ldots$ $\ldots, m_n$ можно выбрать так, что все $n!$ значений $\psi_\sigma = \psi(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ будут различны. В самом деле, рассмотрим функцию

$$D(t_1, \ldots, t_n) = \prod_{\sigma,\tau} \sum_{i=1}^{n} t_i(\alpha_{\sigma(i)} - \alpha_{\tau(i)}),$$

где произведение берется по всем неупорядоченным парам несовпадающих подстановок σ и τ. Функция D представляет собой произведение ненулевых многочленов от $t_1, \ldots, t_n$, поэтому D — ненулевой многочлен над полем K от переменных $t_1, \ldots, t_n$. Но любой ненулевой многочлен принимает ненулевое значение при некоторых целых значениях $t_1 = m_1, \ldots, t_n = m_n$. Эти целые числа $m_1, \ldots, m_n$ и есть искомые.

Прежде чем двигаться дальше, докажем одно вспомогательное утверждение.

Лемма. Любой симметрический многочлен от корней $\alpha_2, \ldots, \alpha_n$ полиномиально выражается через корень α_1 и коэффициенты $a_0, \ldots, a_{n-1}$.

Доказательство. Любой симметрический многочлен от корней $\alpha_2, \ldots, \alpha_n$ выражается через коэффициенты многочлена

$$(x-\alpha_2)\cdot\ldots\cdot(x-\alpha_n) = f(x)/(x-\alpha_1) = x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_0.$$

При этом

$$\begin{aligned} a_{n-1} &= b_{n-2} - \alpha_1, \\ a_{n-2} &= b_{n-3} - b_{n-2}\alpha_1, \\ a_{n-3} &= b_{n-4} - b_{n-3}\alpha_1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

т. е.

$$\begin{aligned} b_{n-2} &= a_{n-1} + \alpha_1, \\ b_{n-3} &= a_{n-2} + \alpha_1 a_{n-1} + \alpha_1^2, \\ b_{n-4} &= a_{n-3} + \alpha_1 a_{n-2} + \alpha_1^2 a_{n-1} + \alpha_1^3, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Таким образом, коэффициенты $b_0, \ldots, b_{n-2}$ полиномиально выражаются через корень α_1 и коэффициенты $a_0, \ldots, a_{n-1}$. □

Выберем числа $m_1, \ldots, m_n$ так, что все $n!$ значений

$$\psi_\sigma = m_1\alpha_{\sigma(1)} + \ldots + m_n\alpha_{\sigma(n)}$$

были бы различны, и рассмотрим многочлен

$$F(x) = \prod_{\sigma\in S_n} (x - m_1\alpha_{\sigma(1)} - \ldots - m_n\alpha_{\sigma(n)}).$$

Коэффициенты этого многочлена — симметрические многочлены с целыми коэффициентами от корней многочлена f, поэтому они рационально выражаются через коэффициенты многочлена f. Таким образом, если f — многочлен над полем K, то F тоже будет многочленом над полем K.

Разложим F в произведение неприводимых над K множителей со старшим коэффициентом 1. Любой такой неприводимый множитель G называют *резольвентой Галуа* многочлена f; для определенности будем считать, что многочлен G имеет корень $m_1\alpha_1 + \ldots + m_n\alpha_n$.

Теорема 21.2 (Галуа). Любой корень многочлена f рационально выражается (над полем K) через один из корней многочлена G.

Доказательство. Рассмотрим многочлен

$$F_1(x) = \prod(x - m_1\alpha_1 - m_2\alpha_{\sigma(2)} - \ldots - m_n\alpha_{\sigma(n)}),$$

где произведение берется по подстановкам $\sigma \in S_n$, для которых $\sigma(1) = 1$. Коэффициенты многочлена F_1 являются симметрическими многочленами от $\alpha_2, \ldots, \alpha_n$, поэтому согласно лемме они рационально выражаются (над полем K) через α_1, т. е. $F_1(x) = g(x, \alpha_1)$, где g — многочлен от двух переменных над полем K. При этом если $\psi = m_1\alpha_1 + \ldots + m_n\alpha_n$, то $g(\psi, \alpha_1) = F_1(\psi) = 0$.

Рассмотрим теперь многочлен

$$F_2(x) = \prod(x - m_1\alpha_2 - m_2\alpha_{\sigma(1)} - \ldots - m_n\alpha_{\sigma(n)}),$$

где произведение берется по подстановкам $\sigma \in S_n$, для которых $\sigma(2) = 2$. Из доказательства леммы видно, что выражения для его коэффициентов будут теми же самыми, что и для F_1, с точностью до замены α_1 на α_2, т. е. $F_2(x) = g(x, \alpha_2)$.

По условию $\psi = m_1\alpha_1 + \ldots + m_n\alpha_n \neq m_1\alpha_2 + m_2\alpha_{\sigma(1)} + \ldots + m_n\alpha_{\sigma(n)}$, т. е. $F_2(\psi) \neq 0$. Таким образом, α_1 является единственным общим корнем многочленов $f(x)$ и $g(\psi, x)$. Это означает, что НОД многочленов $f(x)$ и $g(\psi, x)$ равен $x - \alpha_1$. Но НОД двух многочленов находится по алгоритму Евклида, поэтому α_1 рационально выражается через ψ и коэффициенты многочленов f и g, т. е. α_1 рационально выражается над полем K через ψ. □

Следствие. Все корни резольвенты Галуа рационально выражаются через один из ее корней.

Доказательство. Каждый корень резольвенты Галуа имеет вид $m_1\alpha_{\sigma(1)} + \ldots + m_n\alpha_{\sigma(n)}$. Ясно, что они рационально выражаются через $\alpha_1, \ldots, \alpha_n$. В свою очередь, $\alpha_1, \ldots, \alpha_n$ рационально выражаются через $\psi = m_1\alpha_1 + \ldots + m_n\alpha_n$. □

С помощью резольвенты Галуа удобно строить поле разложения $K(\alpha_1, \ldots, \alpha_n)$. В самом деле, $K(\alpha_1, \ldots, \alpha_n) = K(\psi)$, т. е. вместо присоединения к полю K всех корней многочлена можно присоединить один корень его резольвенты Галуа.

Другое применение резольвенты связано с тем, что с ее помощью можно построить группу Галуа. (Первоначально Галуа строил группу Галуа многочлена именно с помощью резольвенты.)

Пусть $\psi_1 = \psi, \psi_2, \ldots, \psi_r$ — корни резольвенты Галуа G. Как было показано, все они рационально выражаются через ψ, т. е. $\psi_i = R_i(\psi)$, где $R_i \in K(x)$. Соотношение $\psi_i = R_i(\psi)$ можно рассматривать как соотношение между элементами поля $K(\psi)$. Поэтому можно считать, что R_i — многочлен степени не выше $\deg G - 1 = r - 1$. Этот многочлен определен однозначно. Формула $\psi_i = R_i(\psi)$ остается справедливой, если R_i заменить на $R_i + aG$, где a — произвольный многочлен.

Рассмотрим многочлены $G(x)$ и $G_i(x) = G\big(R_i(x)\big)$. Коэффициенты этих многочленов лежат в K и у них есть общий корень ψ. А так как по условию многочлен G неприводим, то любой корень ψ_j многочлена G является также корнем многочлена G_i, т. е. $R_i(\psi_j) = \psi_p$ для некоторого p. Это означает, что $R_i\big(R_j(\psi)\big) = R_p(\psi)$, т. е. $R_iR_j \equiv R_p \pmod G$. Таким образом, для любого корня ψ_s многочлена G выполняется равенство $R_i\big(R_j(\psi_s)\big) = R_p(\psi_s)$. В частности, набор многочленов $R_1, \ldots, R_r$ и соответствующих им преобразований корней $\psi_1 \ldots, \psi_r$ определен инвариантно, т. е. он не зависит от выбора корня ψ_1.

Числу $\psi_i = m_1\alpha_{\sigma_i(1)} + \ldots + m_n\alpha_{\sigma_i(n)}$ однозначно соответствует подстановка σ_i, а ей, в свою очередь, соответствует автоморфизм поля $K(\alpha_1, \ldots, \alpha_n) = K(\psi)$, который мы тоже обозначим σ_i. Итак, корням $\psi_1, \ldots, \psi_r$ резольвенты Галуа соответствуют подстановки $\sigma_1, \ldots, \sigma_r$. Сопоставим подстановке σ_i многочлен R_i. Учитывая, что $\sigma_i(\psi) = \psi_i$, получаем

$$\sigma_i\sigma_j(\psi) = \sigma_i(\psi_j) = \sigma_iR_j(\psi) = R_j(\psi_i) = R_j\big(R_i(\psi)\big),$$

т. е. $\sigma_i\sigma_j \leftrightarrow R_jR_i \bmod G$. Таким образом, группа преобразований $R_1, \ldots, R_r$ антиизоморфна группе подстановок $\sigma_1, \ldots, \sigma_r$. Чтобы установить связь с группой Галуа, остается доказать следующее утверждение.

Теорема 21.3. Группа Галуа многочлена f состоит из подстановок $\sigma_1, \ldots, \sigma_r$.

Доказательство. Требуется доказать, что если $\alpha_1, \ldots, \alpha_n$ — корни многочлена f и $\tau \in S_n$, то условие $\tau \in \{\sigma_1, \ldots, \sigma_r\}$ эквивалентно тому, что для любой рациональной функции φ равенство $\varphi(\alpha_1, \ldots, \alpha_n) = 0$ эквивалентно равенству $\varphi(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) = 0$.

Корни $\alpha_1, \ldots, \alpha_n$ рационально выражаются через ψ_1, поэтому

$$\varphi(\alpha_1, \ldots, \alpha_n) = \Phi(\psi_1) = \Phi(m_1\alpha_1 + \ldots + m_n\alpha_n),$$

где $\Phi \in K(x)$. Таким образом, $\varphi(\alpha_{\tau(1)}, \ldots, \alpha_{\tau(n)}) = \Phi(\widetilde{\psi}_\tau)$, где $\widetilde{\psi}_\tau = m_1\alpha_{\tau(1)} + \ldots + m_n\alpha_{\tau(n)}$. Эквивалентность равенств $\Phi(\psi_1) = 0$ и

$\Phi(\widetilde{\psi}_\tau) = 0$ (для всевозможных рациональных функций Φ) означает, что ψ_1 и $\widetilde{\psi}_\tau$ — корни одного и того же неприводимого многочлена, т. е. $\tau \in \{\sigma_1, \ldots, \sigma_r\}$. □

Следствие. Пусть f — многочлен над полем k с попарно различными корнями $\alpha_1, \ldots, \alpha_n$. Тогда порядок группы Галуа этого многочлена равен степени расширения $[K : k]$, где $K = k(\alpha_1, \ldots, \alpha_n)$.

Доказательство. Оба эти числа равны степени резольвенты Галуа многочлена f. □

Для теории Галуа большое значение имеет следующее утверждение.

Теорема 21.4. Пусть $\alpha_1, \ldots, \alpha_n$ — корни неприводимого многочлена f над полем k и $\varphi \in k(x_1, \ldots, x_n)$.

а) Предположим, что $\varphi(\alpha_1, \ldots, \alpha_n) = \varphi(\alpha_{\sigma_i(1)}, \ldots, \alpha_{\sigma_i(n)})$ для всех подстановок σ_i из группы Галуа. Тогда $\varphi(\alpha_1, \ldots, \alpha_n) \in k$.

б) Пусть $H = \{\sigma_{i_1}, \ldots, \sigma_{i_s}\}$ — такая подгруппа группы Галуа $\{\sigma_1, \ldots, \sigma_r\}$, что если $\varphi(\alpha_1, \ldots, \alpha_n) = \varphi(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ для любой подстановки $\sigma \in H$, то $\varphi(\alpha_1, \ldots, \alpha_n) \in k$. Тогда H совпадает со всей группой Галуа.

Доказательство. а) Корни $\alpha_1, \ldots, \alpha_n$ рационально выражаются через ψ_1, поэтому $\varphi(\alpha_1, \ldots, \alpha_n) = \Phi(\psi_1)$, где $\Phi \in k(x)$. Следовательно, $\varphi(\alpha_{\sigma_i(1)}, \ldots, \alpha_{\sigma_i(n)}) = \Phi(\psi_i)$. Таким образом, $\Phi(\psi_1) = \ldots = \Phi(\psi_r)$, а значит,

$$\Phi(\psi_1) = \frac{1}{r}\big(\Phi(\psi_1) + \ldots + \Phi(\psi_r)\big)$$

— рациональная симметрическая функция от корней $\psi_1, \ldots, \psi_r$ резольвенты Галуа. Поэтому $\varphi(\alpha_1, \ldots, \alpha_n) = \Phi(\psi_1) \in k$.

б) Рассмотрим многочлен

$$g(x) = \prod_{\sigma \in H} \big(x - \sigma(\psi)\big) = (x - \psi_{i_1}) \cdot \ldots \cdot (x - \psi_{i_s}).$$

Его коэффициенты инвариантны относительно действия группы H, поэтому все они лежат в k. Таким образом, коэффициенты многочлена $g(x)$ лежат в k и этот многочлен имеет общие корни с неприводимым над k многочленом $G(x) = (x - \psi_1) \cdot \ldots \cdot (x - \psi_r)$. Следовательно, $g(x) = G(x)$ и $H = \{\sigma_1, \ldots, \sigma_r\}$. □

21.3. Теорема о примитивном элементе

На с. 209 мы упомянули, что поле $k(\alpha_1, \ldots, \alpha_n)$, где $\alpha_1, \ldots, \alpha_n$ — корни многочлена f, порождено над k одним элементом, а именно, корнем ψ резольвенты Галуа многочлена f. Обычно в теории полей для построения элемента, порождающего поле, используется следующая стандартная конструкция.

Теорема 21.5 (о примитивном элементе). Пусть k — поле нулевой характеристики, $\alpha_1, \ldots, \alpha_n$ — алгебраические над k элементы. Тогда поле $k(\alpha_1, \ldots, \alpha_n)$ порождено над k одним элементом θ.

Доказательство. Рассмотрим сначала случай двух элементов α и β. Пусть $f(x)$ и $g(x)$ — неприводимые над k многочлены с корнями α и β. Пусть, далее, $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ — корни многочлена f, $\beta_1 = \beta$, $\beta_2, \ldots, \beta_s$ — корни многочлена g. Выберем $c \in k$ так, что $\alpha_i + c\beta_j \neq \alpha_1 + c\beta_1$ при $j \neq 1$. Положим $\theta = \alpha_1 + c\beta_1 = \alpha + c\beta$. Ясно, что $k(\theta) \subset k(\alpha, \beta)$. Остается доказать, что $k(\alpha, \beta) \subset k(\theta)$. Для этого достаточно доказать, что $\beta \in k(\theta)$. Действительно, в таком случае $\alpha = \theta - c\beta \in k(\theta)$.

Элемент β удовлетворяет уравнениям $g(x) = 0$ и $f(\theta - cx) = 0$, коэффициенты которых лежат в $k(\theta)$. Единственным общим корнем многочленов $g(x)$ и $f(\theta - cx)$ является β, поскольку $\theta - c\beta_j \neq \alpha_i$ при $j \neq 1$. У многочлена $g(x)$ кратных корней нет, поэтому наибольший общий делитель многочленов $g(x)$ и $f(\theta - cx)$ равен $x - \beta$. Наибольший общий делитель двух многочленов над полем $k(\theta)$ является многочленом над $k(\theta)$, поэтому $\beta \in k(\theta)$.

Переход от $n = 2$ к произвольному n делается очевидной индукцией: если $k(\alpha_1, \ldots, \alpha_{n-1}) = k(\theta)$, то $k(\alpha_1, \ldots, \alpha_n) = k(\theta, \alpha_n) = k(\theta')$. □

С помощью теоремы о примитивном элементе можно доказать, например, следующее утверждение о простых делителях набора многочленов.

Теорема 21.6 [Но]. Пусть $f_1(x), \ldots, f_n(x)$ — непостоянные целозначные многочлены, т. е. $f_i(m) \in \mathbb{Z}$ при $m \in \mathbb{Z}$. Пусть, далее, M_i — множество всех простых делителей всех чисел вида $f_i(m) \in \mathbb{Z}$, $m \in \mathbb{Z}$ ($f_i(m) \neq 0$). Тогда множество $M = M_1 \cap \ldots \cap M_n$ бесконечно.

Доказательство. Рассмотрим сначала случай $n = 1$ (в этом случае теорема была доказана Шуром [Shu]). Если $f_1(x)$ — целозначный многочлен степени k, то все коэффициенты многочлена $k! f_1(x)$ целые (см. теорему 12.1 на с. 100). При переходе от многочлена f_1 к многочлену

$k!f_1$ к простым делителям значений многочлена f_1 добавляются лишь простые делители числа $k!$, т. е. некоторое конечное множество. Таким образом, доказательство достаточно провести в случае многочлена f_1 с целыми коэффициентами.

Многочлен $f_1(x)$ принимает значения 0 и ± 1 лишь в конечном числе точек. Поэтому у его значений в целых точках есть хотя бы один простой делитель, т. е. $M_1 \neq \varnothing$. Предположим, что $M_1 = \{p_1, \ldots, p_r\}$ — конечное множество.

Пусть $a \in \mathbb{Z}$ и $f_1(a) = b \neq 0$. Покажем, что

$$g(x) = b^{-1} f_1(a + bp_1 \cdot \ldots \cdot p_r x)$$

— многочлен с целыми коэффициентами, причем $g(x) \equiv 1 \pmod{p_1 \cdot \ldots \cdot p_r}$ при $x \in \mathbb{Z}$. Легко проверить, что если $c \in \mathbb{Z}$, то $(a + cx)^l - a^l = ch_l(x)$, где $h_l(x)$ — многочлен с целыми коэффициентами. Поэтому

$$f_1(a + bp_1 \cdot \ldots \cdot p_r x) - f_1(a) = bp_1 \cdot \ldots \cdot p_r h(x),$$

где $h(x)$ — многочлен с целыми коэффициентами. Остается заметить, что

$$g(x) = b^{-1}\big(f_1(a) + bp_1 \cdot \ldots \cdot p_r h(x)\big) = 1 + p_1 \cdot \ldots \cdot p_r h(x).$$

Для некоторого $x \in \mathbb{Z}$ у целого числа $g(x)$ есть простой делитель p. Сравнение $g(x) \equiv 1 \pmod{p_1 \cdot \ldots \cdot p_r}$ показывает, что $p \notin M_1 = \{p_1, \ldots, p_r\}$. С другой стороны, число $f_1(a + bp_1 \cdot \ldots \cdot p_r x) = bg(x)$ делится на p, поэтому $p \in M_1$. Полученное противоречие означает, что множество M_1 бесконечно.

Переход от случая $n = 1$ к произвольному n делается с помощью теоремы о примитивном элементе. Как и при доказательстве в случае $n = 1$, мы будем считать, что $f_1, \ldots, f_n \in \mathbb{Z}[x]$. Пусть α_i — один из корней многочлена f_i. Согласно теореме о примитивном элементе $\mathbb{Q}(\alpha_1, \ldots, \alpha_n) = \mathbb{Q}(\alpha)$, т. е. $\alpha_i = \varphi_i(\alpha)$, где $\varphi_i(t) \in \mathbb{Q}[t]$. Пусть g — неприводимый многочлен над $\mathbb{Q}$, имеющий корень α. Если $\varphi_i(0) \neq 0$, то заменим φ_i на $\widetilde{\varphi}_i$, где

$$\widetilde{\varphi}_i(t) = \varphi_i(t) - \frac{\varphi_i(0)}{g(0)} g(t).$$

Итак, можно считать, что $\varphi_i(0) = 0$. В таком случае, если N делится на знаменатели всех коэффициентов многочленов φ_i, то $\varphi_i(Nt) \in \mathbb{Z}[t]$.

Многочлены $f_1\big(\varphi_1(t)\big), \ldots, f_n\big(\varphi_n(t)\big) \in \mathbb{Q}[t]$ имеют общий корень α, поэтому все они делятся на $g(t)$. Рассмотрим многочлены $F_i(t) = f_i\big(\varphi_i(Nt)\big)$. Ясно, что $F_i(t) \in \mathbb{Z}[x]$ и $F_i(t)$ делится над $\mathbb{Q}$ на $g(Nt)$,

т. е. $F_i(t) = g(Nt)g_i(t)$, где $g_i(t) \in \mathbb{Q}[t]$. Запишем многочлены g и g_i в виде $g(Nt) = rh(t)$ и $g_i(t) = s_i h_i(t)$, где $r, s_i \in \mathbb{Q}$, $h(t), h_i(t) \in \mathbb{Z}[t]$ и $\operatorname{cont}(h) = \operatorname{cont}(h_i) = 1$. Тогда $F_i(t) = rs_i h(t)h_i(t)$, причем согласно лемме Гаусса $rs_i = \operatorname{cont}(F_i)$ — целое число. Это означает, что $F_i(t)$ делится над $\mathbb{Z}$ на $h(t)$. В частности, все делители значений многочлена h в целых точках являются делителями значений многочлена F_i, которые, в свою очередь, являются делителями значений многочлена f_i. Таким образом, множество M содержит бесконечное подмножество, состоящее из простых делителей значений многочлена h. □

22. Основы теории Галуа

22.1. Соответствие Галуа

Пусть f — многочлен над полем k без кратных корней (но не обязательно неприводимый), $\alpha_1, \ldots, \alpha_n$ — корни многочлена f. Поле $K = k(\alpha_1, \ldots, \alpha_n)$ называют *полем разложения* многочлена f.

Теорема 22.1. Любой элемент $\omega \in K = k(\alpha_1, \ldots, \alpha_n)$ является корнем неприводимого над k многочлена h, все корни которого лежат в K.

Доказательство. Элемент ω можно представить в виде $\omega = g(\alpha_1, \ldots, \alpha_n)$, где $g \in k[x_1, \ldots, x_n]$. Положим $\omega_\sigma = g(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ и рассмотрим многочлен $h(x) = \prod\limits_{\sigma \in S_n} (x - \omega_\sigma)$. Ясно, что все корни многочлена h лежат в K и h — многочлен над полем k, поэтому ω — корень неприводимого множителя многочлена h. □

Следствие. Если многочлен $p(x)$ неприводим над k и один из его корней лежит в $K = k(\alpha_1, \ldots, \alpha_n)$, то и все остальные корни многочлена $p(x)$ лежат в K.

Доказательство. Пусть $\omega \in K$ — корень многочлена p, h — неприводимый над k многочлен, все корни которого лежат в K и $h(\omega) = 0$. Многочлены h и p неприводимы над k и имеют общий корень ω, поэтому все корни многочлена p являются корнями многочлена h, т. е. лежат в K. □

Конечное расширение K поля k называют *нормальным расширением*, или *расширением Галуа*, если любой неприводимый над k многочлен, один из корней которого лежит в K, разлагается над K на линейные множители, т. е. все его корни лежат в K.

Примером не нормального расширения служит поле $\mathbb{Q}(\sqrt[3]{2})$: это поле содержит лишь один из корней многочлена $x^3 - 2$.

Согласно теореме 22.1 поле разложения многочлена является нормальным расширением. Справедливо и обратное утверждение.

Теорема 22.2. Пусть $K \supset k$ — нормальное расширение. Тогда K — поле разложения некоторого многочлена над k.

Доказательство. Пусть $K = k(\alpha_1, \ldots, \alpha_n)$, f_i — неприводимый многочлен над k с корнем α_i, $f = f_1 \ldots f_n$, K' — поле разложения многочлена f над k. С одной стороны, элементы $\alpha_1, \ldots, \alpha_n$ являются корнями многочлена f, поэтому $K \subset K'$. С другой стороны, поле K нормально над k и содержит корень неприводимого над k многочлена f_i ($i = 1, \ldots, n$), поэтому K содержит все корни многочлена f, а значит, $K \supset K'$. □

Следствие. Пусть $K \supset L \supset k$, где K — нормальное расширение поля k, L — произвольное промежуточное поле. Тогда K — нормальное расширение поля L.

Доказательство. Поле K является полем разложения некоторого многочлена f над k. Этот многочлен можно рассмотреть и как многочлен над L, поэтому K — поле разложения некоторого многочлена над L, т. е. K — нормальное расширение поля L. □

Если K — нормальное расширение поля k, то *группой Галуа* поля K над k называют группу автоморфизмов поля K, оставляющих неподвижными все элементы поля k. Группу Галуа поля K над k будем обозначать $G(K, k)$. В том случае, когда K — поле разложения многочлена f, для группы Галуа $G(K, k)$ будем также использовать обозначение $G_k(f)$.

Элементы ω, ω' поля $K \supset k$ называют *сопряженными над полем* k, если ω и ω' — корни одного и того же неприводимого над k многочлена.

Теорема 22.3. Пусть K — нормальное расширения поля k. Элементы $\omega, \omega' \in K$ сопряжены над k тогда и только тогда, когда существует автоморфизм $\sigma \in G(K, k)$, переводящий ω в ω'.

Доказательство. Пусть ω — корень неприводимого над k многочлена p. Если $\omega' = \sigma(\omega)$, то $p(\omega') = p\big(\sigma(\omega)\big) = \sigma\big(p(\omega)\big) = 0$, поэтому элементы ω и ω' сопряжены над k.

Предположим теперь, что ω и ω' — корни неприводимого над k многочлена p. Построение автоморфизма σ начнем с того, что построим изоморфизм $\varphi\colon k(\omega) \to k(\omega')$. Любой элемент поля $k(\omega)$ однозначно представим в виде $a_0 + a_1\omega + \ldots + a_{n-1}\omega^{n-1}$, где $a_i \in k$ и $n = \deg p$. Требуемый автоморфизм имеет вид $\sum\limits_{i=0}^{n-1} a_i\omega^i \mapsto \sum\limits_{i=0}^{n-1} a_i(\omega')^i$. Выберем теперь $\theta \in K \setminus k(\omega)$. Пусть p_1 — неприводимый над k многочлен с корнем θ, а q_1 — неприводимый над $k(\omega)$ делитель многочлена p_1, для которого $q_1(\theta) = 0$. При изоморфизме $\varphi\colon k(\omega) \to k(\omega')$ неприводимый над $k(\omega)$ многочлен q_1 переходит в неприводимый над $k(\omega')$ многочлен $\overline{q}_1$. Пусть θ' — корень многочлена $\overline{q}_1$. Изоморфизм $\varphi : k(\omega) \to k(\omega')$ можно продолжить до изоморфизма $k(\omega, \theta) \to k(\omega', \theta')$. Этот изоморфизм имеет вид $\sum b_i\theta^i \mapsto \sum \varphi(b_i)(\theta')^i$, где $b_i \in k(\omega)$. Такие продолжения изоморфизмов позволяют построить изоморфизм поля K в некоторое подполе $K' \subset K$, переводящий ω в ω'. Этот изоморфизм полей является, в частности, изоморфизмом линейных пространств над полем k. В таком случае из конечномерности K следует, что $K' = K$, т. е. мы получаем автоморфизм поля K. □

Следствие. Если K — нормальное расширение поля k, то элемент $\omega \in K$ инвариантен относительно действия группы Галуа $G(K, k)$ тогда и только тогда, когда $\omega \in k$.

Доказательство. Если элемент $\omega \in K$ инвариантен относительно действия группы Галуа $G(K, k)$, то все сопряженные с ним элементы совпадают с ним самим. Это означает, что ω — корень многочлена $x - \omega$ с коэффициентами из поля k, т. е. $\omega \in k$. □

Условие нормальности расширения весьма существенно. Например, любой автоморфизм поля $\mathbb{Q}(\sqrt[3]{2})$ тождествен, т. е. элемент $\sqrt[3]{2} \notin \mathbb{Q}$ инвариантен относительно действия всех автоморфизмов.

Нормальные расширения отличаются тем свойством, что у них достаточно велика группа автоморфизмов. Это позволяет установить взаимно однозначное соответствие между промежуточными полями и подгруппами группы Галуа.

Пусть K — нормальное расширение поля k. Рассмотрим произвольное промежуточное поле L: $k \subset L \subset K$. Согласно следствию из теоремы 22.2 поле K является нормальным расширением поля L, поэтому можно рассмотреть группу Галуа $G(K, L)$.

Теорема 22.4 (соответствие Галуа). а) Между промежуточными полями $k \subset L \subset K$ и подгруппами группы Галуа $G(K,k)$ имеется взаимно однозначное соответствие: полю L соответствует подгруппа $G(K,L) \subset G(K,k)$, а подгруппе $H \subset G(K,k)$ соответствует поле, состоящее из элементов поля K, инвариантных относительно действия группы H.

б) Промежуточное поле L является нормальным расширением поля k тогда и только тогда, когда подгруппа $G(K,L) \subset G(K,k)$ нормальна. В этом случае имеется точная последовательность

$$0 \to G(K,L) \to G(K,k) \to G(L,k) \to 0.$$

Доказательство. а) Любой автоморфизм поля K, оставляющий неподвижными элементы поля L, оставляет неподвижными и элементы поля $k \subset L$, т. е. $G(K,L) \subset G(K,k)$.

Полю L соответствует группа $G(K,L)$, а группе $G(K,L)$ соответствует поле L', состоящее из тех элементов поля K, которые инвариантны относительно всех автоморфизмов поля K, оставляющих неподвижными элементы поля L. Ясно, что $L' \supset L$. Но в случае нормального расширения любой элемент поля K, инвариантный относительно действия группы $G(K,L)$, лежит в L (следствие теоремы 22.3; другое доказательство — теорема 21.4 (а) на с. 211). Поэтому $L = L'$, т. е. каждому подполю соответствует подгруппа, причем эта подгруппа однозначно определяет подполе.

Группе $H \subset G(K,k)$ соответствует поле L, а полю L соответствует группа $G(K,L) = H'$, которая состоит из тех автоморфизмов поля K, которые оставляют неподвижными элементы, инвариантные относительно H. Ясно, что $H' \supset H$. Но если подгруппа H группы Галуа $G(K,L)$ такова, что все элементы поля K, инвариантные относительно действия H, лежат в L, то H совпадает со всей группой Галуа $G(K,L)$ (теорема 21.4 (б) на с. 211). Таким образом, каждой подгруппе соответствует подполе, причем это подполе однозначно определяет подгруппу.

б) Предположим, что поле L является нормальным расширением поля k. Тогда любой автоморфизм поля K над k переводит поле L в себя (элемент поля L переходит в сопряженный элемент, который снова лежит в L). Таким образом, имеется гомоморфизм $G(K,k) \to G(L,k)$. Ясно, что группа $G(K,L)$ является ядром этого гомоморфизма, поэтому она — нормальная подгруппа в $G(K,k)$.

Предположим теперь, что $G(K,L)$ — нормальная подгруппа в $G(K,k)$, т. е. если $\varphi \in G(K,L)$ и $\psi \in G(K,k)$, то $\psi^{-1}\varphi\psi \in G(K,L)$. Пусть $a \in L$; требуется доказать, что все сопряженные с a элементы $a_1, \ldots, a_l$ лежат в L. По условию $a_1, \ldots, a_l \in K$, причем $a_i = \psi_i(a)$ для некоторого $\psi_i \in G(K,k)$. Если $\varphi \in G(K,L)$, то $\psi_i^{-1}\varphi\psi_i \in G(K,L)$. Поэтому $\psi_i^{-1}\varphi\psi_i(a) = a$, т. е. $\varphi(a_i) = a_i$. Следовательно, $a_i \in L$.

Точная последовательность

$$0 \to G(K,L) \to G(K,k) \to G(L,k) \to 0$$

устроена следующим образом. Поле L является нормальным расширением поля k, поэтому любой автоморфизм $\varphi \in G(K,k)$ сохраняет поле L, а значит, φ можно ограничить на L. Так возникает гомоморфизм $G(K,k) \to G(L,k)$. Его ядром служат автоморфизмы поля K, тождественные на L; они образуют группу $G(K,L)$. Эпиморфность гомоморфизма следует из того, что любой автоморфизм поля L над k можно продолжить до некоторого автоморфизма поля K над k. □

Если L — поле разложения над k многочлена g, а K — поле разложения над k многочлена f, то точная последовательность

$$0 \to G(K,L) \to G(K,k) \to G(L,k) \to 0$$

имеет вид

$$0 \to G_L(f) \to G_k(f) \to G_k(g) \to 0.$$

Теорема 22.5. Пусть L — произвольное расширение поля k и f — многочлен над k. Тогда группа Галуа $G_L(f)$ изоморфна некоторой подгруппе в $G_k(f)$.

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена f. Автоморфизм $\sigma \in G_L(f)$ переставляет корни $\alpha_1, \ldots, \alpha_n$ и оставляет неподвижными все элементы поля $L \supset k$. Поэтому автоморфизм σ сохраняет поле $k(\alpha_1, \ldots, \alpha_n)$, т. е. автоморфизму σ можно сопоставить автоморфизм $\overline{\sigma} \in G_k(f)$, являющийся ограничением σ на поле $k(\alpha_1, \ldots, \alpha_n)$.

Если $\overline{\sigma} = \mathrm{id}$, то автоморфизм σ оставляет на месте все корни $\alpha_1, \ldots, \alpha_n$. Кроме того, по определению σ оставляет на месте все элементы поля L, а значит, $\sigma = \mathrm{id}$. Таким образом, отображение $\sigma \mapsto \overline{\sigma}$ — мономорфизм, т. е. группа $G_L(f)$ изоморфна некоторой подгруппе в $G_k(f)$. □

22.2. Многочлен с группой Галуа S_5

Чтобы привести пример уравнения, не разрешимого в радикалах, нам потребуется многочлен с группой Галуа S_n, $n \geqslant 5$. Мы уже готовы доказать, что многочлен $x^5 - 4x + 2$ над $\mathbb{Q}$ имеет группу Галуа S_5.

Группа $G \subset S_n$ называется *транзитивной*, если для любых двух индексов $i, j \in \{1, \ldots, n\}$ существует подстановка $\sigma \in G$, для которой $\sigma(i) = j$.

Теорема 22.6. Многочлен f (без кратных корней) неприводим тогда и только тогда, когда его группа Галуа транзитивна.

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена f. Если многочлен f неприводим над полем k, то по определению все его корни сопряжены друг с другом, поэтому согласно теореме 22.3 существует автоморфизм поля $k(\alpha_1, \ldots, \alpha_n)$, переводящий α_i в α_j.

Предположим теперь, что группа Галуа G многочлена f транзитивна. Пусть f_1 — произвольный делитель многочлена f над полем k, α_1 — корень многочлена f_1. Возьмем автоморфизм $\sigma_i \in G$, для которого $\sigma_i(\alpha_1) = \alpha_i$. При автоморфизме σ_i соотношение $f_1(\alpha_1) = 0$ переходит в соотношение $f_1(\alpha_i) = 0$, т. е. все корни многочлена f являются также корнями многочлена f_1. Учитывая, что у многочлена f нет кратных корней, получаем, что f_1 делится на f, т. е. многочлен f неприводим. □

Теорема 22.7. Если число n простое и транзитивная группа $G \subset S_n$ содержит хотя бы одну транспозицию (i, j), то $G = S_n$.

Доказательство. Введем на множестве $\{1, \ldots, n\}$ следующее отношение: $i \sim j$, если либо $i = j$, либо в группе G есть транспозиция (i, j). Тождество $(i, j)(j, k)(i, j) = (i, k)$ показывает, что это отношение является отношением эквивалентности.

Пусть $E(i)$ — класс эквивалентности, содержащий элемент i. Покажем, что $\big|E(i)\big| = \big|E(j)\big|$, т. е. все классы эквивалентности состоят из одного и того же числа элементов. Группа G транзитивна, поэтому в ней есть такая подстановка σ, что $\sigma(i) = j$. Пусть $a \in E(i)$, т. е. $(i, a) \in G$. Подстановка $\sigma \cdot (i, a) \cdot \sigma^{-1}$ меняет местами элементы $\sigma(a)$ и $\sigma(i)$, а все остальные элементы оставляет неподвижными, т. е.

$$\sigma \cdot (i, a) \cdot \sigma^{-1} = \big(\sigma(i), \sigma(a)\big) = \big(j, \sigma(a)\big) \in G.$$

Таким образом, $\sigma\big(E(i)\big) \subset E(j)$, поэтому $\big|E(i)\big| \leqslant \big|E(j)\big|$. Неравенство $\big|E(j)\big| \leqslant \big|E(i)\big|$ доказывается аналогично.

По условию число n простое, поэтому класс эквивалентности ровно один. Это означает, что $G = S_n$. □

Теорема 22.8. Пусть f — неприводимый многочлен над $\mathbb{Q}$ простой степени p, причем у f есть ровно два невещественных корня. Тогда группа Галуа многочлена f над $\mathbb{Q}$ равна S_p.

Доказательство. Многочлен f неприводим, поэтому его группа Галуа $G \subset S_p$ транзитивна. Согласно предыдущей теореме достаточно доказать, что группа G содержит некоторую транспозицию. Пример такой транспозиции дает ограничение комплексного сопряжения $z \mapsto \overline{z}$ на поле разложения многочлена f. Действительно, при комплексном сопряжении все вещественные корни многочлена остаются на месте, а оба комплексных корня меняются местами (из этого, в частности, следует, что поле разложения переходит в себя). □

Примером неприводимого многочлена степени 5, у которого есть ровно два комплексных корня, служит многочлен $f(x) = x^5 - 4x + 2$. Неприводимость этого многочлена следует из признака Эйзенштейна. Количество вещественных корней многочлена f не меньше трех, поскольку

$$f(-2) < 0, \quad f(0) > 0, \quad f(1) < 0, \quad f(2) > 0.$$

С другой стороны, количество вещественных корней не может быть больше трех, потому что иначе у производной $f'(x) = 5x^4 - 4$ было бы больше двух вещественных корней.

22.3. Простые радикальные расширения

Поле разложения K многочлена $x^n - c$, где $c \in k$, называют *простым радикальным* расширением поля k.

Теорема 22.9. а) Группа Галуа $G(K, k)$ простого радикального расширения разрешима.

б) Если поле k содержит примитивный корень степени n из единицы, то $G(K, k)$ — подгруппа циклической группы $\mathbb{Z}/n\mathbb{Z}$.

в) Если $c = 1$, то $G(K, k)$ — подгруппа мультипликативной группы $(\mathbb{Z}/n\mathbb{Z})^*$.

Доказательство. а) Пусть α — корень многочлена $x^n - c$, а ε — примитивный корень степени n из единицы. Тогда корни многочлена $x^n - c$ имеют вид $\alpha, \alpha\varepsilon, \ldots, \alpha\varepsilon^{n-1}$, поэтому $K \subset k(\alpha, \varepsilon)$. С другой стороны, $\varepsilon = (\alpha\varepsilon)\alpha^{-1} \in K$, поэтому $k(\alpha, \varepsilon) \subset K$, т. е. $K = k(\alpha, \varepsilon)$.

Пусть $\sigma \in G(K, k)$. Тогда $\sigma(\varepsilon)$ — корень многочлена $x^n - 1$, т. е. $\sigma(\varepsilon) = \varepsilon^a$. При этом ε^a не может быть корнем многочлена $x^m - 1$, где $m < n$, так как иначе элемент $\varepsilon = \sigma^{-1}(\varepsilon^a)$ тоже был бы корнем этого многочлена, а это противоречит примитивности ε. Таким образом, $(a, n) = 1$.

Автоморфизм σ полностью определяется своими значениями на образующих: $\sigma(\varepsilon) = \varepsilon^a$, $\sigma(\alpha) = \varepsilon^b\alpha$. Поэтому такой автоморфизм σ можно обозначить $[a, b]$, где $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $b \in \mathbb{Z}/n\mathbb{Z}$. При этом если $\sigma_i = [a_i, b_i]$, $i = 1, 2$, то

$$\sigma_1\bigl(\sigma_2(\varepsilon)\bigr) = \varepsilon^{a_1 a_2}, \quad \sigma_1\bigl(\sigma_2(\alpha)\bigr) = \varepsilon^{a_1 b_2 + b_1}\alpha,$$

т. е. $\sigma_1\sigma_2 = [a_1a_2, a_1b_2 + b_1]$.

Рассмотрим гомоморфизм $\varphi\colon G(K, k) \to (\mathbb{Z}/n\mathbb{Z})^*$, при котором автоморфизму $\sigma = [a, b]$ сопоставляется элемент $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Ядро этого гомоморфизма состоит из элементов вида $[1, b]$; для таких элементов закон композиции следующий: $[1, b_1][1, b_2] = [1, b_1 + b_2]$. Ядро и образ гомоморфизма φ — абелевы группы, поэтому группа $G(K, k)$ разрешима.

б) Если $\varepsilon \in k$, то $\sigma(\varepsilon) = \varepsilon$. Поэтому $\sigma = [1, b] \in \mathbb{Z}/n\mathbb{Z}$.

в) Если $c = 1$, то можно считать, что $\alpha = 1$. В таком случае $\sigma = [a, 0] \in (\mathbb{Z}/n\mathbb{Z})^*$. □

22.4. Циклические расширения

Нормальное расширение K поля k называют *циклическим* расширением, если группа Галуа $G(K, k)$ является циклической.

Теорема 22.10. Если поле k содержит примитивный корень степени n из единицы, то любое циклическое расширение $K \supset k$ степени n имеет вид $K = k(\beta)$, где β — корень неприводимого над k многочлена $x^n - c$.

Доказательство. Нам потребуется свойство линейной независимости характеров группы. Напомним его формулировку и доказательство. Пусть G — группа, K — поле, K^* — мультипликативная группа этого поля, т. е. множество ненулевых элементов с операцией умножения. *Характером* группы G называют произвольный гомоморфизм $G \to K^*$.

Лемма. Различные характеры группы G линейно независимы над полем K.

Доказательство. Пусть $\{\gamma_1, \ldots, \gamma_n\}$ — минимальное непустое множество линейно зависимых характеров, т. е.

$$\lambda_1\gamma_1(g) + \ldots + \lambda_n\gamma_n(g) = 0 \tag{1}$$

для всех $g \in G$ при некоторых фиксированных $\lambda_1, \ldots, \lambda_n \in K^*$. Ясно, что $n \geqslant 2$. Характеры γ_1 и γ_n различны, поэтому $\gamma_1(h) \neq \gamma_n(h)$ для некоторого $h \in G$. Умножим равенство (1) на $\gamma_n(h)$ и вычтем из полученного произведения равенство $\lambda_1\gamma_1(hg) + \ldots + \lambda_n\gamma_n(hg) = 0$. После несложных преобразований получим

$$\lambda_1\big(\gamma_n(h) - \gamma_1(h)\big)\gamma_1(g) + \ldots + \lambda_{n-1}\big(\gamma_n(h) - \gamma_{n-1}(h)\big)\gamma_{n-1}(g) = 0.$$

Это противоречит минимальности множества $\{\gamma_1, \ldots, \gamma_n\}$. □

Если σ — автоморфизм поля K, то ограничение σ на K^* является характером группы K^*. Поэтому если $\sigma_1, \ldots, \sigma_n$ — различные автоморфизмы поля K и $\alpha_1, \ldots, \alpha_n \in K^*$, то $\alpha_1\sigma_1(\alpha) + \ldots + \alpha_n\sigma_n(\alpha) \neq 0$ для некоторого $\alpha \in K^* \subset K$.

Перейдем непосредственно к доказательству теоремы. Пусть σ — образующая циклической группы $G(K, k)$, ε — примитивный корень степени n из единицы, лежащий в k. Рассмотрим *резольвенту Лагранжа*

$$(\varepsilon, \alpha)_\sigma = \alpha + \varepsilon\sigma(\alpha) + \ldots + \varepsilon^{n-1}\sigma^{n-1}(\alpha).$$

Автоморфизмы $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ различны, поэтому найдется элемент $\alpha \in K$, для которого $(\varepsilon, \alpha)_\sigma = \beta \neq 0$. Легко проверить, что $\sigma(\beta) = \varepsilon^{-1}\beta$ и $\sigma(\beta^n) = \big(\sigma(\beta)\big)^n = \beta^n$. Таким образом, $\sigma(\beta) \neq \beta$, т. е. $\beta \notin k$, и $\sigma^i(\beta^n) = \beta^n$ при $i = 1, \ldots, n-1$, т. е. $\beta^n = c \in k$.

Рассмотрим многочлен

$$x^n - c = (x - \beta)(x - \varepsilon\beta) \cdot \ldots \cdot (x - \varepsilon^{n-1}\beta).$$

Поле $k(\beta)$ является его полем разложения, причем $k(\beta) \subset K$. Автоморфизмы $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ являются различными автоморфизмами поля $k(\beta)$, поэтому порядок группы Галуа поля $k(\beta)$ над k не меньше n, т. е. степень расширения $k(\beta)$ над k не меньше n. С другой стороны, степень расширения K над k равна n, поэтому $k(\beta) = K$. Группа Галуа многочлена $x^n - c$ транзитивна, поэтому он неприводим. □

23. Решение уравнений в радикалах

Расширение L поля k называют *радикальным*, если существует такая последовательность промежуточных полей

$$k = L_0 \subset L_1 \subset \ldots \subset L_r = L,$$

что $L_i = L_{i-1}(\beta_i)$, где $\beta_i^{n_i} \in L_{i-1}$. Иными словами, к полю k последовательно присоединяются корни из элементов полей, полученных на предыдущем шаге.

Пусть f — неприводимый многочлен над полем k, $\alpha_1, \ldots, \alpha_n$ — его корни. Уравнение $f(x) = 0$ называют *разрешимым в радикалах*, если поле $k(\alpha_1, \ldots, \alpha_n)$ содержится в некотором радикальном расширении поля k.

Чтобы сформулировать и доказать критерий разрешимости уравнения в радикалах, нам потребуется понятие разрешимой группы. Поэтому начнем с того, что напомним основные сведения о разрешимых группах.

23.1. Разрешимые группы

Конечную группу G называют *разрешимой*, если существует такая последовательность вложенных подгрупп

$$\{e\} = G_r \subset G_{r-1} \subset \ldots \subset G_0 = G,$$

что G_i — нормальная подгруппа в G_{i-1} и факторгруппа G_{i-1}/G_i абелева (при $i = 1, \ldots, r$).

Для любой абелевой группы G можно построить последовательность вложенных подгрупп, для которой все факторгруппы G_{i-1}/G_i циклические (и даже циклические простых порядков). Поэтому в определении разрешимой группы можно считать, что все факторгруппы G_{i-1}/G_i циклические.

При выяснении связи разрешимости в радикалах уравнения $f(x) = 0$ и разрешимости группы Галуа многочлена f используется соответствие Галуа, которое дает точную последовательность $0 \to H \to G \to G/H \to 0$. При этом про какие-то из этих трех групп бывает известно, что они разрешимы, и нужно сделать вывод о разрешимости остальных групп. Для этих целей мы будем пользоваться следующими утверждениями.

Теорема 23.1. а) Любая подгруппа H разрешимой группы G разрешима.

б) Пусть H — нормальная подгруппа группы G, причем группы H и G/H разрешимы. Тогда группа G разрешима.

в) Пусть H — нормальная подгруппа разрешимой группы G. Тогда группа G/H разрешима.

Доказательство. а) Покажем, что последовательность подгрупп $H_i = G_i \cap H$ обладает требуемыми свойствами, т. е. H_i — нормальная подгруппа в H_{i-1} и факторгруппа H_{i-1}/H_i абелева. Так как $G_i \subset G_{i-1}$, то $H_i = H_{i-1} \cap G_i$. Поэтому H_i — нормальная подгруппа в H_{i-1} и

$$H_{i-1}/H_i = H_{i-1}/(H_{i-1} \cap G_i) \cong G_i H_{i-1}/G_i \subset G_{i-1}/G_i.$$

б) Для разрешимых групп H и G/H возьмем последовательности подгрупп

$$\{e\} = H_n \subset H_{n-1} \subset \ldots \subset H_0 = H,$$
$$\{H\} = A_m \subset A_{m-1} \subset \ldots \subset A_0 = G/H.$$

Положим $G_i = p^{-1}(A_i)$, где $p\colon G \to G/H$ — естественная проекция. Ясно, что $G_m = H$ и $G_0 = G$. Покажем, что последовательность подгрупп

$$\{e\} = H_n \subset H_{n-1} \subset \ldots \subset H_0 = H = G_m \subset G_{m-1} \subset \ldots \subset G_0 = G$$

обладает требуемыми свойствами, т. е. G_i — нормальная подгруппа в G_{i-1} и G_{i-1}/G_i — абелева группа. Второе свойство следует из того, что $G_{i-1}/G_i \cong A_{i-1}/A_i$. Пусть $g_i \in G_i$ и $g_{i-1} \in G_{i-1}$. Тогда

$$p\bigl(g_{i-1}^{-1} g_i g_{i-1}\bigr) = p(g_{i-1})^{-1}\, p(g_i)\, p(g_{i-1}) \in A_i,$$

так как A_i — нормальная подгруппа в A_{i-1}. Поэтому $g_{i-1}^{-1} g_i g_{i-1} \in G_i$, т. е. G_i — нормальная подгруппа в G_{i-1}.

в) Для разрешимой группы G возьмем последовательность подгрупп

$$\{e\} = G_r \subset G_{r-1} \subset \ldots \subset G_0 = G,$$

и положим $A_i = G_i H/H$. Тогда последовательность подгрупп

$$\{H\} = A_r \subset A_{r-1} \subset \ldots \subset A_0 = G/H$$

обладает требуемыми свойствами, т. е. A_i — нормальная подгруппа в A_{i-1} и A_{i-1}/A_i — абелева группа. В самом деле, пусть $g_i H \in A_i$ и $g_{i-1} H \in A_{i-1}$. Тогда

$$(g_{i-1}H)g_iH(g_{i-1}H)^{-1} = g_{i-1}Hg_iHg_{i-1}^{-1} = g_{i-1}g_ig_{i-1}^{-1}H \in A_i.$$

Кроме того,

$$A_{i-1}/A_i \cong G_{i-1}/(G_iH \cap G_{i-1}) \cong (G_{i-1}/G_i)/\big((G_iH \cap G_{i-1})/G_i\big),$$

т. е. группа A_{i-1}/A_i изоморфна факторгруппе абелевой группы, поэтому A_{i-1}/A_i — абелева группа. □

23.2. Уравнения с разрешимой группой Галуа

Воспользовавшись соответствием Галуа и теоремой 22.10 о структуре циклического расширения, нетрудно доказать, что уравнение с разрешимой группой Галуа разрешимо в радикалах.

Теорема 23.2. Пусть f — многочлен без кратных корней над полем k, причем группа Галуа $G_k(f)$ разрешима. Тогда уравнение $f = 0$ разрешимо в радикалах.

Доказательство. Если поле k не содержит примитивный корень степени $d = \big|G_k(f)\big|$ из единицы, то добавим к k примитивный корень ε степени d из единицы, т. е. рассмотрим поле $L = k(\varepsilon)$. Группа Галуа $G_L(f)$ изоморфна некоторой подгруппе разрешимой группы $G_k(f)$, поэтому группа $G_L(f)$ разрешима, причем $\big|G_L(f)\big|$ делит d. В частности, поле L содержит примитивные корни из единицы любой степени, делящей $\big|G_L(f)\big|$.

Для разрешимой группы $G_L(f)$ построим последовательность подгрупп

$$\{e\} = G_r \subset \ldots \subset G_0 = G_L(f),$$

для которой факторгруппы G_{i-1}/G_i циклические. Соответствие Галуа позволяет построить последовательность полей

$$K = L_r \supset \ldots \supset L_0 = L,$$

где K — поле разложения многочлена f над L. При этом расширение $L_i \supset L_{i-1}$ нормально, поэтому последовательность полей $K \supset L_i \supset L_{i-1}$ дает точную последовательность

$$0 \to G(K, L_i) \to G(K, L_{i-1}) \to G(L_i, L_{i-1}) \to 0.$$

Следовательно, $G(L_i, L_{i-1}) \cong G(K, L_{i-1})/G(K, L_i) = G_{i-1}/G_i$ — циклическая группа, порядок которой делит $\big|G_L(f)\big|$. Учитывая, что поле

$L_{i-1} \supset L$ содержит примитивный корень из единицы степени $d_i = \left|G(L_i, L_{i-1})\right|$, получаем, что $L_i = L_{i-1}(\beta_i)$, где β_i — корень многочлена $x^{d_i} - c_i$, $c_i \in L_{i-1}$. Таким образом, L_i — радикальное расширение поля L_{i-1}, а значит, K — радикальное расширение L. Ясно также, что L — радикальное расширение k. Поэтому поле разложения многочлена f является радикальным расширением поля k, т. е. уравнение $f = 0$ разрешимо в радикалах. □

23.3. Уравнения, разрешимые в радикалах

Мы только что доказали, что если группа Галуа уравнения разрешима, то это уравнение разрешимо в радикалах. Докажем теперь обратное утверждение.

Теорема 23.3. Пусть f — многочлен без кратных корней над полем k, причем уравнение $f = 0$ разрешимо в радикалах. Тогда группа Галуа $G_k(f)$ разрешима.

Доказательство. По условию для некоторого поля L, содержащего все корни многочлена f, имеется такая последовательность полей

$$L = L_r \supset \ldots \supset L_0 = k, \tag{1}$$

что $L_i = L_{i-1}(\beta_i)$, где $\beta_i^{n_i} \in L_{i-1}$. Расширение $L \supset k$ при этом не обязательно нормально, поэтому непосредственно воспользоваться соответствием Галуа нельзя. Начнем с того, что построим радикальное расширение $K \supset L$, для которого расширение $K \supset k$ нормально.

Применим индукцию по r. При $r = 0$ утверждение очевидно, поэтому по предположению индукции можно считать, что мы уже построили радикальное расширение $K_{r-1} \supset L_{r-1}$, для которого расширение $K_{r-1} \supset k$ нормально. Положим $K' = K_{r-1}$ и $L' = K'(\beta_r) \supset L$. Шаг индукции заключается в доказательстве следующего утверждения.

Лемма. Пусть $K' \supset k$ — нормальное расширение и $L' = K'(\beta)$, где $\beta^n \in K'$. Тогда существует такое радикальное расширение $K \supset L'$, что расширение $K \supset k$ нормально.

Доказательство. Рассмотрим неприводимый над k многочлен $g(x)$ с корнем $\beta^n \in K'$. Расширение $K' \supset k$ нормально, поэтому все корни многочлена $g(x)$ лежат в K'. Положим $h(x) = g(x^n)$ и рассмотрим

поле K — поле разложения многочлена h над K'. Покажем, что поле K обладает всеми требуемыми свойствами.

1. *Расширение $K \supset k$ нормально.* Действительно, расширение $K' \supset k$ нормально, поэтому K' — поле разложения над k некоторого многочлена $\varphi(x)$. В таком случае K — поле разложения над k многочлена $h(x)\varphi(x)$.

2. $K \supset L' = K'(\beta)$. Действительно, $K' \subset K$ по определению и $\beta \in K$, так как $h(\beta) = g(\beta^n) = 0$.

3. *Расширение $K \supset L'$ радикально.* Пусть $\widehat{\beta}$ — корень многочлена $h(x)$. Тогда $\widehat{\beta}^n$ — корень многочлена $g(x)$, поэтому $\widehat{\beta}^n \in K' \subset L'$. Остается заметить, что поле K получается в результате присоединения к полю L' всех корней $\widehat{\beta}$ многочлена $h(x)$. □

Итак, можно считать, что в (1) поле L — нормальное расширение поля k. Более того, можно считать, что числа n_i простые и степень расширения $L_i \supset L_{i-1}$ равна n_i (присоединение корня степени pq можно заменить на присоединение корня степени p и последующее присоединение корня степени q).

Из нормальности расширения $L \supset k$ следует нормальность расширения $L \supset L_{i-1}$. Коэффициенты многочлена $x^{n_i} - \beta_i^{n_i}$ лежат в L_{i-1}, а его корень β_i лежит в L, но не лежит в L_{i-1}. Поэтому у многочлена $x^{n_i} - \beta_i^{n_i}$ есть неприводимый над L_{i-1} делитель с корнем β_i, причем этот делитель отличен от $x - \beta_i$. Следовательно, поле L содержит корень многочлена $x^{n_i} - \beta_i^{n_i}$, отличный от β_i, а значит, поле L содержит примитивный корень из единицы степени n_i (мы пользуемся тем, что n_i — простое число).

Поле L содержит примитивные корни из единицы всех степеней n_i, поэтому оно содержит примитивный корень ε из единицы, степень которого делится на все n_i. Положим $L'_i = L_i(\varepsilon)$ и рассмотрим последовательность подполей

$$L = L'_r \supset L'_{r-1} \supset \ldots \supset L'_0 = L_0(\varepsilon) \supset L_0 = k.$$

Соответствие Галуа дает последовательность подгрупп

$$\{e\} = G(L, L'_r) \subset G(L, L'_{r-1}) \subset \ldots \subset G(L, L'_0) = G\big(L, k(\varepsilon)\big) \subset G(L, k).$$

Расширение $L'_i \supset L'_{i-1}$ нормально, поскольку L'_i — поле разложения над L'_{i-1} многочлена $x^{n_i} - \beta_i^{n_i}$. Поэтому последовательность полей $L'_{i-1} \subset L'_i \subset L$ дает точную последовательность групп

$$0 \to G(L, L'_i) \to G(L, L'_{i-1}) \to G(L'_i, L'_{i-1}) \to 0.$$

Таким образом, $G(L, L'_{i-1})/G(L, L'_i) \cong G(L'_i, L'_{i-1})$ — циклическая группа порядка n_i. Следовательно, $G\big(L, k(\varepsilon)\big)$ — разрешимая группа.

Следующий шаг — доказательство разрешимости группы $G(L, k)$. Расширение $k(\varepsilon) \supset k$ нормально, поэтому для последовательности полей $k \subset k(\varepsilon) \subset L$ получаем точную последовательность групп

$$0 \to G\big(L, k(\varepsilon)\big) \to G(L, k) \to G(k(\varepsilon), k) \to 0.$$

Группа $G(k(\varepsilon), k)$ абелева (теорема 22.9 (в) на с. 220), поэтому группа $G(L, k)$ разрешима.

Последний шаг — доказательство разрешимости группы $G_k(f) = G(N, k)$, где N — поле разложения многочлена f над k. Последовательность полей $k \subset N \subset L$ дает точную последовательность групп

$$0 \to G(L, N) \to G(L, k) \to G(N, k) \to 0.$$

Таким образом, $G(N, k)$ — факторгруппа разрешимой группы $G(L, k)$, а значит, она сама разрешима. □

Пример. Уравнение

$$x^5 - 4x + 2 = 0$$

неразрешимо в радикалах.

Доказательство. Группа Галуа многочлена $x^5 - 4x + 2 = 0$ над $\mathbb{Q}$ равна S_5 (см. с. 220). Остается доказать, что группа S_5 неразрешима. Прежде всего заметим, что если $H \subset G$ — такая нормальная подгруппа, что группа G/H абелева, то для любых $x, y \in G$ элемент $xyx^{-1}y^{-1}$ лежит в H. В группе S_5 есть нормальная подгруппа A_5, состоящая из четных подстановок. Легко проверить, что любой элемент группы A_5 можно представить в виде $xyx^{-1}y^{-1}$, где $x, y \in A_5$. В самом деле, любой элемент группы A_5 является либо циклом длины 5, либо циклом длины 3, либо произведением двух транспозиций $(ij)(kl)$ с попарно различными i, j, k, l. Для цикла (12345) положим $x = (12534)$ и $y = (12)(35)$; для цикла (123) положим $x = (123)$ и $y = (23)(45)$; для элемента (12)(34) положим $x = (14)(23)$ и $y = (123)$. Таким образом, если $H \subset S_5$ — нормальная подгруппа и группа S_5/H абелева, то $H = A_5$ (или S_5). Но в A_5 уже нет нормальной подгруппы K, для которой факторгруппа A_5/K абелева. □

23.4. Абелевы уравнения

В мемуаре «О специальном классе алгебраически разрешимых уравнений» Абель доказал три важных утверждения, относящихся к разрешимости уравнений в радикалах.

1. Если один из корней неприводимого многочлена f рационально выражается через другой корень, то решение уравнения $f(x) = 0$ сводится к решению нескольких уравнений меньшей степени.

2. Если корни неприводимого многочлена f имеют вид x_1, $\theta(x_1)$, $\theta^2(x_1) = \theta\big(\theta(x_1)\big), \dots, \theta^{n-1}(x_1)$, где θ — такая рациональная функция, что $\theta^n(x_1) = x_1$, то уравнение $f(x) = 0$ решается в радикалах.

3. Если корни неприводимого многочлена f имеют вид x_1, $\theta_2(x_1)$, $\theta_3(x_1), \dots, \theta_n(x_1)$, где θ_i — такие рациональные функции, что $\theta_i\theta_j(x_1) = \theta_j\theta_i(x_1)$, то уравнение $f(x) = 0$ решается в радикалах. Более того, если $\deg f = p_1^{n_1} \dots p_k^{n_k}$, то решение уравнения $f(x) = 0$ сводится к решению n_1 уравнений степени p_1, $\dots$, n_k уравнений степени p_k.

Многочлен f, участвующий в формулировке утверждения 3, называют *абелевым*, а уравнение $f(x) = 0$ называют *абелевым* уравнением. Группа Галуа многочлена g абелева тогда и только тогда, когда резольвента Галуа многочлена g является абелевым многочленом. Таким образом, теорема Абеля является частным случаем теоремы Галуа: уравнение с абелевой группой Галуа разрешимо в радикалах. Тем не менее, методы Абеля сохраняют определенное значение, потому что предложенное им решение абелевых уравнений достаточно конструктивно.

Многочлен f, участвующий в формулировке утверждения 2, будем называть *циклическим абелевым*. У такого многочлена группа Галуа циклическая.

Для решения циклических абелевых уравнений Абель применил методы, разработанные Лагранжем и Гауссом. Его заслуга состоит в том, что он выделил наиболее общий класс уравнений, к которым применимы эти методы. Кроме того, занимаясь теорией эллиптических функций, Абель нашел новый интересный пример циклического абелева уравнения, а именно, уравнение деления лемнискаты. Современное доказательство того, что уравнение деления лемнискаты является циклическим абелевым уравнением, приведено в [ПрС].

Начнем с утверждения 1. Оно относится к многочленам специального вида, но с произвольной группой Галуа. Действительно, у резольвенты Галуа любого многочлена все корни рационально выражаются через один из корней.

Теорема 23.4. а) Пусть f — неприводимый многочлен над полем k (нулевой характеристики), один из корней которого рационально выражается через другой корень. Тогда корни многочлена f можно записать в виде таблицы:

$$\begin{array}{c} x_1^1, \quad x_2^1 = \theta(x_1^1), \quad \ldots, \quad x_p^1 = \theta^{p-1}(x_1^1), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_1^m, \quad x_2^m = \theta(x_1^m), \quad \ldots, \quad x_p^m = \theta^{p-1}(x_1^m), \end{array}$$

где θ — такая рациональная функция, что $\theta^p(x_1^i) = x_1^i$, $i = 1, \ldots, m$.

б) Решение уравнения $f = 0$ сводится к решению уравнения $g = 0$ степени m с коэффициентами из поля k и циклических абелевых уравнений $h_1 = 0, \ldots, h_m = 0$, где h_i — многочлен степени p, коэффициенты которого рационально выражаются (над полем k) через корень y_i многочлена g.

Доказательство. а) Пусть $x_1, \ldots, x_n$ — корни многочлена f и $x_2 = \theta(x_1)$, где θ — рациональная функция. Рассмотрим многочлен $\varphi(x) = \prod_{i=1}^{n} \bigl(x - \theta(x_i)\bigr)$. Коэффициенты этого многочлена являются симметрическими функциями от $x_1, \ldots, x_n$, поэтому они принадлежат полю k. Многочлены f и φ имеют общий корень $x_2 = \theta(x_1)$. Но многочлен f неприводим и $\deg f = \deg \varphi$, поэтому $\theta(x_1), \ldots, \theta(x_n)$ — некоторая перестановка чисел $x_1, \ldots, x_n$, т. е. каждому корню x_i однозначно соответствует такой корень x_j, что $x_j = \theta(x_i)$.

Рассмотрим всевозможные циклы $x_i, \theta(x_i), \theta^2(x_i), \ldots, \theta^{p-1}(x_i)$, где $\theta^p(x_i) = x_i$. Ясно, что любые два цикла (как множества) либо не пересекаются, либо совпадают. Остается лишь доказать, что у всех циклов длина одна и та же. Пусть p — наименьшая длина цикла. Если $\theta^p(x) = x$ для всех x, то все циклы имеют длину p. Если же $\theta^p(x) \neq x$, то уравнения $\theta^p(x) = x$ и $f(x) = 0$ имеют общий корень. Из неприводимости многочлена f следует, что $\theta^p(x_i) = x_i$ для всех $i = 1, \ldots, n$, поэтому все циклы имеют длину p.

б) Чтобы избежать громоздких обозначений, будем считать, что $p = 3$ и $m = 4$. В общем случае доказательство то же самое. Таблицу корней можно записать в виде

$$\begin{array}{lll} x_1, & x_2 = \theta(x_1), & x_3 = \theta^2(x_1), \\ x_4, & x_5 = \theta(x_4), & x_6 = \theta^2(x_4), \\ x_7, & x_8 = \theta(x_7), & x_9 = \theta^2(x_7), \\ x_{10}, & x_{11} = \theta(x_{10}), & x_{12} = \theta^2(x_{10}). \end{array}$$

Пусть q — произвольный симметрический многочлен от трех переменных над полем k. Тогда

$$\varphi(x_1) = q\bigl(x_1, \theta(x_1), \theta^2(x_1)\bigr) = q\bigl(\theta(x_1), \theta^2(x_1), x_1\bigr) = \varphi(x_2).$$

Аналогично $\varphi(x_1) = \varphi(x_3)$. Таким образом, если

$$\varphi(x_i) = q\bigl(x_i, \theta(x_i), \theta^2(x_i)\bigr),$$

то

$$\begin{aligned} &\varphi(x_1) = \varphi(x_2) = \varphi(x_3) = q_1, \quad && \varphi(x_4) = \varphi(x_5) = \varphi(x_6) = q_2, \\ &\varphi(x_7) = \varphi(x_8) = \varphi(x_9) = q_3, && \varphi(x_{10}) = \varphi(x_{11}) = \varphi(x_{12}) = q_4. \end{aligned}$$

Поэтому $q_1+q_2+q_3+q_4 = \dfrac{1}{3}\sum\limits_{i=1}^{12} \varphi(x_i) \in k$. Рассматривая вместо функции q функции q^2, q^3, q^4, получаем, что $\sum q^2, \sum q^3, \sum q^4 \in k$. Это означает, что коэффициенты многочлена $\prod(y - q_i)$ лежат в поле k.

Если r — еще один симметрический многочлен от трех переменных, то можно рассмотреть симметрические многочлены rq^l, $l = 0, 1, 2, 3$. Определим r_i точно так же, как q_i. Система уравнений $r_1q_1^l + r_2q_2^l + r_3q_3^l + r_4q_4^l = R_l$, где $l = 0, 1, 2, 3$ и $R_l \in k$, показывает, что $r_i = \Phi(q_i)$, где Φ — некоторая рациональная функция (одна и та же для всех i).

Пусть $q = t_1 + t_2 + t_3$, $r = t_1t_2 + t_2t_3 + t_3t_1$ и $\widetilde{r} = t_1t_2t_3$. Тогда $q_1 = x_1 + x_2 + x_3 = y_1$ (корень многочлена $\prod(y - q_i)$), $r_1 = x_1x_2 + x_2x_3 + x_3x_1 = \Phi(y_1)$ и $\widetilde{r}_1 = x_1x_2x_3 = \widetilde{\Phi}(y_1)$. Поэтому x_1, x_2, x_3 — корни уравнения

$$x^3 - y_1x^2 + \Phi(y_1)x - \widetilde{\Phi}(y_1) = 0,$$

где Φ и $\widetilde{\Phi}$ — рациональные функции. Это уравнение является циклическим абелевым, поскольку $x_2 = \theta(x_1)$, $x_3 = \theta^2(x_1)$ и $x_1 = \theta^3(x_1)$ □

Теорема 23.5. а) Абелево циклическое уравнение разрешимо в радикалах.

б) Решения абелева циклического уравнения степени $n = pm$ сводится к решению двух абелевых циклических уравнений степеней p и m.

Доказательство. а) Пусть f — абелев циклический многочлен степени n с корнями $x_1, \ldots, x_n$; ε — примитивный корень степени n из единицы; θ — такая рациональная функция, что $x_{k+1} = \theta^k(x_1)$ и $x_1 = \theta^n(x_1)$. Рассмотрим *резольвенту Лагранжа*

$$(\varepsilon^r, x_1) = x_1 + \varepsilon^r\theta(x_1) + \varepsilon^{2r}\theta^2(x_1) + \ldots + \varepsilon^{(n-1)r}\theta^{(n-1)}(x_1).$$

Так как $x_{k+1} = \theta^k(x_1)$, то

$$(\varepsilon^r, x_{k+1}) = \theta^k(x_1) + \varepsilon^r\theta^{k+1}(x_1) + \varepsilon^{2r}\theta^{k+2}(x_1) + \ldots = \sum \varepsilon^{sr}\theta^{k+s}(x_1).$$

Ясно, что $\theta^{k+s}(x_1) = x_1$ при $s = n-k$, поэтому $(\varepsilon^r, x_{k+1}) = \varepsilon^{(n-k)r}(\varepsilon^r, x_1)$. В частности, $(\varepsilon^r, x_{k+1})^n = (\varepsilon^r, x_1)^n$. Следовательно,

$$(\varepsilon^r, x_1)^n = (\varepsilon^r, x_2)^n = \ldots = (\varepsilon^r, x_n)^n = \frac{1}{n}\sum(\varepsilon^r, x_i)^n = u_r(\varepsilon),$$

где u_r — рациональная функция.

Таким образом,

$$x_1 + \varepsilon^r\theta(x_1) + \varepsilon^{2r}\theta^2(x_1) + \ldots + \varepsilon^{(n-1)r}\theta^{(n-1)}(x_1) = \sqrt[n]{u_r(\varepsilon)}$$

при $r = 1, \ldots, n-1$. Кроме того, для $r = 0$ получаем $x_1 + x_2 + \ldots$ $\ldots + x_n = -a_1$, где a_1 — коэффициент многочлена f при x^{n-1}. Сложим все равенства для $r = 0, 1, \ldots, n-1$. Сумма коэффициентов при x_1 будет равна n, а сумма коэффициентов при $\theta^m(x_1)$, $1 \leqslant m \leqslant n-1$, будет равна

$$1 + \varepsilon^m + \varepsilon^{2m} + \ldots + \varepsilon^{(n-1)m} = 0.$$

Итак,

$$nx_1 = a_1 + \sqrt[n]{u_1(\varepsilon)} + \ldots + \sqrt[n]{u_{n-1}(\varepsilon)}.$$

Если же равенство с номером r домножить на ε^{-kr}, то аналогично получим

$$nx_{k+1} = a_1 + \varepsilon^{-k}\sqrt[n]{u_1(\varepsilon)} + \ldots + \varepsilon^{-k(n-1)}\sqrt[n]{u_{n-1}(\varepsilon)}.$$

Несложно получить и чуть более точное выражение:

$$nx_{k+1} = a_1 + y + A_2y^2 + \ldots + A_{n-1}y^{n-1},$$

где $y = \varepsilon^{-k}\sqrt[n]{u_1(\varepsilon)}$, $A_2, \ldots, A_{n-1}$ — постоянные величины, рационально выражающиеся через ε. Действительно,

$$\frac{(\varepsilon^r, x_{k+1})}{(\varepsilon, x_{k+1})^r} = \frac{\varepsilon^{(n-k)r}(\varepsilon^r, x_1)}{\left(\varepsilon^{n-k}(\varepsilon^r, x_1)\right)^r} = \frac{(\varepsilon^r, x_1)}{(\varepsilon, x_1)^r} = \frac{\sqrt[n]{u_r(\varepsilon)}}{\left(\sqrt[n]{u_1(\varepsilon)}\right)^r} = A_r.$$

Это означает, что A_r рационально выражается через ε и симметрические функции от $x_1, \ldots, x_n$.

б) Чтобы избежать громоздких обозначений, будем считать, что $p = 3$ и $m = 4$. В общем случае доказательство то же самое. Пусть

$$\begin{aligned} y_1 &= x_1 + x_5 + x_9 = x_1 + \theta^4(x_1) + \theta^8(x_1), \\ y_2 &= x_2 + x_6 + x_{10} = \theta(x_1) + \theta^5(x_1) + \theta^9(x_1), \\ y_3 &= x_3 + x_7 + x_{11} = \theta^2(x_1) + \theta^6(x_1) + \theta^{10}(x_1), \\ y_4 &= x_4 + x_8 + x_{12} = \theta^3(x_1) + \theta^7(x_1) + \theta^{11}(x_1). \end{aligned}$$

В рассматриваемой ситуации выполняются условия теоремы 23.4 (с заменой θ на θ^4), поэтому x_1, $\theta^4(x_1)$ и $\theta^8(x_1)$ — корни циклического абелева уравнения степени $p = 3$, коэффициенты которого являются рациональными функциями от y_1. Кроме того, y_1, y_2, y_3 и y_4 — корни уравнения степени $m = 4$ с рациональными коэффициентами. Нужно лишь доказать, что это уравнение является циклическим абелевым.

Пусть

$$q_l(x) = \bigl(\theta(x_1) + \theta^5(x_1) + \theta^9(x_1)\bigr)\bigl(x_1 + \theta^4(x_1) + \theta^8(x_1)\bigr)^l.$$

Тогда $q_l(x_1) = y_2 y_1^l$. Кроме того,

$$q_l(x_5) = (x_6 + x_{10} + x_2)(x_5 + x_9 + x_1)^l = q_l(x_1).$$

Аналогично $q_l(x_9) = q_l(x_5)$. Аналогичные рассуждения показывают, что

$$\begin{aligned} y_3 y_2^l &= q_l(x_2) = q_l(x_6) = q_l(x_{10}), \\ y_4 y_3^l &= q_l(x_3) = q_l(x_7) = q_l(x_{11}), \\ y_1 y_4^l &= q_l(x_4) = q_l(x_8) = q_l(x_{12}). \end{aligned}$$

Следовательно, $y_2 y_1^l + y_3 y_2^l + y_4 y_3^l + y_1 y_4^l = \dfrac{1}{4}\sum\limits_{i=1}^{12} q_l(x_i) \in k$. Система уравнений $y_2 y_1^l + \ldots + y_1 y_4^l = T_l$, где $l = 0, 1, 2, 3$ и $T_l \in k$, показывает, что $y_2 = \varphi(y_1)$, $y_3 = \varphi(y_2)$, $y_4 = \varphi(y_3)$ и $y_1 = \varphi(y_4)$. □

Следствие. Циклическое абелево уравнение степени 2^n решается в квадратных радикалах.

23.5. Критерий Абеля–Галуа разрешимости уравнения простой степени

Эварист Галуа погиб на дуэли, не успев опубликовать своих основных исследований по теории разрешимости уравнений в радикалах. Но некоторые свои результаты он всё же успел опубликовать. В небольшой

заметке в «Bulletin des Sciences mathématiques» (1830) Галуа сообщал, что он пришел к следующему результату:

Для того чтобы уравнение простой степени решалось в радикалах, необходимо и достаточно, чтобы при знании двух каких-нибудь его корней остальные выводились из них рационально.

Интересно отметить, что в 1828 г. Абель писал Креллю, что он нашел критерий разрешимости в радикалах уравнения простой степени. Абель сформулировал свой критерий почти так же, как и Галуа: «В любой тройке корней один корень должен рационально выражаться через два других». Но никаких свидетельств о доказательстве Абеля не сохранилось.

Теорема 23.6. а) Неприводимое над $\mathbb{Q}$ уравнение $f = 0$ простой степени p разрешимо в радикалах тогда и только тогда, когда его корни можно занумеровать так, что любая подстановка σ из группы Галуа будет иметь вид $\sigma(i) \equiv ai + b \pmod{p}$, где $a \not\equiv 0 \pmod{p}$.

б) Неприводимое над $\mathbb{Q}$ уравнение $f = 0$ простой степени p разрешимо в радикалах тогда и только тогда, когда все его корни рационально выражаются через любые два корня. (Иными словами, если $\alpha_1, \ldots, \alpha_p$ — корни уравнения, то $\mathbb{Q}(\alpha_1, \ldots, \alpha_p) = \mathbb{Q}(\alpha_i, \alpha_j)$ для любых различных i и j).

Доказательство. а) Для указанной группы закон умножения имеет вид $[a_1, b_1][a_2, b_2] = [a_1a_2, a_1b_2 + b_1]$. Разрешимость такой группы доказана в теореме о простых радикальных расширениях (теорема 22.9 на с. 220). Поэтому остается доказать, что если неприводимое уравнение простой степени p разрешимо в радикалах, то его группа Галуа состоит из преобразований указанного вида.

При доказательстве теоремы об уравнениях, разрешимых в радикалах, было показано, что для разрешимого в радикалах уравнения $f = 0$ существует последовательность радикальных расширений простых степеней

$$L = L'_r \supset L'_{r-1} \supset \ldots \supset L'_0 = L_0(\varepsilon) \supset L_0 = \mathbb{Q},$$

где ε — примитивный корень из единицы степени $[L : \mathbb{Q}]$, расширение $L \supset \mathbb{Q}$ нормально и поле L содержит поле разложения N многочлена f. При этом $G(N, \mathbb{Q})$ — факторгруппа $G(L, \mathbb{Q})$ по $G(L, N)$. Поэтому достаточно доказать, что любой автоморфизм поля L над $\mathbb{Q}$ переставляет корни многочлена f указанным выше образом, т. е. корень с номером i заменяется на корень с номером $ai + b$.

Можно считать, что поле L'_{r-1} содержит не все корни многочлена f. Доказательство теоремы основано на том, что многочлен f неприводим над L'_{r-1} и степень расширения $L \supset L'_{r-1}$ равна p. Это означает, что до самого последнего радикального расширения многочлен f остается неприводимым, а на последнем шаге он сразу разлагается на линейные множители. Требуемое утверждение очевидным образом вытекает из следующей леммы.

Лемма. Пусть многочлен f неприводим над полем k, содержащем примитивный корень из единицы степени q, где q — простое число. Пусть, далее, $K = k(\beta)$, где $\beta^q \in k$. Тогда многочлен f над полем K либо неприводим, либо разлагается на q неприводимых множителей одинаковой степени.

Доказательство. Пусть L — поле разложения многочлена f над k. Поле k содержит примитивный корень степени q из единицы, поэтому $L(\beta)$ — поле разложения многочлена f над $k(\beta)$.

Последовательности расширений $L(\beta) \supset k(\beta) \supset k$ и $L(\beta) \supset L \supset k$ дают точные последовательности

$$\begin{array}{ccccccccc} 0 & \to & G(L(\beta),k(\beta)) & \to & G(L(\beta),k) & \to & G(k(\beta),k) & \to & 0, \\ & & & & \| & & & & \\ 0 & \to & G(L(\beta),L) & \to & G(L(\beta),k) & \to & G(L,k) & \to & 0. \end{array}$$

Поэтому

$$\big|G\big(L(\beta),k(\beta)\big)\big| \cdot \big|G\big(k(\beta),k\big)\big| = \big|G(L,k)\big| \cdot \big|G\big(L(\beta),L\big)\big|,$$

Согласно теореме 22.5 (см. с. 218) группы $G\big(L(\beta),k(\beta)\big)$ и $G(L(\beta),L)$ являются, соответственно, подгруппами в $G(L,k)$ и $G\big(k(\beta),k\big)$. Кроме того, согласно теореме 22.9 (б) на с. 220 группы $G\big(L(\beta),L\big)$ и $G\big(k(\beta),k\big)$ являются подгруппами группы $\mathbb{Z}/q\mathbb{Z}$. По условию q — простое число. Поэтому в $\mathbb{Z}/q\mathbb{Z}$ нет нетривиальных подгрупп, а значит,

$$\Big[G(L,k) : G\big(L(\beta),k(\beta)\big)\Big] = 1 \text{ или } q,$$

причем индекс равен q лишь в том случае, когда группа $G\big(L(\beta),L\big)$ тривиальна, т. е. $G\big(L(\beta),k\big) \cong G(L,k)$. В этом случае $G\big(L(\beta),k(\beta)\big)$ — нормальная подгруппа в $G(L,k)$ индекса q.

Напомним, что многочлен (без кратных корней) неприводим тогда и только тогда, когда его группа Галуа транзитивно действует на корнях (теорема 22.6 на с. 219). Поэтому нужно рассмотреть лишь случай, когда $H = G(L(\beta), k(\beta))$ — нормальная подгруппа в $G = G(L, k)$ индекса q. В этом случае $G/H \cong \mathbb{Z}/q\mathbb{Z}$, поэтому $G = \{H, gH, g^2H, \ldots, g^{q-1}H\}$ для некоторого $g \in G$. Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена f. Положим $H\alpha_i = \{h(\alpha_i) \mid h \in H\}$. Множества $H\alpha_i$ и $H\alpha_j$ либо совпадают, либо не пересекаются. Поэтому множества $H\alpha_1$ и $gH\alpha_1 = Hg(\alpha_1)$ либо совпадают, либо не пересекаются. В первом случае группа H действует на множестве корней транзитивно, а во втором случае множество корней разбивается на q подмножеств одинаковой мощности, на каждом из которых группа H действует транзитивно. Пусть $n = rq$ и H транзитивно действует на множестве $\alpha_{i_1}, \ldots, \alpha_{i_r}$. Тогда H сохраняет все коэффициенты многочлена $(x-\alpha_{i_1})\cdot\ldots\cdot(x-\alpha_{i_r})$, а значит, этот многочлен является неприводимым многочленом над полем $k(\beta)$. □

Итак, многочлен f неприводим над полем L'_{r-1} и разлагается над полем $L'_r = L'_{r-1}(\beta)$, где $\beta^q \in L'_{r-1}$, на линейные множители. Это означает, в частности, что $q = p$. Таким образом, $L = L'_r$ — циклическое расширение степени p поля L'_{r-1}, причем поле L'_{r-1} содержит примитивный корень степени p из единицы. Следовательно, $G(L, L'_{r-1}) = \mathbb{Z}/p\mathbb{Z}$. Пусть σ — образующая этой группы. Корни $\alpha_1, \ldots, \alpha_p$ многочлена f можно занумеровать так, что $\sigma(i) = i + 1$, т. е. σ переводит α_i в α_{i+1}.

Группа $G(L, L'_{r-1})$ является нормальной подгруппой в $G(L, L'_{r-2})$. Пусть τ — произвольная подстановка из группы $G(L, L'_{r-2})$. Тогда $\tau\sigma\tau^{-1} \in G(L, L'_{r-1})$, т. е. $\tau\sigma\tau^{-1} = \sigma^a$ для некоторого a. Это означает, что $\tau\sigma(i) = \sigma^a\tau(i)$, т. е. $\tau(i+1) = \tau(i) + a$. Таким образом,

$$\begin{aligned}
&\tau(2) = \tau(1) + a,\\
&\tau(3) = \tau(2) + a = \tau(1) + 2a,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\tau(i) = \tau(1) + (i-1)a = ai + (\tau(1) - a) = ai + b,
\end{aligned}$$

где $b = \tau(1) - a$. Подстановка τ имеет требуемый вид.

Докажем теперь, что если в группе $G(L, L'_m)$ все подстановки имеют вид $\tau(i) = ai + b$, то в группе $G(L, L'_{m-1})$ все подстановки тоже имеют такой же вид. Для доказательства мы воспользуемся тем, что $G(L, L'_m)$ содержит подстановку $\sigma(i) = i + 1$ и $G(L, L'_m)$ является нормальной подгруппой в $G(L, L'_{m-1})$. Пусть μ — произвольная подстановка из группы

$G(L, L'_{m-1})$. Тогда $\mu\sigma\mu^{-1} \in G(L, L'_m)$, поэтому $\mu\sigma\mu^{-1}(i) = ai + b$. Для $j = \mu^{-1}(i)$ получаем $\mu\sigma(j) = a\mu(j) + b$, т. е. $\mu(j+1) = a\mu(j) + b$. Прежде всего докажем, что $a = 1$. Действительно,

$$\begin{aligned}
&\mu(2) = a\mu(1) + b,\\
&\mu(3) = a\mu(2) + b = a^2\mu(1) + ab + b,\\
&\mu(4) = a\mu(3) + b = a^3\mu(1) + a^2b + ab + b,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\mu(j) = a^{j-1}\mu(1) + (a^{j-2} + a^{j-3} + \ldots + a + 1)b.
\end{aligned}$$

Следовательно, $\mu(1) = \mu(p+1) = a^p\mu(1) + (a^{p-1} + a^{p-2} + \ldots + a + 1)b$, т. е.

$$(1 - a^p)\mu(1) \equiv (a^{p-1} + a^{p-2} + \ldots + a + 1)b \pmod{p}.$$

Умножим обе части на $1 - a$ и воспользуемся тем, что $a^p \equiv a \pmod{p}$. В результате получим

$$(1 - a)^2\mu(1) \equiv (1 - a)b \pmod{p}.$$

Если $a \not\equiv 1 \pmod{p}$, то $\mu(1) \equiv (1 - a)^{-1}b \pmod{p}$. Но тогда те же самые рассуждения показывают, что $\mu(2) \equiv (1 - a)^{-1}b \pmod{p}$, чего не может быть.

б) Если неприводимое уравнение простой степени разрешимо в радикалах, то его группа Галуа состоит из преобразований вида $i \mapsto ai + b$. Любое преобразование такого вида, имеющее две неподвижные точки, тождественно. Это означает, что после присоединения двух корней α_i и α_j группа Галуа сводится к тождественному преобразованию, т. е. все корни лежат в $\mathbb{Q}(\alpha_i, \alpha_j)$.

Предположим теперь, что для любых двух различных корней α_i и α_j поле $\mathbb{Q}(\alpha_i, \alpha_j)$ содержит все остальные корни. Это означает, что если преобразование из группы Галуа оставляет неподвижными два корня, то оно оставляет неподвижными и все остальные корни, т. е. любое нетождественное преобразование имеет не более одной неподвижной точки.

Группа Галуа G транзитивно действует на p-элементном множестве $\{\alpha_1, \ldots, \alpha_p\}$, поэтому $|G|$ делится на p.

Лемма. Если число элементов группы G делится на простое число p, то группа G содержит элемент порядка p.

Доказательство. Пусть $|G| = n = mp$. Применим индукцию по m. При $m = 1$ утверждение очевидно. Если в G есть собственная подгруппа H, для которой индекс $[G : H]$ не делится на p, то $|H|$ делится на p и можно воспользоваться предположением индукции. Поэтому можно считать, что индекс любой собственной подгруппы делится на p.

Для $x \in G$ рассмотрим подгруппу $N_x = \{g \in G \mid gxg^{-1} = x\}$ и класс сопряженных элементов $G_x = \{gxg^{-1} \mid g \in G\}$. Ясно, что $|G_x| = [G : N_x]$. Классы сопряженных элементов либо не пересекаются, либо совпадают, поэтому $n = n_1 + \ldots + n_s$, где n_i — число элементов в i-м классе сопряженности. По условию число n_i либо равно 1, либо делится на p. Если $n_i = 1$, то соответствующий элемент x коммутирует со всеми элементами группы G, т. е. лежит в ее центре $Z(G)$. Количество n_i, равных 1, делится на p и отлично от нуля (единичному элементу группы соответствует $n_i = 1$), поэтому $Z(G)$ — абелева группа, порядок которой делится на p. Следовательно, в $Z(G)$ есть элемент порядка p. □

Элемент σ порядка p в группе $G \subset S_p$ является циклом длины p. После перенумерации корней можно считать, что $\sigma(i) = i + 1$. Покажем, что элемент σ порождает в G нормальную подгруппу. Пусть $\tau \in G$. Тогда $\tau\sigma\tau^{-1} \neq \mathrm{id}$ и $(\tau\sigma\tau^{-1})^p = \mathrm{id}$, т. е. $\tau\sigma\tau^{-1}$ — цикл длины p. Пусть $\tau\sigma\tau^{-1}(i) = i + a(i) = \sigma^{a(i)}(i)$. У цикла длины p в группе S_p не может быть неподвижных точек, поэтому $a(i) \neq 0$ для всех i. Таким образом, функция $a(i)$ на p-элементном множестве принимает не более $p-1$ различных значений, поэтому некоторое значение a она принимает в двух различных точках i и j. Это означает, что преобразование $\sigma^{-a}\tau\sigma\tau^{-1}$ имеет две неподвижные точки. Но любое преобразование из группы G, имеющее две неподвижные точки, тождественно. Поэтому $\tau\sigma\tau^{-1}(i) = \sigma^a$.

Из равенства $\tau\sigma\tau^{-1}(i) = \sigma^a$ следует, что $\tau(i) = ai + b$, где $b = \tau(1) - a$. Группа, состоящая из подстановок такого вида, разрешима. □

Следствие (Кронекер). Если неприводимое над $\mathbb{Q}$ уравнение простой степени $p \geqslant 3$ разрешимо в радикалах, то количество его вещественных корней равно 1 или p.

Доказательство. Число p нечетно, поэтому уравнение степени p имеет хотя бы один вещественный корень. Если разрешимое в радикалах уравнение простой степени p имеет два вещественных корня α_i и α_j, то все его корни лежат в $\mathbb{Q}(\alpha_i, \alpha_j) \subset \mathbb{R}$. □

24. Вычисление групп Галуа

24.1. Дискриминант и группа Галуа

Теорема 24.1. Пусть $A_n \subset S_n$ — знакопеременная группа (т. е. группа четных подстановок), $f \in \mathbb{Z}[x]$ — неприводимый многочлен степени n со страшим коэффициентом 1. Тогда группа Галуа многочлена f над $\mathbb{Q}$ содержится в A_n в том и только том случае, когда дискриминант $D(f)$ является полным квадратом.

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена f. Тогда $D(f) = \prod\limits_{i<j} (\alpha_i - \alpha_j)^2$. Рассмотрим число $\delta = \delta(f) = \prod\limits_{i<j} (\alpha_i - \alpha_j)$. Если $\sigma \in G_{\mathbb{Q}}(f)$, то

$$\sigma(\delta) = \prod_{i<j} \bigl(\sigma(\alpha_i) - \sigma(\alpha_j)\bigr) = (-1)^{\sigma}\delta.$$

По условию многочлен f неприводим. Поэтому, в частности, $\delta \neq 0$. Следовательно, все автоморфизмы $\sigma \in G_{\mathbb{Q}}(f)$ сохраняют δ тогда и только тогда, когда $G_{\mathbb{Q}}(f) \subset A_n$. С другой стороны, все автоморфизмы $\sigma \in G_{\mathbb{Q}}(f)$ сохраняют δ тогда и только тогда, когда $\delta \in \mathbb{Q}$. □

Пример. Пусть $f(x) = x^3 + ax^2 + bx + c$ — неприводимый многочлен над $\mathbb{Z}$, D — его дискриминант. Тогда $G_{\mathbb{Q}}(f) = A_3$, если $\sqrt{D} \in \mathbb{Q}$, и $G_{\mathbb{Q}}(f) = S_3$, если $\sqrt{D} \notin \mathbb{Q}$.

Доказательство. Многочлен f неприводим, поэтому группа Галуа $G_{\mathbb{Q}}(f)$ транзитивна. В S_3 есть только одна транзитивная группа, отличная от S_3, а именно, A_3. □

24.2. Резольвентные многочлены

Пусть $\varphi \in \mathbb{Q}[x_1, \ldots, x_n]$ и G_φ — группа, состоящая из подстановок $\sigma \in S_n$, для которых $\sigma\varphi = \varphi$, т. е.

$$\varphi(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = \varphi(x_1, \ldots, x_n).$$

Под действием элементов S_n из функции φ получаются различные функции $\varphi_1 = \varphi$, $\varphi_2 = \tau_2\varphi, \ldots, \varphi_m = \tau_m\varphi$. При этом $m = |S_n|/|G_\varphi|$.

Пример 24.1. Если $\varphi = x_1x_2 + x_3x_4$, то G_φ состоит из тождественной подстановки и подстановок (12), (34), (12)(34), (13)(24), (14)(23), (1324) и (1423). При этом $\varphi_2 = x_1x_3 + x_2x_4$ и $\varphi_3 = x_1x_4 + x_2x_3$.

Легко проверить, что $G_{\varphi_i} = \tau_i G_\varphi \tau_i^{-1}$. В самом деле, равенство $\sigma\varphi_i = \varphi_i$ эквивалентно равенству $\sigma\tau_i\varphi = \tau_i\varphi$. Поэтому $\tau_i^{-1}\sigma\tau_i \in G_{\varphi_i}$, т. е. $\sigma \in \tau_i G_{\varphi_i}\tau_i^{-1}$.

Пусть $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ — многочлен с целыми коэффициентами и $\varphi \in \mathbb{Z}[x_1, \ldots, x_n]$. Определим группу G_{φ_i} и многочлены $\varphi_1, \ldots, \varphi_m$, как и выше. *Резольвентным многочленом* называют многочлен

$$\mathrm{Res}(\varphi, f)(x) = \prod_{i=1}^{m} \bigl(x - \varphi_i(\alpha_1, \ldots, \alpha_n)\bigr),$$

где $\alpha_1, \ldots, \alpha_n$ — корни многочлена f.

Коэффициенты резольвентного многочлена целые, поэтому его можно вычислить, приближенно вычислив корни многочлена f. (Коэффициенты резольвентного многочлена вычисляются с достаточной точностью и округляются до ближайшего целого числа.)

Теорема 24.2. Пусть резольвентный многочлен $\mathrm{Res}(\varphi, f)$ не имеет кратных корней. В таком случае группа Галуа многочлена f над $\mathbb{Q}$ содержится в группе, сопряженной группе G_φ, тогда и только тогда, когда многочлен $\mathrm{Res}(\varphi, f)$ имеет целочисленный корень.

Доказательство. Предположим сначала, что

$$G_{\mathbb{Q}}(f) \subset \tau G_\varphi \tau^{-1} = G_{\varphi_i},$$

где $\varphi_i = \tau\varphi$. Тогда число $\varphi_i(\alpha_1, \ldots, \alpha_n)$, являющееся корнем многочлена $\mathrm{Res}(\varphi, f)$, сохраняется под действием всех преобразований из группы Галуа, поэтому оно рационально. Но числа $\alpha_1, \ldots, \alpha_n$ — целые алгебраические, а коэффициенты многочлена φ_i целые, поэтому число $\varphi_i(\alpha_1, \ldots, \alpha_n)$ целое.

Предположим теперь, что число $\varphi_i(\alpha_1, \ldots, \alpha_n)$ целое. По условию у резольвентного многочлена нет кратных корней. Это означает, что если

$$\sigma\varphi_i(\alpha_1, \ldots, \alpha_n) = \varphi_j(\alpha_1, \ldots, \alpha_n),$$

то $\tau_j^{-1}\sigma\tau_i \in G_\varphi$. Любая подстановка σ из группы Галуа сохраняет целое число $\varphi_i(\alpha_1, \ldots, \alpha_n)$, поэтому для нее $i = j$, т. е. $\sigma \in \tau_i G_\varphi \tau_i^{-1}$. □

Воспользовавшись теоремами 24.1 и 24.2, можно вычислить группу Галуа любого неприводимого многочлена $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$

с целыми коэффициентами. Прежде всего заметим, что в S_4 с точностью до сопряженности есть лишь следующие транзитивные подгруппы:

1) вся группа S_4;

2) знакопеременная группа A_4;

3) группа диэдра порядка 8, описанная в примере 24.1; эту группу обозначим D_4;

4) группа Клейна порядка 4, состоящая из подстановок (12)(34), (13)(24) и (14)(23); эту группу обозначим V_4;

5) циклическая группа $\mathbb{Z}_4$, порожденная циклом (1234).

Имеют место следующие включения: $V_4 \subset D_4 \cap A_4$ и $\mathbb{Z}_4 \subset D_4$, причем $\mathbb{Z}_4 \not\subset A_4$.

Вычисление группы Галуа начнем с того, что вычислим дискриминант D многочлена f и резольвентный многочлен $\operatorname{Res}(\varphi, f)(x)$ для $\varphi = x_1x_2 + x_3x_4$. Несложные вычисления показывают, что

$$\operatorname{Res}(\varphi, f)(x) = x^3 - a_2x^2 - (a_1a_3 - 4a_4)x - a_4a_1^2 - 4a_4a_2 - a_3^2.$$

Легко проверить, что у многочлена $\operatorname{Res}(\varphi, f)(x)$ нет кратных корней. Пусть, например, $\alpha_1\alpha_2 + \alpha_3\alpha_4 = \alpha_1\alpha_3 + \alpha_2\alpha_4$. Тогда $(\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) = 0$. Но у многочлена f нет кратных корней, поэтому $\alpha_1 \neq \alpha_4$ и $\alpha_2 \neq \alpha_3$.

Если у результантного многочлена нет целочисленных корней, то группа Галуа равна S_4 или A_4. Различить эти группы можно с помощью дискриминанта D: если D — полный квадрат, то группа Галуа равна A_4; в противном случае она равна S_4.

Если же у результантного многочлена есть целочисленный корень, то группа Галуа равна $\mathbb{Z}_4$, V_4 или D_4. Из этих групп только V_4 содержится в A_4. Поэтому если $\sqrt{D}$ — целое число, то группа Галуа равна V_4; в противном случае она равна $\mathbb{Z}_4$ или D_4.

Различить группы $\mathbb{Z}_4$ и D_4 можно с помощью резольвентного многочлена, построенного по функции

$$\varphi = x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2,$$

для которой $G_\varphi = \mathbb{Z}_4$. Но в этом случае у резольвентного многочлена (степени 6) уже могут быть кратные корни. Например, равенство

$$\alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_4^2 + \alpha_4\alpha_1^2 = \alpha_1\alpha_2^2 + \alpha_2\alpha_4^2 + \alpha_4\alpha_3^2 + \alpha_3\alpha_1^2$$

эквивалентно равенству

$$(\alpha_1 - \alpha_2)(\alpha_3 + \alpha_4) + \alpha_3\alpha_4 = 0. \tag{1}$$

Но если каждый корень α_i заменить на $\alpha_i + a$, то при некотором a равенство (1) уже не будет выполняться.

В общем случае от кратных корней резольвентного многочлена можно избавиться, применив более сложное преобразование Чирнгауза. Это — практическая рекомендация. Теоретически же можно воспользоваться следующим утверждением.

Теорема 24.3. Пусть $f \in \mathbb{Z}[x]$ — многочлен степени n без кратных корней и $G \subset S_n$ — произвольная подгруппа. Тогда для них существует такая функция $\varphi \in \mathbb{Z}[x_1, \ldots, x_n]$, что $G_\varphi = G$ и резольвентный многочлен $\operatorname{Res}(\varphi, f)$ не имеет кратных корней.

Доказательство. Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена f. При построении резольвенты Галуа мы показали, что существуют такие целые числа $m_1, \ldots, m_n$, что для всех подстановок $\sigma \in S_n$ числа $m_1\alpha_{\sigma(1)} + \ldots$ $\ldots + m_n\alpha_{\sigma(n)}$ попарно различны. Положим

$$\psi(t, x_1, \ldots, x_n) = \prod_{\sigma \in G} (t - m_1\alpha_{\sigma(1)} - \ldots - m_n\alpha_{\sigma(n)}).$$

Для любой подстановки $\tau \in S_n$ можно рассмотреть многочлен

$$\tau\psi(t, x_1, \ldots, x_n) = \psi(t, x_{\tau(1)}, \ldots, x_{\tau(n)}).$$

Многочлены $\tau_1\psi$ и $\tau_2\psi$ различны тогда и только тогда, когда они различны как многочлены от t при фиксированных $x_1 = \alpha_1, \ldots, x_n = \alpha_n$.

Под действием элементов группы S_n из функции $\psi(t, x_1, \ldots, x_n) = \psi$ получаются различные функции $\psi_1 = \psi, \psi_2, \ldots, \psi_m$. При этом многочлены от t вида $\psi_1(t, \alpha_1, \ldots, \alpha_n), \ldots, \psi_m(t, \alpha_1, \ldots, \alpha_n)$ тоже попарно различны. Поэтому существует $t_0 \in \mathbb{Z}$, для которого числа $\psi_1(t_0, \alpha_1, \ldots, \alpha_n)$, $\ldots, \psi_m(t_0, \alpha_1, \ldots, \alpha_n)$ попарно различны. В таком случае многочлен

$$\begin{aligned}\varphi(x_1, \ldots, x_n) &= \psi(t_0, x_1, \ldots, x_n) = \\ &= \prod_{\sigma \in G} (t_0 - m_1\alpha_{\sigma(1)} - \ldots - m_n\alpha_{\sigma(n)})\end{aligned}$$

искомый. В самом деле, если $\tau \notin G$, то многочлены $\varphi(x_1, \ldots, x_n)$ и $\tau\varphi(x_1, \ldots, x_n)$ различны, поскольку различны их значения в точке $x_1 = \alpha_1, \ldots, x_n = \alpha_n$. □

24.3. Группа Галуа по модулю p

Пусть $f(x) = x^n + a_1x^{n-1} + \ldots + a_n$ — неприводимый многочлен с целыми коэффициентами. Для любого простого числа p можно рассмотреть многочлен $f \pmod p$ над полем $\mathbb{F}_p$ (коэффициенты многочлена f заменяются на соответствующие классы вычетов по модулю p). Многочлен $f \pmod p$ может оказаться приводимым; структура его разложения на неприводимые множители тесно связана со структурой группы Галуа многочлена f над $\mathbb{Q}$. Эту связь мы сейчас изучим и воспользуемся ей для вычисления некоторых групп Галуа.

Мы будем рассматривать лишь такие простые числа p, для которых многочлен $f \pmod p$ не имеет кратных корней, т. е. многочлены $f \pmod p$ и $f' \pmod p$ взаимно просты. Последнее условие эквивалентно тому, что p не делит $R(f, f') = \pm D(f)$. В дальнейшем будем предполагать, что дискриминант $D(f)$ не делится на p.

Корни многочлена $f \pmod p$ не обязательно лежат в поле $\mathbb{F}_p$, но существует конечное расширение поля $\mathbb{F}_p$, содержащее все корни многочлена $f \pmod p$. Чтобы построить такое расширение, достаточно научиться к произвольному конечному полю $\mathbb{F}_q$ присоединять корень неприводимого над $\mathbb{F}_q$ многочлена h. Легко проверить, что факторкольцо

$$K = \mathbb{F}_q[x]/h(x)\mathbb{F}_q[x]$$

является полем. Действительно, если многочлен $g(x) \in \mathbb{F}_q[x]$ не делится на $h(x)$, то он взаимно прост с $h(x)$, поэтому $u(x)g(x) + v(x)h(x) = 1$ для некоторых $u(x), v(x) \in \mathbb{F}_q[x]$. Следовательно, $u \equiv g^{-1} \pmod{h(x)}$. Ясно, что $K = \mathbb{F}_q(\alpha)$, где α — образ элемента x при канонической проекции. При этом $h(\alpha) = 0$, т. е. α — корень многочлена h.

Присоединив к $\mathbb{F}_p$ все корни $\alpha_1, \ldots, \alpha_n$ многочлена $f \pmod p$, получим поле $\mathbb{F}_p(\alpha_1, \ldots, \alpha_n) \cong \mathbb{F}_{p^r}$. Пусть Gal — группа Галуа многочлена f над $\mathbb{Q}$, Gal_p — группа автоморфизмов поля $\mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$ над полем $\mathbb{F}_p$. Любой такой автоморфизм переводит корень α_i в некоторый корень α_j и подстановка корней однозначно задает автоморфизм. Поэтому после нумерации корней можно считать, что Gal_p — подгруппа в S_n. Отметим, что корни многочленов f и $f \pmod p$ лежат в разных множествах, причем между корнями этих многочленов нет естественного взаимно однозначного соответствия.

Теорема 24.4. а) При подходящей нумерации корней многочленов f и $f \pmod p$ группа Gal_p является подгруппой группы Gal.

б) Группа Gal_p является циклической группой порядка r, где r — степень расширения $\mathbb{F}_p(\alpha_1, \ldots, \alpha_n)$ поля $\mathbb{F}_p$.

в) Если многочлен $f \pmod p$ представляет собой произведение неприводимых множителей степеней $n_1, \ldots, n_k$, то группа Gal_p содержит произведение (непересекающихся) циклов, длины которых равны $n_1, \ldots, n_k$.

Доказательство. а) Многочлен, аналогичный резольвенте Галуа, можно построить, заменив целые числа $m_1, \ldots, m_n$ на переменные $u_1, \ldots, u_n$. А именно, пусть $\beta_1, \ldots, \beta_n$ — корни многочлена f. Рассмотрим многочлен

$$F(x, u_1, \ldots, u_n) = \prod_{\sigma \in G} (x - u_1\beta_{\sigma(1)} - \ldots - u_n\beta_{\sigma(n)})$$

и выделим у него неприводимый над $\mathbb{Z}$ множитель $G(x, u_1, \ldots, u_n)$, делящийся на $x - u_1\beta_1 - \ldots - u_n\beta_n$. Точно так же, как и для резольвенты Галуа, доказывается, что группа Галуа Gal состоит из подстановок, соответствующих линейным делителям многочлена G.

Над полем $\mathbb{F}_p$ многочлен $G \pmod p$ разлагается на неприводимые множители $G_1 \pmod p, \ldots, G_l \pmod p$. Любая подстановка корней $\alpha_1, \ldots, \alpha_n$ многочлена $f \pmod p$, принадлежащая группе Gal_p, переводит многочлен $G_i \pmod p$ в тот же самый многочлен $G_i \pmod p$. Поэтому та же самая подстановка корней $\beta_1, \ldots, \beta_n$ не может переводить $G(x, u_1, \ldots, u_n)$ в другой неприводимый множитель многочлена $F(x, u_1, \ldots, u_n)$, поскольку у многочлена $F \pmod p$ нет кратных делителей.

б) В поле характеристики p выполняется соотношение $(x + y)^p = x^p + y^p$. Таким образом, если $x \neq y$, то $x^p - y^p = (x - y)^p \neq 0$. Поэтому отображение $x \mapsto x^p$ является автоморфизмом поля $\mathbb{F}_{p^r}$, оставляющим неподвижными элементы поля $\mathbb{F}_p$. Степени этого автоморфизма переводят x в $x^p, x^{p^2}, \ldots, x^{p^r} = x$. Поле $\mathbb{F}_{p^r}$ получается из поля $\mathbb{F}_p$ присоединением корня ζ многочлена $x^{q-1} - 1$, где $q = p^r$. При этом $\zeta^a \neq \zeta^b$, если $0 < a < b \leqslant q - 1$. Следовательно, автоморфизмы $x \mapsto x^p, x \mapsto x^{p^2}, \ldots, x \mapsto x^{p^r} = x$ попарно различны. С другой стороны, степень расширения $\mathbb{F}_{p^r} \supset \mathbb{F}_p$ равна r, поэтому ζ удовлетворяет уравнению степени r над полем $\mathbb{F}_p$. Любой автоморфизм поля $\mathbb{F}_{p^r}$ над полем $\mathbb{F}_p$ однозначно задается образом элемента ζ, поэтому количество различных автоморфизмов не превосходит r.

в) Группа Gal_p циклическая, поэтому она порождена некоторой подстановкой σ. Представим эту подстановку в виде произведения непересекающихся циклов:

$$\sigma = (1\,2\,\ldots\,j)(j{+}1\,\ldots)\ldots(\ldots\,n).$$

Группа Gal_p транзитивно действует на элементах каждого цикла, поэтому циклы соответствуют неприводимым множителям многочлена $f \pmod p$. □

Пример. Группа Галуа многочлена $x^5 - x - 1$ над $\mathbb{Q}$ равна S_5.

Доказательство. По модулю 2 рассматриваемый многочлен раскладывается на неприводимые множители x^2+x+1 и x^3+x^2+1, поэтому его группа Галуа содержит подстановку вида $(ij)(klm)$.

По модулю 3 многочлен $x^5 - x - 1$ неприводим. В самом деле, если бы этот многочлен был приводим, то у него был бы множитель степени 1 или 2. Произведение всех неприводимых многочленов степени 1 или 2 над полем $\mathbb{F}_3$ равно $x^9 - x$ (см. теорему 13.7 на с. 115). Поэтому многочлен $x^5 - x - 1$ должен иметь общий делитель либо с многочленом $x^5 - x$, либо с многочленом $x^5 + x$, а этого не может быть. Следовательно, группа Галуа содержит цикл (12345).

Группа Галуа содержит подстановку $\big((ij)(klm)\big)^3 = (ij)$. Сопрягая транспозицию (ij) элементом $(12345)^a$, получаем транспозицию $(i+a, j+a)$. При $a = j - i$ последовательно получаем транспозиции (ij), (jp), (pq), (qr), (ri), которые порождают всю группу S_5. □

Фробениус доказал, что если группа Галуа неприводимого многочлена f степени n содержит подстановку, представляющую собой произведение циклов, длины которых равны $n_1, \ldots, n_k$, то существует бесконечно много простых чисел p, для которых многочлен $f \pmod p$ разлагается на неприводимые множители степеней $n_1, \ldots, n_k$. Он вычислил также плотность таких простых чисел p. По поводу теоремы плотности Фробениуса и обобщающей ее теоремы плотности Чеботарева см. [J], [Че], [АТЧ] и [C].

Глава 6
Идеалы в кольцах многочленов

25. Теоремы Гильберта о базисе и о нулях

25.1. Теорема Гильберта о базисе

Теорема Гильберта о базисе появилась в знаменитой работе [Hi2]. В этой работе были предложены совершенно новые методы, с помощью которых удалось доказать существование конечного базиса для инвариантов форм. До этого, в 1868 г., Гордан доказал существование конечного базиса лишь для бинарных форм, причем сделано это было весьма трудоемким перебором. Гильберту же удалось сразу решить ряд центральных проблем теории инвариантов. Правда, его методы были неконструктивны, что побудило Гордана заявить: «Это не математика, это теология!»

Пусть K — некоторое поле (например, $\mathbb{Q}$, $\mathbb{R}$ или $\mathbb{C}$) или кольцо $\mathbb{Z}$, $K[x_1, \ldots, x_n]$ — кольцо многочленов от n переменных с коэффициентами из K.

Теорема 25.1 (Гильберт). Пусть $M \subset K[x_1, \ldots, x_n]$ — произвольное подмножество. Тогда существует такой конечный набор многочленов $m_1, \ldots, m_r \in M$, что любой многочлен $m \in M$ можно представить в виде $m = \lambda_1 m_1 + \ldots + \lambda_r m_r$, где $\lambda_i \in K[x_1, \ldots, x_n]$.

Теорему Гильберта удобнее сформулировать на языке идеалов. Тогда ее будет проще доказывать.

Подмножество $I \subset K[x_1, \ldots, x_n]$ называют *идеалом*, если выполняются следующие два условия:

1) $a, b \in I \Rightarrow a + b \in I$;

2) $a \in I$, $f \in K[x_1, \ldots, x_n] \Rightarrow fa \in I$.

Для любого множества $M \subset K[x_1, \ldots, x_n]$ можно рассмотреть порожденный им идеал $I(M)$, состоящий из всевозможных конечных сумм вида $\lambda_1 m_1 + \ldots + \lambda_r m_r$, где $\lambda_i \in K[x_1, \ldots, x_n]$, $m_i \in M$.

Семейство $\{a_\alpha\}$, $a_\alpha \in I$, называют *базисом* идеала I, если любой элемент $a \in I$ можно представить в виде $a = \lambda_1 a_{\alpha_1} + \ldots + \lambda_t a_{\alpha_t}$, где

$\lambda_i \in K[x_1, \ldots, x_n]$. Идеал I называют *конечно порожденным*, если он обладает конечным базисом.

Для доказательства теоремы 25.1 достаточно доказать, что идеал $I(M)$ конечно порожденный. В самом деле, в таком случае любой элемент множества $M \subset I(M)$ можно выразить через конечный набор элементов $a_1, \ldots, a_s \in I$, а каждый из этих элементов выражается через конечный набор элементов множества M.

Теорема 25.2 (теорема Гильберта о базисе). В кольце $K[x_1, \ldots, x_n]$ любой идеал конечно порожден.

Доказательство. Заметим сначала, что в рассматриваемом кольце K любой идеал конечно порожден. В самом деле, если K — поле, то в нем любой ненулевой идеал совпадает с K и порожден элементом 1. Если же $K = \mathbb{Z}$, то любой идеал имеет вид $m\mathbb{Z}$ и порождается элементом m. (Чтобы доказать это, можно рассмотреть наименьший элемент идеала.)

Пусть $L_n = K[x_1, \ldots, x_n]$ при $n \geqslant 1$, $L_0 = K$. Тогда $K[x_1, \ldots, x_{n+1}] = L_n[x]$, где $x = x_{n+1}$. Как мы уже отметили, при $n = 0$ в кольце L_n любой идеал конечно порожден. Поэтому достаточно доказать, что если в кольце $L = L_n$ любой идеал конечно порожден, то в кольце $L[x]$ любой идеал I тоже конечно порожден.

Шаг 1. Старшие коэффициенты многочленов из идеала $I \subset L[x]$ вместе с нулем образуют некоторый идеал J в кольце L.

В самом деле, пусть $f(x) = ax^n + \ldots$ и $g(x) = bx^m + \ldots$ — некоторые многочлены из идеала I. Можно считать, что $m \leqslant n$. В таком случае многочлен $f(x) + x^{n-m}g(x)$ лежит в идеале I, а его старший коэффициент равен $a+b$. Ясно также, что если $\lambda \in L$ и $\lambda \neq 0$, то старший коэффициент многочлена λf равен λa.

Построение конечного базиса идеала I в $L[x]$ начнем с того, что выберем конечный базис $a_1, \ldots, a_r$ идеала J в L. Элементы $a_1, \ldots, a_r$ являются старшими коэффициентами некоторых многочленов $f_1, \ldots, f_r \in I$.

Шаг 2. Существует такое натуральное число n, что любой многочлен из идеала I является суммой многочлена степени ниже n и многочлена вида $\lambda_1 f_1 + \ldots + \lambda_r f_r$, где $\lambda_i \in L[x]$.

Покажем, что в качестве n можно взять наибольшую из степеней многочленов $f_1, \ldots, f_r$. Возьмем в I произвольный многочлен $f(x) =$

$= ax^N + \ldots$ степени $N \geqslant n$. По определению $a \in J$, поэтому $a = \sum \lambda_i a_i$ для некоторых $\lambda_i \in L[x]$. Рассмотрим многочлен

$$g(x) = f(x) - \sum \lambda_i x^{N-\deg f_i} f_i.$$

У многочлена g коэффициент при x^N равен $a - \sum \lambda_i a_i = 0$, поэтому $\deg g \leqslant N-1$. Если $N-1 \geqslant n$, то эту конструкцию можно повторить и т. д.

Шаг 3. Существует такой конечный набор многочленов $g_1, \ldots, g_s \in I$, что любой многочлен степени ниже n из идеала I можно представить в виде $\lambda_1 g_1 + \ldots + \lambda_s g_s$, где $\lambda_i \in L[x]$.

Коэффициенты при x^{n-1} многочленов степени не выше $n-1$ из идеала I образуют некоторый идеал кольца L. Пусть $b_1, \ldots, b_k$ — базис этого идеала, $g_1, \ldots, g_k$ — многочлены степени $n-1$ из идеала I со старшими коэффициентами $b_1, \ldots, b_k$. Возьмем в идеале I произвольный многочлен h степени $n-1$. Пусть b — старший коэффициент этого многочлена. Тогда $b = \lambda_1 b_1 + \ldots + \lambda_k b_k$, где $\lambda_i \in L[x]$. Поэтому степень многочлена $h - \lambda_1 g_1 - \ldots - \lambda_k g_k$ не превосходит $n-2$. Таким образом, с точностью до элементов идеала, порожденного многочленами $g_1, \ldots, g_k$, нам удалось заменить многочлен степени $n-1$ многочленом степени не выше $n-2$. Аналогично можно выбрать многочлены $g_{k+1}, \ldots, g_l$ так, что с точностью до элемента идеала, порожденного ими, многочлен степени $n-2$ равен многочлену степени не выше $n-3$ и т. д. □

25.2. Теорема Гильберта о нулях

Теорема Гильберта о нулях появилась во второй знаменитой работе Гильберта по теории инвариантов [Hi4]. Эту теорему иногда называют также *теоремой Гильберта о корнях*; ее немецкое название Nullstellensatz общеупотребительно и в англоязычной математической литературе.

Теорема 25.3 (теорема Гильберта о нулях). Пусть

$$f, f_1, \ldots, f_r \in \mathbb{C}[x_1, \ldots, x_n],$$

причем многочлен f обращается в нуль во всех общих нулях многочленов $f_1, \ldots, f_r$. Тогда при некотором натуральном q многочлен f^q принадлежит идеалу, порожденному многочленами $f_1, \ldots, f_r$, т. е. $f^q = g_1 f_1 + \ldots + g_r f_r$ для некоторых $g_1, \ldots, g_r \in \mathbb{C}[x_1, \ldots, x_n]$.

Доказательство. Сначала мы докажем один частный случай теоремы Гильберта о нулях, из которого можно вывести и общую теорему. А именно, мы рассмотрим случай, когда $f = 1$.

Теорема 25.4. Пусть многочлены $f_1, \ldots, f_r \in \mathbb{C}[x_1, \ldots, x_n]$ таковы, что у них нет общих нулей. Тогда существуют такие многочлены $g_1, \ldots, g_r \in \mathbb{C}[x_1, \ldots, x_n]$, что

$$g_1 f_1 + \ldots + g_r f_r = 1.$$

Доказательство. Пусть $I(f_1, \ldots, f_r)$ — идеал кольца $\mathbb{C}[x_1, \ldots, x_n]$, порожденный многочленами $f_1, \ldots, f_r$. Предположим, что не существует таких многочленов $g_1, \ldots, g_r$, что $g_1 f_1 + \ldots + g_r f_r = 1$. Тогда $I(f_1, \ldots, f_r) \neq K$.

Шаг 1. Пусть I — нетривиальный максимальный идеал кольца K, содержащий $I(f_1, \ldots, f_r)$. Тогда кольцо $A = K/I$ является полем.

В самом деле, достаточно проверить, что в кольце K/I любой ненулевой элемент имеет обратный. Если $f \notin I$, то $I + fK$ — идеал, строго содержащий I, поэтому $I + fK = K$. Это, в частности, означает, что существуют такие многочлены $a \in I$ и $b \in K$, что $a + bf = 1$. В таком случае класс $\overline{b} \in K/I$ является обратным для класса $\overline{f} \in K/I$.

Пусть α_i — образ элемента x_i при канонической проекции

$$p : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_n]/I = A.$$

Тогда $A = \mathbb{C}[\alpha_1, \ldots, \alpha_n]$. Таким образом, A — конечно порожденная алгебра над $\mathbb{C}$, являющаяся в то же время полем.

Шаг 2. Если конечно порожденная алгебра $A = \mathbb{C}[\alpha_1, \ldots, \alpha_n]$ над полем $\mathbb{C}$ сама является полем, то A совпадает с $\mathbb{C}$.

Нам понадобится следующее вспомогательное утверждение.

Лемма (лемма Нётер о нормализации). В алгебре $A = \mathbb{C}[\alpha_1, \ldots, \alpha_n]$ можно выбрать алгебраически независимые над $\mathbb{C}$ элементы $y_1, \ldots, y_k$ так, что любой элемент $a \in A$ будет удовлетворять нормированному алгебраическому уравнению над $\mathbb{C}[y_1, \ldots, y_k]$, т. е.

$$a^l + b_1 a^{l-1} + \ldots + b_l = 0, \quad \text{где} \quad b_1, \ldots, b_l \in \mathbb{C}[y_1, \ldots, y_k].$$

Доказательство. Применим индукцию по n. Если элементы $\alpha_1, \ldots, \alpha_n$ алгебраически независимы, то утверждение очевидно. Пусть $f(\alpha_1, \ldots, \alpha_n) = 0$ — алгебраическое соотношение между ними. Если f — многочлен степени m, у которого коэффициент при x_n^m не равен нулю, то

$$\alpha_n^m + b_1\alpha_n^{m-1} + \ldots + b_m = 0, \quad b_1, \ldots, b_m \in \mathbb{C}[\alpha_1, \ldots, \alpha_{n-1}].$$

Остается воспользоваться предположением индукции.

Если же коэффициент при x_n^m равен нулю, сделаем замену $x_n = \xi_n$, $x_i = \xi_i + a_i\xi_n$, $i = 1, \ldots, n-1$. Попробуем подобрать числа $a_i \in \mathbb{C}$ так, чтобы у многочлена

$$g(\xi_1, \ldots, \xi_{n-1}, \xi_n) = f(x_1, \ldots, x_n) = f(\xi_1 + a_1\xi_n, \ldots, \xi_{n-1} + a_{n-1}\xi_n, \xi_n)$$

был ненулевой коэффициент при ξ_n^m. Этот коэффициент равен

$$g_m(0, \ldots, 0, 1) = f_m(a_1, \ldots, a_{n-1}, 1),$$

где f_m и g_m — однородные составляющие старшей степени многочленов f и g. Ясно, что ненулевой однородный многочлен $f_m(x_1, \ldots, x_n)$ не может быть тождественно равен нулю при $x_n = 1$. □

Теперь можно приступить непосредственно к доказательству того, что A совпадает с $\mathbb{C}$. Выберем элементы $y_1, \ldots, y_k \in A$, о которых идет речь в лемме Нётер о нормализации. Покажем, что в таком случае в алгебре $B = \mathbb{C}[y_1, \ldots, y_k]$ любой ненулевой элемент x обратим, т. е. B — поле. По условию A — поле, поэтому x обратим в A. Кроме того, согласно лемме Нётер элемент x^{-1} удовлетворяет уравнению

$$(x^{-1})^l + b_1(x^{-1})^{l-1} + \ldots + b_l = 0, \quad b_1, \ldots, b_l \in B.$$

Умножив обе части этого уравнения на x^{l-1}, получим

$$x^{-1} = -b_1 - b_2x - \ldots - b_lx^{l-1} \in B.$$

Поле $B = \mathbb{C}[y_1, \ldots, y_k]$ представляет собой кольцо многочленов от k переменных над полем $\mathbb{C}$. Но при $k \neq 0$ кольцо многочленов не может быть полем. Поэтому $B = \mathbb{C}$. А любой элемент поля A является корнем многочлена

$$(x^{-1})^l + b_1(x^{-1})^{l-1} + \ldots + b_l, \quad b_1, \ldots, b_l \in B = \mathbb{C}.$$

Следовательно, $A = \mathbb{C}$.

Шаг 3. Многочлены $f_1, \ldots, f_r$ обращаются в нуль в точке

$$(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n.$$

В самом деле, при канонической проекции

$$p\colon \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_n]/I = A = \mathbb{C}$$

элемент x_i переходит в $\alpha_i \in \mathbb{C}$, поэтому многочлен $\varphi(x_1, \ldots, x_n)$ переходит в $\varphi(\alpha_1, \ldots, \alpha_n)$. А так как многочлены $f_1, \ldots, f_r$ принадлежат идеалу I, при канонической проекции они переходят в нуль.

Итак, предположив, что $I(f_1, \ldots, f_r) \neq \mathbb{C}[x_1, \ldots, x_n]$, мы получили, что у многочленов $f_1, \ldots, f_r$ есть общий нуль. А это противоречит условию теоремы. □

Покажем теперь, следуя [R], как из теоремы 25.4 можно получить общую теорему Гильберта о нулях. Для $f = 0$ утверждение очевидно, поэтому будем считать, что $f \neq 0$. Добавим к переменным $x_1, \ldots, x_n$ новую переменную $x_{n+1} = z$ и рассмотрим многочлены $f_1, \ldots, f_r, 1 - zf$. У них нет общих нулей, поэтому

$$1 = h_1 f_1 + \ldots + h_r f_r + h(1 - zf),$$

где $h_1, \ldots, h_r, h$ — некоторые многочлены от переменных $x_1, \ldots, x_n, z$. Положим $z = 1/f$. После приведения к общему знаменателю получим

$$f^q = g_1 f_1 + \ldots + g_r f_r,$$

где $g_1, \ldots, g_r$ — многочлены от $x_1, \ldots, x_n$. Это соотношение имеет требуемый вид. □

Замечание. Если коэффициенты многочленов $f, f_1, \ldots, f_r$ вещественные и при этом f обращается в нуль во всех общих комплексных корнях многочленов $f_1, \ldots, f_r$, то существуют такие многочлены $g_1, \ldots, g_r$ с вещественными коэффициентами, что $f^q = g_1 f_1 + \ldots + g_r f_r$. В самом деле, согласно теореме Гильберта о нулях равенство $f^q = h_1 f_1 + \ldots + h_r f_r$ выполняется для некоторых многочленов $h_1, \ldots, h_r$ с комплексными коэффициентами. Пусть $h_j = g_j + ip_j$, где g_j и p_j — многочлены с вещественными коэффициентами. Тогда $f^q = g_1 f_1 + \ldots + g_r f_r$.

Любой набор однородных многочленов имеет общий тривиальный нуль — начало координат. Поэтому в однородном случае аналогом на-

бора многочленов, не имеющих общих нулей, служит набор многочленов, не имеющих общих нетривиальных нулей. Для однородных многочленов имеется следующий аналог теоремы 25.4.

Теорема 25.5. Пусть $F_1, \ldots, F_r \in \mathbb{C}[x_1, \ldots, x_n]$ — такие однородные многочлены, что у них нет общих нетривиальных нулей. Тогда порожденный ими идеал $I(F_1, \ldots, F_r)$ содержит все однородные многочлены степени $d \geqslant d_0$, где d_0 — некоторое фиксированное число.

Доказательство. По условию единственным общим нулем многочленов $F_1, \ldots, F_r$ является начало координат. Поэтому линейные многочлены $x_1, \ldots, x_n$ обращаются в нуль во всех общих нулях многочленов $F_1, \ldots, F_r$. Согласно теореме Гильберта о нулях $x_i^{p_i} \in I(F_1, \ldots, F_r)$ для некоторого p_i. Положим $d_0 = (p_1 - 1) + \ldots + (p_n - 1) + 1$. Тогда любой моном $X_d = x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ степени $d = a_1 + \ldots + a_n \geqslant d_0$ делится на $x_i^{p_i}$ при некотором i. Поэтому $X_d \in I(F_1, \ldots, F_r)$. □

Простое прямое доказательство теоремы 25.5 приведено в статье Картье и Тейта [CT].

25.3. Многочлен Гильберта

Напомним сначала некоторые определения из области коммутативной алгебры. *Модулем* над кольцом A называют абелеву группу M, на которой линейно действуют элементы кольца A, т. е. для любых $a \in A$ и $m \in M$ определен элемент $am \in M$ и при этом

$$a(m+n) = am + an, \qquad (ab)m = a(bm),$$
$$(a+b)m = am + bm, \qquad 1m = m.$$

Например, если A — поле, то модуль над A — это векторное пространство над A.

Модуль M над кольцом A называют *конечно порожденным*, если любой элемент $m \in M$ можно представить в виде $m = \sum a_i m_i$, где $m_1, \ldots, m_n$ — фиксированный конечный набор элементов M.

Градуированным кольцом называют кольцо $A = \bigoplus_{i=0}^{\infty} A_i$, где A_i — аддитивные подгруппы A, удовлетворяющие условию $A_i A_j \subset A_{i+j}$. *Градуированным модулем* над градуированным кольцом A называют мо-

дуль $M = \bigoplus_{i=0}^{\infty} M_i$, где M_i — аддитивные подгруппы M, удовлетворяющие условию $A_i M_j \subset M_{i+j}$.

В этом параграфе основным примером градуированного кольца будет кольцо $A = K[x_0, \ldots, x_n]$, где K — поле; при этом A_i состоит из однородных многочленов степени i.

Идеал $I \subset K[x_0, \ldots, x_n]$, называют *однородным*, если все однородные составляющие любого элемента идеала I тоже лежат в I (однородной составляющей степени i многочлена $f \in K[x_0, \ldots, x_n]$ называют сумму всех его членов степени i). Легко проверить, что идеал I однороден тогда и только тогда, когда он порожден однородными многочленами $f_1, \ldots, f_k$. В самом деле, если идеал I однороден, то однородные составляющие многочленов, порождающих I, лежат в I и порождают I. Если же идеал I порожден однородными многочленами $f_1, \ldots, f_k$, то элемент $g \in I$ можно сначала записать в виде $g = \sum h_\alpha f_\alpha$, а затем разложить каждый многочлен h_α на однородные составляющие. В результате каждая однородная составляющая g_i многочлена g будет представлена в виде $g_i = \sum x_\beta f_\beta$, поэтому $g_i \in I$.

Идеал I однороден тогда и только тогда, когда его можно представить в виде $I = \bigoplus_{i=0}^{\infty} I_i$, где $I_i = I \cap A_i$. Поэтому факторкольцо $M = A/I$ является градуированным модулем над A с градуировкой $M_i = A_i/(I \cap A_i)$. Поясним это подробнее. Пусть $g, h \in A = K[x_0, \ldots, x_n]$ — некоторые многочлены, g_i и h_i — их однородные составляющие степени i. Классы $g + I$ и $h + I$ совпадают тогда и только тогда, когда при всех i совпадают классы $g_i + I \cap A_i$ и $h_i + I \cap A_i$. Поэтому

$$M = A/I = \bigoplus_{i=0}^{\infty} A_i/(I \cap A_i) = \bigoplus_{i=0}^{\infty} M_i.$$

Действие A на M устроено следующим образом: для $g \in A$ и $f + I \in M$ элемент $g(f + I) \in M$ определяется как $gf + I \in M$. Ясно, что при этом

$$A_i\big(A_j/(I \cap A_j)\big) \subset A_{i+j}/(I \cap A_{i+j}).$$

Теорема 25.6 (Гильберт). Пусть K — поле, $A = K[x_0, \ldots, x_n]$ и $M = \bigoplus_{i=0}^{\infty} M_i$ — конечно порожденный градуированный модуль над A. Тогда существует такой многочлен $p_M(t)$ степени не выше n, что при всех достаточно больших i размерность M_i как векторного пространства над полем K равна $p_M(i)$.

Доказательство. Применим индукцию по n. База индукции: $n = -1$, т. е. $A = K$. В этом случае M — конечномерное векторное пространство над полем K, поэтому $M_i = 0$ при достаточно больших i. Таким образом, $p_M = 0$.

Предположим теперь, что $n \geqslant 0$ и утверждение верно для модулей над кольцом $A' = K[x_0, \ldots, x_{n-1}]$ ($A' = K$ при $n = 0$). Положим $x = x_n$ и рассмотрим A-модули $M' = \{m \in M \mid xm = 0\}$ и $M'' = M/xM$. Эти модули конечно порождены над A, причем они аннулируются умножением на x, т. е. $xM' = 0$ и $xM'' = 0$. Следовательно, M' и M'' — конечно порожденные A'-модули. Поэтому по предположению индукции при достаточно больших i выполняются равенства $\dim M'_i = p_1(i)$ и $\dim M''_i = p_2(i)$, где p_1 и p_2 — многочлены степени не выше $n-1$.

Для любого натурального i имеется точная последовательность

$$0 \to M'_i \to M_i \xrightarrow{\times x} M_{i+1} \to M''_i \to 0,$$

где отображение $M_i \xrightarrow{\times x} M_{i+1}$ — умножение на x. Поэтому

$$\dim M'_i - \dim M_i + \dim M_{i+1} - \dim M''_{i+1} = 0,$$

т. е.

$$\dim M_{i+1} - \dim M_i = \dim M''_{i+1} - \dim M'_i.$$

При достаточно больших i выполняется равенство

$$\dim M''_{i+1} - \dim M'_i = p_2(i+1) - p_1(i) = q(i),$$

где $q(i)$ — многочлен степени не выше $n-1$.

Пусть $f(i) = \dim M_i$. При достаточно больших i выполняется равенство $f(i+1) - f(i) = q(i)$, где q — многочлен степени не выше $n-1$. В таком случае f — многочлен степени не выше n (при достаточно больших i).

Положим $x^{(m)} = x(x-1) \cdot \ldots \cdot (x-m+1)$. Легко проверить, что $(x+1)^{(m)} - x^{(m)} = mx^{(m-1)}$. Многочлены $x^{(0)} = 1, x^{(1)}, \ldots, x^{(n-1)}$ образуют базис пространства многочленов степени не выше $n-1$, поэтому многочлен q можно представить в виде $q(x) = \sum\limits_{s=0}^{n-1} a_s x^{(s)}$. В таком случае многочлен $f_0(x) = \sum\limits_{s=0}^{n-1} \dfrac{a_s}{s+1} x^{(s+1)}$ удовлетворяет соотношению $f_0(i+1) - f_0(i) = q(i)$. Ясно также, что функция $c(i) = f(i) - f_0(i)$ при достаточно

больших i удовлетворяет соотношению $c(i+1)-c(i)=0$, поэтому $c(i)=$ $=c$ — константа. Таким образом, $f(x)=\sum\limits_{s=0}^{n-1}\dfrac{a_s}{s+1}x^{(s+1)}+c$ — многочлен степени не выше n. □

Многочлен $p_M(i)$ называют *многочленом Гильберта* модуля M. Ясно, что этот многочлен целозначный (см. с. 100), поэтому его можно представить в виде

$$p_M(i)=c_0\binom{i}{m}+c_1\binom{i}{m-1}+\ldots+c_m,$$

где $c_0,\ldots,c_m$ — целые числа и $m\leqslant n$. Мы предполагаем, что $c_0\neq 0$. В случае, когда $M=\mathbb{C}[x_0,\ldots,x_n]/I$, где I — однородный идеал, при некоторых естественных ограничениях числа c_0 и m допускают следующую геометрическую интерпретацию.

Однородному идеалу I соответствует алгебраическое множество $V(I)$ в проективном пространстве $\mathbb{C}P^n$, а именно,

$$V(I)=\{(a_0,\ldots,a_n)\in\mathbb{C}P^n\mid f(a_0,\ldots,a_n)=0\ \ \forall f\in I\}.$$

Идеал I называют *простым,* если $fg\in I\Rightarrow f\in I$ или $g\in I$. Для простого идеала I алгебраическое множество $V(I)$ неприводимо, т. е. его нельзя нетривиальным образом представить в виде объединения $V(I_1)$ и $V(I_2)$, где I_1 и I_2 — однородные идеалы. Ограничение, о котором шла выше речь, заключается в том, что идеал I должен быть простым. Тогда число m совпадает с размерностью проективного алгебраического многообразия $V(I)$, а число c_0 совпадает со степенью этого многообразия (степень многообразия размерности m в $\mathbb{C}P^n$ определяется как количество точек пересечения этого многообразия с подпространством размерности $n-m$ в общем положении, т. е. с почти всеми такими подпространствами). Доказательство этого утверждения можно найти в [Мм].

Пример 1. Если $M=\mathbb{C}[x_0,\ldots,x_n]$, то $m=n$ и $c_0=1$.

В самом деле, M_i состоит из однородных многочленов степени i от $n+1$ переменных. Моному $x_0^{i_0}\ldots x_n^{i_n}$ сопоставим последовательность, в которой сначала идут i_0 нулей и одна единица, затем идут i_1 нулей и одна единица, ..., а в конце стоят i_n нулей. Эта последовательность

состоит из $i+n$ чисел, среди которых i нулей и n единиц. Количество таких последовательностей равно

$$\binom{i+n}{n} = \frac{(i+n)\cdot\ldots\cdot(i+1)}{n!} = \frac{i^n}{n!} + \ldots = \binom{i}{n} + \ldots$$

Поэтому $p_M(i) = \dim M_i = \binom{i}{n} + \ldots$

Пример 2. Если $M = A/f_dA$, где $A = \mathbb{C}[x_0, \ldots, x_n]$, а f_d — однородный многочлен степени d, то $m = n-1$ и $c_0 = d$.

В самом деле, умножение на f_d дает точную последовательность

$$0 \to H_{i-d} \xrightarrow{\times f_d} H_i \to M_i \to 0,$$

где H_i — пространство однородных многочленов степени i от $n+1$ переменных. В примере 1 показано, что $\dim H_i = \binom{i+n}{n}$, поэтому

$$\begin{aligned}\dim M_i = \dim H_i - \dim H_{i-d} = \binom{i+n}{n} - \binom{i-d+n}{n} = \\ = d\frac{i^{n-1}}{(n-1)!} + \ldots = c_0\binom{i}{m} + \ldots,\end{aligned}$$

где $c_0 = d$ и $m = n-1$.

Пусть M — градуированный конечно порожденный A-модуль, $p_M(i) = c_0\binom{i}{m} + \ldots$ — многочлен Гильберта модуля M. В таком случае число $m = \dim M$ будем называть *размерностью* модуля M, а число $c_0 = \deg M$ — его *степенью*. Как мы уже упоминали (и примеры 1 и 2 это подтверждают), в случае, когда $I \subset \mathbb{C}[x_0, \ldots, x_n]$ — однородный простой идеал и $M = \mathbb{C}[x_0, \ldots, x_n]/I$, число $\dim M$ — это размерность многообразия $V(I) \subset \mathbb{C}P^n$, а число $\deg M$ — степень этого многообразия.

Обсудим теперь некоторые свойства степени и размерности градуированного A-модуля M, которые нам потребуются в разделе 25.4. Особый интерес представляет случай, когда $M = A/I$, где I — однородный простой идеал. В этом случае M является кольцом без делителей нуля, т. е. M — область целостности. С другой стороны, однородный идеал I прост тогда и только тогда, когда A-модуль $M = A/I$ обладает следующим свойством: если $f \notin I$, то $fm \neq 0$ при $m \neq 0$ (здесь $f \in A$ и $m \in M$). В общем случае A-модуль M будем называть *целостным*, если для любого $f \in A$ либо $fM = 0$, либо $fm \neq 0$ при $m \neq 0$.

До конца этого параграфа будем считать, что $A = K[x_0, \ldots, x_n]$, где K — некоторое поле, причем кольцо A снабжено естественной градуировкой $A = \bigoplus_{i=0}^{\infty} A_i$, где A_i — множество однородных многочленов степени i; M — градуированный конечно порожденный A-модуль, причем $\dim M \geqslant 0$, т. е. $p_M \neq 0$.

Теорема 25.7. Пусть модуль M целостный и $f \in A_d$ — такой однородный многочлен степени d, что $fM \neq 0$. Тогда

$$\dim(M/fM) = \dim M - 1 \quad \text{и} \quad \deg(M/fM) = d \deg M.$$

На языке геометрии это утверждение выглядит так: гиперповерхность степени d высекает на проективном алгебраическом многообразии размерности m и степени r подмногообразие размерности $m-1$ и степени dr.

Доказательство. Пусть $M' = \{m \in M \mid fm = 0\}$. Умножение на f дает точную последовательность

$$0 \to M'_{i-d} \to M_{i-d} \xrightarrow{\times f} M_i \to (M/fM)_i \to 0.$$

Из условия теоремы следует, что $M' = 0$. Поэтому при достаточно больших i выполняется равенство

$$p_{M/fM}(i) = p_M(i) - p_M(i-d).$$

Пусть $\dim M = m$ и $\deg M = r$. Тогда

$$p_M(i) - p_M(i-d) = r\binom{i}{m} - r\binom{i-d}{m} + \ldots = \frac{r}{m!}\left(i^m - (i-d)^m\right) + \ldots =$$

$$= \frac{rmd}{m!} i^{m-1} + \ldots = \frac{rd}{(m-1)!} i^{m-1} + \ldots,$$

т. е. $p_{M/fM}(i) = dr\binom{i}{m-1} + \ldots$, что и требовалось. □

Подмодуль $S \subset M$ называют *однородным*, если он порожден однородными элементами (т. е. элементами однородных слагаемых M_i). Эквивалентное условие: $S = \bigoplus_{i=0}^{\infty} S_i$, где $S_i = S \cap M_i$. При этом фактормодуль M/S имеет естественную градуировку: $M/S = \bigoplus_{i=0}^{\infty} (M_i/S_i)$.

Теорема 25.8. Пусть p — простое число, не делящее $\deg M$. Тогда в M есть такой однородный подмодуль S, что фактормодуль $N = M/S$ удовлетворяет следующим условиям:

(а) $\dim N = \dim M$;

(б) $\deg N$ не делится на p;

(в) модуль N целостный.

На геометрическом языке это соответствует выделению неприводимой компоненты максимальной размерности в случае произвольного алгебраического множества, состоящего из нескольких компонент.

Доказательство. Свойства (а) и (б) выполняются для $S = 0$. Кроме того, модуль M конечно порожден над $A = K[x_0, \ldots, x_n]$, поэтому любая возрастающая последовательность подмодулей M стабилизируется. Следовательно, существует максимальный однородный подмодуль S, для которого выполняются свойства (а) и (б). Покажем, что для максимального подмодуля S выполняется и свойство (в), т. е. модуль $N = M/S$ целостный.

Требуется доказать, что если $f \in A$, то либо $fn = 0$ при всех $n \in N$, либо $fn \neq 0$ при всех $n \neq 0$. Это утверждение достаточно доказать в случае, когда f — однородный многочлен. В самом деле, для произвольного многочлена требуемое утверждение тогда можно будет получить следующим образом. Разложим f и n на однородные составляющие: $f = f_s + f_{s+1} + \ldots$ и $n = n_t + n_{t+1} + \ldots$, где $f_s \neq 0$ и $n_t \neq 0$. Предположим,что $fn = 0$, т. е. $f_s n_t = 0$, $f_{s+1} n_t + f_s n_{t+1} = 0$, $f_{s+2} n_t + f_{s+1} n_{t+1} + f_s n_{t+2} = 0, \ldots$ Из условия $n_t \neq 0$ последовательно получаем $f_s N = 0$, $f_{s+1} N = 0$, $f_{s+2} N = 0, \ldots$ Следовательно, $fN = 0$.

Итак, пусть f — однородный многочлен степени d и $fN \neq 0$. Положим $N' = \{n \in N \mid fn = 0\}$. Умножение на f дает точную последовательность

$$0 \to N'_{i-d} \to N_{i-d} \xrightarrow{\times f} N_i \to (N/fN)_i \to 0,$$

т. е.

$$0 \to N_{i-d}/N'_{i-d} \to N_i \to (N/fN)_i \to 0.$$

Поэтому при больших i выполняется равенство

$$p_N(i) = p_{N/fN}(i) + p_{N/N'}(i - d). \tag{1}$$

Условие $fN \neq 0$ означает, что $fM + S \neq S$. Из максимальности S следует, что модуль

$$N/fN = (M/S)/f(M/S) \cong M/(S + fM)$$

не может одновременно обладать свойствами (а) и (б). Поэтому либо $\dim(N/fN) < \dim N = \dim M$, либо $\dim(N/fN) = \dim M$, но $\deg(N/fN)$ делится на p.

Согласно формуле (1) в первом случае

$$p_{N/N'}(i-d) = \frac{ri^n}{n!} + \ldots,$$

где $n = \dim N$, $r = \deg N$. Во втором случае

$$p_{N/N'}(i-d) = \frac{(r-r_1)i^n}{n!} + \ldots,$$

где $r_1 = \deg(N/fN)$. Так как r не делится на p, а r_1 делится на p, то в обоих случаях $\dim(N/N') = n = \dim M$ и число $\deg(N/N')$, равное r или $r - r_1$, не делится на p. Таким образом, для модуля N/N' выполняются свойства (а) и (б). При этом модуль N/N' имеет вид M/S', где S' — однородный подмодуль M, содержащий S. Из максимальности S следует, что $S' = S$, т. е. $N' = 0$, что и требовалось. □

Теорема 25.9. Пусть $I \subset A = K[x_0, \ldots, x_n]$ — однородный простой идеал, причем размерность целостного A-модуля $M = A/I$ равна нулю, а его степень равна $r \neq 0$, т. е. $p_M(i) = r \neq 0$. Тогда

а) $xM \neq 0$ для некоторого $x = x_j$;

б) $L = M/(x-1)M$ — поле, являющееся расширением степени r поля K.

Доказательство. а) Если $x_j M = 0$ при $j = 0, \ldots, n$, то $x_j \in I$ при всех j, а значит, $M = K$. Таким образом, $p_M(i) = 0$, что противоречит условию $p_M(i) = r \neq 0$.

б) Фиксируем $x = x_j$ так, что $xM \neq 0$. Тогда $xm \neq 0$ при $m \neq 0$, так как модуль M целостный. Это означает, что отображение $M \xrightarrow{\times x} M$ мономорфно. При достаточно больших i выполняется равенство $\dim M_i = p_M(i) = r$, поэтому $\dim M_{i+1} = \dim M_i$. Следовательно, при достаточно больших i отображение $M_i \xrightarrow{\times x} M_{i+1}$ взаимно однозначно.

Рассмотрим в M неоднородный подмодуль $(x-1)M$. Пусть $\pi\colon M \to M/(x-1)M = L$ — естественная проекция. Тогда $\pi(xm) = \pi(m)$. Ясно также, что $x\pi(m) = \pi(xm)$. Поэтому $L \overset{\times x}{\to} L$ — тождественное отображение.

Пусть для определенности отображение $M_i \overset{\times x}{\to} M_{i+1}$ взаимно однозначно при $i \geqslant a$. Покажем, что тогда $L = \pi(M_a) = \pi(M_{a+1}) = \ldots$ Запишем элемент $m \in M$ в виде $m = m_0 + \ldots + m_a + m_{a+1} + \ldots + m_k$, где $m_s \in M_s$. Ясно, что

$$\pi(m_0 + \ldots + m_a) = \pi(x^a m_0 + x^{a-1} m_1 + \ldots + m_a) = \pi(m'),$$

где $m' = x^a m_0 + x^{a-1} m_1 + \ldots + m_a \in M_a$. Кроме того, $m_{a+1} = x m_{a,1}$, $m_{a+2} = x^2 m_{a,2}$, $\ldots$, $m_k = x^{k-a} m_{a,k-a}$, где $m_{a,s} \in M_a$. Поэтому

$$\pi(m_{a+1} + \ldots + m_k) = \pi(m_{a,1} + \ldots + m_{a,k-a}) = \pi(m''),$$

где $m'' = m_{a,1} + \ldots + m_{a,k-a} \in M_a$.

Итак, естественная проекция $M_a \to L$ эпиморфна. С другой стороны, эта проекция по очевидным причинам мономорфна: если $\pi(m_a) = 0$, то $m_a = (x-1)m$, но однородный элемент $m_a \neq 0$ нельзя представить в виде $(x-1)m$. Поэтому проекция $M_a \to L$ взаимно однозначна и $\dim L = \dim M_a = r$.

В рассматриваемой ситуации L является r-мерной алгеброй над полем K (т. е. коммутативным кольцом и одновременно линейным пространством над K). Покажем, что в алгебре L нет делителей нуля. Пусть $l', l'' \in L$ и $l'l'' = 0$. Выше было показано, что $l' = \pi(m')$ и $l'' = \pi(m'')$ где $m', m'' \in M_a$. Поэтому $0 = l'l'' = \pi(m'm'')$, где $m'm'' \in M_{2a}$. При $b \geqslant a$ проекция $M_b \to L$ — изоморфизм, а значит, $m'm'' = 0$. По условию идеал I простой, поэтому в кольце $M = A/I$ нет делителей нуля. Следовательно, $m' = 0$ или $m'' = 0$, т. е. $l' = 0$ или $l'' = 0$.

Теперь уже легко показать, что L — поле, т. е. любой ненулевой элемент $l \in L$ обратим. В самом деле, отображение $x \mapsto lx$, $x \in L$, представляет собой линейное отображение $L \to L$ с нулевым ядром. В конечномерном случае такое отображение — изоморфизм, поэтому, в частности, $lx = 1$ для некоторого $x \in L$. □

25.4. Однородная теорема Гильберта о нулях для p-полей

Следующее утверждение было впервые доказано в статье Гильберта [Hi4], хотя и его использовали многие математики XIX в. без строгого обоснования.

Теорема 25.10. Пусть K — алгебраически замкнутое поле, $A = K[x_0, \ldots, x_n]$, где $n \geqslant 1$. Тогда любые однородные многочлены $f_1, \ldots, f_n \in A$ имеют общий нуль, отличный от начала координат.

Аналогичное утверждение можно доказать и для так называемых p-полей, к которым относится, в частности, поле действительных чисел $\mathbb{R}$.

Пусть p — простое число. Поле K называют *p-полем*, если степень любого его конечного расширения имеет вид p^s. В частности, любое алгебраически замкнутое поле является p-полем для всех простых p, а поле $\mathbb{R}$ является 2-полем.

Теорема 25.11. Пусть K — некоторое p-поле, $A = K[x_0, \ldots, x_n]$, где $n \geqslant 1$. Тогда любые однородные многочлены $f_1, \ldots, f_n \in A$, степени которых не делятся на p, имеют общий нетривиальный нуль.

Доказательство (Г. Фендрих; см. [Pf2], ch. 4). Мы будем пользоваться результатами предыдущего параграфа, а именно, теоремами 25.7–25.9.

Начнем с того, что построим последовательность целостных конечно порожденных градуированных A-модулей $M_0 = A$, $M_1 = A/I_1, \ldots, M_n = A/I_n$, для которых $\dim M_i = n - i$, $\deg M_i$ не делится на p и однородный простой идеал I_i содержит многочлены $f_0, \ldots, f_i$. Модуль $M_0 = A$ удовлетворяет этим условиям, так как $\dim M_0 = n$ и $\deg M_0 = 1$ (см. пример 1 на с. 255).

Предположим, что модули $M_0, \ldots, M_i$ ($i \geqslant 0$) уже построены. Покажем, как по модулю $M_i = A/I_i$ и многочлену f_{i+1} можно построить модуль M_{i+1}. При этом возможны два случая.

Случай 1: $f_{i+1} \notin I_i$, т. е. $f_{i+1} M_i \neq 0$. Положим

$$N_{i+1} = M_i / f_{i+1} M_i \cong A/(I_i + f_{i+1} A).$$

Согласно теореме 25.7 $\dim N_{i+1} = \dim M_i - 1 = n - (i+1)$ и $\deg N_{i+1} = \deg f_{i+1} \deg M_i$. Число $\deg N_{i+1}$ не делится на p, так как оба числа $\deg f_{i+1}$ и $\deg M_i$ на p не делятся.

Случай 2: $f_{i+1} \in I_i$. Из условия $\dim M_i \geqslant 0$ следует, что $x \notin I_i$ (т. е. $x M_i \neq 0$) для некоторого $x = x_j$. В самом деле, если $x_0, \ldots, x_n \in I_i$, то $M_i = K$ или 0, поэтому $p_{M_i} = 0$.

Положим $N_{i+1} = M_i / x M_i$. Согласно теореме 25.7 $\dim N_{i+1} = \dim M_i - 1 = n - (i+1)$ и $\deg N_{i+1} = \deg M_i$, так как степень многочлена x равна 1.

В обоих случаях мы получили некоторый модуль N_{i+1}, но он не обязательно целостный. Чтобы получить целостный модуль, воспользуемся теоремой 25.8. Согласно этой теореме в N_{i+1} есть такой однородный подмодуль S_{i+1}, что фактормодуль

$$M_{i+1} = N_{i+1}/S_{i+1} = A/I_{i+1}$$

обладает всеми требуемыми свойствами: $\dim M_{i+1} = \dim N_{i+1} = n - (i+1)$, $\deg M_{i+1}$ не делится на p и модуль M_{i+1} целостный; при этом I_{i+1} — однородный идеал, содержащий многочлены $f_1, \ldots, f_{i+1}$.

Размерность последнего из построенных модулей M_n равна нулю, поэтому к нему можно применить теорему 25.9. В результате получим поле $L = M_n/(x_j - 1)M_n \cong A/I$. Здесь I — неоднородный простой идеал, обладающий двумя важными для наших целей свойствами: (1) $x_j \equiv 1 \pmod{I}$; (2) $I \supset I_n \ni f_1, \ldots, f_n$.

Поле L является расширением степени $\deg M_n$ поля K. Но, с одной стороны, $\deg M_n$ не делится на p, а с другой стороны, степень любого расширения поля K имеет вид p^s. Поэтому $L = K$.

Пусть $a_i \in K$ — образ элемента x_i при естественной проекции

$$A = k[x_0, \ldots, x_n] \to A/I = L = K.$$

Из свойства (1) следует, что $a_j = 1$, поэтому $a = (a_0, \ldots, a_n) \neq 0$. А из свойства (2) следует, что $f_1(a) = \ldots = f_n(a) = 0$. □

Теорема 25.11 позволяет чисто алгебраически доказать в полиномиальном случае известную теорему Борсука–Улама об общем нуле нечетных функций на сфере.

Теорема 25.12. Пусть $q_1, \ldots, q_n \in \mathbb{R}[x_1, \ldots, x_{n+1}]$ нечетные многочлены, т. е. $q_i(-x) = -q_i(x)$. Тогда эти многочлены имеют общий нуль на единичной сфере $x_1^2 + \ldots + x_{n+1}^2 = 1$.

Доказательство. Перейдем от q_i к однородному многочлену $\widetilde{q}_i$, введя дополнительную переменную x_0. При этом в многочлене q_i моном $x_1^{a_1} \cdot \ldots \cdot x_n^{a_n}$ заменяется на $x_0^{m_0} x_1^{m_1} \cdot \ldots \cdot x_n^{m_n}$, где $m_0 = \deg q_i - m_1 - \ldots - m_n$. У нечетного многочлена степени всех членов нечетны, поэтому числа $\deg q_i$ и $m_1 + \ldots + m_n$ нечетны, а значит, число m_0 четно. Заменив x_0^2 на $x_1^2 + \ldots + x_{n+1}^2$, из многочлена $\widetilde{q}_i$ получим однородный многочлен f_i

нечетной степени. Согласно теореме 25.11 многочлены $f_1, \ldots, f_n$ имеют общий нуль $a = (a_1, \ldots, a_{n+1}) \neq 0$. При всех $t \in \mathbb{R}$ точка ta тоже будет нулем однородных многочленов $f_1, \ldots, f_n$, поэтому можно считать, что $a_1^2 + \ldots + a_{n+1}^2 = 1$. В таком случае $q_i(a) = \widetilde{q}_i(1, a) = f_i(a) = 0$, что и требовалось. □

Из теоремы 25.12 можно получить и обычную теорему Борсука–Улама для нечетных непрерывных функций $g_1, \ldots, g_n$, приближая эти функции многочленами.

26. Базисы Грёбнера

Для решения различных вычислительных задач, связанных с идеалами в кольцах многочленов, весьма удобны базисы Грёбнера. Это понятие было введено Бруно Бухбергером в его диссертации [Bu1], написанной под руководством Вольфганга Грёбнера; см. также [Bu2]. Бухбергер предложил также удобный алгоритм вычисления базиса Грёбнера, что и превратило базисы Грёбнера в эффективный вычислительный аппарат.

Наше изложение теории базисов Грёбнера во многом опирается на первую главу книги [AdL]. Более подробно познакомиться с различными аспектами теории базисов Грёбнера можно по книге [Bu3].

26.1. Многочлены от одной переменной

В случае многочленов от одной переменной над полем K алгоритм нахождения базиса идеала основан на делении с остатком одного многочлена на другой. Первый шаг деления с остатком делается следующим образом. Пусть $f(x) = a_n x^n + \ldots + a_0$, $g(x) = b_m x^m + \ldots + b_0$, причем $n \geqslant m$. Положим $f_1(x) = f(x) - \dfrac{a_n x^n}{b_m x^m} g(x)$. Если $\deg f_1 \geqslant \deg g$, то применим к f_1 аналогичную процедуру и т. д. В конце концов получим $f = qg + r$, где $\deg r < \deg g$ (или $r = 0$). При этом многочлены q и r определены однозначно.

Теорема 26.1. Любой идеал I в кольце $K[x]$ многочленов от одной переменной главный, т. е. порожден одним элементом.

Доказательство. Выберем в I многочлен g минимальной степени. Пусть $f \in I$. Тогда $f = qg + r$, где $\deg r < \deg g$. Но $r = f - qg \in I$, поэтому $r = 0$. Это означает, что идеал I порожден многочленом g. □

Пусть $I(f_1,\dots,f_n)$ — идеал, порожденный многочленами $f_1(x),\dots,f_n(x)$. Многочлен $g(x)$, порождающий этот идеал, называют *наибольшим общим делителем* (НОД) многочленов $f_1,\dots,f_n$ и обозначают $(f_1,\dots,f_n)$. Наибольший общий делитель обладает следующими свойствами:

(1) все многочлены $f_1,\dots,f_n$ делятся на g;

(2) если все многочлены $f_1,\dots,f_n$ делятся на некоторый многочлен h, то h делится на g.

Свойство (1) следует из того, что $f_1,\dots,f_n \in I(f_1,\dots,f_n) = I(g)$. Свойство (2) следует из того, что $g \in I(f_1,\dots,f_n)$, т. е. $g = u_1f_1 + \dots + u_nf_n$, где $u_1,\dots,u_n \in K[x]$.

Свойства (1) и (2) определяют многочлен g однозначно с точностью до пропорциональности. В самом деле, если многочлены g_1 и g_2 делятся друг на друга, то они пропорциональны.

Наибольший общий делитель (f_1,f_2) многочленов f_1 и f_2 можно найти с помощью следующего алгоритма, называемого *алгоритм Евклида*. Для определенности будем считать, что $\deg f_1 \geqslant \deg f_2$. Пусть r_1 — остаток от деления f_1 на f_2, r_2 — остаток от деления f_2 на r_1, $\dots$ $\dots$, r_{k+1} — остаток от деления r_{k-1} на r_k. Степени многочленов r_i строго убывают, поэтому для некоторого n получим $r_{n+1} = 0$, т. е. r_{n-1} делится на r_n. При этом f_1 и f_2 делятся на r_n, так как на r_n делятся многочлены $r_{n-1}, r_{n-2},\dots$ Кроме того, если f_1 и f_2 делятся на некоторый многочлен h, то r_n делится на h, так как на h делятся многочлены $r_1, r_2,\dots$ Таким образом, $r_n = (f_1,f_2)$.

Опираясь на свойства (1) и (2), легко проверить, что

$$(f_1,f_2,\dots,f_n) = \big(f_1,(f_2,\dots,f_n)\big).$$

Это замечание сводит вычисление НОД n многочленов к вычислению НОД двух многочленов.

26.2. Деление многочленов от многих переменных

Чтобы определить деление с остатком для многочленов от многих переменных, нужно фиксировать некоторый порядок на множестве мономов. В дальнейшем мы будем считать, что мономы упорядочены *лексикографически*, т. е. моном $x^\alpha = x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}$ старше монома $x^\beta = x_1^{\beta_1}\cdot\ldots\cdot x_n^{\beta_n}$, если $\alpha_1 = \beta_1,\dots,\alpha_k = \beta_k, \alpha_{k+1} > \beta_{k+1}$ (возможно $k = 0$).

Запись $f = a_\alpha x^\alpha + \ldots$ будет означать, что $a_\alpha x^\alpha$ — старший член многочлена f, т. е. x^α — старший моном, входящий в f.

Пусть $f = a_\alpha x^\alpha + \ldots$ и $g = b_\beta x^\beta + \ldots$ — два многочлена от n переменных. Если некоторый член $c_\gamma x^\gamma$ многочлена f делится на x^β, положим $f_1 = f - \dfrac{c_\gamma x^\gamma}{b_\beta x^\beta} g$. Если некоторый член многочлена f_1 делится на x^β, применим к f_1 аналогичное преобразование и т. д. Чтобы этот процесс сходился за конечное число шагов, можно поступить, например, следующим образом. В качестве $c_\gamma x^\gamma$ будем брать старший из всех членов многочленов f, делящихся на x^β. Тогда порядок старшего члена f, делящегося на x^β, будет строго убывать. А любая строго убывающая последовательность мономов от n переменных конечна. В самом деле, сначала за конечное число шагов пропадет x_1, затем за конечное число шагов пропадет x_2 и т. д.

Аналогично можно определить деление с остатком многочлена f на несколько многочленов $f_1, \ldots, f_s$. В результате получим представление $f = u_1 f_1 + \ldots + u_s f_s + r$, где у многочлена r нет членов, делящихся на старшие мономы многочленов $f_1, \ldots, f_s$. В таком случае будем говорить, что r — *остаток от деления* многочлена f на многочлены $f_1, \ldots, f_s$. Следует отметить, что многочлен r определен не однозначно. Одно из возможных определений базиса Грёбнера как раз и заключается в том, что $f_1, \ldots, f_s$ — базис Грёбнера, если остаток от деления любого многочлена f на $f_1, \ldots, f_s$ определен однозначно.

26.3. Определения базисов Грёбнера

Будем говорить, что (ненулевые) многочлены $g_1, \ldots, g_t \in I$ образуют *базис Грёбнера* идеала I, если у любого (ненулевого) многочлена $f \in I$ старший член делится на старший член одного из многочленов $g_1, \ldots, g_t$.

Теорема 26.2. Многочлены $g_1, \ldots, g_t$ образуют базис Грёбнера идеала I тогда и только тогда, когда выполняется одно из следующих эквивалентных условий:

(а) $f \in I \Leftrightarrow$ остаток от деления f на $g_1, \ldots, g_t$ равен 0;

(б) $f \in I \Leftrightarrow f = \sum h_i g_i$ и старший моном многочлена f равен старшему из произведений старших мономов h_i и g_i;

(в) идеал $L(I)$, порожденный старшими членами элементов идеала I, порожден старшими членами многочленов $g_1, \ldots, g_t$.

Доказательство. Покажем сначала, что если $g_1, \ldots, g_t$ — базис Грёбнера идеала I, то выполняется условие (а). Достаточно доказать, что если r — остаток от деления многочлена $f \in I$ на $g_1, \ldots, g_t$, то $r = 0$. Ясно, что $r = f - \sum h_i g_i \in I$. Поэтому если $r \neq 0$, то старший член r делится на старший член одного из многочленов $g_1, \ldots, g_t$, что противоречит определению многочлена r.

(а) $\Rightarrow$ (б) Согласно определению деления с остатком $f = \sum h_i g_i + r$, где старший моном f равен старшему из произведений старших мономов h_i и g_i. Из (а) следует, что если $f \in I$, то $r = 0$.

(б) $\Rightarrow$ (в) Если $f = ax^\alpha + \ldots \in I$, то $f = \sum h_i g_i$, где $h_i = b_i x^{\beta_i} + \ldots$ и $g_i = c_i x^{\gamma_i} + \ldots$, причем все мономы $x^{\beta_i} x^{\gamma_i}$ не старше x^α. Поэтому $ax^\alpha = \sum\limits_i b_i x^{\beta_i} c_i x^{\gamma_i}$, где суммирование ведется по тем i, для которых $x^{\beta_i} x^{\gamma_i} = x^\alpha$. А так как $c_i x^{\gamma_i} \in L(I)$, то $ax^\alpha \in L(I)$.

Остается доказать, что если выполняется условие (в), то $g_1, \ldots, g_t$ — базис Грёбнера. Пусть $f = ax^\alpha + \ldots \in I$. Тогда

$$ax^\alpha = \sum_i b_i x^{\beta_i} c_i x^{\gamma_i},$$

где $c_i x^{\gamma_i}$ — старшие члены некоторых из многочленов $g_1, \ldots, g_t$. Ясно, что моном x^α делится на моном x^{γ_i} при некотором i. □

Следствие. Если $g_1, \ldots, g_t$ — базис Грёбнера идеала I, то многочлены $g_1, \ldots, g_t$ порождают идеал I.

Это следует из условия (а).

Теорема 26.3. У любого ненулевого идеала $I \subset K[x_1, \ldots, x_n]$ есть базис Грёбнера.

Доказательство. Рассмотрим идеал $L(I)$, порожденный старшими мономами X_α всех многочленов $g_\alpha = a_\alpha X_\alpha + \ldots \in I$. Ясно, что $f \in L(I)$ тогда и только тогда, когда любой моном многочлена f делится на некоторый моном X_α. По теореме Гильберта о базисе идеал $L(I)$ порожден конечным числом многочленов $f_1, \ldots, f_k$. Каждый моном любого из этих многочленов делится на некоторый моном X_α. В результате получаем конечный набор мономов $X_1, \ldots, X_t$, порождающих идеал $L(I)$. Эти мономы являются старшими мономами многочленов $g_1, \ldots, g_t$. Согласно теореме 26.2 (в) многочлены $g_1, \ldots, g_t$ образуют базис Грёбнера идеала I. □

Будем говорить, что многочлены $g_1, \ldots, g_t$ образуют *базис Грёбнера*, если они образуют базис Грёбнера порожденного ими идеала.

Теорема 26.4. Ненулевые многочлены $g_1, \ldots, g_t$ образуют базис Грёбнера тогда и только тогда, когда остаток от деления любого многочлена f на $g_1, \ldots, g_t$ определен однозначно.

Доказательство. Предположим сначала, что многочлены $g_1, \ldots, g_t$ образуют базис Грёбнера. Пусть r_1 и r_2 — остатки от деления f на $g_1, \ldots, g_t$. Тогда многочлены $f - r_1$ и $f - r_2$ лежат в идеале I, порожденном $g_1, \ldots, g_t$. Поэтому $r_1 - r_2 = (f - r_2) - (f - r_1) \in I$. Согласно определению базиса Грёбнера старший моном многочлена $r_1 - r_2$ делится на старший моном одного из многочленов $g_1, \ldots, g_t$. С другой стороны, ни у многочлена r_1, ни у многочлена r_2 нет членов, делящихся на старшие мономы многочленов $g_1, \ldots, g_t$. Поэтому $r_1 - r_2 = 0$.

Предположим теперь, что остаток от деления любого многочлена f на $g_1, \ldots, g_t$ единствен. Требуется доказать, что если $f \in I$, то остаток r от деления f на $g_1, \ldots, g_t$ равен нулю.

Покажем сначала, что если a — некоторое число, то многочлены f и $f - ax^\alpha g_i$, где x^α — моном, дают одинаковые остатки при делении на $g_1, \ldots, g_t$. Напомним, что при делении с остатком элементарное преобразование заключается в уничтожении некоторого монома $c_\gamma x^\gamma$ многочлена f посредством замены f на $f - dx^\delta g_i$. Пусть $g_i = bx^\beta + \ldots$. Если у одного из многочленов f и $f - ax^\alpha g_i$ коэффициент при мономе $x^{\alpha+\beta}$ равен нулю, то многочлен с ненулевым коэффициентом при этом мономе элементарным преобразованием приводится к многочлену с нулевым коэффициентом. Если же у обоих многочленов f и $f - ax^\alpha g_i$ коэффициенты при мономе $x^{\alpha+\beta}$ отличны от нуля, то оба многочлена элементарным преобразованием приводятся к многочлену $f - cx^\alpha g_i$ с ненулевым коэффициентом при мономе $x^{\alpha+\beta}$. Во всех случаях многочлены f и $f - ax^\alpha g_i$ приводятся элементарным преобразованием к одному и тому же многочлену, поэтому при делении на многочлены $g_1, \ldots, g_t$ они дают одинаковые остатки. (Мы пользуемся предположением о единственности остатка.)

Теперь уже легко доказать требуемое. Если $f \in I$, то $f = \sum h_i g_i$. Записав каждый многочлен h_i в виде суммы мономов, получим $f = \sum a_\alpha x^\alpha g_{i_\alpha}$. Многочлены f и $f - \sum a_\alpha x^\alpha g_{i_\alpha} = 0$ дают одинаковые остатки при делении на $g_1, \ldots, g_t$. Но для нулевого многочлена остаток от деления равен нулю, поэтому для многочлена f остаток от деления тоже равен нулю. □

26.4. Алгоритм Бухбергера

Все предшествующие определения базиса Грёбнера не позволяли выяснить за конечное число шагов, будет ли набор $g_1, \ldots, g_t$ базисом Грёбнера. Приведем наконец определение, которое позволяет это выяснить.

Пусть $f = ax_\alpha + \ldots$, $g = bx_\beta + \ldots$ и x_γ — наименьшее общее кратное мономов x_α и x_β. Положим $S(f,g) = \frac{x_\gamma}{ax_\alpha} f - \frac{x_\gamma}{bx_\beta} g$; многочлен $S(f,g)$ строится так, чтобы старшие члены двух его составляющих сократились.

Теорема 26.5 (Бухбергер). Многочлены $g_1, \ldots, g_t$ образуют базис Грёбнера тогда и только тогда, когда при всех $i \neq j$ остаток от деления многочлена $S(g_i, g_j)$ на $g_1, \ldots, g_t$ равен нулю.

Доказательство. Если многочлены $g_1, \ldots, g_t$ образуют базис Грёбнера, то согласно теореме 26.2 (а) многочлен $S(g_i, g_j)$, принадлежащий порожденному ими идеалу I, при делении на них дает остаток 0. Поэтому нужно лишь доказать, что если при всех $i \neq j$ остаток от деления многочлена $S(g_i, g_j)$ на $g_1, \ldots, g_t$ равен нулю, то многочлены $g_1, \ldots, g_t$ образуют базис Грёбнера, т. е. любой многочлен $f \in I$ можно представить в виде $f = \sum h_i g_i$, где старший моном многочлена f равен старшему из произведений старших мономов h_i и g_i (см. теорему 26.2 (б)).

Предварительно докажем одно вспомогательное утверждение.

Лемма. Пусть $f_1, \ldots, f_s$ — многочлены с одним и тем же старшим мономом x^α. Тогда если старший моном многочлена $f = \sum \lambda_i f_i$, где λ_i — числа, строго меньше x^α, то $f = \sum\limits_{i<j} \mu_{ij} S(f_i, f_j)$.

Доказательство. По условию $f_i = a_i x^\alpha + \ldots$ и $f_j = a_j x^\alpha + \ldots$, поэтому $S(f_i, f_j) = \frac{f_i}{a_i} - \frac{f_j}{a_j}$. Ясно также, что

$$f = \sum \lambda_i f_i = \lambda_1 a_1 \left(\frac{f_1}{a_1} - \frac{f_2}{a_2} \right) + (\lambda_1 a_1 + \lambda_2 a_2) \left(\frac{f_2}{a_2} - \frac{f_3}{a_3} \right) + \ldots$$
$$\ldots + (\lambda_1 a_1 + \ldots + \lambda_{s-1} a_{s-1}) \left(\frac{f_{s-1}}{a_{s-1}} - \frac{f_s}{a_s} \right) + (\lambda_1 a_1 + \ldots + \lambda_s a_s) \frac{f_s}{a_s}.$$

Остается заметить, что $\lambda_1 a_1 + \ldots + \lambda_s a_s = 0$. В самом деле, у многочлена $f = \sum \lambda_i f_i$ коэффициент при мономе x^α как раз и равен $\lambda_1 a_1 + \ldots + \lambda_s a_s$, а по условию старший моном многочлена f строго меньше x^α. □

Многочлен $f = ax^\alpha + \ldots \in I$ разными способами можно представить в виде $f = \sum h_i g_i$. Пусть $h_i = b_i x^{\beta_i} + \ldots$ и $g_i = c_i x^{\gamma_i} + \ldots$ Старший из мономов $x^{\beta_i} x^{\gamma_i}$, $i = 1, \ldots, t$, обозначим x^δ. Выберем представление $f = \sum h_i g_i$ так, чтобы моном x^δ был минимален. Требуется доказать, что в таком случае $x^\delta = x^\alpha$. Ясно, что моном x^α не может быть старше монома x^δ. Предположим, что моном x^δ старше монома x^α. Можно считать, что $x^{\beta_i} x^{\gamma_i} = x^\delta$ при $i = 1, \ldots, M$, а при $i = M+1, \ldots, t$ моном x^δ старше монома $x^{\beta_i} x^{\gamma_i}$.

Рассмотрим многочлен $g = \sum\limits_{i=1}^{M} b_i x^{\beta_i} g_i$. Коэффициенты при мономе x^δ у этого многочлена и у многочлена f совпадают, поэтому многочлен g является линейной комбинацией многочленов со старшим мономом x^δ, причем все старшие мономы взаимно сокращаются. В таком случае согласно лемме

$$g = \sum \mu_{ij} S\left(x^{\beta_i} g_i, x^{\beta_j} g_j\right), \tag{1}$$

где суммирование ведется по таким i, j, что $1 \leqslant i \leqslant j \leqslant M$. Старшие мономы многочленов $x^{\beta_i} g_i$ и $x^{\beta_j} g_j$ совпадают, поэтому

$$S\left(x^{\beta_i} g_i, x^{\beta_j} g_j\right) = \frac{x^\delta}{c_i x^{\gamma_i}} g_i - \frac{x^\delta}{c_j x^{\gamma_j}} g_j = \frac{x^\delta}{c_j x^{\gamma_{ij}}} S(g_i, g_j),$$

где $x^{\gamma_{ij}}$ — наименьшее общее кратное мономов x^{γ_i} и x^{γ_j}.

По предположению многочлен $S(g_i, g_j)$ дает остаток 0 при делении на $g_1, \ldots, g_t$. Многочлен $S\left(x^{\beta_i} g_i, x^{\beta_j} g_j\right)$ делится на $S(g_i, g_j)$, поэтому он тоже дает остаток 0 при делении на $g_1, \ldots, g_t$. Алгоритм деления с остатком дает представление $S\left(x^{\beta_i} g_i, x^{\beta_j} g_j\right) = \sum h_{ij\nu} g_\nu$, где наибольшее из произведений старших мономов многочленов $h_{ij\nu}$ и g_ν совпадает со старшим мономом многочлена $S\left(x^{\beta_i} g_i, x^{\beta_j} g_j\right)$; последний моном строго меньше x^δ. Подставим полученное представление многочлена $S\left(x^{\beta_i} g_i, x^{\beta_j} g_j\right)$ в (1), а затем подставим полученное представление многочлена g в $f = g + \ldots$ В результате получим представление многочлена f, которое противоречит предположению о минимальности x^δ. Это противоречие показывает, что $x^\delta = x^\alpha$. □

С помощью теоремы 26.5 легко показать, что следующий алгоритм позволяет найти базис Грёбнера идеала, порожденного многочленами $f_1, \ldots, f_s$. Вычислим остатки от деления многочленов $S(f_i, f_j)$ на $f_1, \ldots, f_s$ и все ненулевые остатки добавим к набору $f_1, \ldots, f_s$. Повторим эту процедуру для полученного набора многочленов и т. д. Ясно, что эта последовательность операций завершается за конечное число

шагов, а согласно теореме 26.5 в итоге получаем базис Грёбнера идеала, порожденного многочленами $f_1, \ldots, f_s$. Этот алгоритм вычисления базиса Грёбнера называют *алгоритм Бухбергера*.

26.5. Приведенный базис Грёбнера

Для одного и того же идеала I алгоритм Бухбергера приводит к разным конечным результатам в зависимости от выбора образующих идеала и последовательности операций. Но этот алгоритм можно модифицировать так, чтобы конечный результат зависел лишь от самого идеала I; эта модификация также принадлежит Бухбергеру.

Первым делом добьемся, чтобы однозначно определено было число элементов базиса Грёбнера. Назовем базис Грёбнера $g_1, \ldots, g_t$ *минимальным*, если $g_i = x^{\alpha_i} + \ldots$ и мономы x^{α_i} и x^{α_j} не делятся друг на друга при $i \neq j$. У любого идеала I есть минимальный базис Грёбнера. В самом деле, пусть $g_1, \ldots, g_t$ — некоторый базис Грёбнера идеала I. Можно считать, что $g_i = x^{\alpha_i} + \ldots$. Если x^{α_1} делится на x^{α_2}, то $g_2, \ldots, g_t$ — базис Грёбнера идеала I. Действительно, если $f = x^{\alpha} + \ldots \in I$, то согласно определению базиса Грёбнера x^{α} делится на x^{α_i} при некотором i. Но x^{α_1} делится на x^{α_2}, поэтому x^{α} делится на x^{α_i} при $i \geqslant 2$. Это означает, что $g_2, \ldots, g_t$ — базис Грёбнера идеала I. Последовательно убирая многочлены, старшие мономы которых делятся на старшие мономы других многочленов, от базиса Грёбнера $g_1, \ldots, g_t$ можно перейти к минимальному базису Грёбнера.

Теорема 26.6. Если $g_1, \ldots, g_t$ и $f_1, \ldots, f_s$ — два минимальных базиса Грёбнера одного и того же идеала I, то $s = t$ и старшие мономы многочленов g_i и $f_{\sigma(i)}$, где σ — некоторая подстановка, совпадают.

Доказательство. Пусть $g_i = x^{\alpha_i} + \ldots$ и $f_j = x^{\beta_j} + \ldots$ С одной стороны, $f_1 \in I$ и $g_1, \ldots, g_t$ — базис Грёбнера идеала I. Поэтому x^{β_1} делится на x^{α_i} при некотором i. После перенумерации можно считать, что $i = 1$. С другой стороны, $g_1 \in I$ и $f_1, \ldots, f_s$ — базис Грёбнера идеала I. Поэтому x^{α_1} делится на x^{β_j} при некотором j, а значит, x^{β_1} делится на x^{β_j}. Из минимальности базиса Грёбнера $f_1, \ldots, f_s$ следует, что $j = 1$. Мономы x^{α_1} и x^{β_1} делятся друг на друга, поэтому $x^{\beta_1} = x^{\alpha_1}$.

Аналогичные рассуждения показывают, что x^{β_2} делится на x^{α_i}. Из минимальности базиса Грёбнера $f_1, \ldots, f_s$ следует, что $x^{\alpha_i} \neq x^{\beta_1}$, т. е. $i \neq 1$. Поэтому после перенумерации получаем $x^{\alpha_2} = x^{\beta_2}$ и т. д. Ясно,

что при этом многочлены $g_1, \ldots, g_t$ и $f_1, \ldots, f_s$ должны исчерпаться одновременно, т. е. $s = t$. □

Теперь уже можно добиться, чтобы однозначно было определено не только число элементов базиса Грёбнера, но и сами эти элементы. Назовем базис Грёбнера $g_1, \ldots, g_t$ *приведенным*, если $g_i = x^{\alpha_i} + \ldots$ и остаток от деления g_i на $g_1, \ldots g_{i-1}, g_{i+1}, \ldots, g_t$ совпадает с g_i, т. е. ни один из входящих в g_i мономов не делится на x^{α_j} при $j \neq i$. Ясно, что любой приведенный базис является также и минимальным.

С помощью минимального базиса Грёбнера $g_1, \ldots, g_t$ приведенный базис идеала I, порожденного многочленами $g_1, \ldots, g_t$, можно построить следующим образом. Пусть h_1 — остаток от деления g_1 на $g_2, \ldots, g_t$; h_2 — остаток от деления g_2 на $h_1, g_3, \ldots, g_t$; h_3 — остаток от деления g_3 на $h_1, h_2, g_4, \ldots, g_t$; $\ldots$; h_t — остаток от деления g_t на $h_1, h_2, \ldots, h_{t-1}$. Тогда $h_1, \ldots, h_t$ — приведенный базис Грёбнера идеала I. В самом деле, из минимальности базиса Грёбнера $g_1, \ldots, g_t$ следует, что старшие мономы многочленов h_i и g_i совпадают при всех i. Поэтому $h_1, \ldots, h_t$ — минимальный базис Грёбнера идеала I. Кроме того, при делении g_i на $h_1, \ldots h_{i-1}, g_{i+1}, \ldots, g_t$ получается остаток h_i, который не содержит членов, делящихся на старшие мономы многочленов $h_1, \ldots h_{i-1}$ и $g_{i+1}, \ldots$ $\ldots, g_t$; последние мономы совпадают со старшими мономами многочленов $h_{i+1}, \ldots, h_t$. Таким образом, $h_1, \ldots h_t$ — приведенный базис Грёбнера.

Теорема 26.7 (Бухбергер). Для любого идеала I существует ровно один приведенный базис Грёбнера.

Доказательство. Существование приведенного базиса Грёбнера только что было доказано. Остается доказать его единственность. Пусть $f_1, \ldots, f_t$ и $g_1, \ldots, g_s$ — два приведенных базиса Грёбнера идеала I. Приведенные базисы минимальны, поэтому согласно теореме 26.6 выполняется равенство $s = t$ и можно считать, что старшие мономы многочленов f_i и g_i совпадают. Предположим, что $f_i - g_i \neq 0$. Тогда старший моном многочлена $f_i - g_i \in I$ делится на старший моном некоторого многочлена g_j. При этом $j \neq i$, так как старший моном многочлена $f_i - g_i$ строго меньше старшего монома многочлена g_i. С другой стороны, если старший моном многочлена g_j делит старший моном многочлена $f_i - g_i$, то он должен делить какой-либо моном одного из многочленов f_i и g_i, а это противоречит приведенности базисов $f_1, \ldots, f_t$ и $g_1, \ldots, g_t$ (напомним, что старшие мономы многочленов g_j и f_j совпадают). □

Глава 7
Семнадцатая проблема Гильберта

27. Суммы квадратов: введение

27.1. Некоторые примеры

Нетрудно доказать, что любой многочлен $p(x)$ с действительными коэффициентами, принимающий неотрицательные значения при всех $x \in \mathbb{R}$, можно представить в виде суммы квадратов двух многочленов с действительными коэффициентами. В самом деле, корни многочлена с действительными коэффициентами разбиваются на действительные корни и пары комплексных корней. Поэтому

$$p(x) = a\prod_{j=1}^{s}(x - z_j)(x - \overline{z_j})\prod_{k=1}^{t}(x - \alpha_k)^{m_k},$$

где $\alpha_k \in \mathbb{R}$. Если $p(x) \geqslant 0$ при всех $x \in \mathbb{R}$, то $a \geqslant 0$ и все числа m_k четны, поэтому действительные корни тоже разбиваются на пары. Следовательно,

$$p(x) = \left(\sqrt{a}\prod_{j=1}^{l}(x - z_j)\right)\left(\sqrt{a}\prod_{j=1}^{l}(x - \overline{z_j})\right),$$

где некоторые из чисел z_j могут быть действительными. Пусть

$$\sqrt{a}\prod_{j=1}^{l}(x - z_j) = q(x) + ir(x),$$

где q и r — многочлены с действительными коэффициентами. Тогда

$$\sqrt{a}\prod_{j=1}^{l}(x - \overline{z_j}) = q(x) - ir(x).$$

В итоге получаем $p(x) = \big(q(x)\big)^2 + \big(r(x)\big)^2$.

Но для многочленов от нескольких переменных аналогичное утверждение уже не всегда верно, т. е. существуют *неотрицательные* многочлены (так мы будем называть многочлены с действительными коэффициентами, которые при всех действительных значениях перемен-

ных принимают неотрицательные значения), которые нельзя представить в виде суммы квадратов многочленов с действительными коэффициентами. Первым это доказал в 1888 г. Гильберт [Hi1], но он не привел явный пример такого многочлена. Первый простой пример привел Т. Моцкин в 1967 г.

Пример 27.1 [Мо]. Многочлен

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

неотрицателен, но его нельзя представить в виде суммы квадратов многочленов с действительными коэффициентами.

Доказательство. Проверим сначала, что $F(x,y) \geqslant 0$. Если $x=0$ или $y=0$, то $F(x,y)=1$. Поэтому будем считать, что $xy \neq 0$. В таком случае числа x^2, y^2 и $x^{-2}y^{-2}$ положительны и их произведение равно 1. Следовательно,

$$x^2+y^2+x^{-2}y^{-2} \geqslant 3,$$

а значит, $x^2y^2(x^2+y^2-3)+1 \geqslant 0$, что и требовалось.

Предположим теперь, что $F(x,y) = \sum f_j(x,y)^2$, где f_j — многочлены с действительными коэффициентами. Тогда $\sum f_j(x,0)^2 = F(x,0) = 1$. Следовательно, $f_j(x,0) = c_j$ — некоторая константа, а значит, $f_j(x,y) = c_j + yg_j(x,y)$. Аналогичные рассуждения показывают, что $f_j(x,y) = c_j' + xg_j'(x,y)$. Ясно, что при этом $c_j = c_j'$ и $f_j(x,y) = c_j + xyh_j(x,y)$. Таким образом,

$$x^2y^2(x^2+y^2-3)+1 = x^2y^2\sum h_j^2 + 2xy\sum c_jh_j + \sum c_j^2,$$

т. е.

$$x^2y^2(x^2+y^2-3) - x^2y^2\sum h_j^2 = 2xy\sum c_jh_j + \sum c_j^2 - 1.$$

Все одночлены, встречающиеся в правой части этого равенства, имеют степень не больше 3, а все одночлены, встречающиеся в левой части этого равенства, имеют степень не меньше 4. В самом деле,

$$\deg h_j = \deg f_j - 2 \leqslant \frac{1}{2}\deg F - 2 = 1.$$

Следовательно, $x^2y^2(x^2y^2-3) - x^2y^2\sum h_j^2 = 0$, а значит, $x^2+y^2-3 = \sum h_j^2$. Получено противоречие, так как $x^2+y^2-3 < 0$ при $x=y=0$. □

Пример 27.2 (R. M. Robinson, 1973). Многочлен

$$S(x,y) = x^2(x^2-1)^2 + y^2(y^2-1)^2 - (x^2-1)(y^2-1)(x^2+y^2-1)$$

неотрицателен, но его нельзя представить в виде суммы квадратов многочленов с действительными коэффициентами.

Доказательство. Проверим сначала, что $S(x,y) \geqslant 0$. Это очевидно для точек, лежащих в незаштрихованной на рис. 6 области, так как для любой такой точки либо $x^2+y^2-1 \leqslant 0$ и $(x^2-1)(y^2-1) \geqslant 0$, либо $x^2+y^2-1 \geqslant 0$ и $(x^2-1)(y^2-1) \leqslant 0$. Но $S(x,y)$ можно записать и по-другому, а именно,

$$S(x,y) = (x^2+y^2-1)(x^2-y^2)^2 + (x^2-1)(y^2-1).$$

При такой записи очевидно, что $S(x,y) \geqslant 0$ для точек, лежащих в заштрихованной области, так как для любой такой точки $x^2+y^2-1 \geqslant 0$ и $(x^2-1)(y^2-1) \geqslant 0$.

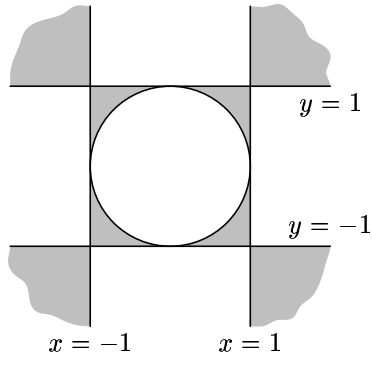

Рис. 6

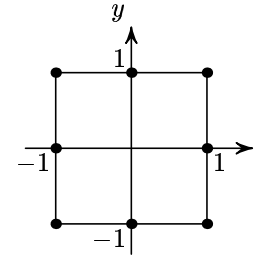

Рис. 7

Предположим теперь, что $S(x,y) = \sum f_j(x,y)^2$. Функция S обращается в нуль в 8 точках, отмеченных на рис. 7. Следовательно, в этих точках обращается в нуль каждая из функций f_j. Но $\deg f_j \leqslant \frac{1}{2}\deg S = 3$, а если кривая степени не более 3 проходит через указанные 8 точек, то она обязательно проходит и через точку $(0,0)$; это мы докажем чуть позже. Итак, $f_j(0,0) = 0$ при всех j, поэтому $S(0,0) = 0$. Но, как легко убедиться, $S(0,0) = 1$. Полученное противоречие показывает, что многочлен $S(x,y)$ нельзя представить в виде суммы квадратов многочленов.

Доказательство того, что кубическая кривая, проходящая через 8 точек пересечения прямых p_i и q_j $(i,j=1,2,3)$, обязательно проходит и через девятую точку, можно найти в книге [ПрС]. Но для рассматриваемой конфигурации точек можно привести и более простое доказательство. Припишем точкам $(\pm1,\pm1)$ вес 1, точкам $(\pm1,0)$ и $(0,\pm1)$ вес -2, а точке $(0,0)$ вес 4. Рассмотрим сумму по этим точкам значений функции x^py^q, умноженных на соответствующие веса. Если $pq=0$, то сумма нулевая. Если $p>0$ и $q>0$, то ненулевой вклад в сумму дают только точки $(\pm1,\pm1)$. При этом сумма окажется ненулевой лишь в том случае, когда оба числа p и q четны. Но у многочлена f_j степени не больше 3 таких одночленов нет. Поэтому взвешенная сумма значений многочлена f_j по рассматриваемым 9 точкам равна нулю. В частности, если f_j обращается в нуль в восьми точках, то f_j обращается в нуль и в девятой точке. □

Пример 27.3 (R. M. Robinson, 1973). Многочлен
$Q(x,y,z)=x^2(x-1)^2+y^2(y-1)^2+z^2(z-1)^2+2xyz(x+y+z-2)$
неотрицателен, но его нельзя представить в виде суммы квадратов многочленов.

Доказательство. Предположим, что $Q(x,y,z)=\sum f_j(x,y,z)^2$. Тогда степень каждого многочлена f_j не превосходит 2. А так как функция $Q(x,y,z)$ обращается в нуль во всех точках (x,y,z) с координатами $x,y,z=0$ или 1, за исключением точки $(1,1,1)$, то во всех этих точках обращаются в нуль функции f_j. Как мы сейчас убедимся, из этого следует, что $f_j(1,1,1)=0$. Но тогда $Q(1,1,1)=0$, а непосредственные вычисления показывают, что $Q(1,1,1)=2$.

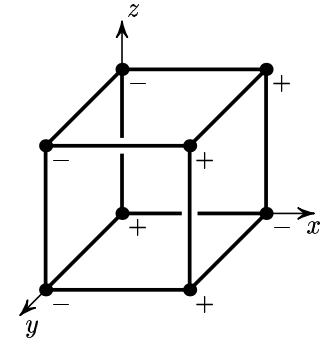

Рис. 8

Припишем восьми рассматриваемым точкам веса ±1 так, как это показано на рис. 8, и рассмотрим сумму по этим точкам функции $f_j(x,y,z)$ с соответствующими весами. Легко проверить, что рассматриваемая сумма равна нулю для следующих функций: $1,x,xy,x^2$. Поэтому она равна нулю и для функции $f_j(x,y,z)$, так как ее степень не превосходит 2. Следовательно, если в семи из восьми рассматриваемых точек функция f_j обращается в нуль, то она обращается в нуль и в восьмой точке.

Докажем теперь, что $Q(x,y,z) \geqslant 0$. Запишем для этого многочлен Q по-другому:

$$\begin{aligned} Q &= x^2(x-1)^2 + \big(y(y-1) - z(z-1)\big)^2 + Q_x = \\ &= y^2(y-1)^2 + \big(z(z-1) - x(x-1)\big)^2 + Q_y = \\ &= z^2(z-1)^2 + \big(x(x-1) - y(y-1)\big)^2 + Q_z, \end{aligned}$$

где

$$\begin{aligned} Q_x &= 2yz(x+y-1)(x+z-1), \\ Q_y &= 2xz(x+y-1)(y+z-1), \\ Q_z &= 2xy(x+z-1)(y+z-1). \end{aligned}$$

Достаточно доказать, что в любой точке (x,y,z) одна из функций Q_x, Q_y, Q_z неотрицательна. Но эти функции не могут быть одновременно отрицательными, так как их произведение представляет собой квадрат многочлена

$$2\sqrt{2}xyz(x+y-1)(x+z-1)(y+z-1). \qquad \square$$

Пример 27.4 (Anneli Lax, Peter D. Lax, 1978). Форма $A(x) = A_1(x) + A_2(x) + A_3(x) + A_4(x) + A_5(x)$, где $x = (x_1, x_2, x_3, x_4, x_5)$ и $A_i(x) = \prod\limits_{j \neq i} (x_i - x_j)$, неотрицательна, но ее нельзя представить в виде суммы квадратов форм.

Замечание. Рассматриваемая форма зависит только от разностей переменных, поэтому ее можно представить в виде формы от четырех переменных. Поделив эту новую форму на четвертую степень одной из переменных, можно получить многочлен степени 4 от 3 переменных.

Проверим сначала, что $A(x) \geqslant 0$. Значение формы $A(x)$ не изменяется при любой перестановке переменных, поэтому можно считать, что $x_1 \geqslant x_2 \geqslant x_3 \geqslant x_4 \geqslant x_5$. В таком случае

$$\begin{aligned} &A_1(x) + A_2(x) = \\ &= (x_1 - x_2)\big((x_1 - x_3)(x_1 - x_4)(x_1 - x_5) - (x_2 - x_3)(x_2 - x_4)(x_2 - x_5)\big) \geqslant 0, \end{aligned}$$

так как $x_1 - x_2 \geqslant 0, x_1 - x_3 \geqslant 0, x_2 - x_3 \geqslant 0$ и т. д. Аналогично доказывается, что $A_4(x) + A_5(x) \geqslant 0$. Ясно также, что $A_3(x)$ представляет собой произведение двух неположительных и двух неотрицательных сомножителей, поэтому $A_3(x) \geqslant 0$.

Предположим теперь, что $A(x) = \sum Q_j(x)^2$, где Q_j — квадратичные формы. Если каждая переменная x_i равна какой-то другой переменной x_k, то $A(x) = 0$, а значит, $Q_j(x) = 0$. Поэтому квадрика $Q_j(x) = 0$ в $\mathbb{R}P^4$ содержит проективную прямую $x_1 = x_2, x_3 = x_4 = x_5$. При перестановках координат получаем 10 прямых такого вида (для задания прямой нужно выбрать 2 координаты из 5). Эти прямые пересекают гиперплоскость общего положения в 10 точках, причем через эти точки должна проходить квадрика $Q_j(x) = 0$. Но в трехмерном пространстве не через любые 10 точек проходит квадрика, поэтому можно ожидать, что форма Q_j тождественно равна нулю. Мы сейчас убедимся, что это действительно так, и тем самым придем к противоречию.

Пусть $Q(x) = \sum c_{ij}x_ix_j$, $c_{ij} = c_{ji}$. По предположению

$$\begin{aligned} 0 = Q(s,s,t,t) = (c_{11} + 2c_{12} + c_{22})s^2 + \\ + 2(c_{13} + c_{14} + c_{15} + c_{23} + c_{24} + c_{25})st + \\ + (c_{33} + c_{44} + c_{55} + 2c_{34} + 2c_{35} + 2c_{45})t^2. \end{aligned}$$

Следовательно,

$$c_{11} + 2c_{12} + c_{22} = 0, \tag{1}$$

$$c_{13} + c_{14} + c_{15} + c_{23} + c_{24} + c_{25} = 0, \tag{2}$$

$$c_{33} + c_{44} + c_{55} + 2c_{34} + 2c_{35} + 2c_{45} = 0. \tag{3}$$

Кроме того, выполняются аналогичные равенства, получающиеся в результате любой перестановки индексов. В частности, из (1) следует, что

$$c_{33} + 2c_{34} + c_{44} = 0. \tag{4}$$

Вычитая (4) из (3), получаем

$$c_{55} + 2c_{35} + 2c_{45} = 0.$$

Пусть $c_{55} = \lambda$. Тогда при попарно различных i и j, отличных от 5, выполняется равенство $c_{i5} + c_{j5} = -\lambda/2$. Следовательно, $c_{15} = c_{25} = c_{35} = c_{45} = -\lambda/4$. Аналогично $c_{21} = c_{31} = c_{41} = c_{51} = c_{15} = -\lambda/4$ и т. д. В результате получаем $c_{ii} = \lambda$ и $c_{ij} = -\lambda/4$ при $i \neq j$. Но в таком случае из (2) следует, что $\lambda = 0$, т. е. $Q(x) = 0$ при всех x.

27.2. Теорема Артина–Касселса–Пфистера

В параграфе 27.1 мы привели примеры неотрицательных многочленов, которые нельзя представить в виде суммы квадратов многочле-

нов. В дальнейшем мы покажем, что любой неотрицательный многочлен можно представить в виде суммы квадратов рациональных функций. Но для многочленов от одной переменной нет существенной разницы между представлением в виде суммы квадратов многочленов и представлением в виде суммы квадратов рациональных функций. Дело в том, что справедливо следующее утверждение.

Теорема 27.1. Пусть K — поле, характеристика которого не равна 2, $f(x)$ — многочлен над K. Предположим, что

$$f(x) = \alpha_1 r_1(x)^2 + \ldots + \alpha_n r_n(x)^2,$$

где $\alpha_i \in K$, $r_i(x)$ — рациональные функции над K. Тогда

$$f(x) = \alpha_1 p_1(x)^2 + \ldots + \alpha_n p_n(x)^2,$$

где $p_i(x)$ — многочлены над K.

Эта теорема имеет долгую историю. В 1927 г. Артин [Ar] доказал, что

$$f(x) = \beta_1 p_1(x)^2 + \ldots + \beta_m p_m(x)^2,$$

где m — некоторое число, не обязательно равное n. Затем в 1964 г. Касселс [Ca] доказал, что можно считать, что $m = n$. А в 1965 г. Пфистер [Pf1] доказал, что можно считать, что $\beta_i = \alpha_i$.

Теорему 27.1 можно применить и к многочлену $f(x_1, \ldots, x_n)$ от n переменных над полем L. Для этого нужно положить, например, $x = x_1$ и $K = L(x_2, \ldots, x_n)$ — поле рациональных функций от переменных $x_2, \ldots, x_n$ над полем L. В результате получим, что в представлении многочлена f в виде суммы квадратов рациональных функций в знаменателях этих рациональных функций можно избавиться от любой из переменных (но нельзя избавиться от всех переменных одновременно).

Доказательство. При $n = 1$ утверждение очевидно, поэтому в дальнейшем будем считать, что $n > 1$ и все $\alpha_i \neq 0$. Доказательство удобно провести на языке квадратичных форм над полем $K(x)$. Пусть $v = (v_1, \ldots, v_n)$ — вектор с координатами из $K(x)$. Положим $\varphi(u, v) = \sum \alpha_i u_i v_i$. Требуется доказать, что если $f \in K[x]$ и $f = \varphi(u, u)$, где $u_i \in K(x)$, то $f = \varphi(w, w)$, где $w_i \in K[x]$. Квадратичная форма $\varphi(u, u)$ может быть либо изотропной (т. е. $\varphi(u, u) = 0$ для некоторого $u \neq 0$), либо анизотропной (т. е. $\varphi(u, u) \neq 0$ при $u \neq 0$).

Случай 1: *форма* $\varphi(u,u)$ *изотропна*. В этом случае нам даже не потребуется условие $f=\varphi(u,u)$ для $u_i\in K(x)$. Иными словами, для любого многочлена f найдется такой вектор u с координатами из $K[x]$, что $f=\varphi(u,u)$.

В равенстве $\varphi(u,u)=0$ можно считать, что u — многочлен; для этого достаточно рациональные функции u_i привести к общему знаменателю. Можно также считать, что многочлены $u_1,\dots,u_n$ взаимно просты в совокупности. Тогда существуют такие многочлены $v_1,\dots,v_n$, что $u_1v_1+\dots+u_nv_n=1$. В самом деле, в виде $u_1f_1+u_2f_2$ можно представить НОД(f_1,f_2); затем в виде $(u_1f_1+u_2f_2)g_1+u_3f_3$ можно представить НОД(f_1,f_2,f_3) и т. д. Поделив каждый многочлен v_i на число $2\alpha_i$, получим такой вектор v, что $\varphi(u,v)=1/2$. А так как $\varphi(u,v+\lambda u)=\varphi(u,v)$ и $\varphi(v+\lambda u,v+\lambda u)=\varphi(v,v)+\lambda$, то после замены v на $v-\varphi(v,v)u$ можно будет считать, что $\varphi(v,v)=0$.

Равенство

$$\varphi(fu+v,fu+v)=f^2\varphi(u,u)+2f\varphi(u,v)+\varphi(v,v)=f$$

показывает, что любой многочлен f можно представить в виде $f=\varphi(w,w)$, где $w=fu+v$.

Случай 2: *форма* $\varphi(u,u)$ *анизотропна*. В этом случае без условия $f=\varphi(u,u)$ для $u_i\in K(x)$ обойтись уже нельзя. Это видно из следующего примера: $K=\mathbb{R}$, $f(x)=-1$ и $\varphi(u,u)=u_1^2+\dots+u_n^2$.

Умножим обе части равенства $f=\varphi(u,u)$ на общий знаменатель рациональных функций $u_1,\dots,u_n$. В результате получим равенство вида $\alpha_1u_1^2+\dots+\alpha_nu_n^2=fu_0^2$, где $u_0,\dots,u_n$ — многочлены. Среди всех равенств такого вида можно выбрать равенство, в котором многочлен u_0 имеет минимальную степень r. Требуется доказать, что $r=0$. Предположим, что $r=\deg u_0>0$. Поделим многочлен u_i на u_0 с остатком и тем самым найдем такой многочлен v_i, что $\deg(u_i-u_0v_i)\leqslant r-1$.

Помимо векторов $u=(u_1,\dots,u_n)$ и $v=(v_1,\dots,v_n)$ рассмотрим векторы $\widetilde{u}=(u_0,\dots,u_n)$ и $\widetilde{v}=(v_0,\dots,v_n)$, где $v_0=1$. Рассмотрим также форму $\widetilde{\varphi}(\widetilde{x},\widetilde{y})=\varphi(x,y)-fx_0y_0$. По условию $\widetilde{\varphi}(\widetilde{u},\widetilde{u})=\varphi(u,u)-fu_0^2=0$. Кроме того, $\widetilde{\varphi}(\widetilde{v},\widetilde{v})=\varphi(v,v)-f$, так как $v_0=1$. Поэтому равенство $\widetilde{\varphi}(\widetilde{v},\widetilde{v})=0$ противоречит условию $r>0$. В дальнейшем будем считать, что $\widetilde{\varphi}(\widetilde{v},\widetilde{v})\neq0$. Это, в частности, означает, что векторы $\widetilde{u}$ и $\widetilde{v}$ не пропорциональны. В таком случае вектор $\widetilde{w}=\widetilde{\varphi}(\widetilde{v},\widetilde{v})\widetilde{u}-2\widetilde{\varphi}(\widetilde{u},\widetilde{v})\widetilde{v}$ ненулевой и $\widetilde{\varphi}(\widetilde{w},\widetilde{w})=0$, так как $\widetilde{\varphi}(\lambda\widetilde{u}-\mu\widetilde{v},\lambda\widetilde{u}-\mu\widetilde{v})=\mu\bigl(-2\lambda\widetilde{\varphi}(\widetilde{u},\widetilde{v})+\mu\widetilde{\varphi}(\widetilde{v},\widetilde{v})\bigr)=0$ при $\lambda=\widetilde{\varphi}(\widetilde{v},\widetilde{v})$ и $\mu=\widetilde{\varphi}(\widetilde{u},\widetilde{v})$.

Итак, мы построили ненулевой вектор $\widetilde{w} = (w_0, w)$ с полиномиальными координатами, удовлетворяющий равенству $\varphi(w,w) - fw_0^2 = 0$. Чтобы прийти к противоречию, достаточно убедиться, что $\deg w_0 < r$. Учитывая, что $v_0 = 1$, получаем

$$\widetilde{w}_0 = \widetilde{\varphi}(\widetilde{v},\widetilde{v})u_0 - 2\widetilde{\varphi}(\widetilde{u},\widetilde{v})v_0 = \Big(\sum_{i=1}^n \alpha_i v_i^2 - f\Big)u_0 - 2\Big(\sum_{i=1}^n \alpha_i u_i v_i - fu_0\Big) =$$
$$= \sum_{i=1}^n \alpha_i\Big(v_i^2 u_0 - 2u_i v_i + \frac{u_i^2}{u_0}\Big) - \sum_{i=1}^n \frac{\alpha_i u_i^2}{u_0} + fu_0 = \frac{1}{u_0}\sum_{i=1}^n \alpha_i (u_i - u_0 v_i)^2,$$

так как $\sum\limits_{i=1}^n \alpha_i u_i^2 = fu_0^2$.

Напомним, что $\deg(u_i - u_0 v_i) \leqslant r-1$. Поэтому

$$\deg w_0 = \deg\Big(\sum_{i=1}^n \alpha_i (u_i - u_0 v_i)^2\Big) - \deg u_0 \leqslant 2(r-1) - r = r-2. \quad \square$$

С помощью теоремы 27.1 можно указать неотрицательный многочлен от n переменных, который нельзя представить в виде суммы n квадратов рациональных функций.

Теорема 27.2. Многочлен $x_1^2 + \ldots + x_n^2 + 1$ нельзя представить в виде суммы n квадратов рациональных функций от переменных $x_1, \ldots, x_n$ над полем $\mathbb{R}$.

Доказательство. Положим $K = \mathbb{R}(x_1, \ldots x_{n-1})$ и $x = x_n$ в условии теоремы 27.1. Предположим, что многочлен $x_1^2 + \ldots + x_n^2 + 1$ представлен в виде суммы n квадратов рациональных функций от $x_1, \ldots, x_n$. Это означает, что многочлен $x^2 + d$, где $d = x_1^2 + \ldots + x_{n-1}^2 + 1 \in K$, можно представить в виде суммы n квадратов элементов поля $K(x)$. В таком случае согласно теореме 27.1 многочлен $x^2 + d$ можно представить в виде суммы n квадратов элементов кольца $K[x]$, т. е.

$$x^2 + d = \sum_{i=1}^n \left(a_{i0} + a_{i1}x + a_{i2}x^2 + \ldots\right)^2.$$

Ясно, что при этом должно выполняться равенство $a_{i2} = a_{i3} = \ldots = 0$. Таким образом,

$$x^2 + d = \sum_{i=1}^n (a_i x + b_i)^2, \quad a_i, b_i \in K.$$

Подставим в полученное равенство такое значение $x = c$, что $c^2 = (a_n c + b_n)^2$, т. е. $(1 \pm a_n)c \pm b_n = 0$ (при $a_n \neq \pm 1$ можно взять любой знак, а при $a_n = \pm 1$ допустим только один знак). В результате получим $d = \sum_{i=1}^{n-1} (a_i c + b_i)^2$, где $c, a_i, b_i \in K$. Иными словами, многочлен $x_1^2 + \ldots + x_{n-1}^2 + 1$ допускает представление в виде суммы $n-1$ квадратов рациональных функций от переменных $x_1, \ldots, x_{n-1}$ над полем $\mathbb{R}$. Повторяя аналогичные рассуждения, в конце концов получим, что многочлен $x_1^2 + 1$ является квадратом рациональной функции от x_1 над полем $\mathbb{R}$. Получено противоречие. □

27.3. Неравенство между средним арифметическим и средним геометрическим

Неравенство между средним арифметическим и средним геометрическим заключается в следующем. Если $x_1, \ldots, x_n$ — неотрицательные числа, то

$$\frac{x_1 + x_2 + \ldots + x_n}{n} \geqslant (x_1 x_2 \ldots x_n)^{1/n}.$$

Заменим x_i на t_i^{2n}. Тогда это неравенство примет вид

$$P(t_1, \ldots, t_n) = \frac{t_1^{2n} + t_2^{2n} + \ldots + t_n^{2n}}{n} - t_1^2 t_2^2 \cdot \ldots \cdot t_n^2 \geqslant 0.$$

Теорема 27.3 (Гурвиц [Hu]). Многочлен $P(t_1, \ldots, t_n)$ можно представить в виде суммы квадратов многочленов.

Доказательство. Положим $y_i = t_i^2$. Для функции $f(y_1, \ldots, y_n)$ рассмотрим

$$Sf(y_1, \ldots, y_n) = \sum_{\sigma \in S_n} f(y_{\sigma(1)}, \ldots, y_{\sigma(n)}).$$

Например,

$$\left.\begin{aligned} Sy_1^n &= (n-1)!(y_1^n + \ldots + y_n^n), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ Sy_1 \cdot \ldots \cdot y_n &= n!\, y_1 \cdot \ldots \cdot y_n. \end{aligned}\right\} (1)$$

Рассмотрим функции

$$\begin{aligned}
\varphi_1 &= S\big((y_1^{n-1} - y_2^{n-1})(y_1 - y_2)\big),\\
\varphi_2 &= S\big((y_1^{n-2} - y_2^{n-2})(y_1 - y_2)y_3\big),\\
\varphi_3 &= S\big((y_1^{n-3} - y_2^{n-3})(y_1 - y_2)y_3y_4\big),\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
\varphi_{n-1} &= S\big((y_1 - y_2)(y_1 - y_2)y_3y_4 \cdot \dots \cdot y_n\big),
\end{aligned}$$

Легко проверить,что

$$\varphi_1 = Sy_1^n + Sy_2^n - Sy_1^{n-1} - Sy_2^{n-1}y_1 = 2Sy_1^n - 2Sy_1^{n-1}y_2.$$

Аналогично

$$\begin{aligned}
\varphi_2 &= 2Sy_1^{n-1}y_2 - 2Sy_1^{n-2}y_2y_3,\\
\varphi_3 &= 2Sy_1^{n-2}y_2y_3 - 2Sy_1^{n-3}y_2y_3y_4,\\
&\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
\varphi_{n-1} &= 2Sy_1^2y_2y_3 \cdot \dots \cdot y_{n-1} - 2Sy_1y_2 \cdot \dots \cdot y_n.
\end{aligned}$$

Следовательно,

$$\varphi_1 + \varphi_2 + \dots + \varphi_{n-1} = 2Sy_1^n - 2Sy_1y_2 \dots y_n.$$

Учитывая соотношения (1), получаем

$$\frac{y_1^n + y_2^n + \dots + y_n^n}{n} - y_1y_2 \cdot \dots \cdot y_n = \frac{1}{2n!}(\varphi_1 + \varphi_2 + \dots + \varphi_{n-1}),$$

т. е.

$$\frac{t_1^{2n} + t_2^{2n} + \dots + t_n^{2n}}{n} - t_1^2t_2^2 \cdot \dots \cdot t_n^2 = \frac{1}{2n!}(\varphi_1 + \varphi_2 + \dots + \varphi_{n-1}),$$

где

$$\begin{aligned}
\varphi_k &= S\big((y_1^{n-k} - y_2^{n-k})(y_1 - y_2)y_3y_4 \cdot \dots \cdot y_{k+1}\big) =\\
&= S\big((y_1 - y_2)^2(y_1^{n-k-1} + y_1^{n-k-2}y_2 + \dots + y_2^{n-k-1})y_3y_4 \cdot \dots \cdot y_{k+1}\big) =\\
&= S\big((t_1^2 - t_2^2)^2(t_1^{2(n-k-1)} + t_1^{2(n-k-2)}t_2^2 + \dots + t_2^{2(n-k-1)})t_3^2t_4^2 \cdot \dots \cdot t_{k+1}^2\big).
\end{aligned}$$

Таким образом, φ_k — сумма квадратов многочленов от $t_1, \dots, t_n$. □

27.4. Теорема Гильберта о неотрицательных многочленах $p_4(x, y)$

Пусть p_k обозначает многочлен степени k. В параграфе 27.1 мы привели примеры неотрицательных многочленов типа $p_6(x, y)$ и $p_4(x, y, z)$, которые нельзя представить в виде суммы квадратов многочленов. Для многочленов типа $p_2(x_1, \ldots, x_n)$ таких примеров не существует. В самом деле, многочлену $p_2(x_1, \ldots, x_n)$ соответствует квадратичная форма

$$F_2(y_1, \ldots, y_{n+1}) = y_{n+1}^2 p_2(y_1/y_{n+1}, \ldots, y_n/y_{n+1}).$$

Любую квадратичную форму можно представить в виде $f_1^2 + \ldots + f_k^2 - f_{k+1}^2 - \ldots - f_{n+1}^2$, где $f_1, \ldots, f_{n+1}$ — линейные формы. Ясно, что многочлен p_2 будет неотрицательным лишь в том случае, когда $f_{k+1} = \ldots = f_{n+1} = 0$.

Гораздо сложнее доказать, что любой неотрицательный многочлен типа $p_4(x, y)$ можно представить в виде суммы квадратов многочленов.

Теорема 27.4 (Гильберт). Любой неотрицательный многочлен типа $p_4(x, y)$ можно представить в виде суммы трех квадратов многочленов.

Мы приведем два доказательства этой теоремы. Первое доказательство более простое, но оно позволяет доказать лишь более слабое утверждение, а именно, будет показано, что $p_4(x, y)$ можно представить в виде суммы нескольких (не обязательно трех) квадратов многочленов. Второе — оригинальное доказательство Гильберта.

Оба доказательства нам будет удобнее проводить не для многочленов, а для однородных форм $F_4(x, y, z)$.

Первое доказательство (Choi–Lam). Мы будем доказывать, что любую неотрицательную однородную форму $F_4(x, y, z)$ можно представить в виде суммы квадратов однородных форм. Первая часть доказательства относится к формам любой степени от любого числа переменных.

Двум формам P и Q степени n от m переменных можно сопоставить форму $\lambda P + \mu Q$, т. е. на множестве всех таких форм имеется естественная структура линейного пространства. Поэтому формы можно считать точками аффинного пространства; начало координат соответствует нулевой форме.

Неотрицательные формы образуют замкнутый выпуклый конус C с вершиной в начале координат O. Ясно, что если Q — ненулевая форма и $Q \in C$, то $-Q \notin C$. Поэтому любая плоскость, проходящая через O и Q, пересекает C по (замкнутому) углу Q_1OQ_2, величина которого строго меньше π. При этом форма Q является выпуклой линейной комбинацией форм Q_1 и Q_2.

Проведем опорные гиперплоскости к конусу C, проходящие через лучи OQ_1 и OQ_2. Они пересекают конус C по некоторым выпуклым конусам строго меньшей размерности. Рассмотрим сечение каждого из этих конусов плоскостью, проходящей через точки O и Q. После нескольких таких операций мы обязательно придем к конусам размерности 1 (лучам).

Точку A замкнутого выпуклого конуса C называют *экстремальной*, если для нее существует опорная гиперплоскость, пересекающая конус C лишь по лучу OA. Иными словами, точка A экстремальная, если она не является внутренней точкой отрезка, концы которого принадлежат конусу C, но не лежат на луче OA. Описанная выше конструкция показывает, что *любая неотрицательная однородная форма Q является выпуклой линейной комбинацией экстремальных неотрицательных форм.*

До сих пор мы рассматривали формы любой степени от любого числа переменных. Но следующее утверждение справедливо лишь для форм степени 4 от 3 переменных.

Лемма 27.1. Любую неотрицательную однородную форму степени 4 $T(x, y, z) \not\equiv 0$ можно представить в виде

$$T = q^2 + T_1,$$

где $q \not\equiv 0$ — квадратичная форма, T_1 — неотрицательная форма.

Следствие. Любая экстремальная неотрицательная форма степени 4 $T(x, y, z)$ является полным квадратом.

Следствие вытекает из леммы очевидным образом: для экстремальной неотрицательной формы T разложение $T = q^2 + T_1$ должно быть тривиальным, т. е. формы q^2 и T_1 должны быть пропорциональны. В свою очередь, из следствия очевидным образом вытекает теорема. В самом деле, выпуклая линейная комбинация экстремальных неотрицательных форм степени 4 от 3 переменных представляет собой сумму квадратов квадратичных форм.

Доказательство. Пусть $Z(T)$ — множество нулей формы T, рассматриваемых с точностью до пропорциональности (т. е. множество нулей этой формы в $\mathbb{R}P^2$).

Случай 1: $Z(T) = \varnothing$. На единичной сфере $x^2 + y^2 + z^2 = 1$ функция T принимает минимальное значение $\mu > 0$, поэтому $T(x, y, z) \geqslant \mu(x^2 + y^2 + z^2)^2$ при всех (x, y, z).

Случай 2: $Z(T)$ *состоит из одной точки*; без ограничения общности можно считать, что $T(1, 0, 0) = 0$. В таком случае коэффициент при x^4 равен 0, поэтому

$$T(x, y, z) = x^3(\alpha_1 y + \alpha_2 z) + x^2 f(y, z) + 2xg(y, z) + h(y, z).$$

Если $\alpha_1 \neq 0$ или $\alpha_2 \neq 0$, то при $x \to \pm\infty$ можно получить отрицательные значения T. Поэтому

$$T(x, y, z) = x^2 f + 2xg + h.$$

Ясно также, что $f \geqslant 0$ и $h \geqslant 0$.

В разложении

$$fT = (xf + g)^2 + (fh - g^2)$$

форма $fh - g^2$ неотрицательна. В самом деле, если $fh - g^2 < 0$ в точке (a, b), то $f(a, b) \neq 0$. Положив $x = -g(a, b)/f(a, b)$, получим $fT < 0$ в точке (x, a, b).

Неотрицательную квадратичную форму $f(x, y)$ можно представить в виде квадрата линейной формы или в виде суммы двух квадратов линейных форм. В соответствии с этим разберем два варианта.

(а) $f = f_1^2$, где $f_1 = \alpha y + \beta z$. В точке $(-\beta, \alpha)$ получаем $fh - g^2 = -g^2 \leqslant 0$, поэтому $g(-\beta, \alpha) = 0$, так как форма $fh - g^2$ неотрицательна. Таким образом, $g = f_1 g_1$. Следовательно,

$$fT \geqslant (xf + g)^2 = (xf_1^2 + f_1 g_1)^2 = f_1^2(xf_1 + g_1)^2 = f(xf_1 + g_1)^2,$$

а значит, $T \geqslant (xf_1 + g_1)^2$.

(б) $f = f_1^2 + f_2^2$, где f_1 и f_2 — линейные формы, не имеющие нетривиальных (т. е. отличных от начала координат) общих нулей. В таком случае $f(y, z) > 0$ при $(y, z) \neq (0, 0)$. Предположим, что $fh - g^2 = 0$ при $(y, z) = (a, b) \neq (0, 0)$. Тогда $T = 0$ при $(x, y, z) = \big(-g(a, b)/f(a, b), a, b\big)$. Приходим к противоречию, так как по предположению у T есть только один нуль в $\mathbb{R}P^2$, а именно $(1, 0, 0)$.

Итак, $fh - g^2 > 0$ при $(y, z) \neq (0, 0)$, а значит, $(fh - g^2)/f^3 \geqslant \mu > 0$ на единичной окружности. Следовательно, $fh - g^2 \geqslant \mu f^3$ при всех (y, z). Поэтому $T \geqslant (fh - g^2)/f \geqslant \mu f^2 = (\sqrt{\mu} f)^2$.

Случай 3: $Z(T)$ *содержит не менее двух точек*; без ограничения общности можно считать, что $T(1,0,0) = T(0,1,0) = 0$. Как и в случае 2, форма T не может содержать членов с x^4 и x^3, а также членов с y^4 и y^3. Поэтому

$$T(x,y,z) = x^2 f(y,z) + 2xzg(y,z) + z^2 h(y,z).$$

В разложении

$$fT = (xf + zg)^2 + z^2(fh - g^2)$$

форма $fh - g^2$ неотрицательна.

При разборе варианта (а) случая 2 мы не пользовались тем, что у формы T есть ровно один нуль. Поэтому если $f = f_1^2$ (или $h = h_1^2$), то можно применить те же самые рассуждения. Остается рассмотреть случай, когда $f > 0$ и $g > 0$. Мы снова разберем два варианта.

(а) $fh - g^2$ имеет нетривиальный нуль (a,b). Пусть $\alpha = -g(a,b)/f(a,b)$,

$$T_1(x,y,z) = T(x + \alpha z, y, z) = x^2 f + 2xz(g + \alpha f) + z^2(h + 2\alpha g + \alpha^2 f).$$

В точке (a,b) получаем

$$h + 2\alpha g + \alpha^2 f = h + 2\frac{-g}{f}g + \frac{g^2}{f^2}f = h - g^2 f = \frac{hf - g^2}{f^2} = 0.$$

Поэтому $h + 2\alpha g + \alpha^2 f = h_1^2$. Таким образом, $T_1(x,y,z) \geqslant (zh_1)^2$, а значит,

$$T(x,y,z) = T_1(x - \alpha z, y, z) \geqslant \big(zh_1(x - \alpha z, y, z)\big)^2.$$

(б) $fh - g^2 > 0$. В таком случае

$$\frac{fh - g^2}{(y^2 + z^2)f} \geqslant \mu > 0,$$

а значит,

$$fT = (xf + zg)^2 + z^2(fh - g^2) \geqslant z^2(fh - g^2) \geqslant \mu z^2(y^2 + z^2)f.$$

В итоге получаем $T \geqslant (\sqrt{\mu}zy)^2 + (\sqrt{\mu}z^2)^2 \geqslant (\sqrt{\mu}z^2)^2$. □ □

Второе доказательство. (Гильберт) Основная идея этого доказательства заключается в том, чтобы рассмотреть множество A, состоящее из тех вещественных форм от трех переменных, которые можно представить в виде $f^2 + g^2 + h^2$, где f, g, h — *вещественные* квадратичные формы, не имеющие нетривиальных общих нулей над полем *комплексных* чисел.

Лемма 27.2. Множество A открыто.

Доказательство. Коэффициенты a_{ijk} формы $\sum a_{ijk}x^iy^jz^k$ можно считать координатами в $\mathbb{R}^n$. Поэтому отображение

$$\Phi\colon (f,g,h) \mapsto F = f^2 + g^2 + h^2$$

представляет собой алгебраическое отображение $\mathbb{R}^{18} \to \mathbb{R}^{15}$ (квадратичная форма от 3 переменных задается 6 коэффициентами, а форма степени 4 задается 15 коэффициентами).

Достаточно доказать, что если $(f,g,h) \in A$, то дифференциал $d\Phi$ отображения Φ в точке (f,g,h) имеет ранг 15, т. е. $\dim\ker\Phi = 3$. Ясно, что

$$d\Phi(u,v,w) = 2(uf + vg + wh),$$

где $(u,v,w) \in \mathbb{R}^{18}$ — тройка квадратичных форм, $uf+vg+wh$ — форма степени 4.

Квадратичные формы f,g,h не имеют нетривиальных общих нулей над $\mathbb{C}$. Покажем, что в таком случае из равенства

$$uf + vg + wh = 0 \tag{1}$$

(u,v,w — квадратичные формы) следует, что

$$u = \nu g - \mu h, \quad v = \lambda h - \nu f, \quad w = \mu f - \lambda g$$

для некоторых $\lambda,\mu,\nu \in \mathbb{C}$.

Достаточно доказать, что

$$u = \nu_1 g - \mu_1 h, \quad v = \lambda_1 h - \nu_2 f, \quad w = \mu_2 f - \lambda_2 g.$$

В самом деле, тогда

$$(\lambda_1 - \lambda_2)hg + (\mu_2 - \mu_1)fh + (\nu_1 - \nu_2)fg = 0.$$

Кривые $f = 0, g = 0$ и $h = 0$ попарно различны, поэтому на кривой $f = 0$ есть точка, не принадлежащая кривым $g = 0$ и $h = 0$. Рассмотрев значения f,g и h в этой точке, получим $\lambda_1 = \lambda_2$. Аналогично доказывается, что $\mu_1 = \mu_2$ и $\nu_1 = \nu_2$.

Докажем, например, что $w = \mu_2 f - \lambda_2 g$. По теореме Гильберта о нулях идеал, порожденный формами f,g и h, содержит некоторую степень любого многочлена, так как эти формы не имеют общих нулей. В частности, x^n при некотором n можно представить в виде

$$x^n = rf + sg + th, \tag{2}$$

где r, s, t — формы степени $n-2$. Рассмотрим равенство (2) с минимальным n. Из (1) и (2) следуют равенства

$$uft + vgt + wht = 0, \quad x^n w = rfw + sgw + thw,$$

поэтому

$$x^n w = (rw - ut)f + (sw - vt)g = af + bg, \tag{3}$$

где a и b — формы степени n. Если $n = 0$, то мы получаем требуемое равенство. Если же $n > 0$, то мы получаем противоречие с минимальностью n. В самом деле, при $x = 0$ равенство (3) превращается в

$$a_0 f_0 + b_0 g_0 = 0,$$

где $a_0 = a(0, y, z)$ и т. д. При этом f_0 и g_0 не имеют общих нулей, а значит, $a_0 = d_0 g_0$ и $b_0 = -d_0 f_0$ для некоторого многочлена $d_0(y, z)$. Положим $d(x, y, z) = d_0(y, z)$ и рассмотрим многочлены $a_1 = a - dg$ и $b_1 = b + df$. Ясно, что

$$a_1 f + b_1 g = af + bg = x^n w$$

и $a_1(0, y, z) = b_1(0, y, z) = 0$, т. е. a_1 и b_1 делятся на x. Сократив на x, получим равенство вида $a_2 f + b_2 g = x^{n-1} w$, что противоречит минимальности n.

Итак, ядро отображения

$$d\Phi\colon (u, v, w) \mapsto 2(uf + vg + wh)$$

состоит из векторов вида

$$(\nu g - \mu h, \lambda h - \nu f, \mu f - \lambda g) = \lambda(0, h, -g) + \mu(-h, 0, f) + \nu(g, -f, 0),$$

поэтому размерность ядра равна 3. □

Лемма 27.3. Пусть $F \in \overline{A} \setminus A$, где $\overline{A}$ — замыкание A. Тогда либо F имеет нетривиальный вещественный нуль, либо над полем $\mathbb{C}$ кривая $F = 0$ имеет по крайней мере две двойные точки.

Доказательство. Ясно, что $F = f^2 + g^2 + h^2$, где f, g и h имеют общий нетривиальный нуль (a, b, c). Если этот нуль не вещественный, то точки (a, b, c) и $(\overline{a}, \overline{b}, \overline{c})$ будут двумя различными двойными точками кривой $F = 0$. В самом деле, эти точки являются нулями функций f, g, h, поэтому они являются двукратными нулями функций f^2, g^2, h^2, а значит, они являются двукратными нулями функции $F = f^2 + g^2 + h^2$. □

Займемся теперь непосредственно доказательством теоремы. Нужно доказать, что любая неотрицательная форма лежит в A. Открытое множество A ограничено поверхностью $\partial A = \overline{A} \setminus A$. Пусть F_1 — произвольная неотрицательная форма степени 4 от 3 переменных. Если $F_1 \in A$, то доказывать уже нечего. Поэтому будем считать, что $F_1 \notin A$. В таком случае отрезок F_0F_1, где $F_0 \in A$ — произвольная точка, должен пересекать ∂A в некоторой точке F_t. Достаточно доказать, что точку F_0 можно выбрать так, что точка F_t совпадет с F_1 (тогда $F_1 = F_t \in \partial A \subset \overline{A}$). Будем считать, что F_t — внутренняя точка отрезка F_0F_1. Точку F_0 можно выбрать так, что F_t имеет нетривиальный вещественный нуль. Дело в том, что согласно лемме 27.3 формы из ∂A, не имеющие нетривиальных вещественных нулей, соответствуют кривым с двумя двойными точками, а такие формы образуют множество коразмерности не менее 2. Действительно, кривая $F = 0$ имеет двойную точку, если система уравнений $F = 0$, $F_x = 0$, $F_y = 0$, $F_z = 0$ имеет решение. Первое уравнение можно не учитывать, так как $xF_x + yF_y + zF_z = nF$, где n — степень формы F (в нашем случае $n = 4$). Кривые $F_x = 0$ и $F_y = 0$ пересекаются в $(n-1)^2$ точках. Кривая $F = 0$ имеет k двойных точек, если кривая $F_z = 0$ проходит через k точек пересечения кривых $F_x = 0$ и $F_y = 0$. Это накладывает k алгебраических соотношений на коэффициенты формы F.

Итак, форма $F_t = (1-t)F_0 + tF_1$ имеет нетривиальный вещественный нуль. Но это противоречит тому, что $F_t \neq F_1$. В самом деле, $F_0 > 0$ и $F_1 \geqslant 0$, поэтому при $t \neq 1$ форма $(1-t)F_0 + tF_1$ принимает строго положительные значения во всех точках, отличных от начала координат. □

28. Теория Артина

Параграф 28 в основном посвящен решению Артина семнадцатой проблемы Гильберта о представимости любого неотрицательного многочлена в виде суммы квадратов рациональных функций. Доказательство Артина не дает никаких оценок достаточного количества этих рациональных функций в представлении многочлена от n переменных. Такую оценку получил Пфистер: неотрицательный многочлен от n переменных можно представить в виде суммы 2^n квадратов рациональных функций. Теорию Пфистера мы обсудим в параграфе 29.

В параграфах 28.1 и 28.2 приведены необходимые сведения из теории вещественных полей; результаты этих параграфов принадлежат Артину и Шрайеру [ArS]. Собственно решение семнадцатой проблемы Гильберта содержится в 28.3. Это доказательство основано на теореме Сильвестра, позволяющей вычислить количество вещественных корней многочлена как индекс некоторой квадратичной формы (см. с. 45). Наше изложение опирается на [Sa].

28.1. Вещественные поля

Поле K называют *упорядоченным*, если оно разбито на три непересекающихся подмножества

$$K = N \cup \{0\} \cup P$$

так, что $N = -P$ (N — *отрицательные* числа, P — *положительные* числа), причем сумма и произведение двух положительных чисел положительны.

Для упорядоченного поля можно ввести обозначение $x - y > 0$, если $x - y \in P$ ($x \geqslant y$, если $x - y \in P$ или $x = y$).

Положим

$$|a| = \begin{cases} a & \text{при } a > 0, \\ 0 & \text{при } a = 0, \\ -a & \text{при } a < 0. \end{cases}$$

Легко проверить, что $|ab| = |a| \cdot |b|$ и $|a + b| \leqslant |a| + |b|$.

В любом упорядоченном поле $1 > 0$, так как обратное неравенство $-1 > 0$ приводит к противоречию: $1 = (-1)(-1) > 0$. В частности, характеристика любого упорядоченного поля равна нулю, поскольку $1 + \ldots + 1 > 0$.

В любом упорядоченном поле $x^2 > 0$. В самом деле, оба неравенства $x > 0$ и $-x > 0$ приводят к одному и тому же неравенству $x^2 > 0$.

Упорядочение поля $\mathbb{Q}$ единственно, а именно, $p/q > 0$ тогда и только тогда, когда $pq > 0$. Действительно, числа p/q и pq получаются друг из друга умножением на $q^{\pm 2} > 0$.

Примером поля, которое нельзя упорядочить, служит любое поле L, в котором элемент -1 является суммой квадратов (и характеристика L не равна 2). В самом деле, любой элемент a поля L является суммой квадратов:

$$a = \left(\frac{1+a}{2}\right)^2 + (-1)\left(\frac{1-a}{2}\right)^2.$$

Поле K называют *формально вещественным*, если элемент -1 нельзя представить в виде суммы квадратов элементов K. Эквивалентное условие: если $b_1^2 + \ldots + b_n^2 = 0$, где $b_1, \ldots, b_k \in K$, то $b_1 = \ldots = b_n = 0$. Для краткости будем называть формально вещественные поля просто *вещественными*.

Любое вещественное поле имеет характеристику 0. В самом деле, если характеристика равна p, то $-1 = \underbrace{1^2 + \ldots + 1^2}_{p-1}$.

Теорема 28.1. Пусть K — вещественное поле, $a \in K$.

а) Если элемент a является суммой квадратов элементов K, то поле $K(\sqrt{a})$ вещественно.

б) Если поле $K(\sqrt{a})$ не вещественно, то элемент $-a$ является суммой квадратов элементов K.

Доказательство. Пусть поле $K(\sqrt{a})$ не вещественно. Тогда, в частности, $K(\sqrt{a}) \neq K$, т. е. $\sqrt{a} \notin K$. Кроме того, элемент -1 является суммой квадратов элементов поля $K(\sqrt{a})$, т. е. в K существуют такие элементы b_i, c_i, что

$$-1 = \sum (b_i + c_i\sqrt{a})^2 = \sum b_i^2 + 2\sqrt{a}\sum b_i c_i + a\sum c_i^2. \qquad (1)$$

Формула (1) показывает, что если $\sum b_i c_i \neq 0$, то $\sqrt{a} \in K$. Поэтому

$$-1 = \sum b_i^2 + a\sum c_i^2. \qquad (2)$$

Пусть a — сумма квадратов элементов K. Формула (2) показывает, что в таком случае предположение (с которого мы начинали доказательство) о том, что поле $K(\sqrt{a})$ не вещественно, приводит к противоречию. Это доказывает утверждение а).

Чтобы доказать утверждение б), запишем формулу (2) в виде

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2}.$$

Остается заметить, что если p и q — суммы квадратов, то $p/q = pq(q^{-1})^2$ тоже сумма квадратов. □

Следствие. Для вещественного поля K одно из полей $K(\sqrt{a})$ и $K(\sqrt{-a})$ обязательно вещественно.

Доказательство. Если поле $K(\sqrt{a})$ не вещественно, то элемент $-a$ является суммой квадратов, поэтому поле $K(\sqrt{-a})$ вещественно. □

Теорема 28.2. Пусть K — вещественное поле и $f \in K[x]$ — неприводимый многочлен нечетной степени. Тогда поле $K(\alpha)$, где α — корень f, вещественно.

Доказательство. Пусть $n = \deg f$. Предположим, что поле $K(\alpha)$ не вещественно. Тогда

$$-1 = \sum g_i(\alpha)^2,$$

где g_i — многочлены степени не выше $n-1$. Многочлен $1 + \sum g_i(x)^2$ имеет корень α, поэтому он делится на f, т. е.

$$-1 = \sum g_i(x)^2 + h(x)f(x),$$

где h — некоторый многочлен. Предположим, что $h = 0$. Тогда $-1 = \sum g_i(x)^2$. Если $\max\limits_i(\deg g_i) = m > 0$, то сумма квадратов коэффициентов многочленов g_i при x^m равна нулю. А если $g_i = c_i \in K$, то $-1 = \sum c_i^2$. Оба варианта противоречат вещественности поля K, поэтому $h \neq 0$.

Степень многочлена $\sum g_i(x)^2$ четна и не превосходит $2n-2$. Поэтому степень многочлена h нечетна и не превосходит $n-2$. У многочлена h есть неприводимый множитель h_1, степень которого нечетна и не превосходит $n-2$. Пусть β — корень многочлена h_1. Тогда $-1 = \sum g_i(\beta)^2$, т. е. элемент -1 является суммой квадратов элементов поля $K(\beta)$. Повторив для многочлена h_1 те же самые рассуждения, что и для многочлена f, получим, что элемент -1 является суммой квадратов элементов поля $K(\gamma)$, где γ — корень некоторого неприводимого многочлена нечетной степени, не превосходящей $n-4$ и т. д. Приходим к противоречию. □

Поле K называют *вещественно замкнутым*, если оно вещественно и любое его вещественное алгебраическое расширение совпадает с K.

Из теоремы 28.2 следует, что в вещественно замкнутом поле любой многочлен нечетной степени имеет корень.

Вещественным замыканием вещественного поля K называют вещественно замкнутое поле R, алгебраическое над K.

У любого вещественного поля K есть вещественное замыкание. В самом деле, рассмотрим частично упорядоченное множество всех вещественных полей, алгебраических над K. Согласно лемме Цорна в этом множестве есть по крайней мере один максимальный элемент R. Ясно, что поле R вещественно замкнуто.

Теорема 28.3. Вещественно замкнутое поле R допускает ровно одно упорядочение, а именно, ненулевой элемент $a \in R$ положителен тогда и только тогда, когда он является квадратом.

Доказательство. Ясно, что равенства $a = t_1^2$ и $-a = t_2^2$, где $t_1, t_2 \in R$, не могут выполняться одновременно, так как иначе $-1 = (t_1/t_2)^2$. Поэтому достаточно доказать, что $\pm a = t^2$, где $t \in R$.

Если $a \neq t^2$, то поле $R(\sqrt{a})$ является собственным расширением поля R, поэтому оно не вещественно. В таком случае согласно теореме 28.1 (б) элемент $-a$ является суммой квадратов элементов R. Тогда согласно теореме 28.1 (а) поле $R(\sqrt{-a})$ вещественно, поэтому оно совпадает с R. Это означает, что $\sqrt{-a} \in R$, т. е. $-a = t^2$, где $t \in R$. □

Теорема 28.4. Пусть K — вещественное поле, причем элемент $a \in K$ нельзя представить в виде суммы квадратов. Тогда существует упорядочение поля K, при котором $a < 0$.

Доказательство. Согласно теореме 28.1 (б) поле $K(\sqrt{-a})$ вещественно. Пусть R — вещественное замыкание поля $K(\sqrt{-a})$. Согласно теореме 28.3 поле R имеет упорядочение, при котором элемент $-a = (\sqrt{-a})^2$ положителен, т. е. элемент a отрицателен. Ограничение этого упорядочения на $K \subset R$ и есть требуемое упорядочение. □

Введем для алгебраического замыкания поля R обозначение $\overline{R}$.

Теорема 28.5. Поле R вещественно замкнуто тогда и только тогда, когда $\overline{R} \neq R$ и $\overline{R} = R(\sqrt{-1})$.

Доказательство. Предположим сначала, что поле R вещественно замкнуто. Тогда уравнение $x^2 + 1 = 0$ не имеет решений в R, поэтому $\overline{R} \neq R$. Докажем, что $\overline{R} = R(\sqrt{-1})$.

Введем для краткости обозначение $i = \sqrt{-1}$. Прежде всего покажем, что в поле $R(i)$ любое квадратное уравнение имеет корень. Корни квадратного трехчлена $x^2 + 2px + q$ находятся по формуле $x_{1,2} = -p \pm \sqrt{p^2 - q}$, поэтому достаточно доказать, что если $a, b \in K$, то $\sqrt{a + ib} \in K(i)$. Иными словами, нужно подобрать $c, d \in K$ так, что $(c + di)^2 = a + bi$, т. е. $c^2 - d^2 = a$ и $2cd = b$. Ясно, что $a^2 + b^2 = (c^2 + d^2)^2$. Поэтому подходящими кандидатами являются

$$c^2 = \frac{\sqrt{a^2 + b^2} + a}{2}, \quad d^2 = \frac{\sqrt{a^2 + b^2} - a}{2}.$$

Прежде всего проверим, что так определенные числа c и d действительно лежат в R. Так как $a^2 \geqslant 0$ и $b^2 \geqslant 0$, то $a^2 + b^2 \geqslant 0$, поэтому согласно теореме 28.3 $\sqrt{a^2+b^2} \in R$. Далее, $\sqrt{a^2+b^2} \geqslant \sqrt{a^2} \geqslant \pm a$ (здесь $\sqrt{a^2+b^2}$ и $\sqrt{a^2}$ — неотрицательные числа). Поэтому $\sqrt{a^2+b^2} \pm a \geqslant 0$, т. е. c и d лежат в R. Равенство $c^2 - d^2 = a$ выполняется автоматически, а равенство $2cd = b$ будет выполняться, если правильно выбрать знаки чисел c и d.

Рассмотрим теперь произвольный многочлен f, неприводимый над R. Запишем его степень n в виде $n = 2^m q$, где q — нечетное число. Докажем индукцией по m, что f имеет корень в $R(i)$. При $m = 0$ это следует из теоремы 28.2. Предположим теперь, что $m > 0$ и требуемое утверждение уже доказано для чисел $1, \ldots, m-1$.

Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена f в некотором расширении поля R. Выберем число $c \in R$ так, чтобы все числа $\alpha_k\alpha_l + c(\alpha_k + \alpha_l)$, где $k \neq l$, были попарно различны. Эти числа являются корнями многочлена g степени $n(n-1)/2$ с коэффициентами из R (коэффициенты лежат в R, так как они являются симметрическими функциями от $\alpha_1, \ldots, \alpha_n$). Число $\deg g = n(n-1)/2$ имеет вид $2^{m-1}q(n-1)$, где $q(n-1)$ — нечетное число. Поэтому к многочлену g можно применить предположение индукции. Без ограничения общности можно считать, что корень $\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)$ многочлена g лежит в $R(i)$.

Докажем, что $R(\alpha_1\alpha_2, \alpha_1 + \alpha_2) = R\big(\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)\big)$. Рассмотрим для этого многочлен F с корнями $\alpha_k\alpha_l$ и многочлен G с корнями $\alpha_k + \alpha_l$; коэффициенты многочленов F и G лежат в R. Пусть $\theta = \alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)$. Ясно, что $G(\alpha_1 + \alpha_2) = 0$ и $F\big(\theta - c(\alpha_1 + \alpha_2)\big) = F(\alpha_1\alpha_2) = 0$, т. е. $\alpha_1 + \alpha_2$ — общий корень многочленов $G(x)$ и $F(\theta - cx)$ с коэффициентами из $R(\theta)$. Из условия $\theta - c(\alpha_k + \alpha_l) \neq \alpha_k\alpha_l$ при $k, l \neq 1, 2$ следует, что $\alpha_1 + \alpha_2$ — единственный общий корень этих многочленов. Кроме того, этот общий корень некратный, так как он является некратным корнем многочлена G. Следовательно, наибольший общий делитель многочленов $G(x)$ и $F(\theta - cx)$ имеет вид $x - (\alpha_1 + \alpha_2)$. Коэффициенты этих многочленов лежат в $R(\theta)$, поэтому $\alpha_1 + \alpha_2 \in R(\theta)$ и

$$\alpha_1\alpha_2 = \theta - c(\alpha_1 + \alpha_2) \in R(\theta) = R\big(\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)\big).$$

Обратное включение $R(\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)) \subset R(\alpha_1\alpha_2, \alpha_1 + \alpha_2)$ очевидно.

Итак, $\alpha_1\alpha_2$, $\alpha_1 + \alpha_2 \in R\big(\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)\big) \subset R(i)$. Поэтому α_1 и α_2 — корни многочлена (степени 2) с коэффициентами из $R(i)$. Но мы уже доказали, что корни любого квадратного многочлена с коэффициентами

из $R(i)$ лежат в $R(i)$. Таким образом, у многочлена f есть корень α_1, лежащий в $R(i)$. Это означает, что $\overline{R} = R(i)$.

Обратное утверждение (если $\overline{R} \neq R$ и $\overline{R} = R(i)$, то поле R вещественно замкнуто) доказывается существенно проще. Между R и $\overline{R} = R(i)$ нет промежуточных полей, поэтому достаточно доказать, что поле R вещественно, т. е. -1 не является суммой квадратов элементов R. По условию $i \notin R$, т. е. -1 не является квадратом. Таким образом, достаточно доказать, что в R сумма квадратов сама является квадратом. Поле $R(i)$ алгебраически замкнуто, поэтому если $a, b \in R$, то $\sqrt{a+bi} \in R(i)$, т. е. в R существуют такие элементы c и d, что $a + bi = (c + di)^2$. В таком случае $a - bi = (c - di)^2$. Поэтому

$$a^2 + b^2 = (a + bi)(a - bi) = (c + di)^2(c - di)^2 = (c^2 + d^2)^2.$$

Остается заметить, что если сумма двух квадратов является квадратом, то и сумма любого числа квадратов тоже будет квадратом. □

28.2. Теорема Сильвестра для вещественно замкнутых полей

Пусть K — упорядоченное поле, f — неприводимый многочлен над K. Будем называть вещественно замкнутое поле $R \supset K$ *вещественным замыканием* поля K, если R алгебраично над K и упорядочение K, индуцированное упорядочением R, совпадает с исходным упорядочением K.

Количество различных вещественных корней вещественного многочлена можно вычислить, не выходя за пределы поля $\mathbb{R}$. Это можно сделать двумя способами: с помощью теоремы Штурма и с помощью теоремы Сильвестра. Обе эти теоремы можно доказать и для упорядоченных полей. Важнейший вывод из этого таков: если f — многочлен над упорядоченным полем K, то в любом вещественном замыкании R поля K число корней многочлена f одно и то же. Первоначально теория Артина опиралась на теорему Штурма; более современное построение теории Артина на основе теоремы Штурма приведено в книге [Л1]. Но теорема Сильвестра во многих отношения более удобна. Мы, следуя [Sa], приведем решение 17-й проблемы Гильберта на основе теоремы Сильвестра.

Сигнатура квадратичной формы φ над упорядоченным полем K определяется следующим образом. Над полем K квадратичную форму φ можно привести к виду

$$\varphi(x) = \lambda_1 x_1^2 + \ldots + \lambda_n x_n^2. \tag{1}$$

Как и в случае поля $\mathbb{R}$, количество положительных λ_i и отрицательных не зависит от того, как именно мы приводим форму φ к виду (1). Действительно, предположим, что есть два разложения $V_+ \oplus V_- \oplus V_0 = W_+ \oplus W_- \oplus W_0$. Тогда $V_+ \cap (W_- \oplus W_0) = 0$, поэтому $\dim V_+ + \dim W_- + \dim W_0 \leqslant 0$, а значит, $\dim V_+ \leqslant \dim W_+$. Аналогично, $\dim W_+ \leqslant \dim V_+$.

Пусть R — вещественное замыкание поля K. Из теоремы 28.5 следует, что степень неприводимого над полем R многочлена равна 1 или 2. Поэтому очевидная модификация рассуждений, использованных при доказательстве теоремы 4.5 (см. с. 45), позволяет доказать следующее утверждение.

Теорема 28.6. Пусть f — многочлен над полем K и $\varphi(x, y)$ — билинейная симметрическая форма на пространстве $K[x]/(f)$, равная следу оператора умножения на xy. Тогда сигнатура формы φ равна количеству различных корней многочлена f, лежащих в вещественном замыкании R поля K.

В частности, как мы уже говорили, количество различных корней многочлена f для всех вещественных замыканий поля K одно и то же.

Форму φ мы будем называть *формой следа* на пространстве $K[x]/(f)$.

Теорема 28.7 (Артин–Шрайер). Пусть K — упорядоченное поле и R, R' — его вещественные замыкания. Тогда существует ровно один изоморфизм $\sigma\colon R \to R'$ над K, причем этот изоморфизм сохраняет порядок.

Доказательство. В вещественно замкнутом поле условие $x > y$ эквивалентно тому, что $x - y$ является квадратом. Поэтому любой изоморфизм $\sigma\colon R \to R'$ сохраняет порядок.

Поле R алгебраично над K, поэтому любой элемент $\alpha \in R$ является корнем неприводимого многочлена f над K. Из теоремы 28.6 следует, что в R и R' многочлен f имеет одинаковое число корней. Пусть этими корнями будут $\alpha_1 < \ldots < \alpha_n$ и $\alpha'_1 < \ldots < \alpha'_n$ соответственно. Выберем в R элементы t_i так, что $t_i^2 = \alpha_{i+1} - \alpha_i$. Согласно теореме о примитивном элементе

$$K(\alpha_1, \ldots, \alpha_n, t_1, \ldots, t_{n-1}) = K(\theta),$$

где $\theta \in R$ — корень некоторого неприводимого над K многочлена g. В поле R' многочлен g имеет столько же корней, сколько в поле R. В част-

ности, у него есть некоторый корень $\theta' \in R'$. Над K существует изоморфизм $K(\theta) \to K(\theta')$. Он представляет собой вложение

$$\sigma\colon K(\alpha_1, \ldots, \alpha_n, t_1, \ldots, t_{n-1}) \to R.$$

Легко проверить, что $\sigma(\alpha_i) = \alpha_i'$. В самом деле, σ переводит корень многочлена f в корень многочлена f, причем $\sigma(\alpha_{i+1}) - \sigma(\alpha_i) = \sigma(t_i^2) > 0$. На $K(\alpha_1, \ldots, \alpha_n)$ отображение σ определено однозначно. В частности, однозначно определен образ элемента α. Теперь с помощью леммы Цорна можно построить однозначно определенный изоморфизм R на R' над K. □

Докажем теперь, что у любого упорядоченного поля есть вещественное замыкание.

Теорема 28.8. Пусть K — упорядоченное поле, K' — его расширение, в котором нет соотношений вида $-1 = \sum \lambda_i a_i^2$, где λ_i — положительные элементы K и $a_i \in K'$. Тогда поле L, полученное из K' присоединением квадратных корней из всех положительных элементов K, вещественно.

Доказательство. Предположим, что поле L не вещественно. Тогда $-1 = \sum b_i^2$, где $b_i \in L$. Поэтому в L есть соотношение вида $-1 = \sum \lambda_i b_i^2$, где λ_i — положительные элементы K и $b_i \in L$. По условию все b_i не могут одновременно лежать в K'. Поэтому определено наименьшее натуральное число r, для которого выполняется некоторое соотношение указанного вида с $b_i \in K'(\sqrt{\mu_1}, \ldots, \sqrt{\mu_r})$, где $\mu_1, \ldots, \mu_r$ — положительные элементы K.

Запишем b_i в виде $b_i = x_i + y_i\sqrt{\mu_r}$, где $x_i, y_i \in K'(\sqrt{\mu_1}, \ldots, \sqrt{\mu_{r-1}})$. Тогда

$$-1 = \sum \lambda_i (x_i + y_i\sqrt{\mu_r})^2 = \sum \lambda_i (x_i^2 + y_i^2\sqrt{\mu_r}) + 2\sqrt{\mu_r} \sum x_i y_i.$$

Если $\sum x_i y_i \neq 0$, то $\sqrt{\mu_r} \in K'(\sqrt{\mu_1}, \ldots, \sqrt{\mu_{r-1}})$, что противоречит минимальности r. Поэтому

$$-1 = \sum \lambda_i x_i^2 + \sum \lambda_i \mu_r y_i^2,$$

где λ_i и $\lambda_i\mu_r$ — положительные элементы K и $x_i, y_i \in K'(\sqrt{\mu_1}, \ldots, \sqrt{\mu_{r-1}})$. Это тоже противоречит минимальности r. □

Следствие 1. У любого упорядоченного поля K есть вещественное замыкание.

Доказательство. Положим $K' = K$. В K нет соотношений вида $-1 = \sum \lambda_i a_i^2$ с положительными λ_i. Поэтому поле L, полученное из K присоединением квадратных корней из всех положительных элементов K, вещественно. Вещественное замыкание поля L и есть требуемое вещественное замыкание поля K. □

Следствие 2. Пусть K — упорядоченное поле и K' — его расширение. Упорядочение поля K можно продолжить на K' тогда и только тогда, когда в K' нет соотношений вида $-1 = \sum \lambda_i a_i^2$, где λ_i — положительные элементы K и $a_i \in K'$.

Доказательство. Ясно, что если соотношения указанного вида есть, то упорядочение нельзя продолжить на K'. Предположим, что таких соотношений нет. Тогда можно построить вещественное поле $L \supset K'$. Рассмотрим его вещественное замыкание R. Упорядочение R индуцирует требуемое упорядочение K'. □

28.3. Семнадцатая проблема Гильберта

Здесь мы наконец докажем, что если вещественная рациональная функция $r(x_1, \ldots, x_n)$ неотрицательна для всех вещественных $x_1, \ldots, x_n$, то ее можно представить в виде суммы квадратов вещественных рациональных функций. Это доказательство годится не только для поля $\mathbb{R}$, но и для произвольного вещественно замкнутого поля R. Требуемое доказательство легко получить из следующей достаточно трудной теоремы.

Теорема 28.9 (Артин–Ленг). Пусть R — вещественно замкнутое поле и $K = R(x_1, \ldots, x_n)$ — упорядоченное конечно порожденное расширение поля R, причем упорядочение поля K согласовано с упорядочением поля R. Тогда существует гомоморфизм R-алгебр

$$\varphi\colon R[x_1, \ldots, x_n] \to R,$$

тождественный на R.

Доказательство. Рассмотрим сначала случай, когда степень трансцендентности K над R равна 1. Можно считать, что элемент $x_1 = x$ трансцендентен над R. Тогда поле K является конечным алгебраическим расширением поля R, поэтому согласно теореме о примитивном

элементе $K = R(x)[y]$. Точно такие же рассуждения, как при доказательстве леммы Нётер о нормализации (см. с. 250), показывают, что элемент y можно выбрать так, чтобы он удовлетворял уравнению $y^l + c_1(x)y^{l-1} + \ldots + c_l(x) = 0$, где $c_1(x), \ldots, c_l(x) \in \mathbb{R}[x]$. При этом будем считать, что степень l минимальна.

Рассмотрим многочлен $f(X, Y) = Y^l + c_1(X)Y^{l-1} + \ldots + c_l(X)$ от независимых переменных X и Y. Любой паре элементов $a, b \in R$, удовлетворяющих соотношению $f(a, b) = 0$, соответствует гомоморфизм R-алгебр $\sigma\colon R[x, y] \to R$, заданный формулами $\sigma(x) = a$ и $\sigma(y) = b$. Покажем, что таких пар $a, b \in R$ бесконечно много.

Пусть R_K — вещественное замыкание поля K. Многочлен $\widetilde{f}(Y) = f(x, Y) \in R(x)[Y]$ имеет в поле R_K корень y, поэтому согласно теореме 28.6 сигнатура формы следа φ на пространстве

$$R(x)[Y]/(\widetilde{f}) \cong R(x)[y]/R(x) = K/R(x)$$

положительна. Эту форму можно привести к диагональному виду с элементами $h_1(x), \ldots, h_s(x) \in R[x]$ на диагонали.

Над вещественно замкнутым полем R любой многочлен раскладывается на линейные и неприводимые квадратичные множители. При этом квадратичные множители имеют вид $(x + \alpha)^2 + \beta^2$, где $\alpha, \beta \in R$. Поэтому они положительны как элементы $R(x)$, и при всех $a \in R$ элементы $(a + \alpha)^2 + \beta^2 \in R$ тоже положительны.

Пусть $x - \lambda_1, \ldots, x - \lambda_t$ — все различные линейные множители, входящие в разложения многочленов $h_1(x), \ldots, h_s(x)$. Упорядочим элементы $x, \lambda_1, \ldots, \lambda_t \in R(x)$; при этом возможны следующие варианты:

$$\ldots < \lambda_i < x < \lambda_j < \ldots; \qquad \ldots < \lambda_i < x; \qquad x < \lambda_j < \ldots$$

Пусть a — любой элемент поля R, удовлетворяющий, соответственно, неравенствам $\lambda_i < a < \lambda_j$; $\lambda_i < a$; $a < \lambda_j$ (таких элементов a бесконечно много). Тогда знаки элементов $h_k(a)$ и $h_k(x)$ совпадают при всех $k = 1, \ldots, s$. Поэтому сигнатура формы φ равна сигнатуре формы с диагональными элементами $h_1(a), \ldots, h_s(a)$.

Покажем, что для почти всех a форма следа φ_a на пространстве $R[Y]/\big(f(a, Y)\big)$ приводится к диагональному виду с элементами $h_1(a), \ldots, h_s(a)$ на диагонали. Действительно, пусть $A(x) = \big(a_{ij}(x)\big)$ — матрица формы φ в базисе $1, Y, \ldots, Y^{l-1}$, а $B(x) = \big(b_{ij}(x)\big)$ — матрица, для которой

$$\big(B(x)\big)^T A(x)B(x) = \operatorname{diag}\big(h_1(x), \ldots, h_s(x)\big).$$

Тогда если $\det B(a) \neq 0$ и ни один из знаменателей рациональных функций $b_{ij}(x)$ не обращается в нуль при $x = a$, то

$$\big(B(a)\big)^T A(a)B(a) = \operatorname{diag}\big(h_1(a), \ldots, h_s(a)\big).$$

Остается заметить, что $A(a)$ — матрица формы φ_a в базисе $1, Y, \ldots$ $\ldots, Y^{l-1}$.

Итак, существует бесконечно много элементов $a \in R$, для которых сигнатура формы φ_a положительна. Для всех таких a многочлен $f(a, Y)$ имеет корень $b \in R$, т. е. $f(a, b) = 0$. Как мы уже говорили, любой такой паре (a, b) соответствует гомоморфизм R-алгебр $\sigma\colon R[x, y] \to R$. Покажем, что почти все такие гомоморфизмы можно продолжать на $R[x, y, x_2, \ldots, x_n] \supset R[x, y]$. Напомним, что $x_2, \ldots, x_n \in R[x_1, \ldots, x_n] =$ $= K = R(x)[y]$, поэтому $x_i = p_i(x, y)/q_i(x)$, где p_i и q_i — многочлены. Пусть $q = q_1 \cdot \ldots \cdot q_n$. По построению $\sigma\big(q(x)\big) = q(a) \neq 0$ для почти всех a. В таких случаях гомоморфизм σ можно продолжить на

$$R[x, y]\left[\frac{1}{q(x)}\right] \supset R[x, y, x_2, \ldots, x_n] \supset R[x_1, \ldots, x_n] = K.$$

Переход от случая, когда степень трансцендентности K над R равна 1, к случаю степени трансцендентности $m \geqslant 1$ делается простой индукцией по m. Предположим, что существование требуемого гомоморфизма доказано для всех полей K, степень трансцендентности которых над R строго меньше m. Рассмотрим поле $K = R(x_1, \ldots, x_n)$, степень трансцендентности которого над R равна m. Выберем промежуточное поле F: $R \subset F \subset K$, для которого степень трансцендентности K над F равна 1. Пусть $R_F \subset R_K$ — вещественные замыкания F и K. Степень трансцендентности R_K над R_F равна 1, поэтому существует гомоморфизм R_F-алгебр $\psi\colon R_F[x_1, \ldots, x_n] \to R_F$.

Степень трансцендентности R_F над R равна $m-1$, поэтому степень трансцендентности поля $R\big(\psi(x_1), \ldots, \psi(x_n)\big) \subset R_F$ над R не превосходит $m - 1$. Ясно также, что на поле $R\big(\psi(x_1), \ldots, \psi(x_n)\big)$ можно задать упорядочение, индуцированное упорядочением поля R_F. Поэтому существует гомоморфизм R-алгебр $\sigma\colon R\big[\psi(x_1), \ldots, \psi(x_n)\big] \to R$. Ограничение композиции отображений ψ и σ на алгебру

$$R[x_1, \ldots, x_n] \subset R_F[x_1, \ldots, x_n]$$

и есть требуемый гомоморфизм. □

Теперь уже легко доказать теорему Артина о неотрицательных рациональных функциях. Пусть k — упорядоченное поле. Рациональную функцию

$$r(x_1,\dots,x_n)=\frac{p(x_1,\dots,x_n)}{q(x_1,\dots,x_n)},\quad \text{где}\quad p,q\in k[x_1,\dots,x_n],$$

называют *неотрицательной*, если $r(a_1,\dots,a_n)\geqslant 0$ при всех $a_1,\dots,a_n\in k$, для которых $q(a_1,\dots,a_n)\neq 0$.

Теорема 28.10 (Артин). Пусть R — вещественно замкнутое поле, $r\in R(x_1,\dots,x_n)$ — неотрицательная рациональная функция. Тогда r можно представить в виде суммы квадратов элементов $R(x_1,\dots,x_n)$.

Доказательство. Предположим, что r не является суммой квадратов элементов поля $R(x_1,\dots,x_n)$. Тогда согласно теореме 28.4 существует упорядочение поля $R(x_1,\dots,x_n)$, для которого $r<0$. Представим r в виде несократимой дроби p/q, где $p,q\in R[x_1,\dots,x_n]$. Рассмотрим содержащую r R-алгебру

$$R\left[x_1,\dots,x_n,\frac{1}{q(x_1,\dots,x_n)}\right].$$

В вещественном замыкании упорядоченного поля $R(x_1,\dots,x_n)$ есть такой элемент γ, что $\gamma^2=-r>0$. Поле $R(x_1,\dots,x_n,\gamma)$ содержится в вещественном замыкании $R(x_1,\dots,x_n)$, а значит, в этом поле можно ввести упорядочение, индуцированное упорядочением вещественного замыкания. По теореме Артина–Ленга существует гомоморфизм

$$\varphi\colon R\left[x_1,\dots,x_n,\frac{1}{q(x_1,\dots,x_n)}\gamma,\frac{1}{\gamma}\right]\to R,$$

тождественный на R.

Ясно, что $\varphi(\gamma)\,\varphi\left(\dfrac{1}{\gamma}\right)=1$ и $\varphi(q)\,\varphi\left(\dfrac{1}{q}\right)=1$, поэтому $\varphi(\gamma)\neq 0$ и $\varphi(q)\neq$ $\neq 0$. Следовательно, $\varphi(r)=-\varphi(\gamma^2)=-\big(\varphi(\gamma)\big)^2<0$. Но

$$\varphi(r)=\frac{p(a_1,\dots,a_n)}{q(a_1,\dots,a_n)},\quad \text{где}\quad a_i=\varphi(x_i).$$

При этом $q(a_1,\dots,a_n)=\varphi(q)\neq 0$. Неравенство $r(a_1,\dots,a_n)<0$ противоречит условию теоремы. □

Для произвольного (т. е. не обязательно вещественно замкнутого) упорядоченного поля теорема Артина неверна (первый пример такого поля приведен в [Dub]; более простой пример можно найти на с. 86 книги [Pf2]). Но, слегка дополнив доказательство теоремы 28.10, для произвольного упорядоченного поля k можно доказать следующее утверждение.

Теорема 28.11. Пусть k — упорядоченное поле и R — его вещественное замыкание. Если рациональная функция $r \in k(x_1, \ldots, x_n)$ такова, что $r(a_1, \ldots, a_n) \geqslant 0$ при всех $a_1, \ldots, a_n \in R$ (если, конечно, значение $r(a_1, \ldots, a_n)$ при этом определено), то r можно представить в виде суммы квадратов элементов $k(x_1, \ldots, x_n)$.

Доказательство. Если r не является суммой квадратов элементов $k(x_1, \ldots, x_n)$, то существует упорядочение поля $k(x_1, \ldots, x_n)$, для которого $r < 0$. Пусть R' — вещественное замыкание поля $k(x_1, \ldots, x_n)$ с таким упорядочением. Можно считать, что $R \subset R'$ (вещественное замыкание поля $k(x_1, \ldots, x_n)$ содержит некоторое вещественное замыкание R_1 поля k, а R_1 и R изоморфны как вещественные замыкания одного и того же поля). В поле R' есть такой элемент γ, что $\gamma^2 = -r > 0$. Введем на R-алгебре

$$R\left[x_1, \ldots, x_n, \frac{1}{q(x_1, \ldots, x_n)}\gamma, \frac{1}{\gamma}\right] \subset R'$$

упорядочение, индуцированное упорядочением R'. Дальнейшие рассуждения в точности те же самые, что и при доказательстве теоремы 28.10. □

Следствие. Если упорядоченное поле k таково, что из условия $r(x_1, \ldots, x_n) < 0$ при всех $x_1, \ldots, x_n \in k$ следует, что $r(x_1, \ldots, x_n) < 0$ при всех $x_1, \ldots, x_n \in R$, где R — вещественное замыкание k, то для поля k верна теорема Артина.

В частности, теорема Артина верна для поля рациональных чисел $\mathbb{Q}$, т. е. любая неотрицательная рациональная функция с рациональными коэффициентами является суммой квадратов рациональных функций с рациональными коэффициентами.

В заключение приведем формулировки двух интересных теорем, доказательства которых опираются на теорему Артина. Точнее говоря, первая из этих теорем выводится из теоремы Артина, а вторая — из первой.

Теорема 28.12 [Ri]. Пусть I — идеал в кольце $\mathbb{R}[x_1, \ldots, x_n]$. Тогда следующие условия эквивалентны:

(1) любой многочлен, обращающийся в нуль во всех общих вещественных нулях многочленов из идеала I, сам лежит в I;

(2) если сумма квадратов многочленов из кольца $\mathbb{R}[x_1, \ldots, x_n]$ лежит в I, то и сами эти многочлены лежат в I.

Теорема 28.13 [St]. Однородная форма F неотрицательна тогда и только тогда, когда существует однородное полиномиальное соотношение вида $\varphi(-F) = 0$, где

$$\varphi(u) = u^{2n+1} + a_1 u^{2n} + \ldots + a_{2n}$$

и коэффициенты $a_1, \ldots, a_{2n}$ являются суммами квадратов однородных форм.

29. Теория Пфистера

29.1. Мультипликативные квадратичные формы

В этом параграфе мы будем рассматривать квадратичные формы над произвольным полем k, характеристика которого не равна 2. Квадратичная форма φ на пространстве k^n задается симметрической матрицей A порядка n. При этом если $x = (x_1, \ldots x_n) \in k^n$, то

$$\varphi(x) = xAx^T = \sum x_i x_j a_{ij}.$$

Квадратичные формы φ и ψ называют *эквивалентными*, если существует такая невырожденная матрица P порядка n, что $\varphi(x) = \psi(Px)$. В таком случае ψ задается матрицей PAP^T. Для эквивалентных форм будем использовать обозначение $\varphi \cong \psi$.

Будем говорить, что форма φ *представляет* элемент $a \in k$, если $a = \varphi(x)$ для некоторого $x \in k^n$. Например, форма $\varphi(x) = x_1^2 + \ldots + x_n^2$ представляет элемент a тогда и только тогда, когда a можно представить в виде суммы n квадратов.

Основным инструментом теории Пфистера служат введенные им мультипликативные формы специального вида. Квадратичную форму φ называют *мультипликативной*, если формы φ и $a\varphi$ эквивалентны для любого ненулевого элемента a, представимого формой φ.

Любая мультипликативная форма φ обладает следующим замечательным свойством: если элементы a и b представимы формой φ, то элемент ab тоже представим формой φ. Дело в том, что эквивалентные формы представляют одно и то же множество элементов поля k. А если мультипликативная форма φ представляет элементы a и b, то форма $a\varphi$ эквивалентна ей и представляет элемент ab.

Введем следующие обозначения. Форму $\varphi(x) = a_1x_1^2+\ldots+a_nx_n^2$ будем обозначать $\langle a_1,\ldots,a_n\rangle$. Для форм $\varphi = \langle a_1,\ldots,a_m\rangle$ и $\psi = \langle b_1,\ldots,b_n\rangle$ положим

$$\varphi\oplus\psi = \langle a_1,\ldots,a_m,b_1,\ldots,b_n\rangle,$$
$$\varphi\otimes\psi = \langle a_1b_1,\ldots,a_mb_1,a_1b_2,\ldots,a_mb_2,\ldots,a_1b_n,\ldots,a_mb_n\rangle.$$

Формы вида $\langle 1,a_1\rangle\otimes\langle 1,a_2\rangle\otimes\ldots\otimes\langle 1,a_n\rangle$, где $a_1\ldots a_n\neq 0$, введенные Пфистером, играют главную роль в его теории. Будем для краткости обозначать такие формы $\langle\langle a_1,\ldots,a_n\rangle\rangle$. Наибольший интерес для нас представляет форма $\langle\langle\underbrace{1,\ldots,1}_{n}\rangle\rangle$, т. е. сумма 2^n квадратов. Но при доказательствах индукцией по n не удается избежать рассмотрения общего случая $\langle\langle a_1,\ldots,a_n\rangle\rangle$.

Теорема 29.1 (Пфистер). Форма $\langle\langle a_1,\ldots,a_n\rangle\rangle$ мультипликативна.

Доказательство. Рассмотрим сначала случай $n=1$. Пусть форма $\langle\langle a_1\rangle\rangle = x_1^2+a_1x_2^2$ представляет элемент $b\neq 0$, т. е. $b = c_1^2+a_1c_2^2$. Положим $A = \begin{pmatrix} 1 & 0\\ 0 & a_1\end{pmatrix}$ и $P = \begin{pmatrix} c_1 & c_2\\ -a_1c_2 & c_1\end{pmatrix}$. Легко проверить, что $PAP^T = bA$ и $\det P\neq 0$. Это означает, что $\langle\langle a_1\rangle\rangle\cong b\langle\langle a_1\rangle\rangle$.

Форма $\langle\langle a_1,\ldots,a_n\rangle\rangle$ имеет вид $\varphi\oplus a_n\varphi$, где $\varphi = \langle\langle a_1,\ldots,a_{n-1}\rangle\rangle$. Поэтому достаточно доказать, что если форма φ мультипликативна и $a\neq\neq 0$, то форма $\varphi\oplus a\varphi$ тоже мультипликативна. Пусть $b = \varphi(x)+a\varphi(y) = \xi+a\eta\neq 0$, где элементы ξ и η представимы формой φ. Если $\xi = 0$, то $\eta\neq 0$, поэтому $\eta\varphi\cong\varphi$, а значит,

$$b(\varphi\oplus a\varphi) = a\eta(\varphi\oplus a\varphi)\cong a\varphi\oplus a^2\varphi\cong\varphi\oplus a\varphi,$$

так как $a^2\varphi\cong\varphi$. Случай $\eta = 0$ рассматривается аналогично. Остается рассмотреть случай $\xi\eta\neq 0$. В этом случае $\varphi\cong\xi\varphi$ и $\varphi\cong\xi^{-1}\varphi\cong(\eta\xi^{-1})\varphi$. Следовательно,

$$b(\varphi\oplus a\varphi) = (\xi+a\eta)(\varphi\oplus a\varphi)\cong(1+a\eta\xi^{-1})(\varphi\oplus(a\eta\xi^{-1})\varphi)\cong$$
$$\cong(1+a\eta\xi^{-1})\langle\langle a\eta\xi^{-1}\rangle\rangle\otimes\varphi.$$

При разборе случая $n = 1$ было показано, что форма $\langle\langle a\eta\xi^{-1}\rangle\rangle$ мультипликативна. Эта форма представляет элемент $1 + a\eta\xi^{-1} = b\xi^{-1} \neq 0$. Следовательно, $(1 + a\eta\xi^{-1})\langle\langle a\eta\xi^{-1}\rangle\rangle \cong \langle\langle a\eta\xi^{-1}\rangle\rangle$, а значит,

$$b(\varphi \oplus a\varphi) \cong \langle\langle a\eta\xi^{-1}\rangle\rangle \otimes \varphi = \varphi \oplus (a\eta\xi^{-1})\varphi \cong \varphi \oplus a\varphi,$$

что и требовалось доказать. □

При доказательстве теоремы Пфистера мы не пользовались тем, что $\operatorname{char} k \neq 2$, поэтому она верна для любого поля. Особенно интересен случай $a_1 = \ldots = a_n = 1$. В этом случае из теоремы Пфистера следует, что в любом поле произведение элементов, представимых в виде суммы 2^n квадратов, тоже представимо в виде суммы 2^n квадратов. При $n = 1, 2, 3$ для такого представления есть явные формулы общего вида. Например, при $n = 1$, т. е. для суммы двух квадратов, требуемое тождество имеет вид $(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2(x_1y_2 - x_2y_1)^2$. Но при $n > 3$ тождеств такого вида уже быть не может.

Нам потребуется следующее вспомогательное утверждение.

Лемма 29.1. Запишем форму $\varphi = \langle\langle a_1, \ldots, a_n\rangle\rangle$, где $a_1 \ldots a_n \neq 0$, в виде $\varphi = \langle 1\rangle \oplus \varphi'$. Пусть форма φ' представляет элемент $b_1 \neq 0$. Тогда $\varphi \cong \langle\langle b_1, \ldots, b_n\rangle\rangle$ для некоторых ненулевых $b_2, \ldots, b_n$.

Доказательство. Применим индукцию по n. При $n = 1$ форма φ' имеет вид $a_1x_1^2$. Если $b_1 = a_1c^2$, то $b_1x_1^2 = a_1(cx_1)^2 \cong a_1x_1^2$. Таким образом, $\langle a_1\rangle \cong \langle b_1\rangle$, а значит, $\langle\langle a_1\rangle\rangle \cong \langle\langle b_1\rangle\rangle$.

Предположим теперь, что требуемое утверждение доказано для всех форм вида $\langle\langle c_1, \ldots, c_{n-1}\rangle\rangle$, где $c_1 \ldots c_{n-1} \neq 0$. Чтобы доказать требуемое утверждение для формы $\varphi = \langle\langle a_1, \ldots, a_n\rangle\rangle$, рассмотрим форму $\psi = \langle\langle a_1, \ldots, a_{n-1}\rangle\rangle = \langle 1\rangle \oplus \psi'$. Ясно, что $\varphi = \psi \oplus a_n\psi$ и $\varphi' = \psi' \oplus a_n\psi$. Поэтому элемент b_1, представимый формой φ', можно записать в виде $b_1 = b_1' + a_nb$, где элементы b_1' и b представляются формами ψ' и ψ, соответственно.

Пусть сначала $b = 0$. В таком случае $b_1' = b_1$. Согласно предположению индукции $\psi \cong \langle\langle b_1, \ldots, b_{n-1}\rangle\rangle$, а значит, $\varphi \cong \langle\langle b_1, \ldots, b_{n-1}, a_n\rangle\rangle$.

Рассмотрим теперь случай $b \neq 0$. В этом случае форма ψ представляет ненулевой элемент b. Согласно теореме Пфистера форма ψ мультипликативна, поэтому $\psi \cong b\psi$. Следовательно, $\varphi' = \psi' \oplus (a_nb)(b^{-1}\psi) \cong \psi' \oplus c_n\psi$, где $c_n = a_nb$. При этом $b_1 = b_1' + c_n$. Пусть $b_1' = 0$. Тогда $b_1 = c_n$ и $\varphi \cong \langle\langle c_n\rangle\rangle \otimes \psi = \langle\langle c_n, a_1, \ldots, a_{n-1}\rangle\rangle = \langle\langle b_1, a_1, \ldots, a_{n-1}\rangle\rangle$.

Остается рассмотреть случай, когда $b_1 = b_1' + c_n$, причем $b_1' c_n \neq 0$. Форма ψ' представляет элемент b_1', поэтому согласно предположению индукции $\psi \cong \langle\langle b_1', b_2, \ldots, b_{n-1}\rangle\rangle$. Следовательно,

$$\begin{aligned}\varphi &\cong \langle\langle b_1', b_2, \ldots, b_{n-1}, c_n\rangle\rangle \cong \langle\langle b_1', c_n, b_2, \ldots, b_{n-1}\rangle\rangle \cong \\ &\cong \langle\langle b_1', c_n\rangle\rangle \otimes \langle\langle b_2, \ldots, b_{n-1}\rangle\rangle.\end{aligned}$$

Пусть $\lambda = b_1'$ и $\mu = c_n$. Тогда $\lambda + \mu = b_1 \neq 0$. Равенство

$$\begin{pmatrix} 1 & 1 \\ \mu & -\lambda \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \begin{pmatrix} 1 & \mu \\ 1 & -\lambda \end{pmatrix} = \begin{pmatrix} \lambda+\mu & 0 \\ 0 & (\lambda+\mu)\lambda\mu \end{pmatrix}$$

показывает, что $\langle b_1', c_n\rangle \cong \langle b_1, b_1 b_1' c_n\rangle$. Поэтому

$$\langle\langle b_1', c_n\rangle\rangle = \langle 1,\ b_1',\ c_n,\ b_1' c_n\rangle \cong \langle 1,\ b_1,\ b_1' c_n,\ b_1 b_1' c_n\rangle = \langle\langle b_1, b_1' c_n\rangle\rangle.$$

Положим $b_n = b_1' c_n$. Тогда

$$\varphi \cong \langle\langle b_1, b_n\rangle\rangle \otimes \langle\langle b_2, \ldots, b_n\rangle\rangle \cong \langle\langle b_1, \ldots, b_n\rangle\rangle. \qquad \square$$

29.2. C_i-поля

В предыдущем параграфе мы познакомились с одним из инструментов теории Пфистера — мультипликативными формами. Другой инструмент этой теории, C_i-поля, был создан в 1933–1936 гг. китайским математиком Чунжцзе Дзеном и в 1952 г. переоткрыт Ленгом.

Поле K называют *C_i-полем*, если любая система однородных многочленов

$$f_1, \ldots, f_r \in K[x_1, \ldots, x_n],$$

для которых $d_1^i + \ldots + d_r^i < n$, где $d_s = \deg f_s$, имеет общий нетривиальный нуль.

Теорема 29.2 (Дзен–Ленг). Если поле L алгебраически замкнуто, то поле $K = L(t_1, \ldots, t_i)$ (т. е. поле рациональных функций от i переменных над полем L) является C_i-полем.

Доказательство. Применим индукцию по i. При $i = 0$ поле K совпадает с L, т. е. поле K алгебраически замкнуто, а условие $d_1^i + \ldots + d_r^i < n$ означает, что $r < n$. В таком случае требуемое утверждение совпадает с однородной теоремой Гильберта о нулях (теорема 25.10 на с. 261).

Шаг индукции заключается в том, чтобы доказать, что если поле L является C_i-полем, то поле $K = L(t)$ является C_{i+1}-полем. Пусть $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ — однородные многочлены, причем $d_1^{i+1} + \ldots + d_r^{i+1} < n$, где $d_s = \deg f_s$. Требуется доказать, что многочлены $f_1, \ldots, f_r$ имеют общий нетривиальный нуль в K. Коэффициенты многочленов $f_1, \ldots, f_r$ лежат в $K = L(t)$, т. е. они являются рациональными функциями над полем L от переменной t. Умножив все эти коэффициенты на подходящий многочлен из кольца $L[t]$, можно будет считать, что коэффициенты многочленов $f_1, \ldots, f_r$ лежат в $L[t]$, т. е. эти коэффициенты являются многочленами от t над полем L. Степени этих многочленов ограничены некоторым числом m, поэтому любой коэффициент α можно представить в виде

$$\alpha = a_0 + a_1 t + \ldots + a_m t^m, \quad \text{где} \quad a_0, \ldots, a_m \in L. \tag{1}$$

При $p = 1, \ldots, n$ положим

$$x_p = x_{p0} + x_{p1} t + \ldots + x_{ps} t^s, \tag{2}$$

где $x_{p0}, \ldots, x_{ps}$ — независимые переменные над полем L, а число s достаточно велико (это число мы определим чуть позже). Заменим в каждой однородной форме $f_1, \ldots, f_r$ коэффициенты и переменные выражениями (1) и (2), соответственно. В результате форма f_j запишется в виде

$$g_0 + g_1 t + \ldots + g_N t^N,$$

где $N = sd_j + m$ и $g_0, \ldots, g_N$ — формы степени d_j от $(s+1)n$ переменных x_{pq} над полем L. Согласно предположению индукции все формы g для многочленов $f_1, \ldots, f_r$ имеют общий нетривиальный нуль, если выполняется неравенство

$$\sum_{j=1}^{r} (sd_j + m + 1) d_j^i < (s+1)n,$$

т. е.

$$(m+1) \sum d_j^i - n < s(n - \sum d_j^{i+1}).$$

По условию $n - \sum d_j^{i+1} > 0$, поэтому требуемое неравенство выполняется при достаточно больших s, например, при $s > (m+1) \sum d_j^i$. $\square$

29.3. Теорема Пфистера о суммах квадратов рациональных функций

В двух предыдущих параграфах мы приготовили основные инструменты для доказательства теоремы Пфистера. Нам понадобится еще следующее свойство квадратичных форм: если невырожденная квадратичная форма φ над полем K изотропна (т. е. $\varphi(u) = 0$ для некоторого $u \neq 0$), то она универсальна (т. е. представляет все элементы поля K). В самом деле, невырожденной квадратичной форме φ соответствует невырожденная билинейная симметрическая форма

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

Поэтому найдется такой вектор v, что $f(u, v) = 1$. В таком случае

$$\varphi(v + \lambda u) = \varphi(v) + \varphi(\lambda u) + 2f(v, \lambda u) = \varphi(v) + 2\lambda.$$

Для любого $b \in K$ можно выбрать такое λ, что $\varphi(v) + 2\lambda = b$.

Из теоремы 29.2 следует, что если поле L алгебраически замкнуто, то любая невырожденная квадратичная форма φ от 2^n переменных над полем $K = L(t_1, \ldots, t_n)$ универсальна. В самом деле, пусть $r \in K$. Рассмотрим вспомогательную квадратичную форму $\widetilde{\varphi}(u, t) = \varphi(u) - rt^2$ от $2^n + 1$ переменных. Согласно теореме 29.2 форма $\widetilde{\varphi}$ имеет нетривиальный нуль (u_0, t_0). Если $t_0 = 0$, то $\varphi(u_0) = 0$, причем $u_0 \neq 0$. Это означает, что форма φ изотропна, а потому универсальна. Если же $t_0 \neq 0$, то $\varphi(t_0^{-1} u_0) = r$, т. е. форма φ представляет r.

Теорема 29.3 (Пфистер). Пусть R — вещественно замкнутое поле и $\varphi = \langle\langle a_1, \ldots, a_n \rangle\rangle$ — невырожденная квадратичная форма от 2^n переменных над полем $R(x_1, \ldots, x_n)$. Тогда если b — сумма квадратов элементов $R(x_1, \ldots, x_n)$, то форма φ представляет b.

Доказательство. Если форма φ изотропна, то она универсальна. Поэтому можно считать, что форма φ анизотропна, т. е. $\varphi(u) \neq 0$ при $u \neq 0$. По условию $b = b_1^2 + \ldots + b_m^2$. Применим индукцию по m. При $m = 1$ утверждение очевидно, так как любая мультипликативная форма представляет элемент 1, а значит, она представляет и элемент $b_1^2 \cdot 1$.

Пусть теперь $m = 2$, т. е. $b = b_1^2 + b_2^2$, причем $b_1 b_2 \neq 0$. Пусть $L = R(i)$ — алгебраическое замыкание поля R. Элемент $\beta = b_1 + ib_2$ поро-

ждает поле $L(x_1,\dots,x_n)$ над полем $R(x_1,\dots,x_n)$, т. е.

$$L(x_1,\dots,x_n)=R(x_1,\dots,x_n)(\beta).$$

Поле R вещественное, поэтому $i\notin R(x_1,\dots,x_n)$ и $\beta\notin R(x_1,\dots,x_n)$.

Форму φ можно рассматривать и как форму над полем $L(x_1,\dots,x_n)\supset$ $\supset R(x_1,\dots,x_n)$. Над этим полем она универсальна, так как поле L алгебраически замкнуто. Поэтому найдутся такие 2^n-мерные векторы u,v с коэффициентами из $R(x_1,\dots,x_n)$, для которых $\varphi(u+\beta v)=\beta$, т. е.

$$\varphi(u)+2\beta f(u,v)+\beta^2\varphi(v)=\beta, \tag{1}$$

где f — билинейная симметрическая форма, соответствующая φ. При этом $v\neq 0$, так как иначе $\beta=\varphi(u)\in R(x_1,\dots,x_n)$. Из анизотропности формы φ следует, что $\varphi(v)\neq 0$.

Неприводимое над $R(x_1,\dots,x_n)$ уравнение для β имеет вид $(\beta-b_1)^2+$ $+b_2^2=0$, т. е.

$$\beta^2-2b_1\beta+b=0. \tag{2}$$

Сравнивая (1) и (2), получаем, в частности, $b=\varphi(u)/\varphi(v)$. Из мультипликативности формы φ следует, что она представляет как элемент $1/\varphi(v)$, так и произведение элементов $\varphi(u)$ и $1/\varphi(v)$, т. е. элемент b.

Предположим теперь, что требуемое утверждение доказано для некоторого $m\geqslant 2$, т. е. любая форма φ вида $\varphi=\langle\langle a_1,\dots,a_n\rangle\rangle$ представляет любой элемент вида $b_1^2+\dots+b_m^2$. Нужно доказать, что форма φ представляет любой элемент вида $b_1^2+\dots+b_m^2+b_{m+1}^2$, где $b_{m+1}\neq 0$. Запишем этот элемент в виде $b_{m+1}^2(b+1)$, где b — сумма m квадратов. Достаточно доказать, что форма φ представляет элемент $c=b+1$. Можно считать, что $c\neq 0$.

Чтобы воспользоваться леммой 29.1 (см. с. 305), запишем форму φ в виде $\varphi=\langle 1\rangle\oplus\varphi'$. Согласно предположению индукции форма φ представляет элемент b, т. е. $b=b_0^2+b'$, где элемент b' представляется формой φ'. Рассмотрим мультипликативную форму $\psi=\varphi\otimes\langle 1,-c\rangle$ от 2^{n+1} переменных. Ясно, что

$$\psi=\langle 1\rangle\oplus\varphi'\oplus(-c)\varphi=\langle 1\rangle\oplus\psi',$$

где форма $\psi'=\varphi'\oplus(-c\varphi)$ представляет элемент

$$b'-c=(b-b_0^2)-(1+b)=-1-b_0^2.$$

При этом $-1-b_0^2\neq 0$, так как $i\notin R(x_1,\dots,x_n)$. В таком случае можно применить лемму 29.1 к форме ψ и элементу $-1-b_0^2$. В результате по-

лучим, что в поле $R(x_1,\dots,x_n)$ существуют такие ненулевые элементы $c_1,\dots,c_n$, что

$$\psi \cong \langle\langle -1-b_0^2, c_1,\dots,c_n\rangle\rangle,$$

т. е. $\psi \cong \langle -1-b_0^2\rangle \otimes \chi = \chi \oplus (-1-b_0^2)\chi$, где $\chi \cong \langle\langle c_1,\dots,c_n\rangle\rangle$.

Применим снова предположение индукции, на этот раз к форме χ. Элемент $1+b_0^2$ является суммой не более чем m квадратов, поэтому форма χ его представляет. В таком случае из мультипликативности формы χ следует, что $\chi \cong (1+b_0^2)\chi$, а значит,

$$\varphi \oplus (-c\varphi) = \psi \cong \chi \oplus (-1-b_0^2)\chi \cong (1+b_0^2)\chi \oplus (-1-b_0^2)\chi.$$

Пусть $\xi = (1+b_0^2)\chi$. Тогда

$$\varphi(Px+Qy) - c\varphi(Rx+Sy) = \xi(x) - \xi(y),$$

где $\begin{pmatrix} P & Q \\ R & S \end{pmatrix} = U$ — невырожденная матрица порядка 2^n. Положив $x = y$, получим $\varphi(Ax) = c\varphi(Bx)$, где $A = P+Q$ и $B = R+S$. Из невырожденности матрицы U следует, что если $x \neq 0$, то $(Ax, Bx) \neq (0,0)$. Если бы одна из матриц A и B оказалась вырожденной, то форма φ была бы изотропной, а мы рассматриваем случай анизотропной формы. Если же обе матрицы невырожденные, то $\varphi \cong c\varphi$, а значит, мультипликативная форма φ представляет элемент c. □

Согласно теореме Артина любой неотрицательный элемент поля $R(x_1,\dots,x_n)$, где R — вещественно замкнутое поле, является суммой квадратов. Поэтому мультипликативная форма $\langle\langle \underbrace{1,\dots,1}_{n}\rangle\rangle$ представляет любой неотрицательный элемент поля $R(x_1,\dots,x_n)$, т. е. любой неотрицательный элемент этого поля можно представить в виде суммы 2^n квадратов.

На с. 280 приведен пример элемента поля $\mathbb{R}(x_1,\dots,x_n)$, который нельзя представить в виде суммы n квадратов. Таким образом, если N — наименьшее число, для которого любой элемент поля $\mathbb{R}(x_1,\dots,x_n)$ можно представить в виде суммы N квадратов, то $n+1 \leqslant N \leqslant 2^n$. В общем случае для N никаких других оценок не известно. Лишь при $n=2$ известно, что $N=4$. Это утверждение доказано двумя разными способами, но оба доказательства весьма сложные. Одно доказательство использует теорию эллиптических кривых над полем $\mathbb{C}(x)$ (см. [CEP] и [Chr]). Другое доказательство опирается на теорему Нётера–Лефшеца о том, что на поверхности общего положения степени $d \geqslant 4$ в трехмерном

проективном пространстве любая кривая высекается некоторой другой поверхностью (см. [Co]).

При доказательстве теоремы Пфистера существенно используется то, что поле R вещественно замкнуто. Для поля $\mathbb{Q}$ теорема Пфистера неверна. Это видно уже при $n = 0$. Действительно, не любое положительное рациональное число является квадратом рационального числа. Но при $n = 0$ требуемая оценка известна: любое положительное рациональное число является суммой квадратов четырех рациональных чисел. В самом деле, согласно теореме Мейера (см. [БШ], [K2] или [C]) любая невырожденная квадратичная форма над полем $\mathbb{Q}$ от $n \geqslant 5$ переменных (нетривиально) представляет нуль, если она представляет нуль над полем $\mathbb{R}$. В частности, если $r > 0$, то форма $x_1^2 + x_2^2 + x_3^2 + x_4^2 - rx_5^2$ представляет нуль над $\mathbb{Q}$.

При $n = 1$, т. е. для многочленов над $\mathbb{Q}$ от одной переменной, первым получил оценку Э. Ландау в 1906 г. в работе [L]. Он показал, что любой неотрицательный многочлен (от одной переменной) с рациональными коэффициентами можно представить в виде суммы 8 квадратов многочленов с рациональными коэффициентами (простое доказательство теоремы Ландау приведено в главе 7 книги [Pf2]). Но эта оценка не точная. Точную оценку получил Пурше [Pu]: любой неотрицательный многочлен над $\mathbb{Q}$ можно представить в виде суммы квадратов 5 многочленов над $\mathbb{Q}$ (подробному изложению теоремы Пурше посвящена глава 17 книги [Raj]).

Для многочленов, обладающих некоторыми специальными свойствами, можно получить и более точные результаты. Например, в [DLS] показано, что если значения многочлена $f(x)$ при всех целых x являются суммами квадратов двух целых чисел, то многочлен $f(x)$ является суммой квадратов двух многочленов с целыми коэффициентами.

Пример неотрицательного многочлена, который над $\mathbb{Q}$ нельзя представить в виде суммы квадратов четырех многочленов, строится достаточно просто. Дело в том, что если

$$ax^2 + bx + c = \sum_{i=1}^{4} (a_i x + b_i)^2,$$

то $4ac - b^2$ — сумма квадратов трех рациональных чисел. Действительно,

$$4ac - b^2 = 4\left(\sum a_i^2\right)\left(\sum b_i^2\right) - 4\left(\sum a_i b_i\right)^2,$$

а если рассмотреть произведение кватернионов $a_1 + a_2 i + a_3 j + a_4 k$ и $b_1 - b_2 i - b_2 j - b_2 k$, то можно убедиться, что

$$\left(\sum a_i^2\right)\left(\sum b_i^2\right) = \left(\sum a_i b_i\right)^2 + \text{сумма трех квадратов.}$$

Теперь легко показать, что квадратный трехчлен $x^2 + x + 4$ нельзя представить в виде суммы квадратов четырех многочленов. Для этого нужно доказать, что 15 нельзя представить в виде суммы квадратов трех рациональных чисел. Если бы 15 равнялось $p^2 + q^2 + r^2$, то после приведения к общему знаменателю мы получили бы сравнение

$$a^2 + b^2 + c^2 \equiv 15d^2 \pmod 8 \equiv -d^2 \pmod 8,$$

где хотя бы одно из чисел a, b, c, d нечетно. Такое сравнение невозможно.

Дополнение

30. Алгоритм Ленстры–Ленстры–Ловаса

В 1982 г. в работе [LLL] был предложен алгоритм (*LLL-алгоритм*, или *алгоритм Ленстры–Ленстры–Ловаса*), позволяющий разложить многочлен над $\mathbb{Z}$ на неприводимые множители за полиномиальное время. Точнее говоря, если $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ и $|f| = \left(\sum_{i=0}^{n} a_i^2\right)^{1/2}$, то для разложения многочлена f на неприводимые множители по этому алгоритму потребуется не более $O\bigl(n^{12} + n^9(\ln|f|)^3\bigr)$ операций.

LLL-алгоритм имеет большой теоретический интерес, но с практической точки зрения он не более эффективен, чем сравнительно простой алгоритм, описанный в разделе 10.2. Вначале оба алгоритма работают одинаково: многочлен f разлагается на неприводимые множители по модулю простого числа p с помощью алгоритма Берлекэмпа, а затем с помощью леммы Гензеля с некоторой точностью вычисляется p-адический неприводимый множитель h многочлена f. Но после этого LLL-алгоритм действует по-другому: для h ищется неприводимый делитель h_0 многочлена f в кольце $\mathbb{Z}[x]$, делящийся на h по модулю p. При этом условие делимости h_0 на h означает, что коэффициенты многочлена h_0 являются координатами точек некоторой решетки, а условие делимости f на h_0 означает, что коэффициенты многочлена h_0 не слишком велики. Для вычисления многочлена h_0 используется алгоритм построения приведенного базиса решетки. Следует отметить, что последний алгоритм имеет также многочисленные применения, не относящиеся к факторизации многочленов.

30.1. Общее описание алгоритма

Перейдем непосредственно к описанию алгоритма факторизации. Будем считать, что многочлены f и f' взаимно просты и $\operatorname{cont}(f) = 1$. Начнем с того, что вычислим результант $R(f, f') \in \mathbb{Z}$. Пусть p — наименьшее простое число, не делящее $R(f, f')$. Тогда степень многочлена $f \pmod p$ равна n и многочлены $f \pmod p$ и $f' \pmod p$ взаимно просты. Чтобы доказать это, достаточно заметить, что $R(f, f') = \pm a_n D(f)$ (а потому a_n не делится на p) и $R(f, f') = \varphi f + \psi f'$, где $\varphi, \psi \in \mathbb{Z}[x]$.

У многочлена $f \pmod p$ нет кратных делителей, поэтому его можно разложить на неприводимые множители по алгоритму Берлекэмпа.

Пусть $h \pmod p$ — один из неприводимых множителей многочлена $f \pmod p$. В дальнейшем мы будем считать, что $h \in \mathbb{Z}[x]$, старший коэффициент многочлена h равен 1 и коэффициенты многочлена h приведены по модулю p, т. е. заключены между 0 и $p-1$.

Рассмотрим разложение многочлена f на неприводимые множители над $\mathbb{Z}$ и перейдем от этого разложения к разложению по модулю p. У многочлена $f \pmod p$ нет кратных неприводимых множителей, поэтому многочлен $h \pmod p$ соответствует ровно одному неприводимому делителю h_0 многочлена f над $\mathbb{Z}$. Таким образом, существует ровно один неприводимый делитель h_0 многочлена f над $\mathbb{Z}$, для которого $h_0 \pmod p$ делится на $h \pmod p$.

Если известен алгоритм, позволяющий по многочлену h вычислять многочлен h_0, то факторизация многочлена f производится просто. Действительно, пусть над $\mathbb{Z}$ задано разложение $f = f_1 f_2$, где для многочлена f_1 известно полное разложение над $\mathbb{Z}$, а для многочлена f_2 известно полное разложение по модулю p (на первом шаге $f_1 = 1$ и $f_2 = f$). Возьмем неприводимый делитель $h \pmod p$ многочлена $f_2 \pmod p$ и вычислим неприводимый делитель h_0 многочлена f_2 над $\mathbb{Z}$, для которого $h_0 \pmod p$ делится на $h \pmod p$. Заменим f_1 на $f_1 h_0$, а f_2 на f_2/h_0. После этого повторяем операцию до тех пор, пока не получим полное разложение многочлена f.

Алгоритм, который для данного многочлена $h \pmod p$ вычисляет многочлен h_0, мы опишем чуть ниже, в разделе 30.3. Этот алгоритм использует алгоритм вычисления приведенного базиса решетки. Поэтому мы сначала обсудим понятие приведенного базиса решетки и алгоритм вычисления приведенного базиса (этот алгоритм также был предложен в работе [LLL]; его тоже часто называют LLL-алгоритмом).

30.2. Приведенный базис решетки

Подмножество $L \subset \mathbb{R}^n$ называют *решеткой ранга* n, если в $\mathbb{R}^n$ существует такой базис $b_1, \ldots, b_n$, что

$$L = \sum_{i=1}^{n} \mathbb{Z} \cdot b_i = \left\{ \sum_{i=1}^{n} r_i b_i \mid r_i \in \mathbb{Z} \right\}.$$

Определителем решетки L называют число

$$d(L) = \left|\det(b_1, \ldots, b_n)\right|,$$

где под b_i подразумевается столбец координат вектора b_i. Определитель

решетки равен объему параллелепипеда, натянутого на векторы $b_1, \ldots, b_n$. Базис решетки не единствен, но определитель матрицы перехода от одного базиса решетки к другому равен ± 1, поэтому число $d(L)$ не зависит от выбора базиса.

Пусть $b_1, \ldots, b_n$ — базис решетки L. При ортогонализации Грама–Шмидта получаем ортогональный (не обязательно ортонормированный) базис

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*, \quad \text{где} \quad \mu_{ij} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)},\ 1 \leqslant j < i \leqslant n.$$

Определение. Базис $b_1, \ldots, b_n$ решетки L называют *приведенным*, если $|\mu_{ij}| \leqslant \frac{1}{2}$ при $1 \leqslant j < i \leqslant n$ и $|b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \geqslant \frac{3}{4} |b_{i-1}^*|^2$ при $1 < i \leqslant n$.

Теорема 30.1 (неравенство Адамара). $d(L) \leqslant \prod\limits_{i=1}^{n} |b_i|$, т. е. объем параллелепипеда не превосходит произведения длин его ребер.

Доказательство. Векторы b_i^* попарно ортогональны, поэтому

$$|b_i|^2 = |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |b_j^*|^2 \leqslant |b_i^*|^2.$$

Кроме того, $d(L) = \prod\limits_{i=1}^{n} |b_i^*|$. □

В следующей теореме собраны основные неравенства для векторов приведенного базиса.

Теорема 30.2. Пусть $b_1, \ldots, b_n$ — приведенный базис решетки L. Тогда:

а) $d(L) \leqslant \prod\limits_{i=1}^{n} |b_i| \leqslant 2^{n(n-1)/4} d(L)$.

б) $|b_j| \leqslant 2^{(i-1)/2} |b_i^*|$ при $1 \leqslant j \leqslant i \leqslant n$.

в) $|b_1| \leqslant 2^{(n-1)/4} d(L)^{1/n}$.

г) Если $x \in L$, $x \neq 0$, то $|b_1| \leqslant 2^{(n-1)/2} |x|$.

д) Если векторы $x_1, \ldots, x_t \in L$ линейно независимы, то $|b_j| \leqslant 2^{(n-1)/2} \max\{|x_1|, \ldots, |x_t|\}$ при $1 \leqslant j \leqslant t$.

Доказательство. а) Из определения приведенного базиса следует, что

$$|b_i^*|^2 \geqslant \left(\frac{3}{4} - \mu_{i,i-1}^2\right)|b_{i-1}^*|^2 \geqslant \frac{1}{2}|b_{i-1}^*|^2,$$

поскольку $|\mu_{i,i-1}| \leqslant 1/2$.

Простая индукция показывает, что $|b_j^*|^2 \leqslant 2^{i-j}|b_i^*|^2$ при $i \geqslant j$. Поэтому

$$|b_i|^2 = |b_i^*|^2 + \sum_{j=1}^{i-1} \mu_{ij}^2 |b_j^*|^2 \leqslant |b_i^*|^2 \left(1 + \frac{1+2+\ldots+2^{i-2}}{2}\right) = |b_i^*|^2 \left(\frac{1+2^{i-1}}{2}\right).$$

Следовательно,

$$\prod_{i=1}^{n} |b_i|^2 \leqslant \frac{1+1}{2} \cdot \frac{1+2}{2} \cdot \ldots \cdot \frac{1+2^{n-1}}{2} \prod_{i=1}^{n} |b_i^*|^2 \leqslant 1 \cdot 2 \cdot \ldots \cdot 2^{n-1} d(L)^2 = 2^{n(n-1)} d(L)^2.$$

б) Из неравенств $|b_j^*|^2 \leqslant 2^{i-j}|b_i^*|^2$ при $i \geqslant j$ и $|b_j|^2 \leqslant \frac{1+2^{j-1}}{2}|b_j^*|^2 \leqslant$ $\leqslant 2^{j-1}|b_j^*|^2$ получаем $|b_j|^2 \leqslant 2^{i-j} \cdot 2^{j-1}|b_j^*|^2 = 2^{i-1}|b_i^*|^2$ при $i \geqslant j$.

в) Согласно б) имеем неравенства $|b_1|^2 \leqslant |b_1^*|^2$, $|b_1|^2 \leqslant 2|b_2^*|^2, \ldots$ $\ldots, |b_1|^2 \leqslant 2^{n-1}|b_n^*|^2$. Перемножив их, получим

$$|b_1|^{2n} \leqslant 2^{n(n-1)/2} \prod_{i=1}^{n} |b_i^*|^2 = 2^{(n-1)/2} d(L)^2.$$

г) Запишем x в виде $x = \sum_{i=1}^{n} r_i b_i = \sum_{i=1}^{n} s_i b_i^*$, где $r_i \in \mathbb{Z}$, $s_i \in \mathbb{R}$. Пусть i — наибольший индекс, для которого $r_i \neq 0$. Тогда $r_i = s_i$. Поэтому

$$|x|^2 \geqslant s_i^2 |b_i^*|^2 = r_i^2 |b_i^*|^2 \geqslant |b_i^*|^2 \geqslant 2^{1-i}|b_1|^2 \geqslant 2^{1-n}|b_1|^2.$$

д) Векторы $x_1, \ldots, x_t$ не могут все лежать в подпространстве, порожденном векторами $b_1, \ldots, b_{t-1}$, поэтому для некоторого вектора x_s выполняется неравенство $|x_s| \geqslant |b_i^*|^2$, где $i \geqslant t$ (см. доказательство г). Следовательно, при $j \leqslant i$ получаем

$$|x_s|^2 \geqslant |b_i^*|^2 \geqslant 2^{j-i}|b_j^*|^2 \geqslant 2^{j-i} \cdot 2^{1-j}|b_j|^2 = 2^{1-i}|b_j|^2 \geqslant 2^{1-n}|b_j|^2. \quad \square$$

Опишем теперь алгоритм вычисления приведенного базиса решетки L. Предположим, что векторы $b_1, \ldots, b_{k-1}$ образуют приведенный базис порождаемой ими решетки (мы начинаем с одного вектора, т. е. с $k = 2$). Добавим к ним вектор b_k, принадлежащий решетке L, но не

лежащий в пространстве, порожденном векторами $b_1, \ldots, b_{k-1}$. Построение базиса решетки, порожденной векторами $b_1, \ldots, b_k$ выполняется следующим образом.

Шаг 1 (выполнение условия $|\mu_{kj}| \leqslant 1/2$). Напомним, что $\mu_{ij} = \frac{(b_i, b_j^*)}{(b_j^*, b_j^*)}$. Предположим, что $|\mu_{kj}| \leqslant 1/2$ при $l < j < k$ (мы начинаем с $l = k$). Заменим b_k на $b_k - qb_l$, где q — ближайшее к μ_{kl} целое число. Это преобразование сохраняет μ_{kj} при $j > l$ (так как $b_j^* \perp b_l$ при $l < j$) и заменяет μ_{kl} на $\mu_{kl} - q$ (так как $(b_l, b_l^*) = (b_l^*, b_l^*)$). Ясно, что $|\mu_{kl} - q| \leqslant 1/2$, поэтому после такой модификации условие $|\mu_{kj}| \leqslant 1/2$ будет выполняться при $l - 1 < j < k$. Затем повторяем эту операцию.

Шаг 2 (выполнение условия $|b_k^*|^2 \geqslant (3/4 - \mu_{k,k-1}^2)|b_{k-1}^*|^2$). Предположим, что $|b_k^*|^2 < (3/4 - \mu_{k,k-1}^2)|b_{k-1}^*|^2$. В таком случае заменим упорядоченный набор $(b_1, \ldots, b_{k-2}, b_{k-1}, b_k)$ на упорядоченный набор $(b_1, \ldots, b_{k-2}, b_k, b_{k-1})$. При этом b_{k-1}^* заменится на $b_k^* + \mu_{k,k-1} b_{k-1}^*$, поэтому $|b_{k-1}^*|^2$ заменится на

$$|b_k^*|^2 + \mu_{k,k-1}^2 |b_{k-1}^*|^2 < \left(\frac{3}{4} - \mu_{k,k-1}^2\right) |b_{k-1}^*|^2 + \mu_{k,k-1}^2 |b_{k-1}^*|^2 = \frac{3}{4} |b_{k-1}^*|^2.$$

Рассматриваем приведенный базис $b_1, \ldots, b_{k-2}$ и применяем для него первый шаг алгоритма. Из того, что $|b_{k-1}^*|^2$ уменьшается, можно вывести сходимость алгоритма (строгое доказательство сходимости алгоритма можно найти в [LLL] и в [Coh]).

30.3. Решетки и факторизация многочленов

Напомним, что нам осталось построить алгоритм, который позволяет для неприводимого делителя $h \pmod p$ многочлена $f \pmod p$ без кратных делителей вычислить неприводимый делитель h_0 многочлена f, для которого $h_0 \pmod p$ делится на $h \pmod p$. При этом можно считать, что h — многочлен со старшим коэффициентом 1.

Для промежуточных вычислений нам потребуется рассматривать делимость по модулю p^k. Поэтому рассмотрим более общий случай: будем считать, что $h \pmod{p^k}$ — неприводимый делитель многочлена $f \pmod{p^k}$ без кратных делителей, старший коэффициент многочлена h равен 1 и h_0 — неприводимый делитель многочлена f, для которого $h_0 \pmod p$ делится на $h \pmod p$. Легко проверить, что в таком случае

$h_0 \pmod{p^k}$ делится на $h \pmod{p^k}$. Действительно, многочлен $f/h_0 \pmod p$ не делится на неприводимый многочлен $h \pmod p$, т. е. эти многочлены взаимно просты. Следовательно, $\lambda h + \mu f/h_0 = 1 - p\nu$ для некоторых $\lambda, \mu, \nu \in \mathbb{Z}[x]$. Умножим обе части этого равенства на $(1+p\nu+\ldots+p^{k-1}\nu^{k-1})h_0$. В результате получим $\lambda_1 h+\mu_1 f \equiv h_0 \pmod{p^k}$. Но $f \pmod{p^k}$ делится на $h \pmod{p^k}$, поэтому $h_0 \pmod{p^k}$ делится на $h \pmod{p^k}$.

Пусть $n = \deg f$ и $l = \deg h$. Фиксируем целое число $m \geqslant l$ и рассмотрим множество всех многочленов с целыми коэффициентами степени не выше m, которые по модулю p^k делятся на h. Как мы только что показали, многочлен h_0 входит в это множество, если $\deg h_0 \leqslant m$.

Сопоставим многочлену $g(x) = a_0 + \ldots + a_m x^m$ точку $(a_0, \ldots, a_m) \in \in \mathbb{R}^{m+1}$. При таком сопоставлении рассматриваемые многочлены образуют некоторую решетку L. Ясно также, что норма $|g| = \left(\sum a_i^2\right)^{1/2}$ является просто евклидовой длиной в $\mathbb{R}^{m+1}$.

Базис решетки L состоит из многочленов $p^k x^i$, $0 \leqslant i < l$, и многочленов $h(x)x^j$, $0 \leqslant j \leqslant m - l$. Координаты этих векторов относительно базиса $1, x, \ldots, x^m$ образуют матрицу вида $\begin{pmatrix} p^k I_l & * \\ 0 & I' \end{pmatrix}$, где I_l — единичная матрица порядка l, а I' — верхняя треугольная матрица с единицами на диагонали. Поэтому $d(L) = p^{kl}$.

Прежде чем перейти к описанию алгоритма вычисления многочлена h_0, докажем две теоремы, дающие нужные для этих целей оценки.

Теорема 30.3. Если многочлен $b \in L$ таков, что $|b|^n \cdot |f|^m < p^{kl}$, то b делится на h_0. (В частности, $(f, b) \neq 1$, где (f, b) — наибольший общий делитель многочленов f и b.)

Доказательство. Можно считать, что $b \neq 0$. Положим $g = (f, b)$. Мы хотим доказать, что g делится на h_0. Для этого достаточно доказать, что $g \pmod p$ делится на $h \pmod p$. В самом деле, если $g \pmod p$ делится на $h \pmod p$ и $f/g \in \mathbb{Z}[x]$, то f/g не делится на h_0, поскольку $h \pmod p$ — однократный делитель многочлена $f \pmod p$. Следовательно, g делится на h_0.

Предположим, что многочлен $g \pmod p$ не делится на $h \pmod p$. Многочлен $h \pmod p$ неприводим, поэтому многочлены $g \pmod p$ и $h \pmod p$ взаимно просты, т. е. существуют такие многочлены $\lambda_1, \mu_1, \nu_1 \in \mathbb{Z}[x]$, что

$$\lambda_1 h + \mu_1 g = 1 - p\nu_1. \tag{1}$$

Пусть $e = \deg g$ и $m' = \deg b$. Ясно, что $0 \leqslant e \leqslant m' \leqslant m$. Положим

$$M = \{\lambda f + \mu b \mid \lambda, \mu \in \mathbb{Z}[x], \deg\lambda < m' - e, \deg\mu < n - e\} \subset$$
$$\subset \mathbb{Z} + \mathbb{Z}\cdot x + \ldots + \mathbb{Z}\cdot x^{n+m'-e-1}.$$

Обозначим через M' образ M при естественной проекции на $\mathbb{Z}\cdot x^e + \ldots$ $\ldots + \mathbb{Z}\cdot x^{n+m'-e-1}$. Прежде всего покажем, что если элемент $\lambda f + \mu b \in M$ проецируется в $0 \in M'$, то $\lambda = \mu = 0$. Действительно, в таком случае $\deg(\lambda f + \mu b) < e$, но $\lambda f + \mu b$ делится на g, а $\deg g = e$. Поэтому $\lambda f + \mu b = 0$, т. е. $\lambda(f/g) = -\mu(b/g)$. Многочлены f/g и b/g взаимно просты, поэтому μ делится на f/g. Но $\deg\mu < n - e = \deg(f/g)$. Следовательно, $\mu = 0$, а значит, $\lambda = 0$.

Таким образом, проекции множеств $\{x^i f \mid 0 \leqslant i < m' - e\}$ и $\{x^j b \mid 0 \leqslant j < n - e\}$ на M', с одной стороны, линейно независимы, а с другой стороны, они порождают M'. Это означает, что проекции этих двух множеств образуют базис решетки M'. В частности, ранг решетки M' равен $n + m' - 2e$. Кроме того, согласно неравенству Адамара $d(M') \leqslant |f|^{m'-e}|b|^{n-e}$. По условию $|f|^m|b|^n < p^{kl}$. Учитывая что $m' \leqslant m$, получаем

$$d(M') \leqslant |f|^m|b|^n < p^{kl}. \tag{2}$$

Покажем, что если $\nu \in M$ и $\deg\nu < e + l$, то $p^{-k}\nu \in \mathbb{Z}[x]$. В самом деле, многочлен $\nu = \lambda f + \mu b$ делится на $g = (f, b)$, поэтому, умножив равенство (1) на $(1 + p\nu_1 + \ldots + p^{k-1}\nu_1^{k-1})\nu/g$, получим

$$\lambda_2 h + \mu_2 h \equiv \nu/g \pmod{p^k}. \tag{3}$$

Мы рассматриваем ситуацию, когда многочлен $f \pmod{p^k}$ делится на $h \pmod{p^k}$. Кроме того, $b \in L$, поэтому $b \pmod{p^k}$ делится на $h \pmod{p^k}$. Из того, что $\nu \in M$, следует, что $\nu = \lambda f + \mu b$, поэтому $\nu \pmod{p^k}$ делится на $h \pmod{p^k}$. В таком случае из (3) следует, что $\nu/g \pmod{p^k}$ тоже делится на $h \pmod{p^k}$. Но $\deg(\nu/g \pmod{p^k}) < e + l - e = l$, а $h \pmod{p^k}$ — многочлен степени l со старшим коэффициентом 1. Поэтому $\nu/g \equiv 0 \pmod{p^k}$, а значит, $\nu \equiv 0 \pmod{p^k}$.

В M' можно выбрать такой базис $b_e, b_{e+1}, \ldots, b_{n+m'-e-1}$, что $\deg b_j = j$. Легко проверить, что $e+l-1 \leqslant n+m'-e-1$. В самом деле, многочлен b делится на g, поэтому $e = \deg g \leqslant \deg b = m'$, а многочлен $f/g \pmod{p}$ делится на $h \pmod{p}$, поэтому $l = \deg h \leqslant \deg f - \deg g = n - e$. Элементы $b_e, \ldots, b_{e+l-1} \in M'$ получаются из многочленов, которые лежат в M и делятся на p^k, посредством проекции, уничтожающей члены степени

ниже e. Поэтому все коэффициенты многочленов $b_e, \dots, b_{e+l-1}$ (в том числе и их старшие коэффициенты) делятся на p^k.

Ясно, что дискриминант $d(M')$ равен модулю произведения старших коэффициентов многочленов $b_e, \dots, b_{n+m'-e-1}$, поэтому он не меньше произведения модулей старших коэффициентов многочленов $b_e, \dots, b_{e+l-1}$. Следовательно, $d(M') \geqslant p^{kl}$. Это противоречит неравенству (2). □

В следующей теореме мы, как и ранее, предполагаем, что h — многочлен со старшим коэффициентом 1, причем многочлен $f \pmod{p^k}$ делится на $h \pmod{p^k}$; L — решетка, состоящая из многочленов степени не выше m, которые по модулю p^k делятся на h; $l = \deg h$ и $n = \deg f$; h_0 — неприводимый делитель многочлена f, для которого $h_0 \pmod{p}$ делится на $h \pmod{p}$, т. е. $h_0 \pmod{p^k}$ делится на $h \pmod{p^k}$.

Теорема 30.4. Пусть $b_1, b_2, \dots, b_{m+1}$ — приведенный базис решетки L. Предположим, что

$$p^{kl} > 2^{mn/2} \binom{2m}{m}^{n/2} |f|^{m+n}.$$

а) В таком случае $\deg h_0 \leqslant m$ тогда и только тогда, когда

$$|b_1| < \left(p^{kl}/|f|^m\right)^{1/n}.$$

б) Предположим, что для некоторого базисного вектора b_j выполняется неравенство

$$|b_j| < \left(p^{kl}/|f|^m\right)^{1/n}. \qquad (*)$$

Пусть t — наибольший из всех таких индексов j. Тогда:

$$\deg h_0 = m + 1 - t; \qquad h_0 = \text{НОД}(b_1, \dots, b_t);$$

неравенство $(*)$ выполняется при $j = 1, \dots, t$.

Доказательство. а) Предположим сначала, что $|b_1| < \left(p^{kl}/|f|^m\right)^{1/n}$, т. е. $|b_1|^n \cdot |f|^m < p^{kl}$. Тогда согласно теореме 30.3 многочлен $b_1 \in L$ делится на h_0. С другой стороны, из условия $b_1 \in L$ следует, что $\deg b_1 \leqslant m$. Поэтому $\deg h_0 \leqslant m$.

Предположим теперь, что $\deg h_0 \leqslant m$, т. е. $h_0 \in L$. Согласно следствию из теоремы Миньотта (см. с. 173) $|h_0| \leqslant \binom{2m}{m}^{1/2} |f|$. Применив теорему 30.2 (г) для $x = h_0$, получим

$$b_1 \leqslant 2^{m/2}|h_0| \leqslant 2^{m/2}\binom{2m}{m}^{1/2}|f|. \tag{4}$$

По условию $2^{mn/2}\binom{2m}{m}^{n/2}|f|^n < p^{kl}/|f|^m$, т. е.

$$2^{m/2}\binom{2m}{m}^{1/2}|f| < \left(p^{kl}/|f|^m\right)^{1/n}. \tag{5}$$

Из (4) и (5) получаем требуемое неравенство $|b_1| < \left(p^{kl}/|f|^m\right)^{1/n}$.

б) Пусть J — множество всех индексов j, для которых выполняется неравенство (*). Согласно теореме 30.3, если $j \in J$, то b_j делится на h_0. Таким образом, многочлен $h_1 = \text{НОД}(b_j \mid j \in J)$ делится на h_0. При этом, если $j \in J$, то b_j делится на h_1 и $\deg b_j \leqslant m$, т. е. b_j принадлежит решетке

$$\mathbb{Z} \cdot h_1 + \mathbb{Z} \cdot h_1 x + \ldots + \mathbb{Z} \cdot h_1 x^{m - \deg h_1}.$$

Векторы $b_1, \ldots, b_m$ линейно независимы, поэтому

$$|J| \leqslant m + 1 - \deg h_1, \tag{6}$$

где $|J|$ — количество элементов множества J.

Согласно следствию из теоремы Миньотта (см. с. 173)

$$|h_0 x^i| = |h_0| \leqslant \binom{2m}{m}^{1/2}|f| \quad \forall i \geqslant 0.$$

При $i = 0, 1, \ldots, m - \deg h_0$ по определению $h_0 x^i \in L$ и эти векторы линейно независимы. Поэтому к ним можно применить теорему 30.2 (д):

$$|b_j| \leqslant 2^{m/2}|h_0 x^i| \leqslant 2^{m/2}\binom{2m}{m}^{1/2}|f| \quad \text{при} \quad 1 \leqslant j \leqslant m + 1 - \deg h_0.$$

По предположению $2^{m/2}\binom{2m}{m}^{1/2}|f| < \left(p^{kl}/|f|^m\right)^{1/n}$, поэтому

$$\{1, 2, \ldots, m + 1 - \deg h_0\} \subset J.$$

Многочлен h_1 делится на h_0, поэтому $\deg h_1 \leqslant \deg h_0$, а значит,

$$|J| \geqslant m + 1 - \deg h_0 \geqslant m + 1 - \deg h_1. \tag{7}$$

Сравнивая неравенства (6) и (7), получаем, что $\deg h_0 = \deg h_1 = t$ и $J = \{1, 2, \ldots, t\}$.

Остается проверить, что $h_0 = \pm h_1$. Многочлен h_0 является делителем многочлена f с содержанием 1, поэтому $\operatorname{cont}(h_0) = 1$. Пусть $j \in J$ и $d_j = \operatorname{cont}(b_j)$. Согласно теореме 30.3 многочлен b_j делится на h_0. Следовательно, многочлен b_j/d_j тоже делится на h_0. Учитывая, что $h_0 \in L$, получаем $b_j/d_j \in L$. Но b_j — элемент базиса решетки L, поэтому $d_j = 1$. Это означает, что $\operatorname{cont}(h_1) = 1$, так как b_j делится на h_1. Итак, многочлен h_1 делится на h_0 и $\operatorname{cont}(h_1) = 1$, поэтому $h_0 = \pm h_1$. □

Теперь уже можно описать алгоритм вычисления многочлена h_0.

Вспомогательный алгоритм. (При фиксированном m алгоритм выясняет, верно ли, что $\deg h_0 \leqslant m$; если это верно, то он вычисляет многочлен h_0.)

Исходные данные:

- многочлен f степени n;
- простое число p;
- натуральное число k;
- многочлен h со старшим коэффициентом 1, для которого $f \pmod{p^k}$ делится на $h \pmod{p^k}$; при этом многочлен $h \pmod p$ неприводим и $f \pmod p$ не делится на $h^2 \pmod p$; мы считаем, что коэффициенты многочлена h приведены по модулю p^k, т. е. заключены между 0 и $p^k - 1$ (при этом $|h|^2 \leqslant 1 + lp^{2k}$);
- натуральное число $m \geqslant l = \deg h$, для которого выполняется неравенство

$$p^{kl} > 2^{mn/2} \binom{2m}{m}^{n/2} |f|^{m+n}. \tag{8}$$

Работа алгоритма. Для решетки L с базисом

$$\{p^k x^i \mid 0 \leqslant i < l\} \cup \{h^k x^j \mid 0 \leqslant j < m - l\}$$

находим приведенный базис $b_1, \ldots, b_{m+1}$.

Если $|b_1| \geqslant \left(p^{kl}/|f|^m\right)^{1/n}$, то $\deg h_0 > m$ и алгоритм останавливается.

Если же $|b_1| < \left(p^{kl}/|f|^m\right)^{1/n}$, то $\deg h_0 \leqslant m$ и $h_0 = \text{НОД}(b_1, \ldots, b_t)$, где число t определено в формулировке теоремы 30.4 (б).

Основной алгоритм. (Вычисление неприводимого множителя h_0 многочлена f, для которого $h_0 \pmod p$ делится на $h \pmod p$.)

Можно считать, что $l = \deg h < \deg f = n$ и коэффициенты многочлена h приведены по модулю p, т. е. заключены между 0 и $p - 1$.

Работа алгоритма. Сначала вычисляем наименьшее натуральное k, для которого неравенство (8) выполняется при $m = n - 1$:

$$p^{kl} > 2^{n(n-1)/2} \binom{2(n-1)}{n-1}^{n/2} |f|^{2n-1}.$$

Затем для разложения $f \equiv hg \pmod{p}$ вычисляем его поднятие Гензеля $f \equiv \overline{hg} \pmod{p^k}$, где k — только что вычисленное натуральное число. При этом $\overline{h} \equiv h \pmod{p}$; коэффициенты многочлена $\overline{h}$ считаем приведенными по модулю p^k.

Пусть u — наибольшее целое число, для которого $l \leqslant (n-1)/2^u$. Последовательно выполняем вспомогательный алгоритм для $m = \left[\frac{n-1}{2^u}\right]$, $\left[\frac{n-1}{2^{u-1}}\right], \ldots, \left[\frac{n-1}{2}\right], n-1$ до тех пор, пока не вычислим многочлен h_0. Если же это не произойдет, то $\deg h_0 > n-1$ и $h_0 = f$, т. е. многочлен f неприводим.

Литература

[АТЧ] *Алгебраическая теория чисел* / Ред. Дж. Касселс, А. Фрёлих., М.: Мир, 1969.

[ББ] Беккенбах Э., Беллман Р., *Неравенства*, М.: Мир, 1965.

[БШ] Боревич З. И., Шафаревич И. Р., *Теория чисел*, М.: Наука, 1972.

[Бу] Бугаенко В. О., *Коммутирующие многочлены*, Математическое Просвещение (третья серия) **Вып. 1** (1997), 140–163.

[В] Ван дер Варден Б. Л., *Алгебра*, М.: Наука, 1976.

[ГНШ] Галочкин А. И., Нестеренко Ю. В., Шидловский А. Б., *Введение в теорию чисел*, М.: Изд-во МГУ, 1995.

[Г] Галуа Э., *Сочинения*, М.–Л.: ОНТИ, 1936.

[ГР] Гаспер Дж., Рахман М., *Базисные гипергеометрические ряды*, М.: Мир, 1993.

[Ге1] Гельфонд А. О., *Трансцендентные и алгебраические числа*, М.: ГИТТЛ, 1952.

[Ге2] Гельфонд А. О., *Исчисление конечных разностей*, М.: Наука, 1967.

[Дэ] Дэвенпорт Г., *Мультипликативная теория чисел*, М.: Наука, 1971.

[К1] Касселс Дж. В. С., *Введение в теорию диофантовых приближений*, М.: ИИЛ, 1961.

[К2] Касселс Дж., *Рациональные квадратичные формы*, М.: Мир, 1982.

[Ки] Кириллов А. А., *Что такое число?*, М.: Наука, 1993.

[Кл] Клейн Ф., *Лекции об икосаэдре и решении уравнений пятой степени*, М.: Наука, 1989.

[Л1] Ленг С., *Алгебра*, М.: Мир, 1968.

[Л2] Ленг С., *Основы диофантовой геометрии*, М.: Мир, 1986.

[М] Макдональд И., *Симметрические функции и многочлены Холла*, М.: Мир, 1985.

[Мм] Мамфорд Д., *Алгебраическая геометрия 1. Комплексные проективные многообразия*, М.: Мир, 1979.

[О] Островский А. М., *Решение уравнений и систем уравнений*, М.: ИИЛ, 1963.

[ПС] Полиа Г., Сеге Г., *Задачи и теоремы из анализа*, В 2-х ч. М.: Наука, 1978.

[По1] Постников М. М., *Теория Галуа*, М.: ГИФМЛ, 1963.

[По2] Постников М. М., *Устойчивые многочлены*, М.: Наука, 1981.

[Пр1] Прасолов В. В., *Наглядная топология*, М.: МЦНМО, 1995.

[Пр2] Прасолов В. В., *Задачи и теоремы линейной алгебры*, М.: Наука, 1996.

[ПрС] Прасолов В. В., Соловьев Ю. П., *Эллиптические функции и алгебраические уравнения*, М.: Факториал, 1997.

[ПрШ] Прасолов В. В., Шварцман О. В., *Азбука римановых поверхностей*, М.: Фазис, 1999.

[С] Серр Ж.-П., *Курс арифметики*, М.: Мир, 1972.

[Т] Табачников С. Л., *Многочлены*, М.: Фазис, 1996.

[ТУ] Тихомиров В. М., Успенский В. В., *Десять доказательств основной теоремы алгебры*, Математическое Просвещение (третья серия) **Вып. 1** (1997), 50–70.

[Хов] Хованский А. Г., *Малочлены*, М.: Фазис, 1997.

[Ч] Чандрасекхаран К., *Введение в аналитическую теорию чисел*, М.: Мир, 1974.

[Че] Чеботарев Н. Г., *Основы теории Галуа*, Л.–М.: ОНТИ, 1937.

[ЭЭМ] *Энциклопедия элементарной математики, кн. 2 (Алгебра)*, М.–Л.: ГИТТЛ, 1951.

[AdL] Adams W. W., Loustaunau Ph., *An introduction to Gröbner bases*, AMS, 1994.

[An] Anderson B., *Polynomial root dragging*, Amer. Math. Monthly **100** (1993), 864–866.

[AnSV] Anderson N., Saff E. B., Varga R. S., *On the Eneström–Kakeya theorem and its sharpness*, Linear Algebra and Appl. **28** (1979), 5–16.

[Anr] Andrushkiw J. W., *Polynomials with prescribed values at critical points*, Bull. Amer. Math. Soc. **62** (1956), 243.

[Ar] Artin E., *Über die Zerlegung definiter Funktionen in Quadrate*, Abh. Math. Sem. Hamburg **5** (1927), 100–115.

[ArS] Artin E., Schreier O., *Algebraische Konstruktion reeler Körper*, Abh. Math. Sem. Hamburg **5** (1927), 85–99.

[As] Askey R., *An inequality for Tchebycheff polynomials and extensions*, J. Approx. Theory **14** (1975), 1–11.

[Ay] Ayoub R. G., *On the nonsolvability of the general polinomial*, Amer. Math. Monthly **89** (1982), 397–401.

[Az] Aziz A., *On the zeros of composite polnomials*, Pacific J. Math. **103** (1982), 1–7.

[B] van den Berg F. J., *Nogmaals over afgeleide Wortelpunten*, Nieuw Archiev voor Wiskunde **15** (1888), 100–164.

[Be] Berg L., *Abschätzung von Nullstellen eines Polynoms*, Z. angew. Math. Mech. **67** (1987), 57–58.

[Ber1] Berlekamp E. R., *Factoring polynomials over finite fields*, Bell System Tech. J. **46** (1967), 1853–1859.

[Ber2] Berlekamp E. R., *Factoring polynomials over large finite fields*, Math. Comp. **24** (1970), 713–735.

[Bern] Bernoulli J., *Ars conjectandi*, Basileae, 1713.

[Beu] Beukers F., *A note on the irrationality of* $\zeta(2)$ *and* $\zeta(3)$, Bull. London Math. Soc. **11** (1979), 268–272.

[Bo] Boyd D. W., *Sharp inequalities for the product of polynomials*, Bull. London Math. Soc. **26** (1994), 449–454.

[Br] Brauer A., *On algebraic equations with all but one root in the interior of the unit circle*, Math. Nachrichten **4** (1950/51), 250–257.

[Bu1] Buchberger B., *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. Thesis, Inst. University of Innsbruck, Austria, 1965.

[Bu2] Buchberger B., *Gröbner bases: An algorithmic method in polynomial ideal theory*, in Multidimensional systems theory (N. K. Bose ed.), Reidel, Dordrecht, 1985, 184–232.

[Bu3] Buchberger B., Winkled F. (Editors), *Gröbner bases and applications*, London Math. Soc. Lecture Notes Series, V. 251, 1998.

[BP] Burnside W. S., Panton A. W., *The theory of equations*, Dublin Univ. Press, Dublin–London, 1928.

[CC] Cahen P.-J., Chabert J.-L., *Integer-valued polynomials*, AMS, 1997.

[CZ] Cantor D. G., Zassenhaus H., *A new algorithm for factoring polynomials over finite fields*, Math. Comp. **36** (1981), 587–592.

[CT] Cartier P.,Tate J., *A simple proof of the main theorem of eliminating theory in algebraic geometry*, L'Enseignement Math. **24** (1978), 311–317.

[Ca] Cassels J. W. S., *On the representation of rational functions as sums of squares*, Acta Arithm. **9** (1964), 79–82.

[CEP] Cassels J. W. S., Ellison W. J., Pfister A., *On sums of squares and on elliptic curves over function fields*, J. Number Theory **3** (1971), 125–149.

[Chr] Christie M. R., *Positive definite rational functions of two variables which are not the sum of three squares*, J. Number Theory **8** (1976), 224–232.

[Chu] Chung-Chun Yang, *A problem on polynomials*, Rev. Roumaine Math. Pures Appl. **22** (1977), 595–598.

[Co] Colliot-Thélène J.-L., *The Noether–Lefschetz theorem and sums of 4 squares in the rational function field* $\mathbb{R}(x, y)$, Compositio Math. **86** (1993), 235–243.

[CS] Cohen G. L., Smith G. H., *A simple verification of Ilieff's conjecture for polynomials with three zeros*, Amer. Math. Monthly **95** (1988), 734–737.

[Coh] Cohen H., *A course in computational algebraic number theory*, Springer, Berlin e.a., 1993.

[CK] Cross G. E., Kannappan Pl. *A functional identity characterizing polynomials*, Aequat. Math. **34** (1987), 147–152.

[Da] Das M., *Sur un déterminant á permutation circulaire pour les polynômes de Tchebychev de première espeèe*, C. R. Acad. Sci. Paris **268** (1969), A385–A386.

[DLS] Davenport H., Lewis D. J., Schinzel A., *Polynomials of certain special types*, Acta Arithm. **9** (1964), 108–116.

[DS] Dobbertin H., Schmieder G., *Zur Charakterisierung von Polynomen durch ihre Null- und Einsstellen*, Arch. Math. **48** (1987), 337–342.

[Dö] Dörge K., *Einfacher Beweis des Hilbertschen Irreduzibilitätssatzes*, Math. Ann. **96** (1927), 176–182.

[Dub] Dubois D. W., *Note on Artin's solution of 17th Hilbert's problem*, Bull. Amer. Math. Soc. **73** (1967), 540–541.

[Dum] Dumas G., *Sur quelques cas d'irréductibilité des polynômes à coefficients rationels*, J. Math. Pures Appl. **2** (1906), 191–258.

[Ed] Edwards H. M., *Galois theory*, Springer, New York e.a., 1984.

[Ev] Evyatar A., *On polynomial equations*, Israel J. Math., **10** (1971), 321–326.

[Fa] Faulhaber J., *Academia algebrae*, Augsburg, 1631.

[Fr] Fried M., *On Hilbert's irreducibility theorem*, J. Number Theory, **6** (1974), 211–231.

[GG] Gardner R. B., Govil N. K., *On the location of zeros of a polynomial*, J. Approx. Theory **76** (1994), 286–292.

[Ga] Garling D. J. H., *A course in Galois theory*, Cambridge Univ. Press, Cambridge e.a., 1986.

[Gr] Grosswald E., *Recent applications of some old work of Laguerre*, Amer. Math. Monthly **86** (1979), 648–658.

[H] Haruki Sh., *A property of quadratic polynomials*, Amer. Math. Monthly **86** (1979), 577–578.

[Hi1] Hilbert D., *Über die Darstellung definierter Formen als Summe von Formenquadraten*, Math. Ann. **32** (1888), 342–350.

[Hi2] Hilbert D., *Über die Theorie der algebraische Formen*, Math. Ann. **36** (1890), 473–534.

[Hi3] Hilbert D., *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. reine angew. Math. **110** (1892), 104–129.

[Hi4] Hilbert D., *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–373.

[Ho] Hornfeck B., *Primteiler von Polynomen*, J. reine angew. Math. **243** (1970), 120.

[Hu] Hurwitz A., *Über der Vergleich des arithmetischen und des geometrischeh Mittels*, J. reine angew. Math. **108** (1891), 266–268.

[J] Janusz G. J., *Algebraic number fields*, AMS, 1996.

[Kl] Kleiman H., *Irreducibility criteria*, J. London Math. Soc. (2) **5** (1972), 133–138.

[Kr] Kronecker L., *Zwei Sätze ueber Gleichungen mit ganzzahligen Coefficienten*, J. reine angew. Math. **53** (1857), 173–175.

[Kru] Krusemeyer M., *Why does the Wronskian work?* Amer. Math. Monthly **95** (1988), 46–49.

[Ku] Kubert D., *The universal ordinary distribution*, Bull. Soc. Math. France **107** (1979), 179–202.

[L] Landau E., *Über die Darstellung definiter Funktionen als Summe von Quadraten*, Math. Ann. **62** (1906), 290–329.

[La] Lang S., *Old and new conjectured diophantine inequalities*, Bull. Amer. Math. Soc. **23** (1990), 37–83.

[Le] Lehmer D. H., *A new approach to Bernoulli polynomials*, Amer. Math. Monthly **95** (1988), 905–911.

[LLL] Lenstra A. K., Lenstra H. W., Lovász L., *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[Lj] Ljunggren W., *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 65–70.

[M1] Mahler K., *An application of Jensen formula to polynomials*, Mathematika **7** (1960), 98–100.

[M2] Mahler K., *On some inequalities for polynomials in several variables*, J. London Math. Soc. **37** (1962), 341–344.

[M3] Mahler K., *An inequality for a pair of polynomials that are relatively prime*, J. Austral. Math. Soc. **4** (1964), 418–420.

[ML] Marcus M., Lopes L., *Inequalities for symmetric functions and Hermitian matrices*, Canad. J, Math. **8** (1956), 524–531.

[Ma1] Marden M., *Geometry of polynomials*, AMS, 1966.

[Ma2] Marden M., *The search for a Rolle's theorem in the complex domain*, Amer. Math. Monthly **92** (1985), 643–650.

[Mi] Mignotte M., *An inequality about factors of polynomials*, Math. Comput. **28** (1974), 1153–1157.

[MS] Mikusiński J., Schinzel A., *Sur la rèductibilitè de certains trinômes*, Acta Arithm. **9** (1964), 91–95.

[Mi] Milnor J., *On polylogarithms, Hurwitz zeta functions, and the Kubert identities*, L'Enseignement Math. **29** (1983), 281–322.

[Mo] Motzkin T. S., *Algebraic Inequalities*, в книге *Inequalities*, Editor O. Shisha, New York: Academic Press, 1967, 199–203.

[Mu] Muirhead R. F., *Some methods applicable to identities and inequalitiies of symmetric algebraic functions of n letters*, Proc. Edinburgh Math. Soc. **21** (1903), 144–157.

[My] Mycielski Y., *Polynomials with preassigned values at their branching points*, Amer. Math. Monthly **77** (1970), 853–855.

[N] Nathanson M. B., *Catalan's equation in $K(t)$*, Amer. Math. Monthly **81** (1974), 371–373.

[NM] Newman D. J., Slater. M. *Waring's problem for the ring of polynomials*, J. Number Theory **11** (1979), 477–487.

[O] O'Hara P. J., *Another proof of Bernstein's theorem*, Amer. Math. Monthly **80** (1973), 673–674.

[Os] Osada H., *The Galois groups of the polynomials $x^n + ax^l + b$*, J. Number Theory **25** (1987), 230–238.

[Ost] Ostrowski A., *Über ganzwertige Polynome in algebraischen Zahlkörpern*, J. reine angew. Math. **149** (1919), 117–124.

[Oz] Ozeki K., *A certain property of polynomials*, Aequat. Math. **25** (1982), 247–252.

[Pe] Perron O., *Algebra II*, Leipzig: de Gruyter, 1933.

[Pf1] Pfister A., *Multiplikative quadratische Formen*, Arch. Math. **16** (1965), 363–370.

[Pf2] Pfister A., *Quadratic forms with applications to alrebra, geometry and topology*, London Math. Soc. Lecture Notes Series, V. 217, 1995.

[Pó] Pólya G., *Über ganzwertige ganze Funktionen*, Rend. Circ. Matem. Palermo **40** (1915), 1–16.

[Pu] Pourchet Y., *Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques*, Acta Arithm. **19** (1971), 89–104.

[R] Rabinowitsch S., *Zum Hilbertschen Nullstellensatz*, Math. Ann. **102** (1929), 520.

[Ra] Rabinowitz S., *The factorization of* $x^5 \pm x + n$, Math. Mag. **61** (1988), 191–193.

[Raj] Rajwade A. R., *Squares*, London Math. Soc. Lecture Notes Series, V. 171, 1993.

[Ri] Risler J.-J., *Une caractérisation des idéaux des variétés algébriques réeles*, C. R. Acad. Sci. **271** (1970), Serie A, 1171–1173.

[Ro] Rogosinski W. W., *Some elementary inequalities for polynomials*, Math. Gaz. **V. 39, N. 327** (1955), 7–12.

[Roi] Roitman M., *On roots of polynomials and of their derivatives*, J. London Math. Soc. (2) **27** (1983), 248–256.

[Ros] Rosen M. I., *Niels Hendrik Abel and equation of the fifth degree*, Amer. Math. Monthly **102** (1995), 495–505.

[Rth] Roth K. F., *Rational approximations to algebraic numbers*, Mathematika **2** (1955), 1–20 (Corrigendum p. 168).

[Ru] Rubinstein Z., *Remarks on a paper by A. Aziz*, Proc. Amer. Math. Soc. **94** (1985), 236–238.

[S] Salmon G., *Lesson introductory to the modern highers algebra*, 5th ed., NY.: Chelsea, 1964.

[Sa] Scharlau W., *Quadratic and hermitian forms*, Springer, Berlin e.a., 1985.

[Sc1] Schinzel A., *Solution d'un problème de K. Zarankiewicz sur les suites des puissances consécutives de nombres irrationnels*, Colloc. Math. **9** (1962), 291–296.

[Sc2] Schinzel A., *Reducibility of polynomials*, в книге Actes Congrès intern. math. 1970. Tome 1, 491–496.

[ScZ] Schinzel A., Zassenhaus H., *A refinement of two theorems of Kronecker*, Michigan Math. J. **12** (1965), 81–85.

[Scm] Schmeisser G., *On Ilieff's conjecture*, Math. Z. **156** (1977), 165–173.

[Sho] Schoenberg I. J., *Mathematical time exposures*, MAA, 1982.

[Shu] Schur I., *Über die Existenz unendlich vieler Primzahlen in einige speziellen arithmetischen Progressionen*, S.-B. Berlin. Math. Ges. **11** (1912), 40–50.

[Shw] Schwarz H., *Über dienige Fälle, in denen Gaussische Reihe* $F(\alpha, \beta, \gamma, x)$ *eine algebraische Function ihres vierten Elementen ist*, Borchardt's J. **75** (1872).

[Sr] Serre J.-P., *Lectures on the Mordell–Weil theorem*, Vieweg, 1989.

[Ss] Sonnenschein H., *A representation for polynomials in several variables*, Amer. Math. Monthly **78** (1971), 45–47.

[St] Stengle G., *Integral solution of Hilbert's seventeenth problem*, Math. Ann. **246** (1979), 33–39.

[Sti] Stillwell J., *Galois theory for beginners*, Amer. Math. Monthly **101** (1994), 22–27.

[Str] Strelitz Sh., *On the Routh–Hurwitz problem*, Amer. Math. Monthly **84** (1977), 542–544.

[Stu] Sturmfels B., *Gröbner bases and convex polytopes*, AMS, 1996.

[Su] Sudbery A., *The number of distinct roots of a polynomial and its derivatives*, Bull. London. Math. Soc. **5** (1973), 13–17

[Sur] Sury B., *The value of Bernouilli polynomials at rational points*, Bull. London Math. Soc. **25** (1993), 327–329.

[Suz] Suzuki J., *On coefficients of cyclotomic polynomials*, Proc. Japan Acad. **A63** (1987), 279–280.

[Sw] Swan R. G., *Factorization of polinomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.

[Th] Thom R., *L'équivalence d'une fonction différentiable et d'un polynome*, Topology **3**, Suppl. 2 (1965), 297–307.

[Tv] Tverberg H., *On the irreducibility of polynomials taking small values*, Math. Scand. **32** (1973), 5–21.

[W] Wahab J. H., *New cases of irreducibility for Legendre polynomials*, Duke Math. J. **19** (1952), 165–176.

[We] Weber H., *Lehrbuch der Algebra, Bd. 1–3*, Braunschweig, 1908.

[Wh] Whiteley J. N., *Some inequalities concerning symmetric functions*, Mathematika **5** (1958), 49–57.

[Wi] Wilf H. S., *Perron–Frobenius theory and the zeros of polynomials*, Proc. Amer. Math. Soc. **12** (1961), 247–250.

[Wt] Witt E., *Über die Kommutativität endlicher Schiefkörper*, Abh. Math. Sem. Hamburg **8** (1931), 413.

Предметный указатель