Неприводимо-радикальные расширения полей

А. Л. КАНУННИКОВ
Московский государственный университет им. М. В. Ломоносова,
Московский центр фундаментальной и прикладной математики

А. И. ПЕКАРСКИЙ
Московский государственный университет им. М. В. Ломоносова
e-mail: xfasolx@yandex.ru

УДК 512.623.3

Ключевые слова: расширения Галуа, разрешимость в радикалах, круговые расширения.

Аннотация

В статье исследованы неприводимо-радикальные расширения полей, т. е. расширения, которые можно получить последовательным присоединением корней неприводимых двучленов. Установлен критерий неприводимой радикальности круговых расширений поля $\mathbb{Q}$, обобщающий теорему Гаусса—Ванцеля о правильных многоугольниках, которые можно построить циркулем и линейкой. Также доказано, что если основное поле содержит все корни из единицы, то всякое нормальное расширение, содержащееся в радикальном, является неприводимо-радикальным. Это обобщает теорему Абеля, восполняющую пробел Руффини в доказательстве неразрешимости общего уравнения степени 5 и выше. Наконец, с помощью неприводимо-радикальных расширений доказано существование радикальной формулы, множество значений которой совпадает с множеством корней данного неприводимого уравнения.

Abstract

A. L. Kanunnikov, A. I. Pekarsky, Irreducible radical field extensions, Fundamentalnaya i prikladnaya matematika, vol. 23 (2021), no. 4, pp. 87—98.

This paper is devoted to irreducible radical field extensions, i.e., extensions that can be obtained by adjunction of roots of irreducible binomials. We find a criterion for cyclotomic extensions to be irreducible radical. This criterion developes the Gauss–Wantzel theorem about constructible polygons. We also prove that any normal solvable extension of some field K is irreducible radical until K has all roots of unity. This generalizes Abel's theorem, which fills the gap in the uncomplete Ruffini proof of the impossibility theorem for the general equation of degree five or higher. Finally, we prove that the root set of any irreducible solvable polynomial coincides with the value set of some radical formula using irreducible radical extensions.

Введение

Вопрос о разрешимости уравнений в радикалах интересовал математиков с древних времён и был главным вопросом алгебры до начала XIX века. К основным вехам в истории этой проблемы относятся:

Фундаментальная и прикладная математика, 2021, том 23, № 4, с. 87—98.

— открытие комплексных чисел итальянскими математиками XVI века при решении уравнений степеней 3 и 4;
— начала теории групп перестановок в работах Лагранжа второй половины XVIII века;
— построение Гауссом в 1796 году правильного 17-угольника с помощью циркуля и линейки и развитая им теория периодов для уравнений деления круга;
— теорема Абеля—Руффини о неразрешимости общего уравнения степени 5 и выше (1824 г.);
— работы Галуа 1828—1832 гг., в которых был дан критерий разрешимости уравнений в радикалах и которые заложили основы теории групп и полей, определив новый этап развития алгебры.

Галуа установил биективное соответствие между подполями поля разложения сепарабельного многочлена и подгруппами его группы автоморфизмов (группы Галуа). При соответствиях Галуа расширениям, содержащимся в радикальных, соответствуют в точности разрешимые группы. Среди радикальных расширений важную роль играют неприводимо-радикальные — те, которые можно получить, последовательно присоединяя корни неприводимых двучленов. Они удобны главным образом по следующей причине: если двучлен $x^n - r^n$ неприводим над полем K, то расширение $K(r)/K$ имеет базис $1, r, \ldots, r^{n-1}$. Классические теоремы Абеля, Галуа, Кронекера и др. о неразрешимости в радикалах используют неприводимо-радикальные расширения. Их исследование начал Гаусс [3] для уравнения $x^n = 1$. Гаусс доказал, говоря современным языком, что круговое расширение $\mathbb{Q}(\varepsilon_n)/\mathbb{Q}$ ($\varepsilon_n = e^{2\pi i/n}$) содержится в неприводимо-радикальным, причём в случае, когда n — произведение степени двойки и различных простых чисел Ферма, это расширение поликвадратично (получается присоединением квадратных радикалов). Мы установили критерий неприводимой радикальности кругового расширения (теорема 7). Согласно этому критерию расширение $\mathbb{Q}(\varepsilon_n)/\mathbb{Q}$ не является неприводимо-радикальным, например, при $n = 7, 19, 33$ и является при $n = 9, 21, 55$. Таким образом, класс радикальных расширений шире класса неприводимо-радикальных расширений.

Важно отметить, что класс разрешимых расширений (расширений, содержащихся в радикальных) шире класса радикальных расширений (пример 1), и именно из-за этого обстоятельства доказательство Руффини 1799 года неразрешимости общего уравнения степени 5 и выше содержало серьёзный пробел. Фактически Руффини доказал более слабое утверждение о том, что поле разложения общего многочлена степени $n \geqslant 5$ не является радикальным. В 1824 году Абель независимо доказал, что оно не содержится в радикальном. Мы обобщим часть теоремы Абеля, восполняющую пробел Руффини, и докажем, что при наличии корней из единицы в основном поле всякое нормальное разрешимое расширение является радикальным и, более того, неприводимо-радикальным (теорема 8).

1. Предварительные сведения и факты

Если не оговорено противное, все элементы и поля содержатся в алгебраическом замыкании $\bar{K}$ данного поля K. Запись $K \xrightarrow{n} L$ означает, что L/K — расширение полей степени n. Хорошо известна лемма о башне: если $K \xrightarrow{m} P \xrightarrow{n} Q$, то $K \xrightarrow{mn} Q$. Минимальный многочлен над K элемента $\alpha \in \bar{K}$ будем обозначать $\mu_\alpha^K(x)$ или просто $\mu_\alpha(x)$, если ясно, о каком поле K идёт речь. Любой первообразный корень степени n из единицы будем обозначать ε_n (при условии, что он существует в $\bar{K}$, т. е. $\operatorname{char} K \nmid n$).

Радикальные расширения

Определение 1. Башня полей

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m \tag{1}$$

называется радикальной, если при каждом $j = 1, \ldots, m$ существуют такие $r_j \in K_j$ и $p_j \in \mathbb{N}$, что $K_j = K_{j-1}(r_j)$. Если при этом для каждого $j = 1, \ldots, m$ двучлен $x^{p_j} - r_j^{p_j}$ неприводим над полем K_{j-1}, то башня (1) называется непривидимо-радикальной. Иногда радикальную башню нам удобнее записывать в виде $(K_0; r_1, r_2, \ldots, r_m)$, последовательно перечисляя присоединяемые радикалы.

Определение 2. Расширение полей L/K называется радикальным (непривидимо-радикальным), если существует радикальная (непривидимо-радикальная) башня (1), для которой $K_0 = K$ и $K_m = L$. Расширение полей L/K называется разрешимым, если оно содержится в радикальном.

Определение 3. Говорят, что элемент α расширения полей L/K выражается в радикалах (в непривидимых радикалах) над K, если α лежит в некотором радикальном (непривидимо-радикальном) расширении поля K.

Говорят, что уравнение $f(x) = 0$, где $f \in K[x]$, разрешимо в радикалах (непривидимых радикалах) над K, если поле разложения многочлена f содержится в некотором радикальном (непривидимо-радикальном) расширении поля K.

Пример 1. Уравнение

$$4x^3 - 3x + \frac{1}{2} = 0$$

имеет корни

$$\cos\frac{2\pi k}{9}, \quad k = 1, 2, 4.$$

Они выражаются в радикалах по формуле Кардано:

$$\left\{2\cos\frac{2\pi}{9},\, 2\cos\frac{4\pi}{9},\, 2\cos\frac{8\pi}{9}\right\} = \sqrt[3]{\frac{-1+\sqrt{-3}}{2}} + \sqrt[3]{\frac{-1-\sqrt{-3}}{2}} = \sqrt[3]{\varepsilon_3} + \sqrt[3]{\bar{\varepsilon}_3}, \tag{2}$$

где значения кубических радикалов всегда выбираются сопряжёнными.

В то же время расширение $\mathbb{Q}\big(\cos(2\pi/9)\big)/\mathbb{Q}$ не является радикальным. В самом деле, оно имеет степень 3, поэтому если оно радикально, то получается присоединением одного радикала, причём действительного. Итак, пусть $\mathbb{Q}\big(\cos(2\pi/9)\big) = \mathbb{Q}\big(\sqrt[n]{a}\big)$, где $a \in \mathbb{Q}$, $r = \sqrt[n]{a} \in \mathbb{R}$. Можно считать, что $n \in \mathbb{N}$ — наименьшее число с условием $r^n \in \mathbb{Q}$. Тогда двучлен $x^n - a$ неприводим над $\mathbb{Q}$, поэтому $n = 3$. Следовательно, расширение $\mathbb{Q}\big(\sqrt[n]{a}\big)$ не является нормальным, так как не содержит комплексных корней двучлена $x^n - a$, в то время как расширение $\mathbb{Q}\big(\cos(2\pi/9)\big)$ нормально.

Лемма 1. *Всякую радикальную башню можно уплотнить до башни с простыми показателями радикалов. При этом неприводимо-радикальная башня уплотняется до неприводимо-радикальной.*

Доказательство. Достаточно последовательно заменять расширения вида $K \subset K(r)$, где $r^{mn} \in K$ $(m, n \in \mathbb{N})$, башней $K \subset K(r^m) \subset K(r)$. Если при этом двучлен $x^{mn} - r^{mn}$ был неприводим над K, то $[K(r) : K] = mn$, следовательно, $[K(r^m) : K] = n$ и $[K(r) : K(r^m)] = m$, поэтому уплотнённая башня тоже неприводимо-радикальная. □

Присоединение радикала простой степени описывает следующая лемма Абеля (сформулированная Абелем для числовых полей).

Лемма 2 (Абель). *Пусть p — простое число, K — поле, $\operatorname{char} K \neq p$, $r \in \bar{K} \setminus K$, $r^p \in K$. Тогда либо двучлен $x^p - r^p$ неприводим над K, либо $r^p \in K^p$ и тогда $K(r) = K(\varepsilon_p)$.*

Доказательство. Имеем $x^p - r^p = (x - r)(x - r\varepsilon)\dots(x - r\varepsilon^{p-1})$, где $\varepsilon = \varepsilon_p$. Если двучлен $x^p - r^p$ имеет над K делитель степени $s \in \{1, \dots, p-1\}$, то его свободный член лежит в K и имеет вид $(-r)^s\varepsilon^t$, откуда следует, что $r^s \in K\varepsilon^{-t}$. Далее, $(s, p) = 1 = us + vp$ для некоторых $u, v \in \mathbb{Z}$, откуда получаем, что $r = (r^s)^u(r^p)^v \in K\varepsilon^{-tu}$. При этом $\varepsilon^{tu} \neq 1$, иначе $r \in K$, что противоречит условию. Поэтому $K(r) = K(\varepsilon^{tu}) = K(\varepsilon)$ и $r^p \in (K\varepsilon^{-tu})^p = K^p$. □

Теорема 1 (Гаусс [3]). *Для каждого простого $p \geqslant 3$ существуют такие числа $t_1, \dots, t_{p-2}$, что $t_1^{p-1}, \dots, t_{p-2}^{p-1} \in \mathbb{Z}[\varepsilon_{p-1}]$ и $\varepsilon_p \in \mathbb{Q}(\varepsilon_{p-1}, t_1, \dots, t_{p-2})$.*

Теорема 2. *Всякое радикальное расширение содержится в неприводимо-радикальном.*

Доказательство. Докажем, что последний этаж произвольной радикальной башни

$$(K; r_1, r_2, \dots, r_m), \quad \text{где} \quad r_i^{k_i} \in K_{i-1} = K(r_1, \dots, r_{i-1}), \quad i = 1, \dots, m, \tag{3}$$

содержится в неприводимо-радикальном расширении поля $K = K_0$, с помощью двойной индукции по

$$N = \max_{1 \leqslant i \leqslant m} \{k_i \mid x^{k_i} - r_i^{k_i} \text{ приводим над } K_{i-1}\}$$

и по m.

(A) Предположим, что для башен с $N < p$ утверждение доказано. Если p составное, то башню с $N = p$ по лемме 1 можно уплотнить до башни с $N < p$ и сразу воспользоваться предположением (A). Для башен с простым $N = p$ проведём индукцию по m.

(B) При $m = 1$ приводимое расширение по лемме 2 имеет вид $K \subset K(\varepsilon_p)$ (обязательно $\operatorname{char} K \neq p$) и по теореме Гаусса 1 содержится в последнем этаже башни с $N = p - 1$, к которой применимо предположение (A). Пусть теперь дана башня (3) с $N = p$, в которой первый радикал r_1 приводим (иначе сразу применимо предположение индукции по m к башне, начинающейся с $K(r_1)$). По доказанному (B) $(K; r_1)$ можно заменить неприводимо-радикальной башней $(K; \rho_1, \ldots, \rho_s)$. Теперь к башне $(K(\rho_1, \ldots, \rho_s); r_2, \ldots, r_m)$ применимо предположение индукции по m. □

Расширения Галуа

Приведём ряд хорошо известных фактов из теории Галуа. Их можно найти, например, в [4]. Конечное нормальное сепарабельное расширение L/K называется *расширением Галуа*. В этом случае группа $\operatorname{Aut}_K L$ содержит ровно $[L : K]$ элементов, называется *группой Галуа* и обозначается также $\operatorname{Gal} L/K$. При этом расширение L/P является расширением Галуа для любого промежуточного поля P ($K \subseteq P \subseteq L$). Каждой подгруппе $H \subseteq G = \operatorname{Gal} L/K$ поставим в соответствие её поле инвариантов

$$L^H = \{\alpha \in L \mid h(\alpha) = \alpha \text{ для каждого } h \in H\}.$$

Отображения $P \mapsto G_P = \operatorname{Gal} L/P$ и $H \mapsto L^H$ называются *соответствиями Галуа*.

Теорема 3 (основная теорема теории Галуа). *Если L/K — расширение Галуа и $G = \operatorname{Gal} L/K$, то соответствия Галуа взаимно обратны. При этом расширение P/K нормально тогда и только тогда, когда подгруппа G_P нормальна в G, и в этом случае $G/G_P \cong \operatorname{Gal} P/K$.*

Связь между разрешимостью уравнения в радикалах и разрешимостью его группы Галуа основана на следующем результате.

Теорема 4. *Пусть L/K — расширение Галуа, $\operatorname{Gal} L/K \cong \mathbb{Z}_n$ и $\varepsilon_n \in K$, в частности, $\operatorname{char} K \nmid n$. Тогда существует такое $r \in L$, что $r^n \in K$ и $L = K(r)$.*

Теорема 5. *Для любого $n \in \mathbb{N}$ круговой многочлен $\Phi_n(x)$ неприводим над $\mathbb{Q}$, круговое расширение имеет степень $\varphi(n)$ и $\operatorname{Gal} \mathbb{Q}(\varepsilon_n)/\mathbb{Q} = \mathbb{Z}_n^*$.*

Следствие 1. *Для любых взаимно простых m и n имеем $\mathbb{Q}(\varepsilon_m) \cap \mathbb{Q}(\varepsilon_n) = \mathbb{Q}$.*

Теорема 6 (Гаусс, Ванцель). *Следующие условия на натуральное число $n \geqslant 3$ равносильны*:

1) *правильный n-угольник можно построить циркулем и линейкой*;
2) *$\varphi(n)$ — степень двойки*;

3) n — *произведение степени двойки и различных простых чисел Ферма* (*возможно отсутствие простых чисел*).

2. Результаты

Неприводимо-радикальные круговые расширения

Теорема 7. *Пусть* $n = 2^{k_0} p_1^{k_1} \dots p_s^{k_s}$ — *каноническое разложение на простые множители* ($2 < p_1 < \dots < p_s$ — *простые числа,* $k_0 \in \mathbb{N}_0$, $s \in \mathbb{N}_0$, $k_1, \dots, k_s \in \mathbb{N}$). *Тогда следующие условия равносильны*:

1) *круговое расширение* $\mathbb{Q}(\varepsilon_n)/\mathbb{Q}$ *является неприводимо-радикальным*;
2) $\varepsilon_q \in \mathbb{Q}(\varepsilon_n)$ *для любого простого делителя* q *числа* $\varphi(n)$;
3) *если* $s > 0$, *то для любого* $j = 1, \dots, s$ *все нечётные простые делители числа* $p_j - 1$ *содержатся среди чисел* $p_1, \dots, p_{j-1}$, *в частности,* p_1 — *простое число Ферма.*

Доказательству предпошлём ряд примеров и замечаний.

Следствие 2. *Примарное круговое расширение* $\mathbb{Q}(\varepsilon_{p^k})/\mathbb{Q}$, *где* p — *простое число и* $k \in \mathbb{N}$, *является неприводимо-радикальным тогда и только тогда, когда либо* $p = 2$, *либо* p — *простое число Ферма.*

Пример 2.

1. Расширение $\mathbb{Q}(\varepsilon_{2^k})/\mathbb{Q}$ является простым неприводимо-радикальным, так как ε_{2^k} — корень кругового многочлена $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$, неприводимого по лемме 5:
$$\mathbb{Q}(\varepsilon_{2^k}) = \mathbb{Q}(\sqrt[2^{k-1}]{-1}).$$
2. Поскольку $\varepsilon_3 = (-1 + i\sqrt{3})/2$, то $\mathbb{Q}(\varepsilon_3) = \mathbb{Q}(\sqrt{-3})$.
3. При $p = 5$ получаем башню
$$\mathbb{Q} \xrightarrow{2} \mathbb{Q}\left(\cos\frac{2\pi}{5}\right) = \mathbb{Q}(\sqrt{5}) \xrightarrow{2} \mathbb{Q}(\varepsilon_5) = \mathbb{Q}\left(\sqrt{\frac{-5-\sqrt{5}}{8}}\right).$$
4. Расширение $\mathbb{Q}(\varepsilon_p^k)/\mathbb{Q}(\varepsilon_p)$ при любом простом p является неприводимо-радикальным, так как
$$\mathbb{Q} \xrightarrow{p-1} \mathbb{Q}(\varepsilon_p) \xrightarrow{p^{k-1}} \mathbb{Q}(\varepsilon_{p^k}),$$
откуда следует, что ε_{p^k} — корень двучлена $x^{p^{k-1}} - \varepsilon_p$, неприводимого над $\mathbb{Q}(\varepsilon_p)$.
5. Расширение $\mathbb{Q}(\varepsilon_7)/\mathbb{Q}$ не является неприводимо-радикальным. В самом деле, его группа Галуа $\mathbb{Z}_7^*$ имеет ровно две собственные подгруппы, которым соответствуют подполя $\mathbb{Q}(\varepsilon_7 + \varepsilon_7^2 + \varepsilon_7^4) = \mathbb{Q}(\sqrt{-7})$ и $\mathbb{Q}(\varepsilon_7 + \varepsilon_7^6) = \mathbb{Q}\big(\cos(2\pi/7)\big)$, поэтому существуют ровно две башни
$$\mathbb{Q} \xrightarrow{2} \mathbb{Q}(\sqrt{-7}) \xrightarrow{3} \mathbb{Q}(\varepsilon_7) \quad \text{и} \quad \mathbb{Q} \xrightarrow{3} \mathbb{Q}(\cos\tfrac{2\pi}{7}) \xrightarrow{2} \mathbb{Q}(\varepsilon_7),$$

ни в одной из которых расширение степени 3 не является простым неприводимо-радикальным. В противном случае, будучи нормальным расширением степени 3, такое расширение содержало бы ε_3, но $\varepsilon_3 \notin \mathbb{Q}(\varepsilon_7)$ по лемме 1.

6. Расширение $\mathbb{Q}(\varepsilon_{21})/\mathbb{Q}$ является неприводимо-радикальным, так как второе расширение в башне

$$\mathbb{Q} \xrightarrow{2} \mathbb{Q}(\varepsilon_3) = \mathbb{Q}(\sqrt{-3}) \xrightarrow{6} \mathbb{Q}(\varepsilon_{21})$$

получается присоединением корня неприводимого двучлена шестой степени над $\mathbb{Q}(\varepsilon_3)$. Это следует из теоремы 4, поскольку группа $\operatorname{Gal}\mathbb{Q}(\varepsilon_{21})/\mathbb{Q}(\varepsilon_3) = \mathbb{Z}_7^*$ циклическая, а поле $\mathbb{Q}(\varepsilon_3)$ содержит $\varepsilon_6 = \varepsilon_3 + 1$.

Доказательство теоремы 7. Докажем импликацию (1) $\Longrightarrow$ (2). Пусть расширение $\mathbb{Q}(\varepsilon_n)/\mathbb{Q}$ является неприводимо-радикальным и

$$\mathbb{Q} = K_0 \xrightarrow{q_1} K_1 \xrightarrow{q_2} \dots \xrightarrow{q_m} K_m = \mathbb{Q}(\varepsilon_n) - \tag{4}$$

неприводимо-радикальная башня, в которой для каждого $j = 1, \dots, m$

1) $K_j = K_{j-1}(r_j)$, $r_j^{q_j} \in K_{j-1}$, q_j — простое число;
2) двучлен $x^{q_j} - r_j^{q_j}$ неприводим над K_{j-1}.

Тогда $\varphi(n) = [\mathbb{Q}(\varepsilon_n) : \mathbb{Q}] = q_1 \dots q_m$. При соответствии Галуа башне полей (4) соответствует композиционный ряд группы Галуа $\operatorname{Gal}\mathbb{Q}(\varepsilon_n)/\mathbb{Q} \cong \mathbb{Z}_n^*$. Поскольку эта группа абелева, то все её подгруппы нормальны, а значит, каждое расширение $K_j/\mathbb{Q}$ нормально. Зафиксируем $j = 1, \dots, m$. Поскольку простое радикальное расширение K_j/K_{j-1} степени $[K_j : K_{j-1}] = q_j$ нормально, то $K_j \ni \varepsilon_{q_j}$. Таким образом, $\varepsilon_{q_1}, \dots, \varepsilon_{q_m} \in \mathbb{Q}(\varepsilon_n)$.

Докажем импликацию (2) $\Longrightarrow$ (3). Пусть $s > 0$, $j = 1, \dots, s$ и q — любой нечётный простой делитель числа $p_j - 1$. Если $q \notin \{p_1, \dots, p_{j-1}\}$, то $(q, n) = 1$, а тогда $\mathbb{Q}(\varepsilon_q) \cap \mathbb{Q}(\varepsilon_n) = \mathbb{Q}$ по лемме 1, следовательно, $\varepsilon_q \notin \mathbb{Q}(\varepsilon_n)$.

Докажем импликацию (3) $\Longrightarrow$ (1). Будем последовательно присоединять к полю $\mathbb{Q}$ корни из единицы следующих степеней: $2^{k_0}, p_1, p_1^{k_1}, p_2, p_2^{k_2}, \dots, p_s, p_s^{k_s}$. Поскольку $2^{k_0}, p_1^{k_1}, \dots, p_s^{k_s}$ — попарно взаимно простые делители числа n, то при всех $j = 1, \dots, s$ поле $\mathbb{Q}(\varepsilon_{2^{k_0} p_1^{k_1} \dots p_j^{k_j}})$ имеет степень над $\mathbb{Q}$

$$\varphi(2^{k_0} p_1^{k_1} \dots p_j^{k_j}) = \varphi(2^{k_0})\varphi(p_1^{k_1}) \dots \varphi(p_j^{k_j}) = \varphi(2^{k_0}) p_1^{k_1 - 1}(p_1 - 1) \dots p_j^{k_j - 1}(p_j - 1).$$

Таким образом, мы получим следующую башню полей в $\mathbb{Q}(\varepsilon_n)$:

$$\mathbb{Q} \xrightarrow{\varphi(2^{k_0})} \mathbb{Q}(\varepsilon_{2^{k_0}}) \xrightarrow{p_1 - 1} \mathbb{Q}(\varepsilon_{2^{k_0} p_1}) \xrightarrow{p_1^{k_1 - 1}} \mathbb{Q}(\varepsilon_{2^{k_0} p_1^{k_1}}) \xrightarrow{p_2 - 1}$$

$$\xrightarrow{p_2 - 1} \mathbb{Q}(\varepsilon_{2^{k_0} p_1^{k_1} p_2}) \xrightarrow{p_2^{k_2 - 1}} \dots \xrightarrow{p_s^{k_s - 1}} \mathbb{Q}(\varepsilon_n). \tag{5}$$

Уплотним эту башню до башни с простыми степенями. Это можно сделать с помощью соответствий Галуа: башне (5) соответствует ряд подгрупп абелевой группы $\operatorname{Gal}\mathbb{Q}(\varepsilon_n)/\mathbb{Q} \cong \mathbb{Z}_n^*$, который можно уплотнить до композиционного и

которому будет соответствовать требуемая башня с простыми степенями, уплотняющая башню (5):

$$\mathbb{Q} \to \ldots \to \mathbb{Q}(\varepsilon_{2^{k_0}p_1^{k_1}}) \to \ldots \to \mathbb{Q}(\varepsilon_{2^{k_0}p_1^{k_1}p_2}) \to \ldots \to \\ \to \mathbb{Q}(\varepsilon_{2^{k_0}p_1^{k_1}p_2^{k_2}}) \to \ldots \to \mathbb{Q}(\varepsilon_n). \quad (6)$$

Докажем, что эта башня является неприводимо-радикальной. Расширения степени 2, очевидно, получаются присоединением квадратных радикалов. Каждое расширение $K \xrightarrow{q} L$, лежащее в башне (6) между $\mathbb{Q}(\varepsilon_{2^{k_0}\ldots p_j^{k_j}})$ и $\mathbb{Q}(\varepsilon_{2^{k_0}\ldots p_j^{k_j}p_{j+1}})$, имеющее нечётную простую степень q, получается присоединением корня неприводимого двучлена степени q по теореме 4, так как $\varepsilon_q \in K$ в силу условия (3):

— число p_1 — число Ферма, т. е. $p_1 - 1$ — степень двойки;
— любой нечётный простой делитель числа $p_2 - 1$ равен p_1;
— любой нечётный простой делитель числа $p_3 - 1$ равен p_1 или p_2 и т. д.

Каждое из остальных расширений $K \to L$ в (6) имеет некоторую степень p_j и по теореме 4 получается присоединением корня неприводимого двучлена степени p_j, поскольку $\varepsilon_{p_j} \in K$ по построению башни. □

Обобщение теоремы Абеля

Для удобства ссылок приведём хорошо известную лемму.

Лемма 3. *Пусть* $\alpha \in \bar{K}$, $\mu_\alpha^K(x) = (x - \alpha_1)\ldots(x - \alpha_n)$ *и* $f \in K[x]$. *Тогда* $f(\alpha_1), \ldots, f(\alpha_n)$ *— все сопряжённые с* $f(\alpha)$ *над* K *элементы.*

Доказательство. Поскольку α — корень многочлена $\mu_{f(\alpha)}\big(f(x)\big) \in K[x]$, то $\mu_\alpha(x) \mid \mu_{f(\alpha)}\big(f(x)\big)$, поэтому элементы $\alpha_1, \ldots, \alpha_n$ являются корнями многочлена $\mu_{f(\alpha)}\big(f(x)\big)$, а это значит, что $f(\alpha_1), \ldots, f(\alpha_n)$ сопряжены с $f(\alpha)$ над K. Других сопряжённых элементов нет, так как

$$F(x) = \prod_{i=1}^{n}(x - f(\alpha_i)) \in K[x]$$

и, следовательно, $\mu_{f(\alpha)}(x) \mid F(x)$. □

Теорему Абеля 1824 года на современном языке можно сформулировать так: при $n \geqslant 5$ поле разложения L общего многочлена

$$x^n + a_1x^{n-1} \ldots + a_{n-1}x + a_n \in \mathbb{C}(a_1, \ldots, a_n)[x] \quad (7)$$

не является разрешимым (коэффициенты $a_1, \ldots, a_n$ — формальные переменные). Доказательство состоит из двух частей:

1) если L является разрешимым, то оно является радикальным;
2) L не является радикальным.

Вторую часть также доказал Руффини в 1799 году. Рассуждения Руффини и Абеля восходят к идее Лагранжа действовать в поле $L = \mathbb{C}(x_1, \ldots, x_n)$ перестановками корней $x_1, \ldots, x_n$ многочлена (7) (несложно показать, что это действие корректно, так как корни $x_1, \ldots, x_n$ алгебраически независимы над $\mathbb{C}$ вслед за коэффициентами). Мы обобщим первую часть теоремы Абеля и докажем следующую теорему общего характера.

Теорема 8. *Пусть* $\operatorname{char} K = 0$ *и* K *содержит все корни из единицы. Если нормальное расширение* L/K *содержится в радикальном, то оно является неприводимо-радикальным.*

Доказательство. По условию существует такая радикальная башня

$$K = K_0 \subset K_1 \subset \ldots \subset K_m, \quad K_j := K_{j-1}(r_j), \quad r_j^{p_j} \in K_{j-1} \quad (j = 1, \ldots, m), \quad (8)$$

что $L \subseteq K_m$. Пользуясь леммой 1, будем считать все показатели p_j простыми. Среди всех таких башен возьмём ту, в которой число m радикалов минимально. Поскольку по предположению $\varepsilon_{p_j} \in K$ при всех j, то $K_{j-1}(r_j) \neq K_{j-1}(\varepsilon_{p_j})$ и по лемме Абеля 2 двучлен $x^{p_j} - r_j^{p_j}$ неприводим над K_{j-1}. Поэтому $1, r_j, \ldots, r_j^{p_j-1}$ — базис в K_j над K_{j-1}.

Будем последовательно заменять радикалы $r_m, \ldots, r_1$ на более удобные, дающие ту же башню (8) и заведомо лежащие в L. Отсюда будет следовать, что $K_m \subseteq L$, т. е. $K_m = L$.

Лемма 4. *Зафиксируем* $i = 1, \ldots, m$ *и обозначим* $r = r_i$, $p = p_i$, $\varepsilon = \varepsilon_{p_i}$. *Для всех* $\beta \in K_i \setminus K_{i-1}$ *существует такое* $\rho \in K_i$, *что* $\rho^p \in K_{i-1}$ *и* $1, \rho, \ldots, \rho^{p-1}$ — *базис в* K_i *над* K_{i-1}, *в разложении по которому* β *имеет коэффициент* 1 *при* ρ. *Если при этом* $\beta \in L$, *то* $\rho \in L$ *и коэффициенты* $c_0, \ldots, c_{p-1} \in K_{i-1}$ *разложения любого элемента*

$$\gamma = c_0 + c_1\rho + \ldots + c_{p-1}\rho^{p-1} \in K_i \cap L \quad (9)$$

лежат в L.

Доказательство. Имеем $\beta = b_0 + b_1 r + \ldots + b_{p-1} r^{p-1}$, $b_0, \ldots, b_{p-1} \in K_{i-1}$, причём $b_k \neq 0$ для некоторого $k \geqslant 1$, так как $\beta \notin K_{i-1}$. Положим $\rho = b_k r^k$. Тогда $\rho^p \in K_{i-1}$ и $\rho, \rho^2, \ldots, \rho^{p-1}$ пропорциональны переставленным степеням $r, r^2, \ldots, r^{p-1}$ ввиду простоты p.

Пусть теперь $\beta \in L$. Сопряжённые с элементом (9) над K_{i-1} элементы по теореме 3 имеют вид

$$\gamma_k = c_0 + c_1\rho\varepsilon^k + \ldots + c_s\rho^s\varepsilon^{ks} + \ldots + c_{p-1}\rho^{p-1}\varepsilon^{k(p-1)}, \quad k = 0, \ldots, p-1.$$

Они тем более сопряжены над K, поэтому вместе с γ лежат в L ввиду нормальности расширения L/K. Зафиксировав $s = 0, \ldots, p-1$, сложим элементы γ_k с коэффициентами ε^{-ks} и поделим на p:

$$c_s\rho^s = \frac{1}{p}\sum_{k=0}^{p-1} \gamma_k \varepsilon^{-ks} \in L$$

(напомним, что $\varepsilon \in K \subseteq L$). В частности, для $\gamma = \beta = b_0 + \rho + \ldots$ получим $\rho \in L$. Отсюда следует, что $c_s = (c_s\rho^s)/\rho^s \in L$ при $s = 1, \ldots, p-1$, а тогда и $c_0 = \gamma - c_1\rho - \ldots - c_{p-1}\rho^{p-1} \in L$. □

По теореме о примитивном элементе расширение L/K порождается одним элементом θ. Ввиду минимальности m $\theta \notin K_{m-1}$, поэтому $(K_m \setminus K_{m-1}) \cap L \neq \varnothing$. Применив лемму 4, заменим радикал $r = r_m$ на «удобный» радикал $\rho = \rho_m \in L$. Определим множество $X_m = \{\theta\}$. Вообще, пусть для некоторого $j = m, \ldots, 2$ определены множества $X_m, \ldots, X_j$ и найдены радикалы $\rho_m, \ldots, \rho_j \in L$ из леммы 4, $K_i = K_{i-1}(\rho_i)$ при $i = m, \ldots, j$. Определим множество

$$X_{j-1} = \{\text{коэффициенты разложений элементов из } X_j \text{ по базису } 1, \rho_j, \ldots, \rho_j^{p_j-1}\} \cup \{\rho_j^{p_j}\} \subseteq K_{j-1}.$$

По лемме 4 $X_{j-1} \subseteq L$. Докажем, что $X_{j-1} \not\subseteq K_{j-2}$. Тогда $(K_{j-1} \setminus K_{j-2}) \cap L \neq \varnothing$, что позволит найти радикал $\rho_{j-1} \in L$, порождающий K_{j-1} над K_{j-2}, и при $j > 2$ определить множество X_{j-2}. Тем самым по индукции будут найдены радикалы $\rho_m, \ldots, \rho_1 \in L$.

Множество

$$\{\rho_m^{l_m} \ldots \rho_j^{l_j} \mid 0 \leqslant l_m < p_m, \ldots, 0 \leqslant l_j < p_j\}$$

является базисом расширения K_m/K_{j-1}. Множество X_{j-1} состоит из $\rho_j^{p_j}$, коэффициентов разложения по этому базису элемента θ, а при $j < m$ — ещё элементов $\rho_m^{p_m}, \ldots, \rho_{j+1}^{p_{j+1}}$:

$$\rho_j^{p_j} \in X_{j-1}; \quad \rho_i^{p_i} \in X_{i-1}[\rho_j, \ldots, \rho_{i-1}] \text{ при } i = j+1, \ldots, m, \text{ если } j < m;$$
$$\theta \in X_{i-1}[\rho_j, \ldots, \rho_m].$$

Если $X_{j-1} \subseteq K_{j-2}$, то отсюда следует радикальность башни

$$K_{j-2} \xrightarrow{p_j} K_{j-2}(\rho_j) \xrightarrow{p_{j+1}} K_{j-2}(\rho_j, \rho_{j+1}) \xrightarrow{p_{j+2}} \ldots \xrightarrow{p_m} K_{j-2}(\rho_j, \ldots, \rho_m)$$

и включение $L \subseteq K_{j-2}(\rho_j, \ldots, \rho_m) = K(r_1, \ldots, r_{j-2}, \rho_j, \ldots, \rho_m)$. Противоречие с минимальностью m. □

Существование точной радикальной формулы

Определим понятие радикальной формулы над некоторым полем K. Присоединим к полю K один из корней двучлена $x^n - a \in K[x]$ и временно задействуем обозначение $\sqrt[n]{a}$ для обозначения только одного этого корня. Далее к полю $K(\sqrt[n]{a})$ присоединим один из корней двучлена $x^m - b(\sqrt[n]{a})$, где $b \in K[x]$, и обозначим этот корень через $\sqrt[m]{b(\sqrt[n]{a})}$. Любой элемент расширения $\left(K;\ \sqrt[n]{a},\ \sqrt[m]{b(\sqrt[n]{a})}\right)$ имеет вид

$$\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} d_{ij}\, \sqrt[n]{a}^{\,j}\, \sqrt[m]{b(\sqrt[n]{a})}^{\,i}. \tag{10}$$

Аналогично для произвольного числа радикалов получим выражение вида

$$\sum_{f=0}^{l}\dots\sum_{i=0}^{m-1}\sum_{j=0}^{n-1} d_{f\dots ij}\,\sqrt[n]{a}^{\,j}\,\sqrt[m]{b(\sqrt[n]{a}\,)}^{\,i}\dots\sqrt[l]{v\big(\dots\sqrt[m]{b(\sqrt[n]{a}\,)}\big)}^{\,f}\ ,$$
$$d_{ij\dots k}\in K,\quad b,\dots,v\in K[x]. \quad (11)$$

Теперь будем придавать радикалам любые значения. Точнее, сначала вместо каждого радикала $\sqrt[n]{a}$ подставим любое из его n значений, потом вместо каждого радикала $\sqrt[m]{b(\sqrt[n]{a}\,)}$ (где $\sqrt[n]{a}$ уже фиксированный элемент) — любое из m значений и т. д. Получим *множество всех значений радикальной формулы* (11). Если это множество совпадает с множеством корней некоторого многочлена $f\in K[x]$, то формулу (11) назовём *точной* для уравнения $f(x)=0$.

Теорема 9. *Если некоторый корень неприводимого многочлена выражается в радикалах, то для его корней существует точная радикальная формула.*

Нам понадобится следующая известная лемма о продолжении вложений полей.

Лемма 1 [4]. *Пусть $\varphi\colon K\to L$ — вложение полей и $\alpha\in\bar{K}$.*

1. *Если $\tilde{\varphi}\colon K(\alpha)\to L$ — продолжение вложения φ, то $\tilde{\varphi}(\alpha)$ — корень многочлена $(\mu_\alpha^K)^\varphi$.*
2. *Обратно, для любого корня $\beta\in L$ многочлена $(\mu_\alpha^K)^\varphi$ отображение*

$$\tilde{\varphi}_\beta\colon K(\alpha)\to L,\quad f(\alpha)\mapsto f^\varphi(\beta)\quad (f\in K[x]) \qquad (12)$$

корректно продолжает φ до вложения.

Пусть элемент α алгебраичен над полем K, а элемент β — над полем $K(\alpha)$. Опишем элементы, сопряжённые к произвольному элементу $\theta\in K(\alpha,\beta)$. Пусть $\alpha_1=\alpha,\dots,\alpha_n$ — сопряжённые с α над K элементы. Пользуясь леммой 1, введём для каждого $r=1,\dots,n$ следующие гомоморфизмы и элементы:

1) $\varphi_r\colon K(\alpha)\to P$ — вложение над K с условием $\varphi_r(\alpha)=\alpha_r$ и образом $K(\alpha_r)\cong K(\alpha)$;
2) $\beta_{r1},\dots,\beta_{rm}\in P$ — все корни многочлена $\big(\mu_\beta^{K(\alpha)}\big)^{\varphi_r}\in K(\alpha_r)[x]$, $\beta_{11}=\beta$;
3) $\Phi_{rs}\colon K(\alpha,\beta)\to P$ — продолжение φ_r с помощью соответствия $\beta\mapsto\beta_{rs}$ $(s=1,\dots,m)$:

$$\begin{array}{ccccc} K & \longrightarrow & K(\alpha) & \longrightarrow & K(\alpha,\beta) \\ & & {\scriptstyle\varphi_r}\big\downarrow\wr & & {\scriptstyle\Phi_{rs}}\big\downarrow\wr \\ & & K(\alpha_r) & \longrightarrow & K(\alpha_r,\beta_{rs}) \end{array}\ .$$

Разложим элемент $\theta\in K(\alpha,\beta)$ по базису $(\beta^i)_{i=0}^{m-1}$ над $K(\alpha)$, а каждый коэффициент этого разложения — по базису $(\alpha^j)_{j=0}^{n-1}$ над K:

$$\theta=\sum_{i=0}^{m-1}c_i\beta^i,\quad c_i=\sum_{j=0}^{n-1}d_{ij}\alpha^j,\quad i=0,\dots,m-1. \qquad (13)$$

Теорема 10. *Во введённых обозначениях элементы, сопряжённые с элементом θ над K, — это в точности элементы*

$$\theta_{rs} = \sum_i \Big(\sum_j d_{ij} \alpha_r^j \Big) \beta_{rs}^i, \quad r = 1, \dots, n, \quad s = 1, \dots, m \quad (\theta_{11} = \theta)$$

(*среди элементов θ_{rs} могут быть одинаковые*).

Доказательство. Каждый элемент θ_{rs} сопряжён с θ над K, так как

$$0 = \Phi_{rs}\big(\mu_\theta(\theta)\big) = \mu_\theta\big(\Phi_{rs}(\theta)\big) = \mu_\theta(\theta_{rs}).$$

Теперь докажем, что каждый элемент $\theta' \in P$, сопряжённый с θ над K, совпадает с одним из θ_{rs}. Пусть $\varphi\colon K(\theta) \to P$ — вложение над K, для которого $\varphi(\theta) = \theta'$. Многочлен $\big(\mu_\alpha^{K(\theta)}\big)^\varphi$ делит многочлен $\mu_\alpha^\varphi = \mu_\alpha$, полностью разложимый в P, а потому имеет в P корень α_r для некоторого $r = 1, \dots, n$. Тогда по лемме 1 вложение φ продолжается до вложения $\tilde\varphi\colon K(\theta, \alpha) \to P$ соответствием $\alpha \mapsto \alpha_r$. Поэтому $\tilde\varphi|_{K(\alpha)} = \varphi_r$, и многочлен $\big(\mu_\beta^{K(\theta,\alpha)}\big)^{\tilde\varphi}$ имеет корень β_{rs} для некоторого $s = 1, \dots, m$. Поэтому вложение $\tilde\varphi$ продолжается до вложения $\Phi\colon K(\theta, \alpha, \beta) \to P$ соответствием $\beta \mapsto \beta_{rs}$. Отсюда вытекает, что

$$\theta' = \varphi(\theta) = \Phi(\theta) = \Phi\Big(\sum_i \Big(\sum_j d_{ij} \alpha^j \Big) \beta^i \Big) = \sum_i \Big(\sum_j d_{ij} \alpha_r^j \Big) \beta_{rs}^i = \theta_{rs}. \qquad \square$$

Применим теорему 10 в доказательстве теоремы 9.

Доказательство теоремы 9. Пусть в обозначениях теоремы 10 многочлены $\mu_\alpha^K(x)$ и $\mu_\beta^{K(\alpha)}(x)$ являются двучленами:

$$\mu_\alpha^K(x) = x^n - a, \quad \mu_\beta^{K(\alpha)}(x) = x^m - b(\alpha) \quad (b(x) \in K[x]).$$

Поскольку радикалы неприводимы, то $\sqrt[n]{a} = \{\alpha_1, \dots, \alpha_n\}$ и $\sqrt[m]{b(\alpha_r)} = \{\beta_{r1}, \dots, \beta_{rm}\}$ при каждом $r = 1, \dots, n$. По теореме 10 множество значений радикальной формулы (10) есть множество элементов, сопряжённых с θ.

Поскольку теорема 10 по индукции распространяется на башни любой высоты, то сказанное распространяется на общую радикальную формулу (11), в которой все радикалы неприводимы. $\square$

А. Л. Канунников поддержан грантом РНФ № 16-11-10013П.

Литература

[1] Артин Э. Теория Галуа. — М.: МЦНМО, 2008.

[2] Ван дер Варден Б. Л. Алгебра. — М.: Мир, 1976.

[3] Гаусс К. Ф. Арифметические исследования. — М.: АН СССР, 1959.

[4] Ленг С. Алгебра. — М.: Мир, 1968.