Как придумать построение правильного семнадцатиугольника (окончание)

А. Л. Канунников

В статье [4] мы рассказали, как доказать теорему Гаусса — Ванцеля и как прийти для этого к периодам Гаусса, используя базовые факты об алгебраических числах. В продолжении статьи мы покажем, как с помощью тех же средств придумать ещё одно доказательство, также восходящее к Гауссу [2, п. 360]. Оно короче, чем рассуждение с периодами, но может показаться менее естественным, поскольку основано на рассмотрении величины, «будто свалившейся с неба», так называемой *резольвенты Лагранжа*. Мы покажем, как прийти к резольвенте Лагранжа естественным путём и как её обобщение применяется в критерии Галуа разрешимости уравнений в радикалах. Интересно, что доказательство теоремы Галуа о циклических расширениях (ключевой в этом критерии) фактически повторяет рассуждение Гаусса с резольвентой.

Напомним, что теорема Гаусса — Ванцеля описывает все натуральные n, при которых правильный n-угольник строится циркулем и линейкой. Наиболее содержательная часть состоит в следующем.

Теорема 1. *Для любого простого числа Ферма $p = 2^m + 1$ число*

$$\varepsilon_p = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

поликвадратично (*выражается в квадратных радикалах*).

Минимальным многочленом числа $\varepsilon = \varepsilon_p$ над $\mathbb{Q}$ является круговой многочлен $\Phi_p(x) = \frac{x^p-1}{x-1}$ [4], поэтому $[\mathbb{Q}(\varepsilon):\mathbb{Q}] = p-1$. В [4] мы построили поликвадратичную башню $\mathbb{Q} \subset \ldots \subset \mathbb{Q}(\varepsilon)$, на каждом шаге присоединяя периоды.

При поддержке гранта Московского центра фундаментальной и прикладной математики.

§ 7. Как прийти к резольвенте Лагранжа

Выясним, можно ли получить ε, сразу присоединив к $\mathbb{Q}$ неприводимый радикал степени $p-1$, т. е. такое $r \in \mathbb{C}$, что $r^{p-1} \in K$ и двучлен $x^{p-1} - r^{p-1}$ неприводим над $\mathbb{Q}$. Предположим, это возможно: $\mathbb{Q}(\varepsilon) = \mathbb{Q}(r)$. Круговое расширение $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ обладает свойством: *все сопряжённые с любым элементом этого расширения лежат в нём* (так как сопряжённые с $f(\varepsilon)$, где $f \in \mathbb{Q}[x]$, имеют вид $f(\varepsilon^k)$). Такие расширения называются *нормальными*. Таким образом, расширение $\mathbb{Q}(r)/\mathbb{Q}$ тоже должно быть нормальным, поэтому все сопряжённые с r — числа $r, r\delta, \ldots, r\delta^{p-2}$, где $\delta = \varepsilon_{p-1}$, — лежат в $\mathbb{Q}(r)$. Значит, $\delta \in \mathbb{Q}(r) = \mathbb{Q}(\varepsilon)$. Но $\mathbb{Q}(\varepsilon_m) \cap \mathbb{Q}(\varepsilon_n) = \mathbb{Q}$ при взаимно простых m и n [3, задача 18], в частности,

$$\mathbb{Q}(\varepsilon_p) \cap \mathbb{Q}(\varepsilon_{p-1}) = \mathbb{Q}. \tag{1}$$

С одной стороны, при $p > 3$ получаем противоречие. С другой стороны, ясно, как спасти рассуждение: нужно вместо поля $\mathbb{Q}$ взять $\mathbb{Q}(\delta)$, тогда $[\mathbb{Q}(\varepsilon, \delta) : \mathbb{Q}(\delta)] = [\mathbb{Q}(\varepsilon) : \mathbb{Q}] = p-1$ благодаря (1).

Итак, попробуем найти r так, что $r^{p-1} \in \mathbb{Q}(\delta)$ и $\mathbb{Q}(\delta, \varepsilon) = \mathbb{Q}(\delta, r)$. Пусть такое r найдено. Тогда $[\mathbb{Q}(\delta, r) : \mathbb{Q}(\delta)] = p-1$ и число $\varepsilon \in \mathbb{Q}(\delta, r)$ имеет вид

$$\varepsilon = a_0 + a_1 r + \ldots + a_{p-2} r^{p-2} \tag{2}$$

для некоторых однозначно определённых $a_0, \ldots, a_{p-2} \in \mathbb{Q}(\delta)$. Сопряжённые с ε, с одной стороны, являются его степенями $\varepsilon, \ldots, \varepsilon^{p-1}$, а с другой, получаются из (2) подстановкой вместо r его сопряжённых $r, r\delta, \ldots, r\delta^{p-2}$. Таким образом,

$$\varepsilon^{n_k} = a_0 + a_1 r\delta^k + \ldots + a_{p-2} r_{p-2} \delta^{k(p-2)},$$
$$n_0 = 1, \quad \{n_1, \ldots, n_{p-2}\} = \{2, \ldots, p-1\}.$$

Сложив все ε^{n_k} с коэффициентами δ^{-k}, получим:

$$\varepsilon + \delta^{-1}\varepsilon^{n_1} + \delta^{-2}\varepsilon^{n_2} + \ldots + \delta^{-p+2}\varepsilon^{n_{p-2}} = (p-1)a_1 r. \tag{3}$$

Выражение $(p-1)a_1 r$ тоже является радикалом степени $p-1$, как и r, если только $a_1 \neq 0$. Это подсказывает идею стартовать с левой части (3) — нужно только *выбрать удачную нумерацию* $n_0, \ldots, n_{p-2}$.

Пример 1. Рассмотрим случай $p = 5$. Тогда $\varepsilon_{p-1} = \delta = i$. Имеем

$$\left.\begin{aligned} \varepsilon = \varepsilon^{n_0} &= a_0 + a_1 r + a_2 r^2 + a_3 r^3, \\ \varepsilon^{n_1} &= a_0 + a_1 ri - a_2 r^2 - a_3 r^3 i, \\ \varepsilon^{n_2} &= a_0 - a_1 r + a_2 r^2 - a_3 r^3, \\ \varepsilon^{n_3} &= a_0 - a_1 ri - a_2 r^2 + a_3 r^3 i \end{aligned}\right\} \quad \Rightarrow \quad \varepsilon^{n_0} - i\varepsilon^{n_1} - \varepsilon^{n_2} + i\varepsilon^{n_3} = 4a_1 r.$$

Расположим степени ε, последовательно возводя в квадрат: $\varepsilon, \varepsilon^2, \varepsilon^4, \varepsilon^8 = \varepsilon^3$, т. е. $(n_1, n_2, n_3) = (2, 4, 3)$. При подстановке вместо ε его сопряжённых выражение $\varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^3$ умножается на степени мнимой единицы i:

$$\mathscr{L}(\varepsilon) := \varepsilon - i\varepsilon^2 - \varepsilon^4 + i\varepsilon^3 \xrightarrow{\cdot i} \varepsilon^2 - i\varepsilon^4 - \varepsilon^8 + i\varepsilon^6 = \mathscr{L}(\varepsilon^2) \xrightarrow{\cdot i} \mathscr{L}(\varepsilon^4) \xrightarrow{\cdot i} \mathscr{L}(\varepsilon^8).$$

Вернёмся к общему случаю. Чтобы добиться того же эффекта циклического сдвига, нужно найти первообразный корень g по модулю p и расположить степени ε, последовательно возводя в степень g: $\varepsilon, \varepsilon^g, \varepsilon^{g^2}, \ldots, \varepsilon^{g^{p-2}}$, т. е. $n_k = g^k$. Ту же самую идею мы применили, придумывая периоды Гаусса. Проведённый анализ и пример подсказывают, что в качестве искомого радикала должна подойти *резольвента Лагранжа* — число $\mathscr{L}(\varepsilon)$, где

$$\mathscr{L}(x) := x + \delta^{-1}x^g + \delta^{-2}x^{g^2} + \ldots + \delta^{-p+2}x^{g^{p-2}} \in \mathbb{Q}(\delta)[x]. \tag{4}$$

Теорема 2. *Для любого простого p существует такое $r \in \mathbb{C}$, что $\mathbb{Q}(\varepsilon_{p-1}, \varepsilon_p) = \mathbb{Q}(\varepsilon_{p-1}, r)$ и $r^{p-1} \in \mathbb{Q}(\varepsilon_{p-1})$, в частности, $\varepsilon_p \in \mathbb{Q}(\varepsilon_{p-1}, r)$.*

Доказательство. Сохраним прежние обозначения ε, δ, g и положим

$$r := \mathscr{L}(\varepsilon) = \varepsilon + \delta^{-1}\varepsilon^g + \delta^{-2}\varepsilon^{g^2} + \ldots + \delta^{-p+2}\varepsilon^{g^{p-2}}. \tag{5}$$

Заметим, что $\mathscr{L}(\varepsilon^g) = \delta\mathscr{L}(\varepsilon) = \delta r$ и вообще

$$\mathscr{L}(\varepsilon^{g^k}) = \delta^k r, \quad k = 0, 1, \ldots, p-2. \tag{6}$$

По [3, теорема 6] числа в левых частях равенств (6) образуют набор сопряжённых с $\mathscr{L}(\varepsilon)$ над $\mathbb{Q}(\delta)$. С другой стороны, числа в правых частях образуют не что иное как набор корней двучлена $x^{p-1} - r^{p-1}$. Казалось бы, это и означает, что данный двучлен является минимальным многочленом для чисел (6). Есть только один нюанс: эти числа должны быть различны, т. е. $r \neq 0$. В противном случае $\mathscr{L}(\varepsilon) = 0$ и $\varepsilon, \varepsilon^g, \ldots, \varepsilon^{g^{p-2}}$ линейно зависимы над $\mathbb{Q}(\delta)$, что неверно в силу (1). Итак, минимальный многочлен $\mu_r^{\mathbb{Q}(\delta)}(x)$ числа r над полем $\mathbb{Q}(\delta)$ равен $x^{p-1} - r^{p-1}$, в частности, $r^{p-1} \in \mathbb{Q}(\delta)$ и $[\mathbb{Q}(\delta, r) : \mathbb{Q}(\delta)] = p-1$. Так как $\mathbb{Q}(\delta, r) \subseteq \mathbb{Q}(\delta, \varepsilon)$ и $[\mathbb{Q}(\delta, \varepsilon) : \mathbb{Q}(\delta)] = p-1$, мы получаем $\mathbb{Q}(\delta, \varepsilon) = \mathbb{Q}(\delta, r)$. □

Из теоремы 2 следует теорема 1, однако для явного выражения числа ε_p в радикалах степени $p-1$ нужны дополнительные усилия, помимо возведения резольвенты $\mathscr{L}(\varepsilon)$ в $(p-1)$-ю степень, см. [5], где приведено более конструктивное доказательство. Однако в любом случае вычисление этим методом гораздо более громоздко, нежели вычисление периодов. Это неудивительно: при последовательном вычислении периодов все участвующие радикалы оставались в поле $\mathbb{Q}(\varepsilon_p)$, в то время как в методе резольвент появляется новый радикал δ.

§ 8. Идеи Лагранжа

Методы решения уравнений 3-й и 4-й степеней, разработанные в XVI веке итальянскими математиками, были основаны на различных подстановках, заменах, использовали те или иные трюки. Лагранж, со свойственным ему педантизмом, пересмотрел и систематизировал накопленные знания, пытаясь найти универсальный метод, пригодный для уравнений высших степеней. Он разработал метод резольвент, идеи которого использовали Руффини, Абель, Гаусс, Галуа, исследуя проблему разрешимости в радикалах после Лагранжа. Именно в труде Лагранжа об алгебраических уравнениях (1771 г.) были заложены начала теории групп (Лагранж установил связь между порядком и индексом подгруппы в группе перестановок, не вводя явно этих терминов, и соответствующую теорему впоследствии назвали в его честь).

Главная идея Лагранжа в следующем: составить многочлен от корней $x_1, \ldots, x_n$ уравнения n-й степени, принимающий при их перестановках менее n значений, которых, однако, хватит с учётом формул Виета, чтобы восстановить $x_1, \ldots, x_n$. Соответствующие функции от корней и возникающие вспомогательные уравнения Лагранж и назвал резольвентами (resolve — разрешить). Рассмотрим примеры при $n = 3$ и 4.

Заметим прежде всего, что уравнение $y^n + ay^{n-1} + \ldots = 0$ сводится заменой $x = y + a/n$ к уравнению с нулевым коэффициентом при x^{n-1}. При $n = 2$ это означает выделение полного квадрата, приводящее к решению квадратного уравнения.

При $n = 3$ рассмотрим уравнение $x^3 + px + q = 0$ с корнями x_1, x_2, x_3. Анализируя вывод формулы Кардано, Лагранж приходит к следующей функции от корней:

$$\mathscr{C} = x_1 + \varepsilon x_2 + \varepsilon^2 x_3, \quad \text{где } \varepsilon = \varepsilon_3.$$

Переставляя x_1, x_2, x_3, получим 6 величин, причём при циклических сдвигах они пропорциональны $\mathscr{C}$:

$$x_2 + \varepsilon x_3 + \varepsilon^2 x_1 = \varepsilon^2 \mathscr{C}, \quad x_3 + \varepsilon x_1 + \varepsilon^2 x_2 = \varepsilon \mathscr{C}.$$

Следовательно, величина $\mathscr{C}^3$ не меняется при таких сдвигах и перестановками из неё можно получить ещё только одну величину:

$$\mathscr{C}'^3 = (x_1 + \varepsilon x_3 + \varepsilon^2 x_2)^3.$$

Поэтому величины $\mathscr{C}^3 + \mathscr{C}'^3$ и $\mathscr{C}^3 \mathscr{C}'^3$ симметрично зависят от x_1, x_2, x_3, а значит, выражаются через p и q. Именно,

$$(y - \mathscr{C}^3)(y - \mathscr{C}'^3) = y^2 + 27qy - 27p^3.$$

Остаётся найти корни этого трёхчлена, извлечь из них кубические корни и найти x_1, x_2, x_3 из системы

$$\begin{cases} x_1 + x_2 + x_3 = 0, \\ x_1 + \varepsilon x_2 + \varepsilon^2 x_3 = \mathscr{C}, \\ x_1 + \varepsilon^2 x_2 + \varepsilon x_3 = \mathscr{C}'. \end{cases}$$

Это — альтернативный способ вывести формулу Кардано

$$x_{1,2,3} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}},$$

где квадратные корни принимают одно и то же значение (неважно, какое), а кубические выбираются так, чтобы их произведение было равно $-p/3$.

Аналогично при $n = 4$ для многочлена с корнями x_1, x_2, x_3, x_4 можно рассмотреть выражение $x_1 + ix_2 - x_3 + ix_4$, четвёртая степень которого выдерживает циклические сдвиги, а потому принимает 6 значений при перестановках корней. Можно проверить, что возникающее уравнение 6-й степени распадается на два кубических, но гораздо проще использовать другие функции от корней, например,

$$\begin{cases} y_1 = x_1x_2 + x_3x_4, \\ y_2 = x_1x_3 + x_2x_4, \\ y_3 = x_1x_4 + x_2x_3. \end{cases} \tag{7}$$

Эти величины являются корнями кубического уравнения, коэффициенты которого полиномиально зависят от коэффициентов исходного многочлена 4-й степени. Вычисления показывают, что

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4) = x^4 + ax^2 + bx + c \quad \Rightarrow$$
$$\Rightarrow \quad (y - y_1)(y - y_2)(y - y_3) = y^3 - ay^2 - 4cy + 4ac - b^2.$$

Система (7) вместе с равенством $x_1 + x_2 + x_3 + x_4 = 0$ позволяет выразить x_1, x_2, x_3, x_4 через y_1, y_2, y_3 (см., например, [1, с. 139–140]).

§ 9. Резольвента Лагранжа в теории Галуа

Центральный результат теории Галуа — критерий разрешимости полиномиального уравнения в радикалах в терминах его группы Галуа. На этом пути Галуа и ввёл разрешимые группы. Не останавливаясь на теории Галуа подробно, докажем теорему 5 о циклических расширениях —

сердцевину критерия Галуа — и убедимся, что в основе лежит идея Гаусса применить резольвенту Лагранжа, как в теореме 2. Фактически Гаусс построил теорию Галуа двучленного уравнения. Начнём с необходимых определений и фактов.

Пусть L/K — конечное (а значит, алгебраическое) расширение полей, $[L:K]=n$. Будем считать все поля подполями в $\mathbb{C}$. Тогда для любого $\alpha\in\mathbb{C}$, алгебраического над K, многочлен $\mu_\alpha^K(x)$ не имеет кратных корней в $\mathbb{C}$ (см. [3, теорема 3]), поэтому α имеет столько сопряжённых над K, какова его степень (нет проблем с сепарабельностью).

Теорема 3 (о примитивном элементе). *Существует такое $\theta\in L$, что $L=K(\theta)$.*

Доказательство. Достаточно для любых $\alpha,\beta\in L$ найти такое θ, что $K(\theta)=K(\alpha,\beta)$ (далее — по индукции). Будем искать θ в виде $\theta=\alpha+c\beta$, где $0\ne c\in K$. Ясно, что $K(\alpha,\beta)=K(\theta)\iff\beta\in K(\theta)$. Рассмотрим многочлены $\mu_\beta^K(x)\in K[x]$ и $\mu_\alpha^K(\theta-cx)\in K(\theta)[x]$, имеющие общий корень β. Добьёмся того, чтобы β был единственным их общим корнем, тогда

$$\big(\mu_\beta(x),\mu_\alpha^K(\theta-cx)\big)=x-\beta\in K(\theta)[x]\quad\Rightarrow\quad\beta\in K(\theta).$$

Пусть $\alpha=\alpha_1,\dots,\alpha_m$ и $\beta=\beta_1,\dots,\beta_n$ — все сопряжённые с α и β. Тогда любой общий корень многочленов $\mu_\beta^K(x)$ и $\mu_\alpha^K(\theta-cx)$ — это такое β_j, что $\theta-c\beta_j=\alpha_i$ для некоторого i. Поскольку поле K бесконечно, элемент c можно выбрать так, чтобы равенство $\alpha+c\beta=\alpha_i+c\beta_j$ выполнялось только при $i=j=1$. □

Рассмотрим группу $\mathrm{Aut}_K L$ автоморфизмов L над K (тождественных на K).

Лемма 1. *Для всех $\alpha\in L$ и $g\in\mathrm{Aut}_K L$ элемент $g(\alpha)$ сопряжён с α над K.*

Доказательство. Имеем $\mu_\alpha^K(g(\alpha))=g(\mu_\alpha^K(\alpha))=g(0)=0$. □

Следствие 1. $|\mathrm{Aut}_K L|\leqslant[L:K]$.

Доказательство. Благодаря теореме 3, каждый автоморфизм $g\in\mathrm{Aut}_K L$ определяется значением на θ, причём $g(\theta)$ находится среди сопряжённых с θ, которых не более $\deg_K(\theta)=[L:K]$ штук. □

Если $|\mathrm{Aut}_K L|=[L:K]$, то L/K называют *расширением Галуа*, а группу $\mathrm{Aut}_K L$ — *группой Галуа* и обозначают также $\mathrm{Gal}_K L$.

Теорема 4. *Если L/K — расширение Галуа с группой G, то подполе*

$$L^G=\{\alpha\in L\mid\forall\, g\in G\ \ g(\alpha)=\alpha\}$$

неподвижных элементов совпадает с K.

Доказательство. По следствию 1, применённому к расширению L/L^G, имеем $|\mathrm{Aut}_{L^G} L| \leqslant [L : L^G]$, а поскольку $G = \mathrm{Aut}_{L^G} L$, то

$$|G| = |\mathrm{Aut}_{L^G} L| \leqslant [L:L^G] \leqslant [L:K] = |G| \quad \Rightarrow \quad [L:L^G] = [L:K] \quad \Rightarrow \quad L^G = K. \qquad \square$$

Замечание. Можно доказать, что в случае конечного расширения L/K равенство $L^G = K$ является критерием того, что L/K — расширение Галуа. Другая равносильная характеризация расширений Галуа — конечные нормальные сепарабельные расширения.

Предположим, что поле K содержит первообразный корень $\delta = \varepsilon_n$ из единицы степени n. Присоединим к полю K неприводимый радикал r степени n. Группа Галуа расширения $K(r)/K$ состоит из автоморфизмов $\phi_0, \ldots, \phi_{n-1}$ таких, что $\phi_j : r \mapsto r\delta^j$. Очевидно, $\phi_i \phi_j = \phi_{i+j \bmod n}$, поэтому $\phi_j = \phi_1^j$. Значит, $\mathrm{Gal}_K K(r) = \langle \phi_1 \rangle_n$ — циклическая группа порядка n. В основе критерия Галуа разрешимости в радикалах лежит обращение этого факта.

Теорема 5. *Пусть L/K — расширение Галуа, $\delta = \varepsilon_n \in K$ и $G = \mathrm{Gal}_K L = \langle g \rangle_n$. Тогда $L = K(r)$ для некоторого такого $r \in L$, что $r^n \in K$.*

Будем следовать доказательству теоремы 2 для расширения $L/K = \mathbb{Q}(\delta, \varepsilon_p)/\mathbb{Q}(\delta)$ и анализу, который нас к нему привёл.

Анализ. Предположим, что искомый радикал r найден. Сопряжённые с r суть $r\delta^k$, $k \in \mathbb{Z}_n$. Можно считать, что $g(r) = r\delta$. Сопряжённые с любым элементом $\alpha = \sum_{j=0}^{n-1} a_j r^j \in L$ $(a_j \in K)$ суть $\sum_{j=0}^{n-1} a_j r^j \delta^{kj} = g^k(\alpha)$, $k \in \mathbb{Z}_n$. Деля k-е равенство на δ^k и складывая полученные равенства, получим *резольвенту Лагранжа* $na_1 r = \sum_{k=0}^{n-1} \varepsilon^{-k} g^k(\alpha)$. При $a_1 \neq 0$ элемент $na_1 r$ также является радикалом, порождающим L. Это подсказывает идею стартовать с резольвенты Лагранжа, построенной по произвольному $\alpha \in L$, имеющему n сопряжённых, т. е. с примитивного элемента расширения L/K.

Доказательство теоремы 5. Найдём примитивный элемент $\alpha \in L$, $L = K(\alpha)$, и рассмотрим резольвенту Лагранжа

$$r = \alpha + \delta^{-1} g(\alpha) + \delta^{-2} g^2(\alpha) + \ldots + \delta^{-n+1} g^{n-1}(\alpha), \tag{8}$$

замечательную тем, что $g(r) = \delta r$ (поскольку $\delta \in K \Rightarrow g(\delta) = \delta$). Отсюда получаем два следствия:

1) $g(r^n) = g(r)^n = r^n \Rightarrow r^n \in L^G = K$ (теорема 4);
2) $\forall\, i \in \{0, \ldots, n-1\}$ $g^i(r) = \delta^i r \Rightarrow r = 0$ или $|Gr| = n$.

Поскольку все элементы из орбиты Gr сопряжены с r над K (лемма 1), при $r \neq 0$ имеем

$$[L : K] = n \leqslant \deg_K(r) = [K(r) : K] \leqslant [L : K] \quad \Rightarrow \quad L = K(r).$$

Таким образом, элемент r искомый, если только он отличен от нуля. Если $r = 0$, то построим аналогичные резольвенты по степеням $\alpha, \dots, \alpha^{n-1}$:

$$r_k = \alpha^k + \delta^{-1} g(\alpha^k) + \delta^{-2} g^2(\alpha^k) + \dots + \delta^{-n+1} g^{n-1}(\alpha^k), \quad k = 1, \dots, n-1. \tag{9}$$

Так как $g(r_k) = \delta r_k$, верны те же следствия: $r_k^n \in K$ и либо $r_k = 0$, либо $L = K(r_k)$. Предположим, что $r_1 = \dots = r_{n-1} = 0$. Тогда набор $(1, \varepsilon^{-1}, \dots, \varepsilon^{1-n})$ является решением однородной системы линейных уравнений с матрицей $(g^j(\alpha^i))_{0 \leqslant i,j \leqslant n-1}$ (при $i = 0$ получается верное равенство $1 + \delta^{-1} + \dots + \delta^{1-n} = 0$). Значит, эта матрица вырожденна, т. е. её определитель равен 0. Но это определитель Вандермонда

$$\prod_{i>j} (g^i(\alpha) - g^j(\alpha)),$$

поэтому $g^k(\alpha) = g^l(\alpha)$ при некоторых $1 \leqslant k < l < n$, а тогда $g^k = g^l$, так как α порождает L. Полученное противоречие показывает, что $r_k \neq 0$ при некотором $k \in \{1, \dots, n-1\}$ и $L = K(r_k)$. □

Список литературы

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

[2] *Гаусс К. Ф.* Арифметические исследования // Труды по теории чисел. М.: АН СССР, 1959.

[3] *Канунников А. Л.* Алгебраические числа как векторы // Математическое просвещение. Сер. 3. Вып. 26. М.: МЦНМО, 2020. С. 111–142.

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

[5] *Скопенков А. Б.* Ещё одно доказательство из книги: теорема Гаусса — Ванцеля // Математическое просвещение. Сер. 3. Вып. 27. М.: МЦНМО, 2021. С. 133–141.

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