УДК 519.642.8

ПАРАМЕТРИЧЕСКИЕ ТРИНОМЫ СО ЗНАКОПЕРЕМЕННОЙ ГРУППОЙ ГАЛУА

Сергеев Александр Эдуардович
к.ф.-м.н., доцент

Потемкина Людмила Николаевна
аспирантка
Кубанский государственный университет, Краснодар, Россия

В статье построены многочлены 3-ей, 4-ой и 5-ой степеней с группами Галуа A_3, A_4 и A_5 соответственно. Также строятся примеры многочленов n-ой степени с группами Галуа изоморфными транзитивной подгруппе группы A_n, но как показывают вычисления на Maple для $3 \le n \le 11$ группа Галуа этих многочленов будет изоморфна A_n. Приводится также обзор известных результатов по нахождению многочленов с группами Галуа A_n

Ключевые слова: ЗНАКОПЕРЕМЕННАЯ ГРУППА, РЕЗОЛЬВЕНТА МНОГОЧЛЕНА, ДИСКРИМИНАНТ МНОГОЧЛЕНА

UDK 519.642.8

PARAMETRIC TRINOMIALS WITH ALTERNATING GALOIS GROUPS

Sergeev Alexander Eduardovich
Cand.Phys.-Math.Sci, associate professor

Potemkina Ludmila Nikolaevna
postgraduate student
Kuban State University, Krasnodar, Russia

In this article, we construct polynomials of third, fourth and fifth degrees with Galois groups as A_3, A_4 and A_5 respectively. In addition, we give examples of polynomials different degrees with Galois groups isomorphic transitive subgroup of group A_n, but calculations with help Maple show that Galois groups of this polynomials is A_n. Also Polynomials with A_n as Galois groups are shown

Keywords: ALTERNATING GROUP, RESOLVENT OF POLYNOMIAL, DISCRIMINANT OF POLYNOMIAL

Как известно, в общем случае вычисление группы Галуа многочленов является трудоемкой работой. Для многочленов степени от 2 до 5 известны критерии, позволяющие вычислять группы Галуа. Построим параметрические триномы третей, четвертой, пятой и n-ой степеней с группами Галуа A_3, A_4, A_5 и A_n соответственно. Также для целых $n \ge 7$ покажем, как можно построить бесконечное число триномов степени n, группа Галуа которых над полем Q изоморфна альтернативной группе Галуа A_n.

Трином третьей степени

Для этого случая имеется ровно два вида триномов: $x^3 + ax + b$ и $x^3 + ax^2 + b$. Известно, что для того, чтобы группа Галуа данных полиномов была изоморфна знакопеременной группе A_3 необходимо и достаточно, чтобы выполнялись следующие условия [1]:

1) данный полином должен быть неприводимым над основным полем (т.е. над полем Q);

2) его дискриминант $D(f)$ должен быть квадратом некоторого элемента поля Q.

Для реализации группы A_3 надо решить диофантово уравнение:

$$-4a^3 - 27b^2 = k^2 \qquad (1)$$

для триномов вида $x^3 + ax + b$ и

$$-4a^3b - 27b^2 = k^2 \qquad (2)$$

для триномов вида $x^3 + ax^2 + b$.

Найдем частное решение для уравнения (1): пусть $a = 3c,\ b = 2c$, тогда $D(f) = 2^2 \cdot 3^3 \cdot c^2 \cdot (-c-1) = k^2 \quad \Rightarrow \quad c = -3k^2 - 1$. Следовательно, $a = 3(-3k^2 - 1)$ и $b = 2(-3k^2 - 1)$.

Таким образом, трином (1) имеет следующий параметрический вид:

$$f(x) = x^3 + 3(-3k^2 - 1)x + 2(-3k^2 - 1),$$

и его дискриминант есть квадрат: $D(f) = \left[2 \cdot 3^2 \cdot k \cdot \left(-3k^2 - 1\right)\right]^2$. Поэтому его группа Галуа $Gal_Q f \cong A_3$.

Пример 1. Пусть $k = 2$, тогда многочлен $f(x) = x^3 - 39x - 26$ – неприводим над полем Q, дискриминант $D(f) = (6^2 \cdot (-13))^2$, поэтому группа Галуа данного многочлена над Q изоморфна A_3.

Найдем частное решение для уравнения (2): пусть $a = 3c$, $b = 2c^2$, тогда $D(f) = 2^2 \cdot 3^3 \cdot c^4 \cdot (-2c-1) = k^2 \quad \Rightarrow \quad c = \frac{3k^2+1}{-2}$. Следовательно, $a = \frac{3(3k^2+1)}{-2}$ и $b = 2 \cdot \left(\frac{3k^2+1}{-2}\right)^2$.

Таким образом, мы получили многочлен

$$f(x) = x^3 + 3 \cdot \left(\frac{3k^2+1}{-2}\right) \cdot x^2 + 2 \cdot \left(\frac{3k^2+1}{-2}\right)^2,$$

и его дискриминант есть квадрат: $D(f)=\left[2\cdot 3^2\cdot k\cdot\left(\frac{3k^2+1}{-2}\right)^2\right]^2$. Поэтому его группа Галуа $Gal_Q f\cong A_3$.

Таким образом, можно получить бесконечно много триномов с группой Галуа A_3.

Трином четвертой степени

Для триномов четвертой степени известно, что для того, чтобы группа Галуа данного полинома была изоморфна знакопеременной группе A_4, необходимо и достаточно, чтобы выполнялись следующие условия [1]:

1) данный полином должен быть неприводимым над основным полем (т.е. над полем Q);
2) его дискриминант должен быть квадратом некоторого элемента поля Q;
3) резольвента $r(x)=x^3-bx^2+(ac-4d)x-(a^2d-4bd+c^2)$, где $a,\ b,\ c,\ d$ – коэффициенты данного полинома, должна быть неприводима над основным полем Q.

Дискриминантом для данного многочлена является выражение вида $D(f)=4^4b^3-3^3a^4$. Сделаем так, чтобы он был квадратом в поле Q; пусть $a=4c,\quad b=3c\quad (c\in Q)$, тогда: $D(f)=4^43^3c^3-3^34^4c^4=4^4(3c)^3(1-c)$. Пусть теперь $1-c=3ct^2$, $t\in Q\setminus\{0\}$, тогда $c=\frac{1}{3t^2+1}$ и $D(f)=4^4\frac{3^3}{(3t^2+1)^3}\cdot\frac{3t^2}{(3t^2+1)}=\frac{4^43^4t^2}{(3t^2+1)^4}$.

Теорема 1. Пусть многочлен $f(x)=x^4+\frac{4}{3t^2+1}x+\frac{3}{3t^2+1}$ является неприводимым над полем Q и $t\in Q\setminus\{0\}$. Тогда группа Галуа этого многочлена над полем Q изоморфна A_4, если многочлен $r(x)=x^3-\frac{12}{3t^2+1}x-\frac{16}{(3t^2+1)^2}$ неприводим над полем Q.

Доказательство. Дискриминант данного многочлена есть $D(f)=\left[\frac{4^2 3^2 t}{\left(3t^2+1\right)^2}\right]^2$, т.е. является квадратом некоторого элемента поля Q. Резольвента для этого многочлена имеет вид $r(x)=x^3-\frac{12}{3t^2+1}x-\frac{16}{\left(3t^2+1\right)^2}$, и, если она неприводима, то, согласно вышеприведенным условиям, группа Галуа $Gal_Q f\cong A_4$.

Пример 2. Пусть $t=1$, тогда $f(x)=x^4+x+\frac{3}{4}$ – неприводим над Q, резольвента $r(x)=x^3-3x-1$ – неприводима над Q, дискриминант многочлена $D(f)=81=9^2$. Следовательно, по теореме 1, группа Галуа этого многочлена изоморфна A_4 над полем Q.

Замечание. 1) Можно доказать, что если $3t^2+1$ не есть квадрат рационального числа, то многочлен $r(x)$ неприводим над Q;

2) как показывают вычисления на Maple, многочлен $r(x)$ до $t\le 10000$ всегда является неприводимым над Q.

Трином пятой степени

Для триномов пятой степени известно, что для того чтобы он имел группу A_5 в качестве группы Галуа, необходимо и достаточно, чтобы выполнялись следующие условия [2]:

1) данный многочлен должен быть неприводимым над основным полем (т.е. над полем Q);
2) его дискриминант должен быть квадратом некоторого элемента поля Q;
3) резольвента $g(z)=\left(z^3-5az^2+15a^2z+5a^3\right)^2-D(f(x))z$, где $D(f(x))$ – дискриминант многочлена $f(x)$ не имеет корней в поле Q.

Дискриминантом для данного многочлена имеет вид $D(f)=5^5b^4+4^4a^5$. Сделаем так, чтобы он был квадратом в поле Q: пусть $a=5c$, $b=4c$ $(c\in Q)$,

тогда $D(f) = 5^5 4^4 c^4 + 4^4 5^5 c^5 = 5^5 (4c)^4 (1+c)$. Пусть теперь $1+c = 5k^2$, $(k \in Q \setminus \{0\})$, тогда $c = 5k^2 - 1$, следовательно, $D(f) = 5^6 4^4 k^2 (5k^2 - 1)^4$.

Справедлива следующая теорема.

Теорема 2. Пусть многочлен $f(x) = x^5 + 5(5k^2 - 1)x + 4(5k^2 - 1)$ является неприводимым над полем Q и $k \in Q \setminus \{0\}$. Тогда, группа Галуа этого многочлена над полем Q изоморфна A_5, если многочлен $g(z)$ неприводим над полем Q.

Доказательство. Дискриминант данного полинома есть $5^6 4^4 k^2 (5k^2 - 1)^4$, т.е. является квадратом некоторого элемента поля Q.. Многочлен $g(z)$ имеет вид:

$$g(z) = \left(z^3 - 25(5k^2 - 1)z^2 + 15 \cdot 5^2 (5k^2 - 1)^2 z + 5^4 (5k^2 - 1)^3\right)^2 - 5^6 4^4 k^2 (5k^2 - 1)^4 z,$$

и если многочлен $g(z)$ – неприводим над полем Q, то по вышеприведенным условиям, группа Галуа данного полинома над полем Q изоморфна A_5.

Пример 3. Пусть $k = 1$, тогда многочлен $f(x) = x^5 + 20x + 16$ – неприводим над Q, многочлен $g(z) = (z^3 - 100z^2 + 15 \cdot 80^2 z + 5^4 \cdot 64)^2 - 5^6 4^8 z$ – неприводим над Q. Следовательно, по теореме 2, группа Галуа данного многочлена изоморфна A_5.

Трином n-ой степени

Рассмотрим полином n-ой степени $f(x) = x^n + ax + b$. Для того чтобы он имел группу A_n в качестве группы Галуа, необходимо и достаточно, чтобы выполнялись следующие условия:

1) данный полином должен быть неприводимым над основным полем (т.е. над полем Q);
2) его дискриминант должен быть квадратом некоторого элемента поля Q;
3) резольвента не должна иметь корней в поле Q.

Замечание. 1) Резольвента даже для многочлена степени ≥ 9 еще не построена;

2) для многочлена даже восьмой степени известно, что для различия всех транзитивных подгрупп группы S_8 построены три резольвенты. Чем больше степень многочлена, тем больше резольвент необходимо, чтобы различить все транзитивные подгруппы группы S_n

Дискриминант данного полинома вычисляется по следующей формуле: $D(f(x)) = (-1)^{n(n-1)/2} n^n b^{(n-1)} + (-1)^{(n-1)(n-2)/2} (n-1)^{(n-1)} a^n$.

Найдем частное решение диофантова уравнения $D(f) = u^2,\ u \in Q$, т.е. имеем уравнение:

$$(-1)^{n(n-1)/2} n^n b^{(n-1)} + (-1)^{(n-1)(n-2)/2} (n-1)^{(n-1)} a^n = u^2. \qquad (3)$$

Пусть $a = nc$, $b = (n-1)c$, где n – **нечетное** число. Решая диофантово уравнение (3), находим, что одним из частных решений его являются:

$$a = n \cdot \left(\frac{nk^2 - (-1)^{n(n-1)/2}}{(-1)^{(n-1)(n-2)/2}} \right), \quad b = (n-1) \cdot \left(\frac{nk^2 - (-1)^{n(n-1)/2}}{(-1)^{(n-1)(n-2)/2}} \right),$$

где n – нечетное число.

Тогда данный многочлен можно записать в параметрической форме:

$$f(x) = x^n + n \cdot \left(\frac{nk^2 - (-1)^{n(n-1)/2}}{(-1)^{(n-1)(n-2)/2}} \right) \cdot x + (n-1) \cdot \left(\frac{nk^2 - (-1)^{n(n-1)/2}}{(-1)^{(n-1)(n-2)/2}} \right).$$

Следовательно, дискриминант данного полинома над полем Q есть квадрат:

$$D(f(x)) = \left[n^{\frac{n+1}{2}} \cdot k \cdot \left((n-1) \cdot \frac{nk^2 - (-1)^{n(n-1)/2}}{(-1)^{(n-1)(n-2)/2}} \right)^{\frac{n-1}{2}} \right]^2 \text{ для нечетных } n.$$

Теперь рассмотрим случай, когда числа n – **четные**. Снова положим $a = nc$, $b = (n-1)c$. Решая диофантово уравнение (3), находим, что одним из частных решений его являются:

$$a = n \cdot \left(\frac{(-1)^{n(n-1)/2}}{(n-1)k^2 - (-1)^{(n-1)(n-2)/2}} \right), \quad b = (n-1) \cdot \left(\frac{(-1)^{n(n-1)/2}}{(n-1)k^2 - (-1)^{(n-1)(n-2)/2}} \right),$$

где $n-$ четное число.

Тогда данный многочлен запишется в виде:

$$f(x)=x^n+n\cdot\left(\frac{(-1)^{n(n-1)/2}}{(n-1)k^2-(-1)^{(n-1)(n-2)/2}}\right)\cdot x+(n-1)\cdot\left(\frac{(-1)^{n(n-1)/2}}{(n-1)k^2-(-1)^{(n-1)(n-2)/2}}\right).$$

Вычисляя дискриминант этого тринома, получим, что он есть квадрат в поле Q и имеет вид:

$$D(f(x))=\left[n^{\frac{n}{2}}\cdot(n-1)^{\frac{n}{2}}\cdot k\cdot\left(\frac{(-1)^{n(n-1)/2}}{(n-1)k^2-(-1)^{(n-1)(n-2)/2}}\right)^{\frac{n}{2}}\right]^2, \text{ для четных } n.$$

Осталось показать, что резольвента не имеет корней над полем Q. Но, к сожалению, на данный период времени не существует утверждения для нахождения резольвенты для данного полинома. Поэтому мы пока не можем утверждать, что данный полином имеет группу A_n в качестве группы Галуа. Мы лишь можем говорить о том, что найденная группа данного многочлена будет являться транзитивной подгруппой группы A_n, при условии, что сам многочлен $f(x)$ неприводим над Q.

Таким образом, справедлива гипотеза:

Гипотеза. Группа $Gal_Q f\cong A_n$.

Пример 4. Пусть $n=11$, $k=2$. Тогда многочлен $f(x)=x^{11}-495x-450$ – неприводим над Q, дискриминант его является квадратом в поле Q и его группа Галуа является подгруппой группы A_n, однако, как показывают вычисления на Maple, $Gal_Q A_{11}$.

Пример 5. Пусть $n=10,\ k=2.$ Тогда многочлен $f(x)=x^{10}-\frac{2}{7}x-\frac{9}{35}$ – неприводим над Q, дискриминант его является квадратом в поле Q и его группа Галуа является подгруппой группы A_{10}, однако, как показывают вычисления на Maple, $Gal_Q A_{10}$.

Триномы степени $n \geq 7$

Будем рассматривать триномы следующего вида:

$$f(X) = X^n + aX^m + b,\ ab \neq 0 \qquad (4)$$

где $n > m > 0$ положительные целые числа.

Теорема 3. Пусть $n \geq 7$ и m нечетное число, взаимно-простое с n, так что $3 \leq m \leq n-4$. Также, пусть p – простое, не делящее $mn(n-m)$, которое расщепляется в поле $Q(\sqrt{(-1)^{\frac{n-1}{2}} n})$, если n – не квадрат натурального числа, и q – другое простое число, не делящее $pnm(n-m)$. Тогда существуют целые числа r и s, удовлетворяющие условию (5):

$$(s(n-m)-r, n) = 1, \quad 0 < s < n, \quad 0 \leq r < n-m \qquad (5)$$

Также существует такое натуральное число $\mathbf{l}$ взаимно-простое с q такое, что:

$$u_p\left(\mathbf{l}^2 + (-1)^{\frac{n+1}{2}} nq^2\right) = 1 \qquad (\text{т.е. } p \| (\mathbf{l}^2 + (-1)^{\frac{n+1}{2}} nq^2)) \qquad (6)$$

Далее, пусть $l = \frac{\mathbf{l}}{q} \in Q$ и $t = \frac{nt_0}{n + (-1)^{(n+1)/2} l^2}$, где t_0 определено равенством:

$$t_0 = (-1)^n \cdot \frac{m^m (n-m)^{n-m}}{n^n}. \qquad (7)$$

Тогда трином $F_t(X) = X^n + t^r X^m + t^s \in Q[X]$ сепарабелен и его группа Галуа над Q изоморфна знакопеременной группе A_n [3].

Пример 6. Положим $n = 25$ и $m = 17$. Тогда $p = 3,\ q = 7,\ r = 7,\ s = 22$, $\mathbf{l} = 40$, $t = \frac{17^{17} \cdot 8^8 \cdot 7^2}{3 \cdot 25^{27}}$. Получаем трином вида:

$$F_t[X] = X^{25} + \left[\frac{17^{17} \cdot 8^8 \cdot 7^2}{3 \cdot 25^{27}}\right]^7 X^{17} + \left[\frac{17^{17} \cdot 8^8 \cdot 7^2}{3 \cdot 25^{27}}\right]^{22} \in Q[X].$$

По теореме 3, $Gal_Q(F_t(X)) \cong A_{25}$.

Теорема 4 [3]. Пусть $n \geq 7$ простое число и m – нечетное такое, что $3 \leq m \leq n-4$. Пусть далее q – простое, не делящее $mn(n-m)$, $\mathbf{l}$ –

рациональное целое число взаимно-простое с nq, k – рациональное целое число взаимно-простое с m, и n – целое число такое, что $0 \le n < \frac{n-1}{2}$. Тогда $l = \frac{\mathbf{l}}{n^{\nu} q^{k}} \in Q$, и $t = \frac{nt_0}{n + (-1)^{(n+1)/2} l^2}$, где где t_0 определено равенством:

$$t_0 = (-1)^n \cdot \frac{m^m (n-m)^{n-m}}{n^n} \qquad (8)$$

Тогда трином $F_t(X) = X^n + t^r X^m + t^s \in Q[X]$ (где r и s, удовлетворяют условию (5) сепарабелен и его группа Галуа над Q изоморфна альтернативной группе A_n.

Пример 7. Положим $n = 17$ и $m = 13.$ Тогда $q = 5,\ \mathbf{l} = 3,\ k = 1,\ n = 0,\ r = 3,$ $s = 13,\ t = -\frac{13^{12} \cdot 2^3 \cdot 5^2}{17^{16}}$. Получаем трином вида

$$F_t[X] = X^{17} + \left[-\frac{13^{12} \cdot 2^3 \cdot 5^2}{17^{16}} \right]^3 X^{13} + \left[-\frac{13^{12} \cdot 2^3 \cdot 5^2}{17^{16}} \right]^{13} \in Q[X].$$

По теореме 4, $Gal_Q(F_t(X)) \cong A_{17}$.

Теорема 5 [3]. Пусть $n \ge 8$ и m взаимно-простое число с n, причем m – четное и такое, что $3 \le m \le n-3$. Также, пусть q – простое не делящее $mn(n-m)$, которое расщепляется в поле $Q\left(\sqrt{(-1)^{(n+2)/2} m(n-m)}\right)$, если $m(n-m)$ – не квадрат натурального числа, и p – другое простое число не делящее $qnm(n-m)$. Тогда существуют целые числа r и s, удовлетворяющие условию (5) и натуральное число $\mathbf{l}$ взаимно-простое с p такое, что:

$$u_q\left(m(n-m)p^2 + (-1)^{\frac{n}{2}} \mathbf{l}^2 \right) = 1 \quad \text{(т.е. } q \mid (m(n-m)p^2 + (-1)^{\frac{n}{2}} \mathbf{l}^2)\text{).} \qquad (9)$$

Далее, пусть $l = \frac{m^{(m-1)/2} (n-m)^{(n-m-1)/2}}{n^{\frac{n}{2}}} \cdot \frac{\mathbf{l}}{p} \in Q$ и $t = t_0 + (-1)^{\frac{n}{2}} l^2$, где t_0 определено равенством $t_0 = (-1)^n \cdot \frac{m^m (n-m)^{n-m}}{n^n}$.

Тогда трином $F_t(X) = X^n + t^r X^m + t^s \in Q[X]$ сепарабелен и его группа Галуа над Q изоморфна альтернативной группе A_n.

Пример 8. Пусть $n = 12$, $m = 7$. Тогда имеем: $p = 17$, $q = 11$, $r = 2$, $s = 5$, $t = \frac{7^7 \cdot 5^4 \cdot 11^2}{12^{11} \cdot 17^2}$. Получаем трином вида:

$$F_t[X] = X^{12} + \left[\frac{7^7 \cdot 5^4 \cdot 11^2}{12^{11} \cdot 17^2}\right]^2 X^7 + \left[\frac{7^7 \cdot 5^4 \cdot 11^2}{12^{11} \cdot 17^2}\right]^5 \in Q[X].$$

По теореме 5, $Gal_Q(F_t(X)) \cong A_{12}$.

Используя эти теоремы можно построить бесконечно много триномов вида $F_t(X) = X^n + t^r X^m + t^s$ для $n \geq 7$, группа Галуа которых будет изоморфна альтернативной группе A_n.

Список используемой литературы

1. Kappe L., Warren B. An elementary test for the Galois group of a quartic polynomial // Amer. Math. Monthly. – 1989. – vol. 4. – p. 133-137.

2. Постников, М.М. Теория Галуа. М.: Факториал, 2003.

3. Alain H. and Salinier S. Rational Trinomials with the Alternating Group as Galois Group, // Number Theory, 90 (2001), 113-129.