УДК 519.115.1

01.00.00 Физико-математические науки

РЕАЛИЗАЦИЯ ГРУПП ГАЛУА ТРИНОМАМИ НАД ПОЛЕМ РАЦИОНАЛЬНЫХ ЧИСЕЛ Q

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

Соколова Ирина Владимировна
к. п. н., доцент
Кубанский государственный аграрный университет, Краснодар, Россия

Известно, что не каждая конечная группа может быть реализована над полем рациональных чисел как группа Галуа некоторого бинома. В связи с этим возникает более общий вопрос: пусть дана конечная транзитивная подгруппа G симметрической группы S на n символах; можно ли эту группу G реализовать как группу Галуа некоторого тринома степени n над полем рациональных чисел? В рассматриваемой статье доказано, что всякую транзитивную подгруппу группы S можно реализовать в виде группы Галуа некоторого конкретного неприводимого над полем рациональных чисел тринома степени n для значений n = 2, 3, 4. Для значений n = 5, 6 приводятся примеры, реализующие конкретные группы Галуа. В случае n = 7 реализуются все транзитивные подгруппы группы S, кроме возможно одной группы изоморфной диэдральной группы D. Дальнейшие вычисления будут направлены на реализацию конкретных групп Галуа для n = 8, 9…, однако количество транзитивных подгрупп группы S при n = 8, 9… очень быстро растёт, поэтому чем больше значение n, тем сложнее реализовать не то что все, а конкретную подгруппу группы S в виде тринома над Q

Ключевые слова: ТРИНОМ, ГРУППА ГАЛУА, ПОДГРУППЫ ГРУППЫ ГАЛУА

UDC 519.115.1

Physical-Mathematical sciences

THE REALIZATION OF GALOIS GROUPS BY TRINOMIALS OVER THE FIELD OF RATIONAL NUMBERS Q

Sergeev Alexandr Eduardovich
Cand. Phys.-Math. Sci., associate Professor

Sokolova Irina Vladimirovna
Cand. Ped. Sci., associate Professor
Kuban State Agrarian University, Krasnodar, Russia

It is known that not every finite group can be realized over the field of rational numbers as a Galois group of some binomial. In this connection, a more general question arises: suppose that there is given a finite transitive subgroup G of the symmetric group S on n symbols; Can this group G be realized as a Galois group of some trinomial of degree n over the field of rational numbers? In this paper we prove that every transitive subgroup of the group S can be realized in the form of the Galois group of a certain trinomial of the degree n, for the values n = 2, 3, 4. For n = 5 , 6 we give examples that realize concrete Galois groups. In the case n = 7, all the transitive subgroups of the group S are realized, except possibly one group of the isomorphic dihedral group D. Further calculations will be directed to the realization of specific Galois groups for n = 8, 9 ..., however, the number of transitive subgroups of the group S for n = 8, 9 ... grows very fast, so the larger the value of n, the more difficult it is to realize not just everything but the specific subgroup of the group S in the form of a trinomial over Q

Keywords: TRINOMIAL, GALOIS GROUPS, SUBGROUPS OF GALOIS GROUPS

Doi: 10.21515/1990-4665-131-124

Реализация групп Галуа триномами над полем рациональных чисел Q

Сейчас, по крайней мере, на данный момент, реализованы все группы Галуа подгруппы S_n для $3 \leq n \leq 15$, но неизвестно, какие группы из них реализуются в виде триномов.

Целью данной работы является сравнительно полный ответ на вышеназванный вопрос для $3 \leq n \leq 7$.

1) n=3

Для этого случая имеется ровно 2 вида триномов, это: x^3+ax+b и x^3+ax^2+b. Как известно, единственными транзитивными подгруппами группы S_3 является сама S_3 и альтернативная группа A_3. Они легко реализуются как группа Галуа триномов. Например, для реализации группы A_3 надо "лишь" решить диофантовы уравнения:

$$-4a^3 -27b^2 = u^2 \text{ для триномов вида } x^3 + ax + b, \tag{1}$$

$$-4a^3b -27b^3 = u^2 \text{ для триномов вида } x^3 + ax^2 + b. \tag{2}$$

Эти уравнения выражают не что иное, как то, что для реализации группы A_3 надо, чтобы выполнялось условие равенства дискриминанта квадрату натурального числа. Решением уравнения (1) является:

$$a = -3(c^2+3b^2),\ b = 2c(c^2+3b^2).$$

Отсюда, задавая целые значения для c и b получим, целые b и a. Например, если $c = 1$, $b = 1$, то $b = 8$, $a = -12$, т.е. таким образом можно получить бесконечно много примеров - триномов с группой Галуа A_3 и естественно с S_3 (ее реализовать еще проще):

$\boldsymbol{Gal(x^3 - 12x + 8) \cong A_3}$

$\boldsymbol{Gal(x^3 + x + 1) \cong S_3}$**.**

Но все-таки этот случай не так интересен, ввиду малого количества транзитивных подгрупп группы S_3.

Поэтому перейдем к следующему случаю:

2) n = 4

Для этого случая имеются ровно 5 транзитивных подгрупп группы S_4: это самая симметрическая группа 24-го порядка S_4, альтернативная группа

12-го порядка A_4, диэдральная группа 8-го порядка D_4, четвертая группа Клейна V_4 и циклическая группа 4-го порядка C_4. Все они, как впоследствии мы увидим, так же легко реализуются, как группы Галуа некоторых триномов. Для этого случая имеются 3 вида триномов: $x^4 + ax + b$, $x^4 + ax^2 + b$ и $x^4 + ax^3 + b$. Мы остановимся лишь на первых двух (так как третий вид тринома легко сводится к первому).

1) $x^4 + ax^2 + b$

Как известно, для этого вида тринома имеет место теорема [1]:

Теорема 1. *Если* $f = x^4 + ax^2 + b$ – *неприводимый полином кольца* Q[x], charF≠2, *тогда:*

i) *если* $\sqrt{b} \in Q$, *то* $Gal(f) \cong V_4$;

ii) *если* $\sqrt{b} \notin Q$ *и* $\sqrt{b(a^2-4b)} \in Q$, *то* $Gal(f) \cong C_4$;

iii) *если* $\sqrt{b} \notin Q$ *и* $\sqrt{b(a^2-4b)} \notin Q$, *то* $Gal(f) \cong D_4$,

Доказательство:

Пусть $m=[Q(\alpha,\beta,\gamma):Q]$. Т.к. $f(x) = x^4 + ax^2 + b$, то кубическая резольвента r(f) имеет вид: $r(f) = x^3 - ax^2 - 4bx + 4ab = (x - a)(x^2 - 4b) = (x - a)(x - 2\sqrt{b})(x + 2\sqrt{b})$, следовательно, по известному критерию (см. [1]) для того чтобы $Gal(f) \cong V_4$ необходимо и достаточно, чтобы степень m была бы равна единице, т.е. чтобы $[Q(\alpha,\beta,\gamma):Q] = 1$. В данном случае мы получаем, что: $m=[Q(\alpha,\beta,\gamma):Q] = [Q(a, 2\sqrt{b}, - 2\sqrt{b}):Q] = 1 \Leftrightarrow \sqrt{b} \in Q$, т.е. пункт i) доказан.

Далее, если $\sqrt{b} \notin Q$, то тогда получаем: $[Q(a, 2\sqrt{b}, - 2\sqrt{b}):Q] = [Q(a, \sqrt{b}):Q] = 2$, и, очевидно, что f(x) имеет вид $f(x)= x^4 + ax^2 + b = \left(x^2 - \frac{\sqrt{a^2-4b}-a}{2}\right)\left(x^2 - \frac{a+\sqrt{a^2-4b}}{2}\right)$, следовательно, для того чтобы f(x) был приводим над $[Q(a, 2\sqrt{b}, - 2\sqrt{b}):Q] = Q[\sqrt{b}]$ (а именно это условие является условием необходимым и достаточным для того, чтобы $Gal(f) \cong C_4$, см. [1]), необходимо и достаточно, чтобы $\sqrt{b(a^2-4b)} \in$ Q. Если же $\sqrt{b(a^2-4b)} \notin$ Q, то тогда f(x) будет неприводимым в Q[$\sqrt{b}$], а это уже в свою очередь является необходимым и достаточным условием для того, чтобы $Gal(f) \cong D_4$ (опять же из [1]). Таким образом, пункты ii) и iii) доказаны, т.е. теорема доказана полностью.

Приведем на эту теорему определенные примеры:

Пример 1.1. Пусть $f(x) = x^4 + 2x^2 + 16$.
По теореме 1 элемент $\sqrt{b} = \sqrt{16} \in$ Q, следовательно $\boldsymbol{Gal(f) \cong V_4}$.

Пример 1.2. Пусть $f(x) = x^4 - 4x^2 + 2$.
По теореме 1 элемент $\sqrt{b} = \sqrt{2} \notin$ Q, а $\sqrt{b(a^2-4b)} = \sqrt{16} \in$ Q, т.е. тогда получаем, что $\boldsymbol{Gal(f) \cong C_4}$.

Пример 1.3. Пусть $f(x) = x^4 - 3x^2 + 2$.
По теореме 1 элемент $\sqrt{b} = \sqrt{2} \notin$ Q, $\sqrt{b(a^2-4b)} = \sqrt{2} \notin$ Q, т.е. получаем, что $\boldsymbol{Gal(f) \cong D_4}$.

Таким образом, в случае, когда $f(x) = x^4 + ax^2 + b$, могут реализоваться только 3 транзитные подгруппы группы S_3, а именно: диэдральная группа 8-го порядка D_4, четвертая группа Клейна V_4 и циклическая группа 4-го порядка C_4.

2) $\boldsymbol{x^4 + ax + b}$

Для этого вида тринома мы показываем, что можно реализовать оставшиеся две группы Галуа (S_4 и A_4). Реализуем вначале группу A_4 таким образом: т.е. необходимыми и достаточными условиями для того, чтобы группа Галуа была изоморфна A_4, являются 2 условия, а именно:

дискриминант полинома f(x) есть квадрат в поле Q и кубическая резольвента r(f) неприводима в Q[x].

Дискриминантом для полинома $f(x) = x^4 + ax + b$ является выражение: $D(f) = 4^4b^3 - 3^3a^4$. Сделаем так, чтобы он был квадратом в поле Q: пусть $a = 4c$, $b = 3c$ ($c \in Z$), тогда дискриминант D(f) примет вид: $D(f) = 4^4 3^3 c^3 - 3^3 4^4 c^4 = 4^4(3c)^3(1-c)$, пусть теперь $1 - c = 3ck^2$ ($k \in Z$), тогда $c = \frac{1}{3k^2+1}$, следовательно, $D(f) = 4^4 \frac{3^3}{(3k^2+1)^3} \cdot \frac{3k^2}{(3k^2+1)} = \frac{4^4 \cdot 3^4 \cdot k^2}{(3k^2+1)^4}$. Как видим, дискриминант D(f) в этом случае есть квадрат. Дадим теперь некоторые примеры:

Пример 2.1) $k = 1$, следовательно, $c = \frac{1}{4}$, $b = \frac{3}{4}$, $a = 1$, следовательно, после умножения полученного полинома на 2^4 получим полином вида: $f(x) = x^4 - 8x + 12$. Его дискриминант $D(f) = 3^4$ – квадрат, а резольвента, которая неприводима Q[x], имеет вид $r(f) = x^3 - 48x - 64$, поэтому получаем, что $Gal(f) \cong \mathbf{A_4}$.

Пример 2.2) $k = 2$, следовательно $c = \frac{1}{13}$, $b = \frac{3}{13}$, $a = \frac{4}{13}$, тогда, после умножения полученного полинома на 13^4, получим полином вида: $f(x) = x^4 + 676x - 6591$, его дискриминант $D(f) = 3^4$ – квадрат, а $r(f) = x^3 - 2636x - 456976$, поэтому получаем, что $Gal(f) \cong \mathbf{A_4}$.

Исходя из вышесказанного, можно выписать параметрическое семейство полиномов, имеющее в качестве группы Галуа группу A_4, а именно: $f(x) = x^4 + 4(3k^2 + 1)^2x + 3(3k^2 + 1)^3$.

Группу S_4 реализовать просто, т.к. особо сложных условий для её реализации нет (дискриминант полинома не является квадратом в Q и кубическая резольвента является неприводимой). В качестве таких примеров можно рассмотреть следующие:

Пример 2.3) $f(x) = x^4 + x + 1$.

Пример 2.4) $f(x) = x^4 + 2x + 2$.

Все они имеют в качестве группы Галуа группу S_4 (т.к. дискриминант полинома не является квадратом в Q и кубическая резольвента является неприводимой).

Таким образом, исходя из этого, мы получаем, что все 5 транзитных подгрупп группы S_4 (т.е. S_4, A4, D4, V_4, C_4) реализуются как группы Галуа некоторых триномов, т.е. с помощью триномов можно реализовать все транзитивные подгруппы группы S_4.

3) n = 5

Для этого случая имеется ровно 5 транзитивных подгрупп группы S_5: это сама симметрическая группа 120-го порядка S_5, альтернативная группа 60-го порядка A_5, диэдральная группа 16-го порядка D_5, фробениусная группа 20-го порядка F_{20} и циклическая группа 5-го порядка C_5.

Все они, как впоследствии мы увидим, так же легко реализуются, как группы Галуа некоторых триномов, за исключением, что очевидно, циклической группы C_5 (по известному критерию Эйлера о числе вещественных корней триномов вида $x^{m+n} + Ax^n + B$) [2].

Для этого случая имеются 2 вида триномов: $x^5 + ax^2 + b$ (т.к. трином $x^5 + ax^3 + b$ приводится к $x^5 + ax^2 + b$, а $x^5 + ax^4 + b$ к $x^5 + ax + b$).

1) x^5 + ax + b

С помощью этого вида тринома можно реализовать все транзитивные подгруппы группы S_5, кроме, конечно же, C_5.

Справедлива следующая теорема:

Теорема 2. *Пусть* $f = x^5 + ax + b$ – *неприводимый трином кольца* Q[x], charF≠2, *тогда* $Gal_Q(f) \cong D_5$ или F_{20} *тогда и только тогда, когда коэффициенты* a *и* b *можно представить в виде:*

$$a = \frac{3125\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)}, \quad b = \frac{3125\lambda\mu^5}{(\lambda-1)^4(\lambda^2-6\lambda+25)},$$

с $\lambda, \mu \in Q$ *и* $\lambda \neq 1, \mu \neq 0$. *Если при этом дискриминант тринома* $D(f) = 4^4a^5 + 5^5b^4$ *есть квадрат рационального числа, то тогда* $Gal_Q(f) \cong D_5$, *если же это не так, то тогда* $Gal_Q(f) \cong F_{20}$.

Доказательство:

Примеv без доказательства тот факт, что если многочлен $(y^3 - 5ay^2 + 15a^2y + 5a^3)^2 - Dy$ имеет кратный корень, то трином вида $f = x^5 + ax + b$ решается в радикалах (а группы D_5 и F_{20} как известно разрешимы) [3]. Пользуясь формулой $D(f) = 4^4a^5 + 5^5b^4$, имеем:

$$(y^3 - 5ay^2 + 15a^2y + 5a^3)^2 - Dy = (y-a)^4(y^2 - 6ay + 25a^2) - 5^5b^4. \quad (3)$$

Пусть полином (3) имеет корень $y_0 \in Q$. Полагая $a = \frac{y_0}{\lambda}$, $b = a\mu$, где λ, μ – некоторые параметры, мы получим, что

$$(a\lambda - a)^4(a^2\lambda^2 - 6a^2\lambda + 25a^2) - 5^5a^5\lambda\mu^4 = 0.$$

Из последнего уравнения и вытекает справедливость теоремы. Для того же чтобы выяснить, какая будет подгруппа, в случае если дискриминант данного тринома является квадратом, надо вспомнить, что $F_{20} \subset S_5$, а $D_5 \subset A_5$, и теорема доказана полностью.

Приведем некоторые примеры:

$\boldsymbol{Gal_Q(x^5 - 5x + 12) \cong D_5}$**,**

$\boldsymbol{Gal_Q(x^5 + 15x + 12) \cong F_{20}}$**,**

$\boldsymbol{Gal_Q(x^5 - 80x + 384) \cong D_5,}$

$\boldsymbol{Gal_Q(x^5 + 750x + 3750) \cong F_{20}}$

$\boldsymbol{Gal_Q(x^5 + 11x + 44) \cong D_5,}$

$\boldsymbol{Gal_Q(x^5 - 40x - 64) \cong F_{20}.}$

Стоит также упомянуть о приемах Ноама Элкиеса (Noam Elkies), который получил следующие триномы с помощью теории эллиптических кривых [4]. Вот они:

$$Gal_Q(4u^2 + 16)x^5 + (5u^2 - 5)x + (4u^2 + 10u + 6) \cong F_{20}$$

и если u = (t – 1)/t, то тогда получаем:

$$Gal_Q(2t^2 + 2)^2x^5 + 5(t^4 - 3t^2 + 1)x + (4t^4 + 10t^3 - 2t^2 - 10t + 4) \cong D_5.$$

В конструктивной теории Галуа Хенрих Матцат получил также некоторые другие триномы с разрешимыми группами Галуа [5]. Вот они:

$$Gal_Q(x^5 - 256\frac{z-1}{z^4(z^2+4z+)}(5x-4)) \cong F_{20}$$

и

$$Gal_Q(x^5 + \frac{4}{3125}\,\frac{(v^2-v-1)^5(v^2-11v-1)}{v^4(v^2+1)^2}(5x-4)) \cong D_5.$$

Для этого вида тринома можно, естественно, реализовать и симметрическую группу S_5. Конечно, существуют очень много примеров и различных критериев для ее реализации, но самый простой критерий дал Кенцо Комацу:

Теорема 3. *Пусть* a *– рациональное число, и пусть p – простое со следующим условиями:*

a) p = 3 или 5, или 7 (mob 8), p≠3

b) (p, a) = 1;

c) $f(x) = x^p + ax + a$ – неприводим над Q. *Тогда группа Галуа* $Gal_Q(x^5 + ax + a) \cong S_p$.

Доказательство этого можно найти в [6].

Из теоремы ясно, что наш случай p = 5 подходит под формулировку этой теоремы.

Примерами на эту теорему могут служить следующие:

$\boldsymbol{Gal_Q(x^5 + 3x + 3) \cong S_5}$,

$\boldsymbol{Gal_Q(x^5 + 101x + 101) \cong S_5}$,

$\boldsymbol{Gal_Q(x^5 + 89x + 89) \cong S_5}$,

2) $\boldsymbol{x^5 + ax^2 + b}$

Выведем в этом случае, подобно тому как это было сделано для степени 4, трином с группой Галуа A_5 (для этого дискриминант резольвента $f_{20}(x)$ (см. [7]) должна быть неприводима):

Попытаемся получить хотя бы частное решение диофантового уравнения $D = b(5^5b^3 + 3^3 2^2 a^5) = u^2$. Пусть $b = ma$, тогда это уравнение примет вид $(5^5m^2a^2)^2 5+(6a)^2 3a^2 m = u^2$, пусть $u = a^2u_1$, тогда мы имеем: $(5^5m^2)^2 5 + (6a)^2 3m = u_1^2$, пусть $3m = m_1^2 \Longrightarrow m = \frac{m_1^2}{3}$, пусть далее $m_1 = 3m_2 \Longrightarrow$ наше исходное уравнение примет следующий вид: $(5^2 3^2 m_2^4)^2 5 + (6a \cdot 9m_{2)}{}^2 = u_1^2 \Longrightarrow: \begin{cases} u_1 - 54am_2 = 5^2 3^2 m_2^4 \\ u_1 + 54am_2 = 5^2 3^2 m_2^4 \end{cases}$, вычтя из второго уравнения системы первое, получим: $108am_2 = 5^2 3^2 4m_2^4$, откуда найдем a (предварительно сделав получим замену $m_2 = 3m_3$): $a = 5^2 3^2 m_3^3$, далее находим $b = 3^5 5^2 m_3^5$. Следовательно, т.к. у полученного тринома дискриминант квадрат $(3^9 5^6 7 m_3^{10})^2$, а соответствующая ему резольвента $f_{20}(x)$ неприводима, то тогда имеем:

$$Gal_Q(x^5 + 5^2 3^2 t^3 x^2 + 3^5 5^2 t^5) \cong A_5.$$

Приведем некоторые примеры:

$$\boldsymbol{Gal_Q(x^5 + 225x^2 + 6075) \cong A_5,}$$

$$\boldsymbol{Gal_Q(x^5 + 14400x^2 + 6220800) \cong A_5,}$$

$$\boldsymbol{Gal_Q(x^5 + 494325x^2 + 2255604975) \cong A_5.}$$

Существуют также для этого вида тринома примеры и с разрешимыми группами Галуа. Однако, в отличие от предыдущего вида тринома, где были получены условия на коэффициенты, при которых в зависимости от дискриминанта реализовывались группы D_5 и F_{20}, в этом случае таких триномов (с разрешимыми группами Галуа) существуют всего 5 [7]. Вот они:

$$\boldsymbol{Gal_Q(x^5 + 5x^2 + 3) \cong D_5,}$$

$$\boldsymbol{Gal_Q(x^5 + 5x^2 - 15) \cong D_5,}$$

$$\boldsymbol{Gal_Q(x^5 + 25x^2 + 300) \cong D_5,}$$

$$\boldsymbol{Gal_Q(x^5 + 250x^2 + 625) \cong F_{20},}$$

$$\boldsymbol{Gal_Q(x^5 + 100x^2 + 1000) \cong F_{20},}$$

Для этого вида тринома можно также, что очевидно, реализовать симметрическую группу S_5.

Таким образом, мы получили, что для случая n = 5 с помощью триномов можно реализовать все транзитивные группы, кроме циклической.

4) n = 6

Для этого случая имеются ровно 16 транзитивных подгрупп группы S_6, это: сама симметрическая группа 720-го порядка S_6, альтернативная группа 120-го порядка A_6, еще одна группа 120-го порядка PGL(2,5) (простая), разрешимая группа 48-порядка G_{48}, две разрешимые группы 36-го порядка G_{36}^1 и G_{36}^2 ($G_{36}^2 \cong C_3^2 \times C_2^2$, а $G_{36}^1 \cong C_3^2 \times C_4$), три разрешимые группы 24-го порядка G_{24}, S_4/V_4 и S_4/C_4, разрешимая группа 18 порядка G_{18}, две разрешимых групп 12 порядка D_6 (диэдральная группа) и альтернативная группа A_4 и две разрешимых групп 6-го порядка S_3 и C_6.

Покажем, что из этого списка можно реализовать все группы как группы Галуа некоторых триномов, за исключением возможно, G_{36}^1 .

Для этого случая (степени 6) рассмотрим 4 вида триномов:
$x^6 + ax + b, x^6 + ax^3 + b, x^6 + ax^4 + b, x^6 + ax^5 + b.$

4.1) $x^6 + ax + b$

Дискриминант этого тринома имеет вид: $5^5a^6 - 6^6b^5$. Опять, как и в случаях для степеней четыре и пять, если мы попытаемся, как там, найти хотя бы частное решение диофатового уравнения $5^5a^6 - 6^6b^5 = u^2$, то мы получим трином вида: $f(x) = x^6 + \frac{6}{1-5a^2}x + \frac{5}{1-5a^2}$, у которого дискриминант является квадратом, а непосредственные вычисления на MAPLE показывают, что:

$$Gal_Q\left(x^6 + \frac{6}{1-5a^2}x + \frac{5}{1-5a^2}\right) \cong A_6.$$

Ясно, что для этого вида тринома можно также легко реализовать и саму симметрическую группу S_6, например:

$$Gal_Q(x^6 + x + a) \cong S_6.$$

Замечание 2. Триномы нечетной степени (больше 3) этого вида не могут иметь в качестве группы Галуа группу C_n ($n > 3$), так как у этих триномов обязательно имеется либо один, либо три вещественных корня (всех пяти корней не вещественных, ни мнимых мы не получим), однако для четных степеней и для этого вида тринома ($x^{2n} + ax + b$) это возможно, ввиду того, что эти триномы могут иметь все шесть корней мнимых и какие-то пять из них выражаются через один). Примером такого вида тринома может служить пример Малле: $X^6 + 6 \cdot 2^3 \cdot 31^4 X - 2^4 35^5$ (в этот трином переводится трином $X^6 - 6X^5 + 2^6 3^6 11^5 7^{-6} 19^{-1}$).

Замечание 3. Используя преобразование триномов вида $X^6 - 6aX^5 - b$ в трином вида $X^6 + aX + b$, легко реализовать все транзитивные подгруппы группы S_n, кроме G^1_{36} (см. ниже).

4.2) $x^6 + ax^3 + b$

Для этого вида тринома имеет место теорема:

Теорема 4. *Пусть* $f(x) = x^6 + ax^3 + b$ - *неприводимый трином степени шесть в* $Q[x]$. *Тогда группами Галуа для этого вида тринома могут быть лишь следующие:* G^2_{36}, G_{18}, D_6 и C_6.

Доказательство. Ясно, что $f(x) = x^6 + ax^3 + b = (x^3 - \alpha)(x^3 - \beta) =$
$= (x - \sqrt[3]{\alpha})(x - \varepsilon\sqrt[3]{\alpha})(x - \varepsilon^2\sqrt[3]{\alpha})(x - \sqrt[3]{\beta})(x - \varepsilon\sqrt[3]{\beta})(x - \varepsilon^2\sqrt[3]{\beta})$, причем $\varepsilon = \frac{-1-i\sqrt{3}}{2}$. Тогда после расщепления будет: $E = Q(\sqrt[3]{\alpha}, \sqrt[3]{\beta}, \sqrt{3})$, и, следовательно, имеет следующие возможности:

$$Q \overset{2}{\subset} Q(a) \overset{3}{\subset} Q\left(\sqrt[3]{\alpha}\right)^{3} \overset{3}{\subset} Q\left(\sqrt[3]{\alpha}, \sqrt[3]{\beta}\right) \overset{2}{\subset} Q(\sqrt[3]{\alpha}, \sqrt[3]{\beta}, \sqrt{-3}),$$

(4)

причем α **— корень уравнения** $y^2 + ay + b = (y - \alpha)(y - \beta)$ **(здесь** $y = x^3$**)**

, следовательно, максимальный порядок у группы Галуа может быть 36, т.е. $\mathbf{Gal_Q(f)} \cong \boldsymbol{G^2_{36}}$, что непосредственно видно из башни полей (4). Если αβ = b = c^3, то очевидно, что, $\sqrt[3]{\alpha} \cdot \sqrt[3]{\beta} = c = Q$, следовательно, в этом где случае $\sqrt[3]{\alpha}$ выражается через $\sqrt[3]{\beta}$ $\left(\sqrt[3]{\alpha} = \frac{c}{\sqrt[3]{\beta}}\right)$, поэтому башня полей примет вид (5):

$$Q \overset{2}{\subset} Q(a) \overset{3}{\subset} Q\left(\sqrt[3]{a}\right)^{2} \overset{2}{\subset} Q(\sqrt[3]{a}, \sqrt{-3}), \qquad (5)$$

и как видно из (5), порядок группы Галуа в этом случае равен 12, т.е. $\mathbf{Gal_Q(f)} \cong \boldsymbol{D_6}$. (Легко понять, что в этом случае только одна из двух транзитивных по подгрупп 12 порядка, а именно D_6, а не A_4 может реализоваться в виде тринома, так как дискриминант этого тринома не может быть квадратом некоторого рационального числа). Трином f будет при этом иметь вид: $\mathbf{x^6 + ax^3 + c^3}$**.** Если $\sqrt{-3}$ выражается через α и β, $\sqrt[3]{a}$ не выражается через $\sqrt[3]{\beta}$, то тогда башня полей примет вид (6):

$$Q \overset{2}{\subset} Q(a) \overset{3}{\subset} Q\left(\sqrt[3]{a}\right)^{2} \overset{3}{\subset} Q(\sqrt[3]{a}, \sqrt[3]{\beta}), \qquad (6)$$

причем αβ = b $\notin Q^3$. Это возможно, если расширение Q(α)/Q будет единственным расширением поля Q степени два, т.е. если $Q\left(\sqrt{D}\right) = Q(\varepsilon) == Q(\sqrt{-3}),$ т.е. $D = t_1^2(-3),$ (где D – дискриминант полинома $x^2 + ax + b$), следовательно, $a^2 - 4b = t_1^2(-3)$, т.е. $3t_1^2 + a^2 = 4b$. Если a = $3t_1$ и, следовательно, получен трином 18, что видно из башни полей (6)). Если β выражается через α, $\sqrt{-3}$ выражается через $\sqrt[3]{\alpha}$ и $\sqrt[3]{\beta}$, то тогда башня примет вид (7):

$$Q \overset{2}{\subset} Q(a) \overset{3}{\subset} Q(\sqrt[3]{a}). \tag{7}$$

Для того чтобы получить полином параметрический с группой Галуа C_6 в равенстве $a^2 - 4b = t_1^2(-3)$ будем считать, что $t_1 = 2t$, тогда $a^2 - 4b = t^2(-12)$ или $12t^2 + a^2 = 4b$. Если $a = 2a_1$, а $a_1 = tu$, то тогда $3t^2 + a_1^2 = b = c^3 = t^2(3 + u^2)$, следовательно, $t = 3 + u^2$, поэтому $a_1 = (3 + u^2)u$, а $b = t^3 + a_1^2 = 3(3 + u^2)^2 +$ $+ (3 + u^2)u^2 = (3 + u^2)^3$, т.е. мы построили трином $\mathbf{f(x) = x^6 + 2(3 + u^2)ux +}$ $\mathbf{+ (3 + u^2)^3}$ с $\mathbf{Gal_Q(f) \cong C_6}$ (порядок группы Галуа равен 6, что видно из башни полей (4)).

Таким образом, теорема доказана полностью.

Естественно, используя теорему 4, можно привести некоторые примеры:

$\mathbf{Gal_Q(x^6 + 4x^3 + 19) \cong G_{36}^2}$,

$\mathbf{Gal_Q(x^6 + 4x^3 + 16) \cong G_{18}}$,

$\mathbf{Gal_Q(x^6 + 12x^3 + 39) \cong G_{18}}$,

$\mathbf{Gal_Q(x^6 + 11x^3 + 64) \cong D_6}$,

$\mathbf{Gal_Q(x^6 + 8x^3 + 64) \cong C_6}$,

$\mathbf{Gal_Q(x^6 + 28x^3 + 343) \cong C_6}$.

Так как группа $G_{36}^2 \cong (C_2 \times C_2) \setminus (C_3 \times C_3)$ содержит две различные подгруппы индекса два, а группа $G_{36}^1 \cong (C_3 \times C_3) \setminus C_4$ только одну, то исходя из башни полей (4), заключаем, что из этих двух групп реализуется в виде тринома (в частности, тринома $\mathbf{x^6 + mx^3 + n}$) только одна - G_{36}^2.

4.3) $\mathbf{x^6 + ax^4 + b}$

Для этого тринома имеет место теорема:

<u>Теорема 5.</u> *Пусть* f(x) = $x^6 + ax^4 + b$ – *неприводимый трином степени шесть в* Q[x]. *Тогда группами Галуа для этого вида тринома могут быть лишь следующие:* G_{48}, $G_{24}^1 \cong 2A_4$, $G_{24}^2 \cong S_4 / C_4$, D_6 *и* A_4.

Доказательство. Пусть $x^2 = t$, следовательно, $f(t) = t^3 + at^2 + b$. Пусть далее β_1, β_2, β_3 – корни f(t), тогда $\pm\sqrt{\beta_1}$, $\pm\sqrt{\beta_2}$, $\pm\sqrt{\beta_3}$ – корни f(x), причем $\beta_1, \beta_2, \beta_3 = -b$, и если β_1, β_2 известны, то $\beta_3 = \frac{-b}{\beta_1\beta_2} \in Q$, поэтому имеем возможности:

$$Q \overset{6}{\subset} Q\left(\sqrt{\beta_1}\right) \overset{4}{\subset} Q\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right) \overset{2}{\subset} Q\left(\sqrt{\beta_1}, \sqrt{\beta_2}\,\sqrt{-b}\right), \qquad (8)$$

т.е. это будет, если, как уже сказано, $\sqrt{\beta_3} = \frac{\sqrt{-b}}{\sqrt{\beta_1\,\beta_2}} \in Q$, у кубического полинома f(t) не все корни выражаются через один и дискриминант $D(f(x)) \neq a^2$. В этом случае, так как это максимально возможная степень расширения, группа Галуа $\mathbf{Gal_Q(f) = G_{48}}$ (степень расширения равна 48, что видно из башни полей (8)).

$$Q \overset{6}{\subset} Q\left(\sqrt{\beta_1}\right) \overset{4}{\subset} Q\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right), \qquad (9)$$

т.е. это будет, если, как уже сказано, $\sqrt{\beta_3} = \frac{\sqrt{-b}}{\sqrt{\beta_1\,\beta_2}} \in Q$, у кубического полинома f(t) не все корни выражаются через один, $\sqrt{-b}$ в свою очередь, выражается через $\sqrt{\beta_1}$, и $\sqrt{\beta_2}$, и дискриминант $D(f(x)) \neq a^2$, т.е.группа Галуа $\mathbf{Gal_Q(f) \cong S_4 / C_4}$ (так как степень расширения равна 24, что видно из башни полей (9)).

$$Q \overset{6}{\subset} Q\left(\sqrt{\beta_1}\right) \overset{2}{\subset} Q\left(\sqrt{\beta_1}, \sqrt{\beta_2}\right) \overset{2}{\subset} Q\left(\sqrt{\beta_1}, \sqrt{\beta_2}, \sqrt{-b}\right), \qquad (10)$$

т.е. это будет, если $\sqrt{\beta}_3 = \frac{\sqrt{-b}}{\sqrt{\beta_1\beta_2}} \in Q$, у кубического полинома f(t) все корни выражаются через один и дискриминант тринома $D(f(x)) \neq \alpha^2$, т.е.

группа Галуа $\mathbf{Gal_Q(f)} \cong \mathbf{S_4/V_4}$ (так как степень расширения равна 24, что видно из башни полей (10)), и это единственная транзитивная подгруппа 24-го порядка, которая содержится в A_6.

$$Q \overset{6}{\subset} Q\left(\sqrt{\beta_1}\right) \overset{2}{\subset} Q\left(\sqrt{\beta_1}, \sqrt{-b}\right) \overset{2}{\subset} Q\left(\sqrt{\beta_1}, \sqrt{\beta_2}, \sqrt{-b}\right), \tag{11}$$

т.е. это будет, если $\sqrt{\beta}_3 = \frac{\sqrt{-b}}{\sqrt{\beta_1\beta_2}} \in Q$, у кубического полинома f(t) все корни выражаются через один и дискриминант тринома $D(f(x)) \neq \alpha^2$ т.е. группа Галуа $\mathbf{Gal_Q(f)} \cong \boldsymbol{G_{24}^1} \cong \boldsymbol{2A_4}$ (так как степень расширения равна 24, что видно из башни полей (11)).

$$Q \overset{6}{\subset} Q\left(\sqrt{\beta_1}\right) \overset{2}{\subset} Q\left(\sqrt{\beta_1}, \sqrt{-b}\right), \tag{12}$$

т.е. этот случай возможен, если $\sqrt{\beta}_3 = \frac{\sqrt{-b}}{\sqrt{\beta_1\beta_2}} \in Q$ у кубического полинома f(t) все корни выражаются через один и $\sqrt{-b}$ в свою очередь, выражается через $\sqrt{\beta_1}$ и $\sqrt{\beta_2}$, и дискриминант $D(f(x)) \neq \alpha^2$, т.е. группа Галуа $\mathbf{Gal_Q(f)} \cong \boldsymbol{A_4}$ (так как степень расширения равна 12, что видно из башни полей (12)).

$$Q \overset{6}{\subset} Q\left(\sqrt{\beta_1}\right) \overset{2}{\subset} Q\left(\sqrt{\beta_1}\, \sqrt{\beta_2}\,\right), \tag{13}$$

т.е. этот случай возможен, если $\sqrt{\beta}_3 = \frac{\sqrt{-b}}{\sqrt{\beta_1\beta_2}} \in Q$, у кубического полинома f(t) все корни выражаются через один и $\sqrt{-b}$ в свою очередь, выражается через $\sqrt{\beta_1}$ и $\sqrt{\beta_2}$, и дискриминант $D(f(x)) \neq \alpha^2$, т.е. группа Галуа $\mathbf{Gal_Q(f)} \cong \boldsymbol{D_6}$ (так как степень расширения равна 12, что видно из башни полей (13)).

$$Q \overset{6}{\subset} Q\left(\sqrt{\beta_1}\right), \tag{14}$$

т.е. это возможно, если $\sqrt{\beta}_3 = \frac{\sqrt{-b}}{\sqrt{\beta_1\beta_2}} \in Q$, $\sqrt{-b}$ в свою очередь, выражается через $\sqrt{\beta_1}$ и $\sqrt{\beta_2}$, а $\sqrt{\beta_2}$ выражается через $\sqrt{\beta_1}$ т.е. $\mathbf{Gal_Q(f)} \cong C_6$ (так как степень расширения равна 6, что видно из башни полей (14)).

Случай (14), как показывает исследование вещественности корней этого вида тринома, невозможен [2].

Таким образом, теорема доказана полностью.

Естественно, используя теорему 5, можно привести некоторые конкретные примеры:

$\mathbf{Gal_Q(x^6 + 5x^4 + 14)} \cong G_{48}$

$\mathbf{Gal_Q(x^6 - 18x^4 - 2)} \cong G_{48}$

$\mathbf{Gal_Q(x^6 - 3x^4 + 1)} \cong G_{24}^1$

$\mathbf{Gal_Q(x^6 - 3x^4 + 3)} \cong G_{24}^1$

$\mathbf{Gal_Q(x^6 + x^4 + 23)} \cong S_4/C_4$

$\mathbf{Gal_Q(x^6 + 6x^4 + 16)} \cong S_4/C_4$

$\mathbf{Gal_Q(x^6 + 7x^4 - 23)} \cong S_4/V_4$

$\mathbf{Gal_Q(x^6 - 17x^4 - 1)} \cong S_4/V_4$

$\mathbf{Gal_Q(x^6 + 8x^4 + 1)} \cong D_6$

$\mathbf{Gal_Q(x^6 + 2x^4 - 2)} \cong D_6$

$\mathbf{Gal_Q(x^6 + 3x^4 - 1)} \cong A_4$

$\mathbf{Gal_Q(x^6 + 27x^4 - 729)} \cong A_4$

4.3) $x^6 + 6ax^5 + b$

Триномы вида $\mathbf{x^6 - 6ax^5 - b}$ впервые встречаются в работе немецкого математика J. Malle [9], в которой он с помощью этих триномов смог реализовать такие группы Галуа, как S_6, A_6, S_5, G_{72}, A_5, G_{48}, S_4, G_{36}, C_6 (заметим, что в работе Малле [9] $A_5 \cong PSL(2, 5)$, $S_5 \cong PGL(2, 5)$, $S_4 \cong S_4/C_4$).

Приведем пример тринома с группой Галуа PSL(2, 5), а также его дискриминант $f(x) = x^6 - 6x^5 -124$, $D(f) = 2^{14} \cdot 3^8 \cdot 19^2 \cdot 31^4$.

Этот же трином, как впоследствии мы увидим, получается и из параметрического примера Малле для этой группы Галуа и, по-видимому, это единственный пример тринома целыми коэффициентами и с группой Галуа PSL(2, 5).

С триномами шестой степени связана следующая теорема, принадлежащая Малле (J. Malle). Сформулируем эту теорему:

***Теорема 6* (Malle).**

(a) *Пусть N – поле расщепления над Q(w) тринома* $g_1(X,w) = X^6 - 6X^5 - \frac{w^5(w-120)}{64(w+8)^2(w+5)}$. *Тогда получаем:* $\mathbf{Gal_{Q(w)}(g_1(X, w)) \cong PGL(2, 5)}$ *для* $v \equiv 1 \ (mod209)$ $(w \in Z)$.

(b) *Пусть N – поле расщепления над Q(w) тринома вида* $g_1(X, v-5) \in Q[x]$. *Тогда получаем:* $\mathbf{Gal_{Q(w)}(g_1(X, v-5)) \cong PSL(2, 5)}$ *для числа* $v \equiv 1 \ (mod35)$ $(v \in Z$.

(c) *Пусть N – поле расщепления над Q(y) тринома* $g_1(X, y) = X^6 - 6X^5 + \frac{(y^2-14y+4)^5}{27(y-16)y^3}$. *Тогда получаем:* $\mathbf{Gal_{Q(y)}(g_2(X, y)) \cong G_{72}}$ *для* $y \equiv 1 \ (mod87)$ $(y \in Z)$.

(d) *Пусть N – поле расщепления над Q(z) тринома* $g_3(X, z) = X^6 - 6X^5 + \frac{4z^5(z^2-45)^5}{27(2z+15)^2(z-6)(z^2-2z-15)^3}$. *Тогда получаем:* $\mathbf{Gal_{Q(z)}(g_3(X, z)) \cong G_{48}}$ *для* $z \equiv 1 \ (mod247)$ $(z \in Z)$.

(e) *Пусть N – поле расщепления над Q(u) тринома вида* $g_3(X, \frac{3(5u^2-1)}{3u^2+1}) \in Q(u)[x]$. *Тогда получаем (взяв в качестве тринома*

$g_4(X, u) = g_3(X, \frac{3(5u^2-1)}{3u^2+1}) \in Q(u)[x])$, *что* $\mathbf{Gal_{Q(u)}(g_3(X, u)) \cong S_4/C_4}$ *для числа* $u \equiv 1(mod143)$ $(u \in Z)$.

Доказательство и более подробную информацию о конструкции этих триномов можно найти в [9].

Заметим, что тот трином, который был приведен выше, а именно $\mathbf{x^6 - 6x^5 - 124}$, получается и из формул Малле (взяв w = -4) и, возможно, это единственный трином с группой Галуа **PSL(2, 5)** и с целыми коэффициентами.

В [9] рассмотрены также следующие примеры:

$\mathbf{Gal_{Q(y)}(g_2(X, 2)) = Gal_{Q(y)}(X^6 - 6X^5 + 2^6 5^5 3^{-3} 7^{-1}) \cong G_{36}^2}$

$\mathbf{Gal_{Q(z)}(g_2(X, 10)) = Gal_{Q(z)}(X^6 - 6X^5 + 2^5 5^5 11^5 3^{-3} 7^{-2} 13^{-3}) \cong S_4/C_4}$

$\mathbf{Gal_{Q(y)}(g_2(X, -2/7)) = Gal_{Q(y)}(X^6 - 6X^5 + 2^6 5^6 11^5 7^{-6} 19^{-1}) \cong C_6}$

Таким образом, как нетрудно видеть, все транзитивные подгруппы группы S_6 реализованы, кроме, возможно, $G_{36}^1 \cong C_3^2/C_4$.

5) $x^7 + ax^z + b$ (n =7)

Для этого случая имеются ровно 7 транзитивных подгрупп группы S_7, а именно: сама симметрическая группа 5040-го порядка S_7, альтернативная группа 2520-го порядка A_7, простая группа 168-го порядка PSL(2, 7), разрешимая группа 42-го порядка F_{42}, разрешимая группа 21-го порядка F_{21}, диэдральная группа 14-го порядка D_7 и циклическая группа 7-го порядка C_7.

Для этого случая, т.е. для случая n = 7, не так много известно о триномах и какие группы из этого списка можн реализовать триномами, поэтому сначала выведем, как и во всех предыдущих случаях, параметрическое семейство триномов с группой Галуа A_7, а затем дадим некоторый обзор по триномам, включая проблему реализации данных групп Галуа.

5.1) $x^7 + ax + b$

Дискриминант этого вида тринома имеет вид $D(f) = -(7^7b^6+6^6a^7)$. Попытаемся найти хотя бы частное решение диофантова уравнения $-(7^7b^6+6^6a^7) = u^2$. Для этого сделаем предварительно замены: $a = -7c$, $b = 6c$, тогда дискриминант примет вид $D(f)= 6^67^7c^7 - 7^76^6c^6 = 6^67^7c^6\cdot(c-1)$. Теперь, сделав еще одну замену $c - 1 = 7k^2$, т.е. $c =7k^2 +1$, получаем, что дискриминант тринома D(f) становится квадратом, а именно: $D(f) = [6^37^4(7k^2 + 1)^3k]^2$, т.е. таким образом, построен трином вида $\mathbf{f(x) = x^7 - 7(7k^2+1)x + 6(7k^2 + 1)}$ ($k\neq0$) с $\mathbf{Gal_Q(f) \leq A_7}$. Но. Как показывают вычисления на MAPLE, получаем, что $\mathbf{Gal_Q(f) \cong A_7}$. Таким образом, построен трином вида $x^7 + ax + b$ с группой Галуа изоморфной группе A_7.

Можно привести конкретные примеры триномов данного выше вида с группой Галуа A_7.

$\mathbf{Gal_Q(x^7 - 56x + 48) \cong A_7}$

$\mathbf{Gal_Q(x^7 - 791x + 687) \cong A_7}$

$\mathbf{Gal_Q(x^7 - 4907x + 4206) \cong A_7}$

$\mathbf{Gal_Q(x^7 - 625688x + 536304) \cong A_7}$

$\mathbf{Gal_Q(x^7 - 6049261736x + 5185081488) \cong A_7}$

Для этого вида тринома можно, естественно, реализовать также симметрическую группу $\mathbf{S_7}$, используя теорему 3 настоящей работы:

$\mathbf{Gal_Q(x^7 +2x +2) \cong S_7}$

$\mathbf{Gal_Q(x^7 + 33x + 33) \cong S_7}$

$\mathbf{Gal_Q(x^7 + 100x + 100) \cong S_7}$

Ясно, что на эту группу (группу S_7) существует множество других примеров, не обязательно подходящих под теорему 3.

Для этого вида тринома можно реализовать также единственную транзитивную простую группу PSL (2, 7). Известно [10] параметрическая реализация этой группы Галуа, а в работе [11] указаны уже достаточные условия для её реализации, а именно:

1) данный полином неприводим над основным полем;
2) дискриминант полинома должен быть квадратом;
3) полином имеет ровно 3 вещественных корня;
4) резольвента P (x) 35-ой степени приводима.

Заметим, что эти условия являются достаточными, так как уже известно, что реализованы все транзитивные группы Галуа подгруппы S для $9 \geq n \geq 3$ со всеми вещественными корнями.

Приведём все известные нам триномы на данный момент с этой группой Галуа:

$$Gal_Q(x^7 + 7x + 3) = PSL(2,7),$$

$$Gal_Q(x^7 + 154x + 99) = PSL(2,7),$$

$$Gal_Q(x^7 + 448x + 384) = PSL(2,7),$$

Первый из этих триномов открыл Тринкс (Trinks, 1977) [12], второй из этих триномов впервые фигурирует в работе [11] в 1979 году, третий же трином получен автором в 1999 году.

Кроме этих 3-х транзитивных подгрупп группы S_7 (т.е. S_7, A_7, PSL(2, 7)), неизвестно, можно ли оставшиеся транзитивные группы Галуа (F_{42}, F_{21}, и D_7) реализовать в виде некоторых триномов. Конечно, ясно, что циклическую группу C_7 нельзя реализовать как группу Галуа в виде некоторого тринома, так как все 7 вещественных корней для триномов вида $x^7 + ax^k + b$ получить невозможно [2]).

Интересная ситуация возникла с группой D_n. До степени 7, как мы помним, и D_4, и D_5, и D_6 реализовывались (см. примеры выше) в виде некоторых триномов. Пока неизвестно, можно ли эту группу (группу D_7) реализовать в виде тринома 7-ой степени, и если вдруг такой трином существует, то до какой максимально возможной степени n можно реализовать группу D_n в качестве триномов? Ясно, однако, что группу D_7 можно реализовать в виде тринома 14-ой степени, однако нам это не интересно, и мы должны искать (или доказать, что её нет) реализацию этой группы виде тринома 7-ой степени. Известны лишь достаточные условия для того, чтобы трином степени 7 вида $x^7 + ax + b$ имел бы группу Галуа D_7 [13]:

1) Трином неприводим над основным полем;
2) Дискриминант данного тринома не является квадратом;
3) Полином
$$P_{21}(x) = x^{21} - 25ax^{15} - 57bx^{14} - 53a^2x^9 - 30abx^7 - 27a^3x^3 + 27a^2bx^2 - 9ab^2x + b$$
должен расщепляться в произведение 3-х неприводимых полиномов 7-ой степени каждый.

Ещё более запутано ситуация с группами F_{42} и F_{21}, хотя это и странно так как эти группы являются разрешимыми , и, по-видимому, должна существовать реализация их в виде триномов подобно тому, как существует реализация групп D_5 и F_{20} в виде триномов пятой степени. Мало того, что неизвестно, существует или нет реализации этих групп виде триномов 7-ой степени, так к тому же (в отличие от группы D_7) для этих групп не получены какие-нибудь простые необходимые или достаточные условия для их реализации. Не стоит забывать и про метод

Студухара [14], однако использовать его в данной ситуации нерационально и сложно.

Таким образом, для степени 7 мы в первые в работе столкнулись с довольно большими проблемами реализации виде триномов почти всех транзитивных подгрупп группы S_7, с которыми ранее мы в работе не сталкивались.

Интересно было бы получить ответы на эти вопросы.

Важным является вопрос о числе вещественных корней у триномов и какие группы Галуа будут получаться в зависимости от этого количества вещественных корней для степеней триномов ≥4.

Например, можно вывести условия, при которых трином вида x^4+ax^2+b имеет все вещественные корни, а именно: сделав замену $x^2=t$, получим трином вида t^2+at+b. Для того чтобы этот трином имел бы все существенные корни, надо, чтобы его дискриминант D(f) = $a^2-4b>0$ кроме того, надо, чтобы еще выполнялись два условия: a < 0 и -a > -a$\sqrt{a^2-4b}$. Приведём некоторые конкретные примеры триномов вида x^4+ax^2+b со всеми вещественными корнями и с их соответствующими группами Галуа:

$\boldsymbol{Gal_Q(x^4+4x^2+1)=V_4,}$

$\boldsymbol{Gal_Q(x^4+13x^2+16)=V_4,}$

$\boldsymbol{Gal_Q(x^4+8x^2+14)=D_4,}$

$\boldsymbol{Gal_Q(x^4+20x^2+30)=D_4,}$

$\boldsymbol{Gal_Q(x^4-4x^2+2)=C_4,}$

$\boldsymbol{Gal_Q(x^4-8x^2+8)=C_4,}$

Таким образом, для этого вида тринома у нас все группы Галуа можно реализовать со всеми вещественными корнями. Оставшиеся транзитивное подгруппы группы S_4, (а это S_4 и A_4), нельзя реализовать в виде триномов со всеми вещественными корнями, и вообще, справедлива теорема:

Теорема 7. *Только трином вида* $\boldsymbol{x^4 + ax^2 + b}$ *может давать все вещественные корни, поэтому, только такие транзитивное группы Галуа, как* $\boldsymbol{C_4}$, $\boldsymbol{D_4}$*,и* $\boldsymbol{V_4}$*, можно реализовать совсеми вещественными корнями.*

С вещественными корнями связана следующая теорема [11]:

Теорема 8. *Пусть p – простое число и f – неприводимый трином степени p кольца Q[X], имеющий точно p – 2 вещественных корня и два невещественных (мнимых) корня в поле Q. Тогда* $\boldsymbol{Gal_Q(f) \cong S_p}$*.*

Исходя из этой теоремы, получаем, что если неприводимый трином степени пять имеет три вещественных корня и два мнимых сопряженных, то тогда $\boldsymbol{Gal_Q(f) \cong S_5}$. Приведём примеры триномов 5-ой степени с тремя вещественными корнями и группой Галуа $\boldsymbol{S_5}$:

$$\boldsymbol{Gal_Q(x^5 - 4x + 2) \cong S_5}$$

$$\boldsymbol{Gal_Q(x^5 - 4x^2 + 2) \cong S_5}$$

$$\boldsymbol{Gal_Q(x^5 - 6x^2 + 3) \cong S_5}$$

Интересно было бы получить какие-нибудь похожие на теорему 7 условия, для которых неприводимые триномы 5-ой степени имели бы всего один вещественной корень и четыре мнимых, и что за группы Галуа могли бы при этих условиях получаться. Как показывают вычисления на MAPLE, если у триномов 5-ой степени один корень вещественный, то тогда можно реализовать конкретными примерами все транзитивное подгруппы группы $\boldsymbol{S_5}$ (кроме, естественно, $\boldsymbol{C_5}$):

$$\boldsymbol{Gal_Q(x^5 - 5x + 12) \cong D_5}$$

$$Gal_Q(x^5 - x + 12) \cong S_5$$

$$Gal_Q(x^5 - 15x + 12) \cong F_{20}$$

$$Gal_Q(x^5 + 20x + 16) \cong A_5$$

Интересно было бы дать для триномов шестой, седьмой и т.д. степеней условия, для которых существует 2, 4, 6, и т.д. вещественных корня и какие группы Галуа при этих условиях могут получаться.

Вообще, интересен вопрос о вещественности корней не триномов, а общих полиномов с различными группами Галуа. На данный момент известно, что все транзитивное подгруппы группы S_n, где $3 \le n \le 13$ реализуются как группы Галуа некоторых полиномов со всеми вещественными корнями!

В заключение работы, хотелось бы сформулировать некоторые теоремы о триномах [16], [17], [18]:

<u>Теорема 9. (Usada).</u> *Пусть полином f(x) =* $x^p - ax + b \in Z[x]$ *– неприводимый над Q трином простой степени p, и целые числа (p – 1)a и pb взаимно просты. Тогда* $Gal_Q(f) \cong S_p$.

<u>Теорема 10. (Osada).</u> *Пусть полином f(x) =* $x^n - ax^1 + b \in Z[x]$ *– неприводимый над Q трином и a =* a_0c^n*, и b =* $b_0^1c^n$*, где* a_0, b_0*, c - целые числа. Тогда, если числа* a_0c *(n–1)1 и n*b_0 *взаимно просты, то группа Галуа* $Gal_Q(f) \cong S_n$, если выполняются условия:

(1) Числа a_0c (n–s)s и nb_0 взаимно просты

(2) $|D_0(f)|$ не квадрат целого числа, где $D_0(f)$ – дискриминант f(x),

т.е. $D_0(f) = n^n b_0^{n-s}$+(-1)$^{n-1}s(n-s)^{n-s}a_0^n c^{ns}$,

(3) Существует такое простое число p, что p|b_0 и p|p^2.

Из этих результатов Осады (Osada [17]), вытекает, что трином $x^n - x - 1$ имеет над Q при любом n ≥ 2 группу Галуа, изоморфную симметрической группе S_n.

Теперь приведём интересную теорему, связанную с группами Галуа триномов простой степени. Она доказана Фейтом [18] с использованием классификации конечных простых групп:

Теорема 11. (Feit. 1979) . *Пусть p – простое число и* $1 \leq k \leq p - 1$. *Пусть* $f(x) = x^p - ax^k + b \in Z[x]$ *– неприводимый над Q трином, и G – группа Галуа тринома f над Q. Тогда может выполняться только одна из следующих возможностей:*

1) *G – разрешимая группа.*
2) $G \cong S_p$ *или* $G \cong A_p$
3) $P = 7$, $G \cong PSL_2(7) = G_{168}$
4) $P = 11$, $G \cong PSL_2(11)$ *или* $G \cong M_{11}$
5) $p = 1 + 2^n$ *– просто число Ферма большее 5 и тогда* $SL_2(2^n) \leq G \leq Aut(SL_2(2^n))$.

Для пунктов 4) и 5) теоремы 11 неизвестны конкретные триномы с соответствующими группами Галуа, на другие пункты теоремы 11 конкретные примеры можно найти в настоящей работе.

Как видно из настоящей работы, вопрос о реализации групп Галуа в виде триномов интересует многих современных математиков, но остается ещё множество нерешенных, интересных проблем, связанных с этим вопросом.

Автор в настоящей работе преследовал цель реализовать (если это возможно и какие возможно) транзитивное подгруппы группы S_n для $3 \leq n \leq 7$, а также познакомить читателя с нерешенными проблемами по этому вопрос.

Литература

1. Сергеев Э. А. Элементы теории Галуа. /Кубан. гос ун-т. Краснодар, 1987.
2. Эйлер Л. Дифференциальное исчисление , М. Л. 1949.
3. Постников М. М. Теория Галуа. М. 1963.
4. Elkies N. Other Aruthmetic Manifestation of Branched Covers. MSRI website 1999.
5. Matzat H. Constructive Galoistherie, «Lect. Notes Math.» № 1284, 1987.
6. Komatsu K. On the Galois Group of x^p + ax^k + a = 0. Tokio, J. Math Vol. 14
7. Dummit D. Solving solvable quintics, Math, Of Compul. Vol. 57, № 195, 1991, 387 – 401
8. Spearman K., Williams K. On solvable quinties x^5 + ax + b and x^5 + ax^2 + b. Rocky Mountain Journal of Mathematics. Vol. 26, № 2, 1996, 753 – 773.
9. Malle G. Polynomials with Galois group PSL(3,2) uber Q, Manuscript, Universitat Karlsruhe, 1968.
10. LaMacchia M.E. Polynomials with Galois group PSL(2,7). Commut. Alg. Vol 8. 1980, 983 – 992.
11. Erbach D. W., Fisher J., McKay J. Polynomials with PLS(2,7) as Galois group. Jornal of Number Theory, Vol. 11. 1979, 69 – 75.
12. Trinks W. Ein Beispell eines Zahlkorpers mit der Galoisgroup PSL(3,2) uber Q, Manuscript, Universitat Karlsruhe, 1986.
13. Jensen C., Yuri N, Polynomials with D_p as Galois Group. Journal of Number Theory, Vol, 15., 1982, 347-375.
14. Stauduhar R. The determination iof Galois Group. Math. Of comput. Vol. 27, № 124ю 1973ю 981-996
15. Ваи дер Варден Б. Л. Алгебра. М. 1979
16. Usida K. Galois group of an equation x^n – ax + b = 0. Tohoku Math. Journal. 1970. Vol. 22 № 4. 670-678
17. Osada H. The Galois Groups of the polynomials x^n + ax^k + b = 0. Tohoku Math. Journal, 1987. Vol. 39. 437-445
18. Feit W. Some consequences of the classification of finite simple groups. Santa Cruz. Conf. Finite Groups. Santa Cruz. Calif.1979, R I.Providence. 175-181.

Literature

1. Sergeev A.E., Sergeev E.A. Foundations of Galois theory. Prosveshenie. Krasnodar. 2014.
2. Eiler L. Differential calculus. M. L. 1949.
3. Postnikov M.M. Galois theory. M. 1963
4. Elkies N. Other Aruthmetic Manifestation of Branched Covers. MSRI website 1999.
5. Matzat H. Constructive Galoistherie, «Lect. Notes Math.» № 1284, 1987.
6. Komatsu K. On the Galois Group of x^p + ax^k + a = 0. Tokio, J. Math Vol. 14

7. Dummit D. Solving solvable quintics, Math, Of Compul. Vol. 57, № 195, 1991, 387 – 401

8. Spearman K., Williams K. On solvable quinties x^5 + ax + b and x^5 + ax^2 + b. Rocky Mountain Journal of Mathematics. Vol. 26, № 2, 1996, 753 – 773.

9. Malle G. Polynomials with Galois group PSL(3,2) uber Q, Manuscript, Universitat Karlsruhe, 1968.

10. LaMacchia M.E. Polynomials with Galois group PSL(2,7). Commut. Alg. Vol 8. 1980, 983 – 992.

11. Erbach D. W., Fisher J., McKay J. Polynomials with PLS(2,7) as Galois group. Jornal of Number Theory, Vol. 11. 1979, 69 – 75.

12. Trinks W. Ein Beispell eines Zahlkorpers mit der Galoisgroup PSL(3,2) uber Q, Manuscript, Universitat Karlsruhe, 1986.

13. Jensen C., Yuri N, Polynomials with D_p as Galois Group. Journal of Number Theory, Vol, 15., 1982, 347-375.

14. Stauduhar R. The determination iof Galois Group. Math. Of comput. Vol. 27, № 124ю 1973ю 981-996

15. Ваи дер Варден Б. Л. Алгебра. М. 1979

16. Usida K. Galois group of an equation x^n – ax + b = 0. Tohoku Math. Journal. 1970. Vol. 22 № 4. 670-678

17. Osada H. The Galois Groups of the polynomials x^n + ax^k + b = 0. Tohoku Math. Journal, 1987. Vol. 39. 437-445

18. Feit W. Some consequences of the classification of finite simple groups. Santa Cruz. Conf. Finite Groups. Santa Cruz. Calif.1979, R I.Providence. 175-181.