

ЕЩЕ ОДНО ДОКАЗАТЕЛЬСТВО ИЗ КНИГИ: НЕРАЗРЕШИМОСТЬ УРАВНЕНИЙ В РАДИКАЛАХ ¹

А. Скопенков ²

Аннотация. Приводятся наброски простых доказательств того, что существует уравнение

- 3-й степени, неразрешимое в *вещественных* радикалах;
- 5-й степени, неразрешимое в *комплексных* радикалах (теорема Галуа).

Заметка адресована тем, кому интересен хотя бы один из этих результатов. Определение разрешимости в радикалах приводится; для понимания доказательств достаточно знакомства с многочленами и умения извлекать корни из комплексных чисел (в конце доказательства теоремы Галуа используется также теорема о размерности башни расширений). Доказательства основаны на идее *сопряжения*.

Разбор доказательств (или их начала) полезен для закрепления тем ‘многочлены’, ‘комплексные числа’, ‘иррациональность’, и ‘числа, построимые циркулем и линейкой’ на кружке или в матклассе. Старшеклассники найдут в заметке задачи для исследования, не претендующие на научную новизну.

1 Введение

Разрешимость в вещественных радикалах.

Рассмотрим калькулятор с кнопками

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

Калькулятор вычисляет числа с абсолютной точностью и имеет неограниченную память. При делении на 0 он выдает ошибку.

Пусть сначала калькулятор *вещественный*, т.е. оперирует с вещественными числами и при извлечении корня четной степени из отрицательного числа выдает ошибку. ³

Следующее утверждение хорошо известно (см., например, [Z], стр. 22).

Если многочлен третьей степени с рациональными коэффициентами имеет ровно один вещественный корень, то этот корень можно получить на вещественном калькуляторе. Более того, это можно сделать так, чтобы извлечение корня происходило только два раза, один раз второй и один раз третьей степени.

Теорема о неразрешимости в вещественных радикалах. *Существует многочлен 3-й степени с рациональными коэффициентами (например, $8x^3 - 6x + 1$), ни один из корней которого невозможно получить на вещественном калькуляторе.*

Эта теорема, по-видимому, является фольклорным результатом. Она доказана в [W] с использованием теории Галуа. Мы приведем набросок ее простого прямого доказательства (и даже теоремы 7.5 ниже).

Следствие. *Трисекция угла неосуществима на вещественном калькуляторе. Или, формально, число $\cos(\alpha/3)$ невозможно получить на нем, имея число $\cos \alpha$ (например, для $\alpha = \pi/3$).*

¹Обновляемая версия: www.mcsme.ru/circles/oim/kroneck.pdf. Заметка основана на занятиях, проведенных в 2011 г. в Кировской ЛМШ, Московской ОВШ и на кружках ‘Математический семинар’, ‘Олимпиады и математика’. Благодарю В.В. Волкова, А.С. Голованова, А.Д. Руховича, Л.М. Самойлова, М.Б. Скопенкова, Г.Р. Челнокова, Л.А. Шабанова и В.В. Шувалова за полезные обсуждения.

²Поддержан грантом фонда Саймонса. Независимый Московский Университет. Инфо: www.mcsme.ru/~skopenko

³Если это определение кажется Вам недостаточно строгим, то примите в качестве определения утверждение леммы о калькуляторе 7.1 ниже, взяв $K = \mathbb{R}$ для вещественного калькулятора и $K = \mathbb{C}$ — для комплексного.

Доказательство. По формуле косинуса тройного угла каждое из чисел $\cos(\pi/9)$, $\cos(7\pi/9)$, $\cos(5\pi/9)$ удовлетворяет уравнению $8x^3 - 6x + 1 = 0$. Значит, то теореме ни одно из них невозможно получить на вещественном калькуляторе. QED

Хорошо известен аналог этого следствия для вещественного калькулятора, на котором корни можно извлекать только второй степени [KS, P, S2].

Разрешимость в комплексных радикалах.

Пусть теперь калькулятор *комплексный*, т.е. оперирует с комплексными числами и при нажатии кнопки $\sqrt{}$ выдает все значения корня.

Следующее утверждение хорошо известно (см., например, [Z], стр. 22).

Все корни любого многочлена третьей или четвертой степени с рациональными коэффициентами можно получить на комплексном калькуляторе. Более того, это можно сделать так, чтобы извлечение корня происходило только

- *два раза, причем один раз третьей степени и один раз второй — для многочлена третьей степени.*
- *четыре раза, причем один раз третьей степени и три раза второй — для многочлена четвертой степени.*

Теорема Галуа. *Существует многочлен 5-й степени (например, $x^5 - 4x + 2$), ни один из корней которого невозможно получить на комплексном калькуляторе.*⁴

Из приведенных теорем нетрудно вывести, что для любого $n \geq 3$ ($n \geq 5$) существует многочлен n -й степени, ни один из корней которого невозможно получить на вещественном (комплексном) калькуляторе.

О чем эта заметка.

Мы приведем *простое доказательство теоремы Галуа* (и даже теоремы Кронекера 8.1). Его идеи являются отправными для *конструктивной теории Галуа* [E2]. Приводимое доказательство отлично от доказательства из [A, FT, S].⁵ Наше изложение основано на замечательной статье [T] и книгах [P, D]. Основное отличие нашего изложения — возможность увидеть, *как такое доказательство можно придумать*. Основные идеи представлены на ‘олимпиадных’ примерах: на простейших частных случаях, свободных от технических деталей, и со сведением к необходимому минимуму алгебраического языка.⁶ Несмотря на отсутствие термина ‘группа’, *идея сопряжения*, на которой основано приводимое доказательство — одна из отправных для теории Галуа. Ср. [S1, L, V].

Более конкретно, основные идеи заключены в леммах о калькуляторе (задачи 2.5, 3.5, 4.8, 5.5, 7.1), о сопряжении (задачи 2.2, 3.2, 4.2, 5.3.b, 7.3.d) и о вещественности (задачи 4.4.a, 5.3.e, 7.3.e, 8.2). Сначала доказывается неразрешимость при условии, что *извлечение корня проходило только один раз*.⁷ Благодаря этому основные идеи преподносятся

⁴Немного ранее была доказана более слабая теорема П. Руффини - Н.Х. Абеля. Она сложнее формулируется [A, FT, S], но более знаменита, ибо именно она решила знаменитую проблему о разрешимости уравнений в радикалах. Наиболее простое известное мне доказательство теоремы Руффини-Абеля (приводимое здесь) дает сразу теорему Галуа.

⁵Почему корни любого уравнения степени ниже 5 выражаются в радикалах через коэффициенты, а степени 5 и выше — нет? Доказательство из [A, FT, S] дает такой ответ: поскольку группа S_n разрешима в точности при $n \leq 4$. Приводимое доказательство дает такой ответ: поскольку 5 простое и больше 3. Простота ‘причины’ неразрешимости косвенно подтверждает простоту доказательства.

⁶Это не только делает материал более доступным, но поможет тем, кто привык к абстрактному изложению, развить математический вкус. Благодаря этому они смогут разумно выбирать проблемы для исследования и ясно излагать собственные открытия, не скрывая ошибок (или известности полученного результата) за чрезмерным формализмом. К сожалению, такое (бессознательное) сокрытие ошибки часто происходит с молодыми математиками, воспитанными на чрезмерно формальных курсах. Происходило и с автором этих строк; к счастью, все мои серьезные ошибки исправлялись *перед* публикациями.

⁷В процессе доказательства возникают дополнительные ограничения, см. далее. Такую неразрешимость можно доказать по-другому [Ch]. Тот способ сложнее переносится на общий случай.

на примере рациональных чисел (а не произвольных полей и даже не полей из башни расширений).

Доказательство намечено в виде задач. (Это характерно не только для дзенских монастырей, но и для серьезного преподавания математики.) К задачам приведены указания и решения. Многие из приведенных задач — удачные темы для исследовательских работ школьников, не претендующих на научную новизну. Например, 7.5 (здесь было бы интересно обойтись без теоремы о размерности башни), задачи из §9 (этот параграф не зависит от §§6-8), 2.4, 3.4, 4.7, 5.1.d и 5.4.

Мы долго будем *придумывать* доказательства. *Изложить* же их можно коротко. Такое изложение приводится в §§7-8. (Освобождение доказательства от деталей, возникших при его придумывании и не нужных для него самого — важная часть его проверки.)

Соглашения.

Через \mathbb{Q} обозначается множество всех рациональных чисел. ‘Многочлен с рациональными коэффициентами’ мы коротко называем многочленом. Многочлен называется *неприводимым*, если он не раскладывается в произведение многочленов меньшей степени.

Для доказательства теоремы Галуа можно считать, что комплексный калькулятор при извлечении корня выдает *одно* значение корня, выбираемое программистом. Так мы и будем считать. При этом обозначение $\sqrt[n]{a}$ для $a \in \mathbb{R}$ сохраняет свой обычный смысл.

Общее замечание к формулировкам задач: если условие задачи является утверждением, то в задаче требуется это утверждение доказать. Если некоторая задача не получается, то читайте дальше — соседние задачи могут оказаться подсказками. (На занятии задача-подсказка выдается только тогда, когда школьник подумал над самой задачей.)

2 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) $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2}$; (c) $\sqrt[3]{7 + 5\sqrt{2}}$; (d) $\sqrt[3]{2}$; (e) $\sqrt{2} + \sqrt[3]{2}$;
(f) $\cos(\pi/5)$; (g) $\cos(2\pi/7)$; (h) $\cos(\pi/9)$.

2.2. Лемма о сопряжении. Если $a, b \in \mathbb{Q}$ и $a + b\sqrt{2}$ — корень многочлена, то $a - b\sqrt{2}$ — тоже его корень.

2.3. Лемма о линейной независимости. Если $a + b\sqrt{2} = 0$ для некоторых $a, b \in \mathbb{Q}$, то $a = b = 0$.

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

2.5. Лемма о калькуляторе. Пусть $K \in \{\mathbb{R}, \mathbb{C}\}$. Число, которое можно получить на K -калькуляторе так, чтобы извлечение корня происходило только один раз, причем второй степени, имеет вид $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$ и, для $K = \mathbb{R}$, $b > 0$.

Задачи 2.1 и 2.4 интересны в связи с неразрешимостью в радикалах, поскольку нам нужно придумать многочлен, корни которого невозможно получить на калькуляторе, а числа из задачи 2.1 являются корнями многочленов (подумайте, каких).

Из утверждения 2.4 и леммы 2.5 о калькуляторе вытекает, что *если многочлен степени выше второй неприводим, то ни один из его корней невозможно получить на вещественном калькуляторе так, чтобы извлечение корня происходило только один раз, причем второй степени.* Это — наше первое продвижение к теоремам о неразрешимости в радикалах. Аналогичные продвижения в следующих двух пунктах (сформулируйте их самостоятельно) вытекают из соответствующих утверждений и лемм о калькуляторе.

3 Одно извлечение корня четвертой степени

3.1. Представимо ли следующее число в виде $a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}$, где $a, b, c, d \in \mathbb{Q}$?

(a) $\sqrt[3]{3}$; (b) $\sqrt[6]{3}$.

3.2. Лемма о сопряжении. Пусть $a, b, c, d \in \mathbb{Q}$ и $a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8}$ корень многочлена. Тогда корнем этого многочлена также является число

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

(b) $a - c\sqrt{2} + i\sqrt[4]{2}(b - d\sqrt{2})$ и $a - c\sqrt{2} - i\sqrt[4]{2}(b - d\sqrt{2})$.

3.3. Лемма о линейной независимости.

(a) Если $a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8} = 0$ для некоторых $a, b, c, d \in \mathbb{Q}$, то $a = b = c = d = 0$.

(b) Если $a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8} = 0$ для некоторых $a, b, c, d \in \mathbb{Q}[i] := \{x + iy : x, y \in \mathbb{Q}\}$, то $a = b = c = d = 0$.

3.4. Утверждение. Если многочлен степени, отличной от 1, 2 и 4, неприводим над \mathbb{Q} , то ни один из его корней не представим в виде $a + br + cr^2 + dr^3$, где $r \in \mathbb{C}$ и $a, b, c, d, r^4 \in \mathbb{Q}$.

3.5. Лемма о калькуляторе. Пусть $K \in \{\mathbb{R}, \mathbb{C}\}$. Число, которое можно получить на K -калькуляторе так, чтобы извлечение корня происходило только один раз, причем четвертой степени, имеет вид $a + br + cr^2 + dr^3$, где $r \in K$ и $a, b, c, d, r^4 \in \mathbb{Q}$.

4 Одно извлечение корня третьей степени

4.1. 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) $\cos(\pi/9)$; (c) $\sqrt[5]{3}$.

Обозначим $\varepsilon := \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$.

4.2. Лемма о сопряжении. Пусть $r \in \mathbb{C}$, $r^3, a, b, c \in \mathbb{Q}$ и многочлен имеет корень $a + br + cr^2$. Тогда корнем этого многочлена также является число

(a) $a + b\varepsilon r + c\varepsilon^2 r^2$.

(b) $a + b\varepsilon^2 r + c\varepsilon r^2$.

4.3. Пусть $r \in \mathbb{C}$, $r^3 \in \mathbb{Q}$ и $r^3 \neq b^3$ ни для какого $b \in \mathbb{Q}$.

(a) Если $a + br + cr^2 = 0$ для некоторых $a, b, c \in \mathbb{Q}$, то $a = b = c = 0$.

(b) **Лемма о линейной независимости.** Если $a + br + cr^2 = 0$ для некоторых $a, b, c \in \mathbb{Q}[\varepsilon] := \{x + y\varepsilon : x, y \in \mathbb{Q}\}$, то $a = b = c = 0$.

4.4. Пусть $r \in \mathbb{C}$, $r^3, a, b, c \in \mathbb{Q}$.

(a) **Лемма о вещественности.** Числа

$$(*) \quad a + br + cr^2, \quad a + b\varepsilon r + c\varepsilon^2 r^2 \quad \text{и} \quad a + b\varepsilon^2 r + c\varepsilon r^2$$

не могут быть тремя попарно различными вещественными числами.

(b) **Лемма о рациональности.** Кубический многочлен с корнями $(*)$ и коэффициентом 1 при x^3 имеет рациональные коэффициенты.

Обозначим для $K = \mathbb{R}, \mathbb{C}$

$$\widehat{K} := \{a + br + cr^2 \mid r \in K, a, b, c, r^3 \in \mathbb{Q}\}.$$

4.5. (a,b,c) Какие из чисел задачи 4.1 лежат в $\widehat{\mathbb{R}}$?

4.6. (a,b,c) Какие из чисел задачи 4.1 лежат в $\widehat{\mathbb{C}}$?

(d) Лежит ли $i\sqrt{3}$ в $\widehat{\mathbb{C}}$?

4.7. Утверждение. (a) Ни один корень квадратного многочлена не лежит в $\widehat{\mathbb{R}}$.

(b) Квадратный многочлен имеет корень из $\widehat{\mathbb{C}}$ тогда и только тогда, когда либо он имеет рациональный корень, либо его дискриминант имеет вид $-3h^2$ для некоторого $h \in \mathbb{Q}$.

(с) Если многочлен степени 3 неприводим над \mathbb{Q} и имеет три вещественных корня, то ни один из них не лежит ни в $\widehat{\mathbb{R}}$, ни в $\widehat{\mathbb{C}}$.

(д) Если многочлен степени выше 3 неприводим над \mathbb{Q} , то ни один из его корней не лежит ни в $\widehat{\mathbb{R}}$, ни в $\widehat{\mathbb{C}}$.

4.8. Лемма о калькуляторе. Пусть $K \in \{\mathbb{R}, \mathbb{C}\}$. Число, которое можно получить на K -калькуляторе так, чтобы извлечение корня происходило только один раз, причем третьей степени, лежит в \widehat{K} .

5 Одно извлечение корня простой степени

5.1. Представимо ли число (а) $\sqrt[3]{3}$; (б) $\cos(2\pi/21)$; (с) $\sqrt[9]{3}$; (д)* $\sqrt[7]{3}$ в виде $a_0 + a_1\sqrt[7]{2} + a_2\sqrt[7]{2^2} + \dots + a_6\sqrt[7]{2^6}$, где $a_0, a_1, a_2, \dots, a_6 \in \mathbb{Q}$?

5.2. Следующие многочлены неприводимы над \mathbb{Q} :

(а) $x^5 - 4$; (б) $x^q - r^q$, где q простое, $r \in \mathbb{C}$, $r^q \in \mathbb{Q}$ и $r^q \neq b^q$ ни для какого $b \in \mathbb{Q}$.

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

$$a = (a_0, a_1, a_2, \dots, a_{q-1}) \quad \text{и} \quad x(r, q, a) := a_0 + a_1 r^k r + a_2 r^2 + \dots + a_{q-1} r^{q-1}.$$

5.3. Пусть q нечетное простое, $a \in \mathbb{Q}^q$, $r \in \mathbb{C}$, $r^q \in \mathbb{Q}$ и $r^q \neq b^q$ ни для какого $b \in \mathbb{Q}$.

(а) Если $x(r, q, a) = 0$, то $a = (0, \dots, 0)$.

(б) **Лемма о сопряжении.** Пусть многочлен неприводим над \mathbb{Q} и имеет корень $x(r, q, a)$. Тогда он имеет также корни $x(r\varepsilon_q^k, q, a)$ для каждого $k = 1, 2, 3, \dots, q-1$.

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

(д) **Лемма о линейной независимости.** Если $b \in \mathbb{Q}^q[\varepsilon_q]$ и $x(r, q, b) = 0$, то $b = (0, \dots, 0)$.

(е) **Лемма о вещественности.** Пусть числа $x(r\varepsilon_q^k, q, a)$, $k = 0, 1, 2, \dots, q-1$, попарно различны. Тогда среди них ровно одно вещественное.

(ф) **Лемма о рациональности.** Многочлен $(x - x(r, q, a))(x - x(r\varepsilon_q, q, a)) \dots (x - x(r\varepsilon_q^{q-1}, q, a))$ имеет рациональные коэффициенты.

Следующее утверждение интересно и нетривиально даже для многочленов третьей степени.

5.4. Утверждение. Если многочлен неприводим над \mathbb{Q} и имеет более одного вещественного корня, то ни один из его корней не представим в виде $x(r, q, a)$ ни для каких $a \in \mathbb{Q}^q$, простого нечетного q и

(а) $r \in \mathbb{R}$, причем $r^q \in \mathbb{Q}$.

(б) $r \in \mathbb{C}$, причем $r^q \in \mathbb{Q}$ и $\sqrt[q]{r^q} \notin \mathbb{Q}$.

5.5. Лемма о калькуляторе. Пусть $K \in \{\mathbb{R}, \mathbb{C}\}$. Число, которое можно получить на K -калькуляторе так, чтобы извлечение корня происходило только один раз, равно $x(r, q, a)$ для некоторых $r \in K$, $q \in \mathbb{Z}$ и $a \in \mathbb{Q}^q$, причем $r^q \in \mathbb{Q}$.

Из утверждения 5.4 и леммы 5.5 о калькуляторе вытекает, что *если многочлен неприводим над \mathbb{Q} и имеет более одного вещественного корня, то ни один из его корней невозможно получить на вещественном калькуляторе так, чтобы извлечение корня происходило только один раз.* Ср. с теоремой 8.3.

6 Два извлечения корня

6.1. Существуют ли рациональных числа a, b, c, d , для которых $\sqrt[3]{2} =$

(а) $\frac{a + \sqrt{b}}{c + \sqrt{b}}$; (б) $a + \sqrt{b} + \sqrt{c}$; (с) $a + \sqrt{b + \sqrt{c}}$; (д) $a + \sqrt{b} + \sqrt{c} + \sqrt{d}$?

6.2. (а) Можно ли число $\cos(2\pi/9)$ получить на вещественном калькуляторе так, чтобы извлечение корня происходило только два раза, причем оба раза простой степени?

(б) Придумайте многочлен пятой степени, ни один из корней которого невозможно получить на комплексном калькуляторе так, чтобы извлечение корня происходило только два раза.

7 Неразрешимость в вещественных радикалах

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

$$F[r] := \{x(r, q, a) \mid a \in F^q\}.$$

7.1. Лемма о калькуляторе. Пусть $K \in \{\mathbb{R}, \mathbb{C}\}$. Число A можно получить на K -калькуляторе тогда и только тогда, когда существуют такие $r_1, \dots, r_{s-1} \in K$ и $n_1, \dots, n_{s-1} \in \mathbb{Z}$, что $n_k \geq 2$,

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \dots \subset Q_{s-1} \subset Q_s \ni A, \quad \text{где } r_k^{n_k} \in Q_k, \quad r_k \notin Q_k \quad \text{и} \quad Q_{k+1} = Q_k[r_k].$$

для любого $k = 1, \dots, s-1$. (Такая последовательность называется башней расширений.)

Поле называется подмножество множества \mathbb{C} , замкнутое относительно операций сложения, умножения, взятия противоположного числа и деления на ненулевое число. (Общее понятие поля нам не нужно; более того, мы будем использовать только поля из башни расширений.)

7.2. Если F поле, то $F[r]$ поле.

7.3. Пусть F поле, q простое, $a \in F^q$, $r \in \mathbb{C}$, $r^q \in F$ и $r^q \neq b^q$ ни для какого $b \in F$.⁸

(а) Многочлен $x^q - r^q$ неприводим над F .

(б) **Лемма о неприводимости.** Многочлен $x^q - r^q$ неприводим над $F[\varepsilon_q]$.

(с) **Лемма о линейной независимости.** Если $b \in F[\varepsilon_q]^q$ и $x(r, q, b) = 0$, то $b = (0, \dots, 0)$.

(д) **Лемма о сопряжении.** Пусть многочлен неприводим над F и имеет корень $x(r, q, a)$. Тогда он имеет также корни $x(r\varepsilon_q^k, q, a)$, $k = 0, 1, 2, \dots, q-1$.

(е) **Лемма о вещественности.** Пусть F поле, $r \in \mathbb{C}$, $r^q \in \mathbb{R}$ и множество из q различных чисел $x(r\varepsilon_q^k, q, a)$, $k = 0, 1, 2, \dots, q-1$, симметрично относительно вещественной оси. Тогда среди этих чисел ровно одно вещественно.

(ф) **Лемма о рациональности.** Многочлен $(x - x(r, q, a))(x - x(r\varepsilon_q, q, a)) \dots (x - x(r\varepsilon_q^{q-1}, q, a))$ имеет коэффициенты из F .

7.4. (а) Докажите теорему о неразрешимости в вещественных радикалах.

(б) Если кубический многочлен имеет три иррациональных вещественных корня, то ни один из них невозможно получить на вещественном калькуляторе.

7.5. Теорема. Если многочлен простой нечетной степени неприводим над \mathbb{Q} и имеет более одного вещественного корня, то ни один из его корней невозможно получить на вещественном калькуляторе.

Комментарий к доказательству. Для многочленов степени выше 3 неприводимость над Q_{s-1} вывести из отсутствия корня в Q_{s-1} уже сложнее, см. лемму о потере неприводимости 7.7.с ниже. Эта лемма перестраивает доказательство (в частности, делает ненужной аналог леммы о рациональности). Итак, исполнение доказательства теоремы 7.5 (и теоремы Кронекера 8.1) отличается от идей, которые к нему привели.

⁸Последнее условие пропущено в [Р, Т, D]. В [Р] утверждение ' $q = p$ ' сверху стр. 581 означает следующее (для $p = 2$): если квадратный трехчлен f неприводим над полем k , содержащим i , и приводим над $k[\sqrt{a}]$ и q простое, то $q = 2$. Это неверно для $f(x) = x^2 + x + 1$ и $q = 3$ и $a = 1$ и $k = \mathbb{Q}[i]$. Ошибка в доказательстве - в предыдущем предложении: (верную) теорему 1 на стр. 572 применить нельзя, т.к. $a = b^q$ возможно.

Для полей $K \subset L$ размерностью $\dim_K L$ поля L над полем K называется наименьшее s , для которого существуют s таких элементов $l_1, \dots, l_s \in L$, что для любого $l \in L$ существуют $k_1, \dots, k_s \in K$, для которых $l = k_1 l_1 + \dots + k_s l_s$.

7.6. (a) Найдите $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt[5]{3}]$.

(b) Если β — корень неприводимого над \mathbb{Q} многочлена p , то $\dim_{\mathbb{Q}} \mathbb{Q}[\beta] = \deg p$.

(c) **Теорема о размерности башни.** Для любых полей $K \subset L \subset M$ выполнено $\dim_K M = \dim_L M \cdot \dim_K L$.

7.7. (a) Если многочлен простой степени q неприводим над полем F , то он неприводим и над $F[\varepsilon_q]$.

(b) Пусть F поле, q простое, $r \in \mathbb{C}$, $r^q \in F$, $r^q \neq b^q$ ни для какого $b \in F$. Если многочлен простой степени p неприводим над F и приводим над $F[r]$, то $q = p$.

(c) **Лемма о потере неприводимости.** Если многочлен простой степени p неприводим над F и приводим над $F[\beta]$ для некоторого корня β неприводимого над F многочлена степени d , то d делится на p .

7.8. (a) Если многочлен простой степени p неприводим над $\mathbb{Q}[\varepsilon_7]$ и приводим над $\mathbb{Q}[\varepsilon_7, \sqrt[7]{2}]$, то $p = 7$ и многочлен имеет корень в $\mathbb{Q}[\varepsilon_7, \sqrt[7]{2}]$.

(b) **Лемма о наличии корня.** Пусть F поле, q простое, $r \in \mathbb{C}$, $r^q, \varepsilon_q \in F$. Если многочлен степени q неприводим над F и приводим над $F[r]$, то многочлен имеет корень в $F[r]$.

8 Доказательства из Книги

Поле называется подмножеством множества \mathbb{C} , замкнутое относительно операций сложения, умножения, взятия противоположного числа и деления на ненулевое число.

Лемма о линейной независимости. Если q простое, поле $F \subset \mathbb{C}$ симметрично относительно $\mathbb{R} \subset \mathbb{C}$, $r \in \mathbb{R} - F$, $r^q \in \mathbb{R} \cap F$ и $A(r) = 0$ для некоторого многочлена A с коэффициентами из F степени меньше q , то $A = 0$.

Доказательство. Оба многочлена A и $t^q - r^q$ с коэффициентами из F имеют корень r . Значит, их НОД имеет корень r и степень k , $0 < k \leq \deg A < q$. Все корни многочлена $t^q - r^q$ есть $r, r\varepsilon_q, r\varepsilon_q^2, \dots, r\varepsilon_q^{q-1}$. Модуль свободного члена НОД'a равен произведению модулей некоторых k из этих корней. Если $q = 2$, то $k = 1$ и $\varepsilon_q = -1$, откуда $r \in F$. Пусть далее $q > 2$. Ввиду симметричности поля F квадрат модуля любого числа из F также лежит в F . Значит, $r^{2k} \in F$. Так как $q > 2$ простое, то $2kx + qy = 1$ для некоторых целых x, y . Тогда $r^{2kx} = r(r^q)^{-y}$, откуда $r \in F$. Противоречие. QED

Доказательство теоремы о неразрешимости в вещественных радикалах. Предположим, напротив, что некоторый корень x_1 уравнения $8x^3 - 6x + 1 = 0$ можно получить на вещественном калькуляторе. Если $F \subset \mathbb{C}$, $r \in \mathbb{C}$ и $r^q \in F$ для некоторого целого положительного q , то обозначим

$$F[r] := \{a_0 + a_1r + a_2r^2 + \dots + a_{q-1}r^{q-1} \mid a_0, \dots, a_{q-1} \in F\}.$$

Так как число x_1 можно получить на вещественном калькуляторе, то существуют такие $r_1, \dots, r_{s-1} \in \mathbb{R}$ и $q_1, \dots, q_{s-1} \in \mathbb{Z}$, что $q_k \geq 2$,

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \dots \subset F_{s-1} \subset F_s \ni x_1, \quad \text{где } r_k^{q_k} \in F_k, \quad r_k \notin F_k \quad \text{и} \quad F_{k+1} = F_k[r_k].$$

для любого $k = 1, \dots, s-1$. Такая последовательность называется *башней расширений*.

Возьмем наименьшее s , для которого существует башня расширений, последнее поле F_s которой содержит некоторый корень уравнения $8x^3 - 6x + 1 = 0$ (возможно, корень, отличный от x_1). Обозначим $F := F_{s-1}$, $q := q_{s-1}$ и $r := r_{s-1}$. Рассматриваемый корень есть $B(r)$ для некоторого многочлена $B \in F[t]$ степени больше 0 и меньше q .

Раскроем скобки в выражении $8B^3(t) - 6B(t) + 1$ и избавимся от степеней t , больших $q-1$, заменяя t^q на $r^q \in F$. Получим многочлен $A \in F[t]$ степени менее q . Так как $A(r) = 0$, то по лемме о линейной независимости $A = 0$. Значит, $8B^3(t) - 6B(t) + 1 = A(t) = 0$ для $t = r\varepsilon_q^k$ и любого $k = 0, 1, \dots, q-1$.

Корни $B(r\varepsilon_q^k)$, $0 \leq k \leq q-1$, уравнения $8x^3 - 6x + 1 = 0$ попарно различны.

(Действительно, $\overline{\varepsilon_q^k} = \varepsilon_q^{-k}$ влечет симметричность поля $F[\varepsilon_q]$ относительно $\mathbb{R} \subset \mathbb{C}$. Если $B(r\varepsilon_q^k) = B(r\varepsilon_q^l)$ для некоторых $0 \leq k < l \leq q-1$, то по лемме о линейной независимости для поля $F[\varepsilon_q]$ ввиду $\deg B > 0$ получим $r \in F[\varepsilon_q]$. Поэтому $r^2, r^3, \dots, r^{q-1} \in F[\varepsilon_q]$. Составим таблицу $a_{kl} \in F$ размера $q \times (q-1)$ из разложений чисел r^k по степеням числа ε_q :

$$r^k = \sum_{l=0}^{q-2} a_{kl} \varepsilon_q^l, \quad 0 \leq k \leq q-1.$$

При помощи нескольких операций прибавления к одной строке другой, умноженной на число из F , можно получить таблицу с нулевой строкой. Значит, имеется ненулевой многочлен степени меньше q с коэффициентами из F и корнем r . Противоречие с леммой о линейной независимости.)

Значит, $q = 2$ или $q = 3$. Если $q = 2$, то по теореме Виета третий корень уравнения $8x^3 - 6x + 1 = 0$ равен $-2B(0) \in F$ — противоречие с минимальностью числа s . Если $q = 3$, то из $\overline{\varepsilon_3} = \varepsilon_3^2$ вытекает $B(r\varepsilon_3) = \overline{B(r\varepsilon_3^2)}$. Это противоречит вещественности и различности последних двух чисел. QED

Теорема Галуа (о неразрешимости в комплексных радикалах) вытекает из следующего результата. (И он, и утверждение 8.3 ниже, интересны и нетривиальны даже для многочленов пятой степени.)

8.1. Теорема Кронекера. Если многочлен простой степени неприводим над \mathbb{Q} , имеет более одного вещественного корня и хотя бы один невещественный, то ни один из его корней невозможно получить на комплексном калькуляторе.

8.2. Лемма о вещественности. Пусть поля F и $F[r]$ симметричны относительно вещественной оси, $a \in F^q$ и множество из q различных чисел $x(r\varepsilon_q^k, q, a)$, $k = 0, 1, 2, \dots, q-1$, симметрично относительно вещественной оси. Тогда среди этих чисел либо все вещественны, либо ровно одно.

8.3. Утверждение. Последовательность извлечений корней назовем *интересной*, если каждый раз

(1) извлекается корень простой степени q , причем из числа, не являющегося q -й степенью никакого числа, полученного на предыдущих шагах.

(2) либо берется вещественное значение извлекаемого корня, либо квадрат модуля извлеченного корня уже получен на предыдущих шагах.

Если многочлен простой степени неприводим над \mathbb{Q} , имеет более одного вещественного корня и хотя бы один невещественный, то ни один из его корней невозможно получить на комплексном калькуляторе, используя интересную последовательность извлечений корней.

8.4. Теорема Гаусса. Корень любой степени $p > 2$ из 1 можно получить на калькуляторе, используя извлечения корней степеней, меньших p .

9 О наименьшем числе радикалов

9.1. (a) Как по многочлену третьей степени узнать, имеет ли он корень вида $a + br + cr^2$, где $a, b, c, r^3 \in \mathbb{Q}$ и $r \in \mathbb{R}$?

(b) То же для $r \in \mathbb{C}$?

Замечание: этот вопрос не покрывается предыдущими результатами для кубических многочленов, не имеющих рациональных корней и имеющих ровно один вещественный корень (например, $x^3 - 2$ или $x^3 + 3x + 2$).

9.2. (3R) Как по многочлену третьей степени узнать, имеет ли он корень, который можно получить на вещественном калькуляторе так, чтобы извлечение корня происходило только один раз?

(3C) Тот же вопрос для комплексного калькулятора.

(4R), (4C) Те же вопросы для многочленов четвертой степени.

(nR), (nC) Те же вопросы для многочленов степени n .

9.3. (1) Как по многочлену четвертой степени узнать, имеет ли он корень, который можно получить на вещественном калькуляторе?

(2) Тот же вопрос, но чтобы извлечение корня происходило только два раза;

(3),(4),... Те же вопросы, но чтобы извлечение корня происходило только 3,4,... раз.

10 Указания и решения

2.1. (a,b,c,e) можно, (d,f,g,h) нельзя.

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

(b) $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2} = 1$.

(d) Пусть можно. 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.

Другие способы — аналогично пунктам (e,h) или утверждению 2.4. Для последнего способа нужна неприводимость многочлена $x^5 - 2$ над \mathbb{Q} . Докажем ее. Все корни многочлена $x^5 - 2$ есть $\sqrt[5]{2}, \sqrt[5]{2}\varepsilon_5, \sqrt[5]{2}\varepsilon_5^2, \sqrt[5]{2}\varepsilon_5^3, \sqrt[5]{2}\varepsilon_5^4$. Пусть он приводим над \mathbb{Q} . Так как у него нет рациональных корней, то сомножители в разложении имеют вторую и третью степень. Модуль свободного члена сомножителя второй степени рационален и равен произведению $\sqrt[5]{4}$ модулей некоторых двух из этих корней. Противоречие.

(e) Пусть можно, т.е. $\sqrt{2} + \sqrt[3]{2} = a + \sqrt{b}$. Число $\sqrt{2} + \sqrt[3]{2}$ является корнем многочлена $((x - \sqrt{2})^3 - 2)((x + \sqrt{2})^3 - 2)$ с рациональными коэффициентами. Тогда по лемме о сопряжении (2.2) этот многочлен имеет корень $a - \sqrt{b}$. По теореме о рациональных корнях у этого многочлена нет рациональных корней. Значит, $b \neq 0$ и корни $a \pm \sqrt{b}$ различны. Но у этого многочлена 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) $\cos(\pi/5) = (\sqrt{5} + 1)/4$.

(h) Аналогично решению пункта (e) получаем, что числа $a + \sqrt{b}$ и $a - \sqrt{b}$ являются различными корнями многочлена $8x^3 - 6x + 1$. Тогда по теореме Виета третий корень равен $-2a \in \mathbb{Q}$. Противоречие.

Другой способ — аналогично утверждению 2.4.

2.2. (Идею этого решения и его обобщений предложил Л. Шабанов.) Подставим в многочлен $x = a + br$ и раскроем скобки, заменяя всюду r^2 на 2. Получим выражение $m + nr$. Подставляя $r = \sqrt{2}$, получаем $m + n\sqrt{2} = 0$. По лемме о линейной независимости (b) $m = n = 0$. Подставляя $r = -\sqrt{2}$, видим, что значение многочлена в точке $a - b\sqrt{2}$ равно $m - n\sqrt{2} = 0$.

2.5. Достаточно доказать, что множество чисел такого вида замкнуто относительно сложения, вычитания, умножения, и деления. Это, естественно, не так.

Поэтому обозначим через \sqrt{c} число, полученное при единственном извлечении корня, где $c \in \mathbb{Q}$. И будем доказывать, что тогда 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 не очевидно только для деления, для чего оно следует из $(a + b\sqrt{c})(a - b\sqrt{c}) = a^2 - b^2c$.

2.4. Аналогично задаче 2.1.e получаем, что числа $a + \sqrt{b}$ и $a - \sqrt{b}$ являются различными корнями данного многочлена. Так как этот многочлен неприводим, то он не имеет рациональных корней. Значит, $b \neq 0$. Поэтому данный многочлен делится на $(x - a)^2 - b$. Противоречие с его неприводимостью над \mathbb{Q} .

3.1. Нельзя.

(a) *Первое решение.* Пусть можно. По леммам о сопряжении и о линейной независимости (3.2.a и 3.3.a) многочлен $x^3 - 3$ имеет два различных вещественных корня. Противоречие.

Второе решение. Пусть можно. По леммам о сопряжении и о линейной независимости (3.2.b и 3.3.b) многочлен $x^3 - 3$ имеет четыре различных корня. Противоречие.

(b) *Первое решение.* Пусть можно. По леммам о сопряжении и о линейной независимости (3.2.a и 3.3.a) многочлен $x^6 - 3$ имеет два различных вещественных корня

$$a + b\sqrt[4]{2} + c\sqrt{2} + d\sqrt[4]{8} = \sqrt[6]{3} \quad \text{и} \quad a - b\sqrt[4]{2} + c\sqrt{2} - d\sqrt[4]{8} = -\sqrt[6]{3}.$$

Тогда $a = c = 0$ и $b + d\sqrt{2} = \sqrt[6]{3}/\sqrt[4]{2}$. Последнее число есть корень многочлена $x^{12} - 9/8$. Значит, $b + d\sqrt{2}$ тоже его корень. Поэтому $b - d\sqrt{2} = -\sqrt[6]{3}/\sqrt[4]{2}$. Отсюда $b = 0$. Противоречие с рациональностью d .

(b) *Второе решение.* Пусть можно. По лемме о сопряжении (3.2.b) многочлен $x^6 - 3$ имеет четыре различных корня x_1, x_2, x_3, x_4 , указанные в 3.2.b. Так как ни один из них не рационален, то $b = c = d = 0$ невозможно. Значит, по лемме о линейной независимости (3.3.b) эти корни различны. Поэтому многочлен $x^6 - 3$ делится на $(x - x_1)(x - x_2)(x -$

$x_3)(x - x_4)$. У многочлена $(x - x_1)(x - x_2)(x - x_3)(x - x_4)$ рациональные коэффициенты (докажите!). Противоречие с неприводимостью многочлена $x^6 - 3$ над \mathbb{Q} .

3.2. (а) Подставим в многочлен $x = a + br$ и раскроем скобки, заменяя всюду r^4 на 2. Получим выражение $k + lr + mr^2 + nr^3$. Подставляя $r = \sqrt[4]{2}$, получаем $k + l\sqrt[4]{2} + m\sqrt{2} + n\sqrt[4]{8} = 0$. По лемме о линейной независимости (3.3.b) $k = l = m = n = 0$. Подставляя $r = -\sqrt[4]{2}$, видим, что значение многочлена в точке $a - b\sqrt[4]{2} + c\sqrt{2} - d\sqrt[4]{8}$ равно $k - l\sqrt[4]{2} + m\sqrt{2} - n\sqrt[4]{8} = 0$.

(б) Аналогично (а), только подставляем $r = i\sqrt[4]{2}$ и $r = -i\sqrt[4]{2}$.

3.3. (а) *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. Так как многочлен $x^4 - 2$ неприводим над \mathbb{Q} , то он не может иметь общий корень с многочленом $a + bx + cx^2 + dx^3$ третьей степени.

(б) Докажите отдельно для вещественной и мнимой части.

3.4. Аналогично задаче 3.1. Отдельно рассматривается более простой случай $r^2 \in \mathbb{Q}$.

3.5. Достаточно доказать, что число, обратное к ненулевому числу такого вида, также имеет такой вид. Это следует из

$$(a + br + cr^2 + dr^3)(a - br + cr^2 - dr^3) = (a + cr^2)^2 - r^2(b + dr^2)^2 \text{ и } (A + Br^2)(A - Br^2) = A^2 - B^2r^4.$$

4.1. Нельзя.

(а) *Первое решение.* Пусть можно. 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. 4.3.a). Поэтому $b^3 = -2abc = 2c^3$. Тогда либо $b = c = 0$, либо $\sqrt[3]{2} = b/c$. Оба случая невозможны.

Второе решение. Пусть можно. По лемме о сопряжении (4.2) многочлен $x^2 - 3$ имеет три корня, заданные формулами (*) с $a, b, c \in \mathbb{Q}$ и $r = \sqrt[3]{2}$. Так как ни один из них не рационален, то $b = c = 0$ невозможно. Значит, по лемме о линейной независимости (4.3.a) эти корни различны. Противоречие.

(б) Пусть можно. Число $\cos(\pi/9)$ является корнем уравнения $4x^3 - 3x = \frac{1}{2}$. Два других его вещественных корня есть $\cos(7\pi/9)$ и $\cos(5\pi/9)$. По лемме о сопряжении (4.2) многочлен $8x^3 - 6x - 1$ имеет три корня x_1, x_2, x_3 , заданные формулами (*) с $a, b, c \in \mathbb{Q}$ и $r = \sqrt[3]{2}$. Так как ни один из них не рационален, то $b = c = 0$ невозможно. Значит, по лемме о линейной независимости (4.3.a) эти корни различны. Противоречие с леммой о вещественности (4.4.a) для $r = \sqrt[3]{2}$.

(с) Пусть можно. По лемме о сопряжении (4.2) многочлен $x^5 - 3$ имеет три корня x_1, x_2, x_3 , заданные формулами (*), где $a, b, c \in \mathbb{Q}$ и $r = \sqrt[3]{2}$. Так как ни один из корней не рационален, то $b = c = 0$ невозможно. Значит, по слабой лемме о линейной независимости (4.3.a) эти корни различны. Поэтому многочлен $x^5 - 3$ делится на $(x - x_1)(x - x_2)(x - x_3)$. По задаче 4.4 многочлен $(x - x_1)(x - x_2)(x - x_3)$ имеет рациональные коэффициенты. Противоречие с неприводимостью над \mathbb{Q} многочлена $x^5 - 3$.

4.2. Аналогично 2.2 и 3.2. Используйте 4.3.a. Подставьте $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ в многочлен и соберите коэффициенты при 1, при $\sqrt[3]{2}$ и при $\sqrt[3]{4}$. Потом подставьте сопряженное число в многочлен.

4.3. (а) Так как многочлен $x^3 - r^3$ не имеет рациональных корней, то он неприводим над \mathbb{Q} .

(б) Докажите отдельно для вещественной и мнимой части.

4.4. (а) Если заменить r на $r\varepsilon$, то множество трех чисел (*) не изменится, они лишь перенумеруются. Значит, ввиду $r^3 \in \mathbb{R}$ можно считать, что $r \in \mathbb{R}$. Тогда $a + br + cr^2 \in \mathbb{R}$. Заметим, что $\overline{\varepsilon^k} = \varepsilon^{-k}$. Поэтому числа $a + br\varepsilon + cr^2\varepsilon^2$ и $a + br\varepsilon^2 + cr^2\varepsilon$ симметричны относительно вещественной оси (т.е. комплексно сопряжены). Значит, они не могут быть вещественными и различными.

(б) При замене r на $r\varepsilon$ наш многочлен переходит в себя. Наш многочлен является суммой одночленов $\lambda_{klmnpq}a^k b^l c^m r^n \varepsilon^p x^q$. Имеем $\lambda_{klmnp,q} = \lambda_{klmn,n+p,q} = \lambda_{klmn,2n+p,q}$. Так как $\varepsilon^p + \varepsilon^{n+p} + \varepsilon^{2n+p}$ равно 0 или 3, то оно рационально. Значит, все коэффициенты рациональны.

4.5. Не лежит ни одно. Доказательство аналогично задаче 4.1. Приведем детали для первого решения пункта (а).

(а) Пусть можно, т.е. $\sqrt{3} = a + br + cr^2$ для некоторых $r \in \mathbb{R}$, $r \notin \mathbb{Q}$, $a, b, c, r^3 \in \mathbb{Q}$. Тогда

$$2 = (a^2 + 2bcr^3) + (2ab + c^2r^3)r + (2ac + b^2)r^2.$$

Так как многочлен $x^3 - r^3$ не имеет рациональных корней, то он неприводим над \mathbb{Q} . Значит, $2ab + c^2r^3 = 2ac + b^2 = 0$ (ср. 4.3.а). Поэтому $b^3 = -2abc = c^3r^3$. Тогда либо $b = c = 0$, либо $r = b/c$. Оба случая невозможны.

4.6. Лежит только $i\sqrt{3}$. Оно получается после извлечения корня кубического из 1.

(а,б,с) Если корень извлекался комплексный и из куба рационального числа, то $\sqrt{3}, \sqrt[5]{3}, \cos(\pi/9) \in \mathbb{Q}[\varepsilon] \cap \mathbb{R} = \mathbb{Q}$, что неверно. Если же корень извлекался комплексный и не из куба рационального числа, то аналогично вещественному случаю.

4.7. Пункты (а), (б), (с), (d) аналогичны задачам 4.5.а, 4.6.d, 4.5.б и 4.6.б, 4.5.с и 4.6.с, соответственно.

4.8. 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 . Так как многочлены $x^3 - r^3$ и $a + br + cr^2$ взаимно просты, то существуют многочлены g и h , для которых $h(x)(a + bx + cx^2) + g(x)(x^3 - r^3) = 1$. Тогда h — искомым.

5.1. (а,б,с) Нельзя. (d) Не знаю.

Указание. Используйте сформулированные ниже леммы. Аналогично второму решению задач 4.1 и 4.5.а.

Решение (а). Пусть можно. Тогда по лемме о сопряжении (5.3.б) многочлен $x^2 - 3$ имеет корни $x(r\varepsilon_7^k, 7, a)$ для $k = 0, 1, 2, \dots, 6$. По лемме о линейной независимости (5.3.д) они попарно различны. Противоречие.

Решение (б). Пусть можно. Обозначим через p многочлен, для которого $\cos 7x = p(\cos x)$. Тогда по леммам о сопряжении и о линейной независимости (5.3.б,д) многочлен $2p(x) + 1$ имеет попарно различные корни $x(r\varepsilon_7^k, 7, a)$ для $k = 0, 1, 2, \dots, 6$. Но все корни этого многочлена вещественны. Противоречие с леммой о вещественности (5.3.е).

Решение (с). Пусть можно. Тогда по леммам о сопряжении и о линейной независимости (5.3.б,д) многочлен $x^9 - 3$ имеет попарно различные корни $x(r\varepsilon_7^k, 7, a)$ для $k = 0, 1, 2, \dots, 6$. По лемме о рациональности (5.3.ф) получаем противоречие.

Решение (d) мне неизвестно.

5.2. (б) Все корни многочлена $x^q - r^q$ есть $r, r\varepsilon_q, r\varepsilon_q^2, \dots, r\varepsilon_q^{q-1}$. Пусть он приводим над \mathbb{Q} . Модуль свободного члена одного из 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 $kx + qy = 1$ для некоторых целых x, y . Тогда $r^{kx} = r(r^q)^{-y}$, откуда $r \in \mathbb{Q}$. Противоречие.

5.3. (а) Вытекает из 5.2.с.

(б) Аналогично задачам 4.2 и 3.2.

(с) Пусть приводим. Аналогично доказательству неприводимости над \mathbb{Q} получим $r \in \mathbb{Q}[\varepsilon_q]$.⁹ Поэтому $r^2, r^3, \dots, r^{q-1} \in \mathbb{Q}[\varepsilon_q]$. Составим таблицу a_{kl} из рациональных чисел размера $q \times (q-1)$ из разложений чисел r^k по степеням числа ε_q :

$$r^k = \sum_{l=0}^{q-2} a_{kl} \varepsilon_q^l, \quad 0 \leq k \leq q-1.$$

При помощи прибавления к одной строке другой, умноженной на рациональное число, можно получить таблицу с нулевой строкой. Значит, имеется многочлен степени меньше q с корнем r . Противоречие с неприводимостью многочлена $x^q - r^q$ над \mathbb{Q} .

(d) Вытекает из (с).

(е) Аналогично задаче 4.4.a. Обозначим $x_k := x(r\varepsilon_q^k, q, a)$. Если заменить r на $r\varepsilon_q$, то множество чисел x_0, x_1, \dots, x_{q-1} не изменится, они лишь перенумеруются. Поэтому можно считать, что $r \in \mathbb{R}$. Тогда $x_0 \in \mathbb{R}$. Заметим, что $\overline{\varepsilon_q^k} = \varepsilon_q^{-k}$. Поэтому для $k > 0$ числа x_k и x_{q-k} симметричны относительно вещественной оси (т.е. комплексно сопряжены). Так как q нечетно и числа x_1, \dots, x_{q-1} попарно различны, то ни одно из них не может быть вещественным.

(f) Аналогично 4.4.b, используя то, что при замене r на $r\varepsilon_q$ наш многочлен переходит в себя.

5.4. Указание к (a). Предположим противное. Аналогично 5.1.abc (и утверждению 4.7.cd) получаем противоречие, используя леммы о сопряженности, о линейной независимости, о вещественности и о рациональности (5.3.bdef).

Решение (a). Предположим противное. Обозначим через q степень извлекаемого корня. Тогда по леммам о сопряжении и о линейной независимости (5.3.b,d) данный многочлен f имеет попарно различные корни $x(r\varepsilon_q^k, q, a)$ для $k = 0, 1, 2, \dots, q-1$. При $q > \deg f$ получаем противоречие. При $q = \deg f$ получаем противоречие по лемме о вещественности (5.3.e). При $q < \deg f$ получаем противоречие по лемме о рациональности (5.3.f).

(b) Аналогично (a).

5.5. Аналогично задачам 4.8 и 3.5.

6.1. Нет.

(a) Домножьте на сопряженное.

(b) 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 $\alpha + \beta\sqrt{b}$ где $\alpha, \beta \in \mathbb{Q}$. Идея доказательства в том, что числа такого вида $\alpha + \beta\sqrt{b}$ (с фиксированным b) ‘ничуть не хуже’ рациональных чисел. Т.е. сумма, разность, произведение и частное чисел такого вида — тоже число такого вида. (Или, говоря научно, такие числа образуют *числовое поле*.) Поэтому можно доказывать аналогично задаче 2.1.d. Ср. с задачей 3.3.a.

6.2. (a) Нельзя.

(b) Годится многочлен f , неприводимый и имеющий более одного вещественного корня. Для последнего достаточно $f(0) > 0$ и $f(1) < 0$. Например, можно взять $x^5 - 4x - 2$.

7.7. (a) Обозначим через $\beta \in \mathbb{C}$ произвольный корень многочлена. По теореме о размерности башни

$$\dim_{F[\varepsilon_q]} F[\beta, \varepsilon_q] \cdot \dim_F F[\varepsilon_q] = \dim_{F[\beta]} F[\beta, \varepsilon_q] \cdot \dim_F F[\beta].$$

Так как многочлен имеет степень q и неприводим над F , то $\dim_F F[\beta] = q$. Имеем $\dim_F F[\varepsilon_q] < q$. Из этого и простоты числа q вытекает, что $\dim_{F[\varepsilon_q]} F[\beta, \varepsilon_q]$ делится на q . Значит, последняя размерность равна q . Поэтому многочлен неприводим над $F[\varepsilon_q]$.

⁹ Другая запись окончания этого решения с использованием понятия размерности: тогда $\dim_{\mathbb{Q}} \mathbb{Q}[r] \leq \dim_{\mathbb{Q}} \mathbb{Q}[\varepsilon_q] \leq q-1$ — противоречие.

(b) Обозначим через $\beta \in \mathbb{C}$ произвольный корень многочлена. По теореме о размерности башни

$$(*) \quad \dim_{F[r]} F[\beta, r] \cdot \dim_F F[r] = \dim_{F[\beta]} F[\beta, r] \cdot \dim_F F[\beta].$$

Так как многочлен неприводим над F , то $\dim_F F[\beta] = p$. Так как многочлен приводим над $F[r]$, то $\dim_{F[r]} F[\beta, r] < p$. Поэтому $\dim_F F[r]$ делится на p . По лемме о неприводимости $\dim_F F[r] = q$ простое. Значит, $q = p$.

(c) Аналогично (b) и (a).

Пункты (a) и (b) являются частным случаем пункта (c) для $\beta = \varepsilon_q$ и $\beta = r$.

7.8. (b) Обозначим через $\beta \in \mathbb{C}$ произвольный корень многочлена. По теореме о размерности башни выполнено равенство (*). Аналогично 7.7.b $\dim_F F[r] = \dim_F F[\beta] = q$. Так как многочлен приводим над $F[r]$, то $\dim_{F[r]} F[\beta, r] < q$. Поэтому $\dim_{F[\beta]} F[\beta, r] < q$. Значит, многочлен $x^q - r^q$ приводим над $F[\beta]$. Тогда по лемме о неприводимости $r^q = b^q$ для некоторого $b \in F[\beta]$. Так как $\varepsilon_q \in F$, то $r \in F[\beta]$. Значит, $\dim_{F[r]} F[\beta, r] = \dim_{F[\beta]} F[\beta, r] = 1$. Поэтому $\beta \in F[r]$.

7.3. Аналогично 5.2.b и 5.3 с заменой \mathbb{Q} на F и рациональности на принадлежность полю F . Заметим, что при этом даже для леммы о сопряжении нужна линейная независимость с коэффициентами из $F[\varepsilon_q]$.

7.4. (a) Предположим, напротив, что некоторый корень уравнения $8x^3 - 6x + 1 = 0$ можно получить на вещественном калькуляторе. Возьмем наименьшее s из леммы о калькуляторе (7.1), для которого некоторый (возможно, другой) корень этого уравнения лежит в Q_s . Так как многочлен $8x^3 - 6x + 1$ третьей степени, то он неприводим над Q_{s-1} . Далее доказываем аналогично доказательству утверждения 5.4.a, с заменой \mathbb{Q} на Q_{s-1} .

(b) Аналогично (a).

7.5. Пусть возможно. Рассмотрим башню расширений из леммы о калькуляторе для $K = \mathbb{R}$. Возьмем такое s , что данный многочлен g неприводим над Q_{s-1} и приводим над Q_s . Обозначим $r := r_{s-1}$, $q := n_{s-1}$ и $F := Q_{s-1}[\varepsilon_q]$. Можно считать, что q простое. Тогда по леммам о неприводимости и о потере неприводимости для $\beta = r$ (7.3.a, 7.7.c) $\deg g = q$. По лемме о потере неприводимости для $\beta = \varepsilon_q$ (7.7.c) g неприводим над F . Так как g приводим над $F[r]$, по лемме о наличии корня (7.8.b) g имеет корень в $F[r]$. Этот корень равен $x(r, q, a)$ для некоторого $a \in F^q$. По лемме о сопряжении (7.3.d) g имеет q корней $x(r\varepsilon_q^k, q, a)$, $k \in \{0, 1, 2, \dots, q-1\}$. По лемме о линейной независимости (7.3.c) эти корни различны. По лемме о вещественности (7.3.e) среди этих корней ровно один вещественный. Противоречие. QED

8.1. Ввиду утверждения 8.3 достаточно показать, что если число можно получить на калькуляторе, то его можно получить на калькуляторе, используя интересную последовательность извлечений корней. То, что можно брать только корни простых степеней, очевидно (при соответствующем преобразовании последовательности извлечений корней могут появиться новые нарушения второй части свойства (1)). Добиться свойства (2) также просто: перед взятием незначительного значения корня $\sqrt[q]{a}$ берем вещественное значение корня $\sqrt[q]{|a^2|}$, если оно еще не получено на предыдущих шагах (при этом общее количество извлечений корней может увеличиться). То, что можно добиться второй части свойства (1) ($r^q \neq b^q$),¹⁰ вытекает из теоремы Гаусса 8.4. QED

8.2. Обозначим $x_k := x_k(r\varepsilon_q^k, q, a)$.

Пусть сначала $r^q \in \mathbb{R}$. Имеем $r = |r|\varepsilon_q^s$ для некоторого s . Если заменить r на $|r|$, то множество чисел x_0, x_1, \dots, x_q не изменится, они лишь перенумеруются. Поэтому можно считать, что $r \in \mathbb{R}$. Тогда $x_0 \in \mathbb{R}$. Заметим, что $\overline{\varepsilon_q^k} = \varepsilon_q^{-k}$. Поэтому для $k > 0$ числа x_k и x_{q-k} симметричны относительно вещественной оси (т.е. комплексно сопряжены). Так

¹⁰Это неочевидно: число $\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} \in \sqrt[3]{1}$, конечно, можно получить, взяв $\sqrt{3}$, но как обобщить этот пример?

как q нечетно и числа x_1, \dots, x_{q-1} попарно различны, то ни одно из них не может быть вещественным.

Пусть теперь $r^q \notin \mathbb{R}$. Тогда $\bar{r}^s = \frac{|r|^{2s}}{r^q} r^{q-s}$. Поэтому для любого $k \in \{0, 1, \dots, q-1\}$ условие $x_k = \bar{x}_k$ равносильно тому, что

$$a_0 = \bar{a}_0, \quad a_1 = \bar{a}_{q-1} \frac{|r|^{2q-2}}{r^q}, \quad a_2 = \bar{a}_{q-2} \frac{|r|^{2q-4}}{r^q}, \dots$$

Эти равенства не зависят от k . Так как среди чисел x_0, \dots, x_{q-1} есть одно вещественное, то все они вещественны. QED

8.3. Пусть возможно. Будем считать, что калькулятор при нажатии кнопки $\sqrt[n]{}$ выдает одно значение корня, выбираемое нами. (Действительно, тогда все значения корня можно получить за n шагов.)

Рассмотрим башню расширений из леммы о калькуляторе для $K = \mathbb{C}$. Возьмем такое s , что данный многочлен g неприводим над Q_{s-1} и приводим над Q_s . Обозначим $r := r_{s-1}$, $q := n_{s-1}$ и $F := Q_{s-1}[\varepsilon_q]$. Ввиду условия (1) по леммам о неприводимости и о потере неприводимости для $\beta = r$ (7.3.a, 7.7.c) $\deg g = q$. По лемме о потере неприводимости для $\beta = \varepsilon_q$ (7.7.c) g неприводим над F . Так как g приводим над $F[r]$, по лемме о наличии корня (7.8.b) g имеет корень в $F[r]$. Этот корень равен $x(r, q, a)$ для некоторого $a \in F^q$. По лемме о сопряжении (7.3.d) g имеет q корней $x(r\varepsilon_q^k, q, a)$, $k \in \{0, 1, 2, \dots, q-1\}$. По лемме о линейной независимости (7.3.c) эти корни различны.

При условии симметричности поля Q_k (относительно вещественной оси), симметричность поля $Q_k[r]$ равносильна тому, что либо $r \in \mathbb{R}$, либо $r\bar{r} = |r|^2 \in Q_k$. Поэтому по индукции с использованием свойства (2) получаем, что все Q_k симметричны. По лемме о вещественности (8.2) получаем противоречие. QED

8.4. (Borrowed from [E1, §24]; we simplify the proof by avoiding use of Lemma 2.) Докажем утверждение при помощи индукции по p для любых, не обязательно простых, p . Если p составное, то $p = ab$ для некоторых a и b . Поэтому $\sqrt[p]{1} = \sqrt[a]{\sqrt[b]{1}}$. Пусть теперь p простое. Пусть g — первообразный корень по модулю p . Обозначим $\alpha := \varepsilon_p$, $\varepsilon := \varepsilon_{p-1}$ и,

$$\text{для } r = 0, 1, 2, \dots, p-2, \quad T_r(x) := x + \varepsilon^r x^g + \varepsilon^{2r} x^{g^2} + \dots + \varepsilon^{(p-2)r} x^{g^{p-2}} \in \mathbb{Z}[\varepsilon][x].$$

Тогда $\alpha = \frac{(T_0 + T_1 + \dots + T_{p-2})(\alpha)}{p-1}$. Имеем $T_0(\alpha) = -1$. Поэтому достаточно доказать, что число $T_r(\alpha)$ выражается через радикалы степени меньше p для каждого $r = 1, 2, \dots, p-2$.

Так как

$$T_r(x^g) \equiv \varepsilon^{-r} T_r(x) \pmod{(x^p - 1)}, \quad \text{то} \quad T_r^{p-1}(x^g) \equiv T_r^{p-1}(x) \pmod{(x^p - 1)}.$$

Возьмем многочлен $a_0 + a_1 x + a_2 x^2 + \dots + a_{p-1} x^{p-1}$ с коэффициентами в $\mathbb{Z}[\varepsilon]$, сравнимый с $T_r^{p-1}(x)$ по модулю $x^p - 1$. Тогда $a_k = a_{kg} \pmod{p}$ для любого $k = 1, 2, \dots, p-1$. Значит, $a_1 = a_2 = \dots = a_{p-1}$. Поэтому $T_r^{p-1}(\alpha) = a_0 - a_1 \in \mathbb{Z}[\varepsilon]$. Значит, число $T_r(\alpha)$ выражается через радикалы степени меньше p . QED

9.1. Ответ: многочлен $x^3 + px + q$ имеет корень указанного вида тогда и только тогда, когда либо многочлен имеет рациональный корень, либо

$$(a) (p/3)^3 + (q/2)^2 \quad (b) |(p/3)^3 + (q/2)^2|$$

есть квадрат рационального числа.

Литература.

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

[Ch] Г.Р. Челноков, Основы теории Галуа в интересных задачах, <http://www.mcsme.ru/circles/oim/materials/grishalouis.pdf>. (засмотрено 11.11.2010)

- [CR] R. Courant and H. Robbins, What is Mathematics, Oxford Univ. Press.
- [D] Dorrier,
- [E1] H.M. Edwards, Galois Theory, Springer Verlag, 1984.
- [E2] H.M. Edwards, The construction of solvable polynomials, Bull. Amer. Math. Soc. 46 (2009), 397-411. Errata: Bull. Amer. Math. Soc. 46 (2009), 703-704.
<http://www.ams.org/journals/bull/2009-46-03/S0273-0979-09-01253-1/>
- [FT] D. Fuchs, S. Tabachnikov, Mathematical Omnibus. AMS, 2007.
<http://www.math.psu.edu/tabachni/Books/taoba.pdf>
- [KS] П. Козлов и А. Скопенков, В поисках утраченной алгебры: в направлении Гаусса (подборка задач), Мат. Просвещение, 12 (2008), 127–144, <http://arxiv.org/abs/0804.4357>
- [L] L. Lerner, Galois Theory without abstract algebra, <http://arxiv.org/abs/1108.4593>.
- [P] В.В. Прасолов, Задачи по алгебре, арифметике и анализу (М.: МЦНМО, 2007)
<ftp://ftp.mccme.ru/users/prasolov/algebra/algebra2.pdf>
- [S] A. Skopenkov, A simple proof of the Abel-Ruffini theorem, Mat. Prosveschenie, 15 (2011) 113-126, <http://arxiv.org/abs/1102.2100>.
- [S1] А. Скопенков, Философски-методическое отступление, в кн. Сборник материалов московских выездных математических школ. Под редакцией А. Заславского, Д. Пермякова, А. Скопенкова, М. Скопенкова и А. Шаповалова, Москва, МЦНМО, 2009.
<http://www.mccme.ru/circles/oim/mvz.pdf> (засмотрено 20.08.2010).
- [S2] A. Skopenkov, Yet another proof from the book: the Gauss theorem on regular polygons, <http://arxiv.org/abs/0908.2029>.
- [T] В.М. Тихомиров, Абель и его великая теорема, Квант, 2003, N1.
<http://kvant.mccme.ru/pdf/2003/01/kv0103abel.pdf>
- [V] Вагутен Н., Сопряженные числа. Квант, 1980, N2,
http://kvant.mccme.ru/1980/02/sopryazhennye_chisla.htm
- [W] Б.Л. ван дер Варден, Алгебра, М: Наука, 1976.
- [ZPSSS] Математика в задачах. Сборник материалов московских выездных математических школ. Под редакцией А. Заславского, Д. Пермякова, А. Скопенкова, М. Скопенкова и А. Шаповалова. Москва, МЦНМО, 2009. <http://www.mccme.ru/circles/oim/mvz.pdf>