Еще несколько доказательств из Книги: разрешимость и неразрешимость уравнений в радикалах *

А. Скопенков §

Аннотация

Основное содержание этой брошюры — простые элементарные доказательства знаменитых теорем Гаусса, Абеля, Галуа и Кронекера о построимости правильных многоугольников и неразрешимости уравнений в радикалах. На примере этих доказательств иллюстрируются некоторые основные идеи алгебры. Определения построимости и разрешимости в радикалах приводится; для понимания доказательств достаточно знакомства с многочленами и умения извлекать корни из комплексных чисел. Брошюра адресована всем любителям изложения глубоких идей на примерах красивых результатов и доказательств: старшекласникам, студентам, учителям, и профессиональным математикам.

Содержание

*Обновляемая версия: http://arxiv.org/abs/0804.4357. Брошюра основана на занятиях, проведенных в ЛШ «Современная математика», Кировской ЛМШ, Московской ВШ, а также на кружках «Математический семинар» и «Олимпиады и математика». Благодарю А.Я. Белова-Канеля, И.И. Богданова, Э.Б. Винберга, В.В. Волкова, М.Н. Вялого, А.С. Голованова, П.А. Дергача, Д. Зунга, А.А. Казначеева, В.А. Клепцына, Г.А. Мерзона, А.А. Пахарева, В.В. Прасолова, А.Д. Руховича, Л.М. Самойлова, М.Б. Скопенкова, Г.Р. Челнокова, Л.А. Шабанова и В.В. Шувалова за полезные замечания и предложения.

§Поддержан грантом фонда Саймонса. Московский Физико-Технический Институт, Независимый Московский Университет; www.mccme.ru/~skopenko

О чем эта брошюра

Основное содержание этой брошюры — простые элементарные доказательства

• теоремы Гаусса о построимости правильных многоугольников (и даже более сильного результата — теоремы Гаусса о понижении, см. §3.3);

• существования уравнения 3-й степени, неразрешимого в *вещественных* радикалах (и даже более сильного результата — сильной вещественной теоремы о неразрешимости, см. §5.5);

• теоремы Галуа о существовании уравнения 5-й степени, неразрешимого в *комплексных* радикалах (и даже более сильного результата — теоремы Кронекера, см. §5.4).

Определения построимости и разрешимости в радикалах, а также формулировки указанных теорем, приведены в §§1.1,1.2. Я не привожу историю этих знаменитых теорем, отсылая заинтересованного читателя к текстам [Gi, Gi1, Ma].

Приводимые доказательства интересны тем, что для их понимания достаточно уметь делить многочлены с остатком, извлекать корни из комплексных чисел и решать системы линейных уравнений. При этом на таких прямых доказательствах ясно видны базовые идеи важной *теории Галуа* (см. подробнее §6.2).

Приводимые доказательства не претендуют на новизну (хотя в этом тексте имеется много педагогических находок, см. подробнее §6.1). Однако, к сожалению, они малоизвестны. Как следствие, малоизвестно, что не только решать квадратные и кубические уравнения, но и доказывать указанные теоремы экономнее не строя и затем применяя теорию Галуа (как, например, в [Kh2, Ki]), а напрямую — но при этом, конечно, открывая и используя базовые идеи этой теории.

Брошюра адресована тем, кому интересен хотя бы один из этих результатов. Старшеклассники найдут в заметке задачи для иследования, не претендующие на научную новизну, см. подробнее §1.3. Разбор доказательств (или их начала) полезен для закрепления тем «многочлены», «комплексные числа», «иррациональность» и «основы линейной алгебры» на кружке или в матклассе. Она может быть занимательным чтением для профессиональных математиков (им достаточно прочитать §5).

Где найти доказательства сформулированных там утверждений и теорем, и вообще как устроена брошюра, написано в §1.4.

1 Введение

1.1 Разрешимость в квадратных радикалах: формулировки

Известно, что

$$(*)\quad \cos\frac{2\pi}{3}=-\frac{1}{2},\quad \cos\frac{2\pi}{4}=0,\quad \cos\frac{2\pi}{5}=\frac{\sqrt{5}-1}{4},\quad \cos\frac{2\pi}{6}=\frac{1}{2},\quad \cos\frac{2\pi}{8}=\frac{1}{\sqrt{2}}.$$

Как обобщить эти формулы (используя только четыре арифметические действия и извлечения корней)? Для формализации этого вопроса введем следующие определения.

Рассмотрим калькулятор с кнопками

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

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.

Вещественное число называется *вещественно построимым*, если его можно получить на вещественном калькуляторе так, чтобы при этом извлекались корни только второй степени (т.е. получить из 1 при помощи сложений, вычитаний, умножений, делений и извлечений квадратного корня из положительных чисел).

Например, вещественно построимы числа

$$\sqrt[4]{2}=\sqrt{\sqrt{2}},\quad \sqrt{2\sqrt{3}},\quad \sqrt{2}+\sqrt{3},\quad \sqrt{1+\sqrt{2}},\quad 1+\sqrt{3-2\sqrt{2}},\quad \frac{1}{1+\sqrt{2}},$$

числа из формулы (*) и даже число $\cos\dfrac{\pi}{60}=\cos 3^\circ$. Про последнее число это не совсем очевидно (но мы это увидим в §3.1).

Вопрос об обобщении формул (*) формализуется так: для каких n число $\cos(2\pi/n)$ вещественно построимо? Ответ дается следующей теоремой.

Теорема Гаусса. *Число* $\cos(2\pi/n)$ *вещественно построимо тогда и только тогда, когда* $n=2^\alpha p_1\dots p_l$, *где* $p_1,\dots,p_l$ *— различные простые числа вида* $2^{2^s}+1$.

Вещественная построимость числа равносильна его *построимости циркулем и линейкой*. Поэтому теорема Гаусса равносильна критерию построимости циркулем и линейкой правильных многоугольников. Мы обсудим эту равносильность в §2.1; впрочем, она не будет использоваться в остальном тексте.

Вещественная непостроимость числа $\cos(2\pi/9)$ влечет следующий результат.

Следствие. *Трисекция угла невозможна на вещественном калькуляторе, если можно извлекать корни только второй степени. Или, формально, число* $\cos(\alpha/3)$ *невозможно получить на нем, имея число* $\cos\alpha$ *(например, для* $\alpha=2\pi/3$*).*

Замечания. (a) Строго говоря, теорема Гаусса не дает настоящего решения проблемы построимости, поскольку неизвестно, какие числа вида $2^{2^s}+1$ являются простыми. Однако теорема Гаусса дает, например, быстрый алгоритм выяснения построимости числа $\cos(2\pi/n)$.

(b) Для практики приближенные методы вычисления тригонометрических функций и решения уравнений более полезны, чем радикальные формулы. Кроме того, уравнения степени выше 4 разрешимы при помощи трансцедентных функций (см. метод Виета в §2.2 и [PS]; о развитии этих идей см., например, [S1]). Однако проблема разрешимости в радикалах интересна как пробная задача современных теорий символьных вычислений и сложности вычислений.

1.2 Неразрешимость в радикалах: формулировки

Следующее утверждение дает достаточное условие разрешимости уравнений третьей степени «в вещественных радикалах».

Утверждение о разрешимости в вещественных радикалах. *Если многочлен третьей степени с рациональными коэффициентами имеет ровно один вещественный корень, то этот корень можно получить на вещественном калькуляторе.* [1] *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, x^3-3x+1), ни один из корней которого невозможно получить на вещественном калькуляторе.*

Следствие. *Трисекция угла невозможна на вещественном калькуляторе. Или, формально, число* $\cos(\alpha/3)$ *невозможно получить на нем, имея число* $\cos\alpha$ *(например, для* $\alpha=2\pi/3$*).*

Доказательство. По формуле косинуса тройного угла каждое из чисел $\cos(2\pi/9)$, $\cos(8\pi/9)$, $\cos(14\pi/9)$ удовлетворяет уравнению $8y^3-6y+1=0$. Замена $x=2y$ превращает его в уравнение $x^3-3x+1=0$. Значит, то теореме ни одно из них невозможно получить на вещественном калькуляторе. QED

Перейдем теперь к формулам, которые могут содержать комплексные числа.

Комплексный калькулятор имеет те же кнопки, что и вещественный, но оперирует с комплексными числами и при нажатии кнопки $\sqrt[n]{}$ выдает все значения корня. На комплексном калькуляторе можно получить число, если на нем можно получить *множество* чисел, содержащих заданное число.

Оказывается, что уравнение третьей степени (например, x^3-3x+1), не разрешимое на вещественном калькуляторе, разрешимо на комплексном.

Утверждение о разрешимости в комплексных радикалах. *Все корни любого многочлена третьей или четвертой степени с рациональными коэффициентами можно получить на комплексном калькуляторе.* [2] *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.*

Однако аналог этого утверждения для более высоких степеней неверен.

Теорема Галуа. *Существует многочлен 5-й степени с рациональными коэффициентами (например, x^5-4x+2), ни один из корней которого невозможно получить на комплексном калькуляторе.* [3]

Из приведенных теорем о неразрешимости тривиально следует, что *для любого $n\geq 3$ ($n\geq 5$) существует многочлен n-й степени, один из корней которого невозможно получить на вещественном (комплексном) калькуляторе.* Более сложно доказывается аналог этого утверждения с заменой слов «один из корней» на «ни один из корней». При этом корни *некоторых* уравнений высоких степеней вполне может быть возможно получить на калькуляторе, см. например, §3.3.

[1] Стандартная терминология: уравнение *разрешимо в вещественных радикалах.*

[2] Стандартная терминология: уравнение *разрешимо в радикалах.*

[3] Немного 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.

1.3 Чем интересны приводимые доказательства

Приводимые доказательства намного проще и короче тех, которые излагаются в стандартных учебниках по алгебре. (Здесь я имею в виду доказательства «с нуля», а не вывод нужной теоремы из построенной перед этим теории, в которой фактически заключается все доказательство.) Сравнение с доказательствами из менее стандартной более популярной литературы приведено в §6.1.

Простота достигнута благодаря тому, что в отличие от большинства учебников , приводимые доказательства не используют термина «группа Галуа» (даже термина «группа»). Несмотря на отсутствие этих *терминов*, *идеи* приводимых доказательств являются *отправными* для теории Галуа и *конструктивной теории Галуа* [E2]. Более подробно это обсуждается в философско-методическом отступлении (§6.2). Похожее по духу изложение других результатов приводится в [Ch1, Le].

Основные идеи демонстрируются по одной и на «олимпиадных» примерах, т.е. на простейших частных случаях, свободных от технических деталей, и со сведением к необходимому минимуму алгебраического языка.

Доказательство разрешимости основано на методе *резольвент Лагранжа*. Доказательства неразрешимости основаны на идее *сопряжения*, замечательно изложенной в [Va] (или, более учено, на идее *автоморфизма поля*).

Неразрешимость доказывается сначала при условии, что *корень извлекался только один раз* (в задачах в §§4.1,4.5,4.6). Благодаря этому основные идеи преподносятся на примере рациональных чисел (а не произвольных полей и даже не полей из башни расширений). Эти основные идеи (сопряжения, поля и другие) заключены в леммах о калькуляторе, о линейной независимости, и о сопряжении (§4 и §5).

Мы показываем, *как можно придумать* приводимые доказательства. Пути к ним намечены в виде задач (§3.2 и §4). Это характерно не только для дзенских монастырей, но и для серьезного преподавания математики. К важнейшим задачам приведены указания и решения (§3.5 и §4.9). Хотя *придумать* доказательства непросто, *изложить* их можно коротко (§3.3 и §5). Освобождение доказательства от деталей, возникших при его придумывании, но не нужных для него самого — важная часть его проверки.

Многие из приведенных задач — удачные темы для исследовательских работ школьников. Описание удачных примеров этой деятельности см. на [M]. А вот работы, уже подготовленные с использованием предыдущих версий этой брошюры: [Sa, Ak]. Примеры таких задач: 4.3.c, 4.5.c, 4.8, 4.10.h, 4.18.d, 4.20, 4.22.d, 4.24, 4.28.a (попроще), 4.29.bc, 4.31.4, 4.28.b, 4.32 (решение мне неизвестно, но может оказаться несложным). Большинство этих задач не претендуют на научную новизну.

1.4 План брошюры

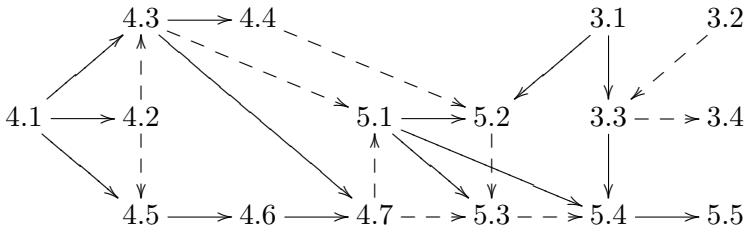
Эту брошюру не обязательно читать подряд. Читатель может выбрать удобную ему последовательность изучения (или вовсе опустить некоторые пункты) на основании приводимого плана. К нему разумно вернуться, если читатель потеряет нить изложения.

В §2.1 приводится переформулировка теоремы Гаусса (упомянутая в §1.1).

В §2.2 доказываются утверждения из §1.2 о разрешимости уравнений 3-й и 4-й степени (в задачах, к важнейшим из которых приведены указания и решения). Эти уравнения естественно сводятся к таким, которые ясно, как решать. Приведенный материал широко известен, но не входит в школьную или университетскую программу.

Каждый пункт из §2 и §6 независим с остальным текстом (т.е. он не используется в остальном тексте и для его изучения достаточно прочитать §1).

Вот схема зависимости остальных пунктов.



Пунктир в схеме означает, что один пункт нужен для мотивировки другого, но формально не используется в другом.

В §3 доказана построимость в теореме Гаусса. План §3 приводится в его начале.

В §4 приведены задачи, подводящие к доказательствам неразрешимости (т.е. непостроимости в теореме Гаусса теоремам о неразрешимости в радикалах). В §4.9 приведены указания и решения к важнейшим задачам из §4. Непостроимость в теореме Гаусса доказана в §5.2; к ней подводят только задачи из §§4.1–4.4. Теорема о неразрешимости в вещественных радикалах и теорема Галуа доказаны в §5.3 и §5.4, соответственно. К ним подводят задачи из §§4.1, 4.5–4.7.

Общие замечания к формулировкам задач. Задачи обозначаются жирными цифрами. Если условие задачи является утверждением, то в задаче требуется это утверждение доказать. Как правило, мы приводим *формулировку* задачи-утверждения перед ее-его *доказательством.* [4] В таких случаях для решения задачи могут потребоваться следующие задачи. Это всегда явно оговаривается в указаниях. Поэтому если некоторая задача не получается, то читайте дальше — соседние задачи могут оказаться подсказками. (На занятии задача-подсказка выдается только тогда, когда школьник или студент подумал над самой задачей.) Некоторые задачи не нужны для подведения к доказательству сформулированных теорем, но интересны сами по себе.

2 Первые шаги

2.1 Связь с построениями циркулем и линейкой

Используя отрезки длины a, b и c, можно построить циркулем и линейкой отрезки длины $a+b$, $a-b$, ab/c, $\sqrt{ab}$. Поэтому если на плоскости задан отрезок длины 1, то отрезок вещественно построимой длины можно построить циркулем и линейкой. Этот простой результат был известен еще древним грекам. Оказывается, верно и обратное.

Основная теорема теории геометрических построений. *Если отрезок длины a можно построить циркулем и линейкой, имея отрезок длины 1, то число a вещественно построимо.*

Этот несложный результат (доказанный лишь в 19-м веке) показывает, что из непостроимости числа $\cos(2\pi/n)$ вытекает непостроимость правильного n-угольника циркулем и линейкой. Для доказательства этого результата можно рассмотреть все возможные случаи появления новых объектов (точек, прямых, окружностей) и показать, что координаты всех построенных точек и коэффициенты уравнений всех проведенных прямых и окружностей являются построимыми. Детали читатель сможет восполнить самостоятельно или найти в [Ko, CR, Ma, P].

[4] В учебниках и курсах часто происходит обратное. Часто студент узнает формулировки красивых результатов и важных проблем, ради которых была придумана теория, только *после* продолжительного изучения этой теории. Иногда — в конце ее изучения, иногда — спустя несколько лет, а иногда не узнает совсем. Это способствует появлению представления о математике как науке, изучающей немотивированные понятия и теории. Такое представление принижает ценность математики.

2.2 Решение уравнений 3-й и 4-й степени в задачах

В этом пункте доказываются утверждения из §1.2 о разрешимости в вещественных и комплексных радикалах уравнений 3-й и 4-й степени в задачах. Хотя указания и решения важнейших задач приведены в конце пункта, к ним желательно обращаться после прочтения и прорешивания каждого подпункта.

Исследование графиков

Начнем с нескольких простых вводных задач.

2.1. (a) Уравнение $ax^3 + bx^2 + cx + d = 0$ сводится к уравнению $x^3 + px + q = 0$ заменой переменной.

(b) Уравнение $ax^4 + bx^3 + cx^2 + dx + e = 0$ сводится к уравнению $x^4 + px^2 + qx + r = 0$ заменой переменной.

2.2. (a) Найдите координаты центра симметрии графика функции $y = -2x^3 - 6x^2 + 4$.

(b) График любого кубического многочлена имеет центр симметрии.

В следующих двух задачах можно пользоваться без доказательства теоремой о промежуточных значениях многочлена: *для многочлена P если $P(a) > 0$ и $P(b) < 0$, то существует такое $c \in [a, b]$, что $P(c) = 0$.*

2.3. Сколько (вещественных) корней имеет уравнение

(a) $x^3 + 2x + 7 = 0$? (b) $x^3 - 4x - 1 = 0$?

2.4. Найдите количество решений уравнения $x^3 + px + q = 0$ (в зависимости от параметров p, q).

Решение уравнений 3-й степени

Следующие задачи посвящены уже собственно общим методам решения кубических уравнений.

В этом пункте «решить уравнение» означает «найти *все* его *вещественные* решения».

2.5. (a) Докажите, что $\sqrt[3]{2+\sqrt{5}} - \sqrt[3]{\sqrt{5}-2} = 1$.

(b) Найдите хотя бы одно решение уравнения $x^3 - 3\sqrt[3]{2}x + 3 = 0$.

Указание. Метод дель Ферро. Так как $(b+c)^3 = b^3 + c^3 + 3bc(b+c)$, то число $b+c$ является корнем уравнения $x^3 - 3bcx - (b^3 + c^3) = 0$.

(c) Решите уравнение $x^3 - 3\sqrt[3]{2}x + 3 = 0$.

2.6. (a) Разложите на множители выражение $a^3 + b^3 + c^3 - 3abc$.

(b) $a^2 + b^2 + c^2 \geq ab + bc + ca$. Когда достигается равенство?

(c) $a^3 + b^3 + c^3 \geq 3abc$ при $a, b, c > 0$.

(d) Разложите выражение $a^3 + b^3 + c^3 - 3abc$ на линейные множители с комплексными коэффициентами.

2.7. (a) Напишите формулу для решения уравнения $x^3 + px + q = 0$ методом дель Ферро (см. задачу 2.5). При каком условии применим этот метод, если квадратные корни разрешается извлекать только из положительных чисел?

(b) Докажите утверждение о разрешимости в вещественных радикалах из §1.2.

При решении некоторых кубических уравнений методом дель Ферро в формулах неожиданным образом возникают комплексные числа — как раз тогда, когда все корни исходного уравнения вещественны. Такие уравнения можно также решать следующим «чисто вещественным» методом. Он также интересен тем, что подводит к *трансцендентным методам* решения уравнений [PS].

2.8. *Метод Виета.* (a) $\sin 3\alpha = 3\sin\alpha - 4\sin^3\alpha$ и $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$.

Указание: используйте без доказательства равенства

$$\cos(\alpha+\beta) = \cos\alpha\cos\beta - \sin\alpha\sin\beta \quad \text{и} \quad \sin(\alpha+\beta) = \sin\alpha\cos\beta + \cos\alpha\sin\beta.$$

(b) Решите уравнение $4x^3 - 3x = \frac{1}{2}$.

(c) Решите уравнение $x^3 - 3x - 1 = 0$.

(d) Используя функции cos и arccos, напишите общую формулу для решения уравнения $x^3+px+q = 0$ методом, намеченным в этой задаче. При каком условии уравнение $x^3 + px + q = 0$ решается этим методом?

Решение уравнений 4-й степени

2.9. Решите уравнение

(a) $(x^2 + 2)^2 = 18(x - 1)^2$. (b) $x^4 + 4x - 1 = 0$. (c) $x^4 + 2x^2 - 8x - 4 = 0$.

Указание к 2.9.b. Метод Феррари. Подберите такие α, b, c, чтобы $x^4 + 4x - 1 = (x^2 + \alpha)^2 - (bx + c)^2$. Для этого найдите хотя бы одно α, для которого квадратный трехчлен $(x^2 + \alpha)^2 - (x^4 + 4x - 1)$ является полным квадратом.

2.10. (a) Найдите формулу для корней уравнения $x^4 + px^2 + qx + r = 0$ методом Феррари (см. задачу 2.9), использующую корень α вспомогательного кубического уравнения. Не забудьте разобрать все случаи!

Замечание. Уравнение $x^4 + ax^3 + bx^2 + cx + d = 0$ можно также решить, подобрав такие α, A, B, что $x^4 + ax^3 + bx^2 + cx + d = \left(x^2 + \frac{ax}{2} + \alpha\right)^2 - (Ax + B)^2$.

(b) Докажите утверждение о разрешимости в комплексных радикалах из §1.2.

Указания и решения к некоторым задачам

2.1. Воспользуйтесь заменами переменной $x' := x + \frac{b}{3a}$ и $x' := x + \frac{b}{4a}$.

2.3. (a) *Ответ*: 1.

Указание. Обозначим $f(x) := x^3+2x+7$. Так как $f(-2) < 0$ и $f(1) > 0$, то по теореме о промежуточных значениях многочлена корень имеется. Ввиду монотонности корень только один.

(b) *Ответ*: 3.

Указание. Обозначим $f(x) := x^3 - 4x - 1$. Так как $f(-2) < 0$, $f(-1) > 0$, $f(0) < 0$, $f(3) > 0$, то по теореме о промежуточных значениях многочлена имеется три корня.

2.4. *Ответ.* Если $p = q = 0$, то корень один. Иначе обозначим $D := \left(\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2\right)$. При $D > 0$ корень один, при $D = 0$ корней два, при $D < 0$ корней три.

Указание. Найдите промежутки возрастания и убывания. Найдите точки локальных экстремумов и значения в них. Для этого продифференцируйте функцию f, т.е. изучите знак выражения $\dfrac{f(x_1) - f(x_2)}{x_1 - x_2}$.

2.5. (a) Обозначим $x := \sqrt[3]{2 + \sqrt{5}} - \sqrt[3]{\sqrt{5} - 2}$. Тогда $x^3 = 4 - 3x$. Это уравнение имеет корень $x = 1$. Ввиду монотонности других корней нет.

Другое решение следует из $\sqrt[3]{\sqrt{5} \pm 2} = (\sqrt{5} \pm 1)/2$.

(b) *Ответ*: $x = -1 - \sqrt[3]{2}$.

Указание. $x^3 - 3\sqrt[3]{2}x + 3 = x^3 - 3bcx + (b^3 + c^3)$, где $b = 1$, $c = \sqrt[3]{2}$.

(c) В силу задачи 2.6.a уравнение $x^3 - 3\sqrt[3]{2}x + 3 = 0$ равносильно уравнению

$$(x + b + c)(x^2 + b^2 + c^2 - bc - bx - cx) = 0 \quad \text{с} \quad b = 1 \quad \text{и} \quad c = \sqrt[3]{2}.$$

По задаче 2.6.b второй сомножитель положителен при любом x (поскольку $b \neq c$). Значит, исходное уравнение имеет единственное решение $x = -b - c = -1 - \sqrt[3]{2}$.

2.6. (a) Поделите $a^3 - 3abc + (b^3 + c^3)$ на $a + b + c$ «уголком».

(d) *Ответ:* для $\varepsilon = (-1 + i\sqrt{3})/2$

$$a^3+b^3+c^3-3abc = (a+b+c)(a^2+b^2+c^2-ab-bc-ca) = (a+b+c)(a+b\varepsilon+c\varepsilon^2)(a+b\varepsilon^2+c\varepsilon).$$

2.8. (b) *Ответ*: $\cos\frac{\pi}{9}$, $\cos\frac{7\pi}{9}$, $\cos\frac{13\pi}{9} = \cos\frac{5\pi}{9}$.

(c) *Указание.* Сведите к (b) заменой $y = 2x$.

Ответ: $2\cos\frac{\pi}{9}$, $2\cos\frac{7\pi}{9}$, $2\cos\frac{13\pi}{9} = 2\cos\frac{5\pi}{9}$.

2.9. *Ответы*: (a) $(-3\sqrt{2} \pm \sqrt{10+12\sqrt{2}})/2$; (b) $(-\sqrt{2} \pm \sqrt{4\sqrt{2}-2})/2$.

3 Доказательство построимости в теореме Гаусса

В §3.1 и §3.3 доказана построимость в теореме Гаусса. В §3.2 основные идеи доказательства из §3.3 иллюстрируются на примерах и задачах. В §3.4 приводится дополнительный материал. Хотя указания и решения к задачам приведены в конце параграфа, к ним желательно обращаться после прочтения и прорешивания каждого пункта.

3.1 Переформулировка построимости в теореме Гаусса

Начнем с простых задач, подводящих к основному результату этого пункта — лемме о комплексификации.

3.1. Число $\cos(2\pi/n)$ вещественно построимо для $n = 3, 4, 5, 6, 8, 10, 15$.

3.2. Лемма об умножении (вещественная версия).
(a) Если $\cos(2\pi/n)$ вещественно построимо, то $\cos(\pi/n)$ вещественно построимо.
(b) Если $\cos(2\pi/n)$ и $\cos(2\pi/m)$ вещественно построимы и m, n взаимно просты, то $\cos(2\pi/mn)$ вещественно построимо.

Из этой леммы вытекает, что вещественная построимость в теореме Гаусса следует из вещественной построимости чисел $\cos(2\pi/n)$ для простых n вида $2^{2^s}+1$.

Комплексное число называется *построимым*, если его можно получить на комплексном калькуляторе так, чтобы при этом извлекались корни только второй степени.

3.3. Число $\cos(2\pi/n)$ построимо тогда и только тогда, когда число

$$\varepsilon_n := \cos(2\pi/n) + i\sin(2\pi/n)$$

построимо.

3.4. Лемма о комплексификации. Комплексное число построимо тогда и только тогда, когда его вещественная и мнимая части вещественно построимы.

Из этой леммы вытекает, что вещественное число построимо тогда и только тогда, когда оно вещественно построимо. [5] Значит, построимость в теореме Гаусса достаточно доказать с заменой «вещественной построимости» на «построимость».

3.2 Метод резольвент Лагранжа

Пункты (a), (b) и (b') следующей просто решить непосредственно. Для решения пунктов (c,d,e) уже нужна новая идея, изложенная далее.

3.5. (a) Число ε_5 построимо.
(b) На комплексном калькуляторе можно получить число ε_7 так, чтобы при этом корни извлекались только второй и третьей степени.
(b') На комплексном калькуляторе можно получить число ε_7 так, чтобы при этом корни второй и третьей степени извлекались только по одному разу, а корни большей степени не извлекались совсем.

[5] Заметим, что на комплексном калькуляторе нет кнопок Re и Im. Однако их можно «реализовать», доказав, что если можно получить число z, то можно получить и $\overline{z}$. Но так будет доказана *построимость* вещественной и мнимой части, а не их *вещественная построимость*. Для доказательства вещественной построимости нужно научиться извлекать корень из комплексного числа при помощи вещественного калькулятора. Это возможно только для корней второй степени. Если в определении построимости и вещественной построимости допускать извлечения корней третьей степени, то аналог леммы о комплексификации будет неверен (см. утверждение в самом конце §1.2).

(c) На комплексном калькуляторе можно получить число ε_{11} так, чтобы при этом корни извлекались только второй и пятой степени.

(d) Число ε_{17} построимо.

(e) Докажите построимость в теореме Гаусса.

Оказывается, что в задачах 3.5.cde (и во многих других ситуациях!) вместо работы с набором корней удобнее работать с некоторыми выражениями от корней — *резольвентами Лагранжа*, которые мы скоро определим.

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

$$(a)\begin{cases} x+y+z+t=a \\ x+iy-z-it=b \\ x-y+z-t=c \\ x-iy-z+it=d \end{cases} \quad . \qquad (b)\begin{cases} x+y+z=a \\ x+\varepsilon y+\varepsilon^2 z=b \\ x+\varepsilon^2 y+\varepsilon z=c \end{cases}, \quad \text{где} \quad \varepsilon := \varepsilon_3 = \frac{-1+i\sqrt{3}}{2}.$$

Ваши решения этой задачи показывают, что вместо «нахождения» корней x, y, z кубического уравнения достаточно найти выражения a, b, c из задачи 3.6.b, и вместо «нахождения» корней x, y, z, t уравнения 4-й степени достаточно найти выражения a, b, c, d от корней из задачи 3.6.a. Эти выражения и называются *резольвентами Лагранжа*. Они «лучше», поскольку они «симметричнее» в следующем смысле.

Для кубического уравнения $a = a(x, y, z)$ — *симметрическая* функция корней (т. е. не меняющаяся при их перестановке). Тогда из теоремы Виета и теореме о представимости симметрического многочлена в виде функции от элементарных симметрических следует, что эту функцию $a(x, y, z)$ можно выразить через коэффициенты уравнения. Функции $b = b(x, y, z)$ и $c = c(x, y, z)$ не симметрические. Но при замене $x \leftrightarrow y$ функция b переходит в εc, а c в $\varepsilon^2 b$ (проверьте!). Значит, функции bc и $b^3 + c^3$ не меняются при этой замене. Аналогично они не меняются при замене $z \leftrightarrow y$. Поэтому функции bc и $b^3 + c^3$ симметрические. Тогда их можно выразить через коэффициенты уравнения, а затем «найти» сами b и c. Так решается кубическое уравнение. Ср. §2.2.

Читателю будет полезно решить уравнение 4-й степени при помощи резольвент Лагранжа (ср. §2.2). А также сообразить, почему же этот метод не работает для общего уравнения 5-й степени.

Доказательство построимости числа $\varepsilon := \varepsilon_5$. Обозначим

$$\begin{aligned} T_0 :=& \varepsilon + \varepsilon^2 + \varepsilon^4 + \varepsilon^8 = -1, \\ T_1 :=& \varepsilon + i\varepsilon^2 - \varepsilon^4 - i\varepsilon^8, \\ T_2 :=& \varepsilon - \varepsilon^2 + \varepsilon^4 - \varepsilon^8 \qquad \text{и} \\ T_3 :=& \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^8. \end{aligned}$$

Тогда $T_0 + T_1 + T_2 + T_3 = 4\varepsilon$. Поэтому достаточно доказать построимость каждого из чисел T_1, T_2, T_3.

При замене ε на ε^2 число T_1 переходит в $-iT_1$. Значит, T_1^4 не меняется при этой замене. Поэтому T_1^4 не меняется при двукратной и трехкратной таких заменах, т.е., при заменах ε на ε^4 и ε на $\varepsilon^8 = \varepsilon^3$. Итак, для любого k число T_1^4 не меняется при замене ε на ε^k.

Раскроем скобки в произведении T_1^4 и заменим ε^5 на 1. Получим равенство

$$T_1^4 = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 \quad \text{для некоторых} \quad a_k \in \mathbb{Z} + i\mathbb{Z}.$$

Так как для любого k число T_1^4 не меняется при замене ε на ε^k, получаем $a_1 = a_2 = a_3 = a_4$. Поэтому $T_1^4 = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$. Значит, T_1 построимо. Аналогично T_2 и T_3 построимы.

В приведенном рассуждении нужно обосновать вывод «$a_1 = a_2 = a_3 = a_4$» (и строго определить, что такое «замена ε на ε^2»). Обоснование для общего случая трудное;

читатель может найти пример такого рассуждения в [E1, §24]. Поэтому, вместо того, чтобы его приводить, мы немного изменим доказательство; именно этим изменением приводимое доказательство отличается от данного в [E1].

Для этого, вместо того, чтобы работать с *числами*, мы будем работать с *многочленами* от одной переменной — и будем подставлять в них ε в качестве аргумента. А именно, определим многочлен $T_1(x) := x + ix^2 - x^4 - ix^8$. Определим многочлены $T_0(x)$, $T_2(x)$ и $T_3(x)$ формулами, аналогичными вышенаписанным. Как и выше, $(T_0 + T_1 + T_2 + T_3)(\varepsilon) = 4\varepsilon$. Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, 3$. Имеем [6]

$$iT_1(x^2) \equiv T_1(x) \mod (x^5 - 1) \quad \Rightarrow \quad T_1^4(x^2) \equiv T_1^4(x) \mod (x^5 - 1) \quad \Rightarrow$$

$$\Rightarrow \quad T_1^4(x^k) \equiv T_1^4(x) \mod (x^5 - 1) \quad \text{для любого } k.$$

Возьмем многочлен $a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ с коэффициентами в $\mathbb{Z} + i\mathbb{Z}$, сравнимый с $T_1^4(x)$ по модулю $x^5 - 1$.

Тогда $a_1 = a_2 = a_3 = a_4$. Поэтому $T_1^4(\varepsilon) = a_0 - a_1 \in \mathbb{Z} + i\mathbb{Z}$. [7]

Значит, $T_1(\varepsilon)$ построимо. Аналогично $T_2(\varepsilon)$ и $T_3(\varepsilon)$ построимы. QED

3.7. (a) Обозначим

$$\beta := \frac{1 + i\sqrt{3}}{2} \quad \text{и} \quad T(x) := x + \beta x^3 + \beta^2 x^9 + \beta^3 x^{27} + \beta^4 x^{81} + \beta^5 x^{243}.$$

Докажите, что $T(x) \equiv \beta T(x^3) \mod (x^7 - 1)$.

(b) Обозначим

$$\beta := \varepsilon_{10} \quad \text{и} \quad T(x) := x + \beta x^2 + \beta^2 x^4 + \beta^3 x^8 + \beta^4 x^{16} + \cdots + \beta^9 x^{512}.$$

Докажите, что $T(x) \equiv \beta T(x^2) \mod (x^{11} - 1)$.

3.3 Доказательство построимости в теореме Гаусса

Изучив (и прорешав) два предыдущих пункта, мы готовы перейти собственно к построению в теореме Гаусса.

Лемма об умножении. *(a) Если ε_n построимо, то ε_{2n} построимо.*

(b) Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{mn} построимо.

Доказательство получается из формул $\varepsilon_{2n} \in \sqrt{\varepsilon_n}$ и $\varepsilon_{mn} = \varepsilon_m^x \varepsilon_n^y$, где x и y — целые числа, для которых $nx + my = 1$. QED

При решении задачи 3.5.a мы использовали различность остатков от деления чисел $2, 2^2, 2^3, 2^4$ на 5. При решении задачи 3.5.cd и 3.7.a мы использовали аналогичное свойство чисел 2 и 11, 6 и 17, 3 и 7. Для общего случая необходимо следующее обобщение.

Теорема о первообразном корне. *Для любого простого p существует число g, для которого остатки от деления на p чисел $g^1, g^2, g^3, \ldots, g^{p-1}$ различны.*

Указание к доказательству для $p = 2^m + 1$ (только этот случай нужен для теоремы Гаусса). Если первообразного корня нет, то сравнение $x^{2^{m-1}} \equiv 1 \bmod p$ имеет $p - 1 = 2^m > 2^{m-1}$ решений. QED

---

[6] Два многочлена называются *сравнимыми по модулю многочлена* $x^5 - 1$, если их разность делится на $x^5 - 1$.

[7] Другой способ, предложенный М. Ягудиным:

$$T_1^4(\varepsilon) = a_0 + a_1\varepsilon + a_2\varepsilon^2 + a_3\varepsilon^3 + a_4\varepsilon^4 = a_0 + a_1\varepsilon^2 + a_2\varepsilon^4 + a_3\varepsilon + a_4\varepsilon^3 =$$

$$= a_0 + a_1\varepsilon^3 + a_2\varepsilon + a_3\varepsilon^4 + a_4\varepsilon^2 = a_0 + a_1\varepsilon^4 + a_2\varepsilon^3 + a_3\varepsilon^2 + a_4\varepsilon.$$

Суммируя эти выражения, получим $4T_1^4(\varepsilon) = a_0 - a_1 - a_2 - a_3 - a_4 \in \mathbb{Z} + i\mathbb{Z}$.

Доказательство построимости в теореме Гаусса. По лемме 3.4 о комплексификации и по лемме об умножении достаточно доказать, что ε_n построимо для любого простого $n = 2^{2^s} + 1$. Так как $n - 1 = 2^m$, то по лемме об умножении $\beta := \varepsilon_{n-1}$ построимо. Обозначим

$$\mathbb{Z}[\beta] := \{a_0 + a_1\beta + a_2\beta^2 + \cdots + a_{n-2}\beta^{n-2} \mid a_0, \ldots, a_{n-2} \in \mathbb{Z}\}.$$

Пусть g — первообразный корень по модулю n. Для

$$r = 0, 1, 2, \ldots, n-2, \quad \text{обозначим} \quad T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \cdots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

Тогда $(T_0 + T_1 + \cdots + T_{n-2})(\varepsilon) = (n-1)\varepsilon$. Имеем $T_0(\varepsilon) = -1$. Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, \ldots, n-2$. Имеем

$$\beta^r T_r(x^g) \equiv T_r(x) \mod (x^n - 1) \quad \Rightarrow \quad T_r^{n-1}(x^g) \equiv T_r^{n-1}(x) \mod (x^n - 1) \quad \Rightarrow$$

$$\Rightarrow \quad T_r^{n-1}(x^k) \equiv T_r^{n-1}(x) \mod (x^n - 1) \quad \text{для любого } k.$$

Возьмем многочлен $a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_2 = \cdots = a_{n-1}$. Поэтому $T_r^{n-1}(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[\beta]$. Значит, $T_r(\varepsilon)$ построимо. QED

3.8. * (a) Если n простое, то из числа 1 можно получить множество чисел, содержащее ε_n, используя четыре арифметические операции и извлечения корней $(n-1)$-й степени (при которых получаются все $n - 1$ значений корня).

(b) *Теорема Гаусса о понижении.* Для любого n из числа 1 можно получить множество чисел, содержащее ε_n, используя четыре арифметические операции и извлечения корней только степеней, строго меньших n (при которых получаются все значения корня).

3.4 Эффективные доказательства построимости

Здесь приводятся другие доказательства построимости в теореме Гаусса и теоремы Гаусса о понижении 3.8.b. Они сложнее вышеприведенных, но дают более реальную возможность получить явные формулы [BK, Sa]. Именно они принадлежит Гауссу.

Интересно бы получить явные формулы и при помощи вышеприведенного метода.

Эффективное доказательство построимости в теореме Гаусса для $n = 5$. Сразу выразить число $\varepsilon := \varepsilon_5$ через радикалы трудно, поэтому сначала выразим некоторые «многочлены от ε». Мы знаем, что $\varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1$. Поэтому

$$(\varepsilon + \varepsilon^4)(\varepsilon^2 + \varepsilon^3) = \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 = -1.$$

Обозначим

$$T_0 := \varepsilon + \varepsilon^4 \quad \text{и} \quad T_1 := \varepsilon^2 + \varepsilon^3.$$

Тогда по теореме Виета числа T_0 и T_1 являются корнями уравнения $t^2 + t - 1 = 0$. Поэтому можно выразить T_0 (и T_1). Поскольку $\varepsilon \cdot \varepsilon^4 = 1$, то по теореме Виета числа ε и ε^4 являются корнями уравнения $t^2 - T_0 t + 1 = 0$. Поэтому можно выразить ε (и ε^4).

Идея доказательства теоремы Гаусса о понижении 3.8.b для общего случая. Достаточно доказать для простого n. Разложим число $n-1$ в произведение $q_1 q_2 \dots q_s$ простых чисел. Обозначим $\varepsilon := \varepsilon_n$. Сначала хорошо бы разбить сумму

$$\varepsilon + \varepsilon^2 + \dots + \varepsilon^{n-1} = -1$$

на q_1 слагаемых $T_0, T_1, \dots, T_{q_1-1}$, которые выражаются в радикалах (иными словами, *сгруппировать* хитрым образом корни уравнения $1 + x + x^2 + \dots + x^{n-1} = 0$). Затем хорошо бы разбить каждую сумму T_k на q_2 слагаемых $T_{k,0} + T_{k,1} + \dots + T_{k,q_2-1}$, которые выражаются в радикалах. И так далее, пока не получим $T_{\underbrace{1,\dots,1}_{s}} = \varepsilon$.

Однако придумать нужные группировки чисел $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$ нетривиально.

3.9. (a) Разбейте числа $\varepsilon_7, \varepsilon_7^2, \dots, \varepsilon_7^6$ на 2 группы по 3 элемента и выразите сумму чисел в каждой группе через квадратные радикалы.

(b) Разбейте числа $\varepsilon_{11}, \varepsilon_{11}^2, \dots, \varepsilon_{11}^{10}$ на 2 группы по 5 элементов и выразите сумму чисел в каждой группе через квадратные радикалы.

3.10. Получите формулы для (a) ε_7, (b) ε_{11}, в которых извлекаются корни только степеней 2, 3, 5. (Ср. с задачей 3.5.c.)

3.11. * Получите формулы для следующих чисел такие, в которых извлекаются корни только степеней 2 и 3.

(a) $\varepsilon_{13} + \varepsilon_{13}^4 + \varepsilon_{13}^3 + \varepsilon_{13}^{12} + \varepsilon_{13}^9 + \varepsilon_{13}^{10}$. (b) $\varepsilon_{13} + \varepsilon_{13}^3 + \varepsilon_{13}^9$. (c) ε_{13}.

Теорема о первообразном корне, приведенная в разделе 3.3, позволяет отождествить множество ненулевых вычетов по простому модулю n, и множество всех вычетов по модулю $n-1$. А именно, выбрав первообразный корень g, мы вычету k по модулю $n-1$ сопоставляем (ненулевой) остаток от деления g^k на n. После этого отождествления построенные выше разбиения начинают выглядеть гораздо проще:

3.12. (a) Выберите первообразный корень g по модулю 7 и посмотрите, чему соответствует полученное в задаче 3.9(a) разбиение для остатков по модулю 6 (остатку k соответствует число ε^{g^k}).
(b) То же для задачи 3.9(b).
(c) То же для наборов из задачи 3.11.

Начнем, тем не менее, с простого случая — со случая простого $n = 2^m + 1$, когда все простые q_i равны 2. Тем самым мы еще раз докажем теорему Гаусса о построимости, но на этот раз, получив более эффективный способ построения соответствующего ε_n.

Эффективное доказательство теоремы Гаусса о построимости. Как и раньше, отметим, что достаточно доказать построимость числа ε_n для n простого, $n - 1 = 2^m$. Выберем и зафиксируем первообразный корень g по модулю n.

Определим теперь числа T_0 и T_1. Читатель, решивший задачу 3.12, наверняка уже заметил, что в упомянутых там случаях происходило разбиение на слагаемые ε_n^k с k, являющимися четными и нечетными степенями g соответственно. Возьмем это за общее определение: положим

$$T_0 := \sum_{\substack{0\leq b\leq 2^m-1,\\ b\equiv 0 \mod 2}} \varepsilon_n^{g^b}, \quad T_1 := \sum_{\substack{0\leq b\leq 2^m-1,\\ b\equiv 1 \mod 2}} \varepsilon_n^{g^b},$$

Кроме того, нам будет удобно обозначить через $T_\emptyset$ уже встречавшееся раньше выражение — сумму всех ε_n^k по всем ненулевым остаткам k:

$$T_\emptyset := \sum_{j=1}^{n-1} \varepsilon_n^j = \sum_{b=0}^{2^m-1} \varepsilon_n^{g^b}.$$

Собственно, как мы уже видели раньше, $T_\emptyset = -1$.

Докажем теперь, что T_0 и T_1 построимы (более того, для их выражения хватит одного извлечения комплексного квадратного корня). Действительно, $T_0+T_1 = T_\emptyset = -1$. Поэтому достаточно проверить, что произведение T_0T_1 также является целым числом. Раскроем скобки в этом произведении:

$$T_0T_1 = \sum_{k=0}^{n-1} N_s\varepsilon_n^s, \tag{1}$$

где N_s это число способов представить вычет s по модулю n как сумму $k+l$, где ε_n^k входит в сумму T_0, а ε_n^l входит в сумму T_1:

$$N_s = \{(b_0, b_1) \mid b_0 \equiv 0,\, b_1 \equiv 1 \mod 2, \quad g^{b_0} + g^{b_1} \equiv s \mod n\}.$$

Теперь несложно увидеть, что все N_s при всех ненулевых s равны. Действительно, умножив любое представление $g^{b_0} + g^{b_1} \equiv s \mod n$ на g, мы получим представление $g^{b_1'} + g^{b_0'} \equiv gs \mod n$, где

$$b_0' = b_1 + 1 \equiv 0 \mod 2, \quad b_1' = b_0 + 1 \equiv 1 \mod 2.$$

Тем самым, $N_{gs} = N_s$ при всех s, и поскольку g — первообразный корень, отсюда следует, что все N_s при $s \neq 0$ равны. Подставив это в (1), получаем

$$T_0T_1 = N_0 + N_1T_\emptyset = N_0 - N_1.$$

Теперь уже ясно, как продолжать доказательство: для перехода от T_0 к T_{00} и T_{10} будем использовать уже сравнение по модулю 4, и так далее. А именно, для любой (в том числе, начинающейся с одного или нескольких нулей) последовательности $A = (a_j, \ldots, a_1, a_0) \in \{0,1\}^j$ любой длины j от 0 до m обозначим

$$\overline{a_{i-1}\ldots a_1a_0} := a_{m-1}2^{m-1} + \cdots + 2a_1 + a_0$$

и положим

$$T_A := \sum_{\substack{0\leqslant b\leqslant n-1,\\ b\equiv \overline{A} \mod 2^j}} \varepsilon_n^{g^b}.$$

Теорема Гаусса о построении будет доказана, как только мы докажем следующую лемму:

Лемма. *Для любого j и любой последовательности $A \in \{0,1\}^j$ число T_A выражается через квадратные радикалы.*

Доказательство. Будем вести доказательство по индукции по длине j слова A. В случае $j = 0$, как мы уже видели, $T_A = T_\emptyset = -1$, и доказывать нечего. Проведем шаг индукции: пусть для какого-то j утверждение леммы уже доказано. Докажем тогда построимость чисел T_{0A} и T_{1A} для произвольного слова A длины j. Опять-таки, $T_{0A}+T_{1A} = T_A$, которое построимо по предположению индукции. Аналогично уже рассмотренному случаю, достаточно доказать построимость произведения $T_{0A}T_{1A}$. Раскрыв скобки, получаем

$$T_{0A}T_{1A} = \sum_s N_s \varepsilon_n^s, \tag{2}$$

где N_s — число решений сравнения $g^{b_0} + g^{b_1} \equiv s \mod n$, где $b_0 \equiv \overline{0A} \mod 2^{j+1}$, $b_1 \equiv \overline{1A} \mod 2^{j+1}$. Аналогично уже рассмотренному случаю T_0 и T_1, любое решение такого сравнения для s можно умножить на g^{2^j}: мы получим решение сравнения $g^{b'_1}+g^{b'_0} = g^{2^j} s$, где

$$b'_0 = b_1 + 2^j \equiv \overline{0A} \mod 2^{j+1}, \quad b'_1 = b_0 + 2^j \equiv \overline{1A} \mod 2^{j+1}.$$

Тем самым, $N_s = N_{g^{2^j} s}$, и сумму в правой части (2) можно представить как

$$T_{0A}T_{1A} = \sum_s N_s \varepsilon_n^s = N_0 + \sum_{0 \le c \le 2^j - 1} \sum_{\substack{0 \leqslant b \leqslant n-1, \\ b \equiv c \mod 2^j}} N_{g^b} \varepsilon_n^{g^b} = N_0 + \sum_{C \in \{0,1\}^j} N_{g^{\overline{C}}} T_C,$$

и эта сумма выражается в квадратных радикалах по предположению индукции.[8] □

Из доказанной леммы немедленно следует теорема Гаусса о построимости: ведь из нее следует, в частности, построимость $T_{\underbrace{0\ldots0}_{m}} = \varepsilon_n$. QED

[8] Вот чуть более сложное окончание доказательства, которое поможет понять обобщение — теорему Гаусса о понижении 3.8.b. Вместо $T_{0A}T_{1A}$ рассмотрим

$$(T_{0A} - T_{1A})^2 = \left(\sum_{Bl \in \mathbb{Z}_2^{m-k}} (-1)^l \varepsilon_n^{g^{\overline{BlA}}} \right)^2 = \sum_{l=0,s=0}^{1,n-1} N_{s,l} (-1)^l \varepsilon_n^s \overset{(*)}{=} \sum_{l=0}^{1} (-1)^l \left(N_{0,l} + \sum_{C \in \mathbb{Z}_2^k} N_{g^{\overline{C}},l} T_C \right).$$

Здесь число $N_{s,l}$ (зависящее от A) есть количество упорядоченных решений

$$l_1, l_2 \in \mathbb{Z}_2, \quad B_1, B_2 \in \mathbb{Z}_2^{m-k-1} \quad \text{системы сравнений} \quad \begin{cases} l_1 + l_2 \equiv l \mod 2 \\ g^{\overline{B_1 l_1 A}} + g^{\overline{B_2 l_2 A}} \equiv s \mod n \end{cases}.$$

Ясно, что $N_{s,l} = N_{g^{2^k} s,l}$. Отсюда вытекает равенство (*).

Эффективное доказательство теоремы Гаусса о понижении 3.8.b. Пусть $n-1 = q_1 q_2 \dots q_m$ — разложение на простые множители (не обязательно различные). Пусть

$$a_i \in \{0, 1, 2, \dots, q_{i+1} - 1\} \quad \text{для каждого} \quad i \in \{0, 1, 2, \dots, m-1\}.$$

Обозначим $\quad \overline{a_{m-1} \dots a_1 a_0} := a_0 + a_1 q_1 + a_2 q_1 q_2 + \dots + a_{m-1} q_1 q_2 \dots q_{m-1}.$

('Запись в системе счисления с переменным основанием.') Для дальнейшего важно, что в начале могут стоять нулевые «цифры». Обозначим через

$$[k, l] := \mathbb{Z}_{q_k} \times \dots \times \mathbb{Z}_{q_l}$$

множество наборов из $(k - l + 1)$ «цифр», которые могут стоять в записи $\overline{a_{m-1} \dots a_1 a_0}$ на местах с k-го справа по l-е справа (a_0 считается первым справа).

Обозначим через g первообразный корень по модулю n. Для $A \in [k, 1]$ обозначим

$$T_A := \sum_{B \in [m, k+1]} \varepsilon_n^{g^{\overline{BA}}}.$$

С помощью индукции по k покажем, как *для любых* k *и* $A \in [1, k]$ *число* T_A *выразить через радикалы.* Тогда для $k = m$ получим выражение числа $T_{\underbrace{\overline{0 \dots 0}}_{m}} = \varepsilon_n$.

База $k = 0$ следует из $T_\emptyset = -1$. Докажем шаг индукции. Обозначим $q := q_{k+1}$ и $\beta := \varepsilon_q$. Для любых $r = 0, 1, 2, \dots, q-1$ и $A \in [k, 1]$ обозначим

$$T_A^{(r)} := T_{0A} + \beta^r T_{1A} + \beta^{2r} T_{2A} + \dots + \beta^{(q-1)r} T_{(q-1)A}.$$

Тогда

$$T_A^{(0)} = T_A \quad \text{и} \quad q T_{lA} = \beta^{-l} T_A^{(0)} + \beta^{-2l} T_A^{(1)} + \dots + \beta^{-(q-1)l} T_A^{(q-1)}.$$

Для любых $r = 1, 2, \dots, q-1$ и $A \in [k, 1]$ имеем

$$(T_A^{(r)})^q = \left(\sum_{Bl \in [m, k+1]} \beta^{lr} \varepsilon_n^{g^{\overline{BlA}}} \right)^q = \sum_{l=0, s=0}^{q-1, n-1} |s, l| \varepsilon_n^s \beta^l \overset{(*)}{=} \sum_{l=0}^{q-1} \beta^l \left(|0, l| + \sum_{C \in [k, 1]} |g^{\overline{C}}, l| T_C \right).$$

Здесь число $|s, l|$ (зависящее от A) есть количество упорядоченных решений $l_1, l_2, \dots, l_q \in \mathbb{Z}_q, \quad B_1, B_2, \dots, B_q \in [m, k+2]$ системы сравнений

$$\begin{cases} r(l_1 + l_2 + \dots + l_q) \equiv l \mod q \\ g^{\overline{B_1 l_1 A}} + g^{\overline{B_2 l_2 A}} + \dots + g^{\overline{B_q l_q A}} \equiv s \mod n \end{cases}.$$

Ясно, что $|s, l| = |g^{q_1 q_2 \dots q_k} s, l|$. Отсюда вытекает равенство (*). Так T_{lA} выражаются через радикалы. QED

3.5 Указания и решения к некоторым задачам из §3

3.3. Вытекает из

$$\varepsilon_n = \cos\frac{2\pi}{n} + \sqrt{\sin^2\frac{2\pi}{n} - 1}, \quad \cos\frac{2\pi}{n} = \frac{\varepsilon_n + \varepsilon_n^{-1}}{2} \quad \text{и} \quad \sin\frac{2\pi}{n} = \frac{\varepsilon_n - \varepsilon_n^{-1}}{2}.$$

Или из задачи 3.4.

3.6. Используйте, что $1 + \varepsilon + \varepsilon^2 = 0$ и $1 + i + i^2 + i^4 = 0$.

3.4. Часть «тогда» очевидна. Для доказательства части «только тогда» напишите $\sqrt{a+bi} = u + vi$ и выразите u, v через a и b с помощью четырех арифметических операций и квадратных радикалов.

3.5. (b') $\varepsilon_7^6 + \varepsilon_7^5 + \cdots + \varepsilon_7 + 1 = 0$. Как решать алгебраические уравнения n-й степени, у которых коэффициенты при k-й и при $(n-k)$-й степенях равны?

3.5.bcd, 3.7. Аналогично приведенному доказательству построимости числа ε_5. См. подробности в §3.3.

3.8. (a) Аналогично доказательству построимости в теореме Гаусса.

(b) Докажем теорему при помощи индукции по n.

Если $n = ab$ для некоторых целых $0 < a, b < n$, то шаг индукции следует из $\varepsilon_n = \sqrt[a]{\varepsilon}_b$.

Если же n простое, то шаг индукции следует из (a).

3.9. (a) Обозначим $\varepsilon := \varepsilon_7$. Выразим

$$T_0 = \varepsilon^{3^0} + \varepsilon^{3^2} + \varepsilon^{3^4} \quad \text{и} \quad T_1 = \varepsilon^3 + \varepsilon^{3^3} + \varepsilon^{3^5}.$$

Малоэффективное доказательство выразимости. Число T_0T_1 есть многочлен от ε с целыми коэффициентами степени меньше 7 (точнее, значение в точке ε некоторого многочлена от x по модулю $x^7 - 1$ с целыми коэффициентами). При замене $\varepsilon \to \varepsilon^3$ числа T_0 и T_1 меняются местами. Поэтому при замене $\varepsilon \to \varepsilon^3$ число T_0T_1 не изменяется. Значит, коэффициент многочлена при ε^s равен его коэффициенту при ε^{3s}. Так как 3 — первообразный корень по модулю 7, то все коэффициенты многочлена, кроме свободного члена, равны. Из этого и $\varepsilon + \varepsilon^2 + \cdots + \varepsilon^6 = -1$ вытекает, что T_0T_1 целое число. Поэтому T_0 и T_1 выражаются.

Эффективное доказательство выразимости. Имеем $T_0T_1 = \sum_{s=0}^{6} N(s)\varepsilon^s$, где N_s есть количество решений $(n, m) \in \mathbb{Z}_3^2$ сравнения $3^{2n} + 3^{2m+1} \equiv s \mod 7$. Ясно, что $N_0 + N_1 + N_2 + \cdots + N_6 = 9$. Нетрудно проверить, что $N_s = N_{3s}$. Поэтому $N_1 = N_2 = \cdots = N_6$. Так как $3^0 + 3^1 \not\equiv 0 \mod 7$, то $N_0 \neq 9$. Из всего этого следует, что $N_0 = 3$ и $N_1 = 1$. Значит, $T_0T_1 = 3 - 1 = 2$. Отсюда $\{T_0, T_1\} = \{\frac{-1-\sqrt{7}}{2}, \frac{-1+\sqrt{7}}{2}\}$.

3.10. (a) Обозначим $\varepsilon := \varepsilon_7$. Имея вычисленные выше T_0 и T_1, выразим ε. Обозначим

$$\beta := \varepsilon_3 \quad \text{и} \quad T_{01} := \varepsilon^{3^0} + \beta\varepsilon^{3^2} + \beta^2\varepsilon^{3^4}.$$

Малоэффективное доказательство выразимости. Число T_{01}^3 есть многочлен от ε с коэффициентами в $\mathbb{Z}[\beta]$ степени меньше 7. При замене $\varepsilon \to \varepsilon^{3^2}$ число T_{01}^3 не изменяется. Значит, коэффициент многочлена при ε^s равен его коэффициенту при $\varepsilon^{3^2 s}$. Так как 3 — первообразный корень по модулю 7, то коэффициенты многочлена при степенях 3^{2n} равны и коэффициенты многочлена при степенях 3^{2n+1} равны. Из этого и определений T_0 и T_1 вытекает, что T_{01}^3 выражается при помощи кубического корня через множества $\mathbb{Z}[\beta, T_0, T_1]$. Поэтому T_{01} выражается как надо.

Эффективное доказательство выразимости. Имеем $T_{01}^3 = \sum_{s=1}^{7}\sum_{l=0}^{2} |s, l|\varepsilon^s\beta^l$, где $|s, l|$ есть количеству решений $(l_1, l_2, l_3) \in \mathbb{Z}_3^3$ системы сравнений

$$\begin{cases} l_1 + l_2 + l_3 \equiv l \mod 3 \\ 3^{2l_1} + 3^{2l_2} + 3^{2l_3} \equiv s \mod 7 \end{cases}.$$

Ясно, что $\sum_{s=1}^{7}\sum_{l=0}^{2}|s,l|=27$. Нетрудно проверить, что $|s,l|=|3^2s,l|$. Поэтому $|1,l|=|2,l|=|4,l|$ и $|3,l|=|5,l|=|6,l|$. Значит, $T_{01}^3=A+BT_0+CT_1$ для некоторых $A,B,C\in\mathbb{Z}[\beta]$. Их несложно найти.

Окончание указаний. Аналогично выражается $T_{02}:=\varepsilon^{3^1}+\beta\varepsilon^{3^3}+\beta^2\varepsilon^{3^5}$. Потом выражается $\varepsilon=\dfrac{T_0+T_{01}+T_{02}}{3}$.

3.11. (a) Обозначим $\varepsilon=\varepsilon_{13}$,

$$A_0:=\varepsilon+\varepsilon^4+\varepsilon^3+\varepsilon^{12}+\varepsilon^9+\varepsilon^{10}\quad\text{и}\quad A_1:=\varepsilon^2+\varepsilon^5+\varepsilon^6+\varepsilon^7+\varepsilon^8+\varepsilon^{11}.$$

Тогда $A_0+A_1=-1$ и $A_0A_1=-3$. Значит, $\{A_0,A_1\}=\{\dfrac{-1-\sqrt{13}}{2},\dfrac{-1+\sqrt{13}}{2}\}$. Из рисунка правильного 13-угольника (или из оценок) видно, что $A_1<0$. Значит, $A_1=\dfrac{-1-\sqrt{13}}{2}$ и $A_0=\dfrac{-1+\sqrt{13}}{2}$.

4 Задачи о неразрешимости в радикалах

В параграфах 4 и 5 через $\mathbb{Q}$ обозначается множество всех рациональных чисел; 'многочлен с рациональными коэффициентами' коротко называется многочленом. Многочлен называется *неприводимым* над множеством F, если он не раскладывается в произведение многочленов меньшей степени с коэффициентами в F. Хотя указания и решения к задачам приведены в конце параграфа, к ним желательно обращаться после прочтения и прорешивания каждого пункта.

4.1 Одно извлечение квадратного корня

Следующие задачи 4.1 и 4.3.c интересны в связи с неразрешимостью в радикалах, поскольку нам нужно придумать многочлен, корни которого невозможно получить на калькуляторе, а числа из задачи 4.1 являются корнями многочленов (подумайте, каких).

4.1. Представимо ли следующее число в виде $a+\sqrt{b}$, где $a,b\in\mathbb{Q}$?

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

4.2. Число $\cos(2\pi/9)$ является корнем уравнения $8x^3-6x+1=0$.

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

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

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

4.4. Лемма о калькуляторе. Пусть $F\in\{\mathbb{R},\mathbb{C}\}$. Число, которое можно получить на F-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 $F=\mathbb{R}$, $b>0$.

Из утверждения 4.3.c и леммы 4.4 о калькуляторе вытекает, что *если многочлен степени выше второй неприводим над $\mathbb{Q}$, 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.

4.2 Одно извлечение корня четвертой степени

Здесь развиваются идеи из §4.1.

4.5. 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) $\sqrt[6]{3}$; (c) $\sqrt[4]{3}$.

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

4.7. 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 $a=b=c=d=0$.

4.8. 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 $a,b,c,d,r^4\in\mathbb{Q}$.

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

4.3 Несколько извлечений квадратных корней

Здесь развиваются идеи из §4.1 и §4.2.

4.10. Существуют ли рациональные числа a,b,c,d, для которых $\sqrt[3]{2}=$
(a) $\dfrac{a+\sqrt{b}}{c+\sqrt{b}}$; (b) $a+\sqrt{b}+\sqrt{c}$; (c) $a+\sqrt{b+\sqrt{c}}$; (d) $a+\sqrt{b}+\sqrt{c}+\sqrt{d}$?

4.11. Следующие числа не являются вещественно построимыми: (a) $\sqrt[3]{2}$; (b) $\cos(2\pi/9)$; (c) произвольный корень уравнения $y^3+y+1=0$; (d) $\cos(2\pi/7)$.

4.12. (a) Оторвем у комплексного калькулятора кнопку ':', но разрешим использовать все рациональные числа. Тогда множество чисел, которые можно получить на калькуляторе, не изменится.

(b) **Лемма о калькуляторе.** Для $F\subset\mathbb{C}$, $r\in\mathbb{C}$ и $r^2\in F$ обозначим $F[r]:=\{a_0+a_1r\mid a_0,a_1\in F\}$.

Число x построимо тогда и только тогда, когда существуют такие $r_1,\dots r_{s-1}\in\mathbb{C}$, что

$$\mathbb{Q}=F_1\subset F_2\subset F_3\subset\ldots\subset F_{s-1}\subset F_s\ni x,\quad\text{где}\quad r_k^2\in F_k,\quad r_k\notin F_k\quad\text{и}\quad F_{k+1}=F_k[r_k]$$

для любого $k=1,\dots,s-1$.

(Такая последовательность называется *башней квадратичных расширений*. Доказательство невозможности, основанное на рассмотрении аналогичных цепочек-башен, называется в математической логике и программировании *индукцией по глубине формулы*.)

(c) Некоторый (или, эквивалентно, каждый) корень кубического многочлена построим тогда и только тогда, когда один из корней этого многочлена рационален.

(d)* Некоторый (или, эквивалентно, каждый) корень многочлена 4-й степени построим тогда и только тогда, когда его *кубическая резольвента* (§2.2) имеет рациональный корень.

4.4 К доказательству непостроимости в теореме Гаусса

Здесь развиваются идеи из §4.3.

4.13. Найдите неприводимый над $\mathbb{Q}$ многочлен, корнем которого является число

(a) $\sqrt{2}+\sqrt{3}$; (b) $\sqrt{2}+\sqrt{3}+\sqrt{5}$; (c) $\sqrt{2+\sqrt{3}}$; (d) $\sqrt{5+\sqrt{6}}$; (e) $\sqrt{5+\sqrt{1+\sqrt{3}}}$.

4.14. (a) Если неприводимый над $\mathbb{Q}[\sqrt{2}] := \{x+y\sqrt{2} \ : \ x,y\in\mathbb{Q}\}$ многочлен P имеет корень вида $a+\sqrt{b}$, где $a,b\in\mathbb{Q}[\sqrt{2}]$, то $\deg P\in\{1,2\}$.

(b) Если неприводимый над $\mathbb{Q}$ многочлен P имеет корень вида $a+\sqrt{b}+\sqrt{c}$, где $a,b,c\in\mathbb{Q}$, то $\deg P\in\{1,2,4\}$.

(c) Если неприводимый над $\mathbb{Q}$ многочлен P имеет корень вида $\sqrt{a}+\sqrt{b+\sqrt{c}}$, где $a,b,c\in\mathbb{Q}$, то $\deg P\in\{1,2,4,8\}$.

(d) Если неприводимый над $\mathbb{Q}$ многочлен P имеет построимый корень, то $\deg P$ есть степень двойки.

4.15. Найдите неприводимый над $\mathbb{Q}$ многочлен, корнем которого является число

(5) ε_5; (7) ε_7; (9) ε_9; (11) ε_{11}; (13) ε_{13}; (25) ε_{25}.

4.16. (a) *Лемма Гаусса.* Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$.

(b) *Признак Эйзенштейна.* Пусть p простое. Если для многочлена с целыми коэффициентами старший коэффициент не делится на p, остальные делятся на p, а свободный член не делится на p^2, то этот многочлен неприводим над $\mathbb{Z}$.

4.17. Докажите непостроимость в теореме Гаусса.

4.5 Одно извлечение корня третьей степени

Здесь развиваются идеи из §4.1 (но в другом направлении, чем в §§4.2–4.4).

4.18. 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) $\cos(2\pi/9)$; (c) $\sqrt[5]{3}$; (d) $\sqrt[3]{3}$.

(e) наименьший положительный корень уравнения $x^3-4x+2=0$.

(f)* единственный вещественный корень уравнения $x^3-6x-6=0$.

(g)* единственный вещественный корень уравнения $x^3-9x-12=0$.

4.19. Пусть $\varepsilon := \varepsilon_3 = \cos\dfrac{2\pi}{3}+i\sin\dfrac{2\pi}{3}$, $r\in\mathbb{R}-\mathbb{Q}$ и $r^3,a,b,c\in\mathbb{Q}$.

(a) **Лемма о сопряжении.** Если многочлен имеет корень $a+br+cr^2$, то корнями этого многочлена являются также числа $a+b\varepsilon r+c\varepsilon^2 r^2$ и $a+b\varepsilon^2 r+c\varepsilon r^2$.

(b) Если $a+br+cr^2=0$, то $a=b=c=0$.

(c) **Лемма о линейной независимости.** Если $k+lr+mr^2=0$ для некоторых $k,l,m\in\mathbb{Q}[\varepsilon] := \{x+y\varepsilon \ : \ x,y\in\mathbb{Q}\}$, то $k=l=m=0$.

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

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

4.6 Одно извлечение корня простой степени

Здесь развиваются идеи из §4.5.

4.22. Представимо ли следующее число в виде $a_0+a_1\sqrt[7]{2}+a_2\sqrt[7]{2^2}+\dots+a_6\sqrt[7]{2^6}$, где $a_0,a_1,a_2,\dots,a_6\in\mathbb{Q}$?

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

(e) наименьший положительный корень уравнения x^7-4x+2.

4.23. Пусть q нечетное простое, $\varepsilon_q := \cos\dfrac{2\pi}{q}+i\sin\dfrac{2\pi}{q}$, A — многочлен степени меньше q, $r\in\mathbb{R}-\mathbb{Q}$ и $r^q\in\mathbb{Q}$.

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

(b) **Слабая лемма о линейной независимости.** Если $A(r) = 0$, то $A = 0$.

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

(d) **Лемма о неприводимости.** Многочлен $x^q - r^q$ неприводим над

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

(e) **Лемма о линейной независимости.** Если $B \in \mathbb{Q}[\varepsilon_q][x]$ — многочлен степени меньше q с коэффициентами в $\mathbb{Q}[\varepsilon_q]$ и $B(r) = 0$, то $B = 0$.

Следующее утверждение интересно и нетривиально даже для многочленов третьей степени.

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

(a) $r \in \mathbb{R}$, причем $r^q \in \mathbb{Q}$. (b) $r \in \mathbb{C}$, причем $r^q \in \mathbb{Q}$ и $r^q \neq b^q$ ни для какого $b \in \mathbb{Q}$.

4.25. 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 $A(r)$ для некоторых $r \in K$, $q \in \mathbb{Z}$ и $A \in \mathbb{Q}[x]$, причем $r^q \in \mathbb{Q}$.

Из утверждения 4.24 и леммы 4.25 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 сильной вещественной теоремой о неразрешимости из §5.5.

4.7 Несколько извлечений корней

Здесь развиваются идеи из §4.6 и §4.3.

4.26. (a-e) Докажите аналоги утверждений задачи 4.23 с заменой $\mathbb{Q}$ на произвольное подмножество $F \subset \mathbb{R}$, замкнутое относительно операций сложения, вычитания, умножения и деления на ненулевое число (и многочленов с коэффициентами в $\mathbb{Q}$ на многочлены с коэффициентами в F).

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

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

Если следующие задачи не получаются, к их решению можно вернуться после §5.

4.28. (a) Один корень (или, эквивалентно, каждый корень) кубического многочлена можно получить на вещественном калькуляторе тогда и только тогда, когда этот многочлен имеет либо хотя бы один рациональный корень, либо ровно один вещественный корень.

(b)* *Гипотеза.* Каждый корень неприводимого многочлена четвертой степени можно получить на вещественном калькуляторе тогда и только тогда, когда хотя бы один корень его кубической резольвенты можно получить на вещественном калькуляторе.

4.8 Дополнительные задачи

4.29. Для каких n число $\cos(2\pi/n)$

(a) рационально?

(b)* представимо в виде $a + \sqrt{b}$, где $a, b \in \mathbb{Q}$?

(c)* можно получить на вещественном калькуляторе?

4.30. Лемма о рациональности. (a) Пусть $\varepsilon := \varepsilon_3$, $r \in \mathbb{R} - \mathbb{Q}$ и $r^3, a, b, c \in \mathbb{Q}$. Кубический многочлен с корнями

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

и коэффициентом 1 при x^3 имеет рациональные коэффициенты.

(b) Пусть q нечетное простое, A — многочлен степени меньше q, $r \in \mathbb{R} - \mathbb{Q}$ и $r^q \in \mathbb{Q}$. Тогда многочлен $(x - A(r))(x - A(r\varepsilon_q)) \dots (x - A(r\varepsilon_q^{q-1}))$ имеет рациональные коэффициенты.

4.31. (3R) 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 $r \in \mathbb{R}$?

(3C) То же для $r \in \mathbb{C}$.

(3CC) То же для $a, b, c, r^3 \in \mathbb{Q}[i]$ и $r \in \mathbb{C}$.

(3Rn), (3Cn), Те же вопросы для корня вида $a_0 + a_1 r + a_2 r^2 + \dots + a_{n-1} r^{n-1}$, где $n \in \mathbb{Z}$, $n \geq 1$, $a_0, a_1, \dots, a_{n-1}, r^n \in \mathbb{Q}$ и $r \in \mathbb{R}$. (Иными словами, как по многочлену третьей степени узнать, имеет ли он корень, который можно получить на вещественном/комплексном калькуляторе так, чтобы извлечение корня происходило только один раз?)

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

4.32. * Пусть $F \in \{\mathbb{R}, \mathbb{C}\}$. Как по многочлену четвертой степени узнать, имеет ли он

(2R), (2C) корень, который можно получить на F-калькуляторе, но чтобы извлечение корня происходило только два раза, причем оба раза простой степени?

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

4.33. (a) Если многочлен простой степени p неприводим над $\mathbb{Q}[\varepsilon_5]$ и приводим над

$$\mathbb{Q}[\varepsilon_5, \sqrt[5]{2}] := \{a_0 + a_1\sqrt[5]{2} + a_2\sqrt[5]{2^2} + a_3\sqrt[5]{2^3} + a_4\sqrt[5]{2^4} \mid a_0, \dots, a_4 \in \mathbb{Q}[\varepsilon_5]\},$$

то $p = 5$ и многочлен имеет корень в $\mathbb{Q}[\varepsilon_5, \sqrt[5]{2}]$.

(b) Если многочлен простой степени p неприводим над $\mathbb{Q}$ и приводим над $\mathbb{Q}[\sqrt[5]{2}]$, то $p = 5$ и многочлен имеет корень в $\mathbb{Q}[\varepsilon_5, \sqrt[5]{2}]$.

(c) Существуют ли целое a, простое q и многочлен простой степени p, неприводимый над $\mathbb{Q}$ и приводимый над $\mathbb{Q}[\sqrt[q]{a}]$, не имеющий корня в $\mathbb{Q}[\sqrt[q]{a}]$?

4.9 Указания и решения к некоторым задачам из §4

Одно извлечение квадратного корня

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

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

(b) $\sqrt[3]{\sqrt{5} + 2} - \sqrt[3]{\sqrt{5} - 2} = 1$. См. задачу 2.5.a и указание к ней.

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

(e) 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 4.3.c.

Еще один способ. Пусть можно. Тогда

$$1 = 1,$$

$$\sqrt[3]{2} = a + b\sqrt{2},$$

$$\sqrt[3]{4} = a' + b'\sqrt{2}$$

для некоторых рациональных чисел a, b, a', b'. Векторы $(1, 0), (a, b), (a', b')$ на плоскости линейно зависимы с рациональными коэффициентами, т.е. существуют $\lambda_0, \lambda_1, \lambda_2$, не все

равные нулю, для которых $\lambda_0(1,0)+\lambda_1(a,b)+\lambda_2(a',b')=0$. Тогда $\lambda_0+\lambda_1\sqrt[3]{2}+\lambda_2\sqrt[3]{4}=0$. Противоречие с леммой о линейной независимости (задача 4.19.b).

(f) 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 (4.3.a) 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.

Другой способ — аналогично (e) и 4.5.b.

(g) Из задачи 4.2 аналогично решению пункта (f) 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 4.3.c.

(h) (И. Брауде-Золотарев) Из равенства $1+\varepsilon_7+\varepsilon_7^2+\cdots+\varepsilon_7^6=0$ получаем $\cos(2\pi/7)+\cos(4\pi/7)+\cos(6\pi/7)=-1/2$. Используя формулы для $\cos 2\alpha$ и $\cos 3\alpha$, получаем, что число $\cos(2\pi/7)$ является корнем уравнения $8t^3+4t^2-4t-1=0$. Заменим $u=2t$, получим $u^3+u^2-2u-1=0$. Это уравнение не имеет рациональных корней. Значит, уравнение $8t^3+4t^2-4t-1=0$ тоже. Поэтому многочлен $8t^3+4t^2-4t-1=0$ неприводим над $\mathbb{Q}$. Значит, по задаче 4.3 получаем утверждение задачи.

Указание к другому решению. Докажите, что ε_7 невозможно получить на калькуляторе так, чтобы корень извлекался только квадратный и только 3 раза. Ср. с задачами 4.10 и 4.11.d.

4.2. Выразите $\cos 3\alpha$ через $\cos\alpha$.

4.3. (a) *Первое решение.* Обозначим через P данный многочлен. Поделим $P(a+bt)$ на t^2-2 с остатком: $P(a+bt)=(t^2-2)Q(t)+mt+n$. [9] Подставляя $r=\sqrt{2}$, получаем $m\sqrt{2}+n=0$. По лемме о линейной независимости (b) $m=n=0$. Подставляя $r=-\sqrt{2}$, получаем $P(a-b\sqrt{2})=0$.

Второе решение. Ввиду возможности делить с остатком на $(x-a)^2-2b^2$ утверждение достаточно доказать для многочленов первой степени. Ввиду иррациональности числа $\sqrt{2}$ если $a+b\sqrt{2}$ является корнем многочлена первой степени, то этот многочлен нулевой. Значит, число $a-b\sqrt{2}$ также является его корнем.

(c) *Первое решение.* Аналогично *еще одному способу* решения задачи 4.1.e.

Второе решение. Если $\sqrt{b}\in\mathbb{Q}$, то утверждение очевидно. Пусть $\sqrt{b}\notin\mathbb{Q}$. Поделим данный многочлен с остатком на $(x-a)^2-2b^2$. В остатке получится многочлен первой степени, имеющий корень $a+\sqrt{b}$. Так как $\sqrt{b}\notin\mathbb{Q}$, то остаток нулевой. Поэтому данный многочлен делится на $(x-a)^2-b$. Противоречие с его неприводимостью над $\mathbb{Q}$.

4.4. 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 $(a+b\sqrt{c})(a-b\sqrt{c})=a^2-b^2c$.

Одно извлечение корня четвертой степени

4.5. Нельзя.

(a) *Первое решение.* Пусть можно. По леммам о сопряжении и о линейной независимости (4.6.a и 4.7.a) многочлен x^3-3 имеет два различных вещественных корня. Противоречие.

[9] Следующая интерпретация этого деления с остатком может оказаться интересной: подставим $x=a+bt$ в многочлен P и раскроем скобки, заменяя всюду t^2 на 2, получим $mt+n$.

Второе решение. Пусть можно. По леммам о сопряжении и о линейной независимости (4.6.b и 4.7.b) многочлен x^3-3 имеет четыре различных корня. Противоречие.

(b) *Первое решение.* Аналогично *еще одному способу* решения задачи 4.1.e.

Второе решение. Пусть можно. По леммам о сопряжении и о линейной независимости (4.6.a и 4.7.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 числа d.

Третье решение. Пусть можно. По лемме о сопряжении (4.6.b) многочлен x^6-3 имеет четыре различных корня x_1,x_2,x_3,x_4, указанные в 4.6.b. Так как ни один из них не рационален, то $b=c=d=0$ невозможно. Значит, по лемме о линейной независимости (4.7.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; ср. с задачей 4.30). Противоречие с неприводимостью многочлена x^6-3 над $\mathbb{Q}$.

(c) Аналогично первому решению пункта (b).

4.6. (a) Подставим в многочлен $x=a+bt+ct^2+dt^3$ и поделим с остатком на t^4-2. Подставляя $t=\sqrt[4]{2}$, получаем по лемме о линейной независимости (4.7.b), что остаток нулевой. Значит, если $r^4=2$, то $a+br+cr^2+dr^3$ есть корень исходного многочлена.

4.7. (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 $-\sqrt[4]{2}=\dfrac{a+c\sqrt{2}}{b+d\sqrt{2}}=A+B\sqrt{2}$ 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.

(b) Докажите отдельно для вещественной и мнимой части.

4.8. Аналогично задаче 4.5. Отдельно рассматривается более простой случай $r^2\in\mathbb{Q}$.

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

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

Несколько извлечений квадратных корней

4.10. 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 4.1.e. Ср. с задачей 4.7.a.

4.11. (a) Предположим, что $\sqrt[3]{2}$ вещественно построимо. Тогда существует такая башня квадратичных расширений

$$\mathbb{Q}=F_1\subset F_2\subset F_3\subset\ldots\subset F_{s-1}\subset F_s\subset\mathbb{R}, \quad \text{что} \quad \sqrt[3]{2}\in F_r\setminus F_{r-1}.$$

Поскольку $\sqrt[3]{2}\notin\mathbb{Q}$, то $r\geq 3$. Значит,

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

Отсюда

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

Поскольку $2 \in \mathbb{Q} \subset F_{r-1}$, то $2-u \in F_{r-1}$. Так как

$$v\sqrt{a} = 2-u \quad \text{и} \quad v \in F_{r-1}, \quad \text{то} \quad 0 = v = 3\alpha^2\beta + \beta^3 a.$$

Так как $3\alpha^2 + \beta^2 a > 0$, получаем $\beta = 0$ — противоречие!

(b,c) Следует из 4.12.c.

(d) Обозначим $\varepsilon := \varepsilon_7$. Так как $\varepsilon \neq 1$, то число ε удовлетворяет уравнению 6-ой степени $\varepsilon^6+\varepsilon^5+\varepsilon^4+\varepsilon^3+\varepsilon^2+\varepsilon+1=0$. Разделим обе части уравнения на ε^3. Положим

$$f := \varepsilon + \varepsilon^{-1}, \quad \text{тогда} \quad \varepsilon^2+\varepsilon^{-2} = f^2-2 \quad \text{и} \quad \varepsilon^3+\varepsilon^{-3} = f(\varepsilon^2+\varepsilon^{-2}-1).$$

$$\text{Получим} \quad f(f^2-3)+(f^2-2)+f+1=0, \quad \text{то есть} \quad f^3+f^2-2f-1=0.$$

Кандидаты на рациональные корни этого уравнения $f = \pm 1$ отвергаются проверкой. Значит, по теореме о кубических уравнениях (4.12.c) число $f = \varepsilon + \varepsilon^{-1}$ не построимо. Поэтому и ε не построимо (поясните).

4.12. (a) Следует из (b).

(b) Это утверждение легко доказывается индукцией по количеству операций калькулятора, необходимых для получения числа, с применением домножения на сопряженное.

(c) Часть «тогда» очевидна. Чтобы доказать часть «только тогда», предположим, что хотя бы один из корней построим. Для каждого из построимых корней z рассмотрим минимальную цепочку расширений

$$\mathbb{Q} = Q_1 \subset Q_2 \subset Q_3 \subset \ldots \subset Q_{r-1} \subset Q_r, \quad \text{для которой} \quad z_1 \in Q_r \setminus Q_{r-1}.$$

Возьмем корень $z = z_1$ с наименьшей длиной l минимальной цепочки.

Если кубическое уравнение не имеет рациональных корней, то $l \geq 2$. Значит,

$$z_1 = \alpha + \beta\sqrt{a}, \quad \text{где} \quad \alpha, \beta \in Q_{l-1}, \quad \sqrt{a} \notin Q_{l-1} \qquad \text{и} \quad \beta \neq 0.$$

Тогда по аналогу леммы о сопряжении $z_2 := \overline{z}_1 = \alpha - \beta\sqrt{a}$ также является корнем уравнения. Поскольку

$$\beta \neq 0, \quad \text{то} \quad \alpha - \beta\sqrt{a} \neq \alpha + \beta\sqrt{a}, \quad \text{т. е.} \quad z_2 \neq z_1.$$

Обозначим z_3 третий корень уравнения (возможно, $z_3 \in \{z_1, z_2\}$). По формуле Виета

$$z_1+z_2+z_3 = (\alpha+\beta\sqrt{a})+(\alpha-\beta\sqrt{a})+z_3 = 2\alpha+z_3 \in \mathbb{Q}, \quad \text{поэтому} \quad z_3 \in Q_{l-1}.$$

Следовательно, для корня z_3 существует цепочка меньшей длины, чем для z_1. Противоречие. QED

К доказательству непостроимости в теореме Гаусса

4.13. Ответы (для старших коэффициентов 1):

(a) $P(x) := ((x-\sqrt{3})^2-2)((x+\sqrt{3})^2-2) = (x^2-5)^2-24$;

(b) $P(x-\sqrt{5})P(x+\sqrt{5})$; (d) $(x^2-1)^2-3$; (e) $((x^2-5)^2-1)^2-3$.

(a) Для доказательства неприводимости примените лемму о сопряжении и получите, что каждое из 4 чисел $\pm\sqrt{2} \pm \sqrt{3}$ является корнем нужного многочлена.

(b) Аналогично (a).

(c) $\sqrt{2+\sqrt{3}} = \frac{1+\sqrt{3}}{\sqrt{2}}$.

(d) Аналогично (a) неприводимый многочлен с коэффициентами в $\mathbb{Q}[\sqrt{3}]$ и корнем $\sqrt{1+\sqrt{3}}$ (и старшим коэффициентом 1) равен $x^2-2-\sqrt{3}$. Значит, любой неприводимый многочлен P с коэффициентами в $\mathbb{Q}$ и корнем $\sqrt{1+\sqrt{3}}$ делится на $x^2-2-\sqrt{3}$. Применяя сопряжение относительно $\mathbb{Q} \subset \mathbb{Q}[\sqrt{3}]$ получаем, что P делится и на $x^2-2+\sqrt{3}$. Так как многочлены $x^2-2-\sqrt{3}$ и $x^2-2+\sqrt{3}$ взаимно просты, то P делится на их произведение.

(e) Аналогично (d).

4.14. Аналогично 4.13.de. См. подробности в доказательстве непостроимости в теореме Гаусса в §5.2.

4.15. Ответы (для старших коэффициентов 1): (5) $x^4+x^3+x^2+x+1$; (7) $x^6+x^5+\cdots+x+1$; (9) x^6+x^3+1; (11) $x^{10}+x^9+\cdots+x+1$; (25) $x^{20}+x^{15}+x^{10}+x^5+1$.

(5) Для доказательства неприводимости примените признак Эйзенштейна к многочлену $\Phi(x+1)=((x+1)^5-1)/x$ и лемму Гаусса.

Одно извлечение корня третьей степени

4.18. Нельзя.

(a) *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. с задачей 4.19.b). Поэтому $b^3=-2abc=2c^3$. Тогда либо $b=c=0$, либо $\sqrt[3]{2}=b/c$. Оба случая невозможны.

Для остальных решений задачи 4.18 обозначим $r=\sqrt[3]{2}$ и обозначим через $x_1,x_2,x_3\in\mathbb{C}$ числа, заданные формулами (*), где $a,b,c\in\mathbb{Q}$.

Второе решение. Пусть можно. По лемме о сопряжении (4.19.a) многочлен x^2-3 имеет три корня x_1,x_2,x_3. Так как ни один из них не рационален, то $b=c=0$ невозможно. Значит, по лемме о линейной независимости (4.3.c) эти корни различны. Противоречие.

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

Первое завершение решения. По лемме о сопряжении (4.19.a) многочлен $8x^3-6x-1$ имеет корень $a+br\varepsilon+cr^2\varepsilon^2$. Так как он вещественный, то его мнимая часть равна нулю. Значит, $br-cr^2=0$. Так как $r\notin\mathbb{Q}$, то $b=c=0$. Противоречие с отсутствием рациональных корней у многочлена $8x^3-6x-1$.

Второе завершение решения. По лемме о сопряжении (4.19.a) многочлен $8x^3-6x-1$ имеет три корня x_1,x_2,x_3. Так как ни один из них не рационален, то $b=c=0$ невозможно. Значит, по лемме о линейной независимости (4.19.c) эти корни различны. Заметим, что $\overline{\varepsilon^k}=\varepsilon^{-k}$. Поэтому числа $a+br\varepsilon+cr^2\varepsilon^2$ и $a+br\varepsilon^2+cr^2\varepsilon$ комплексно сопряжены. Значит, они не могут быть вещественными и различными.

(c) *Первое решение.* Пусть можно. Обозначим $r:=\sqrt[5]{3}$. Разложим числа r^k по степеням числа $\sqrt[3]{2}$:

$$r^k=a_k+b_k\sqrt[3]{2}+c_k\sqrt[3]{4},\qquad 0\le k\le 3.$$

Получим таблицу размера 4×3 из рациональных чисел. При помощи прибавления к одной строке другой, умноженной на рациональное число, можно получить таблицу с нулевой строкой. Значит, имеется многочлен степени меньше 4 с корнем r. Противоречие с неприводимостью многочлена x^5-3 над $\mathbb{Q}$.

Второе решение. Пусть можно. По лемме о сопряжении (4.19.a) многочлен x^5-3 имеет три корня x_1,x_2,x_3. Так как ни один из корней не рационален, то $b=c=0$ невозможно. Значит, по лемме о линейной независимости (4.19.c) эти корни различны. Поэтому многочлен x^5-3 делится на $(x-x_1)(x-x_2)(x-x_3)$. По лемме о рациональности (4.30) многочлен
$(x-x_1)(x-x_2)(x-x_3)$ имеет рациональные коэффициенты. Противоречие с неприводимостью многочлена x^5-3 над $\mathbb{Q}$.

(d) Аналогично (a), (b) получаем, что комплексные корни многочлена x^3-3 есть числа x_1,x_2,x_3. Поэтому $(a+br+cr^2)\varepsilon^s=a+br\varepsilon+a+br\varepsilon^2$ для некоторого $s\in\{1,2\}$. Отсюда по лемме о линейной независимости (4.19.c) $a=0$ и $bc=0$. Поэтому либо $\sqrt[3]{3}=br$, либо $\sqrt[3]{3}=cr^2$. Противоречие.

(e) Аналогично (b).

(f,g) См. задачу 4.31.3R.

4.19. (a) Аналогично 4.3.a и 4.6. Подставим $a+bt+ct^2$ в многочлен и поделим с остатком на t^3-2. Подставляя $t=\sqrt[3]{2}$, получаем по лемме о линейной независимости (4.19.b), что остаток нулевой. Значит, если $r^3=2$, то $a+br+cr^2$ есть корень исходного многочлена.

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

(c) Докажите отдельно для вещественной и мнимой части.

4.20. Аналогично задачам 4.18.abc.

4.21. 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 — искомый.

Одно извлечение корня простой степени

4.22. Нельзя.

Указание. Используйте сформулированные ниже леммы. Аналогично второму решению задачи 4.18.

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

(a) Пусть можно. Тогда по лемме о сопряжении (4.23.c) многочлен x^2-3 имеет корни $A(r\varepsilon_7^k)$ для $k=0,1,2,\dots,6$. По лемме о линейной независимости (4.23.e) они попарно различны. Противоречие.

(b) Пусть можно. Обозначим через p многочлен, для которого $\cos 7x=p(\cos x)$. Тогда по леммам о сопряжении и о линейной независимости (4.23.c,e) многочлен $2p(x)+1$ имеет попарно различные корни $A(r\varepsilon_7^k)$ для $k=0,1,2,\dots,6$. Но все корни этого многочлена вещественны.

Имеем $\overline{\varepsilon_q^k}=\varepsilon_q^{-k}$. Поэтому для $k>0$ числа $x_k:=A(r\varepsilon_q^k)$ 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.

(c) *Первое решение.* Пусть можно. Обозначим $r:=\sqrt[11]{3}$. Разложим числа r^k по степеням числа $\sqrt[7]{2}$:

$$r^k=\sum_{l=0}^{6}a_{kl}\sqrt[7]{2^l},\qquad 0\le k\le 7.$$

Получим таблицу a_{kl} размера 8×7 из рациональных чисел. При помощи прибавления к одной строке другой, умноженной на рациональное число, можно получить таблицу с нулевой строкой. Значит, имеется многочлен степени меньше 8 с корнем r. Противоречие с неприводимостью многочлена $x^{11}-3$ над $\mathbb{Q}$ (a).

Второе решение. Пусть можно. Тогда по леммам о сопряжении и о линейной независимости (4.23.c,e) многочлен $x^{11}-3$ имеет попарно различные корни $A(r\varepsilon_7^k)$ для $k=0,1,2,\dots,6$. По лемме о рациональности (4.30.b) получаем противоречие с неприводимостью многочлена $x^{11}-3$ над $\mathbb{Q}$ (a).

(d) Аналогично (a), (b) получаем, что комплексные корни многочлена x^7-3 есть $A(r\varepsilon_7^k)$ для $k=0,1,2,\dots,6$. 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 (4.23.e) $a_k=0$ для любого $k\ne s$. Поэтому $\sqrt[7]{3}=a_sr^s$. Противоречие.

(e) Аналогично (b).

4.23. (a) 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 раци онален 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.

(b) Вытекает из (a).

(c) Аналогично задачам 4.3.a, 4.6 и 4.19.a. Используйте слабую лемму о линейной независимости (a).

(d) Пусть приводим. Аналогично доказательству неприводимости над $\mathbb{Q}$ получим $r \in \mathbb{Q}[\varepsilon_q]$. 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:

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

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 $\mathbb{Q}$.

(e) Вытекает из (d).

4.24. *Указание к (a).* Предположим противное. Аналогично 4.22.a,b,c (и утверждению 4.20.a,b) получаем противоречие, используя леммы о сопряженности и о линейной независимости (4.23.c,e).

Решение. (a) Предположим противное. Тогда по леммам о сопряжении и о линейной независимости (4.23.c,e) данный многочлен f имеет попарно различные корни $A(r\varepsilon_q^k)$ для $k = 0, 1, 2, \dots, q-1$. При $q > \deg f$ получаем противоречие. При $q = \deg f$ получаем противоречие аналогично 4.22.b. При $q < \deg f$ получаем противоречие аналогично 4.22.c.

(b) Аналогично (a). Для комплексного случая в леммах нужно использовать, что $r^q \ne b^q$ ни для какого $b \in \mathbb{Q}$. Обозначим $x_k := A(r\varepsilon_q^k)$. 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 $r \in \mathbb{R}$.

4.25. Аналогично задачам 4.21 и 4.9.

Несколько извлечений корней

4.27. (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 $x^5 - 4x - 2$.

Дополнительные задачи

4.29. (a) Ответ: $n \in \{1, 2, 3, 4\}$.

4.30. (a) *Первое решение* получается из тождества 3.6.a подстановкой $x - a, br, cr^2$ вместо a, b, c, соответственно.

Второе решение. И при замене r на $r\varepsilon$, и при замене ε на ε^2 наш многочлен переходит в себя, даже если его рассматривать как многочлен от x, r, ε по модулю $\varepsilon^3 - 1$. Значит, его «коэффициент» при $x^k r^l$ при замене ε на ε^2 переходит в себя. Поэтому «коэффициент» при $x^k r^l$ не зависит от ε и, следовательно, рационален. Далее, его «коэффициент» при x^k при замене r на $r\varepsilon$ переходит в себя. Поэтому каждый «коэффициент» при x^k рационален. (Ввиду рассмотрения многочленов, а не чисел, не нужна даже лемма о линейной независимости.)

Указание к третьему решению. Собирая вместе коэффициенты при одинаковых степенях r, имеем

$$x_1 + x_2 + x_3 = 3a + br(1 + \varepsilon + \varepsilon^2) + cr^2(1 + \varepsilon^2 + \varepsilon) = 3a \in \mathbb{Q},$$

$x_1^2 + x_2^2 + x_3^2 = 3a^2 + 2ab(1+\varepsilon+\varepsilon^2)r + (2ac+b^2)(1+\varepsilon^2+\varepsilon)r^2 + 6bcr^3 + c^2(1+\varepsilon+\varepsilon^2)r^4 = 3a^2 + 6bcr^3 \in \mathbb{Q}$ и $x_1^3 + x_2^3 + x_3^3 = \dots$.

Третье решение. Обозначим эти числа через x_1, x_2, x_3. Ввиду теоремы Виета и формул Ньютона достаточно доказать рациональность чисел $x_1^k + x_2^k + x_3^k$ для $k = 1, 2, 3$. Обозначим $P(t) := a + bt + ct^2$. Тогда $P(t)^k = a_0 + a_1 t + \cdots + a_{2k} t^{2k}$ для некоторых $a_0, a_1, \ldots, a_{2k} \in \mathbb{Q}$ (зависящих только от k, a, b, c). Тогда

$$x_1^k + x_2^k + x_3^k = P(r)^k + P(\varepsilon r)^k + P(\varepsilon^2 r)^k = \sum_{s=0}^{2k} a_s r^s (1 + \varepsilon^s + \varepsilon^{2s}) = 3 \sum_{u=0}^{[2k/3]} a_{3u} r^{3u} \in \mathbb{Q}.$$

(b) Аналогично задаче 4.30, используя то, что при каждой из замен r на $r\varepsilon_q$ и ε_q на ε_q^s, $s = 2, 3, \ldots, q-1$, наш многочлен переходит в себя. Подробности приведены в доказательстве леммы о разложении в §5.3.

4.31. (3R,3C) Ответ: многочлен $x^3 + px + q$ имеет корень указанного вида тогда и только тогда, когда либо многочлен имеет рациональный корень, либо

(3R) $(p/3)^3 + (q/2)^2$ (3C) $|(p/3)^3 + (q/2)^2|$

есть квадрат рационального числа. См. [Ak].

5 Доказательства неразрешимости в радикалах

Для понимания этого параграфа достаточно прочитать §1, а также — для §5.2 лемму 3.4 о комплексификации, а для §5.4 теорему Гаусса 3.8 о понижении. *План доказательства* в каждом пункте получается из текста пункта пропуском доказательств лемм. В §5.5 приводится дополнительный материал.

5.1 Лемма о калькуляторе и понятие поля

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

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

Лемма о калькуляторе. *Пусть $F \in \{\mathbb{R}, \mathbb{C}\}$. Число $x \in F$ можно получить на F-калькуляторе тогда и только тогда, когда существуют такие $r_1, \ldots r_{s-1} \in F$ и $q_1, \ldots q_{s-1} \in \mathbb{Z}$, что $q_k \geq 2$,*

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

для любого $k = 1, \ldots, s-1$.

Такая последовательность называется *башней расширений.*

В этой брошюре *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 другой объект). Это понятие полезно для нас тем, что теорема о делении с остатком и ее следствия верны для многочленов с коэффициентами в поле.

Если F поле, q простое и $r \notin F$, то многочлен $t^q - r^q$ неприводим над F (аналогично слабой лемме о линейной независимости 4.23.a, ср. с задачей 4.26). Тогда $F[r]$ поле.

Напомним, что

$$\varepsilon_n := \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}.$$

5.2 Доказательство непостроимости в теореме Гаусса

Так как $\varepsilon_n = \varepsilon_{nk}^k$, то из построимости числа ε_{nk} вытекает построимость числа ε_n. Поэтому и по лемме 3.4 о комплексификации для доказательства вещественной непостроимости в теореме Гаусса достаточно показать, что ε_n непостроимо для

(A) n простого, не представимого в виде $2^m + 1$,

(B) $n = p^2$ квадрата простого.

Лемма о степенях двойки. *Если неприводимый над $\mathbb{Q}$ многочлен P с рациональными коэффициентами имеет построимый корень, то* $\deg P$ *есть степень двойки.*

Эта лемма доказана далее.

Непостроимость числа ε_n следует из леммы о калькуляторе и леммы о степенях двойки для корня ε_n многочлена

- $P(x) := x^{n-1} + x^{n-2} + \cdots + x + 1$ в случае (A) и
- $P(x) := x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1$ в случае (B).

Неприводимость этих многочленов $P(x)$ над $\mathbb{Z}$ вытекает из неприводимости многочленов $P(x+1)$ над $\mathbb{Z}$. Последняя неприводимость доказывается применением следующего *признака Эйзенштейна*:

Пусть p простое. Если для многочлена с целыми коэффициентами старший коэффициент не делится на p, остальные делятся на p, а свободный член не делится на p^2, то этот многочлен неприводим над $\mathbb{Z}$.

Условие этого признака легко проверяется с помощью сравнения $(a+b)^p \equiv a^p + b^p \mod p$.

Неприводимость над $\mathbb{Q}$ вытекает из неприводимости над $\mathbb{Z}$ и следующей леммы Гаусса:

Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$.

И признак Эйзенштейна, и лемма Гаусса легко доказываются переходом к многочленам с коэффициентами $\mathbb{Z}_p$ (для леммы Гаусса рассмотрим разложение $P = P_1P_2$ данного полинома P над $\mathbb{Q}$, возьмем целые n_1 и n_2 такие, что и n_1P_1, и n_2P_2, имеют целые коэффициеты, и возьмем простой делитель p числа n_1n_2).

Лемма о сопряжении. *Пусть $F \subset \mathbb{C}$ — поле, $r \in \mathbb{C} - F$ и $r^2 \in F$. Определим отображение сопряжения $\bar{\cdot} : F[r] \to F[r]$ формулой $\overline{x+yr} := x - yr$. Это отображение корректно определено,*

$$\overline{z+w} = \overline{z} + \overline{w}, \quad \overline{zw} = \overline{z} \cdot \overline{w} \quad \text{and} \quad \overline{z} = z \Leftrightarrow z = x + 0r \in F.$$

Лемма о степенях двойки является случаем $k = 1$ следующего утверждения.

Обобщенная лемма о степенях двойки. *Если*

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset \ldots \subset F_{s-1} \subset F_s \ni \alpha, \quad \text{где} \quad r_k^2 \in F_k, \quad r_k \notin F_k \quad \text{и} \quad F_{k+1} = F_k[r_k]$$

для любого $k = 1, \ldots, s-1$, то для каждого $k = 1, 2, \ldots, s$ степень любого неприводимого над F_k многочлена с коэффициентами из F_k и корнем α есть степень двойки.

Доказательство. Индукция по k вниз. База $k = s$ очевидна. Докажем шаг. Обозначим через P_k любой неприводимый над F_k многочлен с коэффициентами из F_k и корнем α. Будем рассматривать делимость и НОД в F_{k+1}. Так как $P_k(\alpha) = 0$, то P_k делится на P_{k+1}. По лемме о сопряжении для $F = F_k$ и $F[r] = F_{k+1}$ имеем $P_k = \overline{P_k}$ делится на $\overline{P_{k+1}}$. Обозначим $D := GCD(P_{k+1}, \overline{P_{k+1}})$. Так как P_{k+1} неприводим над F_{k+1} и делится на D, то либо $D = 1$, либо $P_{k+1} = D$.

Во втором случае так как $\overline{D} = D$, то $P_{k+1} = D \in F_k[x]$. Значит, $P_k = P_{k+1}$ и шаг индукции доказан.

В первом случае P_k делится на $M := P_{k+1}\overline{P_{k+1}}$. Так как $\overline{M} = M$, то $M \in F_k[x]$. Так как P_k неприводим над F_k, то $P_k = M$. Значит, $\deg P_k = 2 \deg P_{k+1}$ есть степень двойки по предположению индукции. QED

5.3 Доказательство неразрешимости в вещественных радикалах

Основная Лемма (вещественный случай). *Пусть q простое, $F \subset \mathbb{R}$ поле, $r \in \mathbb{R} - F$ и $r^q \in F$.*

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

(b) (сопряжение) Если $P \in F[\varepsilon_q][t]$ и $P(r) = 0$, то $P(r\varepsilon_q^k) = 0$ для любого $k = 0, 1, \ldots, q-1$.

Доказательство части (a). Оба многочлена P и $t^q - r^q$ с коэффициентами из $F[\varepsilon_q]$ имеют корень r. Значит, их НОД имеет корень r и степень k, $0 < k \leq \deg P < q$. Все корни многочлена $t^q - r^q$ есть $r, r\varepsilon_q, r\varepsilon_q^2, \ldots, r\varepsilon_q^{q-1}$. Свободный член НОД'а равен произведению некоторых k из этих корней. Тогда $r^k \in F[\varepsilon_q]$. Так как q простое, то $kx + qy = 1$ для некоторых целых x, y. Тогда $r = (r^k)^x (r^q)^y \in F[\varepsilon_q]$. [10]

Поэтому $r^2, r^3, \ldots, r^{q-1} \in F[\varepsilon_q]$. Составим таблицу $a_{kl} \in F$ размера $q \times (q-1)$ из разложений чисел r^k по степеням числа ε_q:

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

При помощи нескольких операций прибавления к одной строке другой, умноженной на число из F, можно получить таблицу с нулевой строкой.

Значит, имеется ненулевой многочлен P_1 степени меньше q с коэффициентами из F и корнем r. Дальнейшие рассуждения аналогичны первому абзацу. Нужно только заменить P на P_1 и $F[\varepsilon_q]$ на F. Получаем $r \in F$ — противоречие. QED

Доказательство части (b). Так как $P(r) = 0$, то остаток от деления многочлена $P(t)$ на $t^q - r^q$ принимает значение 0 в точке r. Значит, по (a) этот остаток равен нулю. Отсюда вытекает заключение части (b). QED

Доказательство теоремы о неразрешимости в вещественных радикалах. Предположим, напротив, что некоторый корень x_0 уравнения $8x^3 - 6x + 1 = 0$ можно получить на вещественном калькуляторе. Тогда по лемме о калькуляторе для $F = \mathbb{R}$ существует наименьшее s, для которого найдется башня расширений, последнее поле F_s которой содержит некоторый корень x_1 уравнения $8x^3 - 6x + 1 = 0$ (возможно, $x_1 \neq x_0$). Обозначим $F := F_{s-1}$, $q := q_{s-1}$ и $r := r_{s-1}$. Тогда $x_1 = h(r)$ для некоторого многочлена h с коэффициентами в F степени больше 0 и меньше q.

Применим основную лемму (вещественный случай) (b) к многочлену $P(t) := 8h(t)^3 - 6h(t) + 1$. Так как $8h(r)^3 - 6h(r) + 1 = 0$, получим, что $h(r\varepsilon_q^k)$ является корнем уравнения $8x^3 - 6x + 1 = 0$ для любого $k = 0, 1, \ldots, q-1$. Если $h(r\varepsilon_q^k) = h(r\varepsilon_q^l)$ для некоторых $0 \leq k < l \leq q-1$, то по основной лемме (вещественный случай) (a) получим $\deg h = 0$ — противоречие. Итак, числа $h(r\varepsilon_q^k)$, $0 \leq k \leq q-1$, — попарно различные корни уравнения $8x^3 - 6x + 1 = 0$. Значит, $q = 2$ или $q = 3$.

Если $q = 2$, то по теореме Виета третий корень уравнения $8x^3 - 6x + 1 = 0$ равен $-2h(0) \in F$ — противоречие с минимальностью числа s.

Если $q = 3$, то обозначим $h_0 + h_1 t + h_2 t^2 := h(t)$. Так как

$$h(r\varepsilon_3) \in \{\cos(2\pi/9), \cos(8\pi/9), \cos(14\pi/9)\} \subset \mathbb{R}, \quad \text{то} \quad h_1 r - h_2 r^2 = 0.$$

Так как $r \notin F$, то $h_1 = h_2 = 0$. Противоречие с $\deg h > 0$. [11] QED

5.4 Доказательство неразрешимости в радикалах

Теорема Галуа (о неразрешимости в радикалах) вытекает из следующего результата. Он интересен и нетривиален даже для многочленов пятой степени.

[10] Другая запись следующего абзаца с использованием понятия размерности: тогда $\dim_F F[r] \leq \dim_F F[\varepsilon_q] \leq q-1$.

[11] *Другое завершение доказательства для $q = 3$.* Если $q = 3$, то из $\overline{\varepsilon_3} = \varepsilon_3^2$ вытекает $\overline{h(r\varepsilon_3)} = h(r\varepsilon_3^2)$. Это противоречит вещественности и различности последних двух чисел.

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.*

Из следующих лемм только основная лемма (a,c) и лемма об уплотнении прямо используются в доказательстве теоремы Кронекера. Основная лемма (b) используется только для основной леммы (c) .

Основная лемма (c) показывает, что при некоторых предположениях все корни многочлена $g \in F[x]$ являются значениями в «сопряженных» точках некоторого многочлена из $F[x]$.

Основная Лемма. *Пусть q простое, $F \subset \mathbb{C}$ поле, $r \in \mathbb{C} - F$ и $r^q, \varepsilon_q \in F$.*

(a) (линейная независимость) Если $P(r) = 0$ для некоторого многочлена $P \in F[t]$ степени меньше q, то $P = 0$. [12]

Или, эквивалентно, для любого $\alpha \in F[r]$ существуют единственные $a_0, a_1, \dots, a_{q-1} \in F$, для которых $\alpha = a_0 + a_1 r + a_2 r^2 + \dots + a_{q-1} r^{q-1}$.

(b) (сопряжение) Если $P \in F[x,t]$ и $P(x,r) = 0$ как многочлен от x, то $P(x, r\varepsilon_q^k) = 0$ как многочлен от x для любого $k = 0, 1, \dots, q-1$.

(c) (разложение) Если многочлен g простой степени с коэффициентами в F неприводим над F и приводим над $F[r]$, то $g(x) = A(x - x_0)(x - x_1)\dots(x - x_{q-1})$ для некоторого $A \in F$ и попарно различных значений $x_0, x_1, \dots, x_{q-1}$ некоторого многочлена с коэффициентами из F в точках $r, r\varepsilon_q, \dots, r\varepsilon_q^{q-1}$.

Доказательство части (a). Аналогично первому абзацу доказательства вещественной леммы о линейной независимости, с заменой $F[\varepsilon_q]$ на F. QED

Доказательство части (b). Утверждение части (b) инвариантно относительно деления многочлена P с остатком на $t^q - r^q$. Поэтому можно считать, что $\deg_t P < q$. В этом случае часть (b) получается покоэффициентным применением части (a). QED

Доказательство части (c). По условию существует приведенный неприводимый над $F[r]$ делитель многочлена g в $F[r]$. Этот делитель получается подстановкой $t = r$ в некоторый многочлен $h \in F[x,t]$ степени по t больше 0, а по x меньше $\deg g$. Итак, $h(x,r)$ неприводим над $F[r]$ и $g(x) = h(x,r)h_1(x,r)$ для некоторого многочлена $h_1 \in F[x,t]$. Обозначим $\varepsilon := \varepsilon_q$.

Применим (b) к $P(x,t) := g(x) - h(x,t)h_1(x,t)$. Получим, что $g(x)$ делится на многочлен $h(x, r\varepsilon^k)$ в $F[r]$ для любого $k = 0, 1, \dots, q-1$.

Многочлен $h(x, r\varepsilon^k)$ неприводим над $F[r]$ для любого $k = 0, 1, \dots, q-1$.

(Иначе применим (b) к многочлену P, равному разности $h(x, r\varepsilon^k)$ и его сомножителей. Получим, что многочлен $h(x,r)$ приводим над $F[r]$. Противоречие.)

По (a) многочлены $h(x, r\varepsilon^k)$ различны для различных $k = 0, 1, \dots, q-1$. Значит, g делится на их произведение. По (a) это произведение можно однозначно представить в виде

$$a_0(x) + a_1(x)r + \dots + a_{q-1}(x)r^{q-1} \quad \text{для некоторых} \quad a_k \in F[x].$$

Так как произведение переходит в себя при замене $r \to r\varepsilon$ (которая корректно определена по (a)), то по (a) $a_k(x) = a_k(x)\varepsilon^k \in F[x]$ для любого $k = 1, 2, \dots, q-1$. Отсюда $a_k(x) = 0$ для любого $k = 1, 2, \dots, q-1$. Значит, произведение равно $a_0(x) \in F[x]$.

Из этого и неприводимости g над F следует, что g равно этому произведению. Тогда $\deg g = q \deg_x h$. Так как $\deg g$ простое и $\deg_x h < \deg g$, то $\deg_x h = 1$ (и $\deg g = q$). Значит, $-h(0,r) \in F[r]$ есть корень многочлена g. И остальные его корни есть $-h(0, r\varepsilon^k)$ для $k = 0, 1, \dots, q-1$. QED

[12] Аналог леммы о линейной независимости без условия «$\varepsilon_q \in F$» неверен для $q > 2$, $F = \mathbb{R}$ и $r = \varepsilon_q$. Например, условие «$\varepsilon_q \in F$» пропущено в замечательной книге [P, стр. 580-581]. Поясним это тонкое место более детально. В [P] утверждение «$q = p$» вверху стр. 581 (для $p = 2$) означает следующее: если квадратный трехчлен f неприводим над полем k, содержащим i, и приводим над $k[\sqrt[q]{a}]$ для некоторого $a \in K$ и простого q, то $q = 2$. Это неверно для $f(x) = x^2 + x + 1$, $q = 3$, $a = 1$ и $k = \mathbb{Q}[i]$. Ошибка в доказательстве в [P] — в предыдущем предложении: (верную) теорему 1 на стр. 572 применить нельзя, т.к. возможно $a = b^q$ для некоторого $b \in k$ (хоть $\sqrt[q]{a} \notin k$).

Лемма об уплотнении башни расширений. *Если число можно получить на комплексном калькуляторе, то существует башня расширений из леммы о калькуляторе для $F = \mathbb{C}$, для которой при любом $k = 1, 2, \dots, s-1$ число q_k простое, $\varepsilon_{q_k} \in F_k$ и либо $r_k \in \mathbb{R}$, либо $|r_k|^2 \in F_k$.*

Доказательство. При помощи индукции «вниз» по q покажем, что из произвольной башни расширений можно получить башню расширений, для которой $\varepsilon_{q_k} \in F_k$ при любом $q_k > q$. Тогда при $q = 1$ получим башню расширений, для которой $\varepsilon_{q_k} \in F_k$ при любом $k = 1, 2, \dots, s-1$. База: $q = \max_k q_k$; в этом случае доказывать нечего. Для доказательства шага индукции возьмем наименьшее такое k, что $q_k = q$. Вставим между F_{k-1} и F_k «получение ε_q при помощи корней степени меньше q» из теоремы Гаусса о понижении 3.8. Если такого k нет, то шаг индукции очевиден.

Далее заменим извлечение корня составной степени ab на пару извлечений корней a-й и b-й степеней. Условие $\varepsilon_{q_k} \in F_k$ при любом $k = 1, 2, \dots, s-1$ сохранится, ибо если $\varepsilon_{ab} \in F_k$, то $\varepsilon_a \in F_k$ и $\varepsilon_b \in F_k$.

Назовем башню расширений *интересной*, если при любом $k = 1, 2, \dots, s-1$ число q_k простое и $\varepsilon_{q_k} \in F_k$. При помощи индукции «вниз» по l покажем, что из произвольной интересной башни можно получить интересную башню, для которой при любом $k \leq s-l$

$$\overline{F}_k = F_k \quad \text{и} \quad \text{либо} \quad r_k \in \mathbb{R}, \quad \text{либо} \quad |r_k|^2 \in F_k.$$

Тогда при $l = 0$ получим утверждение леммы. База: $l = s-1$; в этом случае доказывать нечего. Докажем шаг индукции. (Если $r_k \in \mathbb{R}$, то шаг индукции очевиден, но следующее рассуждение тоже проходит.) Так как $F_k = \overline{F_k}$ и $r_k^{q_k} \in F_k$, то $|r_k|^{2q_k} = r_k^{q_k}\overline{r_k^{q_k}} \in F_k$. Поэтому $F_k[|r_k|^2] = F_k[\sqrt[q_k]{|r_k|^{2q_k}}]$, где берется вещественное значение корня. Заменим подбашню

$$F_k \subset F_{k+1} \subset \dots \subset F_s \quad \text{на подбашню} \quad F_k \subset F_k[|r_k|^2] \subset F_k[r_k, \overline{r}_k] = F_{k+1}[\overline{r}_k] \subset \dots \subset F_s[\overline{r}_k].$$

Ясно, что интересность башни сохраняется при этой замене. Далее в новой подбашне из каждого набора совпадающих соседних полей оставляем только одно. После чего пользуемся предположением индукции. QED

Доказательство теоремы Кронекера. Предположим, напротив, что некоторый корень данного многочлена g можно получить на комплексном калькуляторе. Тогда возьмем башню расширений из леммы об уплотнении башни расширений. Так как g неприводим над $\mathbb{Q}$ и приводим над последним полем башни, то существует такое s, что g неприводим над F_s и приводим над F_{s+1}. Обозначим $r := r_s$ и $q := q_s$. По основной лемме (c) $g(x) = A(x - x_0)(x - x_1)\dots(x - x_{q-1})$ для некоторого $A \in F_s$ и различных значений $x_0, x_1, \dots, x_{q-1}$ некоторого многочлена $a_0 + a_1 t + \dots + a_{q-1}t^{q-1}$ с коэффициентами из F_s в точках $r\varepsilon_q^k$, $0 \leq k \leq q-1$. Вещественность числа x_k равносильна тому, что $x_k = \overline{x}_k$. Заметим, что $\overline{\varepsilon_q^k} = \varepsilon_q^{-k}$.

Если $r \in \mathbb{R}$, то по основной лемме (a) для любого $k \in \{0, 1, \dots, q-1\}$ условие $x_k = \overline{x}_k$ равносильно тому, что $a_s\varepsilon^{2sk} = \overline{a}_s$ для любого $s = 0, 1, \dots, q-1$. Следовательно, $x_k \in \mathbb{R}$ не более, чем для одного k.

Если $r \notin \mathbb{R}$, то лемме об уплотнении $|r|^2 \in F_s$. Тогда $\overline{r}^s = \dfrac{|r|^{2s}}{r^q} r^{q-s}$, где $\dfrac{|r|^{2s}}{r^q} \in F_s$. Значит, по основной лемме (a) для любого $k \in \{0, 1, \dots, q-1\}$ условие $x_k = \overline{x}_k$ равносильно тому, что $a_0 = \overline{a}_0$ и $a_s = \overline{a}_{q-s}\dfrac{|r|^{2q-2s}}{r^q}$ для любого $s = 1, 2, \dots, q-1$. Эти равенства не зависят от k. Поэтому если среди чисел $x_0, \dots, x_{q-1}$ есть вещественное, то все они вещественны.

Противоречие. QED

Замечания. Отличие доказательства теоремы Кронекера от доказательства теоремы неразрешимости в вещественных радикалах заключается

• в «комплексификации»: r^q и коэффициенты многочлена h могут быть комплексными.

• в необходимости доказывать наличие корня у многочлена, неприводимого над F_{s-1} и приводимого над F_s. (Если брать наименьшее s такое, что данный многочлен имеет корень в F_s, то нужно доказывать неприводимость над F_{s-1}; это менее удобно.)

Наличие корня — нетривиальная часть основной леммы (c) (разложение из наличия корня вывести легко). Чтобы доказывать основную лемму (c), а не ее усиленную версию из следующего пункта (и, тем самым, обойтись без теоремы о размерности башни) в лемме об уплотнении мы добиваемся условия $\varepsilon_{q_k} \in F_k$. Для сильной теоремы о неразрешимости в вещественных радикалах этот трюк не проходит, поэтому ее доказательство более сложно (в частности, использует теорему о размерности башни).

Два разбираемых случая в конце доказательства теоремы Кронекера немного отличаются от случаев, разобранных в конце доказательства из [T].

В начале 2-й колонки на стр. 14 в [T] фактически используется, что $\rho \in R$. А это неверно без дополнительных стараний типа леммы об уплотнении башни расширений.

5.5 Сильная вещественная теорема о неразрешимости

Вещественный аналог теоремы Кронекера (§5.4) следующий.

Сильная вещественная теорема о неразрешимости. *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.*

Доказательство этой «вещественной» теоремы, к которому мы переходим, *сложнее* доказательства «комплексной» теоремы Кронекера.

Сильная лемма о разложении. *Пусть $F \subset \mathbb{C}$ поле, q простое, $r \in \mathbb{C}$, $r^q \in F$. Если многочлен g простой степени с коэффициентами в F неприводим над F и приводим над $F[r]$, то $g(x) = A(x - x_0)(x - x_1)\dots(x - x_{q-1})$ для некоторого $A \in F$ и попарно различных значений $x_0, x_1, \dots, x_{q-1}$ некоторого многочлена с коэффициентами из $F[\varepsilon_q]$ в точках $r, r\varepsilon_q, \dots, r\varepsilon_q^{q-1}$.*

Лемма интересна даже для $F \subset \mathbb{R}$ и даже для $F = \mathbb{Q}$, хотя неразрешимость за одно извлечение корня доказывается и без нее.

Лемма о потере неприводимости. *Если многочлен g простой степени неприводим над полем F и приводим над $F[\varepsilon_q]$, то $q > \deg g$.*

Доказательство леммы приводится в конце этого пункта.

Доказательство сильной леммы о разложении. Аналогично доказательству основной леммы (c). Везде, кроме последнего абзаца, нужно заменить F на $F[\varepsilon_q]$. Перед последним абзацем нужно ставить следующее: *«Так как g делится на произведение, то $\deg g \geq q$. Из этого и леммы о потере неприводимости следует, что g неприводим над $F[\varepsilon_q]$.»* QED

Доказательство сильной вещественной теоремы о неразрешимости. Аналогично доказательству теоремы Кронекера. Отличие только в том, что вместо леммы об уплотнении мы используем только простоту всех q_k, полагаем $F := F_{s-1}[\varepsilon_q]$, вместо основной леммы (c) используем сильную лемму о разложении и не рассматриваем случай $r \notin \mathbb{R}$. QED

Осталось доказать лемму о потере неприводимости. [13]

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 $l = k_1 l_1 + \dots + k_s l_s$.

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

(b) Если β — корень неприводимого над полем F многочлена g, то $\dim_F F[\beta] = \deg g$.

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

[13] Было бы интересно доказать эту лемму (а значит, и сильную вещественную теорему о неразрешимости) без использования теоремы о размерности башни.

Доказательство леммы о потере неприводимости. Обозначим через $\beta \in \mathbb{C}$ произвольный корень многочлена g. 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 g неприводим над F, то $\dim_F F[\beta] = \deg g$. Так как g приводим над $F[\varepsilon_q]$, то $\dim_{F[\varepsilon_q]} F[\beta, \varepsilon_q] < \deg g$. Так как $\deg g$ простое, то $\dim_F F[\varepsilon_q]$ делится на $\deg g$. Так как $\dim_F F[\varepsilon_q] < q$, то $q > \deg g$. (На самом деле, даже $q - 1 > \deg g$.) QED

Для особо заинтересованного читателя приведем *другое доказательство сильной леммы о разложимости*: она вытекает из леммы о потере неприводимости и следующей леммы.

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

Для доказательства необходима еще одна лемма.

Лемма о симметричности. *Пусть F — поле, g — неприводимый над F многочлен, $x_1, \ldots, x_n$ — все его комплексные корни. Тогда существует автоморфизм поля $F(x_1, \ldots, x_n)$, неподвижный на F и переводящий x_1 в x_2.*

Доказательство. Рассмотрим изоморфизм

$$\psi : F(x_1) \to F[x]/(g) \to F(x_2),$$

переводящий x_1 в x_2. Покажем, как продолжить его до автоморфизма поля $F(x_1, \ldots, x_n)$.

Если $F(x_1)$ содержит все корни многочлена g, то и $F(x_2)$ тоже содержит столько же его корней. Тогда $F(x_1) = F(x_2) = F(x_1, \ldots, x_n)$ и утверждение доказано.

Иначе существует корень β_1 многочлена g, не лежащий в $F(x_1)$. Он — корень какого-то из неприводимых множителей $\widehat{g}$ многочлена g над $F(x_1)$. При автоморфизме ψ этот неприводимый множитель переходит в некоторый неприводимый множитель $\psi(\widehat{g})$ многочлена g над $F(x_2)$. Обозначим через β_2 произвольный комплексный корень многочлена $\psi(\widehat{g})$. (β_2 — тоже корень многочлена g; возможно, $\beta_2 = \beta_1$, но $\beta_2 \neq x_2$.) Тогда ψ продолжается до изоморфизма

$$F(x_1, \beta_1) \to F(x_1)[x]/(\widehat{g}) \to F(x_2)[x]/(\psi(\widehat{g})) \to F(x_2, \beta_2).$$

Итак, мы расширили наш изоморфизм ψ до изоморфизма «бóльших» расширений. Продолжая этот процесс, построим требуемый автоморфизм. QED [14]

Доказательство сильной леммы о наличии корня. Пусть $g = g_1 \ldots g_t$ — разложение g на приведенные неприводимые множители над $F(r, \varepsilon_q)$. По лемме о симметричности существует автоморфизм ϕ поля $F(r, \varepsilon_q, x_1, \ldots, x_n)$, неподвижный на F и переводящий некоторый корень x_1 многочлена g_1 в некоторый корень x_2 многочлена g_2. Так как коэффициенты многочлена g лежат в F, то $\phi(g) = g$. Так как $F(r, \varepsilon_q)$ есть поле разложения многочлена $x^q - r^q$ над F, то $\phi(F(r, \varepsilon_q)) = F(r, \varepsilon_q)$ (заметим, что ϕ не обязан быть тождественным на $F(r, \varepsilon_q)$). Значит, многочлен $\phi(g_1)$ неприводим над $F(r, \varepsilon_q)$. Вместе с $\phi(g_1)(x_2) = 0$ и приведенностью многочленов g_1, g_2 это влечет $\phi(g_1) = g_2$. Поэтому $\deg g_1 = \deg g_2$. Аналогично получаем, что все степени сомножителей $g_1, \ldots, g_t$ равны. Так как $\deg g = t \deg g_1$ простое, то $\deg g_1 = 1$. Значит, g имеет корень в $F(r, \varepsilon_q)$. QED

Еще одно доказательство сильной леммы о наличии корня. Обозначим через p степень данного многочлена, а через $\beta \in \mathbb{C}$ — произвольные его корень. По теореме о размерности башни

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

[14] Аналогично доказывается следующий факт. Пусть $F \subset \mathbb{C}$ — поле, $g \in F[x]$ — неприводимый многочлен, а K — поле разложения какого-то многочлена над F. Тогда все неприводимые множители g над K имеют одинаковую степень.

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, $q = p$.

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 $F[\varepsilon_q]$. Тогда можно заменить F на $F[\varepsilon_q]$ и считать, что $\varepsilon_q \in F$.

Так как $\dim_{F[r]} F[\beta, r] < q = \dim_F F[r] = \dim_F F[\beta]$, то $\dim_{F[\beta]} F[\beta, r] < q$. 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 $\beta \in F[r]$. QED

6 Комментарии

6.1 Исторические комментарии

Доказательство построимости в теореме Гаусса получено из [E1, §24] некоторым упрощением (мы обходим использование леммы 2). Оно также более простое по сравнению с доказательством из [KS]. Элементарное доказательство построимости для $n = 17$ приводится, например, в [BK, Ch, D, §37, Gi, P, Po, PS, Ko] (при этом иногда приводятся явные формулы, как с доказательствами утверждений о знаках перед радикалами [D, §37], [Sa], так и без [BK]). Для общего случая оно намечено в [Ga, Gi], где ясности доказательства немного мешает построение общей теории вместо доказательства конкретного результата. Подход из [K] дает объяснение на вопрос «почему», и было бы интересно довести его до полного доказательства.

Доказательство непостроимости в теореме Гаусса основано на [D, Supplement to §§35-37]. Оно более простое по сравнению с доказательствами из [KS].

Другие изложения приводятся, например, в [B, H, Vi, W].

Доказательство теорем о неразрешимости в вещественных и комплексных радикалах основано на замечательных статье [T] и книгах [D, §25, P, дополнение 8] (впрочем, здесь исправлены неточности, см. §5.4). Другое изложение [Sa1] написано Л. Самойловым по курсу, проведенному совместно с В. Волковым и автором. Оно отлично от доказательства из [A, FT, S]. Почему 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 указывает на простоту доказательства.

6.2 Философско-методические комментарии

По моему мнению, именно с *новых идей*, изложенных на уже имеющемся языке, а не с *введения нового языка*, полезно *начинать* изучение любой теории. Как правило, такие идеи наиболее ярко выражаются доказательствами, подобными приведенным здесь.

При изложении материала нужно ориентироваться на объекты, которые основательнее всего укореняются в человеческой памяти. Это — отнюдь не системы аксиом и не логические приемы в доказательстве теорем. Изящное решение красивой задачи, формулировка которой ясна и доступна, имеет больше шансов удержаться в памяти студента, нежели абстрактная теория. Скажем больше, именно по такому решению, при наличии некоторой математической культуры, студент впоследствии сможет восстановить теоретический материал. Обратное же, как показывает опыт, практически невозможно [Ko, предисловие].

Одним из принципов преподавания является «путь познания должен повторять путь развития». [15]

Такой стиль изложения не только делает материал более доступным, но позволяет сильным студентам (для которых доступно даже абстрактное изложение) приобрести математический вкус и стиль с тем, чтобы

(1) разумно выбирать проблемы для исследования и их мотивировки. [16]

(2) ясно излагать собственные открытия, не скрывая ошибки или известности полученного результата за чрезмерным формализмом. [17]

Мода на искусственно формализованное изложение [18] привела к следующему парадоксу. По данному *известному понятию* высшей математики зачастую непросто восстановить *конкретный красивый результат*, для которого это понятие действительно необходимо (и при получении которого это понятие возникло).

Доказательство с использованием некоторого нового термина имеют свои преимущества: оно подготавливает читателя к доказательству тех теорем, которые уже трудно или невозможно доказать без этого термина. [19] Однако такие доказательства, как правило, не должны быть *первыми* доказательствами данного результата (легко себе представить результат *первого* знакомства с теоремой Пифагора на основе понятий векторного пространства и скалярного умножения). Кроме того, при приведении «терминологического» доказательства полезно оговорить его мотивированность не доказываемым результатом, а обучением полезному новому методу (ср. с (1) выше).

Приведенная выше точка зрения разделяется многими математиками (а некоторыми — нет); я унаследовал ее от Ю. П. Соловьева.

Приводимые порой в качестве *основных* приложений теории Галуа теоремы Гаусса и о неразрешимости уравнений в радикалах неубедительны для мотивировки этой теории (так же, как приложение к решению квадратных уравнений неубедительно для мотивировки общей теории разрешимости уравнений произвольной степени в радикалах). Действительно, эти теоремы имеют элементарное доказательство, не использующее «групп Галуа'. В терминах теории Галуа формулируется общий критерий разрешимости алгебраического уравнения в радикалах. Но этот критерий не дает настоящего решения проблемы разрешимости, а лишь сводит ее к трудной задаче вычисления группы Галуа уравнения. (То, что никакая *другая теория* не дает легкого для применений ответа, не позволяет утверждать, что *теория Галуа* дает такой ответ.) Но, конечно, формулировка общего критерия в адекватных проблеме терминах может иметь важное философское значение.

---

[15] Впрочем, это не всегда применимо. Так, изучение геометрии Лобачевского вовсе не обязательно начинать с попыток доказать Пятый Постулат. Геометрия Лобачевского для нас сейчас важна, в первую очередь, ее приложениями в ТФКП, теории чисел, топологии, теории групп, алгебраической геометрии, космологии и т.д., а вовсе не тем, что она демонстрирует независимость Пятого Постулата от остальных аксиом Евклида. С этой точки зрения более плодотворно ее построение не на основе аксиом Евклида-Гильберта, а на основе понятия группы преобразований (Клейн) или римановой метрики (Риман). Аналогично, изучение теории Галуа вовсе не обязательно начинать с задачи о решении алгебраического уравнения в радикалах или квадратных радикалах. С современной точки зрения теория Галуа есть теория алгебраических расширений полей, составляющая неотъемлемую часть алгебры и имеющая приложения и аналоги в других разделах математики (алгебраическая геометрия, теория накрытий, теория инвариантов), а решение алгебраических уравнений в радикалах — это маргинальная задача. (Э. Б. Винберг).

[16] Математик, понимающий, что теория Галуа мотивируется более важными проблемами, чем построимость правильных многоугольников и разрешимость алгебраических уравнений в радикалах, вряд ли станет мотивировать созданную им теорию приложениями, которые можно получить и без его теории.

[17] К сожалению, такое — обычно 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.

[18] Видимо, общепринятый термин «бурбакизация» не очень удачен ввиду 'масштаба и влияния деятельности Бурбаки, независимо от оценки пользы и вреда разных ее аспектов' (А. Шень).

[19] Например, векторное доказательство теоремы Пифагора уже является достаточным основанием для введения понятий векторного пространства и скалярного умножения, хотя эти понятия и не являются необходимыми для доказательства упомянутой теоремы. (Э. Б. Винберг.)

Однако теория Галуа выходит далеко за рамки проблемы разрешимости уравнений в радикалах. Ее популяризации послужила бы дальнейшая публикация интересных теорем, формулируемых без понятий теории Галуа, но при попытках доказать которые она естественно возникает. Примеры таких теорем мне сообщили А.Я. Белов, С.М. Львовский и Г.Р. Челноков (к сожалению, в доступной мне начальной учебной литературе по теории Галуа мне не удалось найти такие теоремы, формулировка которых не была бы скрыта под толщей обозначений и терминов).

Список литературы

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

[Ak] Д. Ахтямов, Решение кубических уравнений при помощи одного извлечения корня, доклад на ММКШ-2013, http://www.mccme.ru/circles/oim/mmks/works2013/akhtyamov2.pdf

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

[BK] Бурда Ю., Кадец Л. Семнадцатиугольник и закон взаимности Гаусса, Мат. Просвещение, 17 (2013). http://www.mccme.ru/free-books/matprosi.html.

[Ch] Н. Н. Чеботарев, Основы теории Галуа. Часть 1. Л., М.: Гостехиздат, 1934.

[Ch1] Г.Р. Челноков, Основы теории Галуа в интересных задачах, http://www.mccme.ru/circles/oim/materials/grishalois.pdf. (версия 11.11.2010)

[CR] Р. Курант, Дж. Роббинс, Что такое математика. М.: МЦНМО, 2004.

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

[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.

[FT] D. Fuchs, S. Tabachnikov, Mathematical Omnibus. AMS, 2007. Рус. перевод: Табачников С.Л., Фукс Д.Б., Математический дивертисмент, М.: МЦНМО, 2011.

[Ga] К. Ф. Гаусс, Арифметические исследования. Труды по теории чисел. М.: Изд-во АН СССР, 1959. С. 9–580.

[Gi] С. Гиндикин, Дебют Гаусса, Квант, 1972 N1, 2–11.

[Gi1] С. Гиндикин, Великое искусство, Квант, 1976 N9, 2–10.

[H] Ch.R. Hadlock, Field Theory and its Classical Problems, Carus Mathematical Monographs 19, The Mathematical Association of America, 1978.

[K] А.А. Кириллов, О правильных многоугольниках, функции Эйлера и числах Ферма, Квант, 1977 N7, 2–9 или Квант, 1994 N6, 15–18.

[Ki] В.А. Кириченко, Построения циркулем и линейкой и теория Галуа, http://www.mccme.ru//dubna/2005/courses/kirichenko.html

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

[Kh1] А.Г. Хованский, Топологическая теория Галуа, Москва, МЦНМО, 200?

[Kh2] А. Г. Хованский Построения циркулем и линейкой, Мат. Просвещение, 17 (2013). http://www.mccme.ru/free-books/matprosi.html.

[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 (v1)

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

[Li] Дж. Литлвуд, Математическая смесь. М.: Наука, 1978.

[M] Московская математическая конференция школьников, http://www.mccme.ru/mmks/index.htm.

[Ma] Ю. И. Манин, О разрешимости задач на построение с помощью циркуля и линейки. В кн. Энциклопедия элементарной математики. Книга четвертая (геометрия). Под редакцией П. С. Александрова, А. И. Маркушевича и А. Я. Хинчина. М., Физматгиз, 1963.

[Po] М. М. Постников, Теория Галуа. М.: Гос. изд-во физ.-мат. л-ры, 1963.

[P] В.В. Прасолов, Задачи по алгебре, арифметике и анализу (М.: МЦНМО, 2007) ftp://ftp.mccme.ru/users/prasolov/algebra/algebra2.pdf

[PS] В.В. Прасолов и Ю.П. Соловьев, Эллиптические функции и алгебраические уравнения. М.: Факториал, 1997. http://www.mccme.ru/prasolov

[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, Базисные вложения и 13-я проблема Гильберта, Мат. Просвещение, 14 (2010), 143–174. http://arxiv.org/abs/1001.4011.

[Sa] А. Сафин, Программа для построения правильных многоугольников циркулем и линейкой, http://www.mccme.ru/mmks/dec08/Safin.pdf

[Sa1] Теорема Кронекера, http://www.cdoosh.ru/lmsh/archive.html, 2011, 10 класс.

[T] В.М. Тихомиров, Абель и его великая теорема, Квант, 2003, N1. http://kvant.mccme.ru/pdf/2003/01/kv0103abel.pdf

[Va] Вагутен Н., Сопряженные числа. Квант, 1980, N2, http://kvant.mccme.ru/1980/02/sopryazhennye_chisla.htm

[Vi] Э. Б. Винберг, Алгебра многочленов. М.: Просвещение, 1980.

[W] Б.Л. ван дер Варден, Алгебра, М: Наука, 1976.