УДК 517.958

НЕКОТОРЫЕ ПРИМЕНЕНИЯ ЗАДАЧИ ЧИРНГАУЗЕНА

И.Г. ГАЛЯУТДИНОВ[1], Е.Е. ЛАВРЕНТЬЕВА[2], Э.Д. ХУСАИНОВА[2]

[1] *Казанский филиал Поволжского государственного университета телекоммуникаций и информатики,*
[2] *Казанский (Приволжский) федеральный университет*
E-mail: ialee-4@mail.ru, ence_khusainova@mail.ru

SOME APPLICATIONS OF TSCHIRNHAUSEN PROBLEM

I.G. GALYAUTDINOV[1], E.E. LAVRENTYEVA[2], E.D. KHUSAINOVA[2]

[1] *Kazan Branch of Povolzhskiy State University of Telecommunications and Informatics,*
[2] *Kazan Federal University*

Аннотация

С помощью преобразования Чирнгаузена найдены минимальные многочлены чисел вида $\operatorname{tg}^2(\pi/n)$ для всех натуральных чисел $n > 2$. Предложены два новых способа решения задачи Чирнгаузена. При первом способе задача сведена к нахождению линейной зависимости некоторой системы векторов. Второй способ решения задачи Чирнгаузена основан на теории результанта двух многочленов. Приведены примеры построения минимальных многочленов.

Ключевые слова: алгебраические числа, минимальные многочлены, круговые поля и их подполя, задача Чирнгаузена.

Summary

Using the transformation Tschirnhausen we find minimal polynomials of number $\operatorname{tg}^2(\pi/n)$ for all $n > 2$, $n \in \mathbb{N}$. Two new ways to solve the Tschirnhausen problem are offered. First way is reduced to finding the linear dependence of some system of vectors. The second way of solving the Tschirnhausen problem is based on the theory of the resultant of two polynomials. Examples of constructing the minimal polynomials are given.

Key words: algebraic numbers, minimal polynomials, circular fields and subfields, Tschirnhausen problem.

Введение

В исторических очерках (см. Н. Бурбаки [1, с. 225]) отмечается, что Г.В. Лейбниц (1646–1716) и его друг Э.В. Чирнгаузен (1651–1708) были единственными математиками своего времени, интересовавшиеся проблемой решения алгебраических уравнений в радикалах. Г.В. Лейбниц пытается решить в радикалах уравнение пятой степени. Э.В. Чирнгаузен думал, что он решил эту проблему, избавившись от всех членов уравнения, кроме двух крайних, с помощью преобразования вида $y = g(x)$, где g — подходящий многочлен четвертой степени. Однако Лейбниц обнаруживает, что уравнения, определяющие коэффициенты многочлена имеют степень более пяти, и, поэтому, считает этот метод безнадежным. Несмотря на это, преобразование Чирнгаузена имеет важные приложения.

В данной работе с помощью преобразования Чирнгаузена мы рассмотрим нахождение минимальных многочленов чисел вида $\operatorname{tg}^2(\pi/n)$ для всех натуральных чисел $n > 2$.

1. Задача Чирнгаузена.

Пусть α — алгебраическое число степени n, $f(x)$ — его минимальный многочлен. Рассмотрим простое алгебраическое расширение $\mathbb{Q}(\alpha)$ и число $t = g(\alpha)$, где $g(x) \in \mathbb{Q}[x]$, $\deg g(x) \leqslant n-1$. Очевидно, что

$\mathbb{Q}\,[(\alpha)]\,:\,\mathbb{Q}=n$, $t\in\mathbb{Q}(\alpha)$. Поэтому число t также является алгебраическим, причем $\mathbb{Q}\subset\mathbb{Q}(t)\subset\mathbb{Q}(\alpha)$. Отсюда следует, что если степень алгебраичности числа t равняется k, то $n=k\,s$, где $s=\mathbb{Q}\,[(\alpha)\,:\,\mathbb{Q}(t)]$. Значит, степень алгебраического числа t является делителем $\deg f(x)=n$. Ставится задача: найти многочлен $\varphi(x)\in\mathbb{Q}[x]$, корнем которого является число t, а также выяснить степень алгебраичности этого числа. Задачу нахождения многочлена $\varphi(x)$ по данным многочленам $f(x)$ $g(x)$ и называют задачей Чирнгаузена [2, с.73]. В литературе (см., например, [3,с.230]) приводятся два метода решения этой задачи. В одном из них используется теория однородных систем линейных уравнений, а в другом — теория симметрических многочленов.

В данной работе предлагаются два новых способа решения задачи Чирнгаузена. При первом способе задача сводится к нахождению линейной зависимости некоторой системы векторов. Суть этого метода заключается в следующем.

Пусть $t = g_1(\alpha)$. Возведя это равенство в квадрат, приходим к равенству $t^2 = g_1^2(\alpha)$. Если $\deg g_1^2(\alpha)\geqslant n$, то, разделив $g_1^2(x)$ на $f(x)$, находим остаток $g_2(x)$, $\deg g_2(x)\leqslant n-1$. Тогда $t^2=g_2(\alpha)$. Таким же образом найдем $t^3=g_3(\alpha),\ldots,t^d=g_d(\alpha)$, где $d>1$, d — наименьший натуральный делитель числа n. Полученные равенства перепишем в виде

$$t-c_1=\varphi_1(\alpha),\quad t^2-c_2=\varphi_2(\alpha),\quad \ldots,t^d-c_d=\varphi_d(\alpha),$$

перенеся свободные члены из правой части в левую. Если t — алгебраическое число степени d, то многочлены $\varphi_1(\alpha),\varphi_2(\alpha),\cdots,\varphi_d(\alpha)$ будут линейно зависимы. Значит, существуют рациональные числа $q_1,q_2,\cdots,q_d$, не все равные нулю одновременно, такие, что

$$q_1\,\varphi_1(\alpha)+q_2\,\varphi_2(\alpha)+\cdots+q_d\,\varphi_d(\alpha)=0.$$

Тогда $q_1\,(t-c_1)+q_2\,(t^2-c_2)+\cdots+q_d\,(t^d-c_d)=\varphi(t)=0$.

Таким образом, найден многочлен $\varphi(x)\in\mathbb{Q}[x]$, корнем которого является число t. Если многочлены $\varphi_1(\alpha),\varphi_2(\alpha),\cdots,\varphi_d(\alpha)$ будут линейно независимы, то степень алгебраичности числа t больше d. Поэтому переходим к следующему делителю d_1 числа n, где $d_1>d$, находим все натуральные степени числа t до t^{d_1} и проверяем линейную зависимость полученных многочленов $\varphi_1(\alpha),\varphi_2(\alpha),\cdots,\varphi_{d_1}(\alpha)$. Так как степень алгебраичности числа $t=g(\alpha)$ не больше n, то на каком-то шаге найдется искомый многочлен $\varphi(x)$. Из рассуждений, приведенных выше, следует, что он будет минимальным многочленом числа t.

Пример 1. Пусть α — корень многочлена $f(x)=x^6-2$, найдем многочлен $\varphi(x)\in\mathbb{Q}[x]$, корнем которого является число $t=\alpha^2+1=g(\alpha)$, и определим степень алгебраичности t.

Очевидно, что α — алгебраическое число степени 6. Степень числа t находится среди делителей числа 6, то есть надо исследовать числа 1, 2, 3, 6. Так как $t\notin\mathbb{Q}$, то степень этого числа не может равняться 1. Поэтому рассмотрим выражения $t=\alpha^2+1$, $t^2=\alpha^4+2\,\alpha^2+1$ и перепишем их в виде $t-1=\alpha^2=\varphi_1(\alpha)$, $t^2-1=\alpha^4+2\,\alpha^2=\varphi_2(\alpha)$. Нетрудно заметить, что многочлены $\varphi_1(\alpha)$, $\varphi_2(\alpha)$ линейно независимы. Значит, степень алгебраичности числа t больше двух. Поэтому исследуем на линейную зависимость выражения, содержащие t, t^2, t^3. Рассуждая как и выше, получим $t-1=\alpha^2=\varphi_1(\alpha)$, $t^2-1=\alpha^4+2\,\alpha^2=\varphi_2(\alpha)$, $t^3/3-1=\alpha^4+\alpha^2=\varphi_3(\alpha)1$, причем $\varphi_1(\alpha)-\varphi_2(\alpha)+\varphi_3(\alpha)=0$, то есть многочлены образуют линейно зависимую систему. Тогда имеем, что $(t-1)-(t^2-1)+(t^3/3-1)=0$. Отсюда следует, что $t^3-3\,t^2+3\,t-3=0$.

Таким образом, найден искомый многочлен $\varphi(x)=x^3-3\,x^2+3\,x-3$ и t — алгебраическое число степени 3.

Второй способ решения задачи Чирнгаузена основан на теории результанта двух многочленов. Приведем необходимые рассуждения. Из равенства $t=g(\alpha)$ имеем, что $F(\alpha)=g(\alpha)-t=0$, то есть число α является корнем многочлена $F(x)$. По условию имеем, что является α корнем и многочлена $f(x)$. Поэтому результант этих многочленов должен равняться нулю, то есть $\mathrm{Res}\,\big(f(x),F(x)\big)=\varphi(t)=0$. Таким образом, будет найден искомый многочлен $\varphi(x)$.

Пример 2. Пусть число α является корнем многочлена $f(x)=x^3-7\,x-7$, найдем многочлен, корнем которого является число $t=-3\,\alpha^2+4\,\alpha+14$.

Вычислим результант многочленов $\varphi(x) = x^3 - 7\,x - 7$ и $F(x) = 3\,x^2 - 4\,x + t - 14$ и приравняем его к нулю. Имеем

$$\begin{vmatrix} 1 & 0 & -7 & -7 & 0 \\ 0 & 1 & 0 & -7 & -7 \\ 3 & -4 & t-14 & 0 & 0 \\ 0 & 3 & -4 & t-14 & 0 \\ 0 & 0 & 3 & -4 & t-14 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -7 & -7 & 0 \\ 0 & 1 & 0 & -7 & -7 \\ 0 & -4 & t+7 & 21 & 0 \\ 0 & 0 & -4 & t+7 & 21 \\ 0 & 0 & 3 & -4 & t-14 \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & 0 & -7 & -7 \\ 0 & t+7 & -7 & -28 \\ 3 & -4 & t+7 & 21 \\ 0 & 3 & -4 & t-14 \end{vmatrix} = t^3 - 7\,t - 7 = 0.$$

Отсюда следует, что числа $t_1 = \alpha$ и $t_2 = -3\,\alpha^2 + 4\,\alpha + 14$ являются корнями одного и того же многочлена $\varphi(x) = x^3 - 7\,x - 7$. Значит, число $t_3 = -3\,t_2^2 + 4\,t_2 + 14 = 3\,\alpha^2 - 5\,\alpha - 14$ также является корнем многочлена $\varphi(x) = x^3 - 7\,x - 7$.

Таким образом, установлено, что все корни этого многочлена рационально выражаются через один.

2. Минимальные многочлены чисел $\mathrm{tg}^2(\pi/n)$.

В работе [4] получены рекуррентные формулы для вычисления минимальных многочленов $t_n(x)$ чисел $\mathrm{tg}(\pi/n)$ для всех натуральных $n \neq 2$. При изучении свойств многочленов $t_n(x)$ установлено, что если n не делится на 4, то многочлен $t_n(x)$ содержит только четные степени переменной x. Это означает, что подстановка $x^2 = t$ переводит многочлен $t_n(x)$ в многочлен $s_n(x)$ степени $\dfrac{1}{2}\,\varphi(n)$, одним из корней которого является число $\mathrm{tg}^2(\pi/n)$. Из неприводимости многочлена $t_n(x)$ следует неприводимость многочлена $s_n(t)$ над полем $\mathbb{Q}$. Таким образом, $s_n(t)$ — минимальный многочлен числа $\mathrm{tg}^2(\pi/n)$.

Следовательно, если n не делится на 4, то минимальный многочлен $s_n(t)$ числа $\mathrm{tg}^2(\pi/n)$ получается из многочлена $t_n(x)$ подстановкой $x^2 = t$.

Приведем простейший пример. Пусть $n = 5$. Тогда $t_5(x) = x^4 - 10\,x^2 + 5$, и его корнями являются числа $\mathrm{tg}(s\,\pi/5)$, где $s = 1, 2, 3, 4$. Подстановка $x^2 = t$ дает $s_5(x) = t^2 - 10\,t + 5$ — минимальный многочлен числа $\mathrm{tg}^2(\pi/5)$. Корнями многочлена $s_5(t)$ являются числа $\mathrm{tg}^2(\pi/5) = \mathrm{tg}^2(4\,\pi/5)$, $\mathrm{tg}^2(2\,\pi/5) = \mathrm{tg}^2(3\,\pi/5)$.

В случае $n \equiv 0 \pmod 4$ вычисление минимального многочлена чисел $\mathrm{tg}^2(\pi/n)$ приводит к задаче Чирнгаузена.

Действительно, известен минимальный многочлен $t_n(x)$ числа $\mathrm{tg}(\pi/n)$. Требуется найти минимальный многочлен $s_n(t)$ числа $t = \mathrm{tg}^2(\pi/n)$.

Из вышеизложенного выше следует, что искомый многочлен $s_n(t)$ с точностью до знака является результантом многочленов $t_n(x)$ и $F(x) = x^2 - t$, то есть $s_n(t) = \pm\,\mathrm{Res}\,\big(t_n(x),\, x^2 - t\big)$.

В случае $n \equiv 0 \pmod 4$ найденный многочлен $s_n(t)$ является неприводимым над полем $\mathbb{Q}$. Действительно, $\mathrm{Res}\,\big(t_n(x),\, x^2 - t\big)$ есть определитель порядка $\deg t_n(x) + 2$ из его вида ясно, что данный определитель является многочленом $s_n(t)$ относительно t и $\deg s_n(t) = \deg t_n(x)$.

В работе [4] показано, что числа $\mathrm{tg}(\pi/n)$ и $\mathrm{tg}^2(\pi/n)$ порождают одно и то же поле, то есть они — алгебраические числа одной и той же степени. Таким образом, число $t = \mathrm{tg}^2(\pi/n)$ является корнем многочлена $s_n(t)$, и степень этого многочлена совпадает со степенью алгебраичности числа $\mathrm{tg}^2(\pi/n)$. Значит, $s_n(t)$ неприводим над полем ? и он — минимальный многочлен числа $\mathrm{tg}^2(\pi/n)$.

Очевидно, что приведенное рассуждение справедливо не только для $\mathrm{tg}(\pi/n)$, но и для любого корня многочлена $t_n(x)$.

Таким образом, имеет место

Теорема 1. *Пусть* $n \equiv 0 \pmod 4$ *и* $t_n(x)$ *— минимальный многочлен числа* $\mathrm{tg}(\pi/n)$. *Тогда минимальный многочлен* $s_n(t)$ *числа* $t = \mathrm{tg}^2(\pi/n)$ *вычисляется по формуле* $s_n(t) = \pm\,\mathrm{Res}\,\big(t_n(x),\, x^2 - t\big)$.

Корнями $s_n(t)$ являются числа $\operatorname{tg}^2(s\,\pi/n)$, где s пробегает приведенную систему вычетов по модулю n, для которых $s \equiv 1 \pmod 4$.

Замечание. *В данной теореме условие $n \equiv 0 \pmod 4$ существенно. Действительно, если это условие не выполняется, то многочлены $t_n(x)$ содержат только четные степени. Значит, в этом случае все корни результанта $\operatorname{Res}\big(t_n(x),\, x^2 - t\big)$ имеют кратность 2. Поэтому при $n \neq 4\,k$ имеет место равенство $\operatorname{Res}\big(t_n(x),\, x^2 - t\big) = \pm\, s_n^2(t)$, где $s_n(t)$ — минимальный многочлен числа $\operatorname{tg}^2(\pi/n)$.*

К примеру, при $n = 5$ имеем $t_5(x) = x^4 - 10\,x^2 + 1$, корнями $t_5(x)$ являются $\operatorname{tg}(\pi/5)$, $\operatorname{tg}(2\,\pi/5)$, $\operatorname{tg}(3\,\pi/5) = -\operatorname{tg}(2\,\pi/5)$, $\operatorname{tg}(4\,\pi/5) = -\operatorname{tg}(\pi/5)$, и $\operatorname{Res}\big(t_n(x),\, x^2 - t\big) = \big(t^2 - 10\,t + 5\big)^2$. Минимальный многочлен $s_5(t)$ числа $\operatorname{tg}^2(\pi/5)$ имеет вид $s_5(t) = t^2 - 10\,t + 5$. Корнями $s_5(t)$ являются числа $\operatorname{tg}^2(\pi/5)$ и $\operatorname{tg}^2(2\,\pi/5)$.

Этот минимальный многочлен ранее был найден из $t_5(x)$ при помощи подстановки $x^2 = t$.

Если $n \equiv 0 \pmod 4$, то согласно лемме 3 работы [4] число $\operatorname{tg}(\pi/n)$ рационально выражается через $\operatorname{tg}^2(\pi/n)$. Поэтому, пользуясь тем, что $s_n(\operatorname{tg}^2(\pi/n)) = 0$, стандартными методами можно получить равенство $\operatorname{tg}(\pi/n) = \psi(\operatorname{tg}^2(\pi/n))$, где $\psi(t)$ — многочлен с рациональными коэффициентами.

Приведем пример.

Пример 3. Найдем многочлены $s_8(t)$, $s_{12}(t)$, $s_{16}(t)$, $s_{20}(t)$ и $s_{24}(t)$.

По теореме 1 имеем $s_n(t) = \operatorname{Res}\big(t_n(x),\, x^2 - t\big)$. Поэтому сначала нужно вычислить минимальные многочлены $t_n(x)$ чисел $\operatorname{tg}(\pi/n)$ для $n = 8, 12, 16, 20, 24$.

Пользуясь рекуррентными формулами, доказанными в работе [4], находим

$$t_8(x) = x^2 + 2\,x - 1,\ t_{12}(x) = x^2 - 4\,x + 1,\ t_{16}(x) = x^4 + 4\,x^3 - 6\,x^2 - 4\,x + 1,$$

$$t_{20}(x) = x^4 - 4\,x^3 - 14\,x^2 - 14\,x + 1,\ t_{24}(x) = x^4 + 8\,x^3 + 2x^2 - 8\,x + 1.$$

Теперь вычислим $s_8(t)$. Имеем

$$s_8(t) = \begin{vmatrix} 1 & 2 & -1 & 0 \\ 0 & 1 & 2 & -1 \\ 1 & 0 & -t & 0 \\ 0 & 1 & 0 & -t \end{vmatrix} = \begin{vmatrix} 1 & 2 & t-1 & 2\,t \\ 0 & 1 & 2 & t-1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{vmatrix} = (t-1)^2 - 4\,t = t^2 - 6\,t + 1.$$

Корнями $s_8(t)$ являются числа $\operatorname{tg}^2(\pi/8)$ и $\operatorname{tg}^2((5\,\pi)/8)$. Аналогичными вычислениями находим

$s_{12}(t) = t^2 - 14\,t + 1$ (корни $\operatorname{tg}^2(\pi/12)$ и $\operatorname{tg}^2((5\,\pi)/12)$),

$s_{16}(t) = t^4 - 28\,t^3 + 70\,t^2 - 28\,t + 1$ (корни $\operatorname{tg}^2(\pi/16)$, $\operatorname{tg}^2((5\,\pi)/16)$, $\operatorname{tg}^2((9\,\pi)/16)$, $\operatorname{tg}^2((13\,\pi)/16)$),

$s_{20}(t) = t^4 - 44\,t^3 + 166\,t^2 - 44\,t + 1$ (корни $\operatorname{tg}^2(\pi/20)$, $\operatorname{tg}^2((9\,\pi)/20)$, $\operatorname{tg}^2((13\,\pi)/20)$, $\operatorname{tg}^2((17\,\pi)/20)$),

$s_{24}(t) = t^4 - 60\,t^3 + 134\,t^2 - 60\,t + 1$ (корни $\operatorname{tg}^2(\pi/24)$, $\operatorname{tg}^2((5\,\pi)/24)$, $\operatorname{tg}^2((13\,\pi)/24)$, $\operatorname{tg}^2((17\,\pi)/24)$).

ЛИТЕРАТУРА

1. **Бурбаки Н.** Алгебра (Многочлены и поля. Упорядоченные группы). — М: Наука, 1965. — 300 с.
2. **Чеботарев Н.Г.** Основы теории Галуа. — М-Л.: ОНТИ ГТТИ, 1934. — 222 с.
3. **Сушкевич А.К.** Основы высшей алгебры. — М-Л.: ОГИЗ, 1941. — 460 с.
4. **Галиева Л.И., Галяутдинов И.Г.** Об одном классе уравнений, разрешимых в радикалах // Известия Вузов. Математика. — 2011. — № 2. — С.22—30.

REFERENCES

1. **Bourbaki N.** Elements of Mathematics. Algebra II: Chapters 4-7. — Springer Science & Business Media, 2003. — 461 p.
2. **Chebotarev N.G.** Fundamentals of Galois theory [Osnovy teorii Galua]. — Moscow-Leningrad, 1934. — 222 p. (in Russian)
3. **Sushkevich A.K.** Fundamentals of Algebra [Osnovy vyshei algebry]. — Moscow-Leningrad, 1941. — 460 p. (in Russian)
4. **Galieva L.I., Galyautdinov I.G.** One class of equations solvable in radicals // Russian Mathematics. — 2011. — V. 55, № 2. — P. 18—25.