К алгоритмам решения алгебраических уравнений

А. Скопенков *

Содержание

1 Единственность способа решения квадратного уравнения 2
2 Решаем уравнения: метод резольвент Лагранжа 3
3 «Вещественная» неразрешимость кубического уравнения 4
Подсказки, указания и решения 5
4 Неразрешимость уравнения 5-й степени «в многочленах» 6
5 Обобщение: функции вместо многочленов 7
6 Формульная выразимость с данным числом радикалов 8
7 Лемма о последнем радикале 9

Теорема Руффини-Абеля о неразрешимости алгебраических уравнений в радикалах — классический результат алгебры, интересный для информатики (теории символьных вычислений). В этом тексте даны ее четкая формулировка и простое доказательство. Чтобы доказывать неразрешимость алгебраических уравнений, мы (вслед за Галуа) придумаем общий способ их решения. Этим же 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, текст начинается с нетривиальных задач о квадратных и кубических уравнениях.

Для изучения этого текста достаточно знакомства с многочленами, комплексными числами и перестановками. При этом спецкурс 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].

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

Мы следуем традиции изучения материала в виде решения и обсуждения задач, см. подробнее [ZSS, п. 1.2 и §26]. К важнейшим задачам приводятся подсказки, указания,

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

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 её утверждение важное.

Номера задач обозначаются жирным шрифтом. Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. *Загадкой* называется не сформулированный чётко вопрос; здесь нужно придумать и чёткую формулировку, и доказательство. Наиболее трудные задачи отмечены звёздочкой *.

1 Единственность способа решения квадратного уравнения

1.1. (Загадка) (a) Всегда ли можно, зная $x+y$ и xy, найти x? Здесь требуется прежде всего придумать формализацию понятия «найти». Вот простейшая формализация: *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 п. (a).)

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 «выражают» (в некотором, строго определенном в п. 2) x через коэффициенты $x+y, xy$ квадратного уравнения.

1.2. *Единственность способа решения квадратного уравнения.* (a) Если для многочленов $f(x,y)$, $p(u,v)$ и $q(u,v,w)$ с вещественными коэффицентами выполнено

$$f^2(x,y) = p(x+y, xy) \quad \text{и} \quad x = q\left(x+y, xy, f(x,y)\right),$$

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

(b) Пусть $k > 0$ целое, $f(x,y)$, $p(u,v)$ и $q(u,v,w)$ — многочлены с вещественными коэффициентами, причем

$$f^k(x,y) = p(x+y, xy) \quad \text{и} \quad x = q(x+y, xy, f(x,y)).$$

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

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

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

Условию утверждения 1.2.a удовлетворяют, например, многочлены

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

Для доказательства утверждения 1.2.b полезны следующие понятия и лемма.

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

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

(b) **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.

Предостережение: не пользуйтесь без доказательства тем, что если значения многочленов *от двух переменных* совпадают в любой точке, то эти многочлены равны.

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

(d) 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 полезны следующие задачи.

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

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

(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 $\varepsilon_5 := \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$.

Обобщение утверждений 1.2 на любое количество шагов формализуется задачей 7.1, для решения которой нужны новые идеи.

1.5. Для каких из утверждений 1.2, 1.3.bcd, 1.4 справедливы их аналоги для многочленов с комплексными коэффициентами?

2 Решаем уравнения: метод резольвент Лагранжа

Обозначим

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

Число n ясно из контекста и пропускается из обозначений.

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

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

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

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 $y-x$).

Задача 1.2.b показывает, что корень x квадратного уравнения выразим в радикалах.

Выразимость в радикалах равносильна существованию таких

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

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

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

В этих равенствах мы опускаем переменные $(x_1,\dots,x_n)$ многочленов $\sigma_1,\dots,\sigma_n,f_1,\dots,f_s$; равенства являются равенствами многочленов.

2.1. Выразим ли в радикалах для $n=3$ многочлен

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

Подсказкой к (c) является следующая задача.

2.2. Многочлен $f \in \mathbb{R}[x_1, x_2, \dots, x_n]$ называется *циклически симметричным*, если $f(x_1, x_2, \dots, x_n) = f(x_2, x_3 \dots, x_{n-1}, x_n, x_1)$.

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

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

2.3. Выразим ли в радикалах для $n = 4$ многочлен

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

См. [ZSS, п. 5.3.2 «метод резольвент Лагранжа»].

Оказывается, для $n = 5$ многочлен x_1 не выразим в радикалах.

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

Теорема Руффини вытекает из леммы 4.4.a (о сохранении четносимметричности).

3 «Вещественная» неразрешимость кубического уравнения

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

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

(a) $f^2 = p(\sigma_1, \sigma_2, \sigma_3)$ и $x = q(\sigma_1, \sigma_2, \sigma_3, f)$. (b) $f^3 = p(\sigma_1, \sigma_2, \sigma_3)$ и $x = q(\sigma_1, \sigma_2, \sigma_3, f)$.

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

3.2. Если $f \in \mathbb{R}[x, y, z]$ и многочлен

(a) f^3; (b) f^2

циклически симметричен, то f циклически симметричен.

3.3. 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

$$f_1^2 = p_0(\sigma_1, \sigma_2, \sigma_3), \quad f_2^3 = p_1(\sigma_1, \sigma_2, \sigma_3, f_1), \quad x = p_2(\sigma_1, \sigma_2, \sigma_3, f_1, f_2).$$

Обобщение утверждения 3.3 на любое количество шагов формализуется определением *выразимости в вещественных радикалах*, которое получается из его комплексного аналога (§2) заменой комплексных коэффициентов на вещественные.

3.4. Выразим ли в вещественных радикалах через $\sigma_1, \sigma_2, \sigma_3$ многочлен x?

Ответ «нет» к задаче 3.4 показывает, что *корень кубического уравнения не выразим в вещественных радикалах через его коэффициенты*. Этот ответ вытекает из следующей леммы.

3.5. 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.

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

Подсказки, указания и решения

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. (b) Индукция по k с применением п. (a) и лемм 1.3.bc.

1.3. (b) Так как f^2 симметричен, то $f(x, y)^2 = f(y, x)^2$ откуда по утверждению 1.4.b $f(x, y) = \pm f(y, x)$.

(c) Используйте аналог утверждений 1.4.ce.

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

1.4. (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) См. указание к 1.3.d.

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 перед задачей 1.2.

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.

3.5. 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 $f = -g$. 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.

3.6. Аналог утверждения 3.4 неверен, см. формулу Кардано 2.1.c, выражающую корень кубического уравнения через его коэффициенты. Подумайте, почему это утверждение не противоречит формуле Кардано. Ключ к ответу — выражение дискриминанта через корни [A]. См. также другую формализацию в п. 5.

4 Неразрешимость уравнения 5-й степени «в многочленах»

Чтобы придумать идею доказательства теоремы Руффини 2.4, докажем следующие более простые факты.

4.1. 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 4.2.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 $k = 3$.

4.2. (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.

4.3. Придумайте многочлен циклически симметричный, но не четносимметрический.

Обозначим

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

4.4. 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 многочлен f^2 четносимметрический, то f четносимметрический.

(c) Любая четная перестановка разлагается в произведение циклов длины 3.

(d) Если для некоторого целого $n \geq 5$ многочлен f^3 четносимметрический, то f четносимметрический.

(e) При любом $n \geq 5$ цикл длины 3 разлагается в произведение циклов длины 5.

Лемма (a) и ее «частные случаи» (b,d) вытекают из (c,e), см. детали в [S].

4.5. *Рациональной функцией* называется пара $f/g := (f, g)$ многочленов, в которой $g \neq 0$, с точностью до следующей эквивалентности: $f/g \sim f'/g'$ при $fg' = f'g$.

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

(b) Определение *рациональной выразимости в вещественных (комплексных) радикалах через рациональные функции* $a_1, \dots, a_t$ аналогично определению выразимости. Выразим ли рационально многочлен x в вещественных радикалах через многочлены $\sigma_1, \sigma_2, \sigma_3$ от x, y, z?

(c) Выразим ли рационально многочлен x_1 в комплексных радикалах через многочлены $\sigma_1, \dots, \sigma_5$ от $x_1, \dots, x_5$?

5 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]

5.1. 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.

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

Из утверждений 5.2, 1.2.a и результатов задач 2.1, 2.3 следует, что общее уравнение n-й степени разрешимо в радикалах для любого $n \leq 4$.

5.3. * (a) **Теорема Абеля.** *Если общее уравнение n-й степени разрешимо в радикалах, то x_1 выразим в радикалах.*

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

Простое доказательство теоремы Абеля приведено в [S].

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 5.2. Поэтому из утверждения 1.2.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.

5.4. Ни для какого $n \geq 3$ общее уравнение n-й степени не разрешимо в вещественных радикалах.

---

[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 $t^2 + pt + q = 0$.

6 Формульная выразимость с данным числом радикалов

6.1. 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.

6.2. (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.

6.3. (a) Если $q > 0$ целое и многочлен f^q четносимметричен, 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.

6.4. Существует ли простое q и непостоянный гомоморфизм

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

6.5. 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.

6.6. (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?

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

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

6.8. (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)?

6.9. *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?

6.10. * 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 $f_1, \dots, f_{k-1}$.

7 Лемма о последнем радикале

Вещественной руффиниевой радикальной формулой называется цепочка операций из определения выразимости в радикалах многочлена x_1 через многочлены $\sigma_1, \dots, \sigma_n$. Иными словами, вещественной руффиниевой радикальной формулой называется набор

- целых положительных чисел $s, k_1, \dots, k_s$,
- многочленов $f_1, \dots, f_s$ и $p_0, p_1, \dots, p_s$ с вещественными коэффициентами от 2 и от $2, 3, \dots, s+2$ переменных соответственно,

для которых справедливы равенства из задачи 5.1.(2).

Решение задачи 1.2.a показывает, что такая формула существует. (Иными словами, квадратное уравнение разрешимо по Руффини в вещественных радикалах. Еще одна формализация приведена в задаче 5.4.)

7.1. (a) Возьмем вещественную руффиниеву радикальную формулу для решения квадратного уравнения, которая *минимальна*, т.е. многочлен f_j^k не представляется в виде многочлена от $x+y, xy, f_1, \dots, f_{j-1}$ ни для каких $j = 1, \dots, s$ и $k < k_s$. Тогда $s = 1$, $k_1 = 2$ и существуют многочлены $a, b \in \mathbb{R}[u, v]$, для которых $f(x,y)b(x+y, xy) = (x-y)a(x+y, xy)$.

(b) Сформулируйте и докажите аналог п. (a) с заменой многочленов $f_1, \dots, f_s$ на функции $\mathbb{R}^2 \to \mathbb{R}$.

7.2. 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»].

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`.

[S] A. Skopenkov, A short elementary proof of the Ruffini-Abel Theorem, `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`