К алгоритмам решения алгебраических уравнений

А. Скопенков *

Содержание

1 Введение

Теоремы Руффини-Абеля-Галуа о неразрешимости алгебраических уравнений в радикалах — классический результат алгебры, интересный для информатики (теории символьных вычислений). В этом тексте даны четкая формулировка и простое доказательство теоремы Руффини. Чтобы доказывать неразрешимость алгебраических уравнений, мы разберем общий способ их решения — метод резольвент Лагранжа. Идея Абеля и Галуа фактически заключается в том, что если уравнение разрешимо в радикалах, то его можно решить этим методом. Этим методом строятся алгоритмы — распознаваемости разрешимости уравнений в радикалах и решения в радикалах разрешимого уравнения.

Основные идеи представлены на «олимпиадных» примерах: на простейших частных случаях, свободных от технических деталей, и со сведением научного языка к необходимому минимуму. Хотя основные результаты касаются уравнений высших степеней, идеи демонстрируются на нетривиальных задачах о квадратных и кубических уравнениях.

Для изучения этого текста достаточно знакомства с многочленами, комплексными числами и перестановками. При этом он содержит красивые сложные результаты. Изучившие (точнее, изрешавшие) его получат хорошее представление об отправных идеях теории Галуа. Они смогут порешать задачи для исследования, связанные с алгеброй, комбинаторикой и информатикой. И выступать со своими результатами на конференциях школьников, например, [M].

В отличие от большинства учебников по этой теме, приводимые задачи и решения не используют термина «группа Галуа» (даже термина «группа»). Несмотря на отсутствие этих *терминов*, *идеи* приводимых доказательств являются *отправными* для *теории Галуа* [ZSS, §28 «О необходимости мотивировок»] и *конструктивной теории Галуа* [E]. Ср. [ZSS, §5], [S].

*Поддержан стипендией Саймонса и грантом фонда Д. Зимина «Династия». Московский Физико-Технический Институт, Независимый Московский Университет; http://www.mccme.ru/~skopenko.

Этот текст основан на занятиях, проведенных автором в разное время в Московской выездной школе по математике, в кружках «Математический семинар» и «Олимпиады и математика». Благодарю А. Кушнира и Г. Челнокова за полезные замечания.

Мы следуем традиции изучения материала в виде решения и обсуждения задач, см. [ZSS, п. 1.2 и §26]. К важнейшим задачам приводятся подсказки, указания, решения и ответы. Они расположены в конце каждого пункта. Однако к ним стоит обращаться после прорешивания каждой задачи. Если задача выделена словом «теорема» («лемма», «следствие» и т. д.) и жирным шрифтом, то ее утверждение важное. Номера задач обозначаются жирным шрифтом. Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. Наиболее трудные задачи отмечены звездочкой.

Замечание. Рассмотрим калькулятор с кнопками

$$1, \quad +, \quad -, \quad \times, \quad : \quad \text{и} \quad \sqrt[n]{\ } \quad \text{для любого } n.$$

Калькулятор оперирует с комплексными числами. Он вычисляет числа с абсолютной точностью и имеет неограниченную память. При делении на 0 он выдаҷт ошибку. При нажатии кнопки $\sqrt[n]{\ }$ он выдаҷт все значения корня. Неформально говоря, комплексное число *радикально*, если его можно получить на комплексном калькуляторе.

Комплексное число называется **радикальным** (radical-like), если его можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству $M \ni x, y$ чисел $x+y, x-y, xy$, числа x/y при $y \neq 0$ и множества $\sqrt[n]{x} \subset \mathbb{C}$ для любого целого $n \geq 2$. Стандартный термин: лежит в некотором радикальном расширении поля $\mathbb{Q}$.

Например, любой корень квадратного уравнения с рациональными коэффициентами является радикальным. То же справедливо для уравнений 3-й и 4-й степени (см., например, [ZSS, п. 4.2]; в п. §2 приведено другое доказательство).

1.1. (a) **Теорема Галуа.** *Ни один корень уравнения* $u^5 - 4u + 2 = 0$ *не является радикальным.*

(b) *There is an algorithm deciding, for* $a_{n-1}, \dots, a_0 \in \mathbb{Q}$*, whether all the roots of the equation* $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ *are radical-like.*

Мы докажем более слабую теорему Руффини 2.5, которая все равно нужна для доказательства теоремы Галуа [S]. Part (b) is implied by the Galois Solvability Criterion 2.8 below, together with an estimation on the number of operations. (This estimation can easily be extracted from the proof of the criterion; the idea is to observe that the 'symmetry subgroup' of S_n cannot be changed more than $\log_2 n! < n \log_2 n$ times.)

In this text equality signs involving polynomial f (or f_j) mean equality of polynomials (покоэффициентное).

2 Решаем уравнения: метод резольвент Лагранжа

Решение квадратного уравнения можно выразить формулами

$$(x-y)^2 = (x+y)^2 - 4xy \quad \text{и} \quad x = \frac{x+y+(x-y)}{2}.$$

Эти формулы показывают, что корень x квадратного уравнения *выразим в радикалах* (в смысле, строго определенном ниже) через коэффициенты $x+y, xy$ квадратного уравнения.

Обозначим

$$\sigma_1(x_1, \dots, x_n) := x_1 + \ldots + x_n, \quad \dots, \quad \sigma_n(x_1, \dots, x_n) = x_1 \cdot \ldots \cdot x_n.$$

Если число n ясно из контекста, то оно пропускается из обозначений.

Многочлен $p \in \mathbb{C}[x_1, \ldots, x_n]$ **выразим в (комплексных) радикалах** если p можно добавить в набор $\{\sigma_1, \ldots, \sigma_n\} \cup \{\lambda\}_{\lambda \in \mathbb{C}}$ многочленов цепочкой операций следующего вида:

• добавить в набор сумму или произведение уже имеющихся многочленов;

• если многочлен из набора равен f^k для некоторых $f \in \mathbb{C}[x_1, \ldots, x_n]$ и целого $k > 1$, то добавить в набор многочлен f.

Замечание. (a) Например, если уже имеются многочлены $x^2 + 2y$ и $x - y^3$, то операциями первого типа можно добавить многочлен $-5(x^2 + 2y)^2 + 3(x^2 + 2y)(x - y^3)^6$. А если имеется многочлен $x^2 - 2xy + y^2$, то операцией второго типа можно добавить многочлен $x - y$ (или $y - x$).

(b) Операции первого типа добавляют многочлен с комплексными коэффициентами от уже имеющихся.

(c) Выразимость в радикалах многочлена x_1 равносильна существованию таких

• целых положительных чисел $s, k_1, \ldots, k_s$,

• многочленов $f_1, \ldots, f_s$ и $p_0, p_1, \ldots, p_s$ с комплексными коэффициентами от n и от $n, n+1, \ldots, n+s$ переменных, соответственно, что

$$\begin{cases} f_1^{k_1} = p_0(\sigma_1, \ldots, \sigma_n) \\ f_2^{k_2} = p_1(\sigma_1, \ldots, \sigma_n, f_1) \\ \ldots \\ f_s^{k_s} = p_{s-1}(\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_{s-1}) \\ x_1 = p_s(\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_s) \end{cases}.$$

В этих равенствах мы опускаем переменные $(x_1, \ldots, x_n)$ многочленов $\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_s$.

(d) Всегда ли можно, зная $x + y$ и xy, найти x? Вот простейшая формализация этого вопроса: *существует ли отображение* $f\colon \mathbb{R}^2 \to \mathbb{R}$, *для которого* $f(x + y, xy) = x$ *при любых* $x, y \in \mathbb{R}$? Ответ: не существует (рассмотрите пары $x = 1, y = 2$ и $x = 2, y = 1$). Итак, выразимость в радикалах не дает «нахождения» в указанном выше смысле.

Аналогично, зная

$$\sigma_1 := x + y + z, \quad \sigma_2 := xy + yz + zx \quad \text{и} \quad \sigma_3 := xyz,$$

невозможно найти $(x - y)(y - z)(z - x)$ (рассмотрите тройки $x = 0, y = 1, z = -1$ и $x = 0, y = -1, z = 1$).

2.1. Какие из следующих многочленов выразимы в радикалах для $n = 3$?

(a) $(x - y)(y - z)(z - x)$; (b) $x^9y + y^9z + z^9x$; (c) x.

В задаче 2.1 и далее используйте основную теорему о симметрических многочленах, см., например, [ZSS, п. 4.6]. Подсказкой к п. (c) являются следующие задачи 2.2.a и 2.4.c.

2.2. Многочлен $f \in \mathbb{R}[u_1, u_2, \ldots, u_n]$ называется **циклически симметрическим**, если $f(u_1, u_2, \ldots, u_n) = f(u_2, u_3, \ldots, u_{n-1}, u_n, u_1)$.

(a) Найдите хотя бы одну пару $\alpha, \beta \in \mathbb{C}$, для которой многочлен $(u + v\alpha + w\beta)^3$ циклически симметрический, а многочлен $u + v\alpha + w\beta$ — нет.

(b) Выразите $x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ в радикалах через некоторые циклически симметрические многочлены от $x_1, x_2, \ldots, x_{10}$.

2.3. Какие из следующих многочленов выразимы в радикалах для $n = 4$?

(a) $(x - y)(x - z)(x - t)(y - z)(y - t)(z - t)$; (b) $xy + zt$; (c) $x + y - z - t$; (d) x.

2.4. Решите системы уравнений (x, y, z, t — неизвестные, a, b, c, d известны, $\varepsilon_3 = \frac{-1+i\sqrt{3}}{2}$):

(a) $\begin{cases} x + y + z + t = a, \\ x + y - z - t = b, \\ x - y + z - t = c, \\ x - y - z + t = d; \end{cases}$ (b) $\begin{cases} x + y + z + t = a, \\ x + iy - z - it = b, \\ x - y + z - t = c, \\ x - iy - z + it = d; \end{cases}$ (c) $\begin{cases} x + y + z = a, \\ x + \varepsilon_3 y + \varepsilon_3^2 z = b, \\ x + \varepsilon_3^2 y + \varepsilon_3 z = c. \end{cases}$

Выражения из задачи 2.4 и называются *резольвентами Лагранжа*. Они «лучше» корней, поскольку «симметричнее» в смысле, осознанном Вами при решении задач 2.2.a и 2.3.c. Сообразите, почему же этот метод не работает для уравнения 5-й степени! Для $n = 5$ многочлен x_1 (и даже $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$) не выразим в радикалах.

2.5. Теорема Руффини. *Ни для какого $n \geq 5$ многочлен x_1 не выразим в радикалах.*

Теорема Руффини вытекает из леммы 5.4.a.

2.6. (a) Если $x_1, \dots, x_5$ — корни многочлена $f \in \mathbb{Q}[x]$ 5-й степени, то

$$T(y) := \prod_{\tau \in S_5} (y - x_{\tau(1)} - \varepsilon_5 x_{\tau(2)} - \varepsilon_5^2 x_{\tau(3)} - \varepsilon_5^3 x_{\tau(4)} - \varepsilon_5^4 x_{\tau(5)}) \in \mathbb{Q}[\varepsilon_5][y].$$

(b) Для некоторого $G \in \mathbb{Q}[\varepsilon_5][y]$ выполнено равенство $T(y) = G(y^5)$. Такой многочлен G называется *разрешающим многочленом* для f.

(c)* Все корни разрешающего многочлена для $f(x) = x^5 + 15x + 11$ радикальны.

2.7. * Все корни уравнения $x^5 + ax + b = 0$ радикальны для

(a) $(a, b) = (15, 11)$; (b) $(a, b) = (-5, 52)$; (c) $(a, b) = (35, 36)$;

(d) $(a, b) = \frac{(15 \pm 20c, 44 \mp 8c)}{c^2+1}$, $c \in \mathbb{Q}$, $c \geq 0$. (Для других (a, b) корни не радикальны [PSo]. Это вытекает из следующего критерия.)

2.8. * **Galois Solvability Criterion (conjecture).** *For each $a_{n-1}, \dots, a_0 \in \mathbb{Q}$ all the roots of the equation $A(x) := x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ are radical if and only if a set of degree 1 polynomials over $\mathbb{Q}$ can be obtained from $\{A\}$ using the following operations:*

- *(factorization) if one of our polynomials equals to P_1P_2 for some non-constant $P_1, P_2 \in \mathbb{Q}[x]$, then replace P_1P_2 by P_1 and P_2;*
- *(extracting a root) if one of our polynomials equals to $P(x^k)$ for some $P \in \mathbb{Q}[x]$, then replace $P(x^k)$ by $P(x)$;*
- *(taking Galois resolution) replace one of our polynomials P by the polynomial*

$$\prod_{\alpha \in S_k} (x - \varepsilon_k y_{\alpha(1)} - \varepsilon_k^2 y_{\alpha(2)} - \dots - \varepsilon_k^k y_{\alpha(k)}),$$

where $y_1, \dots, y_k$ are all the roots of P. (The coefficients of this product are symmetric in $y_1, \dots, y_k$, so they are rational, i.e. $y_1, \dots, y_k$ are 'not required' to calculate the coefficients.)

I would be grateful if a specialist in algebra could confirm that this criterion is correct (and is equivalent to the Galois Solvability Criterion in its usual textbook formulation, please give a reference), or describe required changes. (I asked some specialists since July 2017, but so far obtained no answer.)

3 Единственность способа решения квадратного уравнения

3.1. (a,b) Решите систему уравнений в многочленах $f(x, y)$, $p(u, v)$ и $q(u, v, w)$ с вещественными коэффицентами:

$$(a)\begin{cases} f^2(x, y) = p(x + y, xy) \\ x = q\left(x + y, xy, f(x, y)\right) \end{cases} \quad . \qquad (b)\begin{cases} f^k(x, y) = p(x + y, xy) \\ x = q\left(x + y, xy, f(x, y)\right) \end{cases} \quad , \quad \text{где } k > 0 \text{ целое.}$$

(c,d*) Решите аналоги п. (a,b) с заменой многочлена f на функцию $\mathbb{R}^2 \to \mathbb{R}$ (не предполагаемую непрерывной).

Системе уравнений из 3.1.a удовлетворяют, например, многочлены

$$f(x, y) = x - y, \quad p(u, v) = u^2 - 4v \quad \text{и} \quad q(u, v, w) = \frac{u + w}{2}.$$

3.2. Пусть $f, g \in \mathbb{R}[x, y]$.

(a) **Лемма.** Если $fg = 0$, то $f = 0$ или $g = 0$.

Предостережения: существуют функции $F, G : \mathbb{R} \to \mathbb{R}$, для которых $FG = 0$, $F \neq 0$, $G \neq 0$; существуют два разных многочлена от двух переменных, равные в бесконечном множестве точек; не пользуйтесь без доказательства тем, что если значения многочленов от двух переменных совпадают в любой точке, то эти многочлены равны.

(b) Если $f^2 = g^2$, то $f = g$ или $f = -g$.

(c) Если $f^2 + fg + g^2 = 0$, то $f = 0$ и $g = 0$.

(d) Если $f^3 = g^3$, то $f = g$.

(e) Если $f^5 = g^5$, то $f = g$.

(f) $f^5 - g^5 = (f - g)(f - \varepsilon_5 g)(f - \varepsilon_5^2 g)(f - \varepsilon_5^3 g)(f - \varepsilon_5^4 g)$. Здесь $\varepsilon_5 := \cos\frac{2\pi}{5} + i \sin\frac{2\pi}{5}$.

Для доказательства утверждений 3.1.bd полезны следующие понятия и лемма.

Многочлен f от двух переменных x, y называется *симметрическим*, если $f(x, y) = f(y, x)$, и *антисимметрическим*, если $f(x, y) = -f(y, x)$.

3.3. (a) **Лемма.** Если $f \in \mathbb{R}[x, y]$ — многочлен с вещественными коэффициентами от двух переменных и многочлен f^2 симметрический, то f либо симметрический, либо антисимметрический.

(b) **Лемма.** Если $f \in \mathbb{R}[x, y]$ и многочлен f^{2k+1} симметрический, то f симметрический.

(c) Если $f \in \mathbb{R}[x, y]$ антисимметрический, то существует симметрический многочлен $a \in \mathbb{R}[x, y]$, для которого $f = (x - y)a$.

Для доказательства полезна лемма 3.2.a, очень полезная и при решении других задач.

3.4. Для каких из утверждений 3.2 и 3.3 справедливы аналоги для многочленов с комплексными коэффициентами?

Вот обобщение утверждения 3.1 на любое количество шагов из определения выразимости в радикалах.

3.5. (a) Возьмем систему из замечания (c) в §2 для $n = 2$, в которой f_j и p_j рациональные функции (a не обязательно многочлены), и которая *минимальна*, т.е. нет системы с меньшим s и f_j^k не представляется в виде рациональной функции от $x + y, xy, f_1, \ldots, f_{j-1}$ ни для каких $j = 1, \ldots, s$ и $k < k_j$. Тогда $s = 1$, $k_1 = 2$ и существует рациональная функция $a \in \mathbb{R}(u, v)$, для которой $f_1(x, y) = (x - y)a(x + y, xy)$.

(b)* Сформулируйте и докажите аналог п. (a) с заменой рациональных функции $f_1, \ldots, f_s$ на функции $\mathbb{R}^2 \to \mathbb{R}$ ($p_0, \ldots, p_s$ по-прежнему рациональные функции), и равенств рациональных функций — на равенства функций, определенных для всех $(x, y) \in \mathbb{R}^2$.

3.6. (Загадка) Кубическое уравнение можно решить только одним способом.

Для доказательств полезны [ZSS, п. 5.4.1 «Одно извлечение квадратного корня», п. 5.4.5 «Одно извлечение корня третьей степени»].

4 «Вещественная» неразрешимость кубического уравнения

В этом пункте аргументы (x, y, z) многочленов в формулах часто пропускаются.

4.1. Не существует многочленов $f(x, y, z)$, $p(u, v, w)$ и $q(u, v, w, \tau)$ с вещественными коэффициентами, для которых

$$(a)\begin{cases} f^3 = p(\sigma_1, \sigma_2, \sigma_3) \\ x = q(\sigma_1, \sigma_2, \sigma_3, f) \end{cases}. \qquad (b)\begin{cases} f^2 = p(\sigma_1, \sigma_2, \sigma_3) \\ x = q(\sigma_1, \sigma_2, \sigma_3, f) \end{cases}.$$

Для доказательства полезны следующие понятие и лемма. Многочлен $f \in \mathbb{R}[x, y, z]$ называется **циклически симметрическим**, если $f(x, y, z) = f(y, z, x)$.

4.2. Если $f \in \mathbb{R}[x,y,z]$ и многочлен
(a) f^3; (b) f^2
циклически симметрический, то f циклически симметрический.

4.3. (Замечание; ср. с решением задачи 2.1.c.) Не существует таких многочленов

$$f_1(x,y,z), \quad f_2(x,y,z), \quad p_0(u,v,w), \quad p_1(u,v,w,\tau_1), \quad p_2(u,v,w,\tau_1,\tau_2)$$

с вещественными коэффициентами, для которых

$$\begin{cases} f_1^2 = p_0(\sigma_1,\sigma_2,\sigma_3) \\ f_2^3 = p_1(\sigma_1,\sigma_2,\sigma_3,f_1) \\ x = p_2(\sigma_1,\sigma_2,\sigma_3,f_1,f_2) \end{cases}.$$

Обобщение утверждения 4.3 на любое количество шагов формализуется определением *выразимости в вещественных радикалах*, которое получается из его комплексного аналога (§2) заменой комплексных коэффициентов на вещественные.

Формулы в начале §2 показывают, что x выразим в вещественных радикалах для $n = 2$. Решение задачи 2.1.ab показывает, что каждый из многочленов

$$(x-y)(y-z)(z-x), \quad x^9y + y^9z + z^9x$$

выразим в вещественных радикалах для $n = 3$.

4.4. Теорема. *Многочлен x_1 не выразим в вещественных радикалах для $n = 3$.*

Теорема 4.4 показывает, что *корень кубического уравнения не выразим в вещественных радикалах через его коэффициенты.* Она вытекает из следующей леммы.

4.5. Лемма (о сохранении циклической симметричности). *Если $q > 0$ целое, $f \in \mathbb{R}[x,y,z]$ и многочлен f^q циклически симметрический, то f циклически симметрический.*

4.6. Аналоги каких утверждений этого пункта справедливы для многочленов с комплексными коэффициентами?

Подсказки, указания и решения

2.1. (a) $(x-y)^2(y-z)^2(z-x)^2$ — симметрический многочлен.

(Пункт (a) можно также свести к (b).)

(b) Обозначим $M = x^9y+y^9z+z^9x$ и $N = y^9x+x^9z+z^9y$. Тогда многочлены $M+N$ и MN симметрические. Значит, они являются многочленами от элементарных симметрических многочленов $\sigma_1,\sigma_2,\sigma_3$. Само же M выражается через $M+N$ и MN по «формуле корней квадратного уравнения», см. формулы в начале п. 2.

(c) *Решение кубического уравнения при помощи резольвент Лагранжа.* Для нахождения корней x,y,z кубического уравнения достаточно найти выражения a,b,c из задачи 2.4 (c). (Заметим, что метод дель Ферро фактически приводит к тому же.) По теореме Виета $a = a(x,y,z)$ — коэффициент уравнения. При замене $x \leftrightarrow y$ многочлен $b = b(x,y,z)$ переходит в $\varepsilon_3 c$, а $c = c(x,y,z)$ в $\varepsilon_3^2 b$ (проверьте!). Значит, многочлены bc и b^3+c^3 не меняются при этой замене. Аналогично они не меняются при замене $z \leftrightarrow y$. Поэтому многочлены bc и b^3+c^3 *симметрические*, т. е. не меняются при любой перестановке переменных. Тогда из теоремы Виета и теоремы о представимости симметрического многочлена в виде многочлена от элементарных симметрических многочленов следует, что эти многочлены от x,y,z представляются в виде многочленов от коэффициентов уравнения. Теперь, решая квадратное уравнение, можно получить b^3 и c^3. Далее легко получить сами b и c.

2.2. (a) $x + y\varepsilon_3 + z\varepsilon_3^2$.

(b) Обозначьте

$$M = x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1 \quad \text{и} \quad N = x_2x_4 + x_4x_6 + x_6x_8 + x_8x_{10} + x_{10}x_2.$$

Далее аналогично задаче 2.1.b.

2.3. Для нахождения корней x, y, z, t уравнения 4-й степени достаточно найти выражения a, b, c, d от корней из задачи 2.4 (a). По теореме Виета a — коэффициент уравнения. При замене $x \leftrightarrow y$ многочлены c^2 и d^2 меняются местами, а многочлен b^2 переходит в себя. При циклической замене $x \to y \to z \to t \to x$ многочлены b^2 и d^2 меняются местами, а многочлен c^2 переходит в себя. Значит, многочлены b^2, c^2, d^2 переставляются при любой перестановке переменных. Поэтому виетовские многочлены от них, т. е.

$$b^2 + c^2 + d^2, \quad b^2c^2 + b^2d^2 + c^2d^2, \quad b^2c^2d^2,$$

симметрические. Тогда эти многочлены от x, y, z представляются в виде многочленов от коэффициентов уравнения. Теперь, решая кубическое уравнение, можно получить сами b^2, c^2, d^2. Далее легко получить b, c, d.

3.1. (a) Докажем, что существует такое $\alpha \in \mathbb{R}$, что $f(x, y) = \alpha(x - y)$.

Так как многочлен $f^2 = p$ симметрический, то можно считать, что многочлен q линеен по третьей переменной, т.е. $q(u, v, w) = a(u, v)+b(u, v)w$ для некоторых $a, b \in \mathbb{R}[u, v]$ (иначе изменим q, сохраняя f, p). Тогда $x = a(x + y, xy) + b(x + y, xy)f(x, y)$.

Первое завершение решения. Получаем $pb^2 = f^2b^2 = (x - a)^2 = (y - a)^2$. Отсюда по лемме 3.2.b $x - a = a - y$, так как случай $x - a = y - a$ невозможен. Значит, $a = (x + y)/2$. Тогда $(x - y)^2 = 4f^2b^2 = 4pb^2$. Если многочлен $p = f^2$ постоянный, то многочлен $b = \pm(x - y)/2\sqrt{p}$ не симметрический — противоречие. Поэтому многочлен p не постоянный. Тогда многочлен b постоянный. Значит, $2x = 2q = x + y + 2bf$, откуда $b \neq 0$ и $f = \alpha(x - y)$ для $\alpha = 1/2b$.

Второе завершение решения (написано с использованием текста И. Богданова). Так как многочлен x не симметрический и $x = q(x + y, xy, f(x, y))$, то многочлен f не симметрический. Тогда по лемме 3.3.a f антисимметрический. Значит, $y = q(x + y, xy, -f(x, y))$. Итак,

$$x = a + bf \quad \text{и} \quad y = a - bf, \quad \text{где} \quad a = a(x + y, xy), \quad b = b(x + y, xy) \quad \text{и} \quad f = f(x, y).$$

Тогда $x+y = 2a$ и $xy = a^2-b^2f^2$. Отсюда $(x-y)^2 = 4b^2f^2$. Аналогично первому завершению решения многочлен b постоянный. Значит, $f = \alpha(x - y)$ для $\alpha = \pm 1/2b$.

(b) Докажем, что k четно и существует такое $\alpha \in \mathbb{R}$, что $f(x, y) = \alpha(x - y)$.

Индукция по k с применением п. (a) и обобщения лемм 3.2.be, 3.3. Если k нечетно, то из утверждения 3.3.b получаем, что f симметрический, что противоречит равенству $x = q(x+ y, xy, f(x, y))$. Если $k = 4$ четно, то либо f^2 симметрический, либо антисимметрический. Первый случай сводится к п. (a). Во втором $f^2(x, y)+f^2(y, x) = 0$. Аналогично разбирается случай произвольного четного k.

(c) Аналогично п. (a) олучаем $x = a+bf$. Поэтому f — дробно-рациональная функция. Тогда проходит решение, аналогичное п. (a).

3.2. (a) Определите *старший член* многочлена так, чтобы старший член произведения равнялся произведению старших членов сомножителей.

(b) Следует из п. (a).

(c) Следует из п. (d).

(d) $f^2 + fg + g^2 = \left(f + \frac{g}{2}\right)^2 + \frac{3}{4}g^2 = (f + \varepsilon_3 g)(f + \varepsilon_3^2 g)$, где $\varepsilon_3 := \dfrac{-1 + i\sqrt{3}}{2}$.

(e) Следует из п. (f).

(f) Докажите и примените теорему Безу для многочленов от u с коэффициентами в $\mathbb{R}[v]$.

3.3. (a) Так как f^2 симметрический, то $f(x,y)^2 = f(y,x)^2$. Отсюда по утверждению 3.2.b $f(x,y) = \pm f(y,x)$.

(b) Используйте аналог утверждений 3.2.ce.

(c) См. указание к 3.2.f.

4.5. Обозначим $g(x,y,z) := f(y,z,x)$. Так как f^q циклически симметрический, то $f^q = g^q$. Если q нечетно, то $f = g$, значит, f циклически симметрический. А если q четно, то $f = g$ или $f = -g$. При $f = g$ получаем нужное утверждение, а при $f = -g$ имеем

$$f(x,y,z) = -f(y,z,x) = f(z,x,y) = -f(x,y,z).$$

Поэтому $f = 0$, значит, f циклически симметрический.

5 Неразрешимость уравнения 5-й степени «в многочленах»

Чтобы придумать идею доказательства теоремы Руффини 2.5, докажем следующие более простые факты. Ясно, что многочлен x не является многочленом от $x + y$ и xy.

5.1. Многочлен x_1 не выразим в радикалах для $n = 3$ так, что вторая операция из определения выразимости применяется только для

(a) $k = 2$ (*подсказка:* см. утверждение 4.6); (b) $k = 3$.

5.2. Какие из следующих утверждений верны для любого $f \in \mathbb{C}[x_1, \dots, x_5]$?

(a) Если f^3 циклически симметрический, то f циклически симметрический.

(b) Если f^5 циклически симметрический, то f циклически симметрический.

(c) Если f^3 симметрический, то f симметрический.

(d) Если f^2 симметрический, то f симметрический.

Многочлен $f \in \mathbb{C}[x_1, \dots, x_n]$ называется **четносимметрическим**, если для любого цикла α длины 3 многочлены $f(x_1, x_2, \dots, x_n)$ и $f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)})$ равны.

5.3. (a) Придумайте циклически симметрический многочлен, не являющийся четносимметрическим.

(b) Если перестановка переводит в себя многочлен, построенный Вами в решении задачи 5.2.d, то она представляется в виде композиции циклов длины 3.

Обозначим

$$\varepsilon_q := \cos\frac{2\pi}{q} + i\sin\frac{2\pi}{q}.$$

5.4. Пусть n целое и $f \in \mathbb{C}[x_1, \dots, x_n]$ — многочлен.

(a) **Лемма о сохранении четносимметричности.** *Если $q > 0$ целое, $n \geq 5$ и многочлен f^q четносимметрический, то f четносимметрический.*

(b) Если многочлен f^7 четносимметрический, то f четносимметрический.

(c) Если $n \geq 5$ и многочлен f^3 четносимметрический, то f четносимметрический.

(d) Если $n \geq 5$, то любой цикл длины 3 на n-элементном множестве разлагается в произведение перестановок вида $(ab)(cd)$ с различными a, b, c, d (т.е. в произведение композиций транспозиций с непересекающимися носителями).

Лемма (a) вытекает из и ее «частных случаев» (b,c) (и очевидного обобщения п. (b)). П. (c) вытекает из п. (d). См. детали в [S].

5.5. *Рациональной функцией* называется «формальное отношение многочленов», т.е. пара $f/g := (f, g)$ многочленов, в которой $g \neq 0$, с точностью до следующей эквивалентности: $f/g \sim f'/g'$ при $fg' = f'g$. При этом многочлен f отождествляется с парой $(f, 1)$.

(a) Дайте определения суммы и произведения рациональных функций. Проверьте их корректность.

(b) Определение *рациональной выразимости в вещественных (комплексных) радикалах* аналогично определению выразимости. Выразим ли рационально многочлен x в вещественных радикалах для $n = 3$?

(c) Выразим ли рационально многочлен x_1 в комплексных радикалах для $n = 5$?

6 Обобщение: функции вместо многочленов

Общее уравнение n-й степени разрешимо в (комплексных) радикалах, если существуют такие

• целые положительные числа $s, k_1, \dots, k_s$ и

• многочлены $p_0, p_1, \dots, p_s$ с вещественными коэффициентами и от $n, n+1, \dots, n+s$ переменных соответственно, что

$$\text{если} \quad a_0, \dots, a_{n-1}, x \in \mathbb{R} \quad \text{и} \quad x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 = 0,$$

то существуют числа $f_1, \dots, f_s \in \mathbb{R}$, для которых выполнены равенства, приведенные перед задачей 2.1, в которых $\sigma_1, \dots, \sigma_n$ заменены на $a_{n-1}, \dots, a_0$. В этих равенствах мы опускаем переменные $(x_1, \dots, x_n)$ многочленов $\sigma_1, \dots, \sigma_n$; равенства являются равенствами чисел.[1]

6.1. Для любого n это свойство равносильно каждому из двух следующих:

(1) Тождественную функцию $\mathbb{R} \to \mathbb{R}$ можно добавить в набор функций $\sigma_1, \dots, \sigma_n$ цепочкой операций следующего вида:

• добавить в набор многочлен с вещественными коэффициентами от уже имеющихся функций;

• если функция из набора равна f^k для некоторой функции $f : \mathbb{R}^n \to \mathbb{R}$ и целого $k > 1$, то добавить в набор функцию f.

(2) Существуют

• целые положительные числа $s, k_1, \dots, k_s$,

• многочлены $p_0, p_1, \dots, p_s$ с вещественными коэффициентами и от $n, n+1, \dots, n+s$ переменных соответственно,

• функции $f_1, \dots, f_s : \mathbb{R}^n \to \mathbb{R}$ (не предполагаемые непрерывными)

такие, что справедливы равенства, приведенные перед задачей 2.1. В этих равенствах мы опускаем переменные $(x_1, \dots, x_n)$ функций $f_1, \dots, f_s$ и многочленов $\sigma_1, \dots, \sigma_n$; равенства теперь являются равенствами функций.

6.2. Если x_1 выразим в радикалах, то общее уравнение n-й степени разрешимо в радикалах.

Из утверждений 6.2, 3.1.a и результатов задач 2.1, 2.3 следует, что общее уравнение n-й степени разрешимо в радикалах для любого $n \leq 4$.

6.3. * **Теорема Руффини-Абеля.** *Общее уравнение n-й степени не разрешимо в радикалах ни при каком $n \geq 5$.*

Абель фактически доказал, что если общее уравнение n-й степени разрешимо в радикалах, то x_1 выразим в радикалах. Теорему Руффини-Абеля проще всего вывести из теоремы Галуа 1.1.a.

---

[1] Мы определили свойство числа n (а не конкретного уравнения с заданными коэффициентами, как в *теореме Галуа* [ZSS, §5]).

Вот еще одна формализация понятия «найти x» для $n = 2$, которая не используется в дальнейшем: *существует ли такое отображение f из $\mathbb{R}^2$ в множество $2^{\mathbb{R}}_{fin}$ всех конечных подмножеств множества $\mathbb{R}$, что $f(x+y, xy) \ni x$ при любых $x, y \in \mathbb{R}$?* Ответ «да» на этот вопрос тривиален: определим $f(p, q)$ как (конечное) множество (вещественных) решений уравнения $t^2 + pt + q = 0$.

Определение *разрешимости в вещественных радикалах общего уравнения n-й степени* получается из его комплексного аналога заменой комплексных коэффициентов и чисел на вещественные. Ясно, что справедлив вещественный аналог утверждения 6.2. Поэтому из утверждения 3.1.a следует, что общее уравнения 2-й степени разрешимо в вещественных радикалах. Из теоремы неразрешимости в вещественных радикалах [ZSS, §5] вытекает, что общее уравнение 3-й степени не разрешимо в вещественных радикалах. Значит, ни для какого $n \geq 3$ общее уравнение n-й степени не разрешимо в вещественных радикалах.

7 Формульная выразимость с данным числом радикалов

7.1. В этой задаче имеется 4 пункта (aα), (aβ),(bα),(bβ).

(a) Корни кубического уравнения (b) Корни уравнения 4-й степени не выражаются через его коэффициенты с использованием

(α) квадратных корней. (β) кубических корней.

7.2. (a) Корни кубического уравнения выразимы через его коэффициенты с использованием одного кубического корня и одного квадратного, т.е. так, что в определении выразимости $N = 3$, $\{k_1, k_2\} = \{2, 3\}$ и $k_3 = 1$.

(*Другими словами, 'одного' означает 'однократного использования в программе'.* Например, в программе $u := \sqrt[3]{a}$, $v := u + u$ кубический корень используется один раз.)

(b) Корни уравнения 4-й степени выразимы через его коэффициенты с использованием одного кубического корня и трех квадратных.

Для подмножества $G \subset S_n$ и целого q отображение $G \to \mathbb{Z}_q$ называется *гомоморфизмом* (или *характером*), если оно переводит композицию в произведение.

7.3. (a) Если $q > 0$ целое и многочлен f^q четносимметрический, то для любой четной перестановки α существует такое

$$\chi(\alpha) \in \mathbb{Z}, \quad \text{что} \quad f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}) = \varepsilon_q^{\chi(\alpha)} f(x_1, x_2, \dots, x_n).$$

(b) Построенное в п. (a) для ненулевого f отображение

$$\chi : A_n \to \mathbb{Z}_q := \{\cos\frac{2\pi k}{q} + i \sin\frac{2\pi k}{q} \in \mathbb{C} \ : \ k \in \mathbb{Z}\},$$

из множества A_n всех четных перестановок является гомоморфизмом.

7.4. Существует ли простое q и непостоянный гомоморфизм

(a) $A_3 \to \mathbb{Z}_q$? (b) $A_4 \to \mathbb{Z}_q$?

7.5. Если $n \geq 5$ целое и $q \neq 3$ простое, то любой гомоморфизм $\chi : A_n \to \mathbb{Z}_q$ переводит каждую перестановку в 1.

7.6. (a) Выражаются ли корни кубического уравнения через его коэффициенты с использованием одного корня, т.е. так, что в определении выразимости $N = 2$ и $k_2 = 1$?

(b) Существуют ли целое q и инъективный (=взаимно-однозначный) гомоморфизм $S_3 \to \mathbb{Z}_q$?

(c) Существуют ли целые p, q и гомоморфизмы $\chi : S_4 \to \mathbb{Z}_q$ и $\varphi : \chi^{-1}(1) \to \mathbb{Z}_p$, из которых второй инъективен?

7.7. Выражаются ли корни уравнения 4-й степени через его коэффициенты с использованием

(a) одного корня? (b) двух корней? (b) трех корней?

7.8. (a) Существуют ли целые p, q и гомоморфизмы $\chi : S_4 \to \mathbb{Z}_q$ и $\varphi : \chi^{-1}(1) \to \mathbb{Z}_p$, из которых второй инъективен?

(b) Существуют ли целые p, q, r и гомоморфизмы $\chi : S_4 \to \mathbb{Z}_q$, $\varphi : \chi^{-1}(1) \to \mathbb{Z}_p$ и $\gamma : \varphi^{-1}(1) \to \mathbb{Z}_r$, из которых последний инъективен?

(c) Существуют ли цепочка из четырех гомоморфизмов, аналогичная п. (b)?

7.9. *Подгруппой* в S_n называется подмножество, замкнутое относительно операций взятия композиции и обратного элемента.

(a) Для любого многочлена $f(x_1, x_2, \dots, x_n)$ множество

$$G_f := \{\alpha \in S_n \mid f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}) = f(x_1, x_2, \dots, x_n)\}$$

является подгруппой в S_n.

(b) Перечислите все подгруппы в S_3.

(b') Какие из них могут быть прообразами единицы при гомоморфизме $S_3 \to \mathbb{Z}_q$ для некоторого q?

(c) Перечислите все подгруппы в S_4.

(c') Какие из них могут быть прообразами единицы при гомоморфизме $S_4 \to \mathbb{Z}_q$ для некоторого q?

7.10. * Выражаются ли корни кубического уравнения через его коэффициенты с использованием 'одноэтажных' извлечений корней? Т.е. извлечений корней из выражений, не содержащих корни. Т.е. так, что в определении выразимости p_k не зависит от $f_1, \dots, f_{k-1}$.

Список литературы

[A] Solving equations using one radical, presented by D. Akhtyamov, I. Bogdanov, A. Glebov, A. Skopenkov, E. Streltsova and A. Zykin, `http://www.turgor.ru/lktg/2015/4/index.htm`

[E] H.M. Edwards, The construction of solvable polynomials, Bull. Amer. Math. Soc. 46 (2009), 397-411. Errata: Bull. Amer. Math. Soc. 46 (2009), 703-704.

[M] Московская математическая конференция школьников, `http://www.mccme.ru/mmks/index.htm`.

[PSo] *Прасолов В. В.*, *Соловьев Ю. П.* Эллиптические функции и алгебраические уравнения. М.: Факториал, 1997; `http://www.mccme.ru/prasolov`.

[S] A. Skopenkov, A short elementary proof of the insolvability of the equation of degree 5, `http://arxiv.org/abs/1508.03317`

[ZSS] Математика в задачах: через олимпиады и кружки — к профессии. Под редакцией А. Заславского, А. Скопенкова и М. Скопенкова. Москва, МЦНМО, 2017. `http://www.mccme.ru/circles/oim/materials/sturm.pdf`