Линейная независимость радикалов

А. Канунников, И. Воробьёв

§1. Введение

Как доказать иррациональность чисел

$$\sqrt[3]{\frac{121}{111}},\ \sqrt{2}+\sqrt{3},\ \sqrt{2}+\sqrt[3]{3},\ \sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7},\ \sqrt[5]{3}-\sqrt[5]{2},\ \sqrt{\frac{3}{5}+\frac{\sqrt[17]{2021!}}{2021}+\sqrt[5^{5^5}]{\frac{7^{7^7}}{3^{3^3}}}}?$$

Иррациональность одного радикала — простой, чисто арифметический, вопрос, сводящийся к разложению на простые множители.

Лемма 1. *Пусть $A, B, k \in \mathbb{N}$ и НОД$(A, B) = 1$. Тогда $\sqrt[k]{A/B} \in \mathbb{Q}$, если и только если показатели степеней всех простых делителей в разложениях чисел A и B кратны k.*

Доказательство. Пусть $\sqrt[k]{A/B} = a/b$, где $a, b \in \mathbb{N}$, тогда $Ab^k = Ba^k$. Каждый простой делитель p числа A не делит B и входит в разложения чисел a^k и b^k в степенях, кратных k, поэтому p входит в разложение A в степени, тоже кратной k. Рассуждение с простыми делителями числа B аналогично. В обратную сторону утверждение очевидно. □

Число $\sqrt[3]{\frac{121}{111}} = \sqrt[3]{\frac{11^2}{3\cdot 37}}$ иррационально по лемме 1. Если $\sqrt{2}+\sqrt{3} \in \mathbb{Q}$, то $(\sqrt{2}+\sqrt{3})^2 = 5+2\sqrt{6} \in \mathbb{Q}$, откуда $\sqrt{6} \in \mathbb{Q}$, что неверно по той же лемме. Предположив, что $\sqrt{2}+\sqrt[3]{3} = a \in \mathbb{Q}$, возведём равенство $\sqrt[3]{3} = a - \sqrt{2}$ в куб: $3 = a^3 + 6a - (3a^2+2)\sqrt{2}$ и придём к противоречию: $\sqrt{2} = \frac{a^3+6a-3}{3a^2+2} \in \mathbb{Q}$. Однако остальные числа «голыми руками не возьмёшь»: незатейливое возведение в степень только приумножит количество радикалов.

„Неужели, прочитав статью, я пойму, почему даже последнее, нарочито дикое, число иррационально?“ — наверное, думает читатель в эту минуту. „Да, — ответим мы, — если только вы умеете делить многочлены с остатком и извлекать корни из комплексных чисел. Если пока не умеете, то во всяком случае вы разберётесь со сколь угодно длинными суммами квадратных радикалов.“

На самом деле, мы докажем даже большее: между корнями из рациональных чисел не существует линейных соотношений с рациональными коэффициентами, кроме очевидных отношений пропорциональности, например, $\sqrt{8} = 2\sqrt{2}$. Вот точная формулировка.

Теорема 1. *Пусть $N, k_1, \ldots, k_N \in \mathbb{N}$, $N > 1$, $0 < Q_1, \ldots, Q_N \in \mathbb{Q}$ и $\sqrt[k_i]{Q_i} / \sqrt[k_j]{Q_j} \notin \mathbb{Q}$ при $i \neq j$. Тогда равенство*

$$a_1 \sqrt[k_1]{Q_1} + \ldots + a_N \sqrt[k_N]{Q_N} = 0, \text{ где } a_1, \ldots, a_N \in \mathbb{Q},$$

выполняется только при $a_1 = \ldots = a_N = 0$.

В частности, при $Q_1 = 1$ получим, что *сумма $\sqrt[k_2]{Q_2} + \ldots + \sqrt[k_N]{Q_N}$ иррациональна,* так как равенство $a_1 \sqrt[k_1]{1} + \sqrt[k_2]{Q_2} + \ldots + \sqrt[k_N]{Q_N} = 0$ не может выполняться ни при каком $a_1 \in \mathbb{Q}$.

Чтобы применять теорему 1, нужно проверять иррациональность отдельных радикалов $\sqrt[k_i k_j]{Q_i^{k_j}/Q_j^{k_i}}$ по лемме 1.

Задача 1. Выведите из теоремы 1 и леммы 1 иррациональность трёх последних чисел в начале статьи.

На языке векторов утверждение теоремы 1 формулируется так: числа $\sqrt[k_1]{Q_1}, \ldots, \sqrt[k_N]{Q_N}$ *линейно независимы над* $\mathbb{Q}$ (сравните с некомпланарными векторами на рисунке 1). Условие $\sqrt[k_i]{Q_i} / \sqrt[k_j]{Q_j} \notin \mathbb{Q}$ в этих терминах означает линейную независимость чисел $\sqrt[k_i]{Q_i}$ и $\sqrt[k_j]{Q_j}$ над $\mathbb{Q}$ (линейная независимость двух векторов — это просто их неколлинеарность).

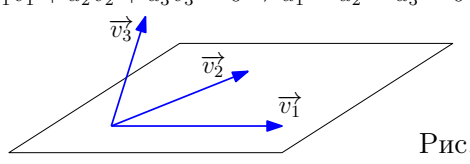


Рис. 1

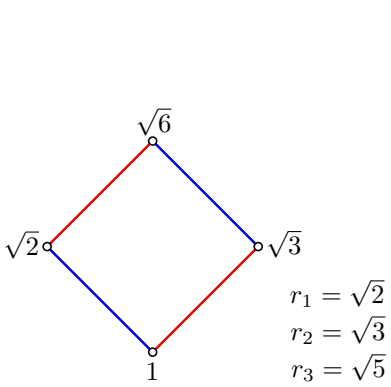
Вообще, взгляд на алгебраические числа (в частности, на радикалы) как на векторы оказывается естественным и продуктивным — он позволяет применять геометрические идеи к алгебраическим задачам [4].

Сформулируем более удобную для доказательства, но, как окажется, равносильную теорему.

Теорема 2. *Пусть $k, n \in \mathbb{N}$, $p_1, \ldots, p_n$ — различные простые числа, $r_1 = \sqrt[k]{p_1}, \ldots, r_n = \sqrt[k]{p_n}$. Тогда система $\{r_1^{l_1} \ldots r_n^{l_n} \mid 0 \leqslant l_1, \ldots, l_n < k\}$ из k^n чисел линейно независима над $\mathbb{Q}$.*

Эту систему удобно представлять в виде n-мерной решётки, см. примеры на рисунке 2.

Задача 2. а) Как связаны наборы чисел на параллельных сторонах квадрата на рисунке 2а и на параллельных рёбрах и гранях куба на рисунке 2б? б) Попробуйте нарисовать гиперкуб (4-мерный куб) и расставить в его вершинах радикалы по тому же принципу.



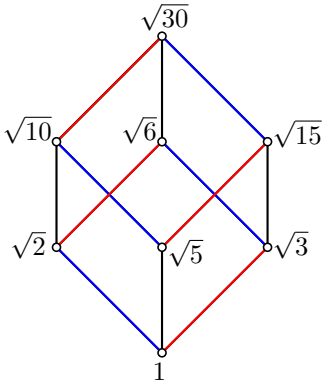


Рис. 2аб

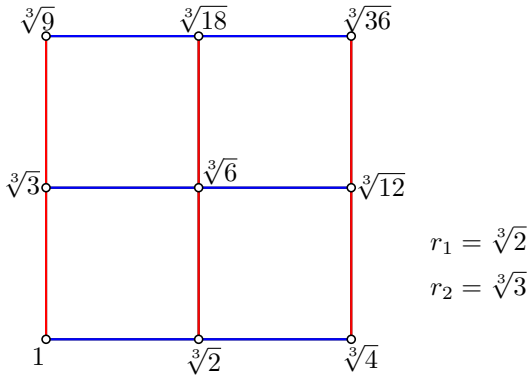


Рис. 2в

Задача 3. Выведите теоремы 1 и 2 друг из друга. *Указание.* 1 ⇒ 2: числа из системы в теореме 2 попарно непропорциональны над $\mathbb{Q}$; 2 ⇒ 1: обобщите рассуждение из следующего примера.

Пример 1. Сведём линейную независимость (по умолчанию — над $\mathbb{Q}$) чисел $1, \sqrt{1/2}, \sqrt[3]{4/3}$ к теореме 2. Выравняем показатели корней: $1, \sqrt[6]{1/2^3}, \sqrt[6]{2^4/3^2}$, домножим второе число на 2, а третье — на 3: $1, \sqrt[6]{2^3}, \sqrt[6]{2^4\cdot 3^4}$ (это не влияет на линейную независимость). Получили подсистему системы $\{\sqrt[6]{2}^{l_1}\sqrt[6]{3}^{l_2} \mid 0 \leqslant l_1, l_2 \leqslant 5\}$, а она линейно независима по теореме 2.

В литературе для школьников неоднократно обсуждался случай квадратных радикалов [2, 4, 6]. В §2 мы разберём его на примерах, подводя ко многим, пусть и не всем, идеям в общей ситуации. Теорема 2 при $n = 1$ доказана в [5]. Общий случай разобран, например в научной статье [7] с помощью теории Галуа. В §3 мы докажем теорему 2 достаточно элементарно, попутно сообщая необходимые сведения об алгебраических числах, интересные и сами по себе. В конце мы приведём совсем короткое доказательство теоремы 1, доступное первокурснику. Всё необходимое для понимания собрано в §4.

§2. Случай квадратных радикалов

Теорему 2 при $k = 2$ можно доказать индукцией по n. База $n = 1$: линейная независимость 1 и $\sqrt{p_1}$ означает просто иррациональность $\sqrt{p_1}$ и имеет место по лемме 1. Разберём случаи $n = 2, 3$ на конкретных примерах — так проще объяснить и понять идеи доказательства. Полное рассуждение с любым k индукцией по n проведём в §3.

Пример 2. Докажем, что числа $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ (рис. 2а) линейно независимы. Пусть $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} = 0$, где $a, b, c, d \in \mathbb{Q}$. Выделим $\sqrt{3}$: $a + b\sqrt{2} + (c + d\sqrt{2})\sqrt{3} = 0$. Если $c + d\sqrt{2} = 0$, то и $a + b\sqrt{2} = 0$, а тогда, ввиду иррациональности $\sqrt{2}$, $c = d = 0$ и $a = b = 0$. Если же $c + d\sqrt{2} \neq 0$, то

$$\sqrt{3} = -\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = -\frac{(a+b\sqrt{2})(c-d\sqrt{2})}{c^2-2d^2} = A + B\sqrt{2}, \text{ где } A = \frac{2bd-ac}{c^2-2d^2},\ B = \frac{ad-bc}{c^2-2d^2} \in \mathbb{Q}.$$

Возведём равенство $\sqrt{3} = A + B\sqrt{2}$ в квадрат:

$$3 = A^2 + 2B^2 + 2AB\sqrt{2} \implies AB = 0, \text{ иначе } \sqrt{2} \in \mathbb{Q}.$$

При $A = 0$ получаем $\sqrt{3/2} = B \in \mathbb{Q}$, при $B = 0$ получаем $\sqrt{3} = A \in \mathbb{Q}$ — противоречие с леммой 1.

Мы свели линейную независимость чисел на рисунке 2а к «инородности» $\sqrt{3}$ по отношению к множеству $\mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ (формально — $\sqrt{3}$ не лежит в нём), подобно тому, как $\sqrt{2}$ инородно по отношению к $\mathbb{Q}$. При этом оказалось важно, что в множестве $\mathbb{Q} + \mathbb{Q}\sqrt{2}$ можно не только складывать, вычитать, умножать, но и делить (не на 0), как и в $\mathbb{Q}$. Прежде чем сделать следующий шаг, введём несколько понятий.

Немного теории. Множество чисел, содержащее 0 и 1 и замкнутое относительно четырёх арифметических действий, называется *числовым полем*. Слово „числовое“ мы будем опускать. Итак, K — поле, если $0, 1 \in K$ и для любых $a, b \in K$ верно $a \pm b, ab \in K$ и $a/b \in K$ при $b \neq 0$. Легко понять, $\mathbb{Q}$ — поле,

причём „самое маленькое“ — любое поле его содержит[1]. Если поле K содержится в поле L, то говорят, что K — *подполе* в L. В этом параграфе все поля лежат в поле $\mathbb{R}$ действительных чисел.

Числа $x_1, \ldots, x_n$ называются *линейно независимыми над полем* K, если равенство $a_1x_1 + \ldots + a_nx_n = 0$, где $a_1, \ldots, a_n \in K$, выполняется только при $a_1 = \ldots = a_n = 0$. Например, числа 1 и $\sqrt{2}$ линейно независимы над $\mathbb{Q}$, но линейно зависимы над $\mathbb{R}$ (равенство $a_1 \cdot 1 + a_2\sqrt{2} = 0$ верно при $a_1 = \sqrt{2}$ и $a_2 = -1$).

Задача 4. Проверьте свойства линейной зависимости/независимости над произвольным полем K:

а) система, содержащая 0 или два числа, отношение которых лежит в K, линейно зависима над K;

б) подсистема линейно независимой системы линейно независима;

в) система $1, x$ линейно независима над K, если и только если $x \notin K$;

г) коэффициенты $a_1, \ldots, a_n \in K$ в записи числа $a_1x_1 + \ldots + a_nx_n$ определены однозначно, если и только если система $x_1, \ldots, x_n$ линейно независима над K.

Наименьшее (по включению) поле, содержащее поле K и числа $\alpha_1, \ldots, \alpha_n$, обозначается $K(\alpha_1, \ldots, \alpha_n)$ и называется полем, порожденным над K этими числами. Опишем поле, порожденное над K одним квадратным радикалом $\sqrt{d} \notin K$, где $d \in K$. Поле $K(\sqrt{d})$, очевидно, состоит из отношений чисел вида $a + b\sqrt{d}$, где $a, b \in K$. Но от иррациональности в знаменателе можно избавиться, домножив на *сопряжённое* $a - b\sqrt{d}$: $\dfrac{1}{a + b\sqrt{d}} = \dfrac{a - b\sqrt{d}}{a^2 - db^2}$ (как в примере 2). Значит,

$$K(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in K\}.$$

Пример 3. Пусть p, q — различные простые числа. Аналогично примеру 2 $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$ и числа $1, \sqrt{p}, \sqrt{q}, \sqrt{pq}$ линейно независимы над $\mathbb{Q}$. Поэтому

$$\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p})(\sqrt{q}) = \{a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \mid a, b, c, d \in \mathbb{Q}\},$$

причём запись чисел в таком виде однозначна.

Пример 4. Докажем, что числа на рисунке 2б линейно независимы над $\mathbb{Q}$. Пусть

$$a_1 + a_2\sqrt{2} + \ldots + a_8\sqrt{30} = 0, \text{ где } a_1, a_2, \ldots, a_8 \in \mathbb{Q}.$$

Шаг 1. Вынося $\sqrt{5}$ за скобки, получим равенство вида $A + B\sqrt{5} = 0$, где $A, B \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$:

$$\underbrace{a_1 + a_2\sqrt{2} + a_3\sqrt{3} + a_5\sqrt{6}}_{A} + \underbrace{(a_4 + a_6\sqrt{2} + a_7\sqrt{3} + a_8\sqrt{6})}_{B}\sqrt{5} = 0. \tag{1}$$

Достаточно доказать, что $A = B = 0$. Тогда, согласно примеру 2, $a_1 = a_2 = a_3 = a_5 = 0$ и $a_4 = a_6 = a_7 = a_8 = 0$.

Шаг 2. Надо доказать, что числа 1 и $\sqrt{5}$ линейно независимы над полем $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Это равносильно условию $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (задача 4в).

Шаг 3. Предположим, что $\sqrt{5} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, т. е., с учётом описания этого поля в примере 3,

$$\sqrt{5} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \text{ где } a, b, c, d \in \mathbb{Q}. \tag{2}$$

Большое число радикалов может отбить желание возводить в квадрат. Однако это можно сделать по-умному, предварительно сгруппировав слагаемые одних из двух способов:

$$\underbrace{a + b\sqrt{2}}_{C} + (\underbrace{c + d\sqrt{2}}_{D})\sqrt{3} = \sqrt{5} = \underbrace{a + c\sqrt{3}}_{C'} + (\underbrace{b + d\sqrt{3}}_{D'})\sqrt{2}, \tag{3}$$

и «не тревожить» C, D, C', D'. Возведём в квадрат первое равенство:

$$C^2 + 3D^2 + 2CD\sqrt{3} = 5.$$

Так как числа 1 и $\sqrt{3}$ линейно независимы над полем $\mathbb{Q}(\sqrt{2})$, то $CD = 0$. Аналогично $C'D' = 0$. Всего 4 варианта: $C = C' = 0$, $C = D' = 0$, $C' = D = 0$ или $D = D' = 0$. Если $C = C' = 0$, то $a = b = c = 0$, поэтому $\sqrt{5} = d\sqrt{6}$, а это противоречит лемме 1. В других случаях получается аналогичное противоречие, так как в правой части равенства (2) остаётся лишь одно ненулевое слагаемое.

[1]Бывают и другие поля: поле вычетов $\mathbb{Z}_p$, поле рациональных функций и др. Любое поле содержит либо $\mathbb{Q}$, либо $\mathbb{Z}_p$.

Задача 5. Докажите теорему 2 при $k = 2$: сделайте шаг индукции от $n-1$ к n, следуя примеру 4.

Прежде чем переходить к радикалам более высокой степени, обсудим, как можно было сделать последний шаг с прицелом на общий случай — без возведения в квадрат. Согласитесь, даже столь безобидное равенство как $\sqrt[5]{3} = a + b\sqrt[5]{2}$ $(a, b \in \mathbb{Q})$ едва ли удастся привести к противоречию лобовым возведением в пятую степень... Что если в равенствах (3) перейти к сопряжённым числам?

Назовём числа вида $a \pm b\sqrt{d}$ над полем K, где $a, b, d \in K$, $\sqrt{d} \notin K$, сопряжёнными. В равенствах (3) сопряжённым к числу $C + D\sqrt{3}$ над полем $\mathbb{Q}(\sqrt{2})$ будет $C - D\sqrt{3}$, а сопряжённым к числу $C' + D'\sqrt{2}$ над полем $\mathbb{Q}(\sqrt{3})$ будет $C' - D'\sqrt{2}$. В то же время сопряжённым к числу $\sqrt{5}$ над обоими полями будет $-\sqrt{5}$. Раз числа равны, то равны и их сопряжённые:

$$C - D\sqrt{3} = -\sqrt{5} = C' - D'\sqrt{2}. \tag{4}$$

Отсюда и из (3) получаем $C = C' = 0$, что невозможно, как показано выше.

Увы, несмотря на кажущуюся строгость, это рассуждение содержит «дыру», однако его можно спасти. Логическая ошибка довольно тонкая, и читатель, который её обнаружит и исправит, вправе собой гордиться.

Задача 6. Почему переход от (3) к (4) не обоснован, и как его доказать?

Переход к сопряжённым часто бывает эффективен. Вот несколько олимпиадных задач на эту тему.

Задача 7. Существуют ли такие рациональные числа a, b, c, d, что $(a + b\sqrt{2})^2 + (c + d\sqrt{2})^2 = 7 + 5\sqrt{2}$?

Задача 8. Найдите первые 1000 знаков после запятой в десятичной записи числа $(6 + \sqrt{35})^{1000}$.

Задача 9. Докажите, что произведение 2^{100} чисел $\pm\sqrt{1} \pm \sqrt{2} \pm \ldots \pm \sqrt{99} \pm \sqrt{100}$ — полный квадрат.

§3. Общий случай

Начнём доказывать теорему 2 при произвольном k, следуя плану в примере 4. При этом на каждом шаге будут возникать новые трудности. Чем дальше в лес — тем больше дров.

Шаг 1: отщепление последнего радикала. Линейное соотношение над $\mathbb{Q}$ (т. е. с коэффициентами из $\mathbb{Q}$) девяти чисел на рисунке 2в можно записать в виде

$$f_0(\sqrt[3]{2}) + f_1(\sqrt[3]{2})\sqrt[3]{3} + f_2(\sqrt[3]{2})\sqrt[3]{9} = 0,$$

где f_0, f_1, f_2 — многочлены степени меньше 3 над $\mathbb{Q}$ (сгруппировали слагаемые как в (1)). Поэтому линейная независимость этих чисел будет следовать из двух фактов:

$$\text{числа } 1, \sqrt[3]{3}, \sqrt[3]{9} \text{ линейно независимы над полем } \mathbb{Q}(\sqrt[3]{2}); \tag{5}$$

$$\text{числа } 1, \sqrt[3]{2}, \sqrt[3]{4} \text{ линейно независимы над полем } \mathbb{Q}. \tag{6}$$

В самом деле, из (5) получаем $f_0(\sqrt[3]{2}) = f_1(\sqrt[3]{2}) = f_2(\sqrt[3]{2}) = 0$, а тогда из (6) коэффициенты многочленов f_0, f_1, f_2 — нулевые. Обобщим это рассуждение и покажем, что достаточно доказать **теорему 2′**: *в обозначениях теоремы 2 числа* $1, r_n, \ldots, r_n^{k-1}$ *линейно независимы над полем* $\mathbb{Q}(r_1, \ldots, r_{n-1})$.

Пусть теорема 2′ доказана. Докажем теорему 2 индукцией по n. При $n = 1$ теоремы совпадают буквально: $\mathbb{Q}(r_1, \ldots, r_{n-1}) = \mathbb{Q}$. Пусть $n > 1$. Переформулируем теорему 2: *если* $F(x_1, \ldots, x_n)$ *— многочлен над* $\mathbb{Q}$*, имеющий по каждой переменной степень меньше* k*, и* $F(r_1, \ldots, r_n) = 0$*, то* $F = 0$ *(т. е. все коэффициенты многочлена* F *нулевые).* Запишем F в виде

$$F(x_1, \ldots, x_n) = f_0(x_1, \ldots, x_{n-1}) + f_1(x_1, \ldots, x_{n-1})x_n + \ldots + f_{k-1}(x_1, \ldots, x_{n-1})x_n^{k-1}.$$

По условию $F(r_1, \ldots, r_n) = 0$. По теореме 2′ имеем $f_j(r_1, \ldots, r_{n-1}) = 0$ для всех $j = 0, \ldots, k-1$. По предположению индукции $f_0 = \ldots = f_{n-1} = 0$, т. е. $F = 0$.

Шаг 2: «инородность» последнего радикала. Пусть K — любое поле, r — такое число, что $r^k \in K$. Выясним, когда

$$\text{числа } 1, r, \ldots, r^{k-1} \text{ линейно независимы над } K. \tag{7}$$

Иными словами, r не должно быть корнем многочлена степени меньше k с коэффициентами из K. При $k = 2$ это просто означает, что $r \notin K$ (задача 4в). При $k > 2$ всё гораздо сложнее и интереснее.

Немного теории. Множество многочленов над полем K обозначается $K[x]$. Многочлен над K положительной степени, который не раскладывается в произведение многочленов меньших степеней, называется *неприводимым* над K. Многочлены над полем можно делить с остатком («уголком»).

Пусть число α является корнем ненулевого многочлена над полем K, тогда оно называется *алгебраическим над K*. Среди всех таких многочленов только один имеет наименьшую степень и старший коэффициент 1 (если бы их было два, то их разность была бы многочленом меньшей степени с корнем α). Он называется *минимальным многочленом* числа α над K, и мы будем его обозначать $\mu_\alpha^K(x)$ или $\mu_\alpha(x)$, если ясно, о каком поле K идёт речь. Степень этого многочлена есть наименьшее такое $m \in \mathbb{N}$, что числа $1, \alpha, \dots, \alpha^m$ линейно зависимы над K. Вот основные свойства многочлена $\mu_\alpha^K(x) = \mu_\alpha(x)$:

1) многочлен $\mu_\alpha(x)$ неприводим над K;

2) любой многочлен из $K[x]$ с корнем α делится на $\mu_\alpha(x)$;

3) неприводимый над K многочлен $p(x)$ с корнем α и старшим коэффициентом 1 равен $\mu_\alpha(x)$.

Доказательство. 1) Если многочлен μ_α раскладывается в произведение многочленов над K меньшей степени, то α — корень одного из сомножителей, что противоречит минимальности степени $\deg \mu_\alpha$.

2) Пусть $f \in K[x]$ и $f(\alpha) = 0$. Разделим f на μ_α с остатком: $f = \mu_\alpha q + s$, где $q, s \in K[x]$ и либо $s = 0$, либо $\deg s < \deg \mu_\alpha$. Второй вариант невозможен, так как $s(\alpha) = f(\alpha) - \mu_\alpha(\alpha)q(\alpha) = 0$.

3) По пункту 2) $p(x)$ делится на $\mu_\alpha(x)$, а так как $p(x)$ неприводим над K, то $p(x)/\mu_\alpha(x) = c \in K$. Поскольку старшие коэффициенты у $p(x)$ и $\mu_\alpha(x)$ равны 1, то $c = 1$. □

Таким образом, (7) $\Leftrightarrow \mu_r^K(x) = x^k - r^k \Leftrightarrow$ двучлен $x^k - r^k$ неприводим над K. Например, утверждения (5) и (6) равносильны соответственно неприводимости двучлена $x^3 - 3$ над $\mathbb{Q}(\sqrt[3]{2})$ и двучлена $x^3 - 2$ над $\mathbb{Q}$, а это значит, что $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$ и $\sqrt[3]{2} \notin \mathbb{Q}$ (кубический многочлен неприводим над полем, если не имеет в нем корней). В общем случае условие «инородности» $r \notin K$ необходимо, но не достаточно. Хотя в нашем случае действующие лица K и r лежат в поле $\mathbb{R}$, мы выйдем в комплексную плоскость — поле $\mathbb{C}$, где двучлен $x^k - r^k$ раскладывается на линейные множители. По формуле Муавра [3]

$$x^k - r^k = (x - r)(x - r\varepsilon)\dots(x - r\varepsilon^{k-1}), \text{ где } \varepsilon = \varepsilon_k = \cos\tfrac{2\pi}{k} + i\sin\tfrac{2\pi}{k}. \tag{8}$$

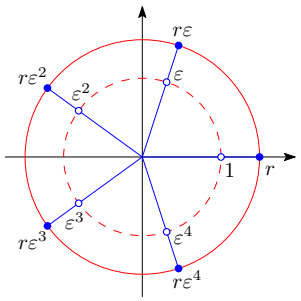


Рис. 3

Лемма 2. *Пусть K — подполе в $\mathbb{R}$, $r \in \mathbb{R}$, $r^k \in K$ и $r, \dots, r^{k-1} \notin K$. Тогда двучлен $x^k - r^k$ неприводим над K.*

Доказательство. Предположим, что двучлен $x^k - r^k$ имеет делитель из $K[x]$ степени $l \in \{1, \dots, k-1\}$ и c — свободный член этого делителя. Из разложения (8) имеем $c = (-r)^l\varepsilon^s$ для некоторого целого s. Поскольку $c \in K \subseteq \mathbb{R}$, $r \in \mathbb{R}$ и $|\varepsilon^s| = 1$, то $r^l = \pm|c| \in K$, что противоречит условию. □

Замечание. Для $r \notin \mathbb{R}$ лемма неверна, например, при $k = 3$ и $r = \varepsilon$ имеем $\varepsilon, \varepsilon^2 \notin \mathbb{R}$, но двучлен $x^3 - 1$ приводим.

Пример 5. Для любого простого p и натурального $k > 1$ имеем $\sqrt[k]{p}, \dots \sqrt[k]{p^{k-1}} \notin \mathbb{Q}$ (лемма 1), поэтому двучлен $x^k - p$ неприводим над $\mathbb{Q}$ (лемма 2)[2], значит, $\mu_{\sqrt[k]{p}}^{\mathbb{Q}}(x) = x^k - p$.

Вообще, теорема $2'$ посредством леммы 2 сведена к **теореме $2''$**: *в тех же обозначениях*

$$r_n, \dots, r_n^{k-1} \notin \mathbb{Q}(r_1, \dots, r_{n-1}). \tag{9}$$

При $n = 1$ это верно по лемме 1. Чтобы прийти к противоречию при $n > 1$, научимся записывать числа из $\mathbb{Q}(r_1, \dots, r_{n-1})$ в виде многочленов от $r_1, \dots, r_{n-1}$. Например, условие $\sqrt[3]{3} \notin \mathbb{Q}(\sqrt[3]{2})$ запишется в виде $\sqrt[3]{3} \neq a + b\sqrt[3]{2} + c\sqrt[3]{4}$ при $a, b, c \in \mathbb{Q}$.

Шаг 3: избавление от иррациональности в знаменателе. Пресловутое «домножение на сопряжённое» работает лишь с квадратными радикалами. Как действовать при $k > 2$, сначала покажем на примере.

[2] В [5] линейная независимость чисел $1, \sqrt[k]{p}, \dots \sqrt[k]{p^{k-1}}$ также сведена к неприводимости двучлена $x^k - p$, установленной по признаку Эйзенштейна.

Пример 6. Избавимся от иррациональности в знаменателе дроби $\dfrac{1}{\sqrt[3]{4}+\sqrt[3]{2}+3}$. Обозначим $r=\sqrt[3]{2}$ и $f(x)=x^2+x+3$. Надо найти такой многочлен $u\in\mathbb{Q}[x]$, что $\frac{1}{f(r)}=u(r)$. Это значит, что многочлен $f(x)u(x)-1$ имеет корень r, а тогда делится на $\mu_r^{\mathbb{Q}}(x)=x^3-2$ (пример 5). Таким образом,

$$u(x)f(x)+v(x)(x^3-2)=1.$$

для некоторого многочлена $v\in\mathbb{Q}[x]$. Многочлены u и v найдём с помощью алгоритма Евклида:

Алгоритм Евклида	Обратный ход алгоритма Евклида
$x^3-2=(x^2+x+3)(x-1)-2x+1$ $x^2+x+3=(2x-1)\left(\frac{1}{2}x+\frac{3}{4}\right)+\frac{15}{4}$	$\frac{15}{4}=f(x)-\big(f(x)(x-1)-(x^3-2)\big)\left(\frac{1}{2}x+\frac{3}{4}\right)=$ $=(x^3-2)\left(\frac{1}{2}x+\frac{3}{4}\right)+f(x)\left(-\frac{1}{2}x^2-\frac{1}{4}x+\frac{7}{4}\right)$

Итак, $(2x^2+x-7)(x^2+x+3)-(2x+3)(x^3-2)=-15$, откуда при $x=r$ получаем

$$\frac{1}{\sqrt[3]{4}+\sqrt[3]{2}+3}=\frac{7-\sqrt[3]{2}-2\sqrt[3]{4}}{15}.$$

Докажем теперь общее утверждение, следуя разобранному примеру.

Лемма 3 (об избавлении от иррациональности в знаменателе)**.** *Если число α алгебраично над полем K и $\deg\mu_\alpha(x)=k$, то каждое число в поле $K(\alpha)$ однозначно записывается в виде*

$$c_0+c_1\alpha+\ldots+c_{k-1}\alpha^{k-1},\ \text{где } c_0,c_1,\ldots,c_{k-1}\in K. \tag{10}$$

Доказательство. Числа такого вида лежат в $K(\alpha)$, поэтому надо проверить, что они сами образуют поле. Замкнутость относительно сложения, вычитания и умножения очевидна. Пусть $f\in K[x]$ и $f(\alpha)\neq 0$. Тогда $f(x)$ не делится на $\mu_\alpha(x)$, а потому эти многочлены взаимно просты. По алгоритму Евклида найдутся такие многочлены $u,v\in K[x]$, что $u(x)f(x)+v(x)\mu_\alpha(x)=1$. При $x=\alpha$ получим $1/f(\alpha)=u(\alpha)$, что преобразуется к виду (10) заменой u его остатком от деления на μ_α. Коэффициенты c_i определены однозначно, иначе α был бы корнем многочлена степени меньше k. □

Задача 10. Избавьтесь от иррациональности в знаменателях: а) $\dfrac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}}$; б) $\dfrac{1}{\sqrt[4]{27}+2\sqrt[4]{3}-1}$.

Вернёмся к доказательству теоремы $2''$. По предположению индукцию двучлен $x^k-r_1^k$ неприводим над $\mathbb{Q}$, двучлен $x^k-r_2^k$ — над $\mathbb{Q}(r_1)$, …, двучлен $x^k-r_{n-1}^k$ — над $\mathbb{Q}(r_1,\ldots,r_{n-2})$. Последовательно избавляясь от иррациональности в знаменателе, представим каждое число из $\mathbb{Q}(r_1,\ldots,r_{n-1})$ однозначно в виде суммы чисел вида

$$ar_1^{l_1}\ldots r_{n-1}^{l_{n-1}},\ \text{где } a\in\mathbb{Q},\ 0\leqslant l_1,\ldots,l_{n-1}<k. \tag{11}$$

Пусть (9) неверно, т. е. r_n^l при некотором $l\in\{1,\ldots,k-1\}$ равно сумме чисел вида (11). В этой сумме должно быть больше одного слагаемого, иначе $r_n^l/(r_1^{l_1}\ldots r_{n-1}^{l_{n-1}})=a\in\mathbb{Q}$, что противоречит лемме 1. Значит, какой-то из радикалов $r_1,\ldots,r_{n-1}$ встречается в двух слагаемых в разных степенях, пусть это r_{n-1}. Итак,

$$r_n^l=A_0+A_1r_{n-1}+\ldots+A_{k-1}r_{n-1}^{k-1}, \tag{12}$$

где среди $A_0,\ldots,A_{k-1}\in\mathbb{Q}(r_1,\ldots,r_{n-2})$ хотя бы два ненулевых. Самое интересное наступает в этот момент — трудность по сравнению со случаем $k=2$ возрастает ещё больше. И вправду, при $k=2$ равенство (12) совсем не страшно: $\sqrt{p_n}=A_0+A_1\sqrt{p_{n-1}}$ и без труда возводится в квадрат. Но при $k>2$ о возведении (12) в k-ю степень даже думать не хочется... На помощь вновь приходят минимальные многочлены. Но если для левой части минимальный многочлен найти легко, то для правой не очевидна даже алгебраичность.

Пример 7. Приведём к противоречию упомянутое выше равенство $\sqrt[5]{3}=a+b\sqrt[5]{2}$, где $a,b\in\mathbb{Q}$, — частный случай (12). По лемме 1 $a\neq 0$ и $b\neq 0$. Согласно примеру 5, $\mu_{\sqrt[5]{3}}(x)=x^5-3$ и $\mu_{\sqrt[5]{2}}(x)=x^5-2$, а тогда $\mu_{a+b\sqrt[5]{2}}(x)=(x-a)^5-2b^5$ (сделали линейную замену $x\mapsto\frac{x-a}{b}$ и умножили на b^5). Получаем противоречие:

$$x^5-3=(x-a)^5-2b^5=x^5-5ax^4+\ldots\ \Longrightarrow\ a=0.$$

Задача 11. Решите уравнение в натуральных числах: $\sqrt[5]{m}+\sqrt[5]{n}=2021$.

Задача 12. Опровергните равенство $\sqrt[6]{3}=a\sqrt[3]{2}+b\sqrt{2}$, где $a,b\in\mathbb{Q}$.

В общем случае путь к минимальному многочлену правой части равенства (12) лежит через *сопряжённые числа*. Вот только что такое, мы определили пока лишь для квадратичных иррациональстей, и в конце §2 наметили рассуждение с переходом к сопряжённым.

Ещё немного теории. Пусть число $\alpha\in\mathbb{C}$ алгебраично над полем K и

$$\mu_\alpha(x)=(x-\alpha_1)\dots(x-\alpha_k)$$

(согласно основной теореме алгебры любой многочлен над $\mathbb{C}$ раскладывается на линейные множители[3]). Числа $\alpha_1,\dots,\alpha_k$ называются *сопряжёнными с* α над K. Обозначим их сумму $\sigma(\alpha)$. По теореме Виета

$$\sigma(\alpha)=\alpha_1+\ldots+\alpha_k \iff \mu_\alpha(x)=x^k-\sigma(\alpha)x^{k-1}+\ldots \tag{13}$$

Пример (7) показывает, что именно коэффициент $-\sigma(\alpha)$ будет играть ключевую роль.

Замечание. Числа $\alpha_1,\dots,\alpha_k$ различны (для доказательства это не нужно): если $\mu_\alpha(x)=(x-\alpha_j)^2g(x)$, то производная $\mu'_\alpha(x)=2(x-\alpha_j)g(x)+(x-\alpha_j)^2g'(x)\in K[x]$ имеет корень α_j, хотя $\deg\mu'_\alpha<\deg\mu_\alpha$.

Ввиду свойства 3) минимального многочлена все алгебраические над K числа разбиваются на классы сопряжённых, каждый из которых состоит из корней какого-то неприводимого над K многочлена.

Пример 8. Разложим двучлен x^4-2 на неприводимые и разобьём его корни на классы сопряжённых над каждым из полей $\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt[4]{2})\subset\mathbb{Q}(\sqrt[4]{2},i)$:

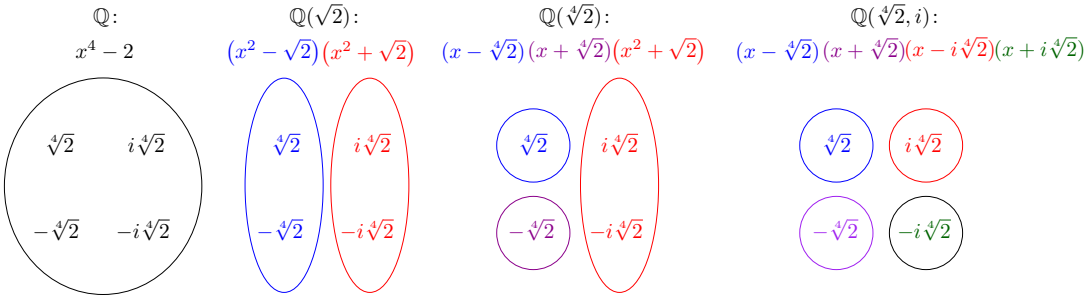


Рис. 4

Пример 9. Для квадратичных иррациональностей $a\pm b\sqrt{d}$ ($a,b,d\in K$, $b\neq0$, $\sqrt{d}\notin K$) данное определение согласовано с привычным понятием сопряжённости:

$$\mu^K_{a\pm b\sqrt{d}}(x)=x^2-2ax+a^2-db^2,\quad \sigma(a\pm b\sqrt{d})=2a.$$

(Кстати, при $K=\mathbb{R}$ и $d=-1$ получаем комплексно-сопряжённые числа $a\pm bi$.) Это спасает приведённое выше обоснование перехода от (3) к (4).

Пример 10. Пусть $a,b\in\mathbb{Q}$, $b\neq0$. Числа $a\pm b\sqrt[k]{2}$, конечно, не будут сопряжёнными при $k>2$ (по аналогии с квадратичными иррациональностями). Сопряжённые с числом $a+b\sqrt[k]{2}$ суть корни многочлена $\mu_{a+b\sqrt[k]{2}}(x)=(x-a)^k-2b^k$ (аналогично примеру 7), т. е. числа $a+b\sqrt[k]{2}\varepsilon^j$, $j=0,\dots,k-1$ (пример на рис. 5). Знак $\pm$ при $k=2$ объясняется тем, что $\varepsilon_2=-1$.

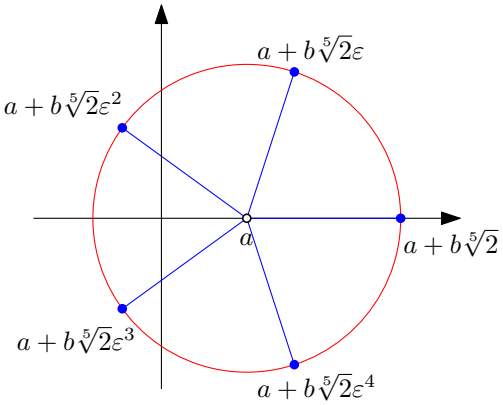


Рис. 5

[3]Мы этим пользоваться не будем: в доказательстве все многочлены раскладываются явно.

Лемма 4. *Пусть K — подполе в $\mathbb{R}$, $r \in \mathbb{R}$, $r \notin K$, $r^k \in K$ для некоторого $k \in \mathbb{N}$. Тогда $\sigma(r) = 0$.*

Доказательство. Существует наименьшее $m \in \mathbb{N}$, такое что $r^m \in K$. По лемме 2 двучлен $x^m - r^m$ неприводим над K, а значит, равен $\mu_r^K(x)$. Так как $r \notin K$, то $m > 1$ и $\sigma(r) = 0$. □

Шаг 4: переход к сопряжённым числам. Пример 10 подсказывает вид сопряжённых к числу вида (10).

Пример 11. Опровергнем равенство $\sqrt[3]{3} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где $a, b, c \in \mathbb{Q}$. Сопряжённые с левой частью суть $\sqrt[3]{3}$, $\sqrt[3]{3}\varepsilon$, $\sqrt[3]{3}\varepsilon^2$, где $\varepsilon = \varepsilon_3$. С другой стороны, рассмотрим многочлен

$$F(x) = \big(x - (a + b\sqrt[3]{2} + c\sqrt[3]{4})\big)\big(x - (a + b\sqrt[3]{2}\varepsilon + c\sqrt[3]{4}\varepsilon^2)\big)\big(x - (a + b\sqrt[3]{2}\varepsilon^2 + c\sqrt[3]{4}\varepsilon)\big).$$

Как показать, что $F(x) \in \mathbb{Q}[x]$, не портя настроение раскрытием скобок? Чистая алгебра: заменим $\sqrt[3]{2}$ на y и $\sqrt[3]{4}$ на y^2. Получим многочлен, не меняющийся при подстановке $y\varepsilon$ вместо y, а значит, y в него входит только в степенях, кратных 3. Заменяя y^3 на 2, получим многочлен $F(x) \in \mathbb{Q}[x]$. Следовательно, $F(x)$ делится на $\mu_{\sqrt[3]{3}}(x) = x^3 - 3$, отсюда $F(x) = x^3 - 3$. Но сумма корней многочлена F равна $3a$ (так как $1 + \varepsilon + \varepsilon^2 = 0$). Значит, $a = 0$ и $\sqrt[3]{3} = b\sqrt[3]{2} + c\sqrt[3]{4}$. Поделим на $\sqrt[3]{2}$: $\sqrt[3]{3/2} = b + c\sqrt[3]{2}$. Аналогично или как в примере 7 получим $b = 0$. Значит, $\sqrt[3]{3} = c\sqrt[3]{4}$, что невозможно по лемме 1.

Лемма 5. *Пусть $\alpha_1 = \alpha, \ldots, \alpha_k$ — все сопряжённые с числом α, алгебраичным над полем K, и $f \in K[x]$. Тогда число $f(\alpha)$ алгебраично над K и для некоторого $d \in \mathbb{N}$*

$$\mu_{f(\alpha)}(x)^d = (x - f(\alpha_1)) \ldots (x - f(\alpha_k)). \tag{14}$$

Доказательство. для наших целей достаточно провести в случае $\mu_\alpha(x) = x^k - r^k$, где $r = \alpha$. Равенство (14) примет вид

$$\mu_{f(r)}(x)^d = (x - f(r))(x - f(r\varepsilon)) \ldots (x - f(r\varepsilon^{k-1})). \tag{15}$$

1. Рассмотрим вспомогательный многочлен

$$G(x, y) = (x - f(y))(x - f(y\varepsilon)) \ldots (x - f(y\varepsilon^{k-1})).$$

Он не меняется при замене y на $y\varepsilon$ (скобки сдвигаются по циклу), а потому все входящие в него степени y кратны k. Поэтому $G(x, r)$ — многочлен с коэффициентами из K и корнем $f(r)$. Значит, число $f(r)$ алгебраично над K и $\mu_{f(r)}(x)$ делит $G(x, r)$.

2. Многочлен $\mu_{f(r)}(f(x)) \in K[x]$ имеет корень r, а потому делится на многочлен $\mu_r(x) = x^k - r^k$. Значит, все корни $r, r\varepsilon, \ldots, r\varepsilon^{k-1}$ этого двучлена являются корнями многочлена $\mu_{f(r)}(f(x))$, т. е. числа $f(r), f(r\varepsilon), \ldots, f(r\varepsilon^{k-1})$ сопряжены.

3. Пусть $d \in \mathbb{N}$ — наименьшее такое число, что $\mu_{f(r)}(x)^d$ делит $G(x, r)$. Докажем, что $G(x, r) = \mu_{f(r)}(x)^d$. Действительно, в противном случае многочлен $G(x, r)/\mu_{f(r)}(x)^d \in K[x]$ имеет некоторый корень $f(r\varepsilon^j)$, а значит, делится на $\mu_{f(r\varepsilon^j)}(x) = \mu_{f(r)}(x)$, что противоречит минимальности d.

Для доказательства в общем случае рассмотрим многочлен

$$G(x, y_1, \ldots, y_k) = (x - f(y_1)) \ldots (x - f(y_k)).$$

Он не меняется при перестановках $y_1, \ldots, y_k$ и по основной теореме о симметрических многочленах [1, стр. 134] выражается через x и элементарные симметрические многочлены $\sigma_1, \ldots, \sigma_k$, определяемые равенством $(x - y_1) \ldots (x - y_k) = x^k - \sigma_1 x^{k-1} + \sigma_2 x^{k-2} - \ldots + (-1)^k \sigma_k$. Поскольку $(x - \alpha_1) \ldots (x - \alpha_k) = \mu_\alpha(x) \in K[x]$, то $G(x, \alpha_1, \ldots, \alpha_k) \in K[x]$. Последующие рассуждения аналогичны. □

Приравняем суммы корней (с кратностями) многочленов в равенстве (15):

$$d\sigma(f(r)) = f(r) + f(r\varepsilon) + \ldots + f(r\varepsilon^{k-1}).$$

Сосчитаем правую часть для $f(x) = c_0 + c_1 x + \ldots + c_{k-1} x^{k-1}$:

$$\begin{array}{lll} f(r) & = c_0 + c_1 r & + \ldots + c_{k-1} r^{k-1}, \\ f(r\varepsilon) & = c_0 + c_1 r\varepsilon & + \ldots + c_{k-1} r^{k-1}\varepsilon^{k-1}, \\ \ldots & & \\ f(r\varepsilon^{k-1}) & = c_0 + c_1 r\varepsilon^{k-1} & + \ldots + c_{k-1} r^{k-1}\varepsilon^{(k-1)^2}. \end{array}$$

Сложим числа в каждом столбике. Так как $\varepsilon^k = 1$, то

$$1 + \varepsilon^j + \varepsilon^{2j} + \ldots + \varepsilon^{(k-1)j} = \frac{1 - \varepsilon^{kj}}{1 - \varepsilon^j} = 0,\ j = 1, \ldots, k-1.$$

Значит, $f(r) + f(r\varepsilon) + \ldots + f(r\varepsilon^{k-1}) = kc_0$, откуда

$$\sigma(c_0 + c_1 r + \ldots + c_{k-1} r^{k-1}) = \tfrac{k}{d} \cdot c_0. \tag{16}$$

Наконец мы готовы привести равенство (12) к противоречию. Пусть A_j — первый ненулевой коэффициент в ряду $A_0, \ldots, A_{k-1}$. Разделим равенство (12) на r_{n-1}^j:

$$\frac{r_n^l}{r_{n-1}^j} = A_j + A_{j+1} r_{n-1} + \ldots + A_{k-1} r_{n-1}^{k-j-1}. \tag{17}$$

Пусть $K = \mathbb{Q}(r_1, \ldots, r_{n-2})$, $R = r_n^l / r_{n-1}^j$. Тогда $R \notin K$, иначе $R = A_j$ и $A_{j+1} = \ldots = A_{k-1} = 0$ ввиду линейной независимости $1, r_{n-1}, \ldots, r_{n-1}^{k-1}$ над K (напомним, среди чисел $A_j, \ldots, A_{k-1}$ хотя бы два ненулевых). При этом $R^k = p_n^l / p_{n-1}^j \in \mathbb{Q}$, поэтому $\sigma(R) = 0$ по лемме 4. В то же время значение σ от правой части (17), согласно (16), пропорционально A_j (играющего роль c_0), а потому не равно 0. Полученное противоречие доказывает теорему 2.

Фактически мы доказали большее: каждое число в поле $\mathbb{Q}(r_1, \ldots, r_n)$ представляется в виде линейной комбинации k^n чисел

$$r_1^{l_1} \ldots r_n^{l_n},\ \text{где } 0 \leqslant l_1, \ldots, l_n < k,$$

с однозначно определёнными рациональными коэффициентами. На языке векторов, эти числа образуют *базис* поля $\mathbb{Q}(r_1, \ldots, r_n)$ над $\mathbb{Q}$. Такое представление достигается избавлением от иррациональности в знаменателе, а однозначность коэффициентов равносильна линейной независимости данной системы.

Короткое доказательство с помощью следа

Используя чуть больше сведений об алгебраических числах, либо владея началами линейной алгебры, можно совсем коротко доказать теорему 1 (не сводя её к теореме 2). В основе рассуждения также лежит некоторая величина, пропорциональная сумме сопряжённых. Но при этом она обладает замечательным свойством линейности, благодаря чему техника сводится к минимуму.

Функция $f\colon L \to \mathbb{C}$, где L — подполе в $\mathbb{C}$, называется *линейной* (точнее, $\mathbb{Q}$-линейной), если $f(ax+by) = af(x)+bf(y)$ для всех $x, y \in L$ и $a, b \in \mathbb{Q}$. Пусть $L = \mathbb{Q}(\sqrt[k_1]{Q_1}, \ldots, \sqrt[k_N]{Q_N})$. В §4 мы покажем, что существует линейная функция $\mathrm{tr}\colon L \to \mathbb{C}$, называемая следом (от англ. trace — след), такая что

$$\text{для каждого } \alpha \in L \text{ найдётся такое } d \in \mathbb{N},\ \text{что } \mathrm{tr}(\alpha) = d\sigma(\alpha) \tag{18}$$

($\sigma(\alpha)$ определено в (13)). Предположим, что $a_1 \sqrt[k_1]{Q_1} + \ldots + a_N \sqrt[k_N]{Q_N} = 0$, где $a_1, \ldots, a_N \in \mathbb{Q}$ не все равны 0. Будем считать, что $a_N \neq 0$. Неожиданным образом уединим не радикал, а коэффициент. Разделим обе части на $\sqrt[k_N]{Q_N}$ и обозначим $R_i = \sqrt[k_i]{Q_i} / \sqrt[k_N]{Q_N}$, $i = 1, \ldots, N-1$:

$$-a_N = a_1 R_1 + \ldots + a_{N-1} R_{N-1}. \tag{19}$$

Так как $R_i^{k_i k_N} \in \mathbb{Q}$ и по условию $R_i \notin \mathbb{Q}$, то $\sigma(R_i) = 0$ по лемме 4, а тогда $\mathrm{tr}(R_i) = 0$ в силу (18). Отсюда в силу линейности след от правой части равенства (19) равен 0. В то же время $\sigma(-a_N) = -a_N \neq 0$ и по (18) $\mathrm{tr}(-a_N) \neq 0$. Это противоречие завершает доказательство теоремы 1.

§4. Дополнение про след

Мы построим функцию след $\mathrm{tr}\colon L \to L$ для любого расширения $L \supseteq \mathbb{Q}$, порожденного конечным числом алгебраических чисел, в частности, для $L = \mathbb{Q}(\sqrt[k_1]{Q_1}, \ldots, \sqrt[k_N]{Q_N})$. Сделаем это двумя способами. Начнём с того, который более соответствует рассуждению в §3 и обогащает его, переводя на язык теории Галуа. Затем мы дадим основное определение следа, объясняющее, кстати, его название. На этом пути нам понадобятся начальные сведения из линейной алгебры:

– базис и размерность расширения, теорема о башне [4, §5];

– операции над матрицами, обратная матрица [1, с. 41–44, 73];

– матрица линейного оператора в базисе, её преобразование при смене базиса [1, с. 234–236].

I подход (в духе теории Галуа)

Нам нужен хорошо известный факт [4, теорема 2]: *множество $\mathbb{A}$ алгебраических (над $\mathbb{Q}$) чисел является полем.* Отсюда $L \subseteq \mathbb{A}$, так как L порождено над $\mathbb{Q}$ алгебраическими числами.

Назовём отображение $\varphi\colon L \to \mathbb{C}$ *вложением*, если $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$ для всех $a, b \in L$ и $\varphi(c) = c$ при $c \in \mathbb{Q}$. В частности, φ линейно: $\varphi(ca) = \varphi(c)\varphi(a) = c\varphi(a)$ при $c \in \mathbb{Q}$ и $a \in L$. Ниже мы покажем, что существует лишь конечное число вложений $\varphi_1, \ldots, \varphi_n$ поля L. Определим

$$\operatorname{tr}(\alpha) = \sum_{j=1}^{n} \varphi_j(\alpha). \tag{20}$$

Задача 13. Не читая далее, а) докажите, что все вложения $\mathbb{Q}(i) \to \mathbb{C}$ суть $a + bi \mapsto a \pm bi$ $(a, b \in \mathbb{Q})$; б) опишите все вложения $\mathbb{Q}\left(\frac{1+i}{\sqrt{2}}\right) \to \mathbb{C}$. Найдите $\operatorname{tr}(1+i)$ в каждом из пунктов.

Вложения открывают новый взгляд на сопряжённые числа, которые прежде мы характеризовали в терминах корней неприводимых многочленов. Пусть $\alpha \in L$ и

$$\mu_\alpha(x) = x^m - c_{m-1}x^{m-1} - \ldots - c_1 x - c_0. \tag{21}$$

Применив любое вложение $\varphi\colon L \to \mathbb{C}$ к обеим частям равенства $\mu_\alpha(\alpha) = 0$:

$$\varphi(\mu_\alpha(\alpha)) = \varphi(\alpha)^m - c_{m-1}\varphi(\alpha)^{m-1} - \ldots - c_1\varphi(\alpha) - c_0 = \mu_\alpha(\varphi(\alpha)) = \varphi(0) = 0,$$

получим, что $\varphi(\alpha)$ сопряжено с α. Обратно, пусть α_j — любое сопряжённое с $\alpha \in L$. Существует ли вложение $L \to \mathbb{C}$, переводящее α в α_j? Такое вложение должно задаваться в поле $\mathbb{Q}(\alpha)$ правилом $f(\alpha) \mapsto f(\alpha_j)$, где $f \in \mathbb{Q}[x]$ (по теореме 3 всякое число из $\mathbb{Q}(\alpha)$ имеет такой вид). С другой стороны, это правило корректно (не зависит от выбора многочлена f) и задаёт вложение $\mathbb{Q}(\alpha) \to \mathbb{C}$, так как для всех $f, g \in \mathbb{Q}[x]$:

$$f(\alpha) = g(\alpha) \Leftrightarrow f(x) - g(x) \vdots \mu_\alpha(x) \Leftrightarrow f(\alpha_j) = g(\alpha_j),$$
$$f(\alpha) + g(\alpha) = (f+g)(\alpha),\ f(\alpha)g(\alpha) = (fg)(\alpha).$$

Не очевидно, впрочем, что это вложение продолжается с $\mathbb{Q}(\alpha)$ на L, но во всяком случае уже можно описать вложения *простых* расширений поля $\mathbb{Q}$ (порождённых одним числом).

Теорема 3. *Пусть $\theta_1 = \theta, \ldots, \theta_n$ — все сопряжённые с $\theta \in \mathbb{A}$. Тогда все вложения $\mathbb{Q}(\theta) \to \mathbb{C}$ суть*

$$\varphi_j\colon f(\theta) \mapsto f(\theta_j)\ (f \in \mathbb{Q}[x]),\ j = 1, \ldots, n.$$

К счастью, расширение, порождённое конечным числом алгебраических чисел, порождается одним числом (т. н. *примитивный элемент*).

Пример 12. Покажем, что $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Включение $\supseteq$ очевидно. Обратно,

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) \ni \frac{1}{\sqrt{2}+\sqrt{3}} = \sqrt{3} - \sqrt{2} \implies \mathbb{Q}(\sqrt{2}+\sqrt{3}) \ni \frac{\sqrt{3}+\sqrt{2}}{2} \pm \frac{\sqrt{3}-\sqrt{2}}{2} = \sqrt{3}, \sqrt{2}.$$

Теорема 4 (о примитивном элементе)**.** *Существует такое $\theta \in L$, что $L = \mathbb{Q}(\theta)$.*

Доказательство. Достаточно для данных $\alpha, \beta \in L$ найти такое $\theta = \alpha + c\beta \in L$, что $\mathbb{Q}(\theta) = \mathbb{Q}(\alpha, \beta)$ (далее — индукция по числу порождающих). Пусть $\alpha = \alpha_1, \ldots, \alpha_m$ и $\beta = \beta_1, \ldots, \beta_n$ — все сопряжённые с α и β. Общие корни многочленов $\mu_\beta(x)$ и $\mu_\alpha(\theta - cx)$ — такие β_j, что $\theta - c\beta_j = \alpha_i$ для некоторого i. Подберём c так, чтобы $\alpha + c\beta \neq \alpha_i + c\beta_j$ при $(i, j) \neq (1, 1)$. Тогда β — единственный корень указанных многочленов и с учётом отсутствия у многочлена $\mu_\beta(x)$ кратных корней (замечание после (13))

$$\big(\mu_\beta(x), \mu_\alpha(\theta - cx)\big) = x - \beta \in \mathbb{Q}(\theta)[x].$$

Итак, $\beta \in \mathbb{Q}(\theta)$, откуда $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\theta)$. □

На практике бывает проще работать с несколькими порождающими, но более просто устроенными.
Задача 14. Опишите все вложения полей $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$, $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$.

Докажем, что функция (20) обладает требуемыми свойствами. Линейность следа вытекает из линейности вложений. Докажем (18). Пусть $\alpha \in L$. По теореме 4 $\alpha = f(\theta)$, где $f \in \mathbb{Q}[x]$. Далее $\varphi_j(\alpha) = \varphi_j(f(\theta)) = f(\varphi_j(\theta))$, что по теореме 3 равно $f(\theta_j)$. Итак,

$$\prod_{j=1}^{n}(x - \varphi_j(\alpha)) = \prod_{j=1}^{n}(x - f(\theta_j)) \overset{\text{теор.5}}{=} \mu_{f(\theta)}(x)^d = \mu_\alpha(x)^d,\ d \in \mathbb{N}. \tag{22}$$

Приравняв суммы корней (с кратностями) многочленов в левой и правой частях, получим (18).

II подход (только линейная алгебра)

След $\operatorname{tr} A$ квадратной матрицы $A = (a_{ij})$ — это сумма её диагональных элементов, $\operatorname{tr} A = \sum_i a_{ii}$. Непосредственно проверяется, что $\operatorname{tr}(AB) = \operatorname{tr}(BA)$ для матриц A и B одного размера. Отсюда следует, что след матрицы оператора не зависит от выбора базиса: $\operatorname{tr}(C^{-1}AC) = \operatorname{tr}(C^{-1}CA) = \operatorname{tr}(A)$. Он называется следом этого оператора.

Из [4, теоремы 8 и 9] следует, что расширения, порождённые конечным числом алгебраических элементов, — это в точности конечные расширения, т. е. расширения конечной размерности. (Кстати, это ещё один способ понять, почему $\mathbb{A}$ — поле.) Степень конечного расширения $L \supseteq K$ обозначается $[L : K]$. Итак, пусть $L \supseteq \mathbb{Q}$ — любое конечное расширение, $L \subset \mathbb{C}$. Пусть $\alpha \in L \subset \mathbb{C}$. След линейного оператора $L \to L$, $x \mapsto \alpha x$, называется следом числа α и обозначается $\operatorname{tr}^L_{\mathbb{Q}}(\alpha)$ или $\operatorname{tr}(\alpha)$, если расширение $L \supseteq \mathbb{Q}$ фиксировано.

Пример 13. Матрица умножения на $\sqrt[3]{2}$ в базисе $1, \sqrt[3]{2}, \sqrt[3]{4}$ расширения $\mathbb{Q}(\sqrt[3]{2}) \supseteq \mathbb{Q}$ есть $A = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$, так как $1 \mapsto \sqrt[3]{2} \mapsto \sqrt[3]{4} \mapsto 2$. Следовательно, $\operatorname{tr}(\sqrt[3]{2}) = \operatorname{tr} A = 0$.

Ясно, что $\operatorname{tr}(\alpha)$ линейно зависит от α. Уточним смысл множителя d в (18) и докажем формулу

$$\boxed{\operatorname{tr}(\alpha) = [L : \mathbb{Q}(\alpha)]\sigma(\alpha),\ \alpha \in L.} \tag{23}$$

Для этого выберем удобный базис в $L/\mathbb{Q}$. Сохраним обозначение (21). Тогда $1, \alpha, \ldots, \alpha^{m-1}$ — базис в $\mathbb{Q}(\alpha) \supseteq \mathbb{Q}$. Возьмём любой базис $e_1, \ldots, e_d$ в расширении $L \supseteq \mathbb{Q}(\alpha)$. По [4, теорема 9 о башне]

$$\underbrace{e_1, e_1\alpha, \ldots, e_1\alpha^{m-1}}_{\text{1-й блок}}, \ldots, \underbrace{e_d, e_d\alpha, \ldots, e_d\alpha^{m-1}}_{d\text{-й блок}}$$

— базис в $L \supseteq \mathbb{Q}$. Векторы i-го блока при умножении на α преобразуются внутри блока по правилу

$$e_i \mapsto e_i\alpha \mapsto e_i\alpha^2 \mapsto \ldots \mapsto e_i\alpha^{m-1} \mapsto e_i\alpha^m = e_i(c_0 + c_1\alpha + \ldots + c_{m-1}\alpha^{m-1}).$$

Поэтому в этом базисе матрица умножения на α блочно-диагональная с d одинаковыми блоками

$$\begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & c_0 \\ 1 & 0 & 0 & \ldots & 0 & c_1 \\ 0 & 1 & 0 & \ldots & 0 & c_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & 0 & c_{m-2} \\ 0 & 0 & 0 & \ldots & 1 & c_{m-1} \end{pmatrix}$$

и её след равен dc_{m-1}. Так как $d = [L : \mathbb{Q}(\alpha)]$ и $c_{m-1} = \sigma(\alpha)$, то формула (23) доказана. Заметим, что она также следует из (22):

$$d = \frac{n}{\deg \mu_\alpha(x)} = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = [L : \mathbb{Q}(\alpha)].$$

Поэтому два данных определения следа эквивалентны.

В заключение отметим, что $\mu_\alpha(x)$ — это минимальный многочлен оператора умножения на α, а $\mu_\alpha(x)^d$ — его характеристический многочлен.

Список литературы

[1] *Э. Б. Винберг.* Курс алгебры. МЦНМО, 2019.

[2] *Л. Камнев.* Иррациональность суммы радикалов. Квант, 1972, №2.

[3] *А. Канунников.* Алгебра и геометрия комплексных чисел. Квант, 2017, №5, 6.

[4] *А. Л. Канунников.* Алгебраические числа как векторы. // Математическое просвещение. Сер. 3. Вып. 26. М.: МЦНМО. 2020. С. 91–122.

[5] *В. Олейников.* Иррациональность и неприводимость. // Квант, 1986, №10.

[6] *В. А. Уфнаровский.* Математический аквариум. МЦНМО, 2010.

[7] *I. Richards.* An Application of Galois Theory to Elementary Arithmetic. Advances in Mathematics 13, p. 268–273. 1974.

Решения задач

1. Все три суммы радикалов иррациональны, так как в каждой из них все радикалы и их отношения иррациональны по лемме 1. Для радикала $\sqrt[17]{2021!}$ в последней сумме для этого достаточно заметить, что простое $p = 2011$, входит в разложение 2021! в первой степени.

2. а) Один набор получается из другого умножением на некоторый радикал, например, $(\sqrt{5}, \sqrt{10}, \sqrt{15}, \sqrt{30}) = \sqrt{5}(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$. б) Чтобы нарисовать гиперкуб, изобразим трёхмерный куб, поместив один квадрат внутрь другого и соединив соответственные вершины (рис. 1а). (Это вид сверху на куб, сделанный из желе и немного расплывшийся после падения на стол.) Теперь аналогично рисуем один куб внутри другого и, соединяя соответственные вершины, получаем гиперкуб. Радикалы на внутреннем кубе уже расставлены на рисунке 2б в статье. Домножая их на $\sqrt{7}$, получаем радикалы на соответственных вершинах внешнего куба.

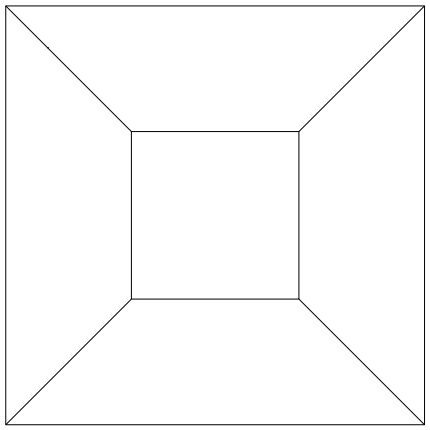


Рис. 1а

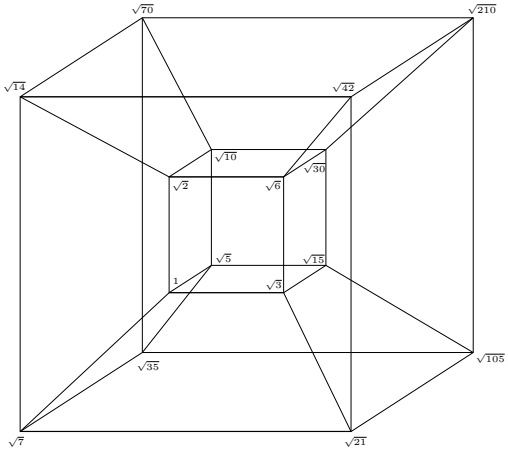


Рис 1б

3. $1 \Rightarrow 2$. Применим теорему 1 к $\{Q_1, \ldots, Q_N\} = \{r_1^{l_1} \ldots r_n^{l_n} \mid 0 \leqslant l_1, \ldots, l_n < k\}$ и $k_1 = \ldots = k_N = k$. Условие $\sqrt[k]{Q_i/Q_j} \notin \mathbb{Q}$ при $i \neq j$ верно по лемме 1.

$2 \Rightarrow 1$. Пусть $p_1, \ldots, p_n$ — простые делители числителей и знаменателей в несократимых представлениях $Q_1, \ldots, Q_N$ и $k = k_1 \ldots k_N$. Тогда $\sqrt[k_i]{Q_i} = \sqrt[k]{Q_i^{k/k_i}}$ пропорционально с рациональным коэффициентом числу вида $\sqrt[k]{p_1^{l_1} \ldots p_n^{l_n}}$, где $0 \leqslant l_1, \ldots, l_n < k$.

4. а) При нуле можно взять ненулевой коэффициент, а при пропорциональных числах kx и lx ($0 \neq k, l \in K$) — коэффициенты l и $-k$ соответственно. Взяв нулевые коэффициенты при остальных элементах системы, получим её нулевую линейную комбинацию, в которой не все коэффициенты равны 0.

б) Пусть система $x_1, \ldots, x_m, x_{m+1}, \ldots, x_n$ линейно независима над K и $a_1x_1 + \ldots + a_mx_m = 0$. Тогда из равенства $a_1x_1 + \ldots + a_mx_m + 0x_{m+1} + \ldots + 0x_n = 0$ следует, что $a_1 = \ldots = a_m = 0$.

в) Если $x \in K$, то положив в равенстве $a \cdot 1 + b \cdot x = 0$ значения $a = x$ и $b = -1$, получим, что 1 и x линейно зависимы над K. Обратно, если $x \notin K$, то из равенства $a \cdot 1 + b \cdot x = 0$, где $a, b \in K$, следует, что $b = 0$ (иначе $x = -a/b \in K$), а тогда и $a = 0$.

г) Если $a_1x_1 + \ldots + a_nx_n = b_1x_1 + \ldots + b_nx_n$, где $a_1, b_1, \ldots, a_n, b_n \in K$, то $(a_1 - b_1)x_1 + \ldots + (a_n - b_n)x_n = 0$. Линейная независимость чисел $x_1, \ldots, x_n$ равносильна равенствам $a_1 - b_1 = \ldots = a_n - b_n = 0$.

5. Пусть для $n - 1$ простых чисел теорема доказана и $\sqrt{p_n} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. Каждое число в этом поле по предположению индукции однозначно представляется в виде суммы 2^{n-1} слагаемых вида $a\sqrt{p_1}^{l_1} \ldots \sqrt{p_{n-1}}^{l_{n-1}}$, $a \in \mathbb{Q}$, $l_i = 0, 1$. Число $\sqrt{p_n}$ равно сумме чисел такого вида, но не равно ни одному из них по лемме 1. Значит, в сумме хотя бы два слагаемых, поэтому какой-то из радикалов $\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}$ в какое-то слагаемое входит, а в какое-то — нет. Пусть это радикал $\sqrt{p_{n-1}}$. Тогда $\sqrt{p_n} = A + B\sqrt{p_{n-1}}$, где $A, B \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-2}}) = K$, причём $AB \neq 0$. Возведём в квадрат: $p_n = A^2 + B^2p_{n-1} + 2AB\sqrt{p_{n-1}}$, откуда $AB = 0$ — противоречие.

6. Проблема — в определении сопряжённого числа. Внутри *каждого конкретного* поля $K(\sqrt{d})$ сопряжение определено формулой $f_d(a + b\sqrt{d}) = a - b\sqrt{d}$ $(a, b \in K)$. Это корректно: a, b определены

однозначно, так как $\sqrt{d} \notin K$. Но не обосновано приравнивание сопряжённых в разных смыслах: если $\alpha = a + b\sqrt{d} = a' + b'\sqrt{d'}$, то почему $f_d(\alpha) = a - b\sqrt{d}$ должно равняться $f_{d'}(\alpha) = a - b\sqrt{d'}$?

Можно данное определение понимать в таком смысле: если α представимо в виде $a+b\sqrt{d}$, где $a, b, d \in K$, $\sqrt{d} \notin K$, то положим сопряжённое к α равным $a - b\sqrt{d}$. Но тогда вывод

$$a + b\sqrt{d} = a' + b'\sqrt{d'} \implies a - b\sqrt{d} = a' - b'\sqrt{d'}$$

есть не что иное как проверка корректности этого определения!

Выход из положения в том, чтобы определить сопряжённое инвариантным способом, не привязанным к конкретному выражению в виде квадратичной иррациональности. Именно, пусть $\alpha \notin K$ является корнем многочлена степени 2 над K. Тогда определим сопряжённое к α как второй корень этого многочлена. Корректность такого определения сводится к очевидной проверке того, что такой многочлен определён однозначно с точностью до числового множителя. Действительно, если $x^2 + px + q$ и $x^2 + p'x + q'$ — два многочлена с корнем α над K, то их разность $(p - p')x + q - q' \in K$ тоже имеет корень α , откуда $p = p'$ (иначе $\alpha = \frac{q'-q}{p-p'} \in K$), а тогда и $q = q'$. Фактически так и вводятся сопряжённые в общей ситуации.

7. Идея — перейти к сопряжённым числам: $(a - b\sqrt{2})^2 + (c - d\sqrt{2})^2 = 7 - 5\sqrt{2} < 0$ — противоречие. Концептуальное обоснование такого перехода — проверка того, что сопряжение $f(a + b\sqrt{2}) = a - b\sqrt{2}$ $(a, b \in \mathbb{Q})$ является вложением (см. определение на с. 9).

8. Сложим данное число с сопряжённым к нему: $(6 + \sqrt{35})^{1000} + (6 - \sqrt{35})^{1000}$. Эта сумма целая (из формулы бинома Ньютона). С другой стороны, сопряжённое число очень мало:

$$(6 - \sqrt{35})^{1000} = \frac{1}{(6 + \sqrt{35})^{1000}} < \frac{1}{10^{1000}},$$

Значит, у исходного числа первые 1000 цифр после запятой — девятки.

9. Рассмотрим 2^{99} многочленов $1 + \varepsilon_2 x_2 + \ldots + \varepsilon_{100} x_{100}$, где $\varepsilon_i \in \{\pm 1\}$. Их произведение — чётный многочлен по каждой из переменных, поэтому он имеет вид $f(x_2^2, \ldots, x_{100}^2)$, где f — многочлен с целыми коэффициентами. В частности, при $x_2 = \sqrt{2}$, …, $x_{100} = \sqrt{100}$ получается целое число, обозначим его d. Повторив рассуждение с противоположными по знаку многочленами $-1 + \varepsilon_2 x_2 + \ldots + \varepsilon_{100} x_{100}$, получим то же число d (поскольку количество многочленов чётно). Значит, произведение из условия равно d^2.

10. а) $\frac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}} = \frac{1}{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}} = \frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{(1+\sqrt{2})^2-3(\sqrt{2}-1)^2} = \frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{8\sqrt{2}-6} = \frac{\left(1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}\right)(4\sqrt{2}+3)}{46}$.

б) Ответ: $\frac{1}{7}\left(3\sqrt[4]{27} + 8\sqrt[4]{9} + 5\sqrt[4]{3} + 8\right)$.

11. $m = k^5$, $n = (2021 - k)^5$, $k = 1, \ldots, 2020$. Решение аналогично примеру 7.

12. Поделим обе части на $\sqrt[3]{2}$: $\mathrm{C}\sqrt[6]{3/4} = a + b\sqrt[6]{2}$. Теперь противоречие выводится аналогично примеру 7.

13. Докажем общее утверждение.

Лемма 6. *Пусть K — подполе в $\mathbb{C}$, $r \in \mathbb{C} \setminus K$, $r^2 \in K$. Тогда все вложения $K(r) \to \mathbb{C}$ над K (т. е. тождественные на K) суть $a + br \mapsto a \pm br$.*

Доказательство. Ясно, что $K(r) = \{a + br \mid a, b \in K\}$ и что всякое вложение $\varphi\colon K(r) \to \mathbb{C}$ над K определяется значением на r. При этом $\varphi(r)^2 = \varphi(r^2) = r^2$, откуда $\varphi(r) = \pm r$. Для знака плюс получаем тождественное вложение, для знака минус — аналог комплексного сопряжения ($K = \mathbb{R}$, $r = i$): $\varphi(a+br) = a - br$. Это вложение над K: свойства $\varphi(x + y) = \varphi(x) + \varphi(y)$ и $\varphi(k) = k$ при $k \in K$ очевидны. Далее

$$\varphi((a+br)(c+dr)) = \varphi(ac+bdr^2+(ad+bc)r) = ac+bdr^2-(ad+bc)r = (a-br)(c-dr) = \varphi(a+br)\varphi(c-dr)$$

для всех $a, b, c, d \in K$. □

а) Применяем лемму 6 для $K = \mathbb{Q}$ и $r = i$; $\mathrm{tr}(1 + i) = (1 + i) + (1 - i) = 2$.

б) Обозначим $\varepsilon = \frac{1+i}{\sqrt{2}}$. Так как $\varepsilon^2 = i$, то $\mathbb{Q}(\varepsilon) = \mathbb{Q}(\varepsilon, i) = \mathbb{Q}(\sqrt{2}, i)$. При любом вложении поля $\mathbb{Q}(\sqrt{2}, i)$ имеем $\sqrt{2} \mapsto \pm\sqrt{2}$ и $i \mapsto \pm i$. Существуют 4 вложения, дающие все комбинации знаков: тождественное φ_{++}, вложения, которые даёт лемма 6,

$$\begin{aligned} &\varphi_{+-}\colon a + bi \mapsto a - bi, && a, b \in \mathbb{Q}(\sqrt{2}) \\ &\varphi_{-+}\colon a' + b'\sqrt{2} \mapsto a' - b'\sqrt{2}, && a', b' \in \mathbb{Q}(i), \end{aligned}$$

и их композиция $\varphi_{--} = \varphi_{+-} \circ \varphi_{-+}$. Отсюда $\mathrm{tr}(1 + i) = (\varphi_{++} + \varphi_{+-} + \varphi_{-+} + \varphi_{--})(1 + i) = 4$.

Заметим, что образы числа ε при всех вложениях образуют набор сопряжённых $\left\{\frac{1\pm i}{\pm\sqrt{2}}\right\} = \{\varepsilon, \varepsilon^3, \varepsilon^5, \varepsilon^7\}$ — корней многочлена $\mu_\varepsilon(x) = x^4 + 1$. Это все первообразные корни 8-й степени из 1 (рис. 2).

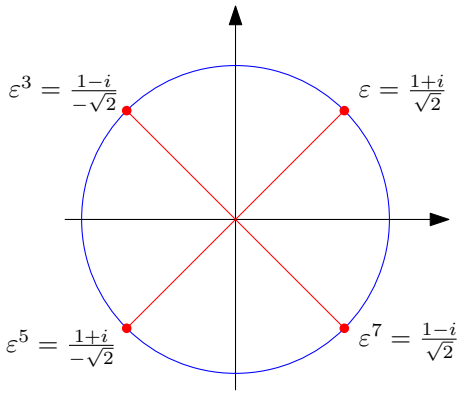


Рис. 2

14. Аналогично решению задачи 13б) получаем 4 вложения поля $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, при которых $\sqrt{2} \mapsto \pm\sqrt{2}$ и $\sqrt{3} \mapsto \pm\sqrt{3}$. Каждое из них продолжается до вложения поля $K(\sqrt{5})$ двумя способами: $\sqrt{5} \mapsto \pm\sqrt{5}$ (аналогично по лемме 6 берём три вложения, меняющие знак у одного из трёх радикалов, и составляем их всевозможные 2^3 композиций).

Опишем вложения поля $L = \mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$. Обозначим $r = \sqrt[12]{2}$. Тогда $\sqrt[4]{2} = r^3$, $\sqrt[6]{2} = r^2$ и $L = \mathbb{Q}(r^3, r^2) = \mathbb{Q}(r)$. Согласно примеру 5 $\mu_r(x) = x^6 - 2$, поэтому по теореме 3 все вложения $\varphi_0, \ldots, \varphi_5$ поля $\mathbb{Q}(r)$ определяются условиями $\varphi_j\colon r \mapsto r\varepsilon^j$, где $\varepsilon = \frac{1+i\sqrt{3}}{2} \in \sqrt[6]{1}$.