ПРОСТОЕ ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ РУФФИНИ О НЕРАЗРЕШИМОСТИ УРАВНЕНИЙ В РАДИКАЛАХ

А. Скопенков [1]

Теорема Руффини-Абеля о неразрешимости в радикалах — классический результат алгебры, интересный для информатики (теории символьных вычислений). В этом тексте даны четкая формулировка и простое доказательство (более слабой) теоремы Руффини. Основные идеи представлены на 'олимпиадных' примерах: на простейших частных случаях, свободных от технических деталей, и со сведением научного языка к необходимому минимуму. Для изучения этого текста достаточно знакомства с многочленами, комплексными числами и перестановками. Однако 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* [S09] и *конструктивной теории Галуа* [E]. Ср. [S, S'].

1 Формульная выразимость в вещественных радикалах

1.1. (a) Всегда ли можно, зная $x+y$ и xy, найти x?

Вот простейшая формализация понятия 'найти': *существует ли отображение* $f\colon \mathbb{R}^2 \to \mathbb{R}$, *для которого* $f(x+y, xy) = x$ *при любых* $x, y \in \mathbb{R}$*?*

(b) Всегда ли можно, зная

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

найти $(x-y)(y-z)(z-x)$? (Формализация аналогична пункту (a).)

Основное определение этого раздела — еще одна формализация понятия 'найти' (см. также сноску в начале §3). Многочлен $f \in \mathbb{R}[x_1, \dots, x_n]$ **выразим в вещественных радикалах через набор многочленов** $a_1, \dots, a_t \in \mathbb{R}[x_1, \dots, x_n]$, если f можно добавить в этот набор цепочкой операций следующего вида:

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

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

Например, если уже имеются многочлены x^2+2y и $x-y^3$, то первой операцией 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 второй операцией можно добавить многочлен $x-y$ (или $y-x$).

1.2. Выразим ли в вещественных радикалах через $x+y$ и xy многочлен x?

Ответ к задаче 1.2 показывает, что *корень квадратного уравнения выразим в вещественных радикалах через его коэффициенты.* Формализация приведена в задаче 3.1.

1.3. Выразим ли в вещественных радикалах через $\sigma_1, \sigma_2, \sigma_3$ многочлен

(a) $(x-y)(y-z)(z-x)$? (b) $x^2y+y^2z+z^2x$? (c)* x?

Ответ 'нет' к задаче 1.3.c вытекает из леммы о сохранении циклической симметричности, см. ниже. Он (и задача 3.1.b ниже) показывает, что *корень кубического уравнения не выразим в вещественных радикалах через его коэффициенты.* [2]

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

[2] Подумайте, почему это не противоречит формуле Кардано, выражающей корень кубического уравнения через его коэффициенты. Ключ к ответу — выражение дискриминанта через корни [A].

Многочлен f от переменных $x_1, x_2, \ldots, x_n$ называется **циклически симметричным**, если многочлены $f(x_1, x_2, \ldots, x_n)$ и $f(x_2, x_3 \ldots, x_{n-1}, x_n, x_1)$ равны.

1.4. Выразите $x_1x_3+x_3x_5+x_5x_7+x_7x_9+x_9x_1$ в вещественных радикалах через некоторые циклически симметричные многочлены от $x_1, x_2, \ldots, x_{10}$.

Лемма о сохранении циклической симметричности. *Если $f \in \mathbb{R}[x, y, z]$ и многочлен f^q циклически симметричен для некоторого $q > 0$, то f циклически симметричен.*

Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. In this text equality signs involving f mean equality of polynomials. Обозначим

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

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

(a) Если $f^3 = g^3$, то $f = g$. *Предостережение:* не пользуйтесь без доказательства тем, что если значения многочленов *от трех переменных* совпадают в любой точке, то эти многочлены равны (покоэффициентно).

(b) Если $fg = 0$, то $f = 0$ или $g = 0$.

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

(d) Если $f^5 = g^5$, то $f = g$.

(e) $f^5 - g^5 = (f - g)(f - \varepsilon_5 g)(f - \varepsilon_5^2 g)(f - \varepsilon_5^3 g)(f - \varepsilon_5^4 g)$.

(f) Рациональной функцией называется 'формальное отношение многочленов'. Дайте четкое определение рациональной функции. Проверьте корректность определения суммы или произведения рациональных функций (на Ваш выбор).

(g) Докажите лемму о сохранении циклической симметричности для нечетного q.

1.6. (a) Существуют функции $F, G : \mathbb{R} \to \mathbb{R}$, для которых $F^2 = G^2$, $F \neq G$, $F \neq -G$.

(b) Если $f, g \in \mathbb{R}[x, y, z]$ и $f^2 = g^2$, то $f = g$ или $f = -g$.

(c) Докажите лемму о сохранении циклической симметричности для четного q.

Подсказки

1.1. (a) Рассмотрите пары $x = 1, y = 2$ и $x = 2, y = 1$.

(b) Рассмотрите тройки $x = 0, y = 1, z = -1$ и $x = 0, y = -1, z = 1$.

1.2. (a) $(x - y)^2 = (x + y)^2 - 4xy$. (b) $x = \dfrac{x + y + (x - y)}{2}$.

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

(Пункт (a) можно также свести к (b).)

(b) Обозначим $M = x^2y+y^2z+z^2x$ и $N = y^2x+x^2z+z^2y$. Тогда многочлены $M+N$ и MN симметрические. Значит, они являются многочленами от элементарных симметрических многочленов $\sigma_1, \sigma_2, \sigma_3$. (Конкретное выражение приведено в [A].) Само же M выражается через $M + N$ и MN по формуле корней квадратного уравнения.

1.4. 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 1.3.b.

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

(c) $f^2 + fg + g^2 = \left(f + \frac{g}{2}\right)^2 + \frac{3}{4}g^2 = (f + \varepsilon_3 g)(f + \varepsilon_3^2 g)$,

1.5.g, 1.6.c. Обозначим $g(x, y, z) := f(y, z, x)$. Так как f^q циклически симметричен, то $f^q = g^q$.

Если q нечетно, то $f = g$, значит, f циклически симметричен. А если q четно, то $f = g$ или $f = -g$. (Для $q = 2, 3, 5$ детали доказательства приведены в предыдущих пунктах.)

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 симметричен.

2 Формульная выразимость в комплексных радикалах

Определение **выразимости в (комплексных) радикалах** получается из его вещественного аналога (§1) заменой вещественных коэффициентов на комплексные.

2.1. Решите комплексный аналог задачи 1.2.

2.2. (a-g) Справедливы ли комплексные аналоги утверждений 1.5?

2.3. (a) Найдите $\alpha, \beta \in \mathbb{C}$, для которых многочлен $(x + y\alpha + z\beta)^3$ циклически симметричен.

(b) Решите комплексный аналог задачи 1.3.c.

2.4. Выразим ли в радикалах многочлен (a) $xy + zt$; (b) $x + y - z - t$; (c) x через $x + y + z + t$, $xy + xz + xt + yz + yt + zt$, $xyz + xyt + xzt + yzt$, $xyzt$?

2.5. Выразим ли в радикалах через элементарные симметрические многочлены от 5 переменных $x_1, \dots, x_5$ многочлен

(a) $\Pi_{j<k}(x_j - x_k)$; (b)* $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$; (c)* x_1.

Ответ в задачах 2.5.bc — нет!

2.6. Теорема Руффини. *Для любого $n \geq 5$ многочлен x_1 не выразим в радикалах через элементарные симметрические многочлены от n переменных $x_1, \dots, x_n$.*

Чтобы придумать основную идею, докажем следующие более простые факты.

2.7. Многочлен x не выражается через многочлены

(a) $x + y, xy$ *рационально*, т.е. без применения второй операции в определении выразимости.

(b) $\sigma_1, \sigma_2, \sigma_3$ от x, y, z *квадратично*, т.е. так, что вторая операция в определении выразимости применяется только для $k = 2$. *Подсказка:* см. утверждение 2.8.a.

(c)* $\sigma_1, \sigma_2, \sigma_3$ от x, y, z *кубично*, т.е. так, что вторая операция в определении выразимости применяется только для $k = 3$.

2.8. (a) Если $f \in \mathbb{C}[x, y, z]$ — многочлен и многочлен f^2 циклически симметричен, то f циклически симметричен.

(b) Верен ли аналог пункта (a) для 4 переменных? А для 5 переменных?

A permutation α is *even* if it is a composition of an even number of transpositions. Многочлен $f \in \mathbb{C}[x_1, \dots, x_n]$ называется **четносимметрическим**, если для любой четной перестановки α многочлены $f(x_1, x_2, \dots, x_n)$ и $f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)})$ равны.

2.9. Придумайте многочлен циклически симметричный, но не четносимметрический.

Теорема Руффини 2.6 вытекает из утверждения 2.10.a.

2.10. Пусть $f \in \mathbb{C}[x_1, \dots, x_n]$ — многочлен.

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

(b) Если для некоторого целого $n \geq 3$ многочлен f^2 четносимметрический, то f четносимметрический.

(c) Если $q > 0$ целое и многочлен f^q четносимметричен, то для любой четной перестановки α существует такое $\chi(\alpha) \in \mathbb{Z}$, что $f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}) = \varepsilon_q^{\chi(\alpha)} f(x_1, x_2, \dots, x_n)$.

(d) Если для некоторых целого $n \geq 3$ и простого $q \neq 3$ многочлен f^q четносимметрический, то f четносимметрический.

2.11. Определение *рациональной выразимости в вещественных (комплексных) радикалах через рациональные функции* $a_1, \dots, a_t$ аналогично определению выразимости. Выразим ли рационально

(a) многочлен x в вещественных радикалах через многочлены $\sigma_1, \sigma_2, \sigma_3$ от x, y, z?

(b) многочлен x_1 в комплексных радикалах через многочлены $\sigma_1, \dots, \sigma_5$ от $x_1, \dots, x_5$?

Подсказки

2.3. $x + y\varepsilon_3 + z\varepsilon_3^2$.

3 Разрешимость уравнений в радикалах

Общее уравнение n-й степени разрешимо в вещественных радикалах, если существуют

• неотрицательные целые 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,

такие, что если $a_0, \dots, a_{n-1}, x \in \mathbb{R}$ и

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

то существуют $f_1, \dots, f_s \in \mathbb{R}$, для которых

$$f_1^{k_1} = p_0(a_0, \dots, a_{n-1}), \quad f_2^{k_2} = p_1(a_0, \dots, a_{n-1}, f_1), \quad \dots$$

$$\dots \quad f_s^{k_s} = p_{s-1}(a_0, \dots, a_{n-1}, f_1, \dots, f_{s-1}), \quad x = p_s(a_0, \dots, a_{n-1}, f_1, \dots, f_s).$$

Обратите внимание, что мы определили свойство числа n (а не конкретного уравнения с заданными коэффициентами, как в *теореме Галуа* [S]). [3]

3.1. (a) Общее уравнение 2-й степени разрешимо в вещественных радикалах.

(b)* Общее уравнение 3-й степени не разрешимо в вещественных радикалах

(c)* То же самое для всех $n \geq 3$.

Результат задач 1.3.c и 3.1.b (а также его сравнение с формулой Кардано) показывает, что определение выразимости в вещественных радикалах не совсем удачно формализует идею разрешимости в радикалах. С одной стороны, вместо вещественных чисел разумнее рассматривать комплексные [S']. С другой стороны, вместо работы с многочленами можно работать с числами — это приводит к теореме Галуа [S]. Однако на примере этой не совсем удачной формализации Вы увидели идею доказательства теоремы Руффини, см. [S'].

Определение **разрешимости в (комплексных) радикалах общего уравнения n-й степени** получается из его вещественного аналога заменой вещественных коэффициентов и чисел на комплексные.

3.2. (a,b) Справедливы ли комплексные аналоги утверждений 3.1.ab?

(c,d) Общие уравнения 3-й и 4-й степени разрешимы в радикалах.

(e) Если x_1 выражается в радикалах через элементарные симметричные многочлены

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

[3] Вот другая формализация понятия 'найти', который 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 $f(x+y, xy) \ni x-y$ при любых $x, y \in \mathbb{R}$?* Поясним, почему этот вопрос (и даже его обобщения на несколько переменных) тривиален.

Отображения $f\colon \mathbb{R}^2 \to 2^{\mathbb{R}}_{fin}$ (т.е. вещественные конечнозначные функции) можно задавать формулами. Например, формула $f(x) = \pm x$ является сокращением формулы $f(x) = \{x, -x\}$, задающей (не более, чем) двузначное отображение f. (Подумайте, сколько значное отображение задает формула $f(x) = \frac{\pm x}{\pm x}$.) Обозначим через $f(p,q)$ (конечное) множество (вещественных) решений уравнения $t^2 + pt + q = 0$. Тогда формула $x - y = f(x+y, xy) - f(x+y, xy)$ задает искомое отображение (подумайте, как!).

то общее уравнение n-й степени разрешимо в радикалах.

3.3. * (a) **Теорема Абеля.** *Если общее уравнение n-й степени разрешимо в радикалах, то x_1 выразим в радикалах через элементарные симметричные многочлены.*

(b) **Теорема Руффини-Абеля.** *Общее уравнение n-й степени не разрешимо в радикалах при любом $n \geq 5$.*

Подсказки

3.1. (a) Возьмите

$$s = 1, \quad k_1 = 2, \quad p_0(y_0, y_1) = y_1^2 - 4y_0, \quad p_1(y_0, y_1, z_1) = \frac{z_1 - y_1}{2} \quad \text{и} \quad f_1 = 2x + a_1.$$

Проверьте, что $f_1^2 = p_0(a_0, a_1)$ и $x = p_1(a_0, a_1, f_1)$.

4 Формульная выразимость с данным числом радикалов

4.1. 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.

4.2. (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.

4.3. Построенное в задаче 2.10.c 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.

4.4. Существует ли простое q и непостоянный гомоморфизм

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

4.5. 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.

4.6. (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?

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

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

4.8. (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)?

4.9. *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?

4.10. * 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`.

[S09] A. Skopenkov, Philosophical and methodical appendix, in: Mathematics as a sequence of problems, Ed. A. Zaslavsky, D. Permyakov, A. Skopenkov, M. Skopenkov, A. Shapovalov, MCCME, Moscow, 2009.

[S] A. Skopenkov, Some more proofs from the Book: solvability and insolvability of equations in radicals, `www.mccme.ru/circles/oim/kroneck.pdf`, `http://arxiv.org/abs/0804.4357`

[S'] A. Skopenkov, A short elementary proof of the Ruffini-Abel Theorem, `http://arxiv.org/abs/1508.03317`