Алгебраические числа как векторы

Жюри проекта: И. Воробьёв, С. Дориченко, А. Жилина, А. Канель–Белов, А. Кануников, Б. Френкин

Введение

В геометрии мы привыкли складывать *векторы* и умножать их на *скаляры* (числа). Этот геометрический язык часто оказывается полезным в совершенно не геометрических ситуациях. В этом проекте мы рассмотрим в качестве векторов *алгебраические числа* — так называются корни многочленов с рациональными коэффициентами. Сами же рациональные числа будут выступать в роли скаляров.

Говорят, что комплексные числа $x_1, \dots, x_n$ *линейно независимы* над $\mathbb{Q}$, если равенство $a_1x_1 + \dots + a_nx_n = 0$, где $a_1, \dots, a_n \in \mathbb{Q}$, возможно только при $a_1 = \dots = a_n = 0$ (ср. с некомпланарными векторами на рисунке 1). Вообще, взгляд на алгебраические числа как на векторы оказывается очень естественным и продуктивным — он позволяет применять геометрические идеи к алгебраическим задачам.

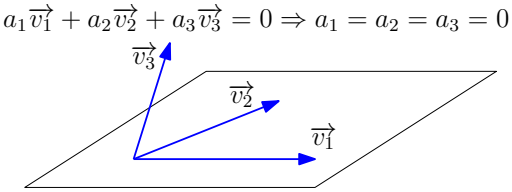


Рис. 1

Как устроен проект? Мы начнём с олимпиадных задач о радикалах для затравки. Некоторые из них можно решить школьными методами, для других нужны новые идеи и методы — начальные сведения об алгебраических числах и полях, изложенные во втором разделе. Вы научитесь удобному языку и аппарату для решения широкого круга задач. Это — предварительная часть проекта.

В третьей части мы сформулируем основную теорему проекта и предложим её доказать по приведённому плану, используя полученные знания. В заключение мы дадим исследовательскую задачу, развивающую и обобщающую теорему.

Что нужно знать заранее? Базовые факты о комплексных числах и многочленах. Главное — уметь извлекать корни из комплексных чисел и делить многочлены с остатком. Если вы мало знакомы с комплексными числами, то заведомо вам будут посильны задачи о квадратных радикалах.

Основы теории алгебраических чисел начали формироваться в трактате Карла Гаусса „Арифметические исследования“ (1801), сыгравшим огромную роль в теории чисел и подготовившим почву (наряду с работами Лагранжа) для открытий Эвариста Галуа, который установил критерий разрешимости уравнений в радикалах (1830) и заложил основы таких современных разделов алгебры, как теория групп и полей. Теория Галуа и теория полей алгераических чисел были систематизированы и разработаны во второй половине XIX и начале XX века усилиями Куммера, Кронекера, Гильберта и др.

1. Задачи для затравки

Если какие-то задачи вызовут затруднения — вернитесь к ним после раздела 2.

1.1. Докажите иррациональность следующих чисел: **а)** $\sqrt[3]{1001}$; **б)** $\sqrt{2}+\sqrt{3}+\sqrt{6}$; **в)** $\sqrt{2}+\sqrt[3]{3}$; **г)*** $\sqrt{2}+\sqrt{3}+\sqrt{5}+\sqrt{7}+\sqrt{11}$; **д)*** $\sqrt[5]{3}-\sqrt[5]{2}$; **е)**** $\sqrt{\dfrac{3}{5}+\dfrac{\sqrt[17]{2020!}}{2020}+\sqrt[5]{7^{7^7}}}$.

Если вы даже не представляете как подступиться к последнему, нарочито дикому, числу, то вот первое соображение: лучше доказывать более сильное утверждение о линейной независимости. Например, в пункте **б)** вот такое:

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=0, \text{ где } a,b,c,d\in\mathbb{Q} \implies a=b=c=d=0.$$

1.2. Найдите многочлен наименьшей степени с рациональными коэффициентами и следующим корнем: **а)** $\sqrt[3]{4}$; **б)** $\sqrt{2}+\sqrt{3}$; **в)** $\sqrt[3]{2}+\sqrt[3]{4}$; **г)*** $\sqrt[8]{8}+\sqrt[9]{9}$; **д)*** $\sqrt{6}+\sqrt{10}+\sqrt{15}$;

е) $\sqrt[3]{1+\sqrt{2}}+\sqrt[3]{1-\sqrt{2}}$; **ё)** $\sqrt[3]{7+5\sqrt{2}}+\sqrt[3]{7-5\sqrt{2}}$ (внешнее сходство обманчиво!);
ж) $\cos\frac{2\pi}{5}$; **з)** $\cos\frac{2\pi}{9}$; **и)*** $\cos\frac{2\pi}{97}$; **к)**** $\cos\frac{2\pi}{n}$ при любом $n\in\mathbb{N}$.

Если нашли многочлен, но нет уверенности, что его степень минимальна, то всё равно укажите этот многочлен. Во всех пунктах, кроме **в)**, **г)**, **и)**, **к)**, напишите многочлен в стандартном виде. Как ни странно, для решения пунктов **и)**, **к)** лучше перейти в комплексную плоскость.

1.3. Какие числа вида $\dfrac{a+bi}{a-bi}$, где $a,b\in\mathbb{Z}$, являются корнями из единицы?

Вот несколько задач на квадратичные иррациональности. В них заложена важная идея ... (обойдёмся без спойлеров).

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

1.5. Найдите первые 1000 знаков после запятой в десятичной записи числа $(6+\sqrt{37})^{1001}$.

1.6. Перемножаются все 2^{100} выражений вида

$$\pm\sqrt{1}\pm\sqrt{2}\pm\ldots\pm\sqrt{99}\pm\sqrt{100}$$

(при всех комбинациях знаков). Докажите, что результат: **а)** целое число; **б)** квадрат целого числа.

2. Немного теории: поля и алгебраические числа

Линейная независимость 1 и $\sqrt{2}$ (над $\mathbb{Q}$) означает просто иррациональность $\sqrt{2}$, известную ещё древним грекам. Увеличим число радикалов.

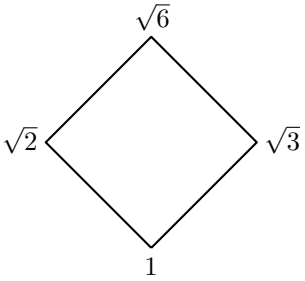


Рис. 2а

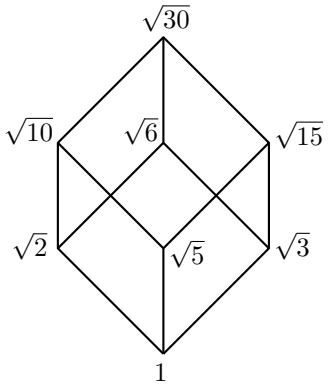


Рис. 2б

2.1. Заполните пропуски в следующем рассуждении.

Докажем, что числа $1,\sqrt{2},\sqrt{3},\sqrt{6}$ линейно независимы над $\mathbb{Q}$. Пусть

$$a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}=0,\ \text{где } a,b,c,d\in\mathbb{Q}.$$

Отделим радикал $\sqrt{3}$:

$$a+b\sqrt{2}+(c+d\sqrt{2})\sqrt{3}=0.$$

Если $c+d\sqrt{2}=0$, то _____
Если же $c+d\sqrt{2}\neq 0$, то

$$\sqrt{3}=-\frac{a+b\sqrt{2}}{c+d\sqrt{2}}=A+B\sqrt{2},\ \text{где } A=\_\_\_\_\_\in\mathbb{Q},\ B=\_\_\_\_\_\in\mathbb{Q}.$$

Завершить доказательство можно разными способами.

На разобранном примере видны некоторые идеи. Мы свели линейную независимость чисел на рисунке 2а к тому, что число $\sqrt{3}$ «инородно» 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 $\mathbb{Q}$, с помощью *избавления от иррациональности в знаменателе*.

Числовое множество, содержащее 0 и 1 и замкнутое относительно четырёх арифметических действий, называется *числовым полем*. Слово „числовое“ мы будем опускать[1]. 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 (числовое) поле его содержит. Если $K\subseteq L$ — поля, то говорят, что K — *подполе* в L.

Говорят, что система чисел[2] $x_1,\ldots,x_n\in\mathbb{C}$ *линейно независима 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 $\mathbb{R}$.

2.2. Простейшие свойства линейной зависимости. Пусть K — поле. Докажите, что:

а) система, содержащая 0 или два пропорциональных над K числа, линейно зависима над K;

б) подсистема линейно независимой системы линейно независима (над тем же полем);

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.

Присоединить к полю K *числа* $\alpha_1,\ldots,\alpha_n$ — значит взять наименьшее (по включению) поле, содержащее K и эти числа. Оно обозначается $K(\alpha_1,\ldots,\alpha_n)$.

2.3. Присоединение квадратного радикала. Пусть K — подполе в $\mathbb{R}$, $0<d\in K$ и $\sqrt{d}\notin K$ (например, $K=\mathbb{Q}$ и $d=2$). Докажите, что

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

причём числа $a,b\in K$ в записи $a+b\sqrt{d}$ определены однозначно.

2.4. Докажите, что $\mathbb{Q}(\sqrt{2}+\sqrt{3})=\mathbb{Q}(\sqrt{2},\sqrt{3})$.

2.5. Избавьтесь от иррациональности в знаменателе: $\dfrac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}}$.

2.6. а) Докажите, что числа в вершинах куба на рис. 2б линейно независимы над $\mathbb{Q}$.

б)* Добавьте ещё $\sqrt{7}$, попробуйте нарисовать гиперкуб и докажите утверждение, аналогичное пункту **а)**. А может, пора сформулировать общую теорему о квадратных радикалах из простых чисел и доказать её по индукции? В частности, из неё будет следовать решение задачи **1.1г)**.

Во что превратится определение линейной зависимости над полем K для степеней $1,\alpha,\alpha^2,\ldots,\alpha^n$ некоторого числа α? Существуют такие числа $c_0,c_1,\ldots,c_n\in K$, не все равные нулю, что

$$c_0+c_1\alpha+c_2\alpha^2+\ldots+c_n\alpha^n=0.$$

Другими словами, α является корнем ненулевого многочлена с коэффициентами из K — такое α называется *алгебраическим над* K. Среди всех таких многочленов только один имеет наименьшую степень и старший коэффициент 1 (почему?). Он называется *минимальным многочленом* числа α над K и часто обозначается $\mu_\alpha^K(x)$. Например, $\mu_i^{\mathbb{R}}(x)=x^2+1$, $\mu_i^{\mathbb{C}}(x)=x-i$. Степень $\deg\mu_\alpha^K(x)$ этого многочлена называется также *степенью* числа α над K и обозначается $\deg_K(\alpha)$. Корни многочлена $\mu_\alpha^K(x)$ называются *сопряжёнными* с α над K.

В случае $K=\mathbb{Q}$ говорят просто об алгебраических числах.

2.7. Пусть число $\alpha\in\mathbb{C}$ алгебраично над полем $K\subseteq\mathbb{C}$. Докажите:

а) $\deg_K(\alpha)$ есть наименьшее такое $n\in\mathbb{N}$, что степени $1,\alpha,\ldots,\alpha^n$ линейно зависимы над K;

б) многочлен $\mu_\alpha^K(x)$ неприводим над K (т. е. не раскладывается в произведение многочленов строго меньшей степени);

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

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

---

[1]Бывают и другие поля, например, поля вычетов, поля рациональных функций, ...

[2]Неупорядоченный набор чисел, в котором могут быть потворы.

Следующим признаком неприводимости многочлена над $\mathbb{Q}$ можно пользоваться без доказательства.

Теорема 1 (признак Эйзенштейна). *Если коэффициенты многочлена $a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ для некоторого простого p удовлетворяют условиям:*

- $p \nmid a_n$,
- $p \mid a_{n-1}, \ldots, p \mid a_0$,
- $p^2 \nmid a_0$,

то этот многочлен неприводим над $\mathbb{Q}$.

2.8. а) Завершите решение задачи **1.1д)**. Пусть $\sqrt[5]{3} - \sqrt[5]{2} = a \in \mathbb{Q}$, тогда $\sqrt[5]{3} = \sqrt[5]{2} + a$. Найдём минимальные многочлены для чисел в левой и правой частях.

б) Решите уравнение в натуральных числах: $\sqrt[5]{m} + \sqrt[5]{n} = 2020$.

Обобщим теперь задачу 2.3.

Теорема 2 (об избавлении от иррациональности в знаменателе). *Пусть число α алгебраично над полем K и имеет степень n. Тогда каждое число в поле $K(\alpha)$ однозначно записывается в виде*

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

2.9. а) Избавьтесь от иррациональности в знаменателе дроби $\dfrac{1}{\sqrt[3]{4} + \sqrt[3]{2} + 3}$. *Указание.* Здесь уже не работает пресловутое домножение на сопряжённое. Найдите такие многочлены $u(x), v(x) \in \mathbb{Q}[x]$, что $u(x)(x^2 + x + 3) + v(x)(x^3 - 2) = 1$. Для этого можно использовать либо обратный ход алгоритма Евклида, либо метод неопределённых коэффициентов.

б) Докажите теорему 2.

Согласно основной теореме алгебры, любой многочлен над $\mathbb{C}$ степени $n > 0$ имеет n корней с учётом кратности. Согласно следующей теореме, многочлен $\mu_\alpha^K(x)$ не имеет кратных корней и, тем самым, *каждое алгебраическое число степени n имеет ровно n сопряжённых (включая себя).*

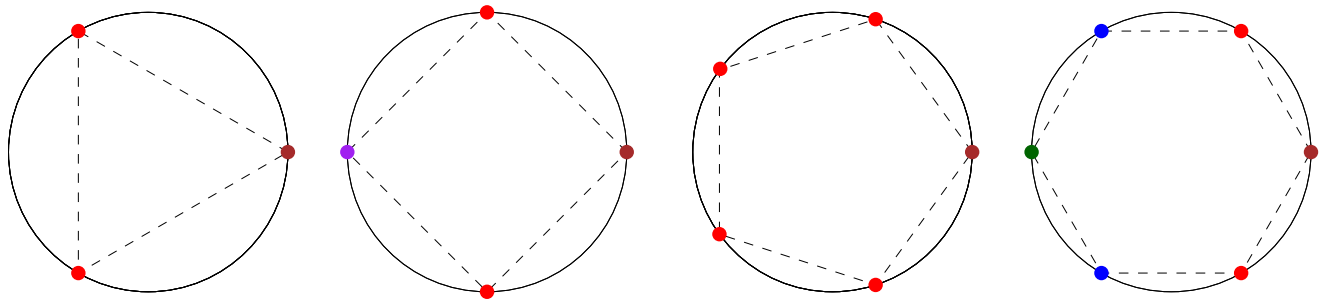
Теорема 3. *Многочлен, неприводимый над некоторым подполем в $\mathbb{C}$, не имеет кратных комплексных корней.*

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

Особого внимания заслуживают корни из единицы. Как известно, комплексные корни уравнения $x^n = 1$ имеют вид

$$1, \varepsilon_n, \varepsilon_n^2, \ldots, \varepsilon_n^{n-1}, \text{ где } \varepsilon_n = \cos\tfrac{2\pi}{n} + i\sin\tfrac{2\pi}{n}$$

(это частный случай формулы Муавра). Разобьём их на классы сопряжённых над полем $\mathbb{Q}$. Для этого нужно разложить двучлен $x^n - 1$ на неприводимые множители над $\mathbb{Q}$: корни каждого множителя образуют класс сопряжённых алгебраических чисел. Разберём примеры при малых n. На рисунке 3 неприводимые множители и их корни выделены одним цветом.



$x^3 - 1 = (x-1)(x^2+x+1)$ $\quad$ $x^4 - 1 = (x-1)(x+1)(x^2+1)$ $\quad$ $x^5 - 1 = (x-1)\times$ $\times(x^4+x^3+x^2+x+1)$ $\quad$ $x^6 - 1 = (x-1)(x+1)\times$ $\times(x^2+x+1)(x^2-x+1)$

Рис. 3

Нужно пояснить лишь неприводимость многочлена $x^4+x^3+x^2+x+1$. Вот более общий факт.

2.11. Докажите, что для любого простого p многочлен

$$\Phi_p(x) = x^{p-1} + \ldots + x + 1$$

неприводим над полем $\mathbb{Q}$. *Указание.* Используйте признак Эйзенштейна (теорема 1). Подумайте, как его применить, ведь все коэффициенты у $\Phi_p(x)$ равны 1.

2.12. Разложите двучлен $x^{12}-1$ на неприводимые над $\mathbb{Q}$ и нарисуйте картинку, аналогичную рисунку 3.

Пусть ε — корень из единицы. Его *порядком* называется наименьшее такое $n \in \mathbb{N}$, что $\varepsilon^n = 1$. Корни порядка n называются *первообразными* корнями степени n. Легко показать, что все такие корни имеют вид ε_n^k, где k взаимно просто с n. Количество чисел среди $1, \ldots, n$, взаимно простых с n, обозначается $\varphi(n)$, функция φ называется *функцией Эйлера.*

Теорема 4. *Корни степени n из единицы сопряжены над $\mathbb{Q}$, если и только если они имеют одинаковый порядок. В частности,* $\deg_{\mathbb{Q}}(\varepsilon_n) = \varphi(n)$ *для всех* $n \in \mathbb{N}$.

Эта теорема равносильна неприводимости над $\mathbb{Q}$ так называемых *круговых многочленов*

$$\Phi_n(x) = \prod_{1 \leqslant k \leqslant n, (k,n)=1} (x - \varepsilon_n^k).$$

Задача 2.11 — простой частный случай. В общем случае не сразу очевидно даже, что коэффициенты у многочлена $\Phi_n(x)$ — рациональные. Доказательство теоремы 4 в общем случае желающие смогут доказать на конференции. В любом случае ей можно пользоваться. С помощью теоремы 4 можно решить задачу 1.3 очень быстро.

Заполните пропуски в решении задачи **1.2в)**. Найдём многочлен $\mu_{\sqrt[3]{4}+\sqrt[3]{2}}(x)$ (по умолчанию — над полем $\mathbb{Q}$). Ключевая идея в том, что $\sqrt[3]{2}$ — корень многочлена $\mu_{\sqrt[3]{4}+\sqrt[3]{2}}(x^2+x)$, который, стало быть, делится на $\mu_{\sqrt[3]{2}}(x) = x^3 - 2$, а значит, имеет также корни $\sqrt[3]{2}\varepsilon$ и $\sqrt[3]{2}\varepsilon^2$, где $\varepsilon = \varepsilon_3$. Следовательно, числа $\sqrt[3]{4}+\sqrt[3]{2}$, $\sqrt[3]{4}\varepsilon^2+\sqrt[3]{2}\varepsilon$, $\sqrt[3]{4}\varepsilon+\sqrt[3]{2}\varepsilon^2$ сопряжены. Далее, они все различны (почему?). Осталось показать, что многочлен

$$\bigl(x - \sqrt[3]{4} - \sqrt[3]{2}\bigr)\bigl(x - \sqrt[3]{4}\varepsilon^2 - \sqrt[3]{2}\varepsilon\bigr)\bigl(x - \sqrt[3]{4}\varepsilon - \sqrt[3]{2}\varepsilon^2\bigr)$$

имеет рациональные коэффициенты — тогда он и будет $\mu_{\sqrt[3]{4}+\sqrt[3]{2}}(x)$. Покажите это.

Обобщением этого рассуждения является следующая теорема — одна из главных в проекте.

Теорема 5. *Если $\alpha = \alpha_1, \ldots, \alpha_n$ — все сопряжённые с числом α над полем K, то для любого многочлена $f(x) \in K[x]$ число $f(\alpha)$ алгебраично над K и его сопряжённые суть $f(\alpha_1), \ldots, f(\alpha_n)$, причём в этом списке могут быть повторы и тогда каждый элемент встречается одно и то же число раз.*

2.13. Докажите теорему 5: **а)** в случае, когда α — корень неприводимого двучлена; **б)** в общем случае. (Для исследования линейной независимости радикалов достаточно пункта **а)**, который проще. В пункте **б)** можно использовать основную теорему о симметрических многочленах.)

Вот план доказательства.

1) Чтобы доказать, что $f(\alpha)$ алгебраично и его сопряжённые находятся среди чисел $f(\alpha_1), \ldots, f(\alpha_n)$, рассмотрите многочлен

$$F(x) = (x - f(\alpha_1)) \ldots (x - f(\alpha_n))$$

и докажите, что $F(x) \in K[x]$.

2) Чтобы доказать, что все числа $f(\alpha_1), \ldots, f(\alpha_n)$ сопряжены над K, рассмотрите многочлен $\mu_{f(\alpha)} f(x)$.

3) Докажите, что все корни многочлена $F(x)$ имеют одинаковую кратность, рассмотрев многочлен $F(x)/\mu_{f(\alpha)}(x)$.

2.14. Найдите все $n \in \mathbb{N}$, при которых число $\cos\frac{2\pi}{n}$: **а)** рационально; **б)** представляется в виде $a + \sqrt{b}$, где $a, b \in \mathbb{Q}$, т. е. $\deg_{\mathbb{Q}}\left(\cos\frac{2\pi}{n}\right) \leqslant 2$.

3. Построение правильных многоугольников

Подумайте, как решить задачу **1.2з)** с помощью теорем 4 и 5. Эта задача — ключевая в доказательстве части «только если» теоремы Гаусса–Ванцеля: *правильный n-угольник строится циркулем и линейкой, если и только если $\varphi(n)$ — степень двойки, т. е. если n — произведение степени двойки и простых чисел Ферма.* Числа Ферма — это числа вида $2^{2^k}+1$. Первые 5 из этих чисел простые: $3, 5, 17, 257, 65537$.

3.1. Постройте с помощью циркуля и линейки правильные: **а)** 5-угольник; **б)** 17-угольник.

3.2. Разработайте алгоритм и напишите программу на компьютере для построения правильного p-угольника при: **а)** $p = 17$; **б)** $p = 257$; **в)** $p = 65537$.

Гаусс построил правильный 17-угольник и доказал, что для любого простого числа Ферма p правильный p-угольник можно построить. Этот случай (пункт а)) не оценивается отдельно, но представляет собой важную ступеньку, и мы рекомендуем разобрать его как вручную, так и с помощью компьютерной программы.

Правильный 257-угольник был построен Ришело в XIX веке; в XXI веке вычисления лучше поручить компьютеру. Программа для $p = 257$ будет оценена отдельным дипломом. Программа для $p = 65537$ будет новым результатом и может быть подана в научный журнал.

3.3. Постройте с помощью циркуля, линейки и трисектора (прибора, делящего угол на три равных угла) корни многочленов: **а)** $8x^3 - 6x + 1$; **б)** $512x^9 - 1152x^7 + 864x^5 - 240x^3 + 18x + 1$. (Это связано с 9- и 27-угольниками.)

3.4. Найдите все простые p, для которых существует единственное $a \in \{1, \ldots, p-1\}$ с условием $p \mid a^3 - 3a + 1$.

3.5. Постройте с помощью циркуля, линейки и трисектора правильные: **а)** 7-угольник; **б)** 13-угольник.

“Один слишком навязчивый аспирант довёл своего руководителя до того, что тот сказал ему: “Идите и разработайте построение правильного многоугольника с 65537 сторонами”. Аспирант удалился, чтобы вернуться через 20 лет с соответствующим построением” (Дж. Литвуд, “Математическая смесь”) А рукопись И. Г. Гермеса, написанная в 1894 г. в результате более чем десятилетних исследований и содержащая построение правильного 65537-угольника, хранится в библиотеке Гёттингенского университета и содержит больше 200 страниц. Но сейчас с помощью компьютера можно добиться этого результата за значительно меньшее время.

4. Линейная независимость радикалов

Теорема 6. *Пусть $N, k_1, \ldots, k_N \in \mathbb{N}$, $N > 1$, $Q_1, \ldots, Q_N \in \mathbb{Q}_+$, причём $\sqrt[k_i]{Q_i} / \sqrt[k_j]{Q_j} \notin \mathbb{Q}$ при всех $i \neq j$. 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 $a_1 \in \mathbb{Q}$.

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

Лемма 1. *Для всех $k \in \mathbb{N}$ и $Q \in \mathbb{Q}_+$ имеем: $\sqrt[k]{Q} \in \mathbb{Q}$, если и только если показатели всех простых делителей числителя и знаменателя в несократимом представлении Q кратны k.*

4.1. Докажите лемму 1.

4.2. Выведите из теоремы 6 и леммы 1 иррациональность чисел из задачи 1.1.

Не умаляя общности, в теореме 6 можно считать все числа Q_i натуральными, а все показатели k_i равными, и доказывать тем самым следующую равносильную теорему.

Теорема 7. *Пусть $k, n \in \mathbb{N}$, $p_1, \ldots, p_n$ — различные простые числа, $r_i = \sqrt[k]{p_i}$ при $i = 1, \ldots, n$. 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 рисунках 2 и 4.

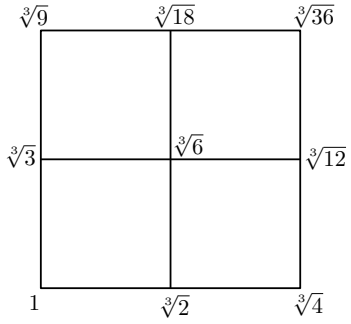


Рис. 4

4.3. Выведите теоремы 6 и 7 друг из друга.

4.4. Как в задаче 2.6, сведите теорему 7 при $k = 2$ к следующему утверждению и докажите его:

$$\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}}).$$

(Рекомендуем использовать переход к сопряжённым числам — так проще понять случай $k > 2$.)

4.5. Докажите, что теорема 7 равносильна **теореме 7′**: *в обозначениях теоремы 7 степени $1, r_n, \ldots, r_n^{k-1}$ линейно независимы над полем $\mathbb{Q}(r_1, \ldots, r_{n-1})$.*

4.6. Пусть K — подполе в $\mathbb{R}$, $r \in \mathbb{R}$, $r^k \in K$ и $r, \ldots, r^{k-1} \notin K$. Докажите, что двучлен $x^k - r^k$ неприводим над K и степени $1, r, \ldots, r^{k-1}$ линейно независимы над K.

Таким образом, теорема 7′ сведена к следующей **теореме 7″**: *в тех же обозначениях*

$$r_n^l \notin \mathbb{Q}(r_1, \ldots, r_{n-1}) \text{ ни для какого } l \in \{1, \ldots, k-1\}.$$

Предположим противное. По предположению индукции каждое число из поля $\mathbb{Q}(r_1, \ldots, r_{n-1})$ однозначно представляется в виде суммы произведений вида $ar_1^{l_1} \ldots r_{n-1}^{l_{n-1}}$, где $a \in \mathbb{Q}$ и все $l_i \in \{0, \ldots, k-1\}$.

4.7. Получите противоречие, если в этой сумме ровно одно слагаемое.

Если в этой сумме хотя бы два слагаемых, то с точностью до перестановки радикалов $r_1, \ldots, r_{n-1}$ можно считать, что

$$r_n^l = A_0 + A_1 r_{n-1} + \ldots + A_{k-1} r_{n-1}^{k-1}, \text{ где } A_0, \ldots, A_{k-1} \in \mathbb{Q}(r_1, \ldots, r_{n-2}), \tag{1}$$

где среди $A_0, \ldots, A_{k-1}$ хотя бы два ненулевых.

4.8. а) Докажите, что $A_0 = 0$.

б) Пусть A_j — первый ненулевой коэффициент в (1). Придите к противоречию, доказав, что $A_j = 0$ (подумайте, как свести задачу к предыдущему пункту). Это завершает доказательство теоремы 7.

4.9. Остаётся ли теорема 7 в силе, если под каждым r_j $(j = 1, \ldots, n)$ понимать некоторое комплексное значение корня $\sqrt[k]{p_j}$?

5. Размерности расширений полей

Для более глубокого понимания алгебраических чисел и решения более трудных задач мы познакомимся с понятием векторного пространства, его размерности и освоим технику расширений полей (всё — для числовых множеств).

Подмножество $V \subseteq \mathbb{C}$, содержащее поле K, называется *векторным пространством над K*, а его элементы — *векторами*, если V замкнуто относительно умножения на числа из K и сложения,

т. е. $a+b, ka \in V$ для любых $a, b \in V$ и $k \in K$. Например, всякое поле является векторным пространством над любым своим подполем.

Предположим, что пространство $V \subseteq \mathbb{C}$ над полем K содержит такие числа $e_1, \ldots, e_n$, что всякое $\alpha \in V$ представляется в виде

$$\alpha = k_1 e_1 + \ldots + k_n e_n \tag{2}$$

с однозначно определёнными коэффициентами $k_1, \ldots, k_n \in K$. Тогда система $e_1, \ldots, e_n$ называется *базисом* пространства V над K, а равенство (2) — *разложением* числа α по этому базису.

5.1. Докажите, что базис пространства можно определить равносильным образом как максимальную по включению линейно независимую систему векторов. Иными словами, система $e_1, \ldots, e_n$ — базис в V над K, если и только если она линейно независима над K, а система $e_1, \ldots, e_n, \alpha$ линейно зависима над K для любого $\alpha \in V$.

Пространство, обладающее конечным базисом, называется конечномерным, а расширение поля, обладающее конечным базисом, называют *конечным*. Число элементов в базисе пространства V над K называется его *размерностью* и обозначается $\dim_K L$. Корректность этого определения, т. е. независимость от выбора базиса, вытекает из следующей леммы.

Лемма 2 (основная лемма о линейной зависимости)**.** *Если числа $f_1, \ldots, f_m$ линейно выражаются над полем K через числа $e_1, \ldots, e_n$ и $m > n$, то числа $f_1, \ldots, f_m$ линейно зависимы над K.*

Пусть $U \subseteq W$ — конечномерные пространства над полем K. Несложно проверить, что всякий базис в U можно дополнить до базиса в V. Тем самым, $\dim_K U \leqslant \dim_K V$ и $\dim_K U = \dim_K V \Leftrightarrow U = V$.

Если K — подполе поля L, то говорят о расширении полей L/K. Очевидно, в этом случае L — векторное пространство над K. Размерность конечного расширения L/K называется также его *степенью* и обозначается $[L : K]$.

5.2. Пусть L/K — конечное расширение. Докажите, что $[L : K] = 2 \Leftrightarrow L = K(\alpha)$ для некоторого такого $\alpha \in L \setminus K$, что $\alpha^2 \in K$.

5.3. Докажите, что числа $1, \alpha, \ldots, \alpha^{n-1}$ образуют базис расширения $K(\alpha)/K$, если и только если число α алгебраично над K и имеет степень n. Итак, если α алгебраично над K, то $\deg_K(\alpha) = [K(\alpha) : K]$.

Полезный инструмент в теории конечных расширений — следующая теорема (докажите её).

Теорема 8 (о размерности башни)**.** *Если $K \subseteq P \subseteq L$ — конечные расширения полей, то*

$$\boxed{\dim_K L = \dim_K P \cdot \dim_P L.}$$

Ср. со свойством логарифмов $\log_a c = \log_a b \cdot \log_b c$.

Вернитесь к задаче для затравки **1.1в)**.

5.4. Найдите все подполя в полях: **а)** $\mathbb{Q}(\sqrt[11]{1024})$; **б)** $\mathbb{Q}(\sqrt[4]{3})$; **в)** $\mathbb{Q}(\varepsilon_5)$; **г)** $\mathbb{Q}(\varepsilon_8)$.

5.5*. Обозначим $\varepsilon = \varepsilon_{17}$. Из теоремы 2 и задачи 2.11 следует, что $\deg(\varepsilon) = 16$.

а) Найдите все $\alpha \in \mathbb{Q}(\varepsilon)$, для которых $\deg(\alpha) = 2, 4, 8$. *Указание:* воспользуйтесь теоремой 5, рассмотрев базис $\varepsilon, \varepsilon^3, \varepsilon^{3^2}, \ldots, \varepsilon^{3^{15}}$ в $\mathbb{Q}(\varepsilon)$ над $\mathbb{Q}$ (докажите, что это базис). Это упорядочение принадлежит Гауссу.

5.6. Найдите все сопряжённые над $\mathbb{Q}$ к числам: **а)** $\sqrt{6} + \sqrt{10} + \sqrt{15}$; **б)** $\sqrt[3]{2} + \sqrt[3]{3}$.

б) Пусть $U_k = \{\alpha \in \mathbb{Q}(\varepsilon) \mid \deg(\alpha) \text{ делит } k\}$, $k = 1, 2, 4, 8, 16$. В частности, $U_1 = \mathbb{Q}$ и $U_{16} = \mathbb{Q}(\alpha)$. Докажите, что $U_1 \subset U_2 \subset U_4 \subset U_8 \subset U_{16}$ — цепочка квадратичных расширений полей. Таким способом можно построить правильный 17-угольник с помощью циркуля и линейки (открытие Гаусса).

Исследовательская задача. Какие правильные n-угольники можно построить с помощью циркуля, линейки и трисектора? Частные случаи: $n = 7, 13, 19, 37$.

Исследовательская задача. Разработайте алгоритм нахождения степени любого алгебраического числа из расширения $\mathbb{Q}\left(\sqrt[k]{p_1}, \ldots, \sqrt[k]{p_n}\right)$, где $p_1, \ldots, p_n$ — различные простые числа. Частные случаи: $k = 2$; k — простое.