# Доказательство Кронекера теоремы Галуа о неразрешимости уравнений в радикалах

представляют Д. Герасимов, Е. Коган,
Е. Морозов, Я. Пан, А. Скопенков *

## Содержание



*Благодарим В. Волкова за полезные обсуждения и Б. Френкина за перевод части текста на русский язык.

*Д. Герасимов:* Физтех-лицей (Долгопрудный),
*Е. Коган, Е. Морозов:* Высшая школа экономики (Москва).
*Я. Пан:* Институт науки и технологии провинции Хенан (Китай).
*А. Скопенков:* Московский Физико-Технический Институт, Независимый Московский Университет. `https://users.mccme.ru/skopenko/`.

*And the leap is not — is not what I think you sometimes see it as — as breaking, as acting. It's something much more like a quiet transition after a lot of patience and — tension of thought, yes — but with that [enlightenment] as its discipline, its orientation, its truth. Not confusion and chaos and immolation and pulling the house down, not something experienced as a great significant moment.*
I. Murdoch, The Message to the Planet

# 1 Введение и основные результаты

## 1.1 Обзор и мотивировки

Этот раздел не используется в дальнейшем.

Данный текст содержит короткое изложение доказательства Кронекера теоремы Галуа 1.3.2 о неразрешимости алгебраических уравнений в радикалах. Это доказательство интересно, так как предположительно оно является самым коротким.

Мы не используем термин «группа Галуа» и даже термин «группа». Тем не менее наше изложение дает неплохую возможность освоить (или освежить в памяти) некоторые идеи, лежащие в основе теории Галуа. Таким образом, данный проект перекидывает мост (показывая, что нет никакой пропасти) между элементарной математикой и теорией Галуа. Проект доступен школьникам, знакомым с многочленами и комплексными числами (знакомства с перестановками не требуется).

Приводимые доказательства не претендуют на новизну (возможно, за исключением методических находок). Главная идея доказательства известна (см. [Do65, §25], [Pr07, Ti03]), и предположительно принадлежит Кронекеру (ошибка в приведенных выше текстах, указанная в [Sk21m, Замечание 8.4.18b], исправлена в [Sk08, PC19] и [Sk21m, §8]). К сожалению, само доказательство не очень широко известно.

Приводимое доказательство интересно также тем, что оно не использует перестановки. Поэтому в качестве «причины» возникновения неразрешимости в радикалах мы видим не тот факт, что группа $A_5$ неразрешима, а что существует многочлен степени 5 с

рациональными коэффициентами, неприводимый над $\mathbb{Q}$, имеющий более одного вещественного корня и хотя бы один невещественный корень. Таким образом, данное доказательство отлично от доказательств теорем Галуа и Абеля, приводимых в [**?**, Ay82, Be10, Br, Ed84, FT, Ha78, Le11, PC19, Pe04, Ro95, St94, Sk15] (комментарии и исправления некоторых ошибок см. в [Sk15]).

## 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 $x, y$,

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

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

**1.2.1.** (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.

(c) Уравнение $x^4 + 4x - 1 = 0$ имеет два вещественных корня, каждый из которых вещественно радикален.

**Теорема 1.2.2.** (a) Число $\cos(2\pi/9)$ не является вещественно радикальным.

(b) Существует многочлен 3-й степени с рациональными коэффициентами (например, $x^3 - 3x + 1$), ни один из корней которого не является вещественно радикальным.

Вы сможете доказать п. (b) этой теоремы с помощью задач, выдаваемых до промежуточного финиша. Разрешается использовать п. (b) без доказательства для решения других задач в §1.2.

**1.2.3.** (a) Для любого $n \geqslant 3$ существует многочлен $n$-й степени с рациональными коэффициентами , один из корней которого не является вещественно радикальным.

(b) Справедлив аналог утверждения п. (a) с заменой слов «один из корней» на «ни один из корней». (При этом корни *некоторых* уравнений высоких степеней (например, $x^5 = 2$) вполне могут быть вещественно радикальны.)

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

### 1.3 Неразрешимость в комплексных радикалах

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 $n > 0$.

**1.3.1.** (a) Любой (комплексный) корень квадратного уравнения с рациональными коэффициентами радикален.

(b) Число $\cos(2\pi/9)$ радикально.

(c,d) То же, что и в п. (a) для многочленов 3-й и 4-й степени.

(e) Если действительная и мнимая части комплексного числа $z$ вещественно радикальны, то число $z$ радикально.

(f) Обратное утверждение к п. (e) неверно.

Аналоги утверждений пп. (a,c,d) для уравнений более высоких степеней неверны.

**Теорема 1.3.2** (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 разрешимости уравнений в радикалах решили доказанные немного ранее более слабые теоремы Руффини–Абеля. Строгие формулировки этих теорем сложнее [Sk21m, Теорема Руффини 8.2.2], [Sk15, Замечание 7]. Более простой способ

решить проблему разрешимости уравнений в радикалах предложен в [Sk21m, Теорема 8.1.13 и ее доказательство в §8.4.F]. Здесь мы предлагаем другой короткий способ: вывести теорему Галуа 1.3.2 из следующего результата.

**Теорема 1.3.3** (Кронекер)**.** Если многочлен простой степени с рациональными коэффициентами неприводим над $\mathbb{Q}$, имеет более одного вещественного корня и хотя бы один невещественный, то ни один из его корней не является радикальным.

Эта теорема интересна и нетривиальна даже для многочлена пятой степени. Вы сможете доказать эту теорему с помощью задач, выдаваемых после промежуточного финиша.

## 1.4 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 условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. *Загадкой* называется не сформулированный четко вопрос; здесь нужно придумать и четкую формулировку, и доказательство. 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 уже знаете решения нескольких предложенных задач. Если Вы подтвердите свои знания, со-

общив нам решения некоторых из них, Вам будет разрешено не получать плюсы по всем этим задачам, но пользоваться ими при решении остальных.

## 2 Доказательства неразрешимости в задачах

В этом тексте «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 (1-2)

**2.1.1.** 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) $\sqrt[3]{2}$;

(e) $\sqrt{2}+\sqrt[3]{2}$; (f) $\sqrt{2+\sqrt{2}}$; (g) $\sqrt{2}+\sqrt{3}+\sqrt{5}$; (h) $\cos(2\pi/9)$?

Для п. (g) вам потребуются идеи из §2.4.

**Лемма 2.1.2** (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 $b > 0$.

**Лемма 2.1.3.** 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 $P$ имеет корень $r$, то $P$ 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 2.1.4.** Если многочлен степени выше второй неприводим над $\mathbb{Q}$, то ни один из его корней не представим в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$.

## 2.2 Одно извлечение корня третьей степени

**2.2.1.** 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 2.2.2.** 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 2.2.3.** Пусть многочлен неприводим над $\mathbb{Q}$ и либо его степень отлична от 3 и 1, либо он имеет более одного вещественного корня. Тогда ни один из его корней не представим в виде $a + br + cr^2$, где $r \in \mathbb{R} - \mathbb{Q}$ и $a, b, c, r^3 \in \mathbb{Q}$.

**Лемма 2.2.4** (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 $a, b, c, r^3 \in \mathbb{Q}$.

## 2.3 Одно извлечение корня простой степени

**2.3.1.** 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 $x^7 - 4x + 2$.

**Лемма 2.3.2.** 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

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

**2.3.3.** 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 2.3.4.** * 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 2.3.5.** Пусть многочлен неприводим над $\mathbb{Q}$ и либо его степень отлична от простого $q$ и от 1, либо он имеет более одного вещественного корня. Тогда ни один из его корней не представим в виде $A(r)$ для некоторых $r \in \mathbb{R} - \mathbb{Q}$ и многочлена $A \in \mathbb{Q}[x]$, причём $r^q \in \mathbb{Q}$.

**Лемма 2.3.6** (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 $q \in \mathbb{Z}$.

Таким образом, если многочлен простой степени, большей 2, неприводим над $\mathbb{Q}$ и имеет более одного вещественного корня, то ни один из этих корней не является вещественно радикальным с извлечением корня только один раз.

## 2.4 Несколько извлечений квадратных корней

**2.4.1.** Существуют ли рациональные числа $a, b, c, d$, для которых $\sqrt[3]{2}$ равно

(a) $a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}$; (b) $\dfrac{a+\sqrt{b}}{c+\sqrt{b}}$; (c) $a + \sqrt{b} + \sqrt{c}$;

(d) $a + \sqrt{b + \sqrt{c}}$; (e) $a + \sqrt{b} + \sqrt{c} + \sqrt{d}$?

**2.4.2.** (a) Число $\sqrt[3]{2}$ не является вещественно радикальным с извлечением корней только квадратных и только два раза.

(b) Число $\cos(2\pi/9)$ не является вещественно радикальным с извлечением корней только два раза.

Если $F \subset \mathbb{C}$, $r \in \mathbb{C}$ и $r^q \in F$ для некоторого целого положительного $q$, то обозначим

$$F[r] := \{a_0 + a_1 r + a_2 r^2 + \ldots + a_{q-1} r^{q-1} \mid a_0, \ldots, a_{q-1} \in F\}.$$

В этом тексте **полем** называется подмножество множества $\mathbb{C}$, замкнутое относительно операций сложения, умножения, вычитания и деления на ненулевое число. Общепринятое название: числовое поле (а *полем* в математике называется более общий объект). Это понятие полезно для нас тем, что теорема делении с остатком верна для многочленов с коэффициентами в поле.

**Лемма 2.4.3** (о радикальном расширении)**.** Если число $a \in \mathbb{C}$ радикально, то некоторое содержащее его поле можно получить из

$\mathbb{Q}$ следующими операциями: заменить поле $F$ на $F[r]$ для некоторого $r \in \mathbb{C}$ такого, что $r^q \in F$ для некоторого простого $q$.

**2.4.4.** (a–d) Докажите аналоги утверждений 2.3.2.(a–d) с заменой $\mathbb{Q}$ на произвольное поле и многочлены над $\mathbb{Q}$ на многочлены над этим полем.

**Лемма 2.4.5.** Пусть $q$ простое, $F \subset \mathbb{R}$ — поле, $r \in \mathbb{R} - F$ и $r^q \in F$. Если многочлен с коэффициентами в $F$ степени 3 имеет три вещественных корня, ни один из которых не лежит в $F$, то ни один из его корней не лежит в $F[r]$.

## 2.5 К теореме Кронекера

В этом пункте $q > 2$ — *простое число,* $r \in \mathbb{C}$ — *комплексное число,* $F \subset \mathbb{C}$ — *поле, содержащее* $\varepsilon = \varepsilon_q$ *и* $r^q$*, но не содержащее* $r$.

**Лемма 2.5.1.** (a) **Неприводимость.** Многочлен $t^q - r^q \in F[t]$ неприводим над $F$.

(b) **Линейная независимость.** Если $P(r) = 0$ для некоторого многочлена $P \in F[t]$ степени меньше $q$, то $P = 0$.

(c) **Сопряжение.** Если $P(r) = 0$ для некоторого многочлена $P \in F[t]$, то $P(r\varepsilon^k) = 0$ для любого $k = 1, \ldots, q-1$.

(d) **Параметрическое сопряжение.** Если $P \in F[x,t]$, причём $P(x,r) = 0$ как многочлен от $x$, то $P(x, r\varepsilon^k) = 0$ как многочлен от $x$ при любом $k = 0, 1, \ldots, q-1$.

(e) **Рациональность.** Для любого $H \in F[x,t]$ верно, что

$$H(x,r)H(x,\varepsilon r)\ldots H(x,\varepsilon^{q-1}r) \in F[x].$$

(f) **Вещественность.** Пусть $F = \overline{F}$, а также $r \in \mathbb{R}$ или $|r|^2 \in F$. Тогда среди значений $A(r\varepsilon^k)$ многочлена $A \in F[t]$ при $k = 0, 1, \ldots, q-1$ либо не более одно является вещественным, либо все эти значения вещественны.

**2.5.2.** (a) Пусть $H \in F[x,t]$ и $H(x,r)$ неприводим над $F[r]$. Тогда для любого $k = 0, 1, \ldots, q-1$ многочлен $H(x, r\varepsilon^k)$ также неприводим над $F[r]$.

(b) Пусть $H \in F[x,t]$ и $H(x,r)$ — неприводимый над $F[r]$ множитель над $F[r]$ неприводимого над $F$ многочлена $G \in F[x]$, причем

$0 < \deg H(x,r) < \deg G$. Тогда $G$ делится над $F$ на произведение

$$H(x,r)H(x,\varepsilon r)\dots H(x,\varepsilon^{q-1}r).$$

(c) Если в условиях п. (b) $\deg G$ простое, то существует такой многочлен $A \in F[t]$, что корни многочлена $G$ равны $A(r\varepsilon^k)$ при $k = 0, 1, \dots, q-1$.

**Лемма 2.5.3** (о сохранении неприводимости)**.** Пусть $F = \overline{F}$, а также $r \in \mathbb{R}$ или $|r|^2 \in F$, причем многочлен $G \in F[t]$ простой степени имеет более одного вещественного корня и не менее одного не вещественного. Если при этом $G$ неприводим над $F$, то $G$ неприводим над $F[r]$.

**Лемма 2.5.4** (о хитром радикальном расширении)**.** (a) Если число $a \in \mathbb{C}$ радикально, то некоторое содержащее его поле можно получить из $\mathbb{Q}$ следующими операциями: заменить поле $F$ на $F[r]$ для некоторого $r \in \mathbb{C}$, такого, что $r \in \mathbb{R}$ или $|r|^2 \in F$, причем $r^q \in F$ для некоторого простого $q$.

(b) То же, что в п. (a), с заменой $r^q \in F$ на $r^q, \varepsilon \in F$.

В доказательстве п. (b) можно использовать без доказательства следующий результат (его элементарное доказательство на одной странице см. в [ZSS, §5], [Sk21m, §8.4.D], [Sk21y]).

**Теорема 2.5.5** (теорема Гаусса о понижении степени)**.** Если $q$ простое, то число $\varepsilon$ радикально с использованием лишь корней степени $q-1$.

## 2.6 Решения задач до промежуточного финиша

**2.1.1.** *Ответы*: (a), (b), (c) — да, (d), (e), (f), (g), (h) — 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) 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 2.1.4.

(e) *Набросок первого решения.* Предположим противное и возведем в куб равенство $\sqrt[3]{2} = a + \sqrt{b} - \sqrt{2}$.

*Набросок второго решения.* Докажем, 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 утверждению (d).

*Набросок третьего решения.* Пусть $\sqrt{2} + \sqrt[3]{2} = a + \sqrt{b}$ для некоторых $a, b \in \mathbb{Q}$. Это число является корнем многочлена $P(x) := ((x-\sqrt{2})^3 - 2)((x+\sqrt{2})^3 - 2)$ с рациональными коэффициентами. По лемме о сопряжении 2.1.3 (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.

(f) *Набросок первого решения.* Предположим противное и возведем в квадрат равенство $\sqrt{2 + \sqrt{2}} = a + \sqrt{b}$.

*Набросок второго решения.* 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 2.1.4 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.

(h) Пусть число $\cos(2\pi/9)$ представимо. Тогда оно является корнем уравнения $4x^3 - 3x = -\frac{1}{2}$. По следствию 2.1.3(f) это уравнение имеет рациональный корень. Противоречие.

**2.1.2.** Обозначим через $\sqrt{c}$ число, полученное при единственном извлечении корня, где $c \in \mathbb{Q}$. Докажем, что все полученные числа имеют вид $a + b\sqrt{c}$, где $a, b \in \mathbb{Q}$. Достаточно доказать, что множество чисел такого вида замкнуто относительно сложения, вычитания,

умножения и деления. Это неочевидно только в случае деления, для которого оно следует из равенства $(a+b\sqrt{c})(a-b\sqrt{c}) = a^2-b^2c$.

**2.1.3.** (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[1] 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.

(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.

**2.1.4.** Пусть, напротив, данный многочлен $P$ имеет корень $x_0 = a \pm \sqrt{b}$, где $\sqrt{b} \notin \mathbb{Q}$. По лемме 2.1.3 (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.

**2.2.1.** *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

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

2.2.2 (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 2.2.2 (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 $\mathbb{Q}[\varepsilon_3]$ 2.2.2 (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 2.2.4.) 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.

(f) Доказательство аналогично п. (c).

**2.2.2.** (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 2.2.2 (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.

**2.2.4.** 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.

**2.3.2.** (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 произведению 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 многочлена $A$.

(c) Доказательство аналогично задачам 2.1.3 (c, d), 2.2.2 (d). Используйте п. (b).

(d) Доказательства повторяют второе и третье доказательства леммы о рациональности 2.2.2 (f). Нужно только везде заменить 3 на $q$ и 2 на $q-1$ (например, во второй строчке второго доказательства $k = 0, 1, 2, \ldots, q$).

## 2.7 Решения остальных задач

**1.2.3.** (a,c) Это следует из Теорем 1.2.2.b,a, соответственно.

**1.3.1.** (c,d) Используйте *методы дель Ферро и Феррари* [Sk21m, §3].

**2.2.1.** (d) Если число $\sqrt[5]{3}$ представимо, то по лемме о рациональности 2.2.2 (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 2.2.2 (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 $\mathbb{Q}[\varepsilon_3]$ 2.2.2 (b′) получаем, что $a = 0$ и $bc = 0$. Поэтому либо $\sqrt[3]{3} = br$, либо $\sqrt[3]{3} = cr^2$. Противоречие.

**2.2.3.** По лемме о рациональности 2.2.2 (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 2.2.2 (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 $\mathbb{Q}[\varepsilon_3]$ 2.2.2 (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.

**2.3.1.** 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 2.3.2 (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 лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 2.3.4 (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 $\varepsilon_7$ является корнем неприводимого[2] многочлена $1 + x + \ldots + x^6$, что противоречит аналогу теоремы 2.1.4 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 2.3.2 (c) и о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 2.3.4 (b) этот многочлен имеет семь попарно различных корней, что невозможно.

(c) Пусть число $\sqrt[11]{3}$ представимо. Тогда по лемме о рациональности 2.3.2 (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 $\mathbb{Q}[\varepsilon_q]$ 2.3.4 (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 2.3.2.c и лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 2.3.4.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.

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

**2.3.3.** (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 2.3.2 (a) получаем $r \in \mathbb{Q}[\varepsilon_q]$. Противоречие.

Пункты (b) и (c) выводятся из п. (a) аналогично соответствующим пунктам задачи 2.3.2.

**2.3.5.** Предположим противное. Обозначим данный многочлен через $P$. При $q < \deg P$ получаем противоречие с леммой о рациональности 2.3.2 (d). При $q \geqslant \deg P$ по лемме о сопряжении 2.3.2 (c) и лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 2.3.4 (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.

**2.4.1.** *Ответы*: нет. Доказательства аналогичны решениям задач 2.1.1.(e,g). (a) *Первое решение.* Перепишем условие в виде $(a + c\sqrt{2}) + (b + d\sqrt{2})\sqrt[4]{2} = 0$. Так как $b + d\sqrt{2} \neq 0$, то $-\sqrt[4]{2} = \frac{a+c\sqrt{2}}{b+d\sqrt{2}} = A + B\sqrt{2}$ для некоторых $A, B \in \mathbb{Q}$. Возводя в квадрат, получаем $A^2 + 2B^2 = 0$. Противоречие.

*Второе решение.* Рассматривая все комплексные корни многочлена $x^4 - 2$, докажем его неприводимость над $\mathbb{Q}$. Поэтому он не может иметь общий корень с многочленом $a+bx+cx^2+dx^3$ не более чем третьей степени.

(b) Домножьте на сопряжённое.

(c) Проще доказать сразу, что $\sqrt[3]{2} \neq a + p\sqrt{b} + q\sqrt{c} + r\sqrt{bc}$, где $a, b, c, p, q, r \in \mathbb{Q}$. Для этого достаточно доказать, что $\sqrt[3]{2} \neq u + v\sqrt{c}$, где $u$ и $v$ - числа вида $\alpha+\beta\sqrt{b}, \alpha, \beta \in \mathbb{Q}$ (с фиксированным $b$) "ничуть не хуже"рациональных чисел, т.е. сумма, разность, произведение и частное чисел такого вида тоже являются числами такого вида (или, говоря научно, такие числа будут образовывать *числовое поле*). Поэтому можно доказывать утверждение аналогично 2.1.1(e).

**2.4.2** (a) Докажем более сильный факт: число $\sqrt[3]{2}$ не является радикальным с извлечением любого количества квадратных корней.

Тогда существует такая башня квадратичных расширений

$$\mathbb{Q} = F_1 \subset F_1 \subset F_2 \subset F_3 \subset ...F_{s-1} \subset F_s \subset \mathbb{R},$$

что $\sqrt[3]{2} \in F_s - F_{s-1}$. Поскольку $\sqrt[3]{2} \notin \mathbb{Q}$, получаем, что $s \geqslant 2$. Значит,

$$\sqrt[3]{2} = \alpha + \beta\sqrt{a}, \quad \text{где} \quad \alpha, \beta, a \in F_{s-1}, \quad \sqrt{a} \notin F_{s-1} \quad \text{и} \quad \beta \neq 0.$$

Отсюда

$$2 = (\sqrt[3]{2})^3 = (\alpha^3 + 3\alpha\beta^2 a) + (3\alpha^2\beta + \beta^3 a)\sqrt{a} = u + v\sqrt{a}.$$

Поскольку $2 \in \mathbb{Q} \subset F_{s-1}$, имеем $2 - u \in F_{s-1}$. Из того, что

$$v\sqrt{a} = 2 - u \quad \text{и} \quad v \in F_{s-1},$$

следует равенство

$$0 = v = 3\alpha^2\beta + \beta^3 a.$$

Так как $3\alpha^2 + \beta^2 a > 0$, то $\beta = 0$. Противоречие.

Решения остальных задач можно найти в [ZSS, §9.1, §9.4.5, §9.4.7] (это §5.1, §5.4.3, §5.4.4 бумажной версии). В частности, доказательства теорем 1.2.2.a и 1.3.3 приведены в [ZSS, §9.4.5, §9.4.7], соответственно.

## Список литературы


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

[ABG] 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`.

[Ay82] *R. G. Ayoub*, On the Nonsolvability of the General Polynomial, Amer. Math. Monthly, 89:6 (1982), 397–401.

[Be06] *J. Bewersdorff,* Galois Theory for Beginners: A Historical Perspective, AMS, 2006.

[Be10] *J. Bergen*, A Concrete Approach to Abstract Algebra: From the Integers to the Insolvability of the Quintic, 2010.

[Br] *J. Brown,* Abel and the insolvability of the quintic, `http://www.math.caltech.edu/~jimlb/abel.pdf`.

[Do65] *H. Dörrie*, 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.

[Ed84] *H. M. Edwards*, Galois Theory. Springer Verlag, 1984.

[FT] *Табачников С. Л., Фукс Д. Б.* Математический дивертисмент, М.: МЦНМО, 2011. `http://www.math.psu.edu/tabachni/Books/taba.pdf`

[Ha78] *Ch. R. Hadlock*, Field Theory and its Classical Problems. The Mathematical Association of America, 1978.

[Le11] *L. Lerner*, Galois Theory without abstract algebra. `http://arxiv.org/abs/1108.4593`.

[PC19] *Y. Pan and Y. Chen.* On Kronecker's Solvability Theorem, `http://arxiv.org/abs/1912.07489`.

[Pe04] *P. Pesic*, Abel's Proof, The MIT Press, 2004, Cambridge, Massachusetts, London, England.

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

[Ro95] *M. I. Rosen*, Niels Hendrik Abel and Equations of the Fifth Degree, Amer. Math. Monthly, 102:6 (1995) 495-505.

[Sk08] *Скопенков А.* Ещё несколько доказательств из Книги: разрешимость и неразрешимость уравнений в радикалах. `http://arxiv.org/abs/0804.4357`.

[Sk10] *Скопенков А.* Базисные вложения и 13-я проблема Гильберта, Мат. Просвещение, 14 (2010) 143–174; `http://arxiv.org/abs/1001.4011`.

[Sk11] *Скопенков А.* Простое доказательство теоремы Абеля о неразрешимости уравнений в радикалах, Мат. Просвещение, 15 (2011), 113–126; http://arxiv.org/abs/1102.2100.

[Sk15] *A. Skopenkov*, A short elementary proof of the Ruffini-Abel Theorem. http://arxiv.org/abs/1508.03317.

[Sk21m] *A. Skopenkov.* Mathematics Through Problems: from olympiades and math circles to a profession. Part I. Algebra. 2021, AMS, Providence. Preliminary version: https://www.mccme.ru/circles/oim/algebra_eng.pdf

[Sk21y] *Скопенков А.* Еще одно доказательство из книги: теорема Гаусса-Ванцеля, Мат. Просвещение, 2021.

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

[Ti03] *Тихомиров В. М.* Абель и его великая теорема, Квант. 2003. N1, 11–15.

[Va] *Вагутен Н.* Сопряжённые числа, Квант. 1980. N2, 26–32.

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