Math-Net.Ru

Общероссийский математический портал

М. И. Зеликин, Д. Д. Киселев, Л. В. Локуциевский, Оптимальное управление и теория Галуа, *Матем. сб.*, 2013, том 204, номер 11, 83–98

DOI: <https://doi.org/10.4213/sm8211>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 35.173.219.12

26 апреля 2023 г., 16:03:50

УДК 512.623.3+517.587+517.977.57

М. И. Зеликин, Д. Д. Киселев, Л. В. Локуциевский

Оптимальное управление и теория Галуа

В решении одного класса задач оптимального управления важную роль играет некоторый специальный многочлен степени $2(n-1)$ с целыми коэффициентами. Линейная независимость набора из k корней этого многочлена над полем $\mathbb{Q}$ влечет существование решения исходной задачи с оптимальным управлением в виде всюду плотной обмотки k -мерного клиффордова тора, проходимой за конечное время. В работе показано, что для всех $n \leq 15$ в качестве k можно выбрать любое натуральное число, не превосходящее $[n/2]$. Развита в работе техника применена к системе многочленов Чебышёва–Эрмита и обобщенных многочленов Чебышёва–Лагерра. Доказано, что для таких многочленов степени $2m$ любая подсистема из $[(m+1)/2]$ корней, квадраты которых попарно различны, линейно независима над полем $\mathbb{Q}$.

Библиография: 11 названий.

Ключевые слова: принцип максимума Понтрягина, алгебра Ли, всюду плотная обмотка, группа Галуа, ортогональные многочлены.

DOI: 10.4213/sm8211

§ 1. Введение

Рассмотрим гладкое $2n$ -мерное симплектическое многообразие M^{2n} . Пусть $(2n-1)$ -мерное стратифицированное подмногообразие $S \subset M$ разделяет M на конечное число открытых областей $\Omega_1, \dots, \Omega_k$: $M = \bigcup \Omega_i$. Рассмотрим непрерывный гамильтониан $H(q, p): M \rightarrow \mathbb{R}$, ограничение которого $H_i = H|_{\Omega_i}$ на любое множество Ω_i определяет гладкую функцию, C^∞ -продолжимую на окрестность множества $\overline{\Omega_i}$.

Одной из основных целей теории оптимального управления является построение оптимального синтеза, т.е. фазового портрета экстремалей, проходящих через каждую начальную точку x_0 . Принцип максимума Понтрягина сводит эту проблему к изучению гамильтоновой системы дифференциальных уравнений с разрывной правой частью, причем разрывы достигаются в тех точках $x_0 \in S$, для которых максимум достигается при нескольких различных значениях управления. В таких точках стандартные теоремы существования и единственности неприменимы. Вопросы существования обобщенного решения обеспечиваются с помощью рассмотрения вспомогательного дифференциального уравнения с многозначной правой частью. В правой части этого уравнения стоит выпуклое замыкание всех предельных точек фазовых скоростей, полученных при стремлении окрестных точек к точке x_0 . Единственность решения, проходящего через x_0 , принципиально не имеет места. Здесь на первый план

выходит проблема описания с помощью функций H_i соответствующей интегральной воронки – конуса решений, входящих в точку x_0 или выходящих из нее. Порядок особенности определяется числом кратных скобок Пуассона от функций H_i , которые обращаются в нуль в точке x_0 (см. [1]).

Для одномерного управления, или, что то же, для поверхности разрыва ко-размерности 1 при особенности первого порядка, в типичной ситуации интегральная воронка состоит из трех экстремалей: две из них лежат по разные стороны от поверхности разрыва, а третья идет по этой поверхности. При особенности второго порядка ситуация общего положения была найдена и исследована в работах Купки [2] и Зеликина–Борисова [3]. Экстремали подходят к точке x_0 (и отходят от нее) за конечное время со счетным числом пересечений поверхности негладкости H (chattering-режим).

Особенности второго порядка для многомерного управления в случае, когда областью изменения управления является сфера, изучались в работах Миллутина [4], Зеликина–Борисова [3] и Зеликина–Локуциевского–Хильдебранда [1]. При подходе к точке x_0 управление за конечное время совершает счетное число оборотов по некоторой окружности. Соответствующая траектория $x(t)$ попадает в точку x_0 , проходя за конечное время некоторый аналог логарифмической спирали. В ряде случаев возможны комбинации таких решений, лежащих в различных двумерных подпространствах.

§ 2. Иррациональная обмотка тора

В этом параграфе будет изучен класс задач, в которых, с одной стороны, сопряжение особых оптимальных траекторий с неособыми неизбежно, а, с другой стороны, в силу [1; теорема 5.1] невозможно регулярное сопряжение.

Рассмотрим оптимизационную задачу

$$J(x) = \int_0^{+\infty} \langle x, Cx \rangle dt \rightarrow \min \quad (2.1)$$

на траекториях управляемой системы

$$\begin{aligned} x^{(q)} &= u, & |u| &\leq 1, & x &\in V, & u &\in U = V; \\ x^{(k)}(0) &= x_k^0 & \text{при } k &\leq q-1. \end{aligned}$$

Здесь V – евклидово пространство со скалярным произведением $\langle \cdot, \cdot \rangle$, а C – некоторая симметрическая билинейная форма. Функция $x(t)$ считается абсолютно непрерывной вместе со своими $2q-1$ производными. Управление $u(t) \in L_1(0; +\infty)$ – измеримая функция.

Пусть $\lambda_1, \dots, \lambda_s$ – собственные числа формы C , а $V_1, \dots, V_s$ – соответствующие собственные подпространства. Очевидно, что если хоть одно из собственных чисел отрицательно, то минимум задачи равен $-\infty$. Поэтому будем считать, что C неотрицательно определена. В этом случае у данной задачи

решение существует и единственно¹ (см. [3]). Если $\dim \ker C \neq 0$, то при проектировании $V \rightarrow V/\ker C$ значение функционала $J(x)$ не изменяется. Поэтому оптимальные траектории задачи с $\dim \ker C \neq 0$ находятся тривиально из решений аналогичной задачи в $V/\ker C$ взятием прообраза.

Аналогичным образом доказывается следующая теорема (подробнее см. [1]).

ТЕОРЕМА 1. Если $L = \text{span}(x_0^0, x_1^0, \dots, x_{q-1}^0)$ лежит в некотором собственном подпространстве V_j , то оптимальная траектория задачи (2.1) остается в L в течение всего времени.

Легко видеть, что если матрица C положительно определена (как было сказано, только такие задачи интересны для рассмотрения), то в данной задаче есть ровно одна особая экстремаль $x = u = 0$, и ее глобальный порядок равен² q . Значит, если q четно, то по теореме 5.1 из [1] регулярное сопряжение неособой траектории с особой $x = u = 0$ не оптимально.

В этом параграфе будут найдены явные решения задачи (2.1) (лежащие в интегральной воронке точки $x = 0$), оптимальное управление в которых движется вдоль всюду плотной обмотки клиффордова тора, вложенного в сферу $|u| = 1$. Сначала сформулируем доказанную ранее³ в [1] теорему о траекториях, не покидающих собственное подпространство V_j формы C . Любую двумерную плоскость L в V_j мы будем рассматривать как комплексную плоскость⁴ $\mathbb{C}$.

ТЕОРЕМА 2. В любой двумерной плоскости $L \subseteq V_j$, содержащей 0 , есть $[q/2]$ пар оптимальных траекторий⁵ задачи (2.1), имеющих вид

$$x(t) = (A_k t^{2q} \exp\{\pm i\alpha_k \ln |t|\})^{(q)}, \quad u(t) = \exp\{\pm i\alpha_k \ln |t|\}, \quad (2.2)$$

где $\alpha_k \in \mathbb{R}_+$ различны и находятся из условий

$$\text{Im } P_q(\alpha) = 0, \quad (-1)^{q+1} \text{Re } P_q(\alpha) > 0, \quad (2.3)$$

а коэффициенты $A_k \in \mathbb{R}_+$ находятся из условия $(-1)^{q+1} \text{Re } P_q(\alpha_k) = 1/A_k$. Здесь

$$P_q(\alpha) = (2q + i\alpha)((2q - 1) + i\alpha) \cdots (1 + i\alpha). \quad (2.4)$$

Если q нечетно, то в L есть еще одна траектория вида $x = t^q/q!$ и $u = 1$.

Отметим, что в решениях (2.2) управление совершает счетное число оборотов по окружности $L \cap \{|u| = 1\}$ при $t \rightarrow 0$ за конечное время. Сама траектория $x(t)$ представляет собой логарифмическую спираль, которая тоже проходит за конечное время.

¹В книге [3] приведено доказательство для одномерного управления. Однако оно дословно переписывается на случай многомерного управления в шаре.

²Точнее, глобальный порядок есть финитная последовательность $(0, \dots, 0, \dim V, 0, \dots)$, где $\dim V$ стоит на q -м месте (подробнее см. [1]).

³В статье [1] формулировка данной теоремы содержит опечатку, хотя доказательство корректно.

⁴Комплексная структура на L выбирается согласованно с евклидовой структурой на $\mathbb{R}^q$.

⁵С точностью до поворота и сдвига по времени.

В некоторых случаях линейные комбинации решений (2.2) дают новые оптимальные решения задачи (2.1), управление в которых уже движется не по окружности, а по тору, вложенному в сферу $|u| = 1$. Для отыскания всех траекторий такого типа мы воспользуемся группой Ли симметрий данной задачи и выделим семейства траекторий, не выходящих за пределы одной орбиты. Для этого выпишем систему принципа максимума. Положим

$$x_1 = x, \quad x'_1 = x_2, \quad \dots, \quad x'_{q-1} = x_q.$$

Тогда гамильтониан (функция Понтрягина) имеет вид $(p_1, \dots, p_q$ – сопряженные переменные)

$$H = -\lambda_0 \langle Cx_1, x_1 \rangle + \langle p_1, x_2 \rangle + \dots + \langle p_q, u \rangle.$$

Нетрудно показать, что $\lambda_0 \neq 0$. Положив $\lambda_0 = 1/2$, получаем

$$p'_1 = Cx_1, \quad p'_2 = -p_1, \quad \dots, \quad p'_q = -p_{q-1}, \quad u = \frac{p_q}{|p_q|}.$$

Вид этой системы сильно упростится, если обозначить

$$z_k = (-1)^{q-k} p_{q-k+1}, \quad z_{q+k} = Cx_k \quad \text{при } k \leq q. \quad (2.5)$$

Тогда $x = C^{-1}z_{q+1}$ и

$$z'_1 = z_2, \quad z'_2 = z_3, \quad \dots, \quad z'_{2q} = Cu, \quad u = (-1)^{q+1} \frac{z_1}{|z_1|}. \quad (2.6)$$

Данная система обладает следующими симметриями.

1. Группа $G_1 = \text{SO}(V_1) \times \text{SO}(V_2) \times \dots \times \text{SO}(V_s) \subseteq \text{SO}(V)$, где $\{V_i\}_{i=1}^s$ – ранее введенные собственные подпространства оператора C , действует на z_k и u одновременными поворотами и переводит векторы скоростей (а значит, и решения) системы (2.6) в себя.

2. Группа $G_2 = \mathbb{R}_+$ действует масштабированием: пусть $\lambda \in \mathbb{R}_+$; тогда $z_k \mapsto \lambda^{2q-k+1} z_k$. На самом деле вектор скорости системы (2.6) удлиняется в λ раз при этом действии. Однако интегральные кривые по-прежнему переходят в интегральные кривые (только скорость движения по ним возрастает в λ раз).

ТЕОРЕМА 3. *Рассмотрим любой набор двумерных плоскостей $L_m \subseteq V_{j_m}$, $m = 1, \dots, N$, где V_{j_m} – какие-то различные⁶ собственные подпространства формы C . Если набор собственных значений $\lambda_{j_1}, \dots, \lambda_{j_N}$ формы C удовлетворяет условию*

$$\frac{P_q(\alpha_{j_1})}{\lambda_{j_1}} = \frac{P_q(\alpha_{j_2})}{\lambda_{j_2}} = \dots = \frac{P_q(\alpha_{j_N})}{\lambda_{j_N}} = \mu$$

для каких-то различных α_{j_m} , то любая траектория вида

$$\begin{aligned} z_1 &= \sum_{m=1}^N b_m t^{2q} \exp\{\pm i\alpha_{j_m} \ln |t|\} y_m, \\ u &= \mu \sum_{m=1}^N b_m \exp\{\pm i\alpha_{j_m} \ln |t|\} y_m \end{aligned} \quad (2.7)$$

⁶Случай $N = 1$ не исключается. При $N = 1$ подойдет любое собственное значение λ_j формы C , лишь бы $\dim V_j \geq 2$.

является оптимальной для задачи (2.1) при любом выборе единичных векторов $y_m \in L_m$ и ненулевых чисел $b_m \in \mathbb{R}$, лишь бы $\mu^2 \sum_{m=1}^N b_m^2 = 1$.

Более того, таким способом описываются все возможные (с точностью до сдвига по времени) оптимальные траектории задачи (2.1), не покидающие какую-либо фиксированную орбиту группы $G = G_1 \times G_2$.

Отметим, что в решениях (2.7) управление движется по обмотке клиффордова тора $(L_1 \times \cdots \times L_N) \cap \{|u| = 1\}$ и проходит ее целиком⁷ за конечное время. Сама траектория $x(t)$ представляет собой соответствующую логарифмическую спираль, которая тоже проходится за конечное время.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3. Поскольку задача (2.1) является выпуклой, то принцип максимума является также и достаточным условием оптимальности. Таким образом, любая траектория принципа максимума, приходящая в начало координат, является оптимальной.

Без ограничения общности будем считать, что базис в V согласован с разложением $V = V_1 \oplus \cdots \oplus V_s$, т.е. $z = (w^1, \dots, w^s)$, где $z \in V$ и $w^j \in V_j$. Действие группы G на z_k определяет представление (π_k обозначает оператор проектирования на k -ю компоненту прямой суммы $\bigoplus_{j=1}^{2q} V$)

$$\varphi: G = \mathbb{R}_+ \times \mathrm{SO}(V_1) \times \mathrm{SO}(V_2) \times \cdots \times \mathrm{SO}(V_s) \rightarrow \mathrm{GL}\left(\bigoplus_{j=1}^{2q} V\right),$$

$$\pi_k \varphi(\lambda, M_1, \dots, M_s) z_k = \lambda^{2q-k+1} (M_1 w_k^1, \dots, M_s w_k^s), \quad \text{где } \lambda \in \mathbb{R}_+, M_j \in \mathrm{SO}(V_j).$$

По теореме существования и единственности для обыкновенных дифференциальных уравнений интегральная кривая системы (2.6) не покинет одной фиксированной орбиты группы Ли G , если и только если в начальной точке $z = (z_1, \dots, z_{2q})$ вектор скорости системы (2.6) касается этой орбиты. Это означает, что

$$\left(z_2, \dots, z_{2q}, (-1)^{q+1} \frac{C z_1}{|z_1|} \right) \in d\varphi(T_e G).$$

Здесь $T_e G$ – касательное пространство к группе Ли G , т.е. алгебра Ли $\mathbb{R} \oplus \mathfrak{so}(V_1) \oplus \cdots \oplus \mathfrak{so}(V_s)$, где $\mathfrak{so}(V_j)$ – алгебра Ли кососимметрических форм на V_j . Вычислив $d\varphi$, получим, что для некоторых $a \in \mathbb{R}$ и $\mathfrak{m}_j \in \mathfrak{so}(V_j)$ выполняется

$$\begin{pmatrix} z_2 \\ z_3 \\ \dots \\ (-1)^{q+1} \frac{C z_1}{|z_1|} \end{pmatrix} = a \begin{pmatrix} 2q z_1 \\ (2q-1) z_2 \\ \dots \\ z_{2q} \end{pmatrix} + \begin{pmatrix} \mathfrak{m} z_1 \\ \mathfrak{m} z_2 \\ \dots \\ \mathfrak{m} z_{2q} \end{pmatrix}, \quad (2.8)$$

где $\mathfrak{m} = (\mathfrak{m}_1, \dots, \mathfrak{m}_s)$. Заметим, что $a \neq 0$, так как в противном случае уравнение (2.8) имеет только тривиальное решение $z_k = 0$. Заменив $\mathfrak{m}$ на $a \cdot \mathfrak{m}$, получаем

$$(-1)^{q+1} \frac{z_1}{a^{2q} |z_1|} = C^{-1} (2q + \mathfrak{m}) ((2q-1) + \mathfrak{m}) \cdots (1 + \mathfrak{m}) z_1 = C^{-1} Q(\mathfrak{m}) z_1. \quad (2.9)$$

⁷Точнее, ту ее половину, что соответствует положительному направлению времени.

Поскольку на z_1 еще можно подействовать масштабной группой, то остается найти все такие матрицы $\mathbf{m} \in \mathfrak{so}(V_1) \oplus \dots \oplus \mathfrak{so}(V_s)$, что у оператора, стоящего в правой части, будет действительное собственное значение знака $(-1)^{q+1}$. Итак, пусть $z = (w^1, \dots, w^s)$ – собственный вектор оператора $C^{-1}Q(\mathbf{m}) = C^{-1}(2q + \mathbf{m})((2q - 1) + \mathbf{m}) \dots (1 + \mathbf{m})$ с собственным значением μ знака $(-1)^{q+1}$. Тогда

$$Q(\mathbf{m}_j)w^j = (2q + \mathbf{m}_j)((2q - 1) + \mathbf{m}_j) \dots (1 + \mathbf{m}_j)w^j = \mu\lambda_j w^j. \quad (2.10)$$

Таким образом, либо $w^j = 0$, либо w^j – собственный вектор оператора $Q(\mathbf{m}_j)$. Исследуем собственные значения оператора из предыдущего равенства. Используя теорему о приведении кососимметрической формы, можно считать, что⁸

$$\mathbf{m}_j = \begin{pmatrix} 0 & \beta_1^j & 0 & 0 & \dots & 0 & 0 \\ -\beta_1^j & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \beta_2^j & \dots & 0 & 0 \\ 0 & 0 & -\beta_2^j & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 0 & \beta_r^j \\ 0 & 0 & 0 & 0 & \dots & -\beta_r^j & 0 \end{pmatrix}.$$

Поскольку собственные значения блочно-диагональной матрицы есть собственные значения ее блоков, то вопрос о собственных значениях сводится к вычислению собственных значений матрицы ранга 2. Более того, каждый собственный вектор w^j будет лежать в некоторой двумерной плоскости $L_j \subseteq V_j$. Воспользовавшись комплексной структурой на L_j , получаем, что многочлен⁹ $P_q(\alpha)$ из (2.4) имеет мнимую часть, равную нулю. Итак, уравнение (2.10) на плоскости L_j с учетом знаков переписывается в виде системы (2.3).

Каждый из сомножителей в формуле (2.4) является комплексным числом, аргумент которого при росте α от 0 до $+\infty$ монотонно возрастает от 0 до $\pi/2$. Следовательно, аргумент их произведения монотонно возрастает от 0 до πq . При этом если q четно, то он $[q/2]$ раз пересекает отрицательную часть действительной оси, а если q нечетно, то он $[q/2]$ раз пересекает положительную часть действительной оси.

Пусть теперь $z = (w^1, \dots, w^s)$ – набор из векторов w^j , каждый из которых либо является собственным вектором оператора $Q(\mathbf{m}_j)$, либо нулевой. Очевидно, что вектор z является собственным вектором исходного оператора $C^{-1}Q(\mathbf{m})$ тогда и только тогда, когда

$$\mu = \frac{P_q(\alpha_{j_1})}{\lambda_{j_1}} = \frac{P_q(\alpha_{j_2})}{\lambda_{j_2}} = \dots = \frac{P_q(\alpha_{j_N})}{\lambda_{j_N}},$$

⁸Последний двумерный блок в матрице $\mathbf{m}_j$ заменяется одномерным нулем, если $r = \dim V_j$ нечетно.

⁹Можно считать, что $1 \in \mathbb{C}$ – это единичная (2×2) -матрица, а $i \in \mathbb{C}$ – (2×2) -матрица с 1 и -1 на побочной диагонали.

где $j_1, \dots, j_N$ – номера ненулевых w^j . Если обозначить $w^{j_m} = b_m y_m$, где y_m – векторы единичной длины, а b_m – ненулевые числа, то мы получим траектории, заявленные в формулировке теоремы (условие b_m получается прямой подстановкой z_1 в (2.6)).

На каждой оптимальной траектории (2.7) управление пробегает обмотку клиффордова тора $\mathbb{T}^N = (L_1 \times \dots \times L_N) \cap \{|u| = 1\}$ и выходит за конечное время на особый режим $x = u = 0$. Тор $\mathbb{T}^N$ вложен в сферу $S^{n-1} = \{|u| = 1\} \subseteq V$ единичного радиуса. Более того, если значения $\alpha_{j_1}, \dots, \alpha_{j_N}$ несоизмеримы над $\mathbb{Q}$, то полученная обмотка тора $\mathbb{T}^N$ является всюду плотной.

В статье [1] доказано, что в задаче (2.1) при $q = 4$ возникают семейства оптимальных траекторий с управлением в виде иррациональной всюду плотной обмотки тора. Положительный ответ на вопрос о линейной независимости корней $\{\alpha_{2j-1}\}_{j=1}^{\lfloor q/2 \rfloor}$ полинома (2.4) над полем рациональных чисел для произвольного q позволит получить описанную картину с иррациональной обмоткой любого k -мерного тора.

Заметим, что многочлен $P_q(\alpha)$ имеет очень специфичную природу коэффициентов. Это дает нам смелость высказать следующую гипотезу.

ГИПОТЕЗА 1. Корни $\{\alpha_{2j-1}\}_{j=1}^{\lfloor q/2 \rfloor}$ многочлена $\text{Im } P_q(\alpha)$ линейно независимы над полем рациональных чисел $\mathbb{Q}$.

Доказательству гипотезы 1 для некоторых конкретных значений q посвящен следующий параграф.

§ 3. Доказательство линейной независимости

3.1. Итак, рассмотрим многочлен $P_n(x) = \prod_{j=1}^{2n} (x + j)$. В [1; теорема 6.2] показано, что существует ровно $\lfloor n/2 \rfloor$ решений следующей системы:

$$\frac{1}{x} \text{Im } P_n(ix) = 0, \quad (3.1)$$

$$(-1)^{n+1} \text{Re } P_n(ix) > 0. \quad (3.2)$$

В доказательстве той же теоремы установлена сепарабельность многочленов $F_n(x) := \frac{1}{x} \text{Im } P_n(ix)$ и $G_n(x) := \text{Re } P_n(ix)$.

Непосредственно из определения многочленов $F_n(x)$ и $G_n(x)$ следует, что существуют многочлены $f_n(x), g_n(x) \in \mathbb{Z}[x]$ такие, что

$$F_n(x) = f_n(x^2), \quad G_n(x) = g_n(x^2). \quad (3.3)$$

Поскольку многочлены $F_n(x)$ и $G_n(x)$ сепарабельны, то из (3.3) непосредственно следует сепарабельность многочленов $f_n(x)$ и $g_n(x)$. Многочлен $f_n(x)$ имеет степень $n - 1$, а многочлен $g_n(x)$ – степень n .

ЛЕММА 1. Пусть $a(x) \in k[x]$ – сепарабельный многочлен степени $n - 1$, где $n \in \mathbb{Z}_{\geq 5}$. Пусть $\text{Gal}_k(a) \cong S_{n-1}$ либо $\text{Gal}_k(a) \cong A_{n-1}$. В этом случае любые $\lfloor n/2 \rfloor$ корней многочлена $A(x) := a(x^2)$, квадраты которых попарно различны, линейно независимы над k .

ДОКАЗАТЕЛЬСТВО. Выберем произвольную систему из $[n/2]$ корней многочлена $A(x)$, квадраты любых двух элементов которой различны. Структура корней многочлена $A(x)$ имеет вид $\{\pm v_i\}_{i=1}^{n-1}$. С точностью до нумерации корней без ограничения общности считаем, что была выбрана система

$$v_1, v_2, \dots, v_{[n/2]}. \quad (3.4)$$

Пусть многочлен $A(x)$ оказался приводимым над полем k . Выберем тогда произвольным образом неприводимую компоненту $A_1(x) \in k[x]$. В силу неприводимости $A_1(x)$ над k группа Галуа $\text{Gal}_k(A_1)$ действует на корнях многочлена $A_1(x)$ транзитивно. Так как множеством $\{v_i^2\}_{i=1}^{n-1}$ исчерпывается система корней многочлена $a(x)$, то из условия на группу $\text{Gal}_k(a)$ следует, во-первых, что ни для какого индекса $i = 1, \dots, n-1$ оба элемента v_i и $-v_i$ не могут быть корнями многочлена $A_1(x)$ одновременно, а во-вторых, существует однозначно определенный набор знаков $\{\gamma_i\}_{i=1}^{n-1} \subset \{-1, 1\}$ такой, что многочлен $A_1(x)$ в своем поле разложения распадается на линейные множители вида

$$A_1(x) = \prod_{i=1}^{n-1} (x - \gamma_i v_i).$$

В частности, $\text{Gal}_k(A) = \text{Gal}_k(A_1) \cong S_{n-1}$. Если теперь $\{v_{ij}\}_{j=1}^r$ — максимальная линейно независимая подсистема в системе (3.4), то ($r \geq 1$, ибо многочлен $a(x)$ неприводим над k по условию) либо $r = [n/2]$, либо

$$v_{i_{r+1}} = \alpha_1 v_{i_1} + \dots + \alpha_r v_{i_r} \quad (3.5)$$

для однозначно определенного набора $\{\alpha_i\}_{i=1}^r$ элементов поля k . Однако существует элемент $\sigma \in \text{Gal}_k(A)$ такой, что

$$v_{ij}^\sigma = v_{ij} \quad \forall j = 1, \dots, r, \quad v_{i_{r+1}}^\sigma = v_{i_n}.$$

Тем самым, $v_{i_{r+1}} = v_{i_n}$ вопреки сепарабельности многочлена $A(x)$.

Предположим теперь, что $s \in \mathbb{Z}_{\geq 2}$ и для всех $t = 1, \dots, s$ многочлен

$$A_t(x) := \frac{A(x)}{\prod_{i=1}^{t-1} (x^2 - v_i^2)}$$

неприводим над полем $k_t := k(v_1, \dots, v_{t-1})$ (при $t = 1$ полагаем $A_1(x) := A(x)$, $k_1 := k$), а многочлен $A_{s+1}(x)$ приводим над полем k_{s+1} . В этом случае любая подсистема из s корней многочлена $A(x)$, квадраты любых двух элементов которой различны, линейно независима над k . В самом деле, в противном случае мы бы получили противоречие с выбором числа s . Если $s \geq [n/2]$, то доказательство закончено. Если же $s < [n/2]$ и при этом группа $\text{Gal}_{k_{s+1}}(a_{s+1})$, где

$$a_t(x) := \frac{a(x)}{\prod_{i=1}^{t-1} (x - v_i^2)}, \quad a_1(x) := a(x), \quad t = 1, \dots, s,$$

является l -транзитивной для

$$l \geq \left\lceil \frac{n}{2} \right\rceil - s, \quad (3.6)$$

то, рассуждая таким же образом, как и для $s = 1$, находим элемент $\sigma \in \text{Gal}_{k_{s+1}}(a_{s+1})$, оставляющий на месте уже выбранную линейно независимую подсистему корней в системе (3.4) и меняющий местами элемент v_n с некоторым другим элементом системы (3.4), линейно выраженным над k_{s+1} через текущую линейно независимую подсистему. Вновь мы получаем противоречие с сепарабельностью многочлена $A(x)$.

Теперь нам осталось оценить степень транзитивности действия группы $\text{Gal}_{k_{s+1}}(a_{s+1})$ на корнях многочлена $a_{s+1}(x)$. Положим

$$K_{t+1} := k(v_1^2, \dots, v_t^2), \quad K_1 := k.$$

Легко видеть, что расширение k_{s+1}/K_{s+1} есть расширение Галуа с элементарной абелевой 2-группой Галуа. Заметим, что

$$K_{s+1} \subseteq k_{s+1} \cap K_n \subseteq k_{s+1},$$

откуда, в частности, следует, что расширение $k_{s+1} \cap K_n / K_{s+1}$ является расширением Галуа. Поэтому группа $\text{Gal}(K_n / k_{s+1} \cap K_n)$ является нормальной подгруппой в группе $\text{Gal}(K_n / K_{s+1})$. Однако поскольку поле разложения многочлена $a_{s+1}(x)$ над k_{s+1} есть композит $K_n \cdot k_{s+1}$, то имеет место изоморфизм

$$\text{Gal}_{k_{s+1}}(a_{s+1}) = \text{Gal}(K_n \cdot k_{s+1} / k_{s+1}) \cong \text{Gal}(K_n / k_{s+1} \cap K_n).$$

Это означает, что группа $\text{Gal}_{k_{s+1}}(a_{s+1})$ является с точностью до изоморфизма нормальной подгруппой в группе $\text{Gal}(K_n / K_{s+1})$, факторгруппа по которой есть элементарная абелева 2-группа; при этом $\text{Gal}(K_n / K_{s+1})$ в свою очередь изоморфна либо S_{n-1-s} , либо A_{n-1-s} . Так как в знакопеременной группе степени ≥ 3 нет собственных нормальных подгрупп, факторгруппа по которым является 2-группой, то степень транзитивности группы $\text{Gal}_{k_{s+1}}(a_{s+1})$ как группы перестановок корней многочлена $a_{s+1}(x)$ не меньше, чем $n-1-s-2 = n-s-3$.

Итак, в наихудшем случае мы получаем степень транзитивности группы $\text{Gal}_{k_s \cap K_n}(a_s)$, равную $n-s-3$. Вспомним, что нам нужна оценка (3.6). Поэтому необходимо установить справедливость оценки

$$\left\lceil \frac{n}{2} \right\rceil - s \leq n - s - 3. \quad (3.7)$$

Но такая оценка справедлива для $n \in \mathbb{Z}_{\geq 5}$.

Лемма 1 доказана.

ЗАМЕЧАНИЕ 1. Лемма 1 показывает на самом деле, что для решения проблемы линейной независимости над полем $\mathbb{Q}$ чисел, удовлетворяющих системе (3.1), (3.2), достаточно, чтобы группа Галуа многочлена $f_n(x)$ над полем $\mathbb{Q}$ действовала на его корнях l -транзитивно (лишь бы при добавлении очередного

корня многочлена $f_n(x^2)$ степень транзитивности уменьшалась не более чем на единицу), где $l \geq [n/2]$. Если, однако, $[n/2] > 5$, то по известной теореме К. Жордана (см. [5; гл. 1, § 3, п. 3]) в качестве искомым групп могут выступать лишь S_{n-1} и A_{n-1} . При натуральных n , удовлетворяющих противоположному неравенству (а это возможно лишь при $n \leq 11$), группа Галуа многочлена $f_{n-1}(x)$ над полем $\mathbb{Q}$ оказывается изоморфной S_{n-1} . Этот факт будет доказан в п. 3.3. Поэтому в любом случае доказательство линейной независимости, основанное на рассуждениях леммы 1, применимо (по крайней мере в интересующем нас случае), лишь когда группа Галуа многочлена $a(x)$ над полем k изоморфна либо S_{n-1} , либо A_{n-1} .

3.2. О линейной независимости корней некоторых ортогональных многочленов. Приведем несколько интересных примеров использования леммы 1. Все эти примеры так или иначе связаны с ортогональными многочленами.

ОПРЕДЕЛЕНИЕ 1. Многочлены

$$L_n^{(\alpha)}(x) := (-1)^n \sum_{j=0}^n \binom{n+\alpha}{n-j} \frac{(-x)^j}{j!},$$

определенные для всех действительных значений $\alpha \in \mathbb{R}$, называются *обобщенными многочленами Чебышёва–Лагерра*.

Для обобщенных многочленов Чебышёва–Лагерра справедлив следующий результат.

ТЕОРЕМА 4. Пусть $\alpha \in \mathbb{Q} \setminus \mathbb{Z}_{<0}$ либо $\alpha = 1 - n - r$ для некоторого $r \in \mathbb{Z}_{\geq 0}$. Тогда для всех натуральных n , кроме, быть может, конечного числа, любая система из $[(n+1)/2]$ корней многочлена $L_n^{(\alpha)}(x^2)$, квадраты любых двух элементов которой различны, линейно независима над $\mathbb{Q}$.

ДОКАЗАТЕЛЬСТВО. Согласно теореме Хаджира (см. [6; теорема 1.3]) для любого фиксированного $r \in \mathbb{Z}_{\geq 0}$ все многочлены $L_n^{(1-n-r)}(x)$, кроме, быть может, конечного числа, имеют над полем $\mathbb{Q}$ группу Галуа, содержащую A_n в качестве подгруппы.

Согласно теореме Филазеты–Лама–Хаджира (см. [7; теорема 1.1]) для любого фиксированного $\alpha \in \mathbb{Q} \setminus \mathbb{Z}_{<0}$ все многочлены $L_n^{(\alpha)}(x)$, кроме, быть может, конечного числа, имеют над полем $\mathbb{Q}$ группу Галуа, содержащую A_n в качестве подгруппы.

Результат теперь получается применением леммы 1. Теорема доказана.

Разберем еще одну серию примеров. Пусть $H_m(x)$ обозначает классический ортогональный многочлен Чебышёва–Эрмита степени m .

ТЕОРЕМА 5. При $n > 12$ многочлены $H_{2n}(x)$ и $\frac{1}{x}H_{2(n+1)}(x)$ удовлетворяют следующему свойству: для каждого указанного многочлена любая подсистема из $[(n+1)/2]$ его корней, квадраты любых двух элементов которой различны, линейно независима над $\mathbb{Q}$.

ДОКАЗАТЕЛЬСТВО. Пусть $K_n^0(x)$, $K_n^1(x)$ – многочлены степени n с целыми коэффициентами такие, что $H_{2n}(x) = K_n^0(x)$ и $H_{2(n+1)}(x) = xK_n^1(x)$. Тогда согласно результатам Шура (см. [5; гл. 5, § 4, п. 2]) при $n > 12$ группы Галуа многочленов $K_n^0(x)$ и $K_n^1(x)$ изоморфны S_n . Остается применить лемму 1. Теорема доказана.

3.3. Обмотка тора. Согласно лемме 1 и результатам из § 2 для существования оптимального решения задачи (2.1) в виде всюду плотной обмотки k -мерного тора для любого $k \leq [n/2]$ нам достаточно установить, что группа Галуа многочлена $f_n(x)$ из (3.3) над полем $\mathbb{Q}$ изоморфна либо S_n , либо A_n при $n \geq 5$. Заметим, что в § 2 данный результат установлен лишь для $n = 4$ (это минимальная размерность, для которой оптимальное управление неоднородно априори).

Мы покажем (с помощью системы компьютерной алгебры Maple V), что $\text{Gal}_{\mathbb{Q}}(f_n) \cong S_{n-1}$ для всех $n = 5, \dots, 15$.

Разберем случай $n = 6$. При таком предположении можно привести доказательство изоморфизма $\text{Gal}_{\mathbb{Q}}(f_6) \cong S_5$ практически без использования Maple V.

ЛЕММА 2. *Многочлен $f_6(x)$ неприводим над $\mathbb{Q}$.*

ДОКАЗАТЕЛЬСТВО. Из непосредственного определения многочленов $f_n(x)$ и $g_n(x)$, указанного в (3.3), следует рекуррентная зависимость

$$\begin{cases} f_{n+1}(x) = (-x + (2n+1)(2n+2))f_n(x) + (4n+3)g_n(x), \\ g_{n+1}(x) = (-x + (2n+1)(2n+2))g_n(x) - (4n+3)xf_n(x). \end{cases} \quad (3.8)$$

С помощью формулы (3.8) можно даже вручную довольно быстро вычислить редукцию многочлена $f_6(x)$ по модулю 29. После приведения данной редукции к унитарному виду получаем

$$\bar{f}_6(x) = x^5 + 10x^4 + 5x^3 + 4x^2 + 3x + 13 \in \mathbb{F}_{29}[x]. \quad (3.9)$$

Неприводимость многочлена (3.9) над полем $\mathbb{F}_{29}$ может быть установлена, например, вычислением наибольшего общего делителя $(x^{29^2} - x, \bar{f}_6(x)) = 1$ или применением алгоритма Берлекэмпса. Отсюда уже следует неприводимость многочлена $f_6(x)$ над полем $\mathbb{Q}$, так как старший коэффициент многочлена $f_6(x)$ взаимно прост с 29.

Теперь нам необходимо доказать, что дискриминант многочлена $f_6(x)$ делится на 563 в нечетной степени. Это, пожалуй, единственное место, где мы используем компьютерные вычисления.

ЛЕММА 3. *Кратность вхождения простого числа 563 в дискриминант многочлена $f_6(x)$ нечетна.*

ДОКАЗАТЕЛЬСТВО. Вычисление дискриминанта многочлена $f_6(x)$ в Maple V дает выражение

$$D(f_6) = 2^{22} \cdot 3^{14} \cdot 5^4 \cdot 7^4 \cdot 13^{12} \cdot 563 \cdot 466267 \cdot 33137953 \cdot 18669593,$$

откуда непосредственно получаем требуемое.

Сформулируем важное

ОПРЕДЕЛЕНИЕ 2. Рассмотрим точную последовательность конечных групп

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\varphi} F = \text{Gal}(K/k) \longrightarrow 1. \quad (3.10)$$

Если существует гомоморфизм $\omega: \text{Gal}(\bar{k}_{\text{sep}}/k) \rightarrow G$ такой, что $\varphi \circ \omega$ является каноническим эпиморфизмом ограничения автоморфизмов поля $\bar{k}_{\text{sep}}$ над k до автоморфизмов группы F , то говорят, что задача погружения расширения (3.10) разрешима.

Нам понадобится следующий замечательный результат.

ТЕОРЕМА 6 (Б. Б. Лурье). Пусть p – простое число, сравнимое с единицей по модулю 4. Пусть $f(x) \in k[x]$ – неприводимый сепарабельный многочлен степени p над полем k характеристики, отличной от 2. Предположим, далее, что задача погружения расширения $k(\sqrt{D(f)})/k$ в расширение с циклической группой Галуа порядка $(p-1)_2$ неразрешима. Тогда группа $\text{Gal}_k(f)$ также неразрешима.

Доказательство этой теоремы можно найти в [8].

ТЕОРЕМА 7. Группа Галуа многочлена $f_6(x)$ над полем $\mathbb{Q}$ изоморфна S_5 .

ДОКАЗАТЕЛЬСТВО. Согласно лемме 2 многочлен $f_6(x)$ степени 5 неприводим над полем $\mathbb{Q}$. Если мы покажем неразрешимость группы $\text{Gal}_{\mathbb{Q}}(f_6)$, то в силу леммы 3 $\text{Gal}_{\mathbb{Q}}(f_6) \cong S_5$. Согласно теореме 6 нам достаточно доказать неразрешимость задачи погружения, связанной с точной последовательностью

$$1 \longrightarrow Z_2 \longrightarrow Z_4 \xrightarrow{\varphi} \text{Gal}(\mathbb{Q}(\sqrt{D(f_6)})/\mathbb{Q}). \quad (3.11)$$

Хорошо известно, что для неразрешимости задачи (3.11) необходима и достаточна невозможность выразить дискриминант $D(f_6)$ в виде суммы двух квадратов элементов поля $\mathbb{Q}$. Доказательство можно найти в [9; гл. 1, § 1].

Итак, если дискриминант $D(f_6)$ представим в виде суммы двух квадратов элементов поля $\mathbb{Q}$, то из хорошо известных свойств символа Гильберта вытекает, что норменный вычет $\left(\frac{563, -1}{563}\right)$ должен равняться единице. Однако

$$\left(\frac{563, -1}{563}\right) = -1,$$

ибо

$$\left(\frac{-1}{563}\right) = (-1)^{(563-1)/2} = -1$$

вопреки предположению. Теорема доказана.

Для случаев $n \in \{5, 7, 8, 9, 10, 11, 12, 13, 14, 15\}$ воспользуемся следующим хорошо известным результатом.

ПРЕДЛОЖЕНИЕ 1. Пусть дан многочлен $f(x) \in \mathbb{Z}[x]$ степени n . Пусть найдены простые числа p_1, p_2, p_3 , не делящие дискриминант $D(f)$ и старший коэффициент многочлена $f(x)$. Пусть многочлен $f(x)$ неприводим по модулю p_1 , разлагается по модулю p_2 в произведение линейного и неприводимого множителей степени $n - 1$, разлагается по модулю p_3 на $n - 2$ линейных и один квадратичный множители. Тогда $\text{Gal}_{\mathbb{Q}}(f) \cong S_n$.

Доказательство этого предложения немедленно следует из классической теоремы Дедекинда (см. [5; гл. 5, § 4, п. 3, теорема 5]), а также из известного факта об образующих симметрической группы (см. [5; гл. 5, § 4, п. 2, предложение 1]). Гораздо более важен тот факт, что коль скоро такие простые числа существуют, то их бесконечно много согласно теореме Чеботарева о плотности (см. [10; теорема 1.1]). Более того, из теоремы Чеботарева следует, что наиболее трудно отыскать подходящее простое число типа p_3 , так как в предположении изоморфизма $\text{Gal}_{\mathbb{Q}}(f) \cong S_n$ при достаточно большом N на каждые N простых чисел будет приходиться лишь $1/(2(n-3)!)$ чисел типа p_3 , в то время как доля чисел типов p_1 и p_2 будет $1/(n-1)$ и $1/(n-2)$ соответственно (см. [11; предложение 4.1.10]).

Приведем таблицу (составленную с помощью Maple V) наименьших простых чисел типов p_1, p_2, p_3 , подходящих согласно предложению 1 для доказательства изоморфизма $\text{Gal}_{\mathbb{Q}}(f_n) \cong S_{n-1}$:

n	p_1	p_2	p_3
5	23	19	17
6	29	23	19
7	37	73	> 200
8	37	41	11
9	83	67	13
10	79	67	> 200
11	61	103	17
12	67	73	17
13	59	103	19
14	67	163	> 200
15	101	79	> 200

Как видно из таблицы, с помощью предложения 1 и леммы 1 можно обосновать существование всюду плотной обмотки $[n/2]$ -мерного тора в качестве оптимального решения задачи управления (3.1) при $n \in \{5, \dots, 15\} \setminus \{7, 10, 14, 15\}$. Случай $n = 7$ можно обосновать применением соответствующей команды подсчета группы Галуа многочлена $f_7(x)$ в Maple V.

Разберем случай $n = 10$.

ПРЕДЛОЖЕНИЕ 2. Группа $\text{Gal}_{\mathbb{Q}}(f_{10})$ изоморфна S_9 .

ДОКАЗАТЕЛЬСТВО. Рассмотрим редукции многочлена $f_{10}(x)$ по модулям

$$29, 37, 43, 67, 79, 157.$$

С помощью рекуррентных формул (3.8) и алгоритма Берлекэмпна легко установить применением теоремы Дедекинда (см. [5; гл. 5, § 4, п. 3, теорема 5]), что группа $\text{Gal}_{\mathbb{Q}}(f_{10})$ имеет при каноническом отождествлении ее с подгруппой в S_9 подстановки с цикловой структурой: 3-цикл, 7-цикл, произведение независимых циклов длин 4 и 5, 8-цикл, 9-цикл, 6-цикл (цикловые структуры приведены в порядке, соответствующем набору выбранных модулей для редукции). Возводя произведение циклов длин 4 и 5 в четвертую и пятую степени, мы получим существование в группе $\text{Gal}_{\mathbb{Q}}(f_{10})$ 5-циклов и 4-циклов соответственно. В частности, группа $\text{Gal}_{\mathbb{Q}}(f_{10})$ действует на корнях многочлена $f_{10}(x)$ 7-транзитивно. В самом деле, стабилизатор k -корней содержит $(9 - k)$ -цикл при $k = 0, \dots, 6$ и является при этом группой перестановок степени $9 - k$.

Так как 7-транзитивная группа перестановок степени 9 обязательно содержит A_9 в качестве подгруппы, то предложение полностью доказано.

Рассмотрим случаи $n \in \{14, 15\}$. Нам достаточно показать, что для каждого такого n существует простое число, редукция по модулю которого многочлена $f_n(x)$ распадается на $n - 2$ линейных и один квадратичный множители.

В случае $n = 14$ сделаем редукцию по модулю 41; мы получим тогда, что многочлен $f_{14}(x)$ распадется в произведение девяти линейных, квадратичного и кубического множителей. В частности, $\text{Gal}_{\mathbb{Q}}(f_{14})$ будет иметь подстановку циклового типа $(3, 2)$, но тогда куб данной подстановки и даст необходимую транспозицию. В силу теоремы Чеботарева о плотности (см. [10; теорема 1.1]) найдется и искомое простое число, редукция по модулю которого даст такое цикловое разложение.

В случае $n = 15$ сделаем редукцию по модулю 67; мы получим тогда, что многочлен $f_{15}(x)$ распадется в произведение двух линейных множителей, множителя степени 10 и множителя степени 3. В частности, $\text{Gal}_{\mathbb{Q}}(f_{15})$ будет иметь подстановку циклового типа $(10, 3)$. Но тогда в группе $\text{Gal}_{\mathbb{Q}}(f_{15})$ будет содержаться и 10-цикл. Так как $10 = 5 \cdot 2$, то искомая транспозиция найдется.

Итак, нами доказан следующий результат.

ТЕОРЕМА 8. *При каждом $n = 4, \dots, 15$ в соответствующей задаче оптимального управления (3.1) (при надлежащем выборе согласно теореме 3 матрицы C) существует оптимальное решение, управление которого проходит всюду плотную обмотку k -мерного тора ($k \leq [n/2]$). Такая обмотка (точнее, ее половина, соответствующая положительному направлению времени) целиком проходится за конечное время. Оптимальное решение представляет собой логарифмическую спираль, которая также проходится за конечное время.*

ЗАМЕЧАНИЕ 2. Предложение 2 вместе с теоремой К. Жордана показывает, что с помощью достаточно небольшого набора простых чисел можно надеяться

доказать существование вложения $A_n \hookrightarrow \text{Gal}_{\mathbb{Q}}(f_{n-1})$ для более репрезентативного набора чисел n . В работе [11] приводятся достаточно быстрые способы определения цикловой структуры с помощью редукции по простому модулю p со временной сложностью $O(n^4 + n^2 \log p)$.

К сожалению, авторам не удалось доказать даже неприводимость над $\mathbb{Q}$ многочленов $f_n(x)$ для бесконечной серии натуральных n . Тем не менее разбор случаев $n \leq 15$ в настоящей работе, а также факт о том, что “почти все” многочлены степени m с рациональными коэффициентами имеют группу Галуа, изоморфную S_m , дает возможность высказать следующую гипотезу.

ГИПОТЕЗА 2. Группа Галуа многочлена $f_n(x)$ при всех натуральных n изоморфна S_{n-1} .

Список литературы

- [1] М. И. Зеликин, Л. В. Локуцкий, Р. Хильдебранд, “Геометрия окрестностей особых экстремалей в задачах с многомерным управлением”, *Математическая теория управления и дифференциальные уравнения*, Сборник статей. К 90-летию со дня рождения академика Евгения Фроловича Мищенко, Тр. МИАН, **277**, МАИК, М., 2012, 74–90; англ. пер.: M. I. Zelikin, L. V. Lokutsievskiy, R. Hildebrand, “Geometry of neighborhoods of singular trajectories in problems with multidimensional control”, *Proc. Steklov Inst. Math.*, **277** (2012), 67–83.
- [2] I. Kupka, “Generic properties of extremals in optimal control problems”, *Differential geometric control theory* (Houghton, MI, 1982), *Progr. Math.*, **27**, Birkhäuser, Boston, MA, 1983, 310–315.
- [3] M. I. Zelikin, V. F. Borisov, *Theory of chattering control with applications to astronautics, robotics, economics, and engineering*, Systems Control Found. Appl., Birkhäuser, Boston, MA, 1994.
- [4] А. А. Милютин, А. Е. Илютович, Н. П. Осмоловский, С. В. Чуканов, *Оптимальное управление в линейных системах*, Наука, М., 1993.
- [5] А. И. Кострикин, *Введение в алгебру. Часть III. Основные структуры алгебры*, Физматлит, М., 2001.
- [6] F. Hajir, “Algebraic properties of a family of generalized Laguerre polynomials”, *Canad. J. Math.*, **61**:3 (2009), 583–603.
- [7] F. Hajir, “On the Galois group of generalized Laguerre polynomials”, *J. Théor. Nombres Bordeaux*, **17**:2 (2005), 517–525.
- [8] Б. Б. Лурье, “Критерий неразрешимости в радикалах уравнения простой степени”, *Докл. РАН*, **388** (2003), 447–448; англ. пер.: B. B. Lur’e, “A criterion for unsolvability by radicals of an equation of prime degree”, *Dokl. Math.*, **67**:1 (2003), 42–43.
- [9] В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа*, Наука, М., 1990; англ. пер.: V. V. Ishkhanov, B. B. Lur’e, D. K. Faddeev, *The embedding problem in Galois theory*, Transl. Math. Monogr., **165**, Amer. Math. Soc., Providence, RI, 1997.
- [10] Н. В. Дуров, “Вычисление группы Галуа многочлена с рациональными коэффициентами”, *Вопросы теории представлений алгебр и групп*. 11, Зап. научн. сем. ПОМИ, **319**, ПОМИ, СПб., 2004, 117–198; англ. пер.: N. V. Durov, “Computation of the Galois group of a polynomial with rational coefficients. I”, *J. Math. Sci. (N. Y.)*, **134**:6 (2006), 2511–2548.

- [11] Н. В. Дуров, “Вычисление группы Галуа многочлена с рациональными коэффициентами. II”, *Вопросы теории представлений алгебр и групп.* 12, Зап. научн. сем. ПОМИ, **321**, ПОМИ, СПб., 2005, 90–135; англ. пер.: N.V. Durov, “Computation of the Galois group of a polynomial with rational coefficients. II”, *J. Math. Sci. (N. Y.)*, **136**:3 (2006), 3880–3907.

Михаил Ильич Зеликин
(Mikhail I. Zelikin)

Механико-математический факультет
Московского государственного университета
им. М. В. Ломоносова
E-mail: mzelikin@mtu-net.ru

Поступила в редакцию
17.01.2013 и 09.04.2013

Денис Дмитриевич Киселев
(Denis D. Kiselev)

Механико-математический факультет
Московского государственного университета
им. М. В. Ломоносова
E-mail: denmexmath@yandex.ru

Лев Вячеславович Локуциевский
(Lev V. Lokutsievskiy)

Механико-математический факультет
Московского государственного университета
им. М. В. Ломоносова
E-mail: lion.lokut@gmail.com