УДК 511.61

НАХОЖДЕНИЕ МИНИМАЛЬНЫХ МНОГОЧЛЕНОВ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ ВИДА $\mathrm{tg}^2(\pi/n)$ С ПОМОЩЬЮ ПРЕОБРАЗОВАНИЯ ЧИРНГАУЗЕНА

И.Г. Галяутдинов, Е.Е. Лаврентьева

Аннотация

Предложены решения двух задач с помощью преобразования Чирнгаузена. Первая задача связана с построением минимальных многочленов чисел вида $\mathrm{tg}^2(\pi/n)$ с помощью преобразования Чирнгаузена для всех натуральных $n > 2$. Вторая задача состоит в нахождении точных значений корней уравнения $x^3 - 7x - 7 = 0$. Решение задачи получено на основе того, что корни уравнения порождают круговое поле $\mathbb{Q}_7$. Приведены примеры построения минимальных многочленов.

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

Введение

В исторических очерках 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, интересовавшимися проблемой решения алгебраических уравнений в радикалах.

Г.В. Лейбниц пытался 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 $g(x)$, имеют степень более пяти, и поэтому считает этот метод безнадежным. Несмотря на это, преобразование Чирнгаузена имеет важные приложения.

С помощью преобразования Чирнгаузена любое уравнение пятой степени без кратных корней можно привести к виду $y^5 + 5y = a$, решая при этом лишь уравнения второй и третьей степени [7, с. 187–190]. Это преобразование позволяет также решить в радикалах уравнения третьей и четвертой степени. При этом уравнение третьей степени приводится к виду $y^3 + q_3 = 0$, а уравнение четвертой степени – к виду $y^4 + q_2 y^2 + q_4 = 0$.

Преобразование Чирнгаузена использовалось также в исследованиях Н.Г. Чеботарева, относящихся к проблеме резольвент, и В.И. Арнольда, касающихся решения тринадцатой проблемы Гильберта.

В связи с этим укажем на статью В.И. Арнольда [8] и на его комментарии к работам А.Н. Колмогорова о суперпозициях [9, с. 445–454]. В библиографии к этим комментариям имеется ссылка на три работы Н.Г. Чеботарева, которые относятся к проблеме суперпозиции функций.

Заметим, что некоторые авторы вместо «Чирнгаузен (Tschirnhausen)» пишут «Чирнгауз» [7, с. 187], [10, с. 92].

В настоящей работе с помощью преобразования Чирнгаузена мы решим две задачи.

Первая задача – это нахождение минимальных многочленов чисел вида $\operatorname{tg}^2 \pi/n$ для всех натуральных чисел $n > 2$.

Из способа нахождения становятся известными все корни найденного минимального многочлена и рациональные связи между ними. Отсюда вытекает возможность нахождения группы Галуа этого многочлена. Как известно, в общем случае нахождение групп Галуа многочленов является весьма сложной задачей, поэтому многочлены, для которых группа Галуа вычисляется сравнительно несложно, представляют особый интерес.

Вторая задача более частная. Она связана с изучением уравнения $\varphi(x) = x^3 - 7x - 7 = 0$. Показывается, что корни этого уравнения порождают кубичное подполе кругового поля $\mathbb{Q}_7$. Это позволяет найти точные значения всех трех (действительных) корней этого уравнения.

Данный пример интересен тем, что, применяя формулы Кардана, найти даже приближенные значения корней указанного уравнения довольно затруднительно. А преобразование Чирнгаузена позволяет найти не только приближенные, но и точные значения корней заданного уравнения.

1. Задача Чирнгаузена

Напомним, что число α называется алгебраическим, если оно является корнем некоторого многочлена с рациональными коэффициентами. Среди таких многочленов найдется единственный нормированный неприводимый над полем $\mathbb{Q}$ многочлен $f(x) \in \mathbb{Q}[x]$, корнем которого является число α. Этот многочлен называется минимальным многочленом числа α, а $\deg f(x)$ – его степенью.

Пусть α – алгебраическое число степени n, $f(x)$ – его минимальный многочлен. Рассмотрим простое алгебраическое расширение $\mathbb{Q}(\alpha)$ и число $t = g(\alpha)$, где $g(x) \in \mathbb{Q}[x]$, $\deg g(x) \leq n-1$. 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 $n = ks$, 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 $f(x)$ и $g(x)$ называют задачей Чирнгаузена [2, с. 73]. В литературе [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 настоящей 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 $\deg g_1^2(\alpha) \geq n$, то разделив $g_1^2(x)$ на $f(x)$, найдем остаток $g_2(x)$, $\deg g_2(x) \leq n-1$. Тогда $t^2 = g_2(\alpha)$. Таким же образом найдем $t^3 = g_3(\alpha), \ldots, t^d = g_d(\alpha)$, где $d > 1$ – наименьший натуральный делитель числа n. Полученные равенства перепишем в виде $t - c_1 = \varphi_1(\alpha)$, $t^2 - c_2 = \varphi_2(\alpha), \cdots, t^d - c_d = \varphi_d(\alpha)$, перенеся свободные члены из правой части в левую. Если t – алгебраическое число степени d, то многочлены $\varphi_1(\alpha), \varphi_2(\alpha), \ldots, \varphi_d(\alpha)$ будут линейно зависимы. Значит, существуют рациональные числа $q_1, q_2, \ldots, q_d$, 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 $\varphi_1(\alpha), \varphi_2(\alpha), \ldots, \varphi_d(\alpha)$ будут линейно независимы, то это означает, что 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 $\varphi_1(\alpha), \varphi_2(\alpha), \ldots, \varphi_{d_1}(\alpha)$. 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 $t \notin \mathbb{Q}[x]$, 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 так же, как и выше, получим $t - 1 = \alpha^2 = \varphi_1(\alpha)$, $t^2 - 1 = \alpha^4 + 2\alpha^2 = \varphi_2(\alpha)$, $t^3/3 - 1 = \alpha^4 + \alpha^2 = \varphi_3(\alpha)$, причем $\varphi_1(\alpha) - \varphi_2(\alpha) + \varphi_3(\alpha) = 0$, то есть многочлены $\varphi_1(\alpha)$, $\varphi_2(\alpha)$, $\varphi_3(\alpha)$ образуют линейно зависимую систему. Тогда имеем, что $(t-1) - (t^2-1) + (t^3/3 - 1) = 0$. Отсюда следует, что $t^3 - 3t^2 + 3t - 3 = 0$.

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

Пример 2. Пусть α – корень многочлена $g(x) = x^3 + x^2 - 2x - 1$; найдем многочлен $\varphi(x) \in \mathbb{Q}[x]$, корнем которого является число $t = \alpha^2 + 2\alpha - 1$, и определим степень алгебраичности t.

Многочлен $g(x)$ не имеет рациональных корней. Значит, α и t – алгебраические числа степени 3. Из условия $t + 1 = \alpha^2 + 2\alpha = \varphi_1(\alpha)$ следует, что

$$t^2 + 2t + 1 = \alpha^4 + 4\alpha^3 + 4\alpha^2 = f(\alpha)(\alpha + 3) + 3\alpha^2 + 7\alpha + 3.$$

Отсюда, учитывая равенство $f(\alpha) = 0$, получаем $t^2 + 2t - 2 = 3\alpha^2 + 7\alpha = \varphi_2(\alpha)$. Перемножая полученные равенства, после упрощений находим $t^3 + 3t^2 - 12 = 10\alpha^2 + 23\alpha = \varphi_3(\alpha)$. Многочлены $\varphi_1(\alpha)$, $\varphi_2(\alpha)$, $\varphi_3(\alpha)$ линейно зависимы: $\varphi_3(\alpha) - 3\varphi_2(\alpha) - \varphi_1(\alpha) = 0$. Значит, $t^3 + 3t^2 - 12 - 3(t^2 + 2t - 2) - (t + 1) = t^3 - 7t - 7 = 0$. Число $t = \alpha^2 + 2\alpha - 1$ является корнем многочлена $\varphi(x) = x^3 - 7x - 7$.

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 α является корнем и многочлена $f(x)$. Поэтому результант этих многочленов должен равняться нулю, то есть $\mathrm{Res}\,(f(x), F(x)) = \varphi(t) = 0$. Таким образом, будет найден искомый многочлен $\varphi(x)$.

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

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

Имеем

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

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

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

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

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

В работе [4] доказаны 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 $s_n(t)$ степени $0.5\varphi(n)$, 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 $t_5(x) = x^4 - 10x^2 + 5$ и его корнями являются числа $\mathrm{tg}(s\pi/5)$, где $s = 1, 2, 3, 4$. Подстановка $x^2 = t$ дает $s_5(t) = t^2 - 10t + 5$ – 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 $n \equiv 0 (\bmod 4)$ 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 изложенного 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 $s_n(t) = \pm\mathrm{Res}\,(t_n(x), x^2 - t)$.

В случае $n \equiv 0 (\bmod 4)$ найденный многочлен $s_n(t)$ является неприводимым над полем $\mathbb{Q}$. Действительно, $\mathrm{Res}\,(t_n(x), x^2 - t)$ есть определитель порядка $\deg t_n(x) + 2$, из его строения очевидно, что этот 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 $\mathbb{Q}$ и он является минимальным многочленом числа $\mathrm{tg}^2(\pi/n)$.

Ясно, 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* $n \equiv 0 (\operatorname{mod} 4)$ *и* $t_n(x)$ – *минимальный многочлен числа* $\operatorname{tg}(\pi/n)$. *Тогда минимальный многочлен* $s_n(t)$ *числа* $t = \operatorname{tg}^2(\pi/n)$ *вычисляется по формуле* $s_n(t) = \pm \operatorname{Res}(t_n(x), x^2 - t)$. *Корнями* $s_n(t)$ *являются числа* $\operatorname{tg}^2(s\pi/5)$, *где* s *пробегает приведенную систему вычетов по модулю* n, *для которых* $s \equiv \equiv 1 (\operatorname{mod} 4)$.

Замечание 1. В теореме 1 условие $n \equiv 0 (\operatorname{mod} 4)$ существенно. Действительно, если это условие не выполняется, то многочлены $t_n(x)$ содержат только четные степени. Значит, в этом случае все корни результанта $\operatorname{Res}(t_n(x), x^2 - t)$ имеют кратность 2. Поэтому при $n \neq 4k$ имеет место равенство $\operatorname{Res}(t_n(x), x^2 - t) = = \pm (s_n(t))^2$, где $s_n(t)$ – минимальный многочлен числа $\operatorname{tg}^2(\pi/n)$.

К примеру, при $n = 5$ имеем $t_5(x) = x^4 - 10x^2 + 1$ с корнями $\operatorname{tg}(\pi/5)$, $\operatorname{tg}(2\pi/5)$, $\operatorname{tg}(3\pi/5) = -\operatorname{tg}(2\pi/5)$, $\operatorname{tg}(4\pi/5) = -\operatorname{tg}(\pi/5)$ и $\operatorname{Res}(t_5(x), x^2 - t) = (t^2 - 10t + 5)^2$. Минимальный многочлен $s_5(t)$ числа $\operatorname{tg}^2(\pi/5)$ имеет вид $s_5(t) = t^2 - 10t + 5$. 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 $n \equiv 0 (\operatorname{mod} 4)$, то согласно лемме 3 работы [4] $\operatorname{tg}(\pi/n)$ 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 два примера.

Пример 4. Найдем многочлены $s_8(t)$, $s_{12}(t)$, $s_{16}(t)$, $s_{20}(t)$ и $s_{24}(t)$.

По теореме 1 имеем $s_n(t) = \operatorname{Res}(t_n(x), x^2 - t)$. 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

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

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

Теперь вычислим $s_8(t)$. Имеем

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

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

Аналогичными вычислениями находим

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

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

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

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

Пример 5. Выразим $\operatorname{tg}(\pi/n)$ как многочлен через $\operatorname{tg}^2(\pi/n)$ при $n = 16, 20, 24$.

Пусть $n = 16$. Тогда $t_{16}(x) = x^4+4x^3-6x^2-4x+1$. Так как $t_{16}(\mathrm{tg}(\pi/16)) = 0$, то $4\,\mathrm{tg}(\pi/16) = (t^2-6t+1)/(1-t)$, $t = \mathrm{tg}^2(\pi/16)$. Отсюда, пользуясь тем, что $s_{16}(t) = t^4-28t^3+70t^2-28t+1$ и $s_{16}(\mathrm{tg}^2(\pi/16)) = 0$, находим $(1-t)(t^3-27t^2+43t+15) = 16$ и $16\,\mathrm{tg}(\pi/16) = -t^3+27t^2-47t+5$, $t = \mathrm{tg}^2(\pi/16)$.

Аналогичные вычисления дают следующие равенства:

$4\,\mathrm{tg}(\pi/16) = (t^2-14t+1)/(1+t)$, $64\,\mathrm{tg}(\pi/20) = -t^3+45t^2-195t+15$, $t = \mathrm{tg}^2(\pi/20)$,

$8\,\mathrm{tg}(\pi/24) = (t^2+2t+1)/(1-t)$, $32\,\mathrm{tg}(\pi/24) = t^3-59t^2+71t+3$, $t = \mathrm{tg}^2(\pi/24)$.

Эти равенства остаются верными, если в них $\mathrm{tg}(\pi/n)$ заменить на любой другой корень многочлена $t_n(x)$, $n = 16, 20, 24$.

3. Поле, порожденное многочленом $\varphi(x) = x^3 - 7x - 7$

В примере 3 показано, что все корни многочлена $\varphi(x)$ рационально выражаются через любой его корень. Отсюда вытекает, что многочлен $\varphi(x)$ порождает нормальные расширения поля $\mathbb{Q}$ с абелевой группой Галуа. Это означает выполнение условий знаменитой теоремы Кронекера–Вебера [5], в силу которой поле, порожденное многочленом $\varphi(x) = x^3 - 7x - 7$, должно содержаться в некотором круговом поле $\mathbb{Q}_m$. Дискриминант многочлена $\varphi(x)$ равен 7^2. Значит, если L – поле, порожденное многочленом $\varphi(x)$ и $L \subset \mathbb{Q}_m$, то m должно быть кратным 7. Поэтому сначала изучим подполя поля $\mathbb{Q}_7$.

Поле $\mathbb{Q}_7$ порождается круговым многочленом $\Phi_7(x) = x^6+x^5+x^4+x^3+x^2+x+1$. Корнями этого многочлена являются числа $u_k = \cos(2\pi k/7) + i\sin(2\pi k/7)$, $k = 1, 2, 3, 4, 5, 6$.

Группа Галуа $G(\mathbb{Q}_7/\mathbb{Q})$ поля $\mathbb{Q}_7$ над $\mathbb{Q}$ (многочлена $\Phi_7(x)$) изоморфна мультипликативной группе классов вычетов, взаимно простых с $n = 7$ [6, с. 213].

Таким образом, $G(\mathbb{Q}_7/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5, \sigma_6\}$, σ_s действует по формуле $\sigma_s(u_k) = u_{ks}$, и умножение автоморфизмов сводится к умножению их индексов по модулю 7. Многочлен $\varphi(x) = x^3 - 7x - 7$ порождает поле степени 3.

Кубичное подполе L, содержащееся в поле $\mathbb{Q}_7$, должно быть инвариантно относительно подгруппы $H \subset G(\mathbb{Q}_7/\mathbb{Q})$ второго порядка. Значит, подгруппа H содержит два автоморфизма: $H = \{\sigma_1, \sigma_6\}$. Используя смежные классы $\sigma_1 H = \{\sigma_1, \sigma_6\}$, $\sigma_2 H = \{\sigma_2, \sigma_5\}$ и $\sigma_3 H = \{\sigma_3, \sigma_4\}$ по H, составим многочлены $\varphi_1(x) = (x-u_1)(x-u_6) = x^2-(u_1+u_6)x+1$, $\varphi_2(x) = (x-u_2)(x-u_5) = x^2-(u_2+u_5)x+1$, $\varphi_3(x) = (x-u_3)(x-u_4) = x^2-(u_3+u_4)x+1$.

Автоморфизмы подгруппы H оставляют на месте коэффициенты многочленов $\varphi_i(x)$, $i = 1, 2, 3$. Так как многочлен $\Phi_7(x)$ неприводим над $\mathbb{Q}$ и $\Phi_7(x) = \varphi_1(x)\,\varphi_2(x)\,\varphi_3(x)$, то не все коэффициенты многочленов $\varphi_i(x)$ $(i = 1, 2, 3)$ являются рациональными числами. Но эти коэффициенты инвариантны относительно автоморфизмов подгруппы H. Значит, $\varphi_i(x) \in L[x]$ и числа $a_1 = u_1+u_6$, $a_2 = u_2+u_5$, $a_3 = u_3+u_4$ порождают поле L. Найдем многочлен $g(y)$ с корнями a_1, a_2, a_3. Имеем $a_1+a_2+a_3 = u_1+u_2+u_3+u_4+u_5+u_6 = -1$, так как это есть сумма корней многочлена $\Phi_7(x)$.

Далее находим

$$\begin{aligned} a_1a_2+a_1a_3+a_2a_3 &= (u_1+u_6)(u_2+u_5)+(u_1+u_6)(u_3+u_4)+(u_2+u_5)(u_3+u_4) = \\ &= (u_3+u_6+u_1+u_4)+(u_4+u_5+u_2+u_3)+(u_5+u_6+u_1+u_2) = \\ &= 2(u_1+u_2+u_3+u_4+u_5+u_6) = -2. \end{aligned}$$

Аналогично имеем $a_1a_2a_3 = (u_1+u_6)(u_2+u_5)(u_3+u_4) = 1$.

Получилось, что числа a_1, a_2, a_3, порождающие поле L, являются корнями уравнения $g(y) = y^3 + y^2 - 2y - 1 = 0$. Но $a_1 = u_1 + u_6 = 2\cos(2\pi/7)$, $a_2 = u_2 + u_5 = 2\cos(4\pi/7)$ и $a_3 = u_3 + u_4 = 2\cos(6\pi/7)$.

Таким образом, известны все корни многочлена $g(y) = y^3 + y^2 - 2y - 1$, порождающего поле $L = \mathbb{Q}(\cos(2\pi/7))$, $L \subset \mathbb{Q}$.

Имеет место

Теорема 2. *Многочлен $\varphi(x) = x^3 - 7x - 7$ порождает поле $L = \mathbb{Q}(\cos(2\pi/7))$, являющееся подполем кругового поля $\mathbb{Q}_7$. Корни многочлена $\varphi(x)$ задаются формулами*

$$x_k = 4\cos^2(2\pi k/7) + 4\cos(2\pi k/7) - 1, \quad k = 1, 2, 3. \tag{1}$$

При этом если $x_1 = \beta$ – любой из этих корней, то два других корня задаются формулами

$$x_2 = -3\beta^2 + 4\beta + 14, \quad x_3 = 3\beta^2 - 5\beta - 14. \tag{2}$$

Доказательство. Выше уже показано, что многочлен $g(y) = y^3 + y^2 - 2y - 1$ порождает поле $L = \mathbb{Q}(\cos(2\pi/7))$ и что $L \subset \mathbb{Q}_7$. В примере 2 показано, что если $y = \alpha$ – корень многочлена $g(y)$, то $x = \beta = \alpha^2 + 2\alpha - 1$ – корень многочлена $\varphi(x) = x^3 - 7x - 7$. Другими словами, корни многочлена $\varphi(x)$ рационально выражаются через корни многочлена $g(y)$.

Верно и обратное. Действительно, из равенства $x = \beta = \alpha^2 + 2\alpha - 1$ получаем

$$(\beta + 1)^2 = \alpha^4 + 4\alpha^3 + 4\alpha = (\alpha^3 + 4\alpha^2 - 2\alpha - 1)(\alpha + 3) + 3\alpha^2 + 7\alpha + 3.$$

Учитывая, что α – корень многочлена $g(y)$, приходим к равенствам $\beta + 1 = \alpha^2 + 2\alpha$ и $\beta^2 + 2\beta - 2 = 3\alpha^2 + 7\alpha$. Отсюда находим $\alpha = \beta^2 - \beta - 5$. Это равенство означает, что корни многочлена $g(y)$ рационально выражаются через корни многочлена $\varphi(x)$. Итак, доказано, что многочлены $g(y)$ и $\varphi(x)$ порождают одно и то же поле $L = \mathbb{Q}(\cos(2\pi/7))$. Так как корнями многочлена $g(y) = y^3 + y^2 - 2y - 1$ являются числа $\cos(2\pi k/7)$, $k = 1, 2, 3$ и корни x_k многочлена $\varphi(x)$ получаются из корней y_k многочлена $g(y)$ по формуле $x_k = y_k^2 + 2y_k - 1$, то формулы (1) доказаны.

В примере 3 показано, что если $x_1 = \beta$ – корень многочлена $\varphi(x) = x^3 - 7x - 7$, то $x_2 = -3\beta^2 + 4\beta + 14$ также его корень. Значит, корнем $\varphi(x)$ является и $x_3 = -3x_2^2 + 4x_2 + 14 = 3\beta^2 - 5\beta - 14$. В том, что числа x_1, x_2, x_3 являются корнями $\varphi(x)$, можно убедиться по формулам Виета.

Таким образом, формулы (2) доказаны.

Многочлены $f(x) \in \mathbb{Q}[x]$ и $g(x) \in \mathbb{Q}[x]$, определяющие одно и то же поле, Н.Г. Чеботарев [2, с. 139] назвал родственными. Корни этих многочленов рационально выражаются друг через друга. Нахождение этой рациональной связи называют обратной задачей Чирнгаузена [2, с. 139].

Если $n \equiv 0 (\mathrm{mod}\, 4)$, то многочлены $t_n(x)$ и $s_n(x)$, о которых говорится в п. 2, являются родственными. Если $x = \alpha$ – корень многочлена $t_n(x)$, то $x = \alpha^2$ – корень многочлена $s_n(x)$. Можно показать, что многочлены $t_n(x)$ и $s_n(x)$ определяют поле $L = \mathbb{Q}(\mathrm{tg}(\pi/n)) = \mathbb{Q}(\mathrm{tg}^2(\pi/n))$, входящее в круговое поле $\mathbb{Q}_n$, при этом $[\mathbb{Q}_n : \mathbb{Q}(\mathrm{tg}(\pi/n))] = 2$.

Summary

I.G. Galyautdinov, E.E. Lavrentyeva. Determination of the Minimal Polynomials of Algebraic Numbers of the Form $\mathrm{tg}^2(\pi/n)$ by the Tschirnhausen Transformation.

Solutions of two problems are offered based on the Tschirnhausen transformation. The first problem is connected with the construction of minimal polynomials of the numbers of the form

$\mathrm{tg}^2(\pi/n)$ by means of the Tschirnhausen transformation for all natural $n > 2$. The second problem consists in finding the exact values of the roots of the equation $x^3 - 7x - 7 = 0$. The solution of the problem is obtained by considering the fact that the roots of the equation produce the circular field $\mathbb{Q}_7$. The examples of the construction of minimal polynomials are provided.

Keywords: algebraic numbers, minimal polynomials, circular fields and subfields, Tschirnhausen transformation.

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 // Изв. вузов. Матем. – 2011. – № 2. – С.22–30.
5. *Шафаревич И.О.* Новое доказательство теоремы Кронекера – Вебера // Труды Матем. Ин-та АН СССР. – 1951. – Т. 38. – С. 382–387.
6. *Кострикин А.И.* Введение в алгебру. Ч. 3. – М.: Физматлит, 2001. – 272 с.
7. *Прасолов В.В.* Многочлены. – М.: МЦИМО, 2003. – 335 с.
8. *Арнольд В.И.* О классах когомологий алгебраической функции, инвариантных относительно преобразования Чирнгаузена // Функциональный анализ и его приложения. – 1970. – Т. 4, № 1. – С. 84–85.
9. *Колмогоров А.И.* Избранные труды. Математика и механика. – М.: Наука, 1985. – 470 с.
10. *Бурбаки Н.* Очерки по истории математики. – М.: Изд-во иностр. лит., 1963. – 292 с.

Поступила в редакцию
15.12.14

Галяутдинов Ильдархан Галяутдинович – кандидат физико-математических наук, доцент кафедры естественных и технических дисциплин, КФ ФГБУ ВПО «Поволжский государственный университет телекоммуникаций и информатики», г. Казань, Россия.

Лаврентьева Елена Евгеньевна – кандидат педагогических наук, доцент кафедры информационных систем, Казанский (Приволжский) федеральный университет, г. Казань, Россия.

E-mail: *ialee-4@mail.ru*