# О линейной независимости радикалов из натуральных чисел

И. Е. Воробьёв

В этой работе приводится альтернативное доказательство двух классических результатов:

- Радикалы из натуральных чисел, все попарные отношения которых иррациональны, линейно независимы над полем рациональных чисел $\mathbb{Q}$.
- Радикалы нечётной степени $n$ из натуральных чисел, свободных от $n$-х степеней, линейно независимы над круговым полем $\mathbb{Q}(\exp(2\pi i/n))$.

## § 1. Введение

При изучении алгебры естественным образом возникают радикалы из натуральных чисел. Между ними имеются тривиальные соотношения типа $\sqrt[3]{16} = 2\sqrt[3]{2}$ и т. п.

Встаёт вопрос о существовании линейных соотношений между радикалами, кроме тривиальных. Здесь возникают эффекты, связанные с комплексными корнями из единицы. Например, $\sqrt{-3}$ выражается над $\mathbb{Q}$ через $\sqrt{3}$ с использованием $\sqrt{-1}$. Чтобы их исключить, ограничимся только положительными вещественными значениями радикалов.

Простейшим фактом рассматриваемого типа является следующий: квадратные корни из натуральных чисел, свободных от квадратов, линейно независимы над полем рациональных чисел.

Мы приведём новое доказательство следующего результата, полученного в работе А. С. Безиковича [4]: *если* $\sqrt[m_i]{n_i}/\sqrt[m_j]{n_j} \notin \mathbb{Q}$ *при* $i, j = 1, \ldots, k$, $i \neq j$, *то* $\sqrt[m_1]{n_1}, \sqrt[m_2]{n_2}, \ldots, \sqrt[m_k]{n_k}$ *линейно независимы над* $\mathbb{Q}$.

Этот факт можно переформулировать так: *Если каждый из различных радикалов* $\sqrt[m_i]{n_i}$ $(i = 1, \ldots, k)$ *нельзя сократить* (*т. е.* $n_i$ *не является точной* $l$*-й степенью, где* $l$ *— какой-либо делитель числа* $m_i$) *и каждое* $n_i$ *свободно от* $m_i$*-х степеней, то* $1, \sqrt[m_1]{n_1}, \sqrt[m_2]{n_2}, \ldots, \sqrt[m_k]{n_k}$ *линейно независимы над* $\mathbb{Q}$.

После такого естественного вопроса можно задаться следующим: *верно ли, что радикалы* $m$*-й степени линейно независимы над расширением*

*поля* $\mathbb{Q}$ *примитивным корнем* $m$*-й степени из* 1? Будет доказано, что это верно для нечётных $m$. В чём-то схожее доказательство приводит Ричардс в [5]. Отметим, однако, что при рассмотрении этого случая нами доказаны некоторые дополнительные факты.

Доказательства основаны на рассмотрении группы Галуа и используют тот факт, что порядок группы Галуа равен степени расширения. Поэтому нам будет удобнее сначала доказать результат про независимость над круговым полем (расширения в нём нормальны, т. е. мы можем говорить о группе Галуа), хотя он и выглядит более сложным. А затем, обобщив его, получить доказательство независимости над полем рациональных чисел.

О теории Галуа см. [2, 3].

## § 2. Все корни квадратные

Начнём с простейшего содержательного случая — когда все корни квадратные.

Теорема 1. *Квадратные корни из натуральных чисел, свободных от квадратов, линейно независимы над* $\mathbb{Q}$*. Иными словами,*

$$1,\ \sqrt{p_1},\ \ldots,\ \sqrt{p_n},\ \sqrt{p_1p_2},\ \ldots,\ \sqrt{p_{n-1}p_n},\ \ldots,\ \sqrt{p_1\cdots p_n},$$

*где* $p_i$ *— попарно различные простые, линейно независимы над* $\mathbb{Q}$*.*

Доказательство. Изложенное ниже рассуждение распространяется на общий случай, почему мы его и приводим, хотя существует элементарное доказательство.

Утверждение равносильно следующему:

$$[\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n}):\mathbb{Q}]=2^n. \tag{1}$$

В самом деле, написанный выше набор чисел есть не что иное, как базис векторного пространства $\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n})$ над $\mathbb{Q}$. Равенство (1) выражает тот факт, что расширение каждым следующим числом нетривиально.

Докажем равенство (1). Предположим противное: найдутся такие простые $p_1,\ldots p_{i+1}$, что расширение $\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_i})$ с помощью $\sqrt{p_{i+1}}$ тривиально.

Возьмём наименьшее $n$ такое, что для некоторого натурального $k$ и различных простых чисел $p_1,\ldots,p_{n+k}$

$$\sqrt{p_{n+1}\cdots p_{n+k}}\in\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n}).$$

(Очевидно, что $n\leqslant i$. При этом возможно, что $n<i$.)

Пусть

$$\mathbb{F}=\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_{n-1}}),\quad \mathbb{E}_1=\mathbb{F}(\sqrt{p_n}),\quad \mathbb{E}_2=\mathbb{F}(\sqrt{p_{n+1}\cdots p_{n+k}}).$$

Имеется включение $\mathbb{E}_1 \supseteq \mathbb{E}_2$. Степень расширения $\mathbb{E}_1$ над $\mathbb{F}$ равна 2. При этом $\mathbb{E}_2$ имеет такую же степень расширения над $\mathbb{F}$, так как нетривиально ввиду минимальности $n$. Следовательно, $\mathbb{E}_1 = \mathbb{E}_2$.

Далее нам потребуется

Лемма 1. *Пусть $\mathbb{F}$ — любое поле характеристики 0, а $m, n$ — его элементы, не являющиеся квадратами. Тогда если $\mathbb{F}(\sqrt{m}) = \mathbb{F}(\sqrt{n})$, то $\sqrt{n} = \alpha\sqrt{m}$ для некоторого $\alpha \in \mathbb{F}$.*

Доказательство леммы. Заметим, что

$$\{a + b\sqrt{n} \mid a, b \in \mathbb{F}\} = \mathbb{F}(\sqrt{n}) = \mathbb{F}(\sqrt{m}) = \{a + b\sqrt{m} \mid a, b \in \mathbb{F}\}.$$

Рассмотрим автоморфизмы поля $\mathbb{F}(\sqrt{n})$, оставляющие $\mathbb{F}$ на месте:

$$\varphi : a + b\sqrt{n} \mapsto a - b\sqrt{n}, \quad \psi : a + b\sqrt{m} \mapsto a - b\sqrt{m}.$$

Количество таких автоморфизмов равно степени расширения, т. е. двум. Один из них тождественный, и так как $\varphi \neq \mathrm{id}$ и $\psi \neq \mathrm{id}$, получаем, что $\varphi = \psi$.

Так как $\sqrt{n}$ — элемент из $\mathbb{F}(\sqrt{m})$, найдутся такие $a, b \in \mathbb{F}$, что $\sqrt{n} = a + b\sqrt{m}$. После применения $\varphi$ к левой части и $\psi$ к правой равенство сохранится. Следовательно, мы можем написать систему уравнений:

$$\begin{cases} \sqrt{n} = a + b\sqrt{m}, \\ -\sqrt{n} = a - b\sqrt{m}. \end{cases}$$

Вычитая из верхнего уравнения нижнее, получаем: $2\sqrt{n} = 2b\sqrt{m}$. □

Окончание доказательства теоремы 1. Применим лемму для $p_{n+1}$, …, $p_{n+k}$ и $p_n$. Получим, что

$$\sqrt{p_n} = \alpha\sqrt{p_{n+1} \dots p_{n+k}}, \quad \alpha \in \mathbb{F}.$$

Домножим обе части на $\sqrt{p_{n+1} \dots p_{n+k}}$:

$$\sqrt{p_n \dots p_{n+k}} = \alpha p_{n+1} \dots p_{n+k}.$$

Следовательно,

$$\sqrt{p_n \dots p_{n+k}} \in \mathbb{F} = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{n-1}}),$$

что противоречит минимальности выбранного нами $n$. □

## § 3. Показатель корня — простое число

Перейдём к случаю, где все корни одной и той же простой степени, и сразу будем доказывать независимость над круговым полем.

Теорема 2. *Пусть $p$ — простое число. Тогда корни $p$-й степени из натуральных чисел, свободных от $p$-х степеней (т. е. чисел, для которых степень вхождения каждого простого меньше, чем $p$), линейно независимы над $\mathbb{Q}(\exp(2\pi i/p))$.*

Доказательство. Пусть

$$\omega = \exp\Big(\frac{2\pi i}{p}\Big) = \cos\Big(\frac{2\pi}{p}\Big) + i\sin\Big(\frac{2\pi}{p}\Big),$$

т. е. $\omega$ — корень $p$-й степени из 1.

Аналогично предыдущему, утверждение теоремы сводится к следующему факту:

$$\big[\mathbb{Q}(\omega, \sqrt[p]{p_1}, \ldots, \sqrt[p]{p_n}) : \mathbb{Q}(\omega)\big] = p^n.$$

Нужная нам линейная независимость вытекает из описания базиса пространства $\mathbb{Q}(\omega, \sqrt[p]{p_1}, \ldots, \sqrt[p]{p_n})$ над $\mathbb{Q}(\omega)$. Возьмём, как в § 2, наименьшее $n$, для которого найдутся натуральное $k$, различные простые числа $p_1, \ldots, p_{n+k}$ и натуральные числа $\alpha_1, \ldots, \alpha_k$, меньшие чем $p$ и такие, что

$$\sqrt[p]{p_{n+1}^{\alpha_1} \cdots p_{n+k}^{\alpha_k}} \in \mathbb{Q}(\omega, \sqrt[p]{p_1}, \ldots, \sqrt[p]{p_n}).$$

Такое $n$ существует. Действительно, рассмотрим наименьшее $n$ такое, что при присоединении ещё одного корня $p$-й степени из простого числа $p_{n+1}$ степень расширения окажется меньше $p$. Минимальный многочлен для $\sqrt[p]{p_{n+1}}$ над построенным полем делит

$$x^p - p_{n+1} = \prod\prod(x - \omega^i \cdot \sqrt[p]{p_{n+1}}),$$

т. е. его свободный член имеет вид $\omega^k \cdot \sqrt[p]{p_{n+1}^l}$, где $l < p$, и тем самым мы нашли в построенном поле радикал нужного вида.

Заметим, что $n > 0$. Предположим, что $\mathbb{Q}(\omega)$ содержит нецелый $\sqrt[p]{m}$. Однако

$$[\mathbb{Q}(\omega) : \mathbb{Q}] < [\mathbb{Q}(\sqrt[p]{m}) : \mathbb{Q}],$$

так как левая часть равна $\varphi(p) = p - 1$ (неприводимый многочлен, аннулирующий $\omega$, — это многочлен деления круга $1+x+x^2+\ldots+x^{p-1}$; подробности см., например, в [1]), а правая равна $p$ (учитывая, что $p$ простое). Противоречие[1)].

Как и раньше, пусть $\mathbb{F} = \mathbb{Q}(\omega)(\sqrt[p]{p_1}, \ldots, \sqrt[p]{p_{n-1}})$. Ясно, что

$$\mathbb{F}(\sqrt[p]{p_n}) \supseteq \mathbb{F}\Big(\sqrt[p]{p_{n+1}^{\alpha_1} \cdots p_{n+k}^{\alpha_k}}\Big).$$

[1)] В доказательстве теоремы 2 мы только в этом месте пользуемся простотой показателя степени.

Заметим, что $[\mathbb{F}(\sqrt[p]{p_n}) : \mathbb{F}] = p$. Действительно, минимальный многочлен для $\sqrt[p]{p_n}$ делит $x^p - p_n = \prod(x - \omega^i \cdot \sqrt[p]{p_n})$. Следовательно, его свободный член, принадлежащий $\mathbb{F} = \mathbb{Q}(\omega)(\sqrt[p]{p_1}, \ldots, \sqrt[p]{p_{n-1}})$, имеет вид $\omega^k \cdot \sqrt[p]{p_n^l}$. В силу минимальности выбранного $n$

$$p = l = [\mathbb{F}(\sqrt[p]{p_n}) : \mathbb{F}].$$

Напомним классический факт.

*Пусть $\mathbb{F}$ — любое поле. Тогда если $\mathbb{F}(\alpha) \supseteq \mathbb{F}(\beta)$ и оба расширения являются расширениями Галуа, то автоморфизмы поля $\mathbb{F}(\alpha)$, которые сохраняют элементы поля $\mathbb{F}$, переводят $\beta$ в сопряжённый элемент.*

Теперь мы готовы доказать ключевую лемму, которая нам потребуется и в доказательстве следующих теорем.

Лемма 2 (основная лемма). *Пусть $\mathbb{F}$ — любое подполе в $\mathbb{C}$, содержащее примитивный корень $m$-й степени из 1, а $n, k$ — элементы из $\mathbb{F}$, не являющиеся $m$-ми степенями. Тогда если $\mathbb{F}(\sqrt[m]{n}) \supseteq \mathbb{F}(\sqrt[m]{k})$, то $\sqrt[m]{k} = \alpha \cdot \sqrt[m]{n^l}$ для некоторого $\alpha \in \mathbb{F}$ и $l < m$.*

Доказательство. Пусть степени расширений $\mathbb{F}(\sqrt[m]{n})$ и $\mathbb{F}(\sqrt[m]{k})$ равны $a$ и $b$ соответственно,

$$\mathbb{F}(\sqrt[m]{n}) = \left\{\alpha_0 + \alpha_1 \cdot \sqrt[m]{n} + \ldots + \alpha_{a-1} \cdot \sqrt[m]{n^{a-1}}\right\} \supseteq$$
$$\supseteq \left\{\beta_0 + \beta_1 \cdot \sqrt[m]{k} + \ldots + \beta_{b-1} \cdot \sqrt[m]{k^{b-1}}\right\} = \mathbb{F}\left(\sqrt[m]{k}\right).$$

Тогда найдём такие $\alpha_0, \ldots, \alpha_{a-1} \in \mathbb{F}$, что

$$\sqrt[m]{k} = \alpha_0 + \alpha_1 \cdot \sqrt[m]{n} + \ldots + \alpha_{a-1} \cdot \sqrt[m]{n^{a-1}}.$$

Существует лишь $a$ автоморфизмов, действующих на $\mathbb{F}(\sqrt[m]{n})$ и сохраняющих элементы из $\mathbb{F}$, и все они переводят $\sqrt[m]{n}$ и $\sqrt[m]{k}$ в сопряжённые (т. е. в другие корни минимальных многочленов).

Опишем сопряжённые этим числам. Минимальные многочлены для $\sqrt[m]{n}$ и $\sqrt[m]{k}$ должны делить $x^m - n$ и $x^m - k$ соответственно. Поэтому сопряжённые для $\sqrt[m]{n}$ и $\sqrt[m]{k}$ равны $\omega^i \cdot \sqrt[m]{n}$ для каких-то $i \in \{0, 1, \ldots, m-1\}$ и $\omega^j \cdot \sqrt[m]{k}$ для каких-то $j \in \{0, 1, \ldots, m-1\}$ соответственно. Пусть $\{\beta_0, \beta_1, \ldots, \beta_{a-1}\}$ — подмножество в $\{0, 1, \ldots, m-1\}$ такое, что $\omega^{\beta_i} \cdot \sqrt[m]{n}$ являются сопряжёнными для $\sqrt[m]{n}$, причём $\beta_0 = 0$. Для каждого $i = 0, 1, \ldots, a-1$ существует автоморфизм, который переводит $\sqrt[m]{n}$ именно в $\omega^{\beta_i} \cdot \sqrt[m]{n}$.

На обе части равенства

$$\sqrt[m]{k} = \alpha_0 + \alpha_1 \cdot \sqrt[m]{n} + \ldots + \alpha_{a-1} \cdot \sqrt[m]{n^{a-1}}$$

будем действовать всевозможными автоморфизмами: сначала применим тождественный, потом переводящий $\sqrt[m]{n}$ в $\omega^{\beta_1}\cdot\sqrt[m]{n}$, потом переводящий $\sqrt[m]{n}$ в $\omega^{\beta_2}\cdot\sqrt[m]{n}$, и так далее. Получится система уравнений:

$$\begin{cases} \sqrt[m]{k} = \alpha_0 + \alpha_1\cdot\sqrt[m]{n} + \ldots + \alpha_{a-1}\cdot\sqrt[m]{n^{a-1}}, \\ \omega^{\gamma_1}\cdot\sqrt[m]{k} = \alpha_0 + \alpha_1\omega^{\beta_1}\cdot\sqrt[m]{n} + \ldots + \omega^{(m-1)\beta_1}\alpha_{a-1}\cdot\sqrt[m]{n^{a-1}}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \omega^{\gamma_{a-1}}\cdot\sqrt[m]{k} = \alpha_0 + \alpha_1\omega^{\beta_{a-1}}\cdot\sqrt[m]{n} + \ldots + \omega^{(m-1)\beta_{a-1}}\alpha_{a-1}\cdot\sqrt[m]{n^{a-1}}. \end{cases}$$

Рассмотрим матрицу этой системы, считая величины $\sqrt[m]{n^i}$ неизвестными, а $\alpha_i\omega^{\beta_j}$ коэффициентами:

$$\begin{pmatrix} \alpha_0 & \alpha_1 & \alpha_2 & \ldots & \alpha_{a-1} \\ \alpha_0(\omega^{\beta_1})^0 & \alpha_1(\omega^{\beta_1})^1 & \alpha_2(\omega^{\beta_1})^2 & \ldots & \alpha_{a-1}(\omega^{\beta_1})^{a-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_0(\omega^{\beta_{a-1}})^0 & \alpha_1(\omega^{\beta_{a-1}})^1 & \alpha_2(\omega^{\beta_{a-1}})^2 & \ldots & \alpha_{a-1}(\omega^{\beta_{a-1}})^{a-1} \end{pmatrix}.$$

Преобразуем матрицу следующим образом. Удалим нулевые столбцы, а каждый из остальных столбцов разделим на соответствующее ему $\alpha_i$. Рассмотрим следующую матрицу:

$$\begin{pmatrix} 1^0 & 1^1 & 1^2 & \ldots & 1^{a-1} \\ (\omega^{\beta_1})^0 & (\omega^{\beta_1})^1 & (\omega^{\beta_1})^2 & \ldots & (\omega^{\beta_1})^{a-1} \\ (\omega^{\beta_2})^0 & (\omega^{\beta_2})^1 & (\omega^{\beta_2})^2 & \ldots & (\omega^{\beta_2})^{a-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (\omega^{\beta_{a-1}})^0 & (\omega^{\beta_{a-1}})^1 & (\omega^{\beta_{a-1}})^2 & \ldots & (\omega^{\beta_{a-1}})^{a-1} \end{pmatrix}.$$

Это матрица Вандермонда, поэтому её определитель не равен 0. А наша (преобразованная) матрица получается из этой матрицы выбрасыванием некоторых столбцов, поэтому все её столбцы линейно независимы. В этом случае матрица приводится элементарными преобразованиями строк к виду, где в какой-то строке ровно одно ненулевое число. Если мы проведём те же элементарные преобразования с уравнениями системы, то выразим какой-то $\sqrt[m]{n^i}$ в виде линейной комбинации левых частей уравнений, т. е. в виде $\alpha\cdot\sqrt[m]{k}$, что и требуется. □

Окончание доказательства теоремы 2. В силу леммы существуют такие $\alpha\in\mathbb{F}$ и $l<p$, что

$$\alpha\cdot\sqrt[p]{p_n^l} = \sqrt[p]{p_{n+1}^{\alpha_1}\cdots p_{n+k}^{\alpha_k}}.$$

Домножив обе части на правую часть в $(p-1)$-й степени, мы получим противоречие с минимальностью $n$. □

## § 4. Показатель корня — нечётное число

Итак, мы решили задачу для простых показателей степеней. Докажем теперь то же самое для равных нечётных.

Теорема 3. *Пусть $m$ — нечётное натуральное число. Корни $m$-й степени из натуральных чисел, свободных от $m$-х степеней, линейно независимы над $\mathbb{Q}(\exp(2\pi i/m))$.*

Доказательство. При доказательстве теоремы 2 мы пользовались простотой показателя корня *только* когда доказывали, что $\mathbb{Q}(\omega)$ не содержит никаких корней соответствующей степени из какого-либо натурального числа (см. замечание 2). Так что достаточно доказать следующую лемму.

Лемма 3. *Пусть $m$ — целое число. Тогда $\mathbb{Q}(\exp(2\pi i/m))$ не содержит никакого $\sqrt[n]{k}$, если этот корень не является квадратным.*

Доказательство. Предположим, что $\mathbb{Q}(\exp(2\pi i/m))$ при некотором $m$ содержит какой-то $\sqrt[n]{k}$, причём этот корень нельзя сократить, т. е. $k$ не является точной $l$-й степенью ни для какого $l$, делящего $n$.

Для любого абелева расширения Галуа любое промежуточное поле между ним и основным полем также является абелевым расширением основного поля. Расширение $\mathbb{Q}(\exp(2\pi i/m))$ абелево и при этом нормально, так как является полем разложения многочлена $x^m-1$.

Так как оно нормально и содержит $\mathbb{Q}(\sqrt[n]{k})$, то оно содержит и поле $\mathbb{Q}(\sqrt[n]{k}, \exp(2\pi i/n))$. Остаётся установить, что последнее не является абелевым расширением. Для этого укажем два его автоморфизма $\varphi$ и $\psi$, которые не коммутируют.

Автоморфизм $\varphi$ — обычное комплексное сопряжение, автоморфизм $\psi$ строится несколько сложнее. Докажем, что

$$\left[\mathbb{Q}\left(\sqrt[n]{k}, \exp\left(\frac{2\pi i}{n}\right)\right) : \mathbb{Q}\left(\exp\left(\frac{2\pi i}{n}\right)\right)\right] > 2.$$

Прежде всего,

$$\left[\mathbb{Q}\left(\exp\left(\frac{2\pi i}{n}\right)\right) : \mathbb{Q}\right] = \varphi(n),$$

потому что минимальный многочлен для $\exp(2\pi i/n)$ — это многочлен деления круга, имеющий степень $\varphi(n)$. Далее,

$$\left[\mathbb{Q}\left(\sqrt[n]{k}, \exp\left(\frac{2\pi i}{n}\right)\right) : \mathbb{Q}\left(\exp\left(\frac{2\pi i}{n}\right)\right)\right] = \frac{\left[\mathbb{Q}\left(\sqrt[n]{k}, \exp\left(\frac{2\pi i}{n}\right)\right) : \mathbb{Q}\right]}{\left[\mathbb{Q}\left(\exp\left(\frac{2\pi i}{n}\right)\right) : \mathbb{Q}\right]} =$$

$$= \frac{\left[\mathbb{Q}\left(\sqrt[n]{k}, \exp\left(\frac{2\pi i}{n}\right)\right) : \mathbb{Q}(\sqrt[n]{k})\right] \cdot [\mathbb{Q}(\sqrt[n]{k}) : \mathbb{Q}]}{\varphi(n)} =$$

$$= \frac{\left[\mathbb{Q}\left(\sqrt[n]{k}, \exp\left(\frac{2\pi i}{n}\right)\right) : \mathbb{Q}(\sqrt[n]{k})\right] \cdot n}{\varphi(n)} \geqslant \frac{2 \cdot n}{\varphi(n)} > 2.$$

Предпоследнее неравенство следует из того, что мы к $\mathbb{Q}(\sqrt[n]{k})$ присоединили $\exp(2\pi i/n)$, причём $\exp(2\pi i/n)$ не лежит в $\mathbb{Q}(\sqrt[n]{k})$ ввиду того, что $\exp(2\pi i/n)$ не вещественно при $n > 2$.

Мы показали, что у $\sqrt[n]{k}$ имеется не менее двух сопряжённых над $\mathbb{Q}(\exp(2\pi i/n))$. Хотя бы один из них не вещественный. Соответствующий автоморфизм мы и обозначим через $\psi$.

Найденные два автоморфизма не коммутируют. Действительно,

$$\varphi\left(\psi(\sqrt[n]{k})\right) = \overline{\psi\left(\varphi(\sqrt[n]{k})\right)},$$

причём по построению это не вещественное число. □

Вместе с леммой 3 доказана и теорема 3. □

## § 5. Независимость над $\mathbb{Q}$

Теперь докажем ту же теорему для чётных $m$ и не над $\mathbb{Q}(\omega)$, а над $\mathbb{Q}$.

Теорема 4. *Пусть $m$ — любое натуральное число. Корни $m$-й степени из натуральных чисел, свободных от $m$-х степеней, линейно независимы над $\mathbb{Q}$.*

Замечание 1. Если в утверждении теоремы заменить поле $\mathbb{Q}$ на $\mathbb{Q}(\exp(2\pi i/m))$, как в теореме 3, то оно станет неверным — например,

$$\sqrt[4]{4} \in \mathbb{Q}\left(\cos\left(\frac{\pi}{4}\right)\right) \subset \mathbb{Q}\left(\exp\left(\frac{2\pi i}{8}\right)\right).$$

Доказательство. Воспользовавшись леммами 2 и 3, докажем утверждение в несколько шагов. В силу теоремы 3 будем считать, что $m$ чётно. Положим

$$\omega = \exp\left(\frac{2\pi i}{m}\right).$$

### Шаг 1

*Докажем, что если последовательно расширять $\mathbb{Q}(\omega)$ корнями $m$-й степени из простых чисел, то каждое следующее расширение будет либо степени $m$, либо степени $m/2$.*

Предположим, что это не так. Будем действовать, как в § 3. Возьмём снова наименьшее $n$, для которого существуют натуральное $k$, различные простые числа $p_1, \dots, p_{n+k}$ и натуральные числа, меньшие чем $m$, $\alpha_1, \dots, \alpha_k$, такие что

$$\sqrt[m]{p_{n+1}^{\alpha_1} \cdots p_{n+k}^{\alpha_k}} \in \mathbb{Q}(\omega, \sqrt[m]{p_1}, \dots, \sqrt[m]{p_n}), \tag{2}$$

причём, в отличие от предыдущих рассуждений, потребуем ещё, чтобы

$$\sqrt[m]{p_{n+1}^{\alpha_1} \cdots p_{n+k}^{\alpha_k}}$$

не являлся квадратным корнем, т. е. какое-то $\alpha_i$ было отлично от $m/2$.

Во-первых, покажем, что такое $n$ существует. Возьмём какое-то расширение $\mathbb{Q}(\omega, \sqrt[m]{p_1}, \dots, \sqrt[m]{p_l})$, степень которого оказалась меньше, чем $m/2$, над полем $\mathbb{Q}(\omega, \sqrt[m]{p_1}, \dots, \sqrt[m]{p_{l-1}})$. Как в доказательстве теоремы 2 получаем, что свободный член минимального многочлена для $\sqrt[m]{p_l}$ имеет вид $\omega^i \cdot \sqrt[m]{p_l^j}$ и не является квадратным корнем, так как иначе многочлен окажется степени $m/2$. Значит, $n = l - 1$ подходит (но может найтись и меньшее значение). Во-вторых, заметим, что $n > 0$, так как по лемме 3 в $\mathbb{Q}(\omega)$ нет неквадратных корней.

Теперь по лемме 2 найдём такое

$$\alpha \in \mathbb{Q}(\omega, \sqrt[m]{p_1}, \dots, \sqrt[m]{p_{n-1}}),$$

что

$$\sqrt[m]{p_{n+1}^{\alpha_1} \cdots p_{n+k}^{\alpha_k}} = \alpha \cdot \sqrt[m]{p_n^l}.$$

Домножив обе части на $\sqrt[m]{p_n^{l(m-1)}}$, получим, что

$$\sqrt[m]{p_n^{l(m-1)} p_{n+1}^{\alpha_1} \cdots p_{n+k}^{\alpha_k}} \in \mathbb{Q}(\omega, \sqrt[m]{p_1}, \dots, \sqrt[m]{p_{n-1}}),$$

что противоречит минимальности $n$.

### Шаг 2

*На этом шаге мы построим множество квадратных корней из натуральных чисел, которое порождает все квадратные корни, лежащие в* $\mathbb{Q}(\omega)$.

Заметим, что в поле $\mathbb{Q}(\omega)$ лежит конечное количество квадратных корней из чисел, свободных от квадратов, потому что по теореме 1 они линейно независимы над $\mathbb{Q}$. Далее, все эти корни можно представить в виде

$$\sqrt{q_1 q_2 \cdots q_{a_1}},\ \sqrt{q_{1+a_1} \cdots q_{a_2}},\ \dots,\ \sqrt{q_{1+a_{k-1}} \cdots q_{a_k}},$$

где $q_i$ простые. Естественно, все эти $a_k$ простых чисел не обязательно различны. Исходя из этого множества корней, построим некоторое другое.

Сначала возьмём простое число $q_1$ и выделим все корни, в которые оно входит, кроме $\sqrt{q_1 q_2 \dots q_{a_1}}$. Умножим их на $\sqrt{q_1 q_2 \dots q_{a_1}}$. Если какую-то целую часть можно вынести за знак корня, то уберём её, и если осталось целое число, то удалим его из множества. Таким образом, мы добились того, что $q_1$ написано только под первым знаком корня. Далее такими же преобразованиями добьёмся того, что под каждым оставшимся знаком корня одно из простых будет *уникально*, (т. е. оно не будет написано ни под каким другим знаком корня).

Получилось некоторое множество корней

$$\sqrt{p_1 p_2 \cdots p_{b_1}},\ \sqrt{p_{1+b_1} \cdots p_{b_2}},\ \dots,\ \sqrt{p_{1+b_{l-1}} \cdots p_{b_l}}. \tag{3}$$

Пронумеруем простые числа под знаками корней так, чтобы простые вида $p_{b_i}$ являлись уникальными.

Заметим, что в поле

$$\mathbb{Q}\big(\sqrt{p_1 p_2 \cdots p_{b_1}},\ \sqrt{p_{1+b_1} \cdots p_{b_2}},\ \dots,\ \sqrt{p_{1+b_{l-1}} \cdots p_{b_l}}\big)$$

в силу его построения содержатся все квадратные корни, которые были в $\mathbb{Q}(\omega)$. Также заметим, что по теореме 1 степень этого расширения равна $2^l$.

### Шаг 3

*На этом шаге мы поймём, как будет возрастать степень расширения при последовательном присоединении* (*в каком-то заданном порядке*) *корней $m$-й степени из простых чисел.*

Будем расширять $\mathbb{Q}(\omega)$ корнями $m$-х степеней из простых чисел в следующем порядке. Сначала расширим по очереди корнями из простых, появляющихся в (3), кроме простых с номерами $b_i$, которые уникальны, и докажем, что каждое следующее расширение имеет степень $m$ (п. 3а). Затем опять же по очереди расширим поле корнями из простых с номерами $b_i$ и покажем, что каждое следующее расширение имеет степень $m/2$ (п. 3б). А дальше уже будем расширять корнями из всех остальных простых в любом порядке и докажем, что каждое следующее расширение имеет степень $m$ (п. 3в). Скомбинировав эти результаты, наконец докажем теорему 4 (шаг 4).

а) Пусть мы расширяем корнями из простых чисел $r_1, \dots, r_s$, содержащихся в (3), причём среди них нет уникальных простых $p_{b_1}, \dots, p_{b_i}$. Предположим, что какое-то расширение корнем $\sqrt[m]{r_k}$ имеет степень, меньшую чем $m$, т. е., как доказано на шаге 1, степень $m/2$. Это означает, что величина $(\sqrt[m]{r_k})^{m/2} = \sqrt{r_k}$ содержится в предыдущем расширении.

Рассмотрим тогда первое расширение вида

$$\mathbb{Q}(\omega, \sqrt[m]{r_1}, \ldots, \sqrt[m]{r_i}), \tag{4}$$

в котором содержится число вида $\sqrt{t}$, где $t$ — произведение каких-то чисел из множества $\{r_{i+1}, \ldots, r_s\}$.

Заметим, что такое $\sqrt{t}$ не содержится в $\mathbb{Q}(\omega)$ из-за того, что мы не присоединяли уникальные простые, а все корни в $\mathbb{Q}(\omega)$ выражаются в виде произведения каких-то корней из (3).

По лемме 2 получаем $\sqrt{t} = \alpha \cdot \sqrt[m]{r_i^j}$, где $\alpha \in \mathbb{Q}(\omega, \sqrt[m]{r_1}, \ldots, \sqrt[m]{r_{i-1}})$ и $j$ делит $m$.

Докажем, что $j = m/2$. Действительно, разделим на $\alpha$ и возведём обе части в квадрат. Получаем, что

$$\sqrt[m]{r_i^{2j}} \in \mathbb{Q}(\omega, \sqrt[m]{r_1}, \ldots, \sqrt[m]{r_{i-1}}).$$

Но ввиду минимальности $i$ расширение $\mathbb{Q}(\omega, \sqrt[m]{r_1}, \ldots, \sqrt[m]{r_{i-1}})$ корнем $\sqrt[m]{r_i}$ должно иметь степень $m$, поэтому $\sqrt[m]{r_i^v}$ при $v < m$ не содержится в поле $\mathbb{Q}(\omega, \sqrt[m]{r_1}, \ldots, \sqrt[m]{r_{i-1}})$. Отсюда $\sqrt{t} = \alpha\sqrt{r_i}$. Домножив обе части на $\sqrt{r_i}$, получим

$$\sqrt{tr_i} \in \mathbb{Q}(\omega, \sqrt[m]{r_1}, \ldots, \sqrt[m]{r_{i-1}}),$$

что противоречит минимальности $i$.

б) В этом пункте мы докажем, что если последовательно расширять $\mathbb{Q}(\omega, \sqrt[m]{r_1}, \ldots, \sqrt[m]{r_s})$ числами вида $\sqrt[m]{p_{b_i}}$, то каждое следующее расширение будет иметь степень $m/2$.

Это утверждение является прямым следствием из шагов 1 и 2. В самом деле, из построения множества корней, содержащихся в (3), видно, что квадратные корни $\sqrt{p_{1+b_{i-1}}}, \ldots, \sqrt{p_{b_i - 1}}$, а также корень $\sqrt{p_{1+b_{i-1}} \cdots p_{b_i}}$, содержатся уже в $\mathbb{Q}(\omega, \sqrt[m]{r_1}, \ldots, \sqrt[m]{r_s})$.

Поэтому $\sqrt[m]{p_{b_i}^{m/2}}$ содержится в $\mathbb{Q}(\omega, \sqrt[m]{r_1}, \ldots, \sqrt[m]{r_s}, \sqrt[m]{p_{b_1}}, \ldots, \sqrt[m]{p_{b_{i-1}}})$. Следовательно, степень расширения этого поля числом $\sqrt[m]{p_{b_i}}$ меньше $m$, т. е. согласно шагу 1 равна $m/2$.

в) В этом пункте мы докажем, что если последовательно расширять поле $\mathbb{Q}(\omega, \sqrt[m]{p_1}, \ldots, \sqrt[m]{p_{b_i}})$ корнями $m$-й степени из простых, не содержащихся в (3), в любом порядке, то каждое следующее расширение будет иметь степень $m$.

Пусть мы расширяем корнями $m$-й степени из простых чисел $s_1, s_2, s_3, \ldots$ Предположим, что расширение поля

$$\mathbb{Q}\left(\omega, \sqrt[m]{p_1}, \ldots, \sqrt[m]{p_{b_i}}, \sqrt[m]{s_1}, \ldots, \sqrt[m]{s_{k-1}}\right)$$

числом $\sqrt[m]{s_k}$ оказалось степени $m/2$.

Возьмём первое расширение из цепочки, которое содержит $\sqrt{n}$, где $n$ удовлетворяет двум условиям:

- $n$ свободно от квадратов;
- у $n$ найдётся такой простой делитель, корнем из которого мы в этой цепочке ещё не расширяли, и он не равен $p_1, \ldots, p_{b_l}$.

Такое $n$ существует, так как $s_k$ обладает обоими указанными свойствами. Далее по лемме 2 получим, что

$$\sqrt{n} = \alpha \cdot \sqrt[m]{p^j},$$

где $p$ — последний элемент, корнем из которого мы расширяли, а $\alpha$ лежит в поле (обозначим его $\mathbb{F}$), которое было получено до присоединения корня из $p$.

Если $n$ делится на $p$, то разделим обе части на $\sqrt{p}$ и возьмём в качестве $n$ новое число под корнем в левой части, а в качестве $j$ — новый показатель в степени числа $p$ под корнем.

Заметим, что $j \neq m$, так как мы взяли первое расширение с такими условиями. Предположим, что $j \neq m/2$. Тогда расширим $\mathbb{F}$ корнями $m$-й степени из всех простых чисел, делящих $n$. Полученное поле $\mathbb{K}$ содержит $\sqrt[m]{p^j}$ и $p = \sqrt[m]{p^m}$. Тогда $\mathbb{K}$ содержит $\sqrt[m]{p}$ в степени меньшей, чем $m/2$. Следовательно, $[\mathbb{K}(\sqrt[m]{p}) : \mathbb{K}] < m/2$, что противоречит результату первого шага.

Итак, $j = m/2$, т. е. $\sqrt{n} = \alpha\sqrt{p}$. Домножив обе части на $\sqrt{p}$, получим $\sqrt{np} = \alpha p$. Следовательно, $\sqrt{np} \in \mathbb{F}$.

Предположим, что $n$ не делится на $p$. Тогда число $np$ обладает указанными выше свойствами. Во-первых, оно свободно от квадратов. Во-вторых, $np$ делится на простое нужного вида (ибо делится на все делители числа $n$).

Пусть теперь $n$ делится на $p$. Тогда число $n/p$ принадлежит $\mathbb{F}$ и обладает нужными свойствами. Во-первых, оно свободно от квадратов. Во-вторых, оно делится на все делители числа $n$, кроме $p$. Следовательно, у него есть простой делитель нужного вида, а именно тот же, что и для $n$ (число $p$ не является таким делителем для $n$, так как корень из него мы в цепочке расширений присоединяли).

В обоих случаях мы получили противоречие с минимальностью расширения.

### Шаг 4

*На этом шаге мы докажем утверждение теоремы.*

Предположим, что для некоторого поля $R = \mathbb{Q}(\sqrt[m]{w_1}, \ldots, \sqrt[m]{w_n})$, где все $w_i$ простые, выполнено неравенство $[R : \mathbb{Q}] < m^n$. В цепочке 3, построен-

ной на шаге 3, найдётся расширение $L$, содержащее $R$. Пусть $L$ получено из $\mathbb{Q}$ присоединением $k$ радикалов $m$-й степени из простых чисел. Тогда $L$ получается из $R$ присоединением $k-n$ таких радикалов, поэтому $[L:R] \leqslant m^{k-n}$. Следовательно,

$$[L:\mathbb{Q}] = [L:R]\cdot[R:Q] < m^{k-n}\cdot m^n = m^k.$$

Теперь докажем, что $[L:\mathbb{Q}] \geqslant m^k$, тем самым получив нужное противоречие.

Пусть $\mathbb{K}$ — подполе в $\mathbb{Q}(\omega)$, получившееся присоединением к $\mathbb{Q}$ всех тех квадратных корней из натуральных чисел, которые содержатся в поле $\mathbb{Q}(\omega)$. Положим $[\mathbb{K}:\mathbb{Q}] = 2^l$. Как следует из доказанного на шаге 3, $[\mathbb{L}:\mathbb{Q}(\omega)] = m^k/2^l$. Отсюда

$$[\mathbb{L}:\mathbb{Q}] = [\mathbb{L}:\mathbb{K}]\cdot[\mathbb{K}:\mathbb{Q}] \geqslant [\mathbb{L}:\mathbb{Q}(\omega)]\cdot[\mathbb{K}:\mathbb{Q}] = \frac{m^k}{2^l}\cdot 2^l = m^k,$$

что и требовалось. □

Выведем из теоремы 4 основной факт.

Теорема 5. *Числа* $1, \sqrt[m_1]{n_1}, \sqrt[m_2]{n_2}, \ldots, \sqrt[m_k]{n_k}$ *обязательно линейно независимы над* $\mathbb{Q}$, *если каждый радикал* $\sqrt[m_i]{n_i}$ *нельзя сократить* (*т. е.* $n_i$ *не является точной* $l$*-й степенью, где* $l$ *— делитель числа* $m_i$) *и каждое* $n_i$ *свободно от* $m_i$*-х степеней.*

Доказательство. Предположим противное. Тогда существуют такие $\gamma_i$, что

$$\sum_{i=1}^{k} \gamma_i \sqrt[m_i]{n_i} = 0.$$

Пусть $M = m_1\cdot\ldots\cdot m_k$ и $\alpha_i = m_1\cdot\ldots\cdot m_{i-1}m_{i+1}\cdot\ldots\cdot m_k = M/m_i$. Тогда

$$0 = \sum_{i=1}^{k} \gamma_i \cdot \sqrt[m_i]{n_i} = \sum_{i=1}^{k} \gamma_i \cdot \sqrt[M]{n_i^{\alpha_i}}.$$

Все $n_i^{\alpha_i}$ свободны от $M$-х степеней, так как $n_i$ свободны от $m_i$-х степеней.

Заметим, что не все $n_i^{\alpha_i}$ различны, так как иначе мы придём к противоречию с теоремой 4. Значит, найдутся такие $i, j$, что $n_i^{\alpha_i} = n_j^{\alpha_j}$, т. е.

$$n_i^{M/m_i} = n_j^{M/m_j}.$$

Следовательно, $\sqrt[m_i]{n_i} = \sqrt[m_j]{n_j}$, но так быть не может, так как радикалы по условию несократимы. □

## § 6. Заключение

В данной работе были приведены альтернативные доказательства классических результатов. Но такими же методами можно исследовать менее изученные области. Например, для нечётного $m$ можно вычислить группу Галуа расширения $\mathbb{Q}(\exp(2\pi i/m))$ числами $\{\sqrt[m]{p_1}, \ldots, \sqrt[m]{p_n}\}$. Из теоремы 3 следует, что она изоморфна прямой сумме $n$ экземпляров группы $\mathbb{Z}_m$.

Вероятно, приведёнными методами вычисляется и соответствующая группа Галуа для чётного $m$.

## Список литературы

[1] *Белов А. Я.* О круговых многочленах // Математическое просвещение. Сер. 3. Вып. 8. М.: МЦНМО, 2004. С. 181–184.

[2] *Винберг Э. Б.* Курс алгебры. М.: МЦНМО, 2021. С. 465–477.

[3] *Ленг С.* Алгебра. М.: Мир, 1968. Гл. 8.

[4] *Besicovitch A. S.* On the Linear Independence of Fractional Powers of Integers // J. Lond. Math. Soc. 1940. V. 15, № 1. P. 3–6.

[5] *Richards I.* An Application of Galois Theory to Elementary Arithmetic // Adv. in Math. 1974. V. 13, № 3. P. 268–273.

Иван Евгеньевич Воробьёв, ВШЭ, студент факультета математики
s19b1_vorobiov@179.ru