Записки научных
семинаров ПОМИ
Том 443, 2016 г.

К. Ю. Гудков, Б. Б. Лурье

ЦИКЛИЧЕСКИЕ РАСШИРЕНИЯ ГАЛУА ДЛЯ УРАВНЕНИЙ 5-Й СТЕПЕНИ

§1. Уравнения 5-й степени и их расширения Галуа.

Нахождение группы Галуа конкретного уравнения представляет собой нетривиальную задачу. Поскольку вопрос разрешимости многочлена в радикалах как исторически основной задачи теории Галуа был сведен к определению разрешимости соответствующей этому многочлену группы Галуа, возникла потребность в распознавании самой этой группы. Конкретно случай $n = 5$ и вопрос различения транзитивных подгрупп S_5 был рассмотрен и достаточно подробно изложен в [1] и в [4]. В частности этот случай интересен потому, что связан с группой самосовмещений икосаэдра и теорией эллиптических кривых. Проблема определения разрешимости была затронута ещё в 19-м веке, когда была найдена в явном виде резольвента 6-го порядка для уравнения 5-й степени (см. [3]), позднее для случая $\mathrm{Gal}(f(x)) \subset D_5$ были сформулированы некоторые критерии в [5] и [6].

Особенностью циклической группы является то, что для неприводимого многочлена f над полем K поле разложения f получается путём добавления любого его корня. Это значит, в частности, что в то время, как для любого неприводимого многочлена над $\mathbb{Q}$ с разрешимой группой Галуа всякий корень многочлена выражается как рациональная функция через какие-то два (см., к примеру, [7], выражение корней для группы D_5 в [8]), для циклической группы, очевидно, выполнено более сильное утверждение: все корни многочлена с циклической группой Галуа выражаются как рациональные функции от любого корня этого многочлена. Известно, что группой Галуа неприводимого многочлена может являться только транзитивная подгруппа S_n, кроме того, имеет место

Утверждение 1 (см. [1], стр. 145)**.** *Любая транзитивная группа подстановок простой степени p содержит цикл длины p.*

Ключевые слова: уравнения 5-й степени, циклическая группа Галуа, характеризация расширений Галуа.

В случае $n = 5$ все транзитивные группы содержат цикл длины 5 и сопряжены одной из перечисленных групп:

$$\begin{aligned} S_5 &= \langle (12345), (12) \rangle, |S_5| = 120, \\ A_5 &= \langle (12345), (123) \rangle, |A_5| = 60, \\ F_{20} &= \langle (12345), (1254) \rangle, |F_{20}| = 20, \\ D_5 &= \langle (12345), (15)(24) \rangle, |D_5| = 10, \\ C_5 &= \langle (12345) \rangle, |C_5| = 5, \\ & C_5 \subset D_5 = A_5 \cap F_{20}. \end{aligned}$$

Основным результатом для $n = 5$ является резольвента 6-го порядка (см. [1], стр. 151), построенная на основе многочлена $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_1x_4 - x_2x_4 - x_2x_5 - x_3x_5$, точно принадлежащего метациклической группе F_{20}:

$$G(z) := (z^3 + B_2 \cdot z^2 + B_4 \cdot z + B_6)^2 - D_f \cdot c^2 \cdot z,$$

где коэффициенты B_2, B_4, B_6, c выражаются через коэффициенты многочлена f, а D_f – его дискриминант.

Имеет место

Теорема 1 (см. [4], стр. 145). *Пусть $f \in K[x]$ является унитарным, неприводимым и не имеющим кратных корней многочленом пятой степени над полем K, $\operatorname{char} K \neq 2$. Тогда его группа Галуа G обладает следующими свойствами:*

(1) *$G \subset A_5$ тогда и только тогда, когда $\sqrt{D_f} \in K$.*
(2) *$G \cong H$, где $H \subset F_{20}$ – некая подгруппа S_5, тогда и только тогда, когда резольвента $G(z)$ имеет корень в K.*
(3) *$G \cong C_5$ тогда и только тогда, когда $K(\theta)$ является полем разложения f для любого его корня θ.*

Кроме того, для уравнений пятой степени справедлива следующая

Теорема 2 (см. [9]). *Для того, чтобы неприводимое уравнение пятой степени над полем K имело симметрическую группу Галуа, достаточно, чтобы его дискриминант не был суммой двух квадратов из K.*

В то время, как условия 1–2 теоремы 1 достаточно наглядны, и понятно, как проверять их выполнение, условие 3, а именно различение групп C_5 и D_5, не всегда видится простым для проверки. Одним

из возможных путей решения этой проблемы является построение резольвенты для циклической группы, используя её смежные классы, но, в силу того, что $[S_5 : C_5] = 24$, она имела бы 24-ю степень.

В нашей работе мы сконструируем резольвенту 6-й степени, аналогичную классической резольвенте, которая бы более полно классифицировала возможные группы Галуа многочлена пятой степени.

Данная работа представляет собой переработанную дипломную работу первого из соавторов, выполненную под руководством второго.

Авторы выражают благодарность А. В. Яковлеву за полезные обсуждения.

§2. Построение резольвенты над полем $K(i)$.

Для конструирования резольвенты нам потребуется добавить в исходное поле корень из -1: $K = K(\sqrt{-1}) = K(i)$. Поскольку наша основная цель отделить группу C_5 от остальных, добавляя новый элемент, мы должны быть уверены, что группа Галуа многочлена не может стать циклической, если она таковой не являлась до добавления этого элемента.

Предложение 1. *Пусть поле коэффициентов многочлена f K является подполем $\mathbb{R}$. Тогда, если при присоединении корня из -1 группа Галуа многочлена f изменилась, то среди корней многочлена f есть комплексные числа.*

Доказательство. Пусть все корни f вещественны, тогда поле разложения f N также вещественно. Но, поскольку при добавлении корня из -1 группа $\mathrm{Gal}(f)$ изменилась, существует цепочка расширений из K в N, в которой присутствует комплексное расширение. Пришли к противоречию с тем, что N вещественно. $\square$

Предложение 1 позволяет нам добавлять корень из -1 в вещественное подполе: действительно, если все корни многочлена f вещественны, то группа Галуа не изменится, а если есть комплексные корни, то группа Галуа не может быть циклической.

При построении резольвенты мы будем рассматривать либо вещественные подполя, либо поля, содержащие корень из -1. Также нам потребуется определить специальный многочлен от пяти переменных $(x_1, \ldots, x_5)$, точно принадлежащий группе C_5 и имеющий минимальную возможную степень. Справедлива

Лемма 1. *Пусть многочлен* $g(x_1, \ldots, x_5)$ *точно принадлежит группе* C_5, *тогда* $\deg(g) \geqslant 3$.

Доказательство. Очевидно, что такой многочлен можно привести к виду, в котором не будет слагаемых степени 1. Действительно, если в многочлене есть слагаемое x_1, то, поскольку под действием перестановки (12345) он должен остаться на месте, в нем есть все слагаемые вида x_i. Поскольку $x_1 + x_2 + x_3 + x_4 + x_5 = \sigma_1 \in K$, от них можно избавиться.

Пусть $\deg(g) = 2$. Тогда возможны 2 варианта:

(1) В многочлене есть слагаемые вида x_i^2. Тогда, поскольку он точно принадлежит группе C_5, в нём должны быть все слагаемые такого вида, т.е. в многочлене присутствует выражение вида $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = \sigma_1^2 - 2\sigma_2 \in K$. Тогда от этого выражения можно избавиться.

(2) Все слагаемые в многочлене имеют вид $x_i x_j$. Пусть имеется слагаемое $x_i x_{i+k}, 0 < k < 5$. Тогда автоматически есть сумма

$$S(x_1, x_2, x_3, x_4, x_5) := \sum_{1 \leqslant i,j \leqslant 5, i+k \equiv j \pmod 5} x_i x_j$$

Обозначим $\sigma = (15)(24) \in D_5$, тогда заметим, что σ действует на индексы следующим образом: $\sigma : i \to (6-i), 1 \leqslant i \leqslant 5$. Поэтому

$$\begin{aligned}\sigma(S(x_1, x_2, x_3, x_4, x_5)) &= \sum_{1 \leqslant i,j \leqslant 5, i+k \equiv j \pmod 5} x_{\sigma(i)} x_{\sigma(j)} \\ &= \sum_{1 \leqslant i',j' \leqslant 5, (6-i')+k \equiv (6-j') \pmod 5} x_{i'} x_{j'} \\ &= \sum_{1 \leqslant i',j' \leqslant 5, j'+k \equiv i' \pmod 5} x_{j'} x_{i'} = S(x_1, x_2, x_3, x_4, x_5)\end{aligned}$$

Таким образом, всякое выражение, инвариантное относительно (12345), будет инвариантно относительно σ, что противоречит условию. □

Теперь введём новое обозначение, пусть $\alpha = (12345) \in S_5$, $\sigma = (1254)$, тогда определим

$$d_\alpha = d_\alpha(x_1, x_2, x_3, x_4, x_5) := \sum_{1 \leqslant i,j \leqslant 5, \alpha(i) = j} x_i x_j (x_i - x_j).$$

Покажем, как σ действует на d_α:

$$\begin{tikzcd} d_\alpha \arrow[d, "\sigma"'] & d_{\alpha^2} \arrow[l, "\sigma"'] \\ d_{\alpha^3} \arrow[r, "\sigma"] & d_{\alpha^4} \arrow[u, "\sigma"] \end{tikzcd}$$

Отметим, что $d_{\alpha^4} = -d_\alpha$ и $d_{\alpha^2} = -d_{\alpha^3}$.

Обозначим

$$r_\alpha = r_\alpha(x_1, x_2, x_3, x_4, x_5) := d_\alpha - i \cdot d_{\alpha^3}.$$

Лемма 2. *Пусть $r_\alpha \neq 0$, тогда*

(1) *r_α точно принадлежит C_5;*
(2) *r_α^2 точно принадлежит D_5;*
(3) *r_α^4 принадлежит F_{20}.*

Доказательство. Поймём, что если $r_\alpha \neq 0$, то r_α точно принадлежит C_5. Действительно, понятно, что $\alpha(r_\alpha) = r_\alpha$, значит, r_α точно принадлежит группе, содержащей C_5. Заметим, что:

$$\begin{aligned} \sigma(r_\alpha) &= \sigma(d_\alpha - i \cdot d_{\alpha^3}) = d_{\alpha^3} - i \cdot d_{\alpha^4} \\ &= d_{\alpha^3} + i \cdot d_\alpha = i \cdot (d_\alpha - i \cdot d_{\alpha^3}) = i \cdot r_\alpha, \end{aligned}$$

поэтому, с учётом того, что $r_\alpha \neq 0$, r_α точно принадлежит C_5, r_α^2 точно принадлежит D_5 и r_α^4 принадлежит F_{20}, что и требовалось доказать. □

Теперь сконструируем резольвенту для группы F_{20} на основе многочлена r_α^4. Возьмём тех же представителей различных классов сопряжённости для F_{20}, что и, к примеру, в [4]:

$$\begin{aligned} &s_1 = e : \alpha = \alpha_1 = (12345), \\ &s_2 = (123) : \alpha_2 = \alpha^{s_2} = (14523), \\ &s_3 = (234) : \alpha_3 = \alpha^{s_3} = (13425), \\ &s_4 = (345) : \alpha_4 = \alpha^{s_4} = (12453), \\ &s_5 = (145) : \alpha_5 = \alpha^{s_5} = (14235), \\ &s_6 = (125) : \alpha_6 = \alpha^{s_6} = (12534). \end{aligned}$$

Тогда сами многочлены будут иметь вид

$$r_{\alpha_j} = d_{\alpha_j} - i \cdot d_{\alpha_j^3}$$

Теперь напишем саму форму резольвенты:

$$R(z) = R(z, x_1, x_2, x_3, x_4, x_5) := \prod_{i=1}^{6} (z - r_{\alpha_i}^4 (x_1, x_2, x_3, x_4, x_5))$$

Заметим, что все коэффициенты $R(z)$ являются симметрическими функциями от x_1, x_2, x_3, x_4, x_5, а значит, выражаются через коэффициенты изначального многочлена f.

Теперь исследуем более подробно вид этой резольвенты. Заметим, что

$$\begin{aligned} R(z^2) &= \prod_{i=1}^{6} (z^2 - r_{\alpha_i}^4) = \prod_{i=1}^{6} (z - r_{\alpha_i}^2) \cdot \prod_{i=1}^{6} (z + r_{\alpha_i}^2) \\ &= \prod_{i=1}^{6} (z - r_{\alpha_i}^2) \cdot \prod_{i=1}^{6} (-z - r_{\alpha_i}^2) = H(z) \cdot H(-z). \end{aligned}$$

Исследуем свойства многочлена $H(z)$. Ясно, что, поскольку все 3-циклы порождают группу A_5, при действии четных перестановок $H(z)$ остаётся на месте.

Предложение 2. *Пусть α_j – одна из перечисленных выше перестановок, τ – произвольная транспозиция, тогда найдётся такое k, что $\tau(r_{\alpha_j}) = \pm i \cdot r_{\alpha_k}$.*

Доказательство. Рассмотрим действие произвольной транспозиции на выражение $r_{(jklmn)}$, где $1 \leqslant j, k, l, m, n \leqslant 5$. Поскольку выражение $r_{(jklmn)}$ инвариантно относительно действия циклической перестановки $(jklmn)$, достаточно проверить действие перестановок $\tau_1 = (jk)$ и $\tau_2 = (jl)$:

$$\begin{aligned} \tau_1(r_{(jklmn)}) &= \tau_1(d_{(jklmn)} - i \cdot d_{(jmknl)}) = d_{(kjlmn)} - i \cdot d_{(kmjnl)} \\ &= d_{(kjlmn)} + i \cdot d_{(jmkln)} = i \cdot (-i \cdot d_{(kjlmn)} + d_{(jmkln)}) \\ &= i \cdot (d_{(jmkln)} - i \cdot d_{(kjlmn)}) = i \cdot r_{(jmkln)} = i \cdot r_{\beta_1}, \end{aligned}$$

при этом $(jmkln) = (jklmn)^{(kml)}, (kml) \in A_5$.

$$\begin{aligned}\tau_2(r_{(jklmn)}) &= \tau_2(d_{(jklmn)} - i \cdot d_{(jmknl)}) = d_{(lkjmn)} - i \cdot d_{(lmknj)} \\ &= d_{(lkjmn)} + i \cdot d_{(jnkml)} = i \cdot (-i \cdot d_{(lkjmn)} + d_{(jnkml)}) \\ &= i \cdot (d_{(jnkml)} - i \cdot d_{(lkjmn)}) = i \cdot r_{(jnkml)} = i \cdot r_{\beta_2},\end{aligned}$$

при этом $(jnkml) = (jklmn)^{(knl)}, (knl) \in A_5$.

Поскольку $[A_5 : C_5] = 12$, β_i либо совпадает с одним из α_j, либо с одним из α_j^4, куда α_j переводят элементы соответствующей группы, сопряжённой D_5. В первом случае мы получаем знак “+”, во втором остаётся понять, что $r_{\alpha_j^4} = -r_{\alpha_j}$, и мы получаем знак “−”. □

Таким образом, чётные перестановки оставляют $H(z)$ на месте, а нечётные меняют его знак. Из этого следует, что все чётные коэффициенты многочлена принадлежат полю K, а нечётные коэффициенты представляют из себя элементы поля K, умноженные на $\sqrt{D}$, т.е.

$$H(z) = z^6 + az^4 + bz^2 + c + \sqrt{D} \cdot (dz^5 + ez^3 + gz).$$

Посмотрим теперь на коэффициенты $H(z)$ как на симметрические многочлены от корней x_1, x_2, x_3, x_4, x_5: $r_{\alpha_i}^2$ является многочленом 6-й степени, поэтому степени коэффициентов при соответствующих степенях $H(z)$ должны быть равны 6, 12, 18, 24, 30 и 36 соответственно. Поскольку степень $\sqrt{D}$ равна 10, $d = 0$. Кроме того, заметим, что

$$c = \prod_{i=1}^{6} r_{\alpha_i}^2 = \Big(\prod_{i=1}^{6} r_{\alpha_i}\Big)^2,$$

из предложения 1 следует, что под действием любой перестановки выражение под квадратом остаётся на месте, поэтому $c \in K^2$. В итоге мы получаем вид многочлена $H(z)$:

$$H(z) = z^6 + az^4 + bz^2 + c^2 + \sqrt{D} \cdot (ez^3 + gz),$$

где a, b, c, e, g являются симметрическими многочленами относительно корней x_1, x_2, x_3, x_4, x_5 степеней 12, 24, 9, 8 и 20, соответственно.

Тогда искомая резольвента имеет вид

$$R(z) = (z^3 + az^2 + bz + c^2)^2 - D \cdot (e^2z^3 + 2egz^2 + g^2z).$$

Используя программный пакет *Maple*, мы смогли явно выразить коэффициенты $R(z)$ (см. Приложение).

Теперь исследуем, в каком случае $R(z)$ имеет кратные корни.

Лемма 3. *Следующие условия равносильны:*

(1) *Резольвента $R(z)$ имеет кратные корни.*
(2) $\forall 1 \leqslant j \leqslant 5$ $r_{\alpha_j} = r_{\alpha_j}(x_1, x_2, x_3, x_4, x_5) = 0$.
(3) *Резольвента имеет вид $R(z) = z^6$.*

Доказательство. Очевидно, что из (2) следует (3), а из (3) следует (1). Докажем оставшийся неочевидный переход.
(1) $\Rightarrow$ (2). Пусть $R(z)$ имеет кратные корни, тогда существуют 5-циклы α, β такие, что $r_\alpha^4 = r_\beta^4$, причём из построения резольвенты следует, что существует 3-цикл $\gamma \in A_5$ такой, что $\beta = \alpha^\gamma$. Тогда r_α^4 инвариантно относительно сопряжения элементами α и γ, а значит, и относительно сопряжения любыми элементами A_5, поэтому для любых i, j $r_{\alpha_i}^4 = r_{\alpha_j}^4$. Значит, найдутся j_1, j_2, для которых $r_{\alpha_{j_1}} = r_{\alpha_{j_2}}$, при этом существует 3-цикл $\delta \in A_5$ такой, что $\alpha_{j_1} = \alpha_{j_2}^\delta$. Отсюда, по аналогии, α_{j_1} инвариантно относительно действия A_5, а значит для любых i, j $r_{\alpha_i} = r_{\alpha_j}$. Теперь вспомним, что из вида многочлена $H(z)$, который использовался для построения резольвенты $R(z)$, следует, что

$$\sum_{i=0}^{6} r_{\alpha_i}^2(x_1, x_2, x_3, x_4, x_5) = 0,$$

а значит, для любых i $r_{\alpha_i}(x_1, x_2, x_3, x_4, x_5) = 0$. □

§3. Основные результаты

Теперь сформулируем основную теорему, доказательство которой следует напрямую из теоремы 1 и свойств резольвенты $R(z)$.

Теорема 3. *Пусть $f \in K[x]$ является унитарным, неприводимым и не имеющим кратных корней многочленом пятой степени над полем K. Кроме того, пусть $R(z)$ не имеет кратных корней. Тогда группа Галуа $G = \mathrm{Gal}(f)$ обладает следующими свойствами:*

(1) *$G \subset A_5$ тогда и только тогда, когда $\sqrt{D_f} \in K$.*
(2) *$G \cong H$, где $H \subset F_{20}$ – некая подгруппа S_5, тогда и только тогда, когда резольвента $R(z)$ имеет корень $\theta \in K$.*
(3) *Если, кроме того, $\theta \in K^2$, то $G \cong H \subset D_5$.*
(4) *Если, кроме того, $\theta \in K^4$, то $G \cong C_5$.*

Таким образом, при условии отсутствия кратных корней у $R(z)$ мы получаем классификацию групп Галуа 5-й степени, которая требует

только вычисления дискриминанта и нахождения корней $R(z)$.

Кроме того, оказывается, что для определения цикличности группы Галуа в вещественном случае условие наличия кратных корней у $R(z)$ можно опустить:

Теорема 4. *Пусть K – вещественное подполе $\mathbb{R}, f \in K[x]$. Если $G = \mathrm{Gal}(f) \cong C_5$, то у резольвенты $R(z)$ нет кратных корней над $K(\sqrt{-1})$.*

Доказательство. Пусть $G \cong C_5$, тогда из этого следует, что все корни многочлена $f(x)$ вещественны. Предположим, что $R(z)$ имеет хотя бы один кратный корень, тогда по лемме 3

$$\forall j \; r_{\alpha_j}(x_1, x_2, x_3, x_4, x_5) = 0.$$

Поскольку все корни вещественны, а $f(x)$ не имеет кратных корней, для определённости положим

$$x_1 > x_2 > x_3 > x_4 > x_5.$$

Пусть циклической группе, содержащей цикл (12345), соответствует выражение

$$r_\alpha(x_1, x_2, x_3, x_4, x_5) = d_\alpha(x_1, x_2, x_3, x_4, x_5) - i \cdot d_{\alpha^3}(x_1, x_2, x_3, x_4, x_5) = 0.$$

Поскольку из того, что комплексное число равно нулю, следует равенство нулю его комплексной и вещественной частей,

$$d_\alpha(x_1, x_2, x_3, x_4, x_5) = 0,$$
$$d_{\alpha^3}(x_1, x_2, x_3, x_4, x_5) = 0,$$

значит,

$$d_{\alpha^4}(x_1, x_2, x_3, x_4, x_5) = -d_\alpha(x_1, x_2, x_3, x_4, x_5) = 0,$$
$$d_{\alpha^3}(x_1, x_2, x_3, x_4, x_5) = -d_{\alpha^2}(x_1, x_2, x_3, x_4, x_5) = 0,$$

откуда и выражение вида

$$d_{(12345)}(x_1, x_2, x_3, x_4, x_5) = x_1x_2(x_1 - x_2) + x_2x_3(x_2 - x_3) + x_3x_4(x_3 - x_4) + x_4x_5(x_4 - x_5) + x_1x_5(x_5 - x_1)$$

тоже равняется нулю.

Теперь заметим, что выражение $d_\alpha(x_1, x_2, x_3, x_4, x_5)$ инвариантно относительно одновременного сдвига корней на константу ($\forall i\ T_k(x_i) = x_i + k$): действительно,

$$T_k(x_i x_j(x_i - x_j)) = (x_i + k)(x_j + k)((x_i + k) - (x_j + k))$$
$$= (x_i + k)(x_j + k)(x_i - x_j) = x_i x_j(x_i - x_j) + k(x_i^2 - x_j^2) + k^2(x_i - x_j).$$

Таким образом, когда мы сложим все выражения вида $x_i x_j(x_i - x_j)$, при преобразовании все появившиеся слагаемые по циклу сократятся. Тогда сдвинем корни на x_5:

$$T_{x_5}(d_{(12345)}(x_1, x_2, x_3, x_4, x_5)) = (x_1 - x_5)(x_2 - x_5)(x_1 - x_2)$$
$$+ (x_2 - x_5)(x_3 - x_5)(x_2 - x_3) + (x_3 - x_5)(x_4 - x_5)(x_3 - x_4) = 0.$$

Заметим, что в силу неравенств между корнями все слагаемые в сумме строго больше нуля, тогда как само оно равняется нулю. Пришли в противоречию с предположением о том, что $R(z)$ имеет кратный корень. □

§4. Приложение.

Здесь приводятся явные выражения для коэффициентов построенной резольвенты $R(z)$ и код на языке *Maple*, позволяющий вычислить эти выражения.

Все выражения написаны в терминах элементарных симметрических многочленов σ_i от корней многочлена f и в предположении, что f приведён к виду с коэффициентом при четвёртой степени равным нулю ($\sigma_1 = 0$).

```
with(LinearAlgebra):
with(PolynomialTools):
A := Matrix([[1, 2, 3, 4, 5], [1, 4, 5, 2, 3], [1, 3, 4, 2, 5],
             [1, 2, 4, 5, 3], [1, 4, 2, 3, 5], [1, 2, 5, 3, 4]]):
alpha := k -> (A[k, 1], A[k, 2], A[k, 3], A[k, 4], A[k, 5]):

R1 := (i, j, k, l, m) -> x[i]*x[j]*(x[i]-x[j])+x[j]*x[k]*(x[j]-x[k])+
x[k]*x[l]*(x[k]-x[l])+x[l]*x[m]*(x[l]-x[m])+x[m]*x[i]*(x[m]-x[i]):
 R := (i, j, k, l, m) -> (R1(i, j, k, l, m)-I*R1(i, l, j, m, k))^2;
Discrim := (x[1]-x[2])*(x[1]-x[3])*(x[1]-x[4])*(x[1]-x[5])*(x[2]-x[3])*
(x[2]-x[4])*(x[2]-x[5])*(x[3]-x[4])*(x[3]-x[5])*(x[4]-x[5]):

F := (z-R(alpha(1)))*(z-R(alpha(2)))*(z-R(alpha(3)))*
(z-R(alpha(4)))*(z-R(alpha(5)))*(z-R(alpha(6))):
C := collect(F, z):
```

```
K := CoefficientList(C, z):

a := subs({x[1]+x[2]+x[3]+x[4]+x[5] = 0}, convert(K[5], 'elsymfun'));
b := subs({x[1]+x[2]+x[3]+x[4]+x[5] = 0}, convert(K[3], 'elsymfun'));
c := subs({x[1]+x[2]+x[3]+x[4]+x[5] = 0},
              convert(product(R(alpha(i)), i = 1 .. 6), 'elsymfun'));
e := subs({x[1]+x[2]+x[3]+x[4]+x[5] = 0},
                          convert(normal(K[4]/Discrim), 'elsymfun'));
g := subs({x[1]+x[2]+x[3]+x[4]+x[5] = 0},
                          convert(normal(K[2]/Discrim), 'elsymfun'));
```

В итоге получаем явные выражения для коэффициентов резольвенты:

$$R(z) = (z^3 + az^2 + bz + c^2)^2 - D \cdot (e^2 z^3 + 2egz^2 + g^2 z), \text{ где}$$

$$\begin{aligned} a = {} & -48\sigma_2^6 + 216(-9-13i)\sigma_2\sigma_3^2\sigma_4 + 8(-49+12i)\sigma_2^3\sigma_3^2 + 8(-73+264i)\sigma_2^2\sigma_4^2 \\ & + 32(13-9i)\sigma_2^4\sigma_4 + 1000(-4-3i)\sigma_2\sigma_5^2 + 27(7+24i)\sigma_3^4 + 160(-7-24i) \\ & + 480(11+2i)\sigma_2^2\sigma_3\sigma_5 + 1800(-3+4i)\sigma_3\sigma_4\sigma_5, \end{aligned}$$

$$\begin{aligned} b = {} & 640(2939+1773i)\sigma_2\sigma_3^2\sigma_4^2 + 432(1801-1593i)\sigma_2\sigma_3^6\sigma_4 \\ & + 64(12364-2127i)\sigma_2^5\sigma_3^2\sigma_4^2 + 5888(-29+7i)\sigma_2^7\sigma_3^2\sigma_4 + 128(-3894+1967i)\sigma_2^6\sigma_4^3 \\ & + 1024(102-41i)\sigma_2^8\sigma_4^2 + 32(2321-328i)\sigma_2^6\sigma_3^4 + 144(-842+8631i)\sigma_2^2\sigma_3^4\sigma_4^2 \\ & + 40000(243-149i)\sigma_2^3\sigma_3\sigma_5^3 + 512(701+1207i)\sigma_2^5\sigma_3^3\sigma_5 + 400000(33-19i)\sigma_2\sigma_4^2\sigma_5 \\ & + 832(-539+27i)\sigma_2^4\sigma_3^4\sigma_4 + 864(-1041+2413i)\sigma_2^2\sigma_3^5\sigma_5 + 150000(-41+38i)\sigma_2^2\sigma_5^4 \\ & + 1125000(1+7i)\sigma_3^3\sigma_5^3 + 1000000(24+7i)\sigma_4\sigma_5^4 + 64(-4706+4133i)\sigma_2^7\sigma_5^2 \\ & + 150000(101+77i)\sigma_2^2\sigma_3^2\sigma_4\sigma_5^2 + 256(49-4i)\sigma_2^9\sigma_3^2 + 1024(-13+3i)\sigma_2^{10}\sigma_4 \\ & + 32(-54352-5189i)\sigma_2^3\sigma_3^2\sigma_4^3 + 16(95273-54064i)\sigma_2^4\sigma_4^4 + 144(913-84i)\sigma_2^3\sigma_3^6 \\ & + 128(-21021+12928i)\sigma_2^2\sigma_4^5 + 3600(527-336i)\sigma_3^4\sigma_4^3 + 8000(133+706i)\sigma_2^4\sigma_3\sigma_4^2\sigma_5 \\ & + 260000(-42+31i)\sigma_2^3\sigma_4^2\sigma_5^2 + 800(3607-17276i)\sigma_2^2\sigma_3\sigma_4^3\sigma_5 \\ & + 3600(-1751+1318i)\sigma_2\sigma_3^3\sigma_4^2\sigma_5 + 1080(-3967+2381i)\sigma_3^5\sigma_4\sigma_5 \\ & + 21120(147-121i)\sigma_2^5\sigma_4\sigma_5^2 + 243(-527+336i)\sigma_3^8 + 768\sigma_2^{12} \\ & + 360000(17-31i)\sigma_3^2\sigma_4^2\sigma_5^2 + 160(3326-35293i)\sigma_2^3\sigma_3^3\sigma_4\sigma_5 \\ & + 128(-4853-7246i)\sigma_2^6\sigma_3\sigma_4\sigma_5 + 500000(-74+7i)\sigma_2\sigma_3\sigma_4\sigma_5^3 \\ & + 27000(91-313i)\sigma_2\sigma_3^4\sigma_5^2 + 16000(-539+652i)\sigma_3\sigma_4^4\sigma_5 \\ & + 2000(-2236+73i)\sigma_2^4\sigma_3^2\sigma_5^2 + 2560(31+17i)\sigma_2^8\sigma_3\sigma_5 + 3840(527-336i)\sigma_4^6, \end{aligned}$$

$$
\begin{aligned}
c = {} & 24(19-42i)\sigma_2^2\sigma_3^2\sigma_5 + 4(-2434+2637i)\sigma_2^2\sigma_3^2\sigma_4^2 + 200(136-123i)\sigma_2\sigma_3\sigma_4^2\sigma_5 \\
& + 12500(7-i)\sigma_3\sigma_5^3 + 1500(-38+9i)\sigma_2\sigma_3^2\sigma_5^2 + 16(456-383i)\sigma_2^3\sigma_4^3 \\
& + 27(-44+117i)\sigma_3^6 + 36(167-231i)\sigma_2\sigma_3^4\sigma_4 + 64i\sigma_2^9 + 500(3+i)\sigma_2^2\sigma_4\sigma_5^2 \\
& + 320(-24+7i)\sigma_2\sigma_4^4 + 64(3-13i)\sigma_2^7\sigma_4 + 4(-152+711i)\sigma_2^3\sigma_3^4 \\
& + 32(79-172i)\sigma_2^4\sigma_3^2\sigma_4 + 200(-11-2i)\sigma_2^4\sigma_5^2 + 900(7+24i)\sigma_3^3\sigma_4\sigma_5 \\
& + 528(-4+7i)\sigma_2^5\sigma_4^2 + 320(1-8i)\sigma_2^5\sigma_3\sigma_5 + 160(-53+104i)\sigma_2^3\sigma_3\sigma_4\sigma_5 \\
& + 16(-4+49i)\sigma_2^6\sigma_3^2 + 40(44-117i)\sigma_3^2\sigma_4^3 + 5000(-4-3i)\sigma_4^2\sigma_5^2,
\end{aligned}
$$

$$
\begin{aligned}
e = {} & 64(13-9i)\sigma_2^4 + 96(38+41i)\sigma_2\sigma_3^2 + 80(44-117i)\sigma_4^2 + 16(-249+307i)\sigma_2^2\sigma_4 \\
& + 200(-31-17i)\sigma_3\sigma_5,
\end{aligned}
$$

$$
\begin{aligned}
g = {} & 100000(38+41i)\sigma_5^4 + 128(5643-4849i)\sigma_2^5\sigma_3^2\sigma_4 + 64(40271+6197i)\sigma_2\sigma_3^2\sigma_4^3 \\
& + 144(14657-13051i)\sigma_2^2\sigma_3^4\sigma_4 + 128(-19656+8233i)\sigma_2^3\sigma_3^2\sigma_4^2 + 256(261-23i)\sigma_2^8\sigma_4 \\
& + 512(-131+158i)\sigma_2^7\sigma_3^2 + 256(-1336-27i)\sigma_2^6\sigma_4^2 + 64(-5261+9373i)\sigma_2^4\sigma_3^4 \\
& + 320(2759+263i)\sigma_2^4\sigma_4^3 + 432(-3116-237i)\sigma_3^4\sigma_4^2 + 64(-19032-1949i)\sigma_2^2\sigma_4^4 \\
& + 864(-718+1199i)\sigma_2\sigma_3^6 + 256(3116+237i)\sigma_4^5 + 1024(-5+i)\sigma_2^{10} \\
& + 64(2927-4161i)\sigma_2^5\sigma_5^2 + 216(10533-14869i)\sigma_3^5\sigma_5 + 5760(-718+1199i)\sigma_2\sigma_3^3\sigma_4\sigma_5 \\
& + 6560(191-863i)\sigma_2^2\sigma_3\sigma_4^2\sigma_5 + 1600(-1019+792i)\sigma_2^3\sigma_4\sigma_5^2 \\
& + 36000(-29-278i)\sigma_3^2\sigma_4\sigma_5^2 + 1600(-2826+2543i)\sigma_3\sigma_4^3\sigma_5 \\
& + 8000(439-102i)\sigma_2\sigma_4^2\sigma_5^2 + 20000(-193-126i)\sigma_2\sigma_3\sigma_5^3 \\
& + 2400(1213+1391i)\sigma_2^2\sigma_3^2\sigma_5^2 + 128(2431+13067i)\sigma_2^4\sigma_3\sigma_4\sigma_5 \\
& + 64(2769-35417i)\sigma_2^3\sigma_3^3\sigma_5 + 640(-113-191i)\sigma_2^6\sigma_3\sigma_5.
\end{aligned}
$$

Литература

1. М. М. Постников, *Теория Галуа*, Физматгиз, 1963.
2. Ф. Клейн, *Лекции об икосаэдре и решении уравнений пятой степени*, Пер. с нем. Под ред. А. Н. Тюрина. Наука. Гл. ред. физ.-мат. лит., 1989.
3. Н. Г. Чеботарев, *Основы теории Галуа*, Гос. техн.-теор. изд-во, 1934.
4. David A. Cox, *Galois theory*, 2nd edition, A John Wiley Sons, inc., 2012.
5. C. Jensen, N. Yui, *Polynomials with D_p as Galois group.* — J. Number Theory **15** (1982), 347–375.
6. C. Williamson, *Odd degree polynomials with dihedral Galois groups.* — J. Number Theory **34** (1990), 153–173.
7. Э. Галуа, *Математические работы*, Институт компьютерных исследований, 2002.
8. B. Spearman, K. Williams, *Dihedral quintic polynomials and a theorem of Galois.* — Indian J. Pure Appl. Math. **30**, No. 9 (1999).

9. Б. Лурье, *Критерий неразрешимости в радикалах уравнений простой степени.* — Докл. РАН **388** (2003), 447–448.

Gudkov K. Y., Lur'e B. B. Cyclic Galois extensions for quintic equation.

The authors investigate cyclic Galois extensions for quintic equation, and construct resolvent for real fields and fields, containing square root of -1. Also they prove a theorem that characterizes all Galois extensions for quintics.

Поступило 15 декабря 2015 г.

С.-Петербургский
государственный университет
Университетский пр. 28, Петродворец,
198504 Санкт-Петербург, Россия
E-mail: konstantingudkov@gmail.com

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
наб. р. Фонтанки, д. 27,
191023 С.-Петербург, Россия
E-mail: lurje@pdmi.ras.ru