К алгоритмам решения алгебраических уравнений

представляют Б. Вукорепа, А. Глебов,
А. Еннэ, А. Скопенков, А. Чиликов *

1 Введение и формулировки результатов

1.1 О чём этот цикл задач

Знаменитые теоремы[1] Руффини 2.7, Абеля и Галуа 1.3, 1.4 о неразрешимости алгебраических уравнений в радикалах — классический результат алгебры, интересный для информатики (теории символьных вычислений). Формулировки этих теорем приведены ниже.

Основное содержание данного текста — изложение глубоких идей алгебры (точнее, теории Галуа) на красивых простых доказательствах этих теорем, см. [ZSS, § 27]. Замечательно, что при этом для понимания приводимых доказательств достаточно уметь делить многочлены с остатком, извлекать корни из комплексных чисел, умножать перестановки и решать системы линейных уравнений. И тот, кто не дойдёт до полного доказательства основных резуль-

*Благодарим Я. Абрамова, Д. Елисеева, А. Канунникова, О. Орел, А. Петухова, Н. Хорошавкину, Г. Челнокова и жюри ЛКТГ за обсуждения и перевод частей текста.

Б. Вукорепа: Загребский Университет. *А. Глебов:* Новосибирский Государственный Университет. *А. Еннэ:* Петрозаводский Государственный Университет. *А. Скопенков:* Московский Физико-Технический Институт, Независимый Московский Университет. `http://www.mccme.ru/~skopenko`. *А. Чиликов:* Московский Государственный Технический Университет им. Баумана, Московский Физико-Технический Институт.

[1] Из §1 далее используется только §1.5, можно сразу перейти к нему и решению задач.

татов, сможет порешать задачи для исследования, см. [E2, Es, AB, Ko17, Saf] и ссылки в этих работах.

Перед доказательствами неразрешимости 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 же методом строятся и алгоритмы — например, распознаваемости разрешимости уравнений в радикалах.

Для практики приближённые методы решения уравнений более полезны, чем радикальные формулы. Кроме того, уравнения можно решать при помощи трансцендентных функций (см. метод Виета [ZSS, п. 4.2] и [PSo]). Однако проблема разрешимости в радикалах интересна как пробная задача современных теорий символьных вычислений и сложности вычислений.

О новизне. Приводимые в решениях доказательства не претендуют на новизну (хотя, возможно, читатели сумеют придумать что-то новое). Все же в этом тексте имеется много методических находок, см. [ZSS, п. 5.2.1, 5.2.2], и доказательства отличны от приведенных и цитированных в [ZSS, §5]. Однако, к сожалению, приводимые доказательства малоизвестны. Как следствие, малоизвестно, что не только решать квадратные и кубические уравнения, но и доказывать указанные теоремы экономнее, не строя и затем применяя теорию Галуа (как, например, в стандартных учебниках по алгебре), а напрямую [2] — но при этом, конечно, переоткрывая и используя базовые идеи этой теории.

[2] Как, например, в [Dor, §25], [Pr07-2, дополнение 8], [FT, Лекция 5], [ZSS, §5], [Dor, St94, Kol, Ler, T, Sk11, Sk15] и здесь. Изложение в [Al] ближе к этому стилю. Хотя большая часть [Al] посвящена изложению теории, не нужной для доказательства ослабленной версии теоремы Абеля, объявленной в качестве основного результата (см. [Sk15, конец замечания 7]), автору книги [Al] удалось избежать немотивированного изложения части этой теории. Доказательство из [Al] более коротко и понятно изложено в [FT, Лекция 5] и, возможно, в [Sk11]. Заметим, что доказательства в большинстве этих источников неполны, см. [ZSS, сноска 12 на стр. 113 и конец §5.5.4], [Sk15, Обсуждение]. Несмотря на эти недостатки, вышеупомянутые элементарные изложения были для нас полезнее, чем формальные изложения (в стандартных учебниках, излагающих теории), которые начинаются с нескольких сотен страниц определений и следствий, роль которых в доказательстве теоремы о неразрешимости неясна на момент их формулировки. Немотивированное изложение служит «главным образом для

1.2 Неразрешимость в вещественных радикалах

Вещественное число называется **вещественно радикальным**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений корней целых положительных степеней из положительных чисел. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству $M \subset \mathbb{R}$, содержащему числа x, y,

$$\text{чисел} \quad x+y, x-y, xy, \quad \text{числа } x/y \text{ при } y \neq 0$$

$$\text{и числа } \sqrt[n]{x} \text{ при } x > 0 \text{ и целом } n > 0.$$

Вещественная радикальность числа α равносильна существованию таких

- целых положительных чисел $s, k_1, \ldots, k_s$,
- вещественных чисел $f_1, \ldots, f_s$ и многочленов $p_0, p_1, \ldots, p_s$ от $0, 1, \ldots, s$ переменных, соответственно, с рациональными коэффициентами, что

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

Замечание 1.1. (a) Любой вещественный корень квадратного уравнения с рациональными коэффициентами вещественно радикален.

(b) Уравнение $x^3 + x + 1 = 0$ имеет ровно один вещественный корень, который вещественно радикален [ZSS, п. 4.2], см. также задачу 2.8 (c).

(c) Уравнение $x^4 + 4x - 1 = 0$ имеет два вещественных корня, каждый из которых вещественно радикален [ZSS, п. 4.2], см. также задачу 2.10 (d).

того, чтобы затруднить непосвященным овладение своей наукой и тем самым повысить ее авторитет» [Ar84, стр. 49]. Заметим, что для многих именно *мотивированное* изложение повышает авторитет математики.

(d) Любое вещественно построимое число [ZSS, п. 5.1.2] вещественно радикально.

(e) Существует многочлен 3-й степени с рациональными коэффициентами (например, x^3-3x+1), ни один из корней которого не является вещественно радикальным. (Это доказано в п. (f).)

(f) Число $\cos(2\pi/9)$ не является вещественно радикальным.

Действительно, по формуле косинуса тройного угла каждое из чисел $\cos(2\pi/9)$, $\cos(8\pi/9)$, $\cos(14\pi/9)$ удовлетворяет уравнению $8y^3-6y+1=0$. По нижеприведенной теореме 1.2 ни одно из них не является вещественно радикальным.

(g) Трисекция угла невозможна при помощи вещественных радикалов, т.е. существует такое α (например, $\alpha=2\pi/3$), что число $\cos\alpha$ вещественно радикально, а число $\cos(\alpha/3)$ — нет. (Это следует из п. (f).)

Теорема 1.2 (о разрешимости в вещественных радикалах)**.** Следующие условия на многочлен f третьей степени с рациональными коэффициентами равносильны:

(i) многочлен f имеет либо хотя бы один рациональный корень, либо ровно один вещественный корень;

(ii) многочлен f имеет вещественно радикальный корень;

(iii) все вещественные корни многочлена f вещественно радикальны.

Единственность вещественного корня «укороченного» уравнения $x^3+px+q=0$ равносильна условию «$p=q=0$ или $(p/3)^3+(q/2)^2>0$» [ZSS, задача 8.1.5.d].

Равносильность $(ii)\Leftrightarrow(iii)$ очевидна и следует из замечания 1.1.a. Разрешимость в теореме 1.2 (т.е. $(i)\Rightarrow(ii)$) доказывается *методом дель Ферро* [ZSS, п. 4.2]; см. другое доказательство в п. 2.3. Неразрешимость в теореме 1.2 (т.е. $(ii)\Rightarrow(i)$) доказывается сложнее. Более просто доказывается аналогичный результат о *неразрешимости в многочленах*, см. п. 2.5.

1.3 Неразрешимость в комплексных радикалах

Перейдём к формулам, которые могут содержать комплексные числа. Оказывается, кубическое уравнение (например, x^3-3x+1), не-

разрешимое в вещественных радикалах, разрешимо в комплексных.

Комплексное число называется (комплексно) **радикальным**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений корней целых положительных степеней. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству M, содержащему числа x, y,

$$\text{чисел } x+y, x-y, xy, \quad \text{числа } x/y \text{ при } y \neq 0$$

и любого такого числа $r \in \mathbb{C}$, что $r^n = x$ для некоторого целого $n > 0$.

Например, любой (комплексный) корень квадратного уравнения с рациональными коэффициентами является радикальным. Аналогичные утверждения справедливы для уравнений 3-й и 4-й степени. Они доказываются *методами дель Ферро и Феррари* [ZSS, п. 4.2]; см. другое доказательство в п. 2.3. Однако аналог этих утверждений для более высоких степеней неверен.

Теорема 1.3 (Галуа)**.** Существует уравнение 5-й степени с рациональными коэффициентами (например, $x^5 - 4x + 2 = 0$), ни один из корней которого не является радикальным.

Знаменитую проблему о разрешимости уравнений в радикалах решили доказанные немного ранее более слабые теоремы Руффини–Абеля. Теорема Руффини 2.7 сложнее формулируется, но подводит нас к доказательству теоремы Галуа. Четкая формулировка теоремы Абеля еще более сложна и здесь не приводится, см. [Sk15, Замечание 7]. Экономнее решить проблему разрешимости, доказав следующую теорему Галуа (более слабую и более просто доказываемую, чем теорема Галуа 1.3). Для $X \subset \mathbb{C}$ комплексное число называется *X-радикальным*, если его можно получить из множества $X \cup \{1\}$ при помощи операций из определения радикальности.

Теорема 1.4 (Галуа)**.** Существуют такие $a_0, a_1, a_2, a_3, a_4 \in \mathbb{C}$, что ни один корень уравнения $x^5 + a_4x^4 + \ldots + a_1x + a_0 = 0$ не является $\{a_0, a_1, \ldots, a_4\}$-радикальным.

Теорема 1.5. Существует алгоритм, определяющий для данных $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$, все ли корни уравнения $x^n + a_{n-1}x^{n-1} + \ldots +$

$a_1x + a_0 = 0$ радикальны.

Теорема 1.5 доказывается при помощи критерия разрешимости Галуа 2.13.b и оценки на число операций.

1.4 План

Этот проект распадается на три формально независимых куска (в первых двух используется определение радикальности из п. 2.2).

(1) В п. 2.3 обсуждается метод (резольвент Лагранжа) решения уравнений. Формально он не используется в доказательствах неразрешимости. Однако знакомство с ним будет полезно, поскольку доказательства неразрешимости были придуманы при анализе этого метода, поскольку это знакомство поможет контролировать правильность промежуточных гипотез, возникающих при доказательствах неразрешимости, и поскольку этот метод нужен для доказательства теоремы 1.5.

(2) Доказательство теоремы Руффини 2.7 основано на идее симметрии и намечено в п. 3.1. К нему подводит п. 2.5. П. 2.4 подводит и к п. 2.5, и к доказательству теоремы Галуа 1.4.

(3) Доказательство теоремы 1.2 о разрешимости в вещественных радикалах основано на идее сопряжения (или алгебраической симметрии). К нему подводят п. 2.1, 3.2 и 3.3.

Теоремы 1.3 и 1.5 не доказываются в этом тексте, см. доказательство первой в [ZSS, §5], [Sk19, §9]. Теорема Галуа 1.4 доказывается в дополнительных задачах, ср. [Sk15, Sk19], при помощи редукции к теореме Руффини 2.7, использующей идею сопряжения (п. 2.1, 3.2 и 3.3).

1.5 Рекомендации участникам

Участник (или группа участников) конференции, решающий задачи проекта, получает «боб» за каждое *записанное* решение, оцененное в «+» или «+.». Дополнительные бобы могут выдаваться за красивые решения, решения сложных проблем, или оформление некоторых решений в системе TEX. У жюри бесконечно много бобов. Решения можно сдавать и устно, отдавая один боб за каждые пять попыток (неважно, удачных или нет).

Если задача выделена словом «теорема» («лемма», «следствие» и т. д.) и жирным шрифтом, то её утверждение более важное. Как правило, мы приводим (в виде задачи) *формулировку* красивого или важного утверждения *перед* его *доказательством*. В таких случаях для доказательства утверждения могут потребоваться последующие задачи. Если Вы застряли на какой-то другой задаче, также перейдите к следующим, они могут помочь.

Приглашаем Вас обсуждать с жюри возникающие вопросы. Особо успешным решателям мы выдаем *дополнительные задачи* для исследования.

Пожалуйста, сообщите нам, если Вы знаете решения каких-то из предложенных задач. Если Вы подтвердите свои знания, сообщив нам решения некоторых из них, Вам будет разрешено не получать плюсы по всем этим задачам, но пользоваться ими при решении остальных.

2 Задачи до промежуточного финиша

В этом тексте равенства, включающие многочлен f (или f_j) означают равенство многочленов (покоэффициентное). В п. 2.1, 3.2 и 3.3 «многочлен с рациональными коэффициентами» коротко называется многочленом. Обозначим

$$\varepsilon_q := \cos(2\pi/q) + i\sin(2\pi/q).$$

2.1 Одно извлечение квадратного корня

2.1. Представимо ли следующее число в виде $a+\sqrt{b}$, где $a, b \in \mathbb{Q}$:
(a) $\sqrt{3+2\sqrt{2}}$; (b) $\frac{1}{7+5\sqrt{2}}$; (c) $\sqrt[3]{7+5\sqrt{2}}$; (d) $\cos(2\pi/5)$;
(e) $\sqrt[3]{2}$; (f) $\sqrt{2}+\sqrt[3]{2}$; (g) $\cos(2\pi/9)$;
(h)* $\sqrt{2+\sqrt{2}}$; (i)* $\cos(2\pi/7)$; (j) $\sqrt{2}+\sqrt{3}+\sqrt{5}$.

Лемма 2.2. Пусть $r \in \mathbb{R}-\mathbb{Q}$ и $r^2 \in \mathbb{Q}$.

(a) **О неприводимости.** Многочлен x^2-r^2 неприводим над $\mathbb{Q}$.

(b) **О линейной независимости.** Если $a, b \in \mathbb{Q}$ и $a+br=0$, то $a=b=0$.

(c) Если многочлен имеет корень r, то этот многочлен делится на x^2-r^2.

(d) **О сопряжении.** Если многочлен имеет корень r, то корнем этого многочлена является также число $-r$.

(e) **О сопряжении.** Если $a, b \in \mathbb{Q}$ и многочлен имеет корень $a + br$, то корнем этого многочлена является также число $a - br$.

(f) Если $a, b \in \mathbb{Q}$ и кубический многочлен имеет корень $a + br$, то он имеет рациональный корень.

Теорема 2.3. Если многочлен степени выше второй неприводим над $\mathbb{Q}$, то ни один из его корней не представим в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$.

Лемма 2.4 (о расширении)**.** Пусть число можно получить из числа 1 при помощи нескольких операций сложений, вычитаний, умножений, делений на ненулевые числа, и одной операции извлечения квадратного корня из положительного числа (т.е. число вещественно построимо с извлечением корня только один раз). Тогда оно имеет вид $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$ и $b > 0$.

2.5.* Для каких n число $\cos(2\pi/n)$ представимо в виде $a + \sqrt{b}$, где $a, b \in \mathbb{Q}$?

Подсказки к п. 2.1

2.2. (a) Если многочлен $x^2 - r^2$ приводим над $\mathbb{Q}$, то он имеет рациональный корень. Противоречие.

(b) Если $b \neq 0$, то $r = -a/b \in \mathbb{Q}$, что невозможно. Поэтому $b = 0$, а значит, $a = 0$.

(c) Поделим многочлен с остатком[3] на $x^2 - r^2$:

$$P(x) = (x^2 - r^2)Q(x) + mx + n.$$

Подставляя $x = r$, по лемме о линейной независимости (см. п. (b)) получаем, что остаток нулевой.

(d) Из п. (c) следует, что если $R^2 = r^2$, то R есть корень многочлена.

Указание к другому решению. Отображение $u \mapsto \overline{u}$ множества $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}$ в себя корректно определено формулой $\overline{a + br} := a - br$. Кроме того, $\overline{u + v} = \overline{u} + \overline{v}$ и $\overline{u \cdot v} = \overline{u} \cdot \overline{v}$ для любых $u, v \in \mathbb{Q}[\sqrt{2}]$.

[3] Это деление с остатком — то же самое, что «замена» x^2 на r^2.

(e) Обозначим через P многочлен из условия, и пусть $G(t){:=}P(a+bt)$. Тогда $G(r)=0$. Значит, по пункту (d) имеем $G(-r)=0$.

(f) Если $b=0$, то утверждение доказано. В противном случае по п. (e) многочлен имеет (различные) корни $a\pm br$, значит третий корень рационален по теореме Виета.

2.4. Было бы достаточно доказать, что множество чисел такого вида замкнуто относительно сложения, вычитания, умножения и деления. Это, естественно, не так: $(1+\sqrt{2})+(1+\sqrt{3})$ не представимо в виде $a\pm\sqrt{b}$, где $a,b\in\mathbb{Q}$ (докажите!).

2.2 Определение радикальности многочлена

Решение квадратного уравнения $t^2+bt+c=0$ можно выразить формулами

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

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

Обозначим элементарные симметрические многочлены

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

Если число n и аргументы $x_1,\dots,x_n$ ясны из контекста, то они пропускаются из обозначений.

Многочлен $p\in\mathbb{C}[x_1,\dots,x_n]$ называется (комплексно) **радикальным** если p можно добавить в набор $\{\sigma_1,\dots,\sigma_n\}\cup\mathbb{C}$ многочленов цепочкой операций следующего вида:

- добавить в набор сумму или произведение уже имеющихся многочленов;
- если многочлен из набора равен f^k для некоторых $f\in\mathbb{C}[x_1,\dots,x_n]$ и целого $k>1$, то добавить в набор многочлен f.

Замечание 2.6. (a) Например, к многочленам x^2+2y и $x-y^3$ операциями первого типа можно добавить многочлен $-5(x^2{+}2y)^2+3(x^2+2y)(x-y^3)^6$. А к многочлену $x^2-2xy+y^2$ операцией второго типа можно добавить многочлен $x-y$ (или $y-x$).

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

(c) По теореме Виета $\sigma_1, \ldots, \sigma_n$ есть коэффициенты многочлена

$$t^n - \sigma_1 t^{n-1} + \ldots + (-1)^{n-1}\sigma_{n-1}t + (-1)^n\sigma_n \in \mathbb{C}[x_1, \ldots, x_n][t]$$

с корнями $x_1, \ldots, x_n$. Поэтому радикальность многочлена x_1 равносильна выразимости (в указанном смысле) через коэффициенты этого многочлена его корня x_1.

(d) Радикальность многочлена x_1 равносильна существованию таких

- целых положительных чисел $s, k_1, \ldots, k_s$,
- многочленов $f_1, \ldots, f_s$ от n переменных и $p_0, p_1, \ldots, p_s$ от $n, n+1, \ldots, n+s$ переменных, соответственно, с комплексными коэффициентами, 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 $\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_s$.

(e) Всегда ли можно, зная $x + y$ и xy, однозначно 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 (действительно, рассмотрите пары $x = 1, y = 2$ и $x = 2, y = 1$). Итак, радикальность не дает «нахождения» в указанном выше смысле.

Аналогично, зная $\sigma_1 = x + y + z$, $\sigma_2 = xy + yz + zx$ и $\sigma_3 = xyz$, невозможно однозначно найти $(x - y)(y - z)(z - x)$ (действительно, рассмотрите тройки $x = 0, y = 1, z = -1$ и $x = 0, y = -1, z = 1$).

Теорема 2.7 (Руффини)**.** Ни для какого $n \geqslant 5$ многочлен x_1 не радикален.

Из доказательства будет вытекать, что даже многочлен $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$ не радикален для $n = 5$.

2.3 Решение уравнений малых степеней

2.8. Какие из следующих многочленов радикальны для $n = 3$?
(a) $(x-y)(y-z)(z-x)$; (b) $x^9y + y^9z + z^9x$; (c) x.

В задаче 2.8 и далее используйте основную теорему о симметрических многочленах, см., например, [ZSS, 4.6.3c]. Подсказкой к п. (c) являются следующие задачи 2.9.a и 2.11.c.

2.9. 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) Получите многочлен $x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ операциями из определения радикальности из некоторых *циклически* симметрических многочленов от $x_1, x_2, \ldots, x_{10}$.

2.10. Какие из следующих многочленов радикальны 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.

2.11. Решите системы уравнений (x, y, z, t — неизвестные, a, b, c, d известны):

$$\text{(a)} \quad \begin{cases} x+y+z+t=a, \\ x+y-z-t=b, \\ x-y+z-t=c, \\ x-y-z+t=d; \end{cases} \qquad \text{(b)} \quad \begin{cases} x+y+z+t=a, \\ x+iy-z-it=b, \\ x-y+z-t=c, \\ x-iy-z+it=d; \end{cases}$$

$$\text{(c)} \quad \begin{cases} x+y+z=a, \\ x+\varepsilon_3 y+\varepsilon_3^2 z=b, \\ x+\varepsilon_3^2 y+\varepsilon_3 z=c. \end{cases}$$

Выражения из задачи 2.11 называются *резольвентами Лагранжа*. Они «лучше» корней, поскольку «симметричнее» в следующем смысле.

Решение кубического уравнения при помощи резольвент Лагранжа (решение задачи 2.8(c)). Для нахождения корней x, y, z кубического уравнения достаточно найти выражения a, b, c из задачи 2.11 (c). (Заметим, что метод дель Ферро из задачи [ZSS, 4.2.2] 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 (утверждение [ZSS, 4.6.3c]) 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.

Ввиду теоремы Руффини 2.7 метод резольвент Лагранжа, продемонстрированный на примере решения уравнений 3-й и 4-й степени (задачи 2.8 (c) и 2.10 (d)), не работает для уравнения 5-й степени. Сообразите, почему!

Обозначим через Σ_q множество перестановок q-элементного множества. For a permutation $\alpha \in \Sigma_q$ denote

$$\vec{u}_\alpha := (u_{\alpha(1)}, \ldots, u_{\alpha(q)}).$$

Определим *резольвенту Лагранжа* как

$$t(u_1, \ldots, u_q) := \varepsilon_q u_1 + \varepsilon_q^2 u_2 + \ldots + \varepsilon_q^q u_q.$$

Определим *резольвенту Галуа* как

$$Q(u_1, \ldots, u_q, y) := \prod_{\alpha \in \Sigma_q} (y - t(\vec{u}_\alpha)) \in \mathbb{Q}[\varepsilon_q][u_1, \ldots, u_q, y].$$

2.12. (a) Имеем $Q(\varepsilon_q u_1, \ldots, \varepsilon_q u_q, y) = Q(u_1, \ldots, u_q, y)$.

(b) Для некоторого $R_Q \in \mathbb{Q}[\varepsilon_q][z]$ имеем $Q(u_1, \ldots, u_q, y) = R_Q(u_1, \ldots, u_q, y^q)$.

(c) Если $x_1, \ldots, x_5$ — корни многочлена $f \in \mathbb{Q}[x]$ 5-й степени, то $Q(x_1, \ldots, x_5, y) \in \mathbb{Q}[\varepsilon_5][y]$ и даже $Q(x_1, \ldots, x_5, y) \in \mathbb{Q}[y]$.

Многочлен $R_Q(x_1, \ldots, x_5, z) \in \mathbb{Q}[z]$ называется *разрешающим многочленом* для f.

(d)* Все корни разрешающего многочлена для $f(x) = x^5 + 15x + 11$ (а значит, и самого многочлена f) радикальны.

Теорема 2.13.* (a) При $a, b \in \mathbb{R}$ все корни уравнения $x^5 + ax + b = 0$ радикальны тогда и только тогда, когда $a = \dfrac{15 \pm 20c}{c^2+1}$ и $b = \dfrac{44 \mp 8c}{c^2+1}$ для некоторого $c \in \mathbb{Q}$, $c \geqslant 0$.

(b) (**Критерий Галуа разрешимости**) Для любых $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$ все корни уравнения $A(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ радикальны тогда и только тогда, когда некоторый набор многочленов степени 1 с коэффициентами в $\mathbb{Q}$ может быть получен из $\{A\}$ при помощи следующих операций:

• (факторизация) если один из многочленов равен $P_1 P_2$ для некоторых $P_1, P_2 \in \mathbb{Q}[x]$, не являющихся константами, то заменим $P_1 P_2$ на P_1 и P_2;

• (извлечение корня) если один из наших многочленов равен $P(x^q)$ для некоторого $P \in \mathbb{Q}[x]$, то заменим $P(x^q)$ на $P(x)$;

• (взятие резольвенты Галуа) заменим один из наших многочленов P на многочлен $Q(y_1, \ldots, y_q, y)$, где $y_1, \ldots, y_q$ – все корни многочлена P. (По задаче 2.12.c $Q(y_1, \ldots, y_q, y) \in \mathbb{Q}[y]$.)

Часть (a) выводится из (b) [PSo]. Часть «тогда» в (b) проще и доказывается методом резольвент Лагранжа, разобранным в этом пункте. Часть «только тогда» в (b) сложнее и доказывается аналогично теоремам Галуа 1.3, 1.4.

2.4 Единственность способа решения квадратного уравнения

Системы уравнений из этого и следующего пунктов возникают при решении уравнений в радикалах («при помощи одного радикала»), см. замечание 2.6.d.

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

(a) $\begin{cases} f^2(x,y) = p(x+y, xy) \\ x = q\left(x+y, xy, f(x,y)\right) \end{cases}$.

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

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

Системе уравнений из 2.14.a удовлетворяют, например, многочлены

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

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

Для доказательства утверждений 2.14.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 $f(x,y) = -f(y,x)$.

2.16. (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 2.15.a, очень полезная и при решении других задач.

2.17. Для каких из утверждений 2.15 и 2.16 справедливы аналоги для многочленов с комплексными коэффициентами?

Вот обобщение утверждения 2.14 на любое количество шагов из определения радикальности (п. 2.2).

2.18. *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) Возьмем систему из замечания 2.6.(d) для $n = 2$, в которой f_j и p_j рациональные функции, а 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 $f_1(x, y) = (x - y)a(x + y, xy)$.

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

2.5 Неразрешимость «в вещественных многочленах»

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

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

$$\begin{cases} f(x,y,z)^k = p\big(\sigma_1(x,y,z), \sigma_2(x,y,z), \sigma_3(x,y,z)\big) \\ x = q\big(\sigma_1(x,y,z), \sigma_2(x,y,z), \sigma_3(x,y,z), f(x,y,z)\big) \end{cases}.$$

(a) для $k = 1$; (b) для $k = 3$; (c) для $k = 2$;
(d) для любого целого $k > 0$.

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

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

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

циклически симметрический, то f циклически симметрический.

Замечание 2.21 (ср. с решением задачи 2.8.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 замечания 2.21 на любое количество шагов формализуется определением *вещественной радикальности*, которое получается из его комплексного аналога (§2.3) заменой комплексных коэффициентов на вещественные.

Формулы в начале п. 2.2 показывают, что многочлен x вещественно радикален для $n = 2$. Решение задачи 2.8.ab показывает, что оба многочлена

$$(x-y)(y-z)(z-x) \quad \text{и} \quad x^9y + y^9z + z^9x$$

вещественно радикальны для $n = 3$.

Теорема 2.22. Многочлен x не является вещественно радикальным для $n = 3$.

Теорема 2.22 есть еще одна формализация того, что *корень кубического уравнения не выразим в вещественных радикалах через его коэффициенты*, ср. с замечанием 1.1.e. Она вытекает из следующей леммы.

Лемма 2.23 (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.

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

3 Задачи после промежуточного финиша

3.1 Неразрешимость «в многочленах»

Определение радикальности многочлена приведено в п. 2.2. Формально, теорема Руффини 2.7 вытекает из леммы 3.4. Самое трудное и интересное — придумать формулировку этой леммы. Для этого докажем следующие более простые факты. Сообразите, почему многочлен x не является многочленом от $x+y$ и xy.

3.1. Многочлен x_1 не радикален для $n=3$ так, что вторая операция из определения радикальности применяется только для

(a) $k=2$ (*подсказка:* см. задачу 2.24); (b) $k=3$.

3.2. 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.

Циклом длины 3 называется перестановка n-элементного множества, переставляющая некоторые 3 элемента по циклу и оставляющая на месте каждый из оставшихся элементов. 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.

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

(b) Если перестановка переводит в себя многочлен, построенный Вами в решении задачи 3.2.d, то она представляется в виде композиции циклов длины 3.

Лемма 3.4 (о сохранении четносимметричности)**.** Если $q > 0$ целое, $f \in \mathbb{C}[x_1, \ldots, x_5]$ и многочлен f^q четносимметрический, то f четносимметрический.

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

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

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

(c) Если $n \geqslant 5$, 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).

3.6. Определение *рациональной* вещественной (комплексной) радикальности аналогично определению радикальности, только вместо многочленов берутся рациональные функции (с соответствующими коэффициентами; см. определение в задаче 2.18). Является ли многочлен x_1

(a) вещественно рационально радикальным для $n = 3$?

(b) (комплексно) рационально радикальным для $n = 5$?

3.2 Одно извлечение корня третьей степени

Здесь развиваются идеи из п. 2.1.

3.7. Представимо ли следующее число в виде $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, где $a, b, c \in \mathbb{Q}$:

(a) $\sqrt{3}$; (b) $\frac{1}{1+5\sqrt[3]{2}+\sqrt[3]{4}}$; (c) $\cos(2\pi/9)$; (d) $\sqrt[5]{3}$; (e) $\sqrt[3]{3}$;

(f) наибольший вещественный корень многочлена $x^3 - 4x + 2$;

(g)* единственный вещественный корень многочлена $x^3 - 6x - 6$;

(h)* единственный вещественный корень многочлена $x^3 - 9x - 12$?

Лемма 3.8. Пусть $r \in \mathbb{R} - \mathbb{Q}$ и $r^3 \in \mathbb{Q}$.

(a) **О неприводимости.** Многочлен $x^3 - r^3$ неприводим над $\mathbb{Q}$.

(b) **О линейной независимости.** Если $a, b, c \in \mathbb{Q}$ и $a+br+cr^2 = 0$, то $a = b = c = 0$.

(b′) **О линейной независимости над $\mathbb{Q}[\varepsilon_3]$.** Если

$$k, l, m \in \mathbb{Q}[\varepsilon_3] := \{u + v\varepsilon_3 \colon u, v \in \mathbb{Q}\}$$

и $k + lr + mr^2 = 0$, то $k = l = m = 0$.

(c) Если многочлен имеет корень r, то этот многочлен делится на $x^3 - r^3$.

(d) **О сопряжении.** Если многочлен имеет корень r, то корнями этого многочлена являются также числа $\varepsilon_3 r$ и $\varepsilon_3^2 r$.

(e) **О сопряжении.** Если $a, b, c \in \mathbb{Q}$ и многочлен имеет корень $x_0 := a + br + cr^2$, то корнями этого многочлена являются также числа

$$x_1 := a + b\varepsilon_3 r + c\varepsilon_3^2 r^2 \quad \text{и} \quad x_2 := a + b\varepsilon_3^2 r + c\varepsilon_3 r^2.$$

(f) **О рациональности.** Если $a, b, c \in \mathbb{Q}$, то число $a + br + cr^2$ является корнем некоторого ненулевого многочлена степени 3.

Теорема 3.9. Если многочлен неприводим над $\mathbb{Q}$ и имеет корень вида $a + br + cr^2 \notin \mathbb{Q}$, где $r \in \mathbb{R} - \mathbb{Q}$ и $a, b, c, r^3 \in \mathbb{Q}$, то степень многочлена равна 3 и он имеет ровно один вещественный корень.

Лемма 3.10 (о расширении)**.** Число, вещественно радикальное с извлечением корня только один раз, причём третьей степени, имеет вид $a + br + cr^2$, где $r \in \mathbb{R}$ и $a, b, c, r^3 \in \mathbb{Q}$.

3.3 Одно извлечение корня простой степени

3.11. Представимо ли следующее число в виде

$$a_0 + a_1\sqrt[7]{2} + a_2\sqrt[7]{2^2} + \ldots + a_6\sqrt[7]{2^6},$$

где $a_0, a_1, a_2, \ldots, a_6 \in \mathbb{Q}$?

(a) $\sqrt{3}$; (b) $\cos\frac{2\pi}{21}$; (c) $\sqrt[11]{3}$; (d) $\sqrt[7]{3}$;

(e) какой-нибудь из корней многочлена $x^7 - 4x + 2$.

Ответы: не представимы. Доказательства аналогичны решениям задач 3.7. Используйте сформулированные ниже леммы.

Лемма 3.12. Пусть q простое, $r \in \mathbb{R} - \mathbb{Q}$ и $r^q \in \mathbb{Q}$.

(a) **О неприводимости.** Многочлен $x^q - r^q$ неприводим над $\mathbb{Q}$.

(b) **О линейной независимости.** Если A — многочлен степени меньше q и $A(r) = 0$, то $A = 0$.

(c) **О сопряжении.** Если многочлен имеет корень r, то он имеет также корни $r\varepsilon_q^k$ для каждого $k = 1, 2, 3, \ldots, q - 1$.

(d) **О рациональности.** Если A — многочлен, то число $A(r)$ является корнем некоторого ненулевого многочлена степени не выше q.

Обозначим

$$\mathbb{Q}[\varepsilon_q] := \{a_0 + a_1\varepsilon_q + a_2\varepsilon_q^2 + \ldots + a_{q-2}\varepsilon_q^{q-2} \ : \ a_0, \ldots, a_{q-2} \in \mathbb{Q}\}.$$

3.13. Пусть q простое, $r \in \mathbb{C} - \mathbb{Q}[\varepsilon_q]$ и $r^q \in \mathbb{Q}[\varepsilon_q]$.

(a) Многочлен $x^q - r^q$ неприводим над $\mathbb{Q}[\varepsilon_q]$.

(b), (c) Докажите аналоги пунктов (b), (c) предыдущей задачи для многочлена с коэффициентами в $\mathbb{Q}[\varepsilon_q]$.

Лемма 3.14.* Пусть q простое, $r \in \mathbb{R} - \mathbb{Q}$ и $r^q \in \mathbb{Q}$.

(a) **О неприводимости над** $\mathbb{Q}[\varepsilon_q]$**.** Многочлен $x^q - r^q$ неприводим над $\mathbb{Q}[\varepsilon_q]$.

(b) **О линейной независимости над** $\mathbb{Q}[\varepsilon_q]$**.** Если A — многочлен степени меньше q с коэффициентами в $\mathbb{Q}[\varepsilon_q]$ и $A(r) = 0$, то $A = 0$.

Теорема 3.15. Пусть многочлен неприводим над $\mathbb{Q}$ и имеет иррациональный корень $A(r)$ для некоторых многочлена $A \in \mathbb{Q}[x]$ и $r \in \mathbb{R}$, причём $r^q \in \mathbb{Q}$ для некоторого простого q. Тогда многочлен имеет степень q и при $q \neq 2$ не имеет других вещественных корней.

Доказательство аналогично доказательствам теорем 2.3, 3.9 и решениям задач 3.11 (abc). Используйте леммы о сопряжении 3.12 (c), о рациональности 3.12 (d) и о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b).

Лемма 3.16 (о расширении)**.** Число, вещественно радикальное с извлечением корня только один раз, равно $A(r)$ для некоторых $A \in \mathbb{Q}[x]$ и $r \in \mathbb{R}$, причём $r^q \in \mathbb{Q}$ для некоторого $q \in \mathbb{Z}$.

Доказательство аналогично лемме 3.10 о расширении.

3.17. (a–d) Докажите аналоги утверждений задачи 3.12 с заменой $\mathbb{Q}$ на произвольное подмножество $F \subset \mathbb{R}$, замкнутое относительно операций сложения, вычитания, умножения и деления на ненулевое число (и многочленов с коэффициентами в $\mathbb{Q}$ на многочлены с коэффициентами в F).

Решения задач до промежуточного финиша

2.1. *Ответы*: (a), (b), (c), (d) — да, (e), (f), (g), (h), (i) — нет.

(a), (c) Имеем $\sqrt{3+2\sqrt{2}} = \sqrt[3]{7+5\sqrt{2}} = 1+\sqrt{2}$.

(b) Имеем $\frac{1}{7+5\sqrt{2}} = \frac{7-5\sqrt{2}}{7^2-2\cdot 5^2} = -7+5\sqrt{2}$.

(d) Имеем $\cos(2\pi/5) = (\sqrt{5}-1)/4$.

(e) Пусть число $\sqrt[3]{2}$ представимо. Тогда

$$2 = (\sqrt[3]{2})^3 = (a^3+3ab)+(3a^2+b)\sqrt{b}.$$

Так как $3a^2+b \neq 0$, то $\sqrt{b} \in \mathbb{Q}$. Значит, $\sqrt[3]{2} \in \mathbb{Q}$ — противоречие.

Другой способ — аналогично теореме 2.3.

(f) *Набросок первого решения.* Проще доказать сразу, что

$$\sqrt[3]{2} \neq a+p\sqrt{b}+q\sqrt{c}+r\sqrt{bc}, \quad \text{ни для каких} \quad a,b,c,p,q,r \in \mathbb{Q}.$$

Для этого достаточно доказать, что $\sqrt[3]{2} \neq u+v\sqrt{c}$ ни для каких чисел $u,v,c \in \mathbb{Q}[\sqrt{b}] := \{x+y\sqrt{b}\colon x,y \in \mathbb{Q}\}$. Идея доказательства состоит в том, что числа из $\mathbb{Q}[\sqrt{b}]$ (с фиксированным b) «ничуть не хуже» рациональных чисел, т. е. сумма, разность, произведение и частное чисел из $\mathbb{Q}[\sqrt{b}]$ тоже являются числами из $\mathbb{Q}[\sqrt{b}]$ (или, говоря научно, $\mathbb{Q}[\sqrt{b}]$ — *числовое поле*). Поэтому можно доказывать утверждение аналогично п. (e).

Набросок второго решения. Пусть число $\sqrt{2}+\sqrt[3]{2} = a+\sqrt{b}$ представимо. Оно является корнем многочлена $P(x) := ((x-\sqrt{2})^3-2)((x+\sqrt{2})^3-2)$ с рациональными коэффициентами. По п. (e) $\sqrt{2}+\sqrt[3]{2} \notin \mathbb{Q}$. Значит, $\sqrt{b} \notin \mathbb{Q}$. По лемме о сопряжении 2.2 (e) для $r=\sqrt{b}$, многочлен P имеет корень $a-\sqrt{b}$. Так как $\sqrt{b} \notin \mathbb{Q}$, то корни $a \pm \sqrt{b}$ различны. Но у многочлена P только два вещественных корня: $\sqrt{2}+\sqrt[3]{2}$ и $-\sqrt{2}+\sqrt[3]{2}$. Поэтому $a+\sqrt{b} = \sqrt{2}+\sqrt[3]{2}$ и $a-\sqrt{b} = -\sqrt{2}+\sqrt[3]{2}$. Отсюда $\sqrt[3]{2} = a \in \mathbb{Q}$. Противоречие.

(g) Пусть число $\cos(2\pi/9)$ представимо. По формуле косинуса тройного угла оно является корнем уравнения $4x^3-3x = -\frac{1}{2}$. По лемме 2.2 (f) это уравнение имеет рациональный корень. Противоречие.

Другой способ — аналогично теореме 2.3.

(h) Корнями многочлена $P(x) := (x^2-2)^2-2$ являются четыре числа $\pm\sqrt{2\pm\sqrt{2}}$, где знаки + и − не обязательно согласованы. Все

эти числа иррациональны. Значит, по теореме 2.3 достаточно доказать, что многочлен P не разлагается в произведение двух квадратных трехчленов с рациональными коэффициентами. Эта неразложимость следует из того, что произведение любых двух корней многочлена P иррационально.

(i) (Использован текст И. Брауде-Золотарёва.) Из равенства

$$\cos(2\pi/7) + \cos(4\pi/7) + \cos(6\pi/7) + \ldots + \cos(14\pi/7) = 0$$

получаем $\cos(2\pi/7)+\cos(4\pi/7)+\cos(6\pi/7) = -1/2$. Используя формулы косинуса двойного и тройного угла, получаем, что число $\cos(2\pi/7)$ является корнем уравнения $8t^3 + 4t^2 - 4t - 1 = 0$. Сделав замену $u = 2t$, получим $u^3+u^2-2u-1 = 0$. Это уравнение не имеет рациональных корней. Значит, уравнение $8t^3+4t^2-4t-1 = 0$ тоже не имеет рациональных корней. Поэтому многочлен $8t^3+4t^2-4t-1 = 0$ неприводим над $\mathbb{Q}$. Теперь непредставимость вытекает из леммы 2.2 (f).

(j) Аналогично п. (f).

2.3. Пусть, напротив, данный многочлен P имеет корень $x_0 = a \pm \sqrt{b}$. По лемме 2.2 (e) о сопряжении и аналогично ей, корнем многочлена P является также число $x_1 = a \mp \sqrt{b}$. При $b = 0$ утверждение очевидно. Поэтому считаем, что $b \neq 0$. Тогда $x_0 \neq x_1$. Значит, $P(x)$ делится на $(x - a)^2 - b$. Так как $\deg P > 2$, то многочлен P приводим. Противоречие.

2.4. Обозначим через $\sqrt{c}$ число, полученное при единственном извлечении корня, где $c \in \mathbb{Q}$. Докажите, что все полученные числа имеют вид $a + b\sqrt{c}$, где $a, b \in \mathbb{Q}$.

2.5. Ответ: тогда и только тогда, когда $n \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Или, эквивалентно, $\varphi(n) \in \{1, 2, 4\}$.

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

(Пункт (a) можно также свести к (b).)

(b) Обозначим

$$M = x^9y + y^9z + z^9x \quad \text{и} \quad N = y^9x + x^9z + z^9y.$$

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. 2.2.

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

(b) Обозначим

$$M = x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1 \quad \text{и}$$

$$N = x_2x_4 + x_4x_6 + x_6x_8 + x_8x_{10} + x_{10}x_2.$$

Далее аналогично задаче 2.8.b.

2.10. (a) Квадрат $(x-y)^2(x-z)^2(x-t)^2(y-z)^2(y-t)^2(z-t)^2$ симметричен, см. 2.8.a.

(b) Положим

$$M = xy + zt, \quad N = xz + yt, \quad K = xt + yz.$$

По 2.8.c, M «выразим в радикалах при помощи многочленов»

$$M + N + K, \quad MN + MK + NK, \quad MNK.$$

Аналогично решениям задач 2.8.c выше и 2.10.d ниже, эти многочлены симметрические. Поэтому $M = xy + zt$ радикален.

(c) Положим

$$M = (x+y-z-t)^2, \quad N = (x+z-y-t)^2, \quad K = (x+t-y-z)^2.$$

Повторяя решение пункта (b), получим $M = (x+y-z-t)^2$. Теперь легко получить и $x+y-z-t$.

Решение уравнения 4-й степени при помощи резольвент Лагранжа (решение задачи 2.10.d). Для нахождения корней x, y, z, t уравнения 4-й степени достаточно найти выражения a, b, c, d от корней из задачи 2.11.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.

2.11. Используйте равенства $1 + \varepsilon + \varepsilon^2 = 0$ и $1 + i + i^2 + i^3 = 0$.

2.12. Для наглядности приведем решения при $q = 5$.

(a) Имеем

$$t(\varepsilon_5 \vec{u}_\alpha) = t(u_{\alpha(5)}, u_{\alpha(1)}, u_{\alpha(2)}, u_{\alpha(3)}, u_{\alpha(4)}) = t(\vec{u}_{\alpha\circ(54321)}).$$

Следовательно,

$$Q(\varepsilon_5 u_1, \ldots, \varepsilon_5 u_5, y) = \prod_{\alpha\in\Sigma_5} (y - t(\varepsilon_5 \vec{u}_\alpha)) =$$

$$= \prod_{\alpha\in\Sigma_5} (y - t(\vec{u}_{\alpha\circ(54321)}) = Q(u_1, \ldots, u_5, y).$$

Здесь

• $(54321) \in \Sigma_5$ – это цикл, который отправляет 5 в 4, 4 в 3, ..., 1 в 5.

• последнее равенство справедливо, потому что когда α пробегает Σ_5, то же делает и $\alpha \circ (54321)$.

(b) Для каждого $k = 0, 1, 2, \ldots, 120$ найдётся однородный многочлен $P_k \in \mathbb{Q}[\varepsilon_5][u_1, \ldots, u_5]$ («степени» $120 - k$) такой, что коэффициент при y^k в Q равен $P(u_1, \ldots, u_5)$, т.е.

$$Q(u_1, \ldots, u_5, y) = \sum_{k=0}^{120} P_k(u_1, \ldots, u_5) y^k.$$

По (a) и из однородности имеем

$$P_k(u_1, \ldots, u_5) = P_k(\varepsilon_5 u_1, \ldots \varepsilon_5 u_5) = \varepsilon_5^{-k} P_k(u_1, \ldots, u_5).$$

Если k не кратно 5, то $P_k(u_1, \ldots, u_5) = 0$, что и требовалось.

(c) Многочлен $Q(u_1, \ldots, u_5, y)$ симметричен по $u_1, \ldots, u_5$. Значит, все коэффициенты (P_k из пункта (b)) соответствующего многочлена из $\mathbb{Q}[\varepsilon_5, u_1, \ldots, u_q][y]$ симметричны по $u_1, \ldots, u_5$. Теперь утверждение $Q(x_1, \ldots, x_5, y) \in \mathbb{Q}[\varepsilon_5][y]$ следует из основной теоремы о

симметрических многочленах, формул Виета и того факта, что коэффициенты f рациональны.

Теперь утверждение $Q(x_1, \dots, x_5, y) \in \mathbb{Q}[y]$ доказывается аналогично [ZSS, !]

2.14. (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 2.15.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 2.16.a f антисимметрический. Значит, $y = q(x + y, xy, -f(x, y))$. Итак,

$$x = a + bf \quad \text{и} \quad y = a - bf,$$

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

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 2.15.be, 2.16. Если k нечетно, то из утверждения 2.16.b получаем, что f симметрический, что противоречит равенству $x = q(x + y, xy, f(x, y))$. Если $k = 4$, то f^2 либо 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) получаем $x = a + bf$. Поэтому f — дробно-рациональная функция. Тогда решение аналогично п. (a).

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

(b) Следует из п. (a).

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

(d) Следует из п. (c).

(e) Следует из п. (f).

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

2.16. (a) Так как f^2 симметрический, то $f(x, y)^2 = f(y, x)^2$. Отсюда по утверждению 2.15.b $f(x, y) = \pm f(y, x)$.

(b) Используйте аналог утверждений 2.15.ce.

(c) См. указание к 2.15.f.

2.17. *Ответ:* 2.15.abf, 2.16.abc.

2.22. При $n = 3$ множество вещественно радикальных многочленов содержится в множестве циклически симметрических многочленов. Это утверждение доказывается при помощи индукции по количеству операций из определения радикальности. Шаг индукции вытекает из леммы 2.23 о сохранении циклической симметричности.

Поскольку многочлен x не является циклически симметрическим, то он не является вещественно радикальным.

2.23. Доказательство можно найти в [Sk19, п. 9.4.2].

2.24. *Ответ:* 2.19.abcd, 2.20.b, 2.23 для всех q, не делящихся на 3.

К алгоритмам решения алгебраических уравнений

представляют Б. Вукорепа, А. Глебов,
А. Еннэ, А. Скопенков, А. Чиликов

Решения задач после промежуточного финиша

3.1. (b) Используйте аналог задачи 3.2.c для $n = 3$.

3.2. *Ответ:* (c) — верно, (a), (b), (d) — неверно.

(a) См. 2.9.a.

(b) Рассмотрите многочлен $x_1 + \varepsilon_5 x_2 + \varepsilon_5^2 x_3 + \varepsilon_5^3 x_4 + \varepsilon_5^4 x_5$.

(d) Рассмотрите многочлен $\prod\limits_{i<j}(x_i - x_j)$.

(c) Так как f^3 симметрический, то

$$f^3(x_1, x_2, x_3, x_4, x_5) = f^3(x_2, x_1, x_3, x_4, x_5).$$

Извлекая корень третьей степени, имеем

$$f(x_1, x_2, x_3, x_4, x_5) = \varepsilon_3^q f(x_2, x_1, x_3, x_4, x_5) = \varepsilon_3^{2q} f(x_1, x_2, x_3, x_4, x_5).$$

Отсюда $\varepsilon_3^{2q} = 1$, поэтому $\varepsilon_3^q = 1$. Аналогично $f(\vec{x}) = f(\vec{x}_\alpha)$ для любой перестановки α, меняющей местами два элемента из множества $\{x_1, x_2, x_3, x_4, x_5\}$. Поэтому f симметрический.

3.3. (a) $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$.

(b) Докажите, что любая перестановка, переводящая в себя многочлен из задачи 3.2.d, является четной. А тогда она представляется в виде композиции циклов длины 3, см. [ZSS, п. 23.2.4].

3.4. Доказательство можно найти в [Sk15].

3.5. (c) Обозначим через a, b, c, d, e пять различных элементов данного множества. $(abc) = (ac)(de)(ab)(de)$.

3.6. *Ответ:* (a), (b) — нет.

Леммы 2.23 о сохранении циклической симметричности и 3.4 о сохранении четносимметричности верны и для рациональных функций, см. [Sk15], [Sk19, п. 9.4.2]. Далее аналогично решению задачи 2.22.

3.7. *Ответы*: (a), (c), (d), (e), (f), (h) — нет, (b), (g) — да.

Обозначим $r := \sqrt[3]{2}$.

(a) Пусть число $\sqrt{3}$ представимо.

Первое решение. Тогда

$$3 = (a^2 + 4bc) + (2ab + 2c^2)\sqrt[3]{2} + (2ac + b^2)\sqrt[3]{4}.$$

Так как многочлен $x^3 - 2$ не имеет рациональных корней, то он неприводим над $\mathbb{Q}$. Значит, $2ab + 2c^2 = 2ac + b^2 = 0$ (ср. с задачей 3.8 (b)). Поэтому $b^3 = -2abc = 2c^3$. Тогда либо $b = c = 0$, либо $\sqrt[3]{2} = b/c$. Оба случая невозможны.

Второе решение. Обозначим $P(x) := x^2 - 3$. По лемме 3.8 (e) о сопряжении P имеет три корня x_0, x_1, x_2, введённых в формулировке леммы. Так как ни один из них не рационален, то равенство $b = c = 0$ невозможно. Значит, по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_3]$ 3.8 (b′) эти корни различны. Противоречие.

(b) Имеем $(1 + 5\sqrt[3]{2} + \sqrt[3]{4})(3 + \sqrt[3]{2} - 8\sqrt[3]{4}) = -75$. (Это равенство несложно получить методом неопределённых коэффициентов или при помощи алгоритма Евклида для многочленов $x^3 - 2$ и $x^2 + 5x + 1$, см. решение задачи 3.10.) Поэтому

$$\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}} = -\frac{1}{25} - \frac{1}{75} \cdot \sqrt[3]{2} + \frac{8}{75} \cdot (\sqrt[3]{2})^2.$$

(c) Пусть число $\cos(2\pi/9)$ представимо. Оно является корнем уравнения $4x^3 - 3x = -\frac{1}{2}$. Два других его вещественных корня есть $\cos(8\pi/9)$ и $\cos(4\pi/9)$.

Применим второе решение пункта (a) для $P(x) := 8x^3 - 6x - 1$. Получим, что корни x_0, x_1, x_2 различны. Так как $\overline{\varepsilon_3} = \varepsilon_3^2$, то $\overline{x_2} = x_1$. Значит, x_2 и x_1 не могут быть вещественными и различными. Противоречие.

(d) Если число $\sqrt[5]{3}$ представимо, то по лемме о рациональности 3.8 (f) оно является корнем некоторого кубического многочлена. Противоречие с неприводимостью многочлена $x^5 - 3$ над $\mathbb{Q}$.

(e) Аналогично п. (a), (c) получаем, что комплексные корни многочлена $x^3 - 3$ есть числа x_0, x_1, x_2, введённые в формулировке леммы 3.8 (e). Поэтому $(a + br + cr^2)\varepsilon_3^s = a + br\varepsilon_3 + cr^2\varepsilon_3^2$ для некоторого $s \in \{1, 2\}$. Отсюда по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_3]$

3.8 (b′) получаем, что $a = 0$ и $bc = 0$. Поэтому либо $\sqrt[3]{3} = br$, либо $\sqrt[3]{3} = cr^2$. Противоречие.

(f) Доказательство аналогично п. (c).

(g) Это уравнение имеет корень $\sqrt[3]{2} + \sqrt[3]{4}$.

(h) Единственный вещественный корень этого уравнения — $\sqrt[3]{3} + \sqrt[3]{9}$. Пусть, напротив, это число выражается в требуемом виде. Применим второе решение пункта (a) для $P(x) := x^3 - 9x - 12$. Получим, что числа x_0, x_1, x_2 — все корни многочлена P.

С другой стороны, все корни данного уравнения —

$$y_0 := \sqrt[3]{3} + \sqrt[3]{9}, \quad y_1 := \sqrt[3]{3}\varepsilon_3 + \sqrt[3]{9}\varepsilon_3^2, \quad y_2 := \sqrt[3]{3}\varepsilon_3^2 + \sqrt[3]{9}\varepsilon_3.$$

Поскольку данное уравнение имеет ровно один вещественный корень, получаем, что $x_0 = y_0$ и либо $x_1 = y_1$, $x_2 = y_2$, либо, наоборот, $x_2 = y_1$, $x_1 = y_2$.

Обозначим $R(x) := \sqrt[3]{3}x + \sqrt[3]{9}x^2$, а также $S(x) := a + brx + cr^2x^2$ и $S(x) := a + brx^2 + cr^2x$ для первого и второго случая соответственно. Тогда многочлен $R(x) - S(x)$ имеет 3 различных корня $1, \varepsilon_3, \varepsilon_3^2$. Но его степень не выше второй. Поэтому $R = S$. Значит, $\sqrt[3]{3} = br$ или $\sqrt[3]{3} = cr^2$. Противоречие.

3.8. (a) Если многочлен $x^3 - r^3$ приводим над $\mathbb{Q}$, то он имеет рациональный корень. Противоречие.

(b) Предположим противное. Поделим $x^3 - r^3$ на $a + bx + cx^2$ с остатком. По п. (a) остаток ненулевой. Оба многочлена $x^3 - r^3$ и $a + bx + cx^2$ имеют корень $x = r$. Значит, остаток имеет корень $x = r$. Следовательно, остаток имеет иррациональный корень. Противоречие с тем, что степень остатка равна 1.

(b′) Рассмотрите вещественную и мнимую части.

Замечание. Это утверждение равносильно неприводимости многочлена $x^3 - r^3$ над $\mathbb{Q}[\varepsilon_3]$. Если многочлен $x^3 - r^3$ неприводим над $\mathbb{Q}[\varepsilon_3]$, то многочлен $k + lx + mx^2 \in \mathbb{Q}[\varepsilon_3][x]$ не может иметь корень r. Если многочлен $x^3 - r^3$ приводим над $\mathbb{Q}[\varepsilon_3]$, то один из сомножителей дает линейную зависимость чисел $1, r, r^2$ над $\mathbb{Q}[\varepsilon_3]$.

(c) Поделим многочлен с остатком на $x^3 - r^3$. Подставляя $x = r$, по лемме о линейной независимости п. (b) получаем, что остаток нулевой.

(d) По п. (c) получаем, что если $R^3 = r^3$, то R есть корень многочлена.

(e) Обозначим через P многочлен из условия, и пусть $G(t) := P(a + bt + ct^2)$. Тогда $G(r) = 0$. Значит, по п. (d) имеем $G(r\varepsilon_3) = 0 = G(r\varepsilon_3^2)$.

(f) *Первое доказательство.* Достаточно доказать утверждение для $a = 0$. Для числа $t = br + cr^2$ выполнено равенство $t^3 = b^3r^3 + c^3r^6 + 3bcr^3t$.

Иными словами, ввиду того, что $u^3 + v^3 + w^3 - 3uvw$ делится на $u + v + w$, число $a + br + cr^2$ является корнем многочлена

$$(x - a)^3 - 3bcr^3(x - a) - b^3r^3 - c^3r^6.$$

Второе доказательство. Обозначим $x_0 = a + br + cr^2$. Разложим числа x_0^k при $k = 0, 1, 2, 3$ по степеням числа r:

$$x_0^k = a_k + b_k r + c_k r^2.$$

Достаточно найти числа $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$, не все из которых равны нулю, удовлетворяющие условию $\lambda_0 + \lambda_1 x_0 + \lambda_2 x_0^2 + \lambda_3 x_0^3 = 0$. Для этого нужно, чтобы эти числа удовлетворяли системе уравнений

$$\begin{cases} \lambda_0 a_0 + \ldots + \lambda_3 a_3 = 0, \\ \lambda_0 b_0 + \ldots + \lambda_3 b_3 = 0, \\ \lambda_0 c_0 + \ldots + \lambda_3 c_3 = 0. \end{cases}$$

Как известно, однородная (т. е. с нулевыми правыми частями) система линейных уравнений с рациональными коэффициентами, в которой уравнений меньше, чем переменных, имеет нетривиальное рациональное решение. Значит, требуемые числа найдутся.

Полученный многочлен имеет степень ровно 3 ввиду лемм 3.8 (e, b′).

Третье доказательство. Обозначим $A(x) := a + bx + cx^2$. Произведение $(x - A(t_0))(x - A(t_1))(x - A(t_2))$ является симметрическим многочленом от t_0, t_1, t_2. Значит, оно является многочленом от x и от элементарных симметрических многочленов от t_0, t_1, t_2. Значения этих элементарных симметрических многочленов при $t_k = r\varepsilon_3^k$, $k = 0, 1, 2$, равны коэффициентам многочлена $x^3 - r^3$, которые рациональны. Поэтому рассмотренное произведение является искомым многочленом.

3.9. По лемме о рациональности 3.8 (f) существует многочлен степени не выше 3 с корнем $a+br+cr^2$. Из этого факта и из неприводимости над $\mathbb{Q}$ данного многочлена P получаем, что $\deg P \leqslant 3$. По лемме о сопряжении 3.8 (e) многочлен P имеет три корня x_0, x_1, x_2, введённых в формулировке леммы. Так как многочлен P неприводим над $\mathbb{Q}$, то ни один из корней не рационален. Поэтому равенство $b = c = 0$ невозможно. Значит, по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_3]$ 3.8 (b′) корни x_0, x_1, x_2 различны. Следовательно, $\deg P = 3$.

Так как $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$, то $\overline{x_2} = x_1$. Значит, x_2 и x_1 не могут быть вещественными и различными. Следовательно, $x_2, x_1 \in \mathbb{C} - \mathbb{R}$. Поэтому P имеет ровно один вещественный корень.

3.10. Пусть при извлечении корня третьей степени получилось число r. Если $|r| \in \mathbb{Q}$, то утверждение очевидно. Если $|r| \notin \mathbb{Q}$, то многочлен $x^3 - r^3$ неприводим над $\mathbb{Q}$.

Достаточно доказать, что $\frac{1}{a+br+cr^2} = h(r)$ для некоторого многочлена h. По лемме о неприводимости, многочлен x^3-r^3 неприводим над $\mathbb{Q}$. Поэтому он взаимно прост с $a+bx+cx^2$. Значит, существуют многочлены g и h, для которых $h(x)(a+bx+cx^2)+g(x)(x^3-r^3) = 1$. Тогда h — искомый многочлен.

3.11. Обозначим $r := \sqrt[7]{2}$ и $A(x) := a_0 + a_1x + a_2x^2 + \ldots + a_6x^6$.

(a) Пусть число $\sqrt{3}$ представимо. Тогда по лемме о сопряжении 3.12 (c) многочлен $x^2 - 3$ имеет корни $A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \ldots, 6$. Так как этот многочлен не имеет рациональных корней, то по то по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) эти корни различны. Противоречие.

(b) Обозначим через P многочлен, для которого $\cos 7x = P(\cos x)$ (Докажите, что такой многочлен существует!).

Первое решение. Пусть число $\cos\frac{2\pi}{21}$ представимо. Аналогично п. (a) данный многочлен P имеет попарно различные корни $x_k := A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \ldots, 6$. Так как $P(0) > 0$, $P(1) < 0$ и $P(2) > 0$, то многочлен P имеет вещественный корень x_k, отличный от x_0. Имеем $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$. Поэтому $x_k = \overline{x_k} = x_{7-k}$. Противоречие.

Второе решение. Корнями многочлена $2P(x)+1$ являются вещественные числа $y_k := \cos\frac{2(3k+1)\pi}{21}$ при $k = 0, \ldots, 6$. Одно из них, а именно $y_2 = -1/2$, рационально.

В следубщем абзаце мы докажем, что число y_0 иррационально. (Иначе из равенства $\varepsilon_{21}^2 - 2y_0\varepsilon_{21} + 1 = 0$ следует, что $\varepsilon_{21} = a + i\sqrt{b}$ для некоторых $a, b \in \mathbb{Q}$. Тогда и число $\varepsilon_7 = \varepsilon_{21}^3$ тоже имеет такой вид. Но ε_7 является корнем неприводимого[4] многочлена $1 + x + \ldots + x^6$, что противоречит аналогу теоремы 2.3 для чисел вида $a + i\sqrt{b}$.)

Итак, число y_0 иррационально и является корнем многочлена $\frac{2P(x)+1}{2x+1}$ степени 6. Тогда по леммам о сопряжении 3.12 (c) и о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) этот многочлен имеет семь попарно различных корней, что невозможно.

(c) Пусть число $\sqrt[11]{3}$ представимо. Тогда по лемме о рациональности 3.12 (d) существует ненулевой многочлен степени не выше 7 с корнем $\sqrt[11]{3}$. Противоречие с неприводимостью многочлена $x^{11} - 3$ над $\mathbb{Q}$.

(d) Пусть число $\sqrt[7]{3}$ представимо. Аналогично п. (a) все комплексные корни многочлена $x^7 - 3$ есть $A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \ldots, 6$. Поэтому $A(r)\varepsilon_7^s = A(r\varepsilon_7)$ для некоторого $s \in \{1, 2, 3, 4, 5, 6\}$. Отсюда по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) $a_k = 0$ для любого $k \neq s$. Поэтому $\sqrt[7]{3} = a_s r^s$. Противоречие.

(e) Пусть какой-нибудь из корней представим. Данный многочлен P не имеет рациональных корней. Тогда по лемме о сопряжении 3.12.c и лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14.b P имеет попарно различные корни $x_k := A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \ldots, 6$. Так как $P(0) > 0$, $P(1) < 0$ и $P(2) > 0$, то P имеет вещественный корень x_k, отличный от x_0. Имеем $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$. Поэтому $x_k = \overline{x_k} = x_{7-k}$. Противоречие.

3.12. (a) Все корни многочлена $x^q - r^q$ есть $r, r\varepsilon_q, r\varepsilon_q^2, \ldots, r\varepsilon_q^{q-1}$. Пусть он приводим над $\mathbb{Q}$. Модуль свободного члена одного из унитарных сомножителей разложения рационален и равен произведе-

[4]Неприводимость многочлена $g(x) = 1 + x + \ldots + x^6$ можно показать, например, применив признак Эйзенштейна [ZSS, п. 5.5.2] к многочлену $g(x+1)$. Впрочем, здесь достаточно доказать, что у него нет рациональных делителей степени 1 и 2.

нию модулей некоторых k из этих корней, $0 < k < q$. Значит, $r^k \in \mathbb{Q}$. Так как q простое, то имеем $kx + qy = 1$ для некоторых целых x, y. Тогда $r = (r^k)^x (r^q)^y \in \mathbb{Q}$. Противоречие.

(b) Предположим противное. Рассмотрим многочлен $A(x)$ наименьшей степени, для которого лемма не выполняется. Поделим $x^q - r^q$ на $A(x)$ с остатком $R(x)$. Тогда $\deg R < \deg A$, $R(r) = 0$ и по п. (a) многочлен $R(x)$ ненулевой. Противоречие с выбором A.

(c) Доказательство аналогично задачам 2.2 (c, d), 3.8 (d). Используйте п. (b).

(d) Доказательства повторяют второе и третье доказательства леммы о рациональности 3.8 (f). Нужно только везде заменить 3 на q и 2 на $q-1$ (например, во второй строчке второго доказательства $k = 0, 1, 2, \ldots, q$).

3.13. (a) Пусть многочлен приводим. Свободный член одного из унитарных сомножителей разложения лежит в $\mathbb{Q}[\varepsilon_q]$ и равен $\pm r^k \varepsilon_q^m$ для некоторого m. Поэтому $r^k \in \mathbb{Q}[\varepsilon_q]$. Далее аналогично лемме 3.12 (a) получаем $r \in \mathbb{Q}[\varepsilon_q]$. Противоречие.

Пункты (b) и (c) выводятся из п. (a) аналогично соответствующим пунктам задачи 3.12.

3.14. (a) Пусть многочлен приводим. Аналогично доказательству леммы о неприводимости над $\mathbb{Q}[\varepsilon_q]$ 3.13 (a) имеем $r \in \mathbb{Q}[\varepsilon_q]$. Поэтому $r^2, r^3, \ldots, r^{q-1} \in \mathbb{Q}[\varepsilon_q]$.

В следубщем абзаце мы докажем, что имеется многочлен степени меньше q с корнем r. Это будет противоречить неприводимости многочлена $x^q - r^q$ над $\mathbb{Q}$.

Разложим число r^k по степеням числа ε_q для $k = 0, 1, \ldots, q-1$:

$$r^k = a_{k,0} + a_{k,1}\varepsilon_q + \ldots + a_{k,q-2}\varepsilon_q^{q-2}.$$

Достаточно найти числа $\lambda_0, \ldots, \lambda_{q-1} \in \mathbb{Q}$, не равные одновременно нулю, для которых

$$\lambda_0 a_{0,m} + \ldots + \lambda_{q-1} a_{q-1,m} = 0 \quad \text{при любом} \quad m = 0, 1, \ldots, q-2.$$

Такие числа существуют по аналогии с соответствующим рассуждением во втором доказательстве леммы о рациональности 3.8 (f).

(b) Утверждение вытекает из п. (a).

3.15. Предположим противное. Обозначим данный многочлен через P. При $q < \deg P$ получаем противоречие с леммой о рациональности 3.12 (d). При $q \geqslant \deg P$ по лемме о сопряжении 3.12 (c) и лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) многочлен P имеет попарно различные корни $x_k = A(r\varepsilon_q^k)$ для $k = 0, 1, 2, \ldots, q-1$. При $q > \deg P$ получаем противоречие. При $q = \deg P$ из условий $q \neq 2$ и $\overline{x_k} = x_{q-k} \neq x_k$ получаем единственность вещественного корня.

Список литературы

[Al] *Алексеев В. Б.* Теорема Абеля. М.: Наука, 1976.

[AB] *Akhtyamov D., Bogdanov I.* Solvability of cubic and quartic equations using one radical. http://arxiv.org/abs/1411.4990.

[Ar84] *Арнольд В.И.* Обыкновенные дифференциальные уравнения, М. Наука, 1984.

[Dor] *Dörrie H.* 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.

[E2] *Edwards H. M.* The construction of solvable polynomials // Bull. Amer. Math. Soc. 2009. V. 46. P 397–411. Errata: Bull. Amer. Math. Soc. 46 (2009), 703-704.

[Es] *Esterov A.* Galois theory for general systems of polynomial equations, https://arxiv.org/abs/1801.08260

[FT] *Табачников С. Л., Фукс Д. Б.* Математический дивертисмент, М.: МЦНМО, 2011.

[Ka] *Канунников А. Л.* Начала теории Галуа: разрешимость алгебраических уравнений в радикалах. http://www.mathnet.ru/conf1015.

[Ko17] *Коган Е.* Множественная сложность построения правильного многоугольника, https://arxiv.org/abs/1711.05807.

[Kol] *Колосов В. А.* Теоремы и задачи алгебры, теории чисел и комбинаторики. М.: Гелиос, 2001.

[Ler] *Lerner L.* Galois Theory without abstract algebra. http://arxiv.org/abs/1108.4593.

[Pr07-2] *Прасолов В. В.* Задачи по алгебре, арифметике и анализу. М.: МЦНМО, 2007.

[PSo] *Прасолов В. В.*, *Соловьев Ю. П.* Эллиптические функции и алгебраические уравнения. М.: Факториал, 1997.

[Saf] *Сафин А.* Программа для построения правильных многоугольников циркулем и линейкой (доклад на ММКШ-2008). http://www.mccme.ru/mmks/dec08/Safin.pdf.

[Sk10] *Скопенков А.* Базисные вложения и 13-я проблема Гильберта // Мат. Просвещение. 2010. № 14. С. 143–174; http://arxiv.org/abs/1001.4011.

[Sk11] *Скопенков А.* Простое доказательство теоремы Абеля о неразрешимости уравнений в радикалах // Мат. Просвещение. 2011. № 15. С. 113–126; http://arxiv.org/abs/1102.2100.

[Sk15] *Skopenkov A.* A short elementary proof of the insolvability of the equation of degree 5. http://arxiv.org/abs/1508.03317.

[Sk19] *Skopenkov A.* Mathematics via problems: from olympiades and math circles to a profession. Algebra. AMS, Providence, to appear.

[St94] *Stillwell J.* Galois theory for beginners, Amer. Math. Monthly, 101 (1994), 22-27.

[T] *Тихомиров В. М.* Абель и его великая теорема // Квант. 2003. № 1. С. 11–15.

[Vag] *Вагутен Н.* Сопряжённые числа // Квант. 1980. № 2. С. 26–32.

[ZSS] Элементы математики в задачах: через олимпиады и кружки к профессии. Сборник под редакцией А. Заславского, А. Скопенкова и М. Скопенкова. МЦНМО, 2018. http://www.mccme.ru/circles/oim/materials/sturm.pdf.

4 Additional problems for successful teams

4.1. (a) Let $x, y, r \in \mathbb{R}$, $p, g \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[u, v, w]$ be such that $g(x, y) \notin \mathbb{Q}(x + y, xy)$ and

$$\begin{cases} r^2 = p(x + y, xy) \\ g(x, y) = p_1(x + y, xy, r) \end{cases}$$

(cf. Problem 2.14.c). Then $r \in \mathbb{Q}(x, y)$.

(b) Let $x, y, r \in \mathbb{R}$, $p \in \mathbb{Q}[\sqrt{2}][u, v]$, $g \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[\sqrt{2}][u, v, w]$ be such that $g(x, y) \notin \mathbb{Q}(x + y, xy, \sqrt{2})$ and the equations of (a) hold. Then there are $\rho \in \mathbb{Q}(x, y)$, $\pi \in \mathbb{Q}[\sqrt{2}][u, v]$ and $\pi_1 \in \mathbb{Q}[\sqrt{2}][u, v, w]$ such that the equations of (a) hold with r, p, p_1 replaced by ρ, π, π_1.

(c) **Rationalization Lemma.** Let $x, y, r \in \mathbb{R}$ and $F \subset \mathbb{R}$ a field containing $x + y, xy, r^2$ but not r. If $F(r) \cap \mathbb{Q}(x, y) \not\subset F$, then there is $\rho \in \mathbb{Q}(x, y)$ such that $\rho^2 \in F$ and $F(\rho) = F(r)$.

4.2. Denote $a_j = \sigma_j(x_1, x_2, x_3)$, $j = 1, 2, 3$.

(a) Let $x_1, x_2, x_3, r \in \mathbb{R}$, $p, g \in \mathbb{Q}[u_1, u_2, u_3]$ and $p_1 \in \mathbb{Q}[u_1, u_2, u_3, v]$ be such that $g(x_1, x_2, x_3) \notin \mathbb{Q}(a_1, a_2, a_3)$ and

$$\begin{cases} r^2 = p(a_1, a_2, a_3) \\ g(x_1, x_2, x_3) = p_1(a_1, a_2, a_3, r) \end{cases}.$$

Then $r \in \mathbb{Q}(x_1, x_2, x_3)$.

(b) **Rationalization Lemma.** Let $x_1, x_2, x_3, r \in \mathbb{R}$ and $F \subset \mathbb{R}$ a field containing a_1, a_2, a_3, r^2 but not r. If $F(r) \cap \mathbb{Q}(x_1, x_2, x_3) \not\subset F$, then there is $\rho \in \mathbb{Q}(x_1, x_2, x_3)$ such that $\rho^2 \in F$ and $F(\rho) = F(r)$.

(c) **Proposition.** If $x_1, x_2, x_3 \in \mathbb{R}$ and x_1 is $\{a_1, a_2, a_3\}$-expressible by quadratic real radicals, then x_1 is $\{a_1, a_2, a_3\}$-expressible by quadratic real radicals so that every radical is in $\mathbb{Q}(x_1, x_2, x_3)$.

4.3. (a) Let $x, y, r \in \mathbb{C}$, $p \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[u, v, w]$ be such that

$$\begin{cases} r^3 = p(x + y, xy) \\ x = p_1(x + y, xy, r) \end{cases}$$

(cf. Problem 2.14.d for $k = 3$). Then $r \in \mathbb{Q}[\varepsilon_3](x, y)$.

(b) Same as (a) with $x = p_1(x + y, xy, r)$ replaced by $g(x, y) = p_1(x + y, xy, r)$ for some $g \in \mathbb{Q}[u, v]$ such that $g(x, y) \notin \mathbb{Q}(x + y, xy)$.

(c) **Rationalization Lemma.** Let $x, y, r \in \mathbb{C}$ and $F \subset \mathbb{C}$ a field containing $x+y, xy, \varepsilon_3, r^3$ but not r. If $F(r) \cap \mathbb{Q}(x,y) \not\subset F$, then there is $\rho \in \mathbb{Q}(x,y)$ such that $\rho^3 \in F$ and $F(\rho) = F(r)$.

(d) **Rationalization Lemma.** Same as (c) with x, y replaced by $x_1, \ldots, x_n$ and $x+y, xy$ replaced by $\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)$.

(e) **Rationalization Lemma.** Same as (d) with r^3, ρ^3 replaced by r^q, ρ^q for a prime q and ε_3 replaced by ε_q.

(f) **Proposition.** If

$$x_1, \ldots, x_n \in \mathbb{C}, \quad M := \{\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)\}$$

and x_1 is M-expressible by radicals, then x_1 is M-expressible by radicals so that every radical is in $\bigcup_{q=3}^{\infty} \mathbb{Q}[\varepsilon_q](x_1, \ldots, x_n)$.

4.4. There are numbers $x, y \in \mathbb{R}$ such that if $p \in \mathbb{Q}[u,v]$ and $p(x,y) = 0$, then $p = 0$.

Such numbers are called *algebraically independent over* $\mathbb{Q}$.

4.5. (a) Докажите достаточность в критерии 2.13 Галуа разрешимости уравнения.

(b) Докажите необходимость в критерии 2.13 для $n \leqslant 4$.

(c) Сформулируйте и докажите аналог критерия 2.13 для 1-радикальности (т.е. для радикальности с одним извлечением корня).

(d) Сформулируйте и докажите вещественный аналог критерия 2.13.

4.6. Пусть $x_1, \ldots, x_n \in \mathbb{C}$ — все корни многочлена $A \in \mathbb{Q}[t]$ с учетом кратности, q простое, $r \in \mathbb{C} - \mathbb{Q}$, $r^q \in \mathbb{Q}$, $U \in \mathbb{Q}[\vec{u}]$,v $U(\vec{x}) \in \mathbb{Q}[r] - \mathbb{Q}$ и $\mathrm{id} \in G \subset \Sigma_n$.

(a) Верно ли, что если $\sum_{\alpha \in G} U(\vec{x}_\alpha) \in \mathbb{Q}$, то $\sum_{\alpha \in G} U(\vec{x}_{\alpha\tau}) \in \mathbb{Q}$ для любой перестановки $\tau \in \Sigma_n$?

(b) Верно ли, что если $\prod_{\alpha \in G} (t - U(\vec{x}_\alpha)) \in \mathbb{Q}[t]$, то $\sum_{\alpha \in G} (t - U(\vec{x}_{\alpha\tau})) \in \mathbb{Q}[t]$ для любой перестановки $\tau \in \Sigma_n$?