Наш семинар: математические сюжеты

Алгебраические числа как векторы

А. Л. Канунников

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

Для понимания статьи понадобятся начальные сведения о комплексных числах и многочленах (главное — уметь извлекать корни из комплексных чисел и делить многочлены с остатком). Рекомендуем по ходу чтения решать задачи, в конце статьи к ним приведены решения.

§ 1. Линейная независимость чисел

Начнём с простого примера. Как известно со времён древних греков, число $\sqrt{2}$ иррационально. Геометрически это можно сформулировать так: *«векторы» 1 и $\sqrt{2}$ не пропорциональны ни с каким рациональным коэффициентом*. Давайте тогда *натянем* на эти векторы «плоскость» — множество $\mathbb{Q}+\mathbb{Q}\sqrt{2}=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ (рис. 1). По любому «вектору» $a+b\sqrt{2}$ его «коэффициенты» a и b (если угодно, абсцисса и ордината) восстанавливаются однозначно: если $a+b\sqrt{2}=a'+b'\sqrt{2}$, $a,b,a',b'\in\mathbb{Q}$, то $a-a'=(b'-b)\sqrt{2}$, откуда $b'=b$ (иначе $\sqrt{2}=\frac{a-a'}{b'-b}\in\mathbb{Q}$), а тогда и $a=a'$.

При поддержке Московского центра фундаментальной и прикладной математики, грант «Структурная теория и комбинаторно-логические методы в теории алгебраических систем».

Замечание. Плоскость на рис. 1 отличается от обычной евклидовой плоскости, во-первых, тем, что координаты на ней рациональные (а не любые действительные), а во-вторых, тем, что на ней нет длин и углов.

Понятно, что вместо $\sqrt{2}$ можно взять любое иррациональное число. Возьмём $\sqrt[3]{2}$ и рассмотрим плоскость $\mathbb{Q}+\mathbb{Q}\sqrt[3]{2}$. Интуитивно очевидно, что число $\sqrt[3]{4}$ не лежит в этой плоскости, т. е. *векторы* 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ *некомпланарны*: равенство

$$\sqrt[3]{4}=a+b\sqrt[3]{2} \qquad (1)$$

не выполняется ни при каких $a, b\in\mathbb{Q}$.

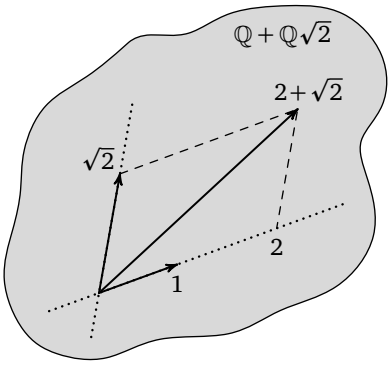

Рис. 1

Задача 1. Докажите это строго.

Понятия пропорциональности (коллинеарности) и компланарности обобщаются до понятия *линейной зависимости* любого количества векторов. Дадим соответствующее определение для чисел.

Определение 1. Система комплексных чисел $v_1, \ldots, v_n$ называется *линейно зависимой над* $\mathbb{Q}$, если $c_1v_1+\ldots+c_nv_n=0$ для некоторых рациональных $c_1, \ldots, c_n$, среди которых хотя бы одно отлично от нуля. В противном случае система $v_1, \ldots, v_n$ называется *линейно независимой над* $\mathbb{Q}$.

Замечания. Подчеркнём, что линейная зависимость или независимость — это свойство именно *системы*[1)] чисел (векторов), хотя часто говорят «векторы линейно зависимы».

Отметим простейшие свойства, сразу вытекающие из определения (проверьте их):

- система, содержащая нуль или два одинаковых числа, линейно зависима;
- система из одного числа линейно зависима в точности тогда, когда это число — нуль;
- подсистема линейно независимой системы линейно независима;
- система чисел линейно зависима в точности тогда, когда хотя бы одно из них *линейно выражается* через остальные (например, если $c_n\neq 0$ в определении 1, то $v_n=-\frac{c_1}{c_n}v_1-\ldots-\frac{c_{n-1}}{c_n}v_{n-1}$).

[1)] Свойство именно «футбольной команды», а не «каждого игрока в отдельности» (А. В. Михалёв).

Задача 2 (для решения понадобится материал статьи). В качестве затравки предлагаем доказать линейную независимость следующих систем чисел:

а) $1, \sqrt[10]{2}, \sqrt[10]{4}, \sqrt[10]{8}, \sqrt[10]{16}, \ldots, \sqrt[10]{512}$;

б) $1, \sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \ldots, \sqrt[100]{2}$;

в) $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \sqrt{11}, \sqrt{13}, \ldots, \sqrt{991}, \sqrt{997}$ (под радикалами — простые числа);

г) $1, \sqrt[3]{5}, \sqrt[3]{25}, \sqrt[5]{3}, \sqrt[5]{9}, \sqrt[5]{27}, \sqrt[5]{81}$;

д) $\cos\frac{2\pi}{17}, \cos\frac{4\pi}{17}, \cos\frac{6\pi}{17}, \ldots, \cos\frac{16\pi}{17}$.

§ 2. Алгебраические числа

Во что превратится определение 1 линейной зависимости для степеней $1, \alpha, \alpha^2, \ldots, \alpha^n$ некоторого числа α? Существуют такие рациональные числа $c_0, c_1, \ldots, c_n$, 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 рациональными коэффициентами. Такие числа называются *алгебраическими*.

Множество всех алгебраических чисел обозначается буквой $\mathbb{A}$. Очевидно, $\mathbb{Q} \subset \mathbb{A}$, $i \in \mathbb{A}$ ($i^2 = -1$), $\sqrt[5]{2} \in \mathbb{A}$. Приведём пару примеров посложнее.

Пример 1. Покажем, что $\alpha = \sqrt{2} + \sqrt{3} \in \mathbb{A}$. Дважды возведём в квадрат: $\alpha^2 = 5 + 2\sqrt{6} \Rightarrow (\alpha^2 - 5)^2 = 24$, т. е. α — корень многочлена $(x^2-5)^2 - 24 = x^4 - 10x^2 + 1$.

Пример 2. Число $c = \cos\frac{2\pi}{9}$ алгебраическое, так как по формуле косинуса тройного угла $4c^3 - 3c = \cos\frac{2\pi}{3} = -\frac{1}{2}$.

Существование неалгебраических или *трансцендентных* чисел можно вывести из соображений мощности: ненулевых многочленов с рациональными коэффициентами — счётное множество, и у каждого — конечное число корней, поэтому множество $\mathbb{A}$ счётно, в то время как множество $\mathbb{C}$ континуально. Это простое, с сегодняшней высоты, рассуждение появилось лишь после первых работ Кантора по теории множеств в 1870-х годах. Первое же доказательство было получено раньше совсем из других соображений: в 1844 году Лиувилль доказал, что алгебраические числа «плохо» (в некотором смысле) приближаются рациональными, и, используя это, построил примеры трансцендентных чисел. Вот одно из них: $\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$ (см. [2, 5, 8]). Позднее была доказана трансцендент-

ность чисел e (Эрмит, 1873), π (Линдеман, 1882), e^π (Гельфонд, 1929). Однако до сих пор никто не знает, являются ли числа $e \pm \pi$, $e\pi$, e/π хотя бы иррациональными!

Среди всех ненулевых многочленов над $\mathbb{Q}$ с корнем $\alpha \in \mathbb{A}$ существует единственный многочлен наименьшей степени со старшим коэффициентом 1: если бы их было два, то их разность была бы многочленом меньшей степени с корнем α.

Определение 2. Указанный многочлен называется *минимальным многочленом числа* α и часто обозначается $\mu_\alpha(x)$, а его степень называется *степенью* числа α и обозначается $\deg \alpha$.

Алгебраические числа степени 1 — это в точности рациональные числа: $\deg \alpha = 1 \iff \mu_\alpha(x) = x - \alpha \iff \alpha \in \mathbb{Q}$. Алгебраические числа степени 2 называются *квадратичными иррациональностями*. Примеры: $\sqrt{2}$, i, $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$. Если $\deg \alpha = 2$, то $\alpha^2 = p\alpha + q$ для некоторых $p, q \in \mathbb{Q}$, но $\alpha \notin \mathbb{Q}$. Иными словами, числа $1, \alpha, \alpha^2$ линейно зависимы, а числа $1, \alpha$ линейно независимы над $\mathbb{Q}$. Вообще, геометрически

$$\deg \alpha \text{ — это такое наименьшее } n \in \mathbb{N},$$
$$\text{что числа } 1, \alpha, \alpha^2, \ldots, \alpha^n \text{ линейно зависимы над } \mathbb{Q}.$$

В задаче 1 фактически предлагается доказать, что $\deg \sqrt[3]{2} = 3$, а в задаче 2а — что $\deg \sqrt[10]{2} = 10$. Казалось бы, очевидно, что $\deg \sqrt[n]{2} = n$ для всех $n \in \mathbb{N}$, но для аккуратного доказательства нужно убедиться, что $\mu_{\sqrt[n]{2}}(x) = x^n - 2$. Почему это может быть не так? Вдруг двучлен $x^n - 2$ приводим над $\mathbb{Q}$, т. е. раскладывается в произведение многочленов степеней $< n$ с рациональными коэффициентами? Тогда $\sqrt[n]{2}$ является корнем одного из сомножителей. Можно ещё допустить, что двучлен $x^n - 2$ неприводим над $\mathbb{Q}$, но всё равно существует другой многочлен над $\mathbb{Q}$ степени $< n$ с корнем $\sqrt[n]{2}$… Подобные вопросы осмысленны для любого алгебраического числа α, и, чтобы в них разобраться, нужно знать два главных свойства минимального многочлена.

$$\text{Многочлен } \mu_\alpha \text{ неприводим над } \mathbb{Q}. \tag{2}$$

В самом деле, если многочлен μ_α раскладывается в произведение многочленов над $\mathbb{Q}$ меньшей степени, то α — корень одного из сомножителей, что противоречит минимальности $\deg \mu_\alpha$.

$$\text{Любой многочлен } f \in \mathbb{Q}[x] \text{ с корнем } \alpha \text{ делится на } \mu_\alpha. \tag{3}$$

Для доказательства поделим с остатком: $f = \mu_\alpha q + r$, где $q, r \in \mathbb{Q}[x]$ и либо $r = 0$, либо $\deg r < \deg \mu_\alpha$. Вторая возможность исключается, так как $r(\alpha) = f(\alpha) - \mu_\alpha(\alpha) q(\alpha) = 0$.

Из (2) и (3) следует, что *если мы нашли неприводимый над* $\mathbb{Q}$ *многочлен с корнем* α *и старшим коэффициентом* 1, *то это и есть* μ_α.

Вернёмся к радикалам. Равенство $\deg \sqrt[n]{2} = n$, как мы поняли, равносильно неприводимости двучлена $x^n - 2$. Как её доказать? Существует ли вообще алгоритм разложения данного многочлена на неприводимые над Q? Да, такой алгоритм был разработан Кронекером в XIX веке, но он трудоёмкий. Сформулируем один полезный признак неприводимости.

Теорема 1 (признак Эйзенштейна [6]). *Если коэффициенты многочлена* $a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *для некоторого простого* p *удовлетворяют условиям*: $p \nmid a_n$, $p \mid a_{n-1}, \ldots, a_0$, $p^2 \nmid a_0$, *то он неприводим над* $\mathbb{Q}$.

Пример 3 (неприводимость некоторых двучленов). а) Двучлен $x^n - 2$ неприводим по признаку Эйзенштейна. Этот признак применим вообще к двучленам $x^n \pm p_1 \ldots p_k$, где $p_1, \ldots, p_k$ — различные простые числа.

б) Но, скажем, к двучлену $x^3 - 4$ признак Эйзенштейна неприменим. Зато *для кубического* (*и квадратного*) *многочлена неприводимость над* $\mathbb{Q}$ *равносильна отсутствию рациональных корней*. А их можно найти перебором: *если несократимая дробь* m/n *является корнем многочлена*

$$f(x) = a_k x^k + \ldots + a_0 \in \mathbb{Z}[x],$$

где $a_k, a_0 \neq 0$, *то* $m \mid a_0$ *и* $n \mid a_k$ (*в частности, при* $a_k = 1$ *все рациональные корни — целые*), см., например, [1, глава 3, § 6]. Отсюда следует, что двучлен $x^3 - 4$ неприводим над $\mathbb{Q}$, а значит, $\deg \sqrt[3]{4} = 3$.

в) Пойдём дальше. Двучлен $x^5 - 4$ тоже не имеет рациональных корней, однако этого уже недостаточно для неприводимости: вдруг он раскладывается на множители степеней 2 и 3? Чтобы это опровергнуть, можно выйти в комплексную плоскость и разложить этот двучлен на линейные множители:

$$x^5 - 4 = \left(x - \sqrt[5]{4}\right)\left(x - \omega \sqrt[5]{4}\right)\left(x - \omega^2 \sqrt[5]{4}\right)\left(x - \omega^3 \sqrt[5]{4}\right)\left(x - \omega^4 \sqrt[5]{4}\right),$$

где $\omega = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$. Отсюда следует, что любой квадратный множитель двучлена $x^5 - 4$ со старшим коэффициентом 1 имеет свободный член вида $\omega^k \sqrt[5]{16}$ ($k \in \mathbb{Z}$), модуль которого $\sqrt[5]{16}$ иррационален (почему?).

Приведём другое изящное рассуждение. Двучлен $x^5 - 4$ неприводим $\Leftrightarrow$ $\deg \sqrt[5]{4} = 5$ $\Leftrightarrow$ $1, \sqrt[5]{4}, \sqrt[5]{4^2}, \sqrt[5]{4^3}, \sqrt[5]{4^4}$ линейно независимы над $\mathbb{Q}$. Но

Число α	Многочлен $\mu_\alpha(x)$
$\alpha \in \mathbb{Q}$	$x - \alpha$
$\sqrt[n]{2}$	$x^n - 2$
i	$x^2 + 1$
$\sqrt{2} + \sqrt{3}$	$x^4 - 10x^2 + 1$
$\cos \frac{2\pi}{9}$	$4x^3 - 3x + \frac{1}{2}$

Рис. 2

это просто переставленные числа $1, \sqrt[5]{2}, \sqrt[5]{2^2}, \sqrt[5]{2^3}, \sqrt[5]{2^4}$ с целыми коэффициентами, а их линейная независимость нам уже известна: она равносильна неприводимости двучлена $x^5 - 2$.

Задача 3. Обобщите рассуждение из примера 3в). Именно, пусть двучлен $x^n - r^n$ неприводим над $\mathbb{Q}$. Докажите, что n — наименьшее натуральное число со свойством $r^n \in \mathbb{Q}$. Верно ли обратное в случае: а) $r \in \mathbb{R}$; б) $r \in \mathbb{C}$?

Задача 4. Установите критерий неприводимости двучлена $x^n - a \in \mathbb{Q}[x]$ в случаях: а) $a > 0$ или n нечётно; б) $a < 0$, $n = 4$; в)** $a < 0$, $n = 2^s$, $s \geqslant 2$; г)** $a < 0$.

Задача 5. Найдите многочлен $\mu_\alpha(x)$ для а) $\alpha = \sqrt[3]{1 + \sqrt{2}} + \sqrt[3]{1 - \sqrt{2}}$; б) $\alpha = \sqrt[3]{7 + 5\sqrt{2}} + \sqrt[3]{7 - 5\sqrt{2}}$ (значения корней — арифметические). (Внеш-

нее сходство обманчиво!) Для этого составьте кубический многочлен, имея перед глазами формулу Кардано [1, глава 3, § 9] для его корня.

Задача 6. Докажите, что все комплексные значения корня любой степени из алгебраического числа алгебраичны.

Мы завершим этот параграф двумя естественными вопросами об алгебраических числах.

Q1 *Верно ли, что сумма, разность, произведение и отношение алгебраических чисел являются алгебраическими числами*?

Ответ положительный, см. далее теорему 4.

Q2 *С учётом задачи* 6 *всякое число, получаемое из рациональных с помощью арифметических операций и извлечения корня, алгебраично. Вопрос*: *всякое ли алгебраическое число получается таким способом, т. е. выражается в радикалах*?

Отрицательный ответ был великим открытием первой половины XIX века. Ответ дал замечательный французский математик Эварист Галуа, когда ему не было 20 лет! На самом деле он установил критерий разрешимости уравнений в радикалах. Отметим, что привести пример конкретного многочлена над $\mathbb{Q}$, корни которого не выражаются в радикалах, с полным доказательством не так просто. Например, подойдёт многочлен $x^5 - 4x + 2$.

§ 3. Избавление от иррациональности в знаменателе

Этот известный со школы сюжет тесно связан с алгебраическими числами. С квадратичными иррациональностями всё просто — для избавления от иррациональности в знаменателе достаточно умножить на сопряжённое число, например:

$$\frac{1}{\sqrt{2}-1} = \sqrt{2}+1, \quad \frac{1}{\sqrt{7}-\sqrt{3}} = \frac{\sqrt{7}+\sqrt{3}}{4}.$$

Но уже с кубическими корнями дело обстоит гораздо сложнее.

Пример 4. Избавимся от иррациональности в знаменателях:

$$\text{а)}\ \frac{1}{\sqrt[3]{4}-\sqrt[3]{2}-2}; \quad \text{б)}\ \frac{1}{\sqrt[3]{4}+\sqrt[3]{2}+3}.$$

В пункте а) ещё можно схитрить, разложив знаменатель на множители:

$$\frac{1}{\sqrt[3]{4}-\sqrt[3]{2}-2} = -\frac{(2+1)(2-2^3)}{18(\sqrt[3]{2}+1)(\sqrt[3]{2}-2)} = -\frac{(\sqrt[3]{4}-\sqrt[3]{2}+1)(\sqrt[3]{4}+2\sqrt[3]{2}+4)}{18},$$

но в пункте б) аналогичный приём приведёт к новым иррациональностям, к тому же мнимым. Покажем на этом примере, как действовать, когда в знаменателе стоит многочлен от одной иррациональности. В нашем случае это $\alpha^2+\alpha+3$, где $\alpha=\sqrt[3]{2}$. Надо представить дробь $1/(\alpha^2+\alpha+3)$ в виде многочлена от α, т. е. найти такой многочлен $u(x)\in\mathbb{Q}[x]$, что

$$\frac{1}{\alpha^2+\alpha+3}=u(\alpha).$$

Это значит, что многочлен $(x^2+x+3)u(x)-1$ имеет корень α, т. е., в силу (3), делится на $\mu_\alpha(x)=x^3-2$. Таким образом, для некоторого многочлена $v(x)\in\mathbb{Q}[x]$ имеем:

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

Но это не что иное как линейное представление наибольшего общего делителя многочленов x^2+x+3 и x^3-2.

Задача 7. Найдите многочлены $u(x)$ и $v(x)$ либо по алгоритму Евклида, либо методом неопределённых коэффициентов в предположении $\deg u<3$, $\deg v<2$.

Решив задачу 7, получим:

$$(2x^2+x-7)(x^2+x+3)-(2x+3)(x^3-2)=-15 \quad\Rightarrow\quad \frac{1}{\alpha^2+\alpha+3}=-\frac{2\alpha^2+\alpha-7}{15}.$$

Прежде чем обобщить этот пример, введём для данного числа $\alpha\in\mathbb{C}$ множества

$$\begin{aligned}&\mathbb{Q}[\alpha]=\{f(\alpha)\mid f\in\mathbb{Q}[x]\},\\&\mathbb{Q}(\alpha)=\{f(\alpha)/g(\alpha)\mid f,g\in\mathbb{Q}[x],\ g(\alpha)\neq 0\}.\end{aligned}\tag{4}$$

Очевидно, $\mathbb{Q}[\alpha]$ замкнуто относительно сложения, вычитания и умножения, а $\mathbb{Q}(\alpha)$ — ещё и относительно деления (на ненулевые числа), причём это наименьшие множества с такими свойствами, содержащие $\mathbb{Q}$ и α. Возможность избавляться от иррациональности в знаменателях дробей из $\mathbb{Q}(\alpha)$ формально означает равенство $\mathbb{Q}(\alpha)=\mathbb{Q}[\alpha]$. Например, для $\alpha=\sqrt{2}$ это так:

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}.$$

Проанализировав пример 4, логично предположить, что это верно для любого алгебраического числа α. На самом деле это даже критерий алгебраичности!

Теорема 2. *Для всех* $\alpha\in\mathbb{C}$: $\mathbb{Q}(\alpha)=\mathbb{Q}[\alpha]\ \Leftrightarrow\ \alpha\in\mathbb{A}$.

Доказательство. $\Rightarrow$ Если $\mathbb{Q}(\alpha)=\mathbb{Q}[\alpha]$, $\alpha\neq 0$, то $\frac{1}{\alpha}=g(\alpha)$ для некоторого $g(x)\in\mathbb{Q}[x]$, т. е. $\alpha g(\alpha)-1=0$ и $\alpha\in\mathbb{A}$.

$\Leftarrow$ Пусть $\alpha\in\mathbb{A}$, $g\in\mathbb{Q}[x]$ и $g(\alpha)\neq 0$. Поскольку многочлен μ_α неприводим, то НОД (g,μ_α) равен либо μ_α, либо 1. Первый случай невозможен, иначе $\mu_\alpha\,|\,g$ и $g(\alpha)=0$. Значит, многочлены g и μ_α взаимно просты и по алгоритму Евклида $u(x)g(x)+v(x)\mu_\alpha(x)=1$ для некоторых $u,v\in\mathbb{Q}[x]$. Подставив сюда $x=\alpha$, получим $1/g(\alpha)=u(\alpha)$. Значит, $\mathbb{Q}(\alpha)=\mathbb{Q}[\alpha]$. □

Задача 8. Избавьтесь от иррациональности в знаменателе:

а) $\dfrac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}}$; б) $\dfrac{\alpha}{\alpha+1}$, если $\alpha^3-\alpha+1=0$.

§ 4. Сопряжённые числа

Сопряжённые квадратичные иррациональности $a\pm b\sqrt{2}$ $(a,b\in\mathbb{Q},\ b\neq 0)$ являются корнями квадратного трёхчлена над $\mathbb{Q}$ — их минимального многочлена

$$\mu_{a\pm b\sqrt{2}}(x)=x^2-2ax+a^2-2b^2.$$

Распространим понятие сопряжённости на любые алгебраические числа. Пусть $\alpha\in\mathbb{A}$. Согласно основной теореме алгебры *любой многочлен положительной степени с комплексными коэффициентами раскладывается на линейные множители*, в частности,

$$\mu_\alpha(x)=(x-\alpha_1)\dots(x-\alpha_n),\quad \text{где } n=\deg\alpha,\ \alpha=\alpha_1. \tag{5}$$

Определение 3. *Сопряжёнными* с числом $\alpha\in\mathbb{A}$ называются все корни многочлена μ_α.

Замечание. Не путайте с комплексно-сопряжёнными числами! Эти два понятия совпадают только для корней квадратных трёхчленов над $\mathbb{Q}$ с отрицательным дискриминантом: например, $\pm i$, $(3\pm i\sqrt{11})/4$ — пары сопряжённых в обоих смыслах.

Поскольку многочлен μ_α неприводим, то согласно следующей теореме он не имеет кратных корней, т. е. числа $\alpha_1,\dots,\alpha_n$ различны.

Теорема 3. *Неприводимый над $\mathbb{Q}$ многочлен не имеет кратных комплексных корней.*

Доказательство. Пусть многочлен $f\in\mathbb{Q}[x]$ имеет кратный корень. Тогда это корень и его производной f', а значит, и их наибольшего общего делителя (f,f'). Последний может быть найден алгоритмом Евклида, а потому если $f\in\mathbb{Q}[x]$, то и $(f,f')\in\mathbb{Q}[x]$. Далее, $0<\deg(f,f')\leqslant\deg f'=$ $=\deg f-1$. Значит, (f,f') — нетривиальный делитель многочлена f. □

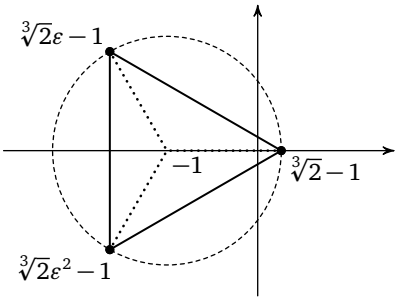

Рис. 3

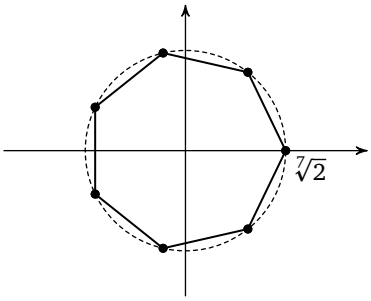

Рис. 4

Таким образом, *всякое алгебраическое число имеет ровно столько сопряжённых* (*включая себя*), *какова его степень*.

Пример 5. Пусть $a, b \in \mathbb{Q}, b \neq 0$. Числа $a \pm b\sqrt[3]{2}$, конечно, не будут сопряжёнными (как было бы для квадратичных иррациональностей). Число $a + b\sqrt[3]{2}$ иррационально и является единственным действительным корнем многочлена $(x-a)^3 - 2b^3$, который, стало быть, неприводим над $\mathbb{Q}$. Два других его корня и являются сопряжёнными к числу $a + b\sqrt[3]{2}$ — это числа $a + b\varepsilon\sqrt[3]{2}$ и $a + b\varepsilon^2\sqrt[3]{2}$, где $\varepsilon = (-1 + i\sqrt{3})/2$ — комплексный кубический корень из 1 (рис. 3).

Пример 6. В примере 1 мы показали, что число $\alpha = \sqrt{2} + \sqrt{3}$ — корень многочлена $x^4 - 10x^2 + 1$. Вот все его корни: $\pm\sqrt{2} \pm \sqrt{3}$. Чтобы с полным правом назвать их сопряжёнными, убедимся в неприводимости многочлена $x^4 - 10x^2 + 1$ над $\mathbb{Q}$. Очевидно, он не имеет рациональных корней и не раскладывается в произведение двух квадратных трёхчленов: или сумма, или произведение любых двух его корней не лежит в $\mathbb{Q}$.

Пример 7. Сопряжённые с числом $\cos\frac{2\pi}{9}$ суть

$$\cos\Big(\frac{2\pi}{9} \pm \frac{2\pi}{3}\Big) = \cos\frac{4\pi}{9}, \cos\frac{8\pi}{9},$$

см. пример 2. Вообще $\cos(2\pi/n) \in \mathbb{A}$ для любого $n \in \mathbb{N}$: как известно, $\cos n\varphi = T_n(\cos\varphi)$, где $T_n(x) = 2^{n-1}x^n + \ldots \in \mathbb{Z}[x]$ — многочлены Чебышёва, следовательно, $T_n(\cos(2\pi/n)) = \cos 2\pi = 1$. Однако найти минимальный многочлен для числа $\cos(2\pi/n)$ и сопряжённые ему числа не так просто, см. далее пример 11.

Пример 8. Все n комплексных значений корня $\sqrt[n]{a}$, где $a \in \mathbb{Q}$, сопряжены, коль скоро двучлен $x^n - a$ неприводим над $\mathbb{Q}$ (для каких a это так, см. задачу 4). См. рис. 4, где $n = 7$ и $a = 2$.

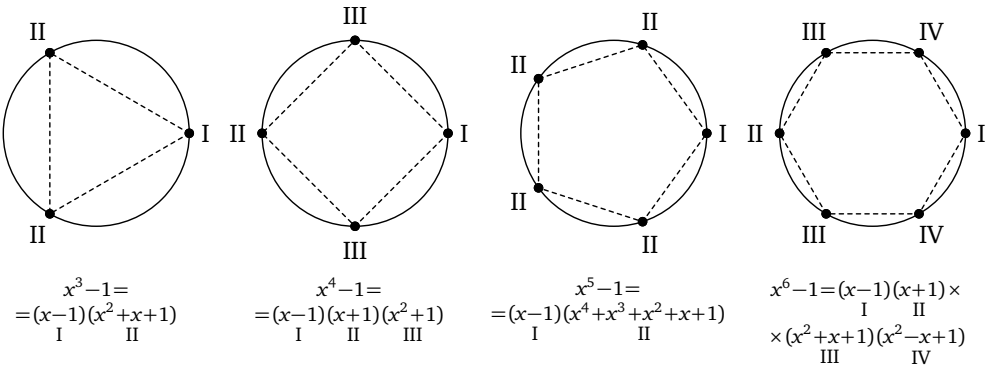

Рис. 5

Пример 9. Особого внимания заслуживают корни из единицы

$$\sqrt[n]{1}=\{1,\varepsilon,\varepsilon^2,\ldots,\varepsilon^{n-1}\},\quad \text{где}\ \ \varepsilon=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}. \tag{6}$$

Чтобы разбить их на классы сопряжённых, нужно разложить двучлен x^n-1 на неприводимые множители над $\mathbb{Q}$: корни каждого множителя образуют класс сопряжённых алгебраических чисел. Разберём примеры для малых n (рис. 5). В пояснении нуждается лишь неприводимость многочлена $\frac{x^5-1}{x-1}$. Сделав замену $x-1=y$, получим многочлен

$$\frac{(y+1)^5-1}{y}=y^4+5y^3+10y^2+10y+5,$$

неприводимый по признаку Эйзенштейна (теорема 1).

Можно заметить, что в этих примерах корни каждого неприводимого множителя имеют один *порядок*. Порядок некоторого корня δ из единицы — это наименьшее $k\in\mathbb{N}$ со свойством $\delta^k=1$, обозначение $O(\delta)$ (от англ. order — порядок). Например, $O(-1)=2$, $O(i)=O(-i)=4$. Корни из единицы порядка n называются *первообразными корнями* степени n. Легко доказать, что в обозначениях формулы (6) имеем $O(\varepsilon^k)\mid n$ и $O(\varepsilon^k)=n \iff \text{НОД}(k,n)=1$. Количество таких k от 1 до n обозначается $\varphi(n)$, функция φ называется *функцией Эйлера*.

Рассмотрим многочлен, корнями которого являются все корни из единицы данного порядка:

$$\Phi_n(x)=\prod_{\delta\,:\,O(\delta)=n}(x-\delta)=\prod_{1\leqslant k\leqslant n,\,(k,n)=1}(x-\varepsilon^k).$$

Он называется *круговым*. Классифицируем корни степени n по их порядкам и в соответствии с этим разложим двучлен x^n-1 на множители:

$$\sqrt[n]{1} = \bigsqcup_{d|n} \{\delta \mid O(\delta) = d\} \quad \Rightarrow \quad x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{7}$$

Оказывается, это и есть разбиение $\sqrt[n]{1}$ на классы сопряжённых и, соответственно, разложение двучлена $x^n - 1$ на неприводимые над $\mathbb{Q}$. Однако доказать неприводимость круговых многочленов не так-то просто, см., например, [1, глава 10, § 3, пример 3]. (О круговых многочленах рекомендуем статью [7].) Приведём ещё один пример — для $n = 12$ (рис. 6).

$$\begin{matrix} & \text{I} & \text{II} & \text{III} & \text{IV} & \text{V} & \text{VI} \\ x^{12}-1 = & (x-1) & (x+1) & (x^2+x+1) & (x^2+1) & (x^2-x+1) & (x^4-x^2+1) \\ & \Phi_1(x) & \Phi_2(x) & \Phi_3(x) & \Phi_4(x) & \Phi_6(x) & \Phi_{12}(x) \end{matrix}$$

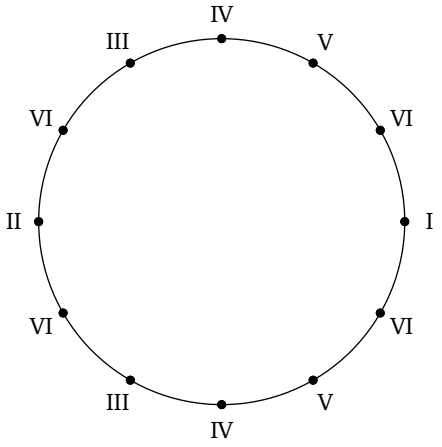

Рис. 6

На самом деле из определения круговых многочленов не очевидно даже, что их коэффициенты целые! Но это несложно выводится из разложения в формуле (7).

Задача 9. Проведите это рассуждение.

Задача 10. Найдите все целые ненулевые a и b, для которых $\dfrac{a+bi}{a-bi}$ — корень из единицы.

Задача 11. Найдите сопряжённые с числами из задачи 5.

А теперь с помощью сопряжённых чисел мы ответим на вопрос Q1 предыдущего параграфа и даже докажем несколько больше. Начнём с примера.

Пример 10. Покажем, что $\sqrt[3]{3} + \sqrt{2} \in \mathbb{A}$. Имеем

$$t = \sqrt[3]{3} + \sqrt{2} \quad \Rightarrow \quad (t - \sqrt{2})^3 = 3,$$

и после раскрытия скобок получаем $A(t) + B(t)\sqrt{2} = 0$ для некоторых $A, B \in \mathbb{Q}[x]$. Уединение $\sqrt{2}$ с последующим возведением в квадрат равнозначно домножению на сопряжённое $A(t) - B(t)\sqrt{2}$. Итак, $\sqrt[3]{3} + \sqrt{2}$ — корень многочлена $f(x) = A^2(x) - 2B^2(x) \in \mathbb{Q}[x]$, а значит, алгебраическое число. Какие у него сопряжённые? Найдём все корни $f(x)$:

$$f(s) = 0 \quad \Leftrightarrow \quad A(s) \pm B(s)\sqrt{2} = 0 \quad \Leftrightarrow \quad (s \mp \sqrt{2})^3 = 3 \quad \Leftrightarrow$$
$$\Leftrightarrow \quad s = \varepsilon^k \sqrt[3]{3} \pm \sqrt{2}, \quad k = 0, 1, 2, \quad \text{где } \varepsilon = \frac{-1 + i\sqrt{3}}{2}.$$

Означает ли это, что полученные 6 чисел сопряжены? Пока ещё нет: вдруг многочлен $f(x)$ приводим… Со всей уверенностью можно лишь утверждать, что *среди этих чисел содержатся сопряжённые* к $\sqrt[3]{3} + \sqrt{2}$. Доказывать неприводимость $f(x)$ непосредственно довольно муторно. Чуть позже, с помощью сильнодействующих средств, мы сделаем это элегантно, см. пример 15 и задачу 16. А сейчас обобщим проведённое рассуждение.

Теорема 4. *Если $\alpha_1, \ldots, \alpha_n$ — все сопряжённые с $\alpha \in \mathbb{A}$, а $\beta_1, \ldots, \beta_m$ — все сопряжённые с $\beta \in \mathbb{A} \setminus \{0\}$, то для любой операции $* \in \{+, -, \cdot, /\}$ число $\alpha * \beta$ алгебраическое и его сопряжённые содержатся среди чисел $\alpha_i * \beta_j$, $i = 1, \ldots, n$, $j = 1, \ldots, m$.*

Замечание. Не обязательно все числа $\alpha_i * \beta_j$ сопряжены с $\alpha * \beta$, простой пример: $\alpha = \beta = \sqrt{2}$.

Начнём доказывать теорему 4, следуя примеру 10, в котором $\alpha = \sqrt{2}$, $\beta = \sqrt[3]{3}$ и $* = +$. В этом случае $(x - \sqrt{2})^3 - 3 = \mu_\beta(x - \alpha)$ и

$$f(x) = \mu_\beta(x - \alpha_1)\mu_\beta(x - \alpha_2) = \prod_{i,j}(x - \alpha_i - \beta_j).$$

Рассмотрим такой многочлен в общей ситуации:

$$f(x) = \prod_{i,j}(x - \alpha_i - \beta_j) = \mu_\beta(x - \alpha_1) \ldots \mu_\beta(x - \alpha_n).$$

Если этот многочлен имеет рациональные коэффициенты, то в силу (3) он делится на $\mu_{\alpha+\beta}(x)$, и теорема 4 доказана для операции сложения (для других операций доказательство аналогично). Почему же $f(x) \in \mathbb{Q}[x]$? Суть в том, что этот многочлен не меняется при перестановках $\alpha_1, \ldots, \alpha_n$. Более формально, переставлять нужно не числа, а переменные. Вот точная и более общая формулировка.

Теорема 5. *Если многочлен $F(x, y_1, \ldots, y_n) \in \mathbb{Q}[x, y_1, \ldots, y_n]$ не меняется при перестановках $y_1, \ldots, y_n$ и если числа $\alpha_1, \ldots, \alpha_n$ образуют набор корней некоторого многочлена над $\mathbb{Q}$, то $F(x, \alpha_1, \ldots, \alpha_n) \in \mathbb{Q}[x]$.*

Доказательство легко вытекает из формул Виета и основной теоремы о симметрических многочленах, см. [1, глава 3, § 8] и [5, § 9.1, теорема 9.2].

Задача 12. Докажите теорему 5 при $n = 2$.

Из теоремы 5 следует ещё одна полезная теорема, позволяющая по сопряжённым с $\alpha \in \mathbb{A}$ найти сопряжённые с числами из $\mathbb{Q}(\alpha)$.

Теорема 6. *Если $\alpha_1, \ldots, \alpha_n$ — все сопряжённые с $\alpha \in \mathbb{A}$, то для любого многочлена $f(x) \in \mathbb{Q}[x]$ все сопряжённые с $f(\alpha)$ суть $f(\alpha_1), \ldots, f(\alpha_n)$.*

Замечание. Среди чисел $f(\alpha_1), \ldots, f(\alpha_n)$ могут быть равные, например, в тривиальном случае, когда $f = \text{const}$.

Доказательство. Многочлен $\mu_{f(\alpha)}(f(x)) \in \mathbb{Q}[x]$ имеет корень α, а значит, согласно (3) делится на многочлен $\mu_\alpha(x)$ и потому имеет корни $\alpha_1, \ldots, \alpha_n$. Это доказывает, что $f(\alpha_1), \ldots, f(\alpha_n)$ сопряжены с $f(\alpha)$. Других сопряжённых нет, так как $(x - f(\alpha_1)) \ldots (x - f(\alpha_n)) \in \mathbb{Q}[x]$ по теореме 5. □

Пример 11. Пусть $n \geqslant 3$. Поскольку согласно примеру 9 сопряжённые к

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

суть ε_n^k, где $(k, n) = 1$, то, применив теорему 6 к $\alpha = \varepsilon_n$ и $f(x) = \dfrac{x + x^{n-1}}{2}$, получим набор сопряжённых чисел: $\cos(2\pi k/n)$, где $(k, n) = 1$. Минимальный многочлен $\mu_{\cos 2\pi/n}(x)$ ищется так. Надо взять круговой многочлен $\Phi_n(x)$, поделить его на $x^{\varphi(n)/2}$ и сделать замену $y = (x + x^{-1})/2$:

$$\mu_{\cos 2\pi/n}(x)\Big(\frac{x + x^{-1}}{2}\Big) = \frac{\Phi_n(x)}{x^{\varphi(n)/2}}.$$

Например, при $n = 5$:

$$\frac{x^4 + x^3 + x^2 + x + 1}{x^2} = \Big(x + \frac{1}{x}\Big)^2 + x + \frac{1}{x} - 1 = 4y^2 + 2y - 1 = \mu_{\cos 2\pi/5}(y).$$

Вычислите по тому же рецепту $\mu_{\cos 2\pi/9}(y)$ и сравните с примером 2.

Задача 13. Найдите $\deg \sin\dfrac{2\pi}{n}$ при каждом $n \in \mathbb{N}$.

§ 5. Поля всё шире и шире

Для более глубокого изучения алгебраических чисел и решения более трудных задач мы познакомимся с понятием поля и освоим технику расширений полей. Будем рассматривать лишь поля, содержащиеся в $\mathbb{C}$.

Определение 4. Подмножество в $\mathbb{C}$ называется *полем*, если оно содержит числа 0 и 1 и замкнуто относительно сложения, вычитания, умножения и деления (не на нуль). Если K, L — поля и $K \subseteq L$, то говорят, что K — *подполе* поля L или что L — *расширение* поля K.

- Вот пример цепочки или, как чаще говорят, *башни* подполей:
$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R} \subset \mathbb{C}.$$
- Множества $\mathbb{Z}$, $[0, \infty)$, $\mathbb{Q} + \mathbb{Q}\sqrt[3]{2}$ полями не являются (почему?).
- Легко понять, что $\mathbb{Q}$ — самое маленькое (числовое) поле: оно содержится в любом числовом поле.
- В силу теоремы 4 *множество* $\mathbb{A}$ *всех алгебраических чисел является полем*.
- Говорят, что поле $\mathbb{Q}(\alpha)$, определённое в (4), получается присоединением к полю $\mathbb{Q}$ числа α. Аналогично определяется поле $K(\alpha)$ для любого поля K и, более общо, $K(\alpha_1, \ldots, \alpha_n)$ как наименьшее поле, содержащее K и числа $\alpha_1, \ldots, \alpha_n$, — как говорят, *поле, порождённое над* K *числами* $\alpha_1, \ldots, \alpha_n$.

Ясно, что $K(\alpha, \beta) = K(\alpha)(\beta) = K(\beta)(\alpha)$, т. е. числа можно присоединять все сразу, а можно последовательно в любом порядке. Также ясно, что $K(\alpha) \subseteq L \iff K \subseteq L$, $\alpha \in L$ (здесь K, L — поля, $\alpha \in \mathbb{C}$).

Пример 12. Докажем, что $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Включение $\supseteq$ очевидно. Обратно,
$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) \ni \frac{1}{\sqrt{2}+\sqrt{3}} = \sqrt{3}-\sqrt{2} \quad \Rightarrow$$
$$\Rightarrow \quad \mathbb{Q}(\sqrt{2}+\sqrt{3}) \ni \frac{\sqrt{3}+\sqrt{2}}{2} \pm \frac{\sqrt{3}-\sqrt{2}}{2} = \sqrt{3}, \sqrt{2}.$$

Задача 14. Докажите, что
$$\mathbb{Q}(\varepsilon_3) = \mathbb{Q}(\varepsilon_6) = \mathbb{Q}(i\sqrt{3}) \subset \mathbb{Q}(i, \sqrt{3}) = \mathbb{Q}(i + \sqrt{3}) = \mathbb{Q}(\varepsilon_{12}),$$
где $\varepsilon_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$.

Для любого поля K можно определить линейную зависимость чисел $v_1, \ldots, v_n \in \mathbb{C}$ над K (определение 1 с заменой $\mathbb{Q}$ на K), а также понятия, связанные с алгебраичностью.

Определение 5. Число $\alpha \in \mathbb{C}$ называется *алгебраическим* над полем $K \subseteq \mathbb{C}$, если оно является корнем некоторого ненулевого многочлена над K. Аналогично случаю поля $\mathbb{Q}$ определяются минимальный многочлен $\mu_\alpha^K(x)$, степень $\deg_K \alpha = \deg \mu_\alpha^K(x)$ и сопряжённые с α: в определениях 2 и 3 заменяем $\mathbb{Q}$ на K.

Пример 13. Любое комплексное число алгебраично над $\mathbb{R}$ и сопряжено со своим комплексно-сопряжённым числом.

Справедливы аналоги утверждений (2), (3) и теоремы 3. Дело в том, что с многочленами над любым полем можно обращаться как мы привыкли: делить с остатком, применять алгоритм Евклида, раскладывать на неприводимые множители (см., например, [1, глава 3, § 5]).

Пример 14. Разложим двучлен x^4-2 на неприводимые над каждым из полей башни

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2}, i)$$

и разобьём его корни на классы сопряжённых:

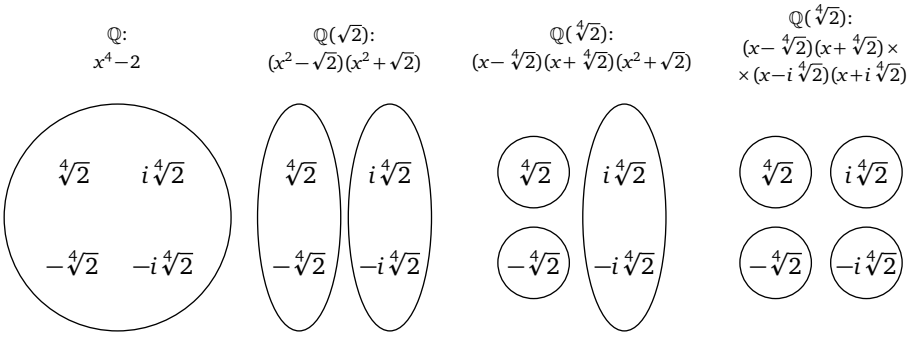

Рис. 7

В частности, $\deg_{\mathbb{Q}}(\sqrt[4]{2}) = 4$, $\deg_{\mathbb{Q}(\sqrt{2})}(\sqrt[4]{2}) = 2$, $\deg_{\mathbb{Q}(\sqrt[4]{2})}(\sqrt[4]{2}) = 1$.

Вообще при расширении поля неприводимые множители «измельчаются» и, соответственно, сопряжённые — корни одного неприводимого множителя — дробятся на более мелкие группы.

Если K — подполе поля L и число α алгебраично над K,
то α тем более алгебраично над L и $\mu_\alpha^L(x) \mid \mu_\alpha^K(x)$.

В самом деле, многочлен над K с корнем α можно рассматривать и над бóльшим полем L. При этом с точки зрения поля L многочлен $\mu_\alpha^K(x)$ — это просто какой-то многочлен над L с корнем α, поэтому $\mu_\alpha^L(x) \mid \mu_\alpha^K(x)$ аналогично (3).

Задача 15. Разложите многочлен $\Phi_{12}(x) = x^4 - x^2 + 1$ (см. пример 9) на неприводимые и разбейте его корни на сопряжённые над полями $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(i\sqrt{3})$.

А теперь покажем, как геометрические идеи помогают работать с алгебраическими числами.

Определение 6. Подмножество $L \subseteq \mathbb{C}$, содержащее поле K, называется *векторным пространством над* K, если L замкнуто относительно сложения и умножения на числа из K, т. е. $a+b, ka \in L$ для любых $a, b \in L$ и $k \in K$.

Важное замечание: *всякое поле является векторным пространством над любым своим подполем.*

Определение 7. Пусть L — векторное пространство над K. Предположим, что L содержит такие числа $e_1, \ldots, e_n$, что всякое $\alpha \in L$ представляется в виде

$$\alpha = k_1 e_1 + \ldots + k_n e_n \tag{8}$$

с однозначно определёнными коэффициентами $k_1, \ldots, k_n \in K$. Тогда система $e_1, \ldots, e_n$ называется *базисом* пространства L над K, равенство (8) — *разложением* числа α по этому базису, а число n — *размерностью* L над K и обозначается $\dim_K L$ (от англ. dimension — размерность). Если к тому же L является полем, то говорят, что L — *конечное расширение* поля K, размерность $\dim_K L$ называют *степенью расширения* и обозначают $[L:K]$, при этом пишут $K \overset{n}{\longrightarrow} L$.

Это определение размерности как количества элементов в базисе нуждается в *проверке корректности*: базисов-то много, почему во всех одно и то же число элементов? Проведём доказательство на языке векторов. Прежде всего отметим, что векторы любого базиса линейно независимы (иначе у нулевого вектора было бы два разложения по базису). Поэтому достаточно доказать **основную лемму о линейной зависимости:** *если «много» векторов выражается через «мало», то «много» линейно зависимы* (Э. Б. Винберг). Вот точная формулировка.

Теорема 7. *Если $m > n$ и векторы $f_1, \ldots, f_m$ выражаются через векторы $e_1, \ldots, e_n$, то векторы $f_1, \ldots, f_m$ линейно зависимы.*

Доказательство. Проведём индукцию по n. Случай $n = 1$ очевиден. Пусть $n > 1$ и для числа $n-1$ утверждение верно. При каждом $i = 1, \ldots, m$ выразим f_i через $e_1, \ldots, e_n$ и обозначим через c_i коэффициент при e_1: $f_i = c_i e_1 + \ldots$. Если $c_1 = \ldots = c_m = 0$, то $f_1, \ldots, f_m$ выражаются через $n-1$ векторов и сразу применимо предположение индукции. Если же среди c_i есть ненулевой, то для удобства можно считать, что $c_1 \neq 0$. Тогда векторы

$$f_2 - \frac{c_2}{c_1} f_1, \ \ldots, \ f_m - \frac{c_m}{c_1} f_1$$

выражаются через $e_2, \ldots, e_n$ и по предположению индукции линейно зависимы. Следовательно, векторы $f_1, \ldots, f_m$ тоже линейно зависимы. □

Замечания. 1. Все понятия, связанные с линейной зависимостью, естественнее определять для абстрактных векторных пространств, а не для полей — их частных случаев, но для наших целей это не оправдано.

2. Расширение поля может содержать *бесконечную линейно независимую систему*, т. е. такую, всякая конечная подсистема которой линейно независима. Тогда оно не имеет конечного базиса и называется *бесконечномерным*. Например, степени $1, \alpha, \alpha^2, \ldots$ любого трансцендентного числа α, очевидно, линейно независимы. Следовательно, расширение $\mathbb{Q} \subset \mathbb{C}$ бесконечномерно. Расширение $\mathbb{Q} \subset \mathbb{A}$ тоже бесконечномерно, например, система $\{\sqrt[n]{2} \mid n \in \mathbb{N}\}$ линейно независима (аналогично задаче 2б).

Обобщим и уточним теорему 2 (доказательство аналогично).

Теорема 8. *Для любого поля K и любого числа α имеем*

$$K(\alpha) = K[\alpha] \quad \Longleftrightarrow \quad \alpha \text{ алгебраично над } K \quad \Longleftrightarrow \quad \dim_K K(\alpha) < \infty.$$

Если эти условия выполнены и $n = \deg \alpha$, то $1, \alpha, \ldots, \alpha^{n-1}$ — базис в $K(\alpha)$ над K и $\dim_K K(\alpha) = n$.

Основной инструмент в теории конечных расширений — следующая теорема.

Теорема 9 (о размерности башни). *Если $K \subseteq P \subseteq L$ — конечные расширения полей, то*

$$\dim_K L = \dim_K P \cdot \dim_P L.$$

Вам ничего не напоминает эта формула? Ну, конечно! Это же свойство логарифмов

$$\log_a c = \log_a b \cdot \log_b c.$$

И это совсем не удивительно, ведь, если вдуматься, размерность — это своего рода логарифм… Взгляните: $\dim_{\mathbb{R}} \mathbb{R}^n = n$. Впрочем, это только аналогия, а вот формальное доказательство.

Доказательство. Выберем базис $e_1, \ldots, e_n$ в P над K и базис $f_1, \ldots, f_m$ в L над P. Тогда mn произведений $e_i f_j$ образуют базис в L над K. В самом деле, разложив любой элемент $\alpha \in L$ по базису $f_1, \ldots, f_m$, а коэффициенты этого разложения — по базису P над K, получим представление α в виде линейной комбинации элементов $e_i f_j$. Это представление единственно ввиду их линейной независимости над K: если

$$\sum_{i,j} c_{ij} e_i f_j = \sum_j \Big(\sum_i c_{ij} e_i \Big) f_j = 0,$$

где $c_{ij} \in K$, то, во-первых, $\sum_i c_{ij} e_i = 0$ при всех j (так как $f_1, \ldots, f_m$ линейно независимы над P), а во-вторых, $c_{ij} = 0$ при всех i, j (так как $e_1, \ldots, e_n$ линейно независимы над K). □

Теорема о размерности башни настолько же проста, насколько и эффективна.

Пример 15. Найдём $d = \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$. Ввиду теоремы 9 из рис. 8 ясно, что $d = 2a = 3b$. Кроме того, очевидно, что $b \leqslant 2$ (если вдруг $\sqrt{2} \in \mathbb{Q}(\sqrt[3]{3})$, то $b = 1$). Отсюда $a = 3$, $b = 2$ и $d = 6$.

В качестве базиса в $\mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, в соответствии с доказательством теоремы 9, можно взять попарные произведения чисел из любых базисов в $\mathbb{Q}(\sqrt{2})$ и $\mathbb{Q}(\sqrt[3]{3})$, см. рис. 9.

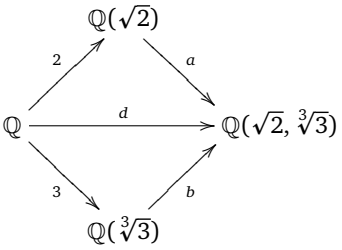

Рис. 8

$\sqrt{2}$	$\sqrt{2}\sqrt[3]{3}$	$\sqrt{2}\sqrt[3]{9}$
1	$\sqrt[3]{3}$	$\sqrt[3]{9}$

Рис. 9

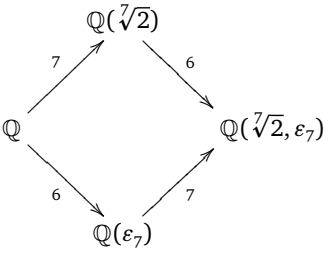

Рис. 10

Задача 16. Вернитесь к примеру 10 и докажите, что $\deg(\sqrt{2} + \sqrt[3]{3}) = 6$.

Указание. Присоедините к полю $\mathbb{Q}(\sqrt{2} + \sqrt[3]{3})$ число $\sqrt[3]{3}$ и докажите, что это расширение тривиально (имеет степень 1).

Пример 16. Пусть K — наименьшее поле, содержащее все корни двучлена $x^7 - 2$ (его *поле разложения*). Найдём $\dim_{\mathbb{Q}} K$. Ясно, что $K = \mathbb{Q}(\sqrt[7]{2}, \varepsilon_7)$. Далее, $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[7]{2}) = 7$ и $\dim_{\mathbb{Q}} \mathbb{Q}(\varepsilon_7) = 6$. Из диаграммы на рис. 10 получаем ответ: $\dim_{\mathbb{Q}} K = 7 \cdot 6 = 42$.

Задача 17. Решите аналогичную задачу для двучленов а) $x^8 - 2$; б) $x^6 + 4$; в) $x^6 + 3$.

Задача 18. Докажите, что $\mathbb{Q}(\varepsilon_m) \cap \mathbb{Q}(\varepsilon_n) = \mathbb{Q}$ при взаимно простых m и n.

В заключение параграфа покажем, как почти устно доказать, что $\mathbb{A}$ — поле. Пусть $\alpha, \beta \in \mathbb{A}$, $\beta \neq 0$. По теореме 8 расширения башни $\mathbb{Q} \to \mathbb{Q}(\alpha) \to \to \mathbb{Q}(\alpha)(\beta)$ конечны, а тогда по теореме 9 размерность $n = \dim_{\mathbb{Q}} \mathbb{Q}(\alpha, \beta)$ конечна. Следовательно, степени $1, \gamma, \ldots, \gamma^n$ любого $\gamma \in \mathbb{Q}(\alpha, \beta)$ линейно зависимы над $\mathbb{Q}$, т. е. $\gamma \in \mathbb{A}$. Применяем это к $\gamma = \alpha * \beta$, где $* \in \{+, -, \cdot, /\}$.

§ 6. Квадратичные расширения

Так называются расширения степени 2. Очевидно, $K(r)$ — квадратичное расширение поля K, если $r^2 \in K$, но $r \notin K$ (примеры: $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$, $\mathbb{R} \subset \mathbb{R}(i) = \mathbb{C}$). На самом деле других квадратичных расширений не бывает, и для доказательства достаточно выделить полный квадрат в квадратном трёхчлене.

Теорема 10. *Всякое расширение степени 2 получается присоединением квадратного радикала. Иными словами, если $K \subset L$ — поля и $\dim_K L = 2$, то $L = K(r)$ для некоторого $r \in L$ с условием $r^2 \in K$.*

Доказательство. Возьмём любое $\alpha \in L \setminus K$. Тогда $L = K(\alpha) = K[\alpha]$ и $\alpha^2 = p\alpha + q$ для некоторых $p, q \in K$. Отсюда

$$\left(\alpha - \frac{p}{2}\right)^2 = q + \frac{p^2}{4} \in K,$$

и можно взять $r = \alpha - \dfrac{p}{2}$. □

Пусть $K \subset K(r)$ — квадратичное расширение, $r^2 \in K$. Сопряжённым к числу $a + br$, где $a, b \in K$, $b \neq 0$, служит число

$$\overline{a + br} = a - br.$$

Мы обозначили его как комплексно сопряжённое неслучайно; как легко проверить, оно обладает теми же свойствами:

- $\overline{z * w} = \bar{z} * \bar{w}$, $* \in \{+, -, \cdot, /\}$;
- $\bar{\bar{z}} = z$;
- $\bar{z} = z \iff z \in K$.

Пример 17. Числа Фибоначчи $1, 1, 2, 3, 5, 8, 13, 21, \ldots$ определяются рекуррентно: $F_1 = F_2 = 1$, $F_n = F_{n-1} + F_{n-2}$ при $n \geqslant 3$. И хотя эти числа целые, их явная формула удивительным образом содержит квадратичные иррациональности:

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Переход к сопряжённым квадратичным иррациональностям часто оказывается эффективным. Вот пара фольклорных олимпиадных задач на эту тему.

Задача 19. 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 20. Найдите первые 1000 знаков после запятой в десятичной записи числа $(6+\sqrt{35})^{1000}$.

В заключение обсудим обобщение одной распространённой задачи о квадратных радикалах — доказательства иррациональности чисел вида

$$b_1\sqrt{a_1}+\ldots+b_m\sqrt{a_m} \tag{9}$$

для любого $m\in\mathbb{N}$, любых различных натуральных $a_1,\ldots,a_m$, свободных от квадратов (т. е. не делящихся на квадрат простого), и любых целых ненулевых $b_1,\ldots,b_m$ (см., например, [3]). Это доказывается индукцией по числу простых делителей произведения $a_1\ldots a_m$, шаг которой основан на переходе к сопряжённым квадратичным иррациональностям. Мы сделаем больше — опишем числа, сопряжённые к алгебраическому числу (9), в частности, найдём его степень, а также покажем геометрическую интерпретацию применённого метода — он сродни выбору базиса заданного набора векторов. Главные идеи ясны на примере с двумя радикалами.

Пример 18. Покажем, что $1,\sqrt{2},\sqrt{3},\sqrt{6}$ — базис поля $\mathbb{Q}(\sqrt{2},\sqrt{3})$. В силу теоремы 9 это равносильно тому, что $1,\sqrt{3}$ — базис в $\mathbb{Q}(\sqrt{2},\sqrt{3})$ над $\mathbb{Q}(\sqrt{2})$, а это значит, что $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$. Предположим, что $\sqrt{3}=a+b\sqrt{2}$, где $a,b\in\mathbb{Q}$. Перейдём к сопряжённым: $-\sqrt{3}=a-b\sqrt{2}$, откуда $a=0$ и $\sqrt{3}=b\sqrt{2}$. Записав $b=k/l$, где $k,l\in\mathbb{N}$, получим $3l^2=2k^2$. Двойка входит в разложение левой части в чётной степени, а в разложение правой — в нечётной. Противоречие.

Итак, каждое число из $\mathbb{Q}(\sqrt{2},\sqrt{3})$ однозначно представимо в виде $\alpha=a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, где $a,b,c,d\in\mathbb{Q}$. Найдём его сопряжённые. Их количество равно $\dim_{\mathbb{Q}}\mathbb{Q}(\alpha)\leqslant\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3})=4$. Запишем $\alpha_{++}:=\alpha$ двумя способами:

$$\alpha_{++}=a+b\sqrt{2}+(c+d\sqrt{2})\sqrt{3}\in\mathbb{Q}(\sqrt{2})(\sqrt{3}),$$
$$\alpha_{++}=a+c\sqrt{3}+(b+d\sqrt{3})\sqrt{2}\in\mathbb{Q}(\sqrt{3})(\sqrt{2}).$$

Теперь ясно, что $\alpha_{+-}:=a+b\sqrt{2}-(c+d\sqrt{2})\sqrt{3}$ сопряжено с α над $\mathbb{Q}(\sqrt{2})$, а $\alpha_{-+}:=a+c\sqrt{3}-(b+d\sqrt{3})\sqrt{2}$ сопряжено с α над $\mathbb{Q}(\sqrt{3})$. Кроме того, $\alpha_{--}:=a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$ сопряжено с α_{+-} над $\mathbb{Q}(\sqrt{3})$. Следовательно, все 4 числа сопряжены над $\mathbb{Q}$. Почему у α нет других сопряжённых? Казалось бы, мы нашли уже четыре, но проблема в том, что среди них могут быть равные. Воспользуемся уже знакомым приёмом — покажем, что многочлен $(x-\alpha_{++})(x-\alpha_{+-})(x-\alpha_{-+})(x-\alpha_{--})$ имеет рациональные коэффициенты. В самом деле, перемножим отдельно первые две скобки,

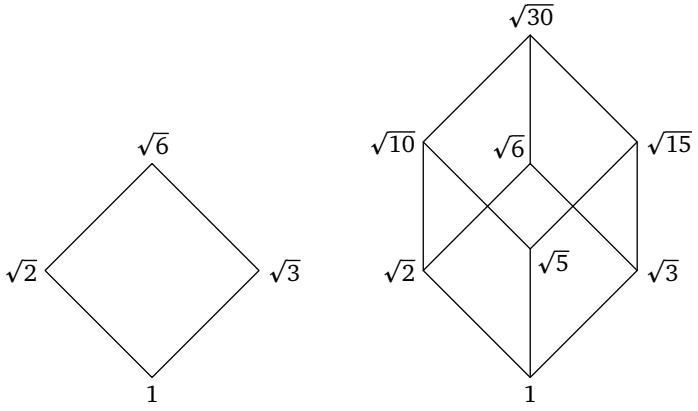

Рис. 11

отдельно последние две — в обоих произведениях «испарится» $\sqrt{3}$. Получатся многочлены над $\mathbb{Q}(\sqrt{3})$, причём с сопряжёнными коэффициентами: $\sqrt{3}$ встретится в них с разными знаками, поэтому при умножении он тоже исчезнет.

Перейдём к общей ситуации. Пусть $p_1, \ldots, p_n$ — различные простые числа. Рассмотрим поле $P = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$ и 2^n произведений

$$\sqrt{p_1}^{k_1} \ldots \sqrt{p_n}^{k_n}, \quad \text{где } k_1, \ldots, k_n \in \{0, 1\}. \tag{10}$$

Их удобно поместить в вершины n-мерного *булева куба* $\mathbb{Z}_2^n$, см. рис. 11 ($n = 2$, $n = 3$).

Теорема 11. *Числа* (10) *образуют базис поля* P *над* $\mathbb{Q}$, *в частности*, $\dim_{\mathbb{Q}} P = 2^n$. *Сопряжённые к числу*

$$\alpha = f(\sqrt{p_1}, \ldots, \sqrt{p_n}), \quad \textit{где } f \in \mathbb{Q}[x_1, \ldots, x_n], \tag{11}$$

суть числа

$$f(\pm\sqrt{p_1}, \ldots, \pm\sqrt{p_n}) \quad (\textit{максимум } 2^n \textit{ штук}). \tag{12}$$

Отметим, что если все числа (12) различны, то утверждение о сопряжённых очевидно, ведь сопряжённых всего не более 2^n. Например, из первого утверждения теоремы сразу следует, что 2^n чисел $\pm\sqrt{p_1} \pm \ldots \pm \sqrt{p_n}$ образуют набор сопряжённых. Однако среди чисел (12) могут быть повторяющиеся, и тогда надо провести более тонкое рассуждение.

Доказательство. Сначала покажем, что второе утверждение теоремы следует из первого. Если два числа вида $f(\pm\sqrt{p_1}, \ldots, \pm\sqrt{p_n})$ отличаются только знаком при одном радикале, скажем, при $\sqrt{p_1}$, то они сопряжены

над $\mathbb{Q}(\sqrt{p_2}, \ldots, \sqrt{p_n})$ и тем более над $\mathbb{Q}$. Следовательно, все эти числа сопряжены над $\mathbb{Q}$ (от каждого из них можно перейти к любому другому, меняя знаки у радикалов последовательно). Покажем, что других сопряжённых нет (аналогично примеру 18). Рассмотрим многочлен $F(x, y_1, \ldots, y_n)$, равный произведению 2^n скобок $x - f(\pm y_1, \ldots, \pm y_n)$. Очевидно, F чётен по каждой из переменных y_i (не меняется при замене y_i на $-y_i$), а значит, каждое y_i входит в F только в чётных степенях. Поэтому при подстановке $y_i = \sqrt{p_i}$ получим многочлен с рациональными коэффициентами. В силу (3) имеем $\mu_\alpha(x) \mid F(x, \sqrt{p_1}, \ldots, \sqrt{p_n})$.

Теперь докажем первое утверждение индукцией по n. При $n = 1$ оно следует из иррациональности $\sqrt{p_1}$. Чтобы сделать шаг от n к $n+1$, покажем, что $\sqrt{p_{n+1}} \notin P$. В противном случае $\sqrt{p_{n+1}} = f(\sqrt{p_1}, \ldots, \sqrt{p_n})$, где f — многочлен над $\mathbb{Q}$. По доказанному сопряжённые к правой части суть $f(\pm\sqrt{p_1}, \ldots, \pm\sqrt{p_n})$. Среди них должно быть ровно два различных, причём противоположных (как у левой части $\sqrt{p_{n+1}}$). Это возможно, только если это число вида $a\sqrt{p_{i_1} \ldots p_{i_s}}$, где $a \in \mathbb{Q}$, $1 \leqslant i_1 < \ldots < i_s \leqslant n$. Записав $a = k/l$, где $k, l \in \mathbb{N}$ (очевидно, $a > 0$), $k, l \in \mathbb{Z}$, и возведя в квадрат, получим $l^2 p_{n+1} = k^2 p_{i_1} \ldots p_{i_s}$. Простое p_{n+1} входит в разложение левой части в нечётной степени, а в разложение правой — в чётной. Противоречие с основной теоремой арифметики. □

Как же найти сопряжённые с α без повторов, в частности, найти $\deg \alpha$? Идея ясна на примере.

Пример 19. Число $\alpha = \sqrt{6} + \sqrt{10} + \sqrt{15}$ ($p_1 = 2$, $p_2 = 3$, $p_3 = 5$) сохраняется при смене знака у всех радикалов $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, и сопряжённых у него не 8, а 4:

$$\sqrt{6} + \sqrt{10} + \sqrt{15}, \quad -\sqrt{6} + \sqrt{10} - \sqrt{15},$$
$$\sqrt{6} - \sqrt{10} - \sqrt{15}, \quad -\sqrt{6} - \sqrt{10} + \sqrt{15}. \quad (13)$$

Покажем на этом примере, как алгоритмически найти сопряжённые без повторов. Рассмотрим радикалы (10), входящие в (11) с ненулевыми коэффициентами. Будем последовательно присоединять их, пропуская те, что присоединились автоматически по ходу дела, тогда каждый присоединяемый радикал увеличит степень (текущего) расширения вдвое. Например, для $\alpha = \sqrt{6} + \sqrt{10} + \sqrt{15}$ получим башню

$$\mathbb{Q} \xrightarrow{2} \mathbb{Q}(\sqrt{6}) \xrightarrow{2} \mathbb{Q}(\sqrt{6}, \sqrt{10}),$$

к которой радикал $\sqrt{15} = \frac{1}{2}\sqrt{6}\sqrt{10}$ уже присоединён. Представим α в виде $f(\sqrt{6}, \sqrt{10})$, где $f(x, y) = x + y + \frac{1}{2}xy$. Видно, что сопряжённые (13) имеют

вид $f(\pm\sqrt{6}, \pm\sqrt{10})$: знак при $\sqrt{15}$ уже нельзя выбирать произвольно, он однозначно определяется по знакам при $\sqrt{6}$ и $\sqrt{10}$.

Геометрическая интерпретация и алгоритм. Для практической реализации описанного алгоритма удобно вместо выражений (11) работать с наборами их показателей $(k_1, \dots, k_n) \in \mathbb{Z}_2^n$. Например,

$$\sqrt{6} = \sqrt{2}^1\sqrt{3}^1\sqrt{5}^0 \leftrightarrow (1,1,0),$$
$$\sqrt{10} = \sqrt{2}^1\sqrt{3}^0\sqrt{5}^1 \leftrightarrow (1,0,1),$$
$$\sqrt{15} = \sqrt{2}^0\sqrt{3}^1\sqrt{5}^1 \leftrightarrow (0,1,1).$$

Равенство $\sqrt{15} = \frac{1}{2}\sqrt{6}\sqrt{10}$ соответствует тому, что вектор $(0,1,1)$ равен сумме векторов $(1,1,0)$ и $(1,0,1)$ (поскольку $1+1=0$ в $\mathbb{Z}_2$). Вообще описанный выбор произведений (10) есть не что иное как стандартный способ выбрать базис из данного набора векторов: *очередной вектор из набора включается в базис, если он не выражается через уже выбранные векторы*. Реализуя этот способ, записывают координаты векторов по столбцам матрицы, которую приводят к ступенчатому виду методом Гаусса (см., например, [1, глава 2, § 1]).

Пример 20. Найдём степень числа

$$\alpha = a\sqrt{10} + b\sqrt{14} + c\sqrt{35} + d\sqrt{42} + e\sqrt{105},$$

где $0 \neq a, b, c, d, e \in \mathbb{Q}$, и сопряжённые с этим числом. Здесь четыре простых делителя: $p_1=2$, $p_2=3$, $p_3=5$, $p_4=7$. Запишем показатели радикалов по столбцам $v_1, \dots, v_5$ матрицы и приведём её к ступенчатому виду над полем $\mathbb{Z}_2$:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Соотношения между столбцами до и после преобразований строк одни и те же, поэтому столбцы v_1, v_2, v_4 линейно независимы и $v_3 = v_1 + v_2$, $v_5 = v_1 + v_4$. То же на языке радикалов:

$$\mathbb{Q} \xrightarrow{2} \mathbb{Q}(\sqrt{10}) \xrightarrow{2} \mathbb{Q}(\sqrt{14}) \xrightarrow{2} \mathbb{Q}(\sqrt{42}) \ni \sqrt{35} = \frac{1}{2}\sqrt{10}\sqrt{14},$$
$$\sqrt{105} = \frac{1}{2}\sqrt{10}\sqrt{42}.$$

Следовательно, сопряжёнными с числом

$$\alpha = f(\sqrt{10}, \sqrt{14}, \sqrt{42}),$$

где

$$f(x,y,z)=ax+by+\frac{1}{2}cxy+dz+\frac{1}{2}exz,$$

являются $2^3=8$ чисел: $f(\pm\sqrt{10},\pm\sqrt{14},\pm\sqrt{42})$ и, значит, $\deg\alpha=8$.

Теорема 12. *В обозначениях теоремы* 11 *пусть* $P_1,\dots,P_s$ *— произведения каких-то из* $p_1,\dots,p_n$, *такие, что* $\alpha=f(\sqrt{P_1},\dots,\sqrt{P_r})$, *где*

$$f(x)\in\mathbb{Q}[x]\quad и\quad \mathbb{Q}(\sqrt{P_1})\xrightarrow{2}\mathbb{Q}(\sqrt{P_1},\sqrt{P_2})\xrightarrow{2}\dots\xrightarrow{2}\mathbb{Q}(\sqrt{P_1},\dots,\sqrt{P_r}).$$

Тогда сопряжённые с α *суть* 2^r *чисел*

$$f(\pm\sqrt{P_1},\dots,\pm\sqrt{P_r})\quad и\quad \mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{P_1},\dots,\sqrt{P_r}).$$

Доказательство. Утверждение о сопряжённых доказывается так же, как в теореме 11. Далее, поскольку

$$\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{P_1},\dots,\sqrt{P_r})=2^r=\deg\alpha=\dim_{\mathbb{Q}}\mathbb{Q}(\alpha)$$

и

$$\mathbb{Q}(\alpha)\subseteq\mathbb{Q}(\sqrt{P_1},\dots,\sqrt{P_r}),$$

получаем $\mathbb{Q}(\alpha)=\mathbb{Q}(\sqrt{P_1},\dots,\sqrt{P_r})$. □

Задача 21 (XIX Турнир городов, осень 1997, основной вариант, 10–11 классы). Перемножаются все 2^{100} выражений вида

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

(при всевозможных комбинациях знаков). Докажите, что результат: а) целое число; б) квадрат целого числа. (*А. Я. Канель-Белов*)

* * *

В статье [4] мы покажем, как с помощью полученных знаний об алгебраических числах можно найти открытое Гауссом построение правильного 17-угольника циркулем и линейкой.

Решения задач

1. В принципе это можно доказать «в лоб»: возвести в куб, заменить $\sqrt[3]{4}$ на $a+b\sqrt[3]{2}$ и отделить рациональную часть от иррациональной. Но это рутинно, а главное — не обобщается на числа $1,\sqrt[n]{2},\dots,\sqrt[n]{2^{n-1}}$ при произвольном $n\in\mathbb{N}$. Поступим иначе. Равенство (1) означает, что $\sqrt[3]{2}$ —

корень трёхчлена x^2-bx-a. Поэтому $\sqrt[3]{2}$, будучи также корнем двучлена x^3-2, является корнем и следующих многочленов:

$$\begin{gathered} x^3-2-x(x^2-bx-a)=bx^2+ax-2, \\ bx^2+ax-2-b(x^2-bx-a)=(a+b^2)x+ab-2 \end{gathered} \tag{14}$$

(мы применили к многочленам x^3-2 и x^2-bx-a алгоритм Евклида). Отсюда $(a+b^2)\sqrt[3]{2}+ab-2=0$, а тогда, так как $a,b\in\mathbb{Q}$, то получаем $a+b^2=ab-2=0$, откуда $b^3=-2$, что невозможно.

2. а) Двучлен $x^{10}-2$ неприводим по признаку Эйзенштейна.

б) Числа $1, r, r^2, \ldots, r^{100!-1}$ линейно независимы над $\mathbb{Q}$, так как двучлен $x^{100!}-2$ неприводим.

в) См. теорему 11.

г) Аналогично примеру 15.

д) Пусть $\varepsilon=\cos\frac{2\pi}{17}+i\sin\frac{2\pi}{17}$. В силу примера 9 числа $\varepsilon, \varepsilon^{-1}, \varepsilon^2, \varepsilon^{-2}, \ldots, \varepsilon^8, \varepsilon^{-8}$ линейно независимы. Тогда их суммы по два: $\varepsilon+\varepsilon^{-1}, \varepsilon^2+\varepsilon^{-2}, \ldots, \varepsilon^8+\varepsilon^{-8}$ тем более линейно независимы. Остаётся заметить, что $\varepsilon^k+\varepsilon^{-k}=2\cos\frac{2\pi k}{17}$.

3. Наименьшее d с таким свойством заведомо делит n (так как $r^{n-dq}\in\mathbb{Q}$ для всех $q\in\mathbb{Z}$), поэтому $x^d-r^d \mid x^n-r^n$. Обратно, пусть двучлен

$$x^n-a=(x-r)(x-r\varepsilon)\ldots(x-r\varepsilon^{n-1})$$

приводим над $\mathbb{Q}$ ($\varepsilon=e^{2\pi i/n}$). Если m — степень его нетривиального делителя, то $r^m\varepsilon^d\in\mathbb{Q}$ для некоторого $d\in\mathbb{N}$.

а) Если $r\in\mathbb{R}$, то отсюда следует, что $r^m\in\mathbb{Q}$, так что ответ положительный.

б) В общем случае, когда $r\in\mathbb{C}$, ответ отрицательный, например, при $r=\varepsilon_3$: двучлен x^3-1 приводим, но $\varepsilon_3, \varepsilon_3^2\notin\mathbb{Q}$.

4. Разложим $a\in\mathbb{Q}$ на простые множители: $a=\pm p_1^{k_1}\ldots p_t^{k_t}$, $k_1,\ldots,k_t\in\mathbb{Z}$ ($t=0$ при $a=\pm1$).

а) Если $a>0$ или n нечётно, то можно взять действительное значение корня $r=\sqrt[n]{a}$. По пункту а) предыдущей задачи двучлен x^n-r^n неприводим, если и только если n — минимальное число со свойством $r^n\in\mathbb{Q}$. С другой стороны, для всех $d\in\mathbb{N}$ имеем

$$r^d\in\mathbb{Q} \quad\Leftrightarrow\quad \forall\, i\in\{1,\ldots,t\}\ n \mid k_i d \quad\Leftrightarrow\quad n \mid (k_1,\ldots,k_t)d.$$

Минимальное d, удовлетворяющее этому условию, равно n, если и только если

$$(n,k_1,\ldots,k_t)=1 \tag{$*$}$$

(В частности, при $n > 1$ обязательно $t > 0$, т. е. $a \neq \pm 1$.) Итак, условие $(*)$ — критерий в пункте а).

б) Памятуя об известном разложении $x^4+4=(x^2-2x+2)(x^2+2x+2)$ и стремясь его обобщить, запишем $a=-4b^4$, где $b>0$, и разложим двучлен x^4-a на неприводимые над $\mathbb{R}$:

$$x^4-a=x^4+4b^4=(x^2-2bx+2b^2)(x^2+2bx+2b^2). \qquad (15)$$

Поскольку разложение над $\mathbb{R}$ единственно, то над $\mathbb{Q}$ двучлен либо неприводим, либо раскладывается точно так же. Последнее равносильно следующему: $b\in\mathbb{Q} \iff a\in -4\mathbb{Q}^4 \iff$ все k_i кратны 4, кроме показателя при двойке, который сравним с 2 по модулю 4.

в) (Понадобится материал § 5.) Докажем, что при $s\geqslant 2$ над любым полем $K\subseteq\mathbb{C}$:

$$x^{2^s}-a \text{ неприводим над } K \quad\Leftrightarrow\quad a\notin K^2 \text{ и } a\notin -4K^4.$$

$\Rightarrow$ При $a\in K^2$ раскладываем разность квадратов, а при $a\in -4K^4$ раскладываем как в (15).

$\Leftarrow$ Индукция по s. База $s=2$. Пусть $a=d^4$, тогда корни двучлена x^4-a имеют вид $\pm d, \pm id$. Сумма или произведение любых двух из них не лежит в K: $-d^2\notin K$, иначе $a=d^4\in K^2$; $d\pm id\notin K$, иначе $-4a=d^4(1\pm i)^4=-4d^4\in K^4$ и $a\in -4K^4$. Шаг $s\to s+1$. По условию $a=c^2$, где $c\notin K$. Имеем

$$x^{2^{s+1}}-a=(x^{2^s}-c)(x^{2^s}+c).$$

Двучлены $x^{2^s}\pm c$ неприводимы над $K(c)$ по предположению индукции, так как $\pm c\notin K(c)^2$, $-4K(c)^4$. Поскольку разложение двучлена $x^{2^{s+1}}-a$ на неприводимые над $K(c)$ единственно и множители имеют коэффициенты $\pm c\notin K$, то над K двучлен неприводим.

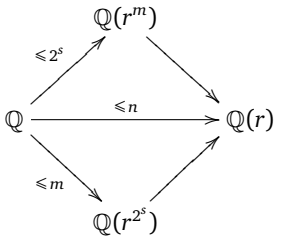

Рис. 12

г) Пусть $n=2^s m$, где m нечётно, и $r\in\sqrt[n]{a}$. Тогда (рис. 12) двучлен x^n-a неприводим над $\mathbb{Q} \iff$

$$\iff \dim_{\mathbb{Q}}\mathbb{Q}(r)=n \iff$$

$$\iff \begin{cases}\dim_{\mathbb{Q}}\mathbb{Q}(r^m)=2^s,\\ \dim_{\mathbb{Q}}\mathbb{Q}(r^{2^s})=m\end{cases} \iff \begin{cases}\text{двучлен } x^{2^s}-a \text{ неприводим над } \mathbb{Q},\\ \text{двучлен } x^m-a \text{ неприводим над } \mathbb{Q}.\end{cases}$$

С учётом пунктов а) и в) окончательно получаем критерий для $a<0$:

- $s=0,1$, $m>1$: условие $(*)$;
- $s\geqslant 2$, $m=1$: $a\notin -4\mathbb{Q}^4$;
- $s\geqslant 2$, $m>1$: условие $(*)$ и $a\notin -4\mathbb{Q}^4$.

5. а) Пусть $u=\sqrt[3]{1+\sqrt{2}}$, $v=\sqrt[3]{1-\sqrt{2}}$. Тогда

$$(u+v)^3=u^3+v^3+3uv(u+v)=2-3(u+v),$$

т. е. $u+v$ — корень многочлена x^3+3x-2. Он не имеет корней в $\mathbb{Q}$, а потому неприводим и совпадает с $\mu_{u+v}(x)$.

б) Аналогично приходим к многочлену $x^3+3x-14$, но он имеет корень 2, причём единственный действительный ввиду возрастания на $\mathbb{R}$. Значит, $\sqrt[3]{7+5\sqrt{2}}+\sqrt[3]{7-5\sqrt{2}}=2$ и $\mu_2(x)=x-2$.

6. Если $\alpha\in\mathbb{A}$, $r\in\sqrt[n]{\alpha}$ и $f(\alpha)=0$, то $g(\alpha)=0$ для $g(x)=f(x^n)$.

7. *I способ.* Действуем по алгоритму Евклида:

$$x^3-2=(x^2+x+3)(x-1)-2x+1,$$
$$x^2+x+3=(2x-1)\Big(\frac{1}{2}x+\frac{3}{4}\Big)+\frac{15}{4},$$

$$\frac{15}{4}=g(x)-(g(x)(x-1)-f(x))\Big(\frac{1}{2}x+\frac{3}{4}\Big)=$$
$$=f(x)\Big(\frac{1}{2}x+\frac{3}{4}\Big)+g(x)\Big(-\frac{1}{2}x^2-\frac{1}{4}x+\frac{7}{4}\Big).$$

II способ. Можно считать, что $\deg u<3$ и $\deg v<2$. Найдём такие a,b,c,d, что

$$(ax+b)(x^3-2)-(ax^2+cx+d)(x^2+x+3)=1,$$

приравняв коэффициенты при $1,x,x^2,x^3$:

$$\begin{cases} -2b-3d=1,\\ -2a-3c-d=0,\\ -3a-c-d=0,\\ b-a-c=0 \end{cases}\Leftrightarrow\begin{cases} a=2c,\\ b=a+c=3c,\\ d=-\frac{1}{3}(2b+1)=-2c-\frac{1}{3},\\ c=-3a-d=-4c+\frac{1}{3} \end{cases}\Leftrightarrow\begin{cases} c=\frac{2}{15},\\ a=\frac{1}{15},\\ b=\frac{1}{5},\\ d=-\frac{7}{15}. \end{cases}$$

8. а) $\dfrac{1}{1+\sqrt{2}-\sqrt{3}+\sqrt{6}}=\dfrac{1}{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}=$
$$=\frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{(1+\sqrt{2})^2-3(\sqrt{2}-1)^2}=\frac{1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}}{8\sqrt{2}-6}=$$
$$=\frac{\big(1+\sqrt{2}+(\sqrt{2}-1)\sqrt{3}\big)(8\sqrt{2}+6)}{92}.$$

б) $\alpha^3-\alpha+1=0\ \Rightarrow\ (\alpha+1)(\alpha^2-\alpha+1)=\alpha\ \Rightarrow\ \dfrac{\alpha}{\alpha+1}=\alpha^2-\alpha+1$ (повезло). Либо действуем по описанному алгоритму.

9. Индукция по n: 1) $\Phi_1(x) = x-1$; 2) если $\Phi_k(x) \in \mathbb{Z}[x]$ при всех $k < n$, то

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n, d\neq n} \Phi_d(x)} \in \mathbb{Z}[x],$$

так как старшие коэффициенты многочленов в знаменателе равны 1. Это, кстати, способ вычислять круговые многочлены рекуррентно.

10. Пусть $\varepsilon = \dfrac{a+bi}{a-bi}$ — первообразный корень из единицы степени n. Тогда $\dim_{\mathbb{Q}} \mathbb{Q}(\varepsilon) = \varphi(n)$. С другой стороны, так как $ab \neq 0$, то $\dim_{\mathbb{Q}} \mathbb{Q}(\varepsilon) = \dim_{\mathbb{Q}} \mathbb{Q}(i) = 2$. Но $\varphi(n) = 2 \iff n = 3, 4, 6$ (несложное упражнение). При $n = 3, 6$ получаем $\mathbb{Q}(\varepsilon) = \mathbb{Q}(i\sqrt{3}) \neq \mathbb{Q}(i)$, а $n = 4$ подходит: $\varepsilon = \pm i$. Отсюда $a = \pm b$.

11. а) В обозначениях решения задачи 5: $u+v$, $u\varepsilon + v\varepsilon^2$, $u\varepsilon^2 + v\varepsilon$, где $\varepsilon = e^{2\pi i/3}$. б) 2.

12. Многочлен от y_1, y_2, не меняющийся при перестановках y_1 и y_2, есть линейная комбинация мономов $y_1^k y_2^k$ и выражений

$$y_1^k y_2^{k+l} + y_1^{k+l} y_2^k = y_1^k y_2^k (y_1^l + y_2^l).$$

Сумма в скобках выражается через $y_1 + y_2$ и $y_1 y_2$: раскладываем по биному

$$y_1^l + y_2^l = (y_1 + y_2)^l - \dots$$

и т. д. (получаются такие же выражения, но с меньшими степенями). Далее подставим вместо y_1 и y_2 корни α_1 и α_2 трёхчлена над $\mathbb{Q}$. Он равен $t^2 - (\alpha_1 + \alpha_2)t + \alpha_1\alpha_2$, поэтому $\alpha_1 + \alpha_2, \alpha_1\alpha_2 \in \mathbb{Q}$. Доказательство при $n > 2$ проходит по той же схеме, но гораздо труднее доказать, что всякий симметрический многочлен выражается через так называемые *элементарные симметрические* (аналоги $y_1 + y_2$ и $y_1 y_2$ при $n = 2$).

13. Сведём задачу к случаю косинуса:

$$\sin \frac{2\pi}{n} = \cos\Big(\frac{\pi}{2} - \frac{2\pi}{n}\Big) = \cos \frac{2\pi(n+4)}{4n}.$$

Знаменатель несократимой дроби, равной $\dfrac{n+4}{4n}$, равен

$$\frac{4n}{(4n, n+4)} = \frac{4n}{(16, n+4)}.$$

С учётом примера 11 имеем

$$\deg \sin \frac{2\pi}{n} = \frac{1}{2}\varphi\Big(\frac{4n}{(16, n+4)}\Big).$$

В таблице приведены все возможные случаи.

n	$(16, n+4)$	$\frac{1}{2}\varphi\Big(\frac{4n}{(16,n+4)}\Big)$
нечётно	1	$\frac{1}{2}\varphi(4n)=\varphi(n)$
$2(2m+1)$	2	$\frac{1}{2}\varphi(2n)=\varphi(n)$
$4(2m+1)$	$8(2,m+1)$	$\frac{1}{2}\varphi\Big(\frac{2(2m+1)}{(2,m+1)}\Big)=\frac{1}{4}\varphi(n)$, так как $\varphi(2(2m+1))=\varphi(2m+1)$
$8m$	4	$\frac{1}{2}\varphi(n)$

14. Поскольку $\varepsilon_3=(-1+i\sqrt{3})/2$ и $\varepsilon_6=\varepsilon_3+1$, то $\mathbb{Q}(\varepsilon_3)=\mathbb{Q}(\varepsilon_6)=\mathbb{Q}(i\sqrt{3})$, а так как

$$\varepsilon_{12}=\cos\frac{\pi}{6}+i\sin\frac{\pi}{6}=\frac{\sqrt{3}+i}{2},$$

то $\mathbb{Q}(\varepsilon_{12})=\mathbb{Q}(i+\sqrt{3})$. Далее, $\varepsilon_{12}+\varepsilon_{12}^{-1}=\sqrt{3}$, поэтому $\mathbb{Q}(\varepsilon_{12})\ni\sqrt{3}$, а тогда $\mathbb{Q}(\varepsilon_{12})=\mathbb{Q}(i+\sqrt{3},\sqrt{3})=\mathbb{Q}(i,\sqrt{3})$.

15. Разложение над каждым из трёх полей получается группировкой корней $(\pm\sqrt{3}\pm i)/2$ многочлена $\Phi_{12}(x)$ на две пары одним из трёх способов:

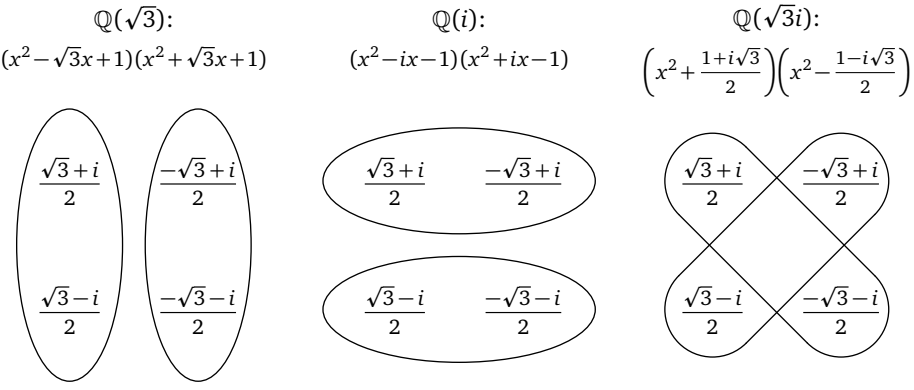

Рис. 13

16. Положим $\alpha=\sqrt{2}+\sqrt[3]{3}$ (рис. 14). Расширение $\mathbb{Q}(\alpha)\xrightarrow{d}\mathbb{Q}(\sqrt{2},\sqrt[3]{3})$ может быть получено присоединением $\sqrt{2}$, поэтому его степень $d\leqslant 2$. Но оно также получается присоединением $\sqrt[3]{3}$, следовательно, двучлен x^3-3 приводим над $\mathbb{Q}(\alpha)$, а тогда имеет в $\mathbb{Q}(\alpha)$ корень. Этим корнем

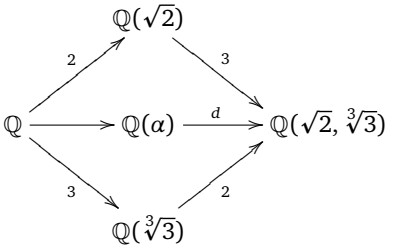

Рис. 14

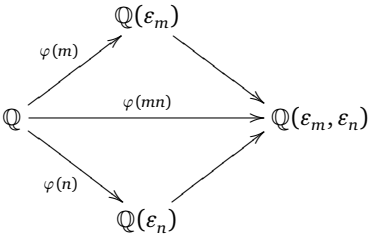

Рис. 15

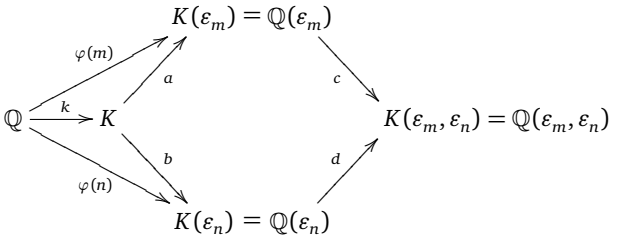

Рис. 16

может быть только действительное число $\sqrt[3]{3}$, значит, $\sqrt[3]{3} \in \mathbb{Q}(\alpha)$, т. е. $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha, \sqrt[3]{3}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, в частности $\deg \alpha = 6$.

17. а) Поскольку $\varepsilon_8 = (1+i)/\sqrt{2}$, то $K = \mathbb{Q}(\sqrt[8]{2}, \varepsilon_8) = \mathbb{Q}(\sqrt[8]{2}, i)$ — расширение степени 16: расширение $\mathbb{Q}(\sqrt[8]{2})$ имеет степень 8 (ввиду неприводимости двучлена $x^8 - 2$) и не содержит i.

б) $K = \mathbb{Q}(\alpha, \varepsilon_6)$, где $\alpha = i\sqrt[3]{2}$ и $\varepsilon_6 = (1 + i\sqrt{3})/2$. Поскольку $K \ni \alpha^3 = -2i$, то $K = \mathbb{Q}(i\sqrt[3]{2}, i\sqrt{3}, i) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$. Это расширение имеет степень 12.

в) $K = \mathbb{Q}(\alpha, \varepsilon_6)$, где $\alpha = i\sqrt[6]{3}$, причём $\alpha^3 = -i\sqrt{3}$, поэтому $K = \mathbb{Q}(\alpha)$. Это расширение степени 6, так как двучлен $x^6 + 3$ неприводим над $\mathbb{Q}$ по признаку Эйзенштейна.

18. Поскольку $(m, n) = 1$, то $\varphi(mn) = \varphi(m)\varphi(n)$, $\varepsilon_m\varepsilon_n$ — первообразный корень степени mn из единицы и $\mathbb{Q}(\varepsilon_m, \varepsilon_n) = \mathbb{Q}(\varepsilon_m\varepsilon_n)$. Из рис. 15 теперь следует, что $\dim_{\mathbb{Q}(\varepsilon_m)} \mathbb{Q}(\varepsilon_m, \varepsilon_n) = \varphi(n)$.

Положим $K = \mathbb{Q}(\varepsilon_m) \cap \mathbb{Q}(\varepsilon_n)$ и $k = \dim_{\mathbb{Q}} K$. Надо доказать, что $k = 1$ (рис. 16). Очевидно, $d \leqslant a$ и $c \leqslant b$. С другой стороны, по доказанному выше получаем $c = \varphi(n)$ и $d = \varphi(m)$. В то же время $ka = \varphi(m)$ и $kb = \varphi(n)$. Итак, $a \geqslant d = \varphi(m) = ka$, откуда $k = 1$.

19. Перейдём к сопряжённым числам:

$$(a - b\sqrt{2})^2 + (c - d\sqrt{2})^2 = 7 - 5\sqrt{2} < 0$$

— противоречие.

20. Сложим данное число с сопряжённым к нему:

$$(6+\sqrt{35})^{1000}+(6-\sqrt{35})^{1000}.$$

Эта сумма целая (по формуле 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.

21. б) Рассмотрим 2^{99} многочленов $1+\varepsilon_2x_2+\ldots+\varepsilon_{100}x_{100}$, где все ε_i равны ±1. Их произведение — чётный многочлен по каждой из переменных, а потому имеет вид $f(x_2^2,\ldots,x_{100}^2)$ и целые коэффициенты. В частности, при $x_2=\sqrt{k}$, $k\in\{2,\ldots,100\}$, получается целое число, обозначим его d. Повторив рассуждение с противоположными по знаку многочленами $-1+\varepsilon_2x_2+\ldots+\varepsilon_{100}x_{100}$, получим то же число d (поскольку количество многочленов чётно). Значит, произведение из условия равно d^2.

Список литературы

[1] *Винберг Э. Б.* Курс алгебры. М.: МЦНМО, 2017.

[2] *Каибханов А.*, *Скопенков А.* Примеры трансцендентных чисел // Математическое просвещение. Сер. 3. Вып. 10. М.: МЦНМО. 2006. С. 176–184.

[3] *Камнев Л.* Иррациональность суммы радикалов // Квант. 1972. № 2. С. 26–27.

[4] *Канунников А. Л.* Как придумать построение правильного семнадцатиугольника // Математическое просвещение. Сер. 3. Вып. 26. М.: МЦНМО, 2020. С. 143–166.

[5] *Нестеренко Ю. В.* Теория чисел. М.: Академия. 2008.

[6] *Олейников В.* Иррациональность и неприводимость // Квант. 1986. № 10. С. 6–10.

[7] *Сендеров В.*, *Спивак А.* Многочлены деления круга // Квант. 1998. № 1. С. 11–18.

[8] *Фельдман Н.* Алгебраические и трансцендентные числа // Квант. 1983. № 7. С. 2–7.

Андрей Леонидович Канунников, мехмат МГУ,
Московский центр фундаментальной и прикладной математики
andrew.kanunnikov@gmail.com