А. Э. Сергеев, А. В. Яковлев, О спектрах Галуа многочленов, зависящих от целочисленных параметров,
Зап. научн. сем. ПОМИ, 2005, том 321, 275–280

Записки научных
семинаров ПОМИ
Том 321, 2005 г.

А. Э. Сергеев, А. В. Яковлев

О СПЕКТРАХ ГАЛУА МНОГОЧЛЕНОВ, ЗАВИСЯЩИХ ОТ ЦЕЛОЧИСЛЕННЫХ ПАРАМЕТРОВ

Пусть $F(x;t_1,\ldots,t_r)$ – многочлен от $r+1$ переменных с рациональными коэффициентами, неприводимый как многочлен над полем $\mathbb{Q}(t_1,\ldots,t_r)$, и пусть n – его степень как многочлена от x. Пусть, далее, $\mathfrak{C}_n$ – множество классов сопряженности транзитивных подгрупп симметрической группы S_n. Мы называем подмножество $\mathfrak{A} \subseteq \mathfrak{C}_n$ целочисленным спектром Галуа многочлена $F(x;t_1,\ldots,t_r)$, если выполнены условия:

(1) Для любых целых чисел $a_1,\ldots,a_r$, таких что многочлен $F(x;a_1,\ldots,a_r)$ неприводим над $\mathbb{Q}$, класс сопряженности группы Галуа (над $\mathbb{Q}$) поля разложения многочлена $F(x;a_1,\ldots,a_r)$ принадлежит $\mathfrak{A}$.

(2) Для всякого класса $\mathfrak{a}$ сопряженных подгрупп группы S_n, принадлежащего $\mathfrak{A}$, существуют такие целые числа $a_1,\ldots,a_r$, что многочлен $F(x;a_1,\ldots,a_r)$ неприводим над $\mathbb{Q}$, а класс сопряженности группы Галуа (над $\mathbb{Q}$) его поля разложения равен $\mathfrak{a}$.

Задача описания подмножеств множества $\mathfrak{C}_n$, которые могут быть целочисленными спектрами Галуа параметрического многочлена $F(x;t_1,\ldots,t_r)$, достаточно трудна уже для небольших n. В настоящей работе завершается ее решение для $n=4$, начатое первым из авторов в [1]. Прежде, чем сформулировать результат, введем обозначения для классов сопряженных транзитивных подгрупп группы S_4:

S_4 – класс, состоящий из единственной группы S_4;

A_4 – класс, состоящий только из знакопеременной группы A_4;

V_4 – класс, состоящий из единственного нормального делителя группы S_4, имеющего порядок 4;

D_4 – класс, состоящий из диэдральных подгрупп порядка 8 группы S_4;

C_4 – класс, состоящий из транзитивных циклических подгрупп порядка 4 группы S_4.

Теорема 1. *Подмножества* $\{A_4, C_4\}$, $\{A_4, D_4\}$, $\{V_4, C_4\}$, $\{A_4, D_4, C_4\}$, $\{A_4, V_4, C_4\}$, $\{A_4, D_4, V_4\}$, $\{A_4, D_4, V_4, C_4\}$ *множества* $\mathfrak{C}_4$ *классов сопряженных подгрупп симметрической группы* S_4 *не могут быть целочисленными спектрами Галуа ни для каких многочленов* $F(x; t_1, \dots, t_r) \in \mathbb{Q}[x; t_1, \dots, t_r]$. *Для каждого из множеств* $\mathfrak{C}_4 = \{S_4, A_4, D_4, V_4, C_4\}$, $\{S_4, A_4, D_4, V_4\}$, $\{S_4, D_4, V_4, C_4\}$, $\{S_4, A_4, D_4, C_4\}$, $\{S_4, A_4, D_4\}$, $\{S_4, A_4, V_4\}$, $\{S_4, A_4, C_4\}$, $\{S_4, D_4, V_4\}$, $\{S_4, D_4, C_4\}$, $\{S_4, V_4, C_4\}$, $\{D_4, V_4, C_4\}$, $\{S_4, A_4\}$, $\{S_4, D_4\}$, $\{S_4, V_4\}$, $\{S_4, C_4\}$, $\{A_4, V_4\}$, $\{D_4, V_4\}$, $\{D_4, C_4\}$, $\{S_4\}$, $\{A_4\}$, $\{D_4\}$, $\{V_4\}$, $\{C_4\}$ *существует параметрический многочлен* $F(x; t_1, \dots, t_r) \in \mathbb{Q}[x; t_1, \dots, t_r]$, *целочисленным спектром Галуа которого является это множество.*

Эта теорема суммирует результаты, полученные в [1]. Отрицательные результаты вытекают из теоремы Гильберта о неприводимости (точнее, из ее целочисленного варианта), а положительные доказываются явным предъявлением соответствующих многочленов. Трудной частью положительных результатов является доказательство того, что ни при каких специализациях параметров группа Галуа предъявленного параметрического многочлена не принимает запрещенное значение.

И только для одного подмножества множества $\mathfrak{C}_4$ оставалось неясным, может ли оно быть целочисленным спектром параметрического многочлена. Речь идет о множестве $\{S_4, A_4, V_4, C_4\}$. Высказывалось предположение, что многочленом с таким спектром может быть многочлен

$$x^4 + (2t^2 - 2t - 4)x^2 + 4(t^2 - t)x + (t^3 + 6t^2 - 6t + 1);$$

однако доказать, что ни при каком целом значении t его группой не может стать диэдральная группа D_4, не получалось. Немного изменив многочлен, нам удалось преодолеть эту трудность. Доказательство этого результата и является целью настоящей работы.

Теорема 2. *Целочисленный спектр Галуа многочлена*

$$F(x, t) = x^4 + (2t^2 - 2t - 4)x^2 + 8((t^2 - t)/2)^{102}x + (t^3 + 6t^2 - 6t + 1)$$

состоит из классов $\{S_4, A_4, V_4, C_4\}$ *сопряженных подгрупп группы* S_4.

Замечание. Наша модификация состояла в том, что мы заменили коэффициент $8((t^2-t)/2)$ при первой степени x на $8((t^2-t)/2)^{102}$. Выбор числа 102 в качестве показателя степени в значительной степени случаен: важно, чтобы этот показатель был достаточно большим, и полезно, чтобы он делился на 3.

Доказательство. При $t = -1, 0, 1, 2$ мы получаем многочлены

$$x^4 + 8x + 12, \qquad x^4 - 4x^2 + 1, \qquad x^4 - 4x^2 + 2, \qquad x^4 + 8x + 21,$$

группы Галуа которых равны соответственно A_4, V_4, C_4, S_4 (в этом легко убедиться, например, обратившись к любой компьютерной программе, вычисляющей группы Галуа многочленов). Остается показать, что при $t \neq -1, 0, 1, 2$ группа Галуа многочлена $F(x,t)$ не является диэдральной группой. Но если группа Галуа многочлена четвертой степени является диэдральной группой, то один из корней кубической резольвенты должен быть рациональным: если все корни резольвенты иррациональны, то резольвента является неприводимым над $\mathbb{Q}$ многочленом, и степень ее поля разложения, которое содержится в поле разложения исходного многочлена 4-й степени, делится на 3. Поэтому нам достаточно доказать, что при $t \neq -1, 0, 1, 2$ кубическая резольвента многочлена $F(x,t)$ не имеет рациональных корней.

Лемма 1. *Пусть b, c, d – вещественные числа. Если $|b| + |c| + 1 < d/3$, то многочлен $f(x) = x^3 + bx + (c - d^3)$ имеет единственный вещественный корень α, причем $|d - \alpha| < 1/3$. Если при этом d – корень $f(x)$, а $3b$ – целое число, то $b = 0$.*

Доказательство. В предположениях леммы $d > 1$, $|b|, |c| < d/3$; поэтому

$$|b| < d^2/3, \qquad |c| < d^3/3,$$

и $d^3 - c \geqslant d^3 - |c| \geqslant 2d^3/3$. Отсюда получаем следующую оценку для дискриминанта многочлена $f(x)$:

$$-4b^3 - 27(c - d^3)^2 \leqslant -27(2d^3/3)^2 + 4(d^2/3)^3 = (-12 + 4/27)d^6 < 0.$$

Таким образом, дискриминант многочлена $f(x)$ отрицателен, а значит, этот многочлен имеет единственный вещественный корень α. Заметим, что при наших предположениях

$$|d(b + 1/3) + (c \pm b/3 \pm 1/27)| \leqslant$$
$$\leqslant d(|b| + |c| + 1) + (|b| + |c| + 1) < (d + 1)d/3 < 2d^2/3 < d^2,$$

поэтому

$$f(d+1/3) = d^2 + d(b+1/3) + (c+b/3+1/27) \geqslant \\ \geqslant d^2 - |d(b+1/3) + (c+b/3+1/27)| > d^2 - d^2 = 0,$$

и аналогично

$$f(d-1/3) = -d^2 + d(b+1/3) + (c-b/3-1/27) \leqslant \\ \leqslant -d^2 + |d(b+1/3) + (c-b/3-1/27)| < -d^2 + d^2 = 0.$$

Таким образом, единственный вещественный корень многочлена $f(x)$ принадлежит промежутку $(d-1/3, d+1/3)$.

Предположим теперь, что $3b$ – целое число. Если $b \neq 0$, то $|b| \geqslant 1/3$, а из неравенства $|b|+|c|+1 < d/3$ следует, что $|c| < d/3$; поэтому тогда

$$|f(d)| = |d^3 + bd + (c-d^3)| = |bd+c| \geqslant |bd| - |c| > d/3 - d/3 = 0,$$

а это значит, что d – не корень $f(x)$.

Лемма 2. *Пусть a, b, c, d – вещественные числа. Если*

$$1 + |b| + |c| + |ab| + |a|^2 + |a|^3 < d/3,$$

то многочлен $f(x) = x^3 + ax^2 + bx + (c-d^3)$ имеет единственный вещественный корень α, причем $|d-a/3-\alpha| < 1/3$. Если при этом числа a, b целые, а $d-a/3$ – корень $f(x)$, то $3b = a^2$.

Доказательство. Положим $x = y - a/3$; тогда

$$f(x) = x^3 + ax^2 + bx + (c-d^3) = y^3 + b_1 y + (c_1 - d^3),$$

где $b_1 = b - a^2/3$, $c_1 = 2a^3/9 - ab/3 + c$. В условиях леммы

$$1 + |b_1| + |c_1| = 1 + |b - a^2/3| + |2a^3/9 - ab/3 + c| \leqslant \\ \leqslant 1 + |b| + |a^2/3| + |2a^3/9| + |ab/3| + |c| \leqslant \\ \leqslant 1 + |b| + |c| + |ab| + |a|^2 + |a|^3 < d/3,$$

поэтому по лемме 1 многочлен $y^3 + b_1 y + (c_1 - d^3)$ имеет единственный вещественный корень β, причем $|d-\beta| < 1/3$. Следовательно, у многочлена $x^3 + ax^2 + bx + (c-d^3)$ единственный вещественный корень $\alpha = \beta - a/3$, и $|d - a/3 - \alpha| < 1/3$. Если числа a, b целые и $d - a/3$ – корень $f(x)$, то d – корень многочлена $y^3 + b_1 y + (c_1 - d^3)$, а $3b_1 = 3b - a^2$ – целое число; по последнему утверждению леммы 1 это возможно, только если $b_1 = b - a^2/3 = 0$.

Лемма 3. *Если a, b, c, d – целые числа, $a^2 \neq 3b$ и*

$$1 + |b| + |c| + |ab| + |a|^2 + |a|^3 < d/3,$$

то многочлен $f(x) = x^3 + ax^2 + bx + (c - d^3)$ не имеет рациональных корней.

Доказательство. Поскольку при целых a, b, c, d все коэффициенты многочлена $f(x) = x^3 + ax^2 + bx + (c - d^3)$ целые, а его старший коэффициент равен 1, любой рациональный корень $f(x)$ является целым. В то же время, по лемме 2 этот корень должен принадлежать открытому промежутку

$$(d - a/3 - 1/3, d - a/3 + 1/3)$$

и не должен быть равным $d - a/3$; если a не делится на 3, то в указанном промежутке нет целых чисел, а если a делится на 3, то $d - a/3$ – единственное принадлежащее ему целое число.

Мы можем теперь завершить доказательство теоремы 2. Для этого, как отмечалось, достаточно показать, что при целом $t \neq -1, 0, 1, 2$ кубическая резольвента многочлена 4-й степени

$$F(x,t) = x^4 + (2t^2 - 2t - 4)x^2 + 8((t^2 - t)/2)^{102}x + (t^3 + 6t^2 - 6t + 1)$$

не имеет рациональных корней.

Для сокращения записи обозначим число $(t^2 - t)/2$ через z; заметим, что при любом целом t число z тоже целое, причем если $t \neq -1, 0, 1, 2$, то $|z| \geqslant 2$, $2|z| = |t| \cdot |t - 1| \geqslant |t|$. Далее, положим

$$u(t) = 2t^2 - 2t - 4, \quad v(t) = t^3 + 6t^2 - 6t + 1, \quad w(t) = 2z^{34}.$$

Тогда $F(x,t) = x^4 + u(t)x^2 + (w(t))^3x + v(t)$, а кубическая резольвента многочлена $F(x,t)$ принимает вид

$$y^3 + a(t)y^2 + b(t)y + (c(t) - (d(t)^3)),$$

где $a(t) = -u(t)$, $b(t) = -4v(t)$, $c(t) = 4u(t)v(t)$, $d(t) = (w(t))^2 = 4z^{68}$.

Оценим коэффициенты резольвенты (при $t \neq -1, 0, 1, 2$). Сначала заметим, что

$$\begin{aligned} |u(t)| &= |2t^2 - 2t - 4| \leqslant 2|t^2| + 2|t| + 4 \leqslant 8|t|^2 \leqslant 32|z|^2 = 2^5|z|^2; \\ |v(t)| &= |t^3 + 6t^2 - 6t + 1| \leqslant |t|^3 + 6|t|^2 + 6|t| + 1 < 14|t|^3 \\ &\leqslant 112|z|^3 < 2^7|z|^3. \end{aligned}$$

Теперь находим

$$|a(t)| = |u(t)| \leqslant 2^5|z|^2; \quad |b(t)| = 4|v(t)| \leqslant 2^9|z|^3;$$
$$|c(t)| = 4|u(t)| \cdot |v(t)| \leqslant 2^{14}|z|^5.$$

Поэтому

$$1 + |b(t)| + |c(t)| + |a(t)b(t)| + |a(t)|^2 + |a(t)|^3 \leqslant 1 + 2^9|z|^3 + 2^{14}|z|^5 +$$
$$+2^5|z|^2 \cdot 2^9|z|^3 + 2^{10}|z|^4 + 2^{15}|z|^6 \leqslant (1 + 2^5 + 2^{14} + 2^{14} + 2^{10} + 2^{15})|z|^6 <$$
$$< 2^{17}|z|^6 \leqslant |z|^{23} < 4/3|z|^{68} = d(t)/3.$$

Покажем теперь, что при наших предположениях $(a(t))^2 \neq 3b(t)$. Если бы это было не так, то целое число t было бы корнем многочлена

$$(a(t)/2)^2 - 3b(t)/4 = (t^2 - t - 2)^2 + 3(t^3 + 6t^2 - 6t + 1) = t^4 + t^3 + 15t^2 - 14t + 7$$

с целыми коэффициентами, и потому оно было бы делителем свободного члена 7 этого многочлена, т.е. было бы равно ± 1 или ± 7; ни одно из этих чисел не является корнем нашего многочлена.

Таким образом, при $t \neq -1, 0, 1, 2$ коэффициенты кубической резольвенты многочлена $F(x,t)$ удовлетворяют всем требованиям леммы 3, и потому резольвента не имеет рациональных корней.

Литература

1. А.Э.Сергеев, *Обратная задача для спектров полиномов.* — Деп. в ВИНИТИ, 881-В2004 (25.05.2004), 1–35.

Sergeev A. E., Yakovlev A. V. On the Galois spectra of polynomials with integral parameters.

We prove that there exists a polynomial $F(x,t)$ with rational coefficients whose degree with respect to x is equal to 4, such that for every integer the Galois group of the decomposition field of the polynomial $F(x,a)$ is not the dihedral group, but any other transitive subgroup of the group S_4 can be represented as the Galois group of the decomposition field of the polynomial $F(x,a)$ for some integer a.

С.-Петербургский
государственный университет
E-mail: yakovlev@yak.pdmi.ras.ru

Поступило 10 декабря 2004 г.