Применение теории Галуа к оптимальному управлению

Д.Д. Киселев
Всероссийская академия внешней торговли
г. Москва
denmexmath@yandex.ru

Аннотация

Мы исследуем линейную независимость над $\mathbb{Q}$ элементов из некоторого специального $[n/2]$-элементного подмножества корней многочлена $\operatorname{Im}(ix+1)\dots(ix+2n)$. Исследования находят применение в теории оптимального синтеза траекторий в обобщенной задаче Фуллера: мы показываем, что существует обобщенная задача Фуллера, в которой для любого натурального $k \leqslant 249\,994\,914$ существует оптимальное управление, за конечное время пробегающее половину всюду плотной обмотки k-мерного тора, отвечающей положительному направлению времени. В предположении неприводимости многочленов Зеликина–Локуциевского над $\mathbb{Q}$ для почти всех простых степеней, принадлежащих арифметической прогрессии $\{26 + 69k \mid k \in \mathbb{N}\}$, показывается, что в качестве k может быть взято сколь угодно большое натуральное число.

1 Введение

Рассмотрим обобщенную задачу Фуллера вида

$$J(x) = \int_0^{+\infty} \langle x, Cx \rangle \, dt \to \min \tag{1}$$

на траекториях управляемой системы

$$\begin{aligned} &|x^{(n)}| \leqslant 1, \quad x \in V; \\ &x^{(k)}(0) = x_k^0,\ 0 \leqslant k \leqslant n-1, \end{aligned}$$

где V – конечномерное евклидово пространство достаточно высокой размерности M (можно взять любое $M > 2n$) со скалярным произведением $\langle \cdot, \cdot \rangle$, а C – некоторый невырожденный самосопряженный линейный оператор. Функция $x(t)$ считается абсолютно непрерывной вместе со своими $n-1$ производными. Управление $u(t) = x^{(n)}(t) \in L_1(0; +\infty)$. Поскольку в указанных предположениях задача (1) является выпуклой, то существование глобально оптимального решения равносильно разрешимости системы принципа максимума Понтрягина; при любых начальных условиях такое решение существует и единственно (см. [1]). Ясно, что для минимизации интеграла в (1) необходимо как можно быстрее выйти на особых режим $x = u = 0$; весь вопрос в том, насколько сложным может быть соответствующее управление.

Copyright © by the paper's authors. Copying permitted for private and academic purposes.

In: A.A. Makhnev, S.F. Pravdin (eds.): Proceedings of the International Youth School-conference «SoProMat-2017», Yekaterinburg, Russia, 06-Feb-2017, published at http://ceur-ws.org

Определим $[n/2]$-элементное множество $B \subset \mathbb{R}$ решений системы

$$\begin{cases} \operatorname{Im} \prod_{j=1}^{2n} (ix+j) = 0, \\ (-1)^{n-1} \operatorname{Re} \prod_{j=1}^{2n} (ix+j) > 0, \\ x > 0. \end{cases} \tag{2}$$

Всюду ниже примем обозначение

$$P_n(x) = (x+1)\dots(x+2n). \tag{3}$$

В работе [1] было установлено следующее утверждение

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

$$\frac{P_n(i\alpha_{j_1})}{\lambda_{j_1}} = \frac{P_n(i\alpha_{j_2})}{\lambda_{j_2}} = \dots = \frac{P_n(i\alpha_{j_N})}{\lambda_{j_N}} = \mu.$$

для каких-то различных $\alpha_{j_m} \in B$, то любое управление вида

$$u = \sum_{m=1}^{N} \exp\Big\{\pm i\alpha_m \ln|t|\Big\} y_m \tag{4}$$

является оптимальным для задачи (1) *при любом выборе единичных векторов $y_m \in L_m$ в следующем смысле: при любом выборе единичных векторов $y_m \in L_m$ и числа $T > 0$ управление, заданное формулой* (4) *на отрезке* $[0, T]$*, и равное нулю вне его, является единственным оптимальным управлением в задаче* (1) *для некоторых начальных условий* $(x_0^0, \dots, x_{n-1}^0)$.

Отметим, что в (4) управление движется по обмотке клиффордова тора $\mathbb{T}^N = (L_1 \times \ldots \times L_N) \cap \{|u| = 1\}$, проходит ее половину, соответствующую положительному направлению времени, причем за конечное время выходит на особый режим $x = u = 0$. Сама траектория $x(t)$ представляет собой соответствующую обобщенную логарифмическую спираль, которая тоже проходится за конечное время. Более того, если значения $\alpha_{j_1}, \dots, \alpha_{j_N}$ линейно независимы над $\mathbb{Q}$, то полученная обмотка тора $\mathbb{T}^N$ является всюду плотной.

Таким образом, возникает следующая задача

Проблема 1. *Пусть V_B – $\mathbb{Q}$-линейная оболочка, порожденная элементами множества B из* (2)*. Какой может быть размерность* $\dim_{\mathbb{Q}} V_B$*?*

Рассмотрим многочлен[2] $f_n(x) \in \mathbb{Z}[x]$ степени $n-1$, определяемый следующим образом:

$$x f_n(x^2) = \operatorname{Im} P_n(ix). \tag{5}$$

В работе [1] было выведено достаточное условие равенства $\dim_{\mathbb{Q}} V_B = [n/2]$: достаточно, чтобы $A_{n-1} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_n)$. Также в [1] показано, что для всех $n < 17$ искомое вложение имеется: при $n < 17$ группа $\mathrm{Gal}_{\mathbb{Q}}(f_n)$ содержит знакопеременную группу A_{n-1}.

В работе [2] доказана оценка снизу: для любого натурального $n > 3$ справедливо неравенство $\dim_{\mathbb{Q}} V_B \geqslant 2$. Таким образом, для любого $n > 3$ можно построить обобщенную задачу Фуллера (1), выбрав оператор C согласно теореме 1, в которой будет существовать оптимальное управление, проходящее за конечное время половину всюду плотной обмотки 2-мерного тора, отвечающей положительному направлению времени.

В данной работе мы анонсируем результаты, существенно усиливающие результаты работ [1, 2]. В частности, мы при $n = 499\,989\,828$ даем набросок доказательства существования в задаче (1) оптимального управления (если соответствующим образом выбрать оператор C согласно теореме 1, но такой выбор, очевидно, всегда возможен), пробегающего за конечное время половину всюду плотной обмотки k-мерного тора, отвечающей положительному направлению времени, для любого наперед заданного натурального $k \leqslant 249\,994\,914$ – это наилучший на текущий момент результат.

[1] Случай $N = 1$ не исключается. В этом случае подойдет любое собственное значение λ_j формы C, лишь бы $\dim V_j \geqslant 2$.

[2] Многочлен $f_n(x)$ будем называть *многочленом Зеликина–Локуциевского*.

2 Основные результаты

2.1 Формулировки и наброски доказательств

Всюду далее для простого $q > 3$ символом x_q обозначается выражение

$$x_q = 1 + \frac{1}{2} + \ldots + \frac{1}{q-1}. \tag{6}$$

Всюду далее для простого r символом $\mathbb{Z}_r$ обозначается кольцо целых r-адических чисел (кольцо нормирований поля $\mathbb{Q}_r$). Всюду далее символом $\mathbb{P}$ обозначается множество всех простых чисел.

В следующей теореме при некоторых условиях вычисляется группа Галуа над $\mathbb{Q}$ многочлена Зеликина–Локуциевского $f_n(x)$.

Теорема 2. *Пусть $n = p + 1$ для некоторого простого $p > 5$, причем числа $q = 2n + 1$ и $r = 2n + 7$ также просты, $x_q \not\equiv 0 (\operatorname{mod} q^3)$, а 889 не является квадратом по модулю r. Тогда имеется изоморфизм $\mathrm{Gal}_{\mathbb{Q}}(f_n) \cong S_{n-1}$, а потому все элементы множества B линейно независимы над $\mathbb{Q}$, т.е. $\dim_{\mathbb{Q}} V_B = [n/2]$.*

Набросок доказательства. Сначала покажем, что в условиях теоремы группа $\mathrm{Gal}_{\mathbb{Q}}(f_n)$ как группа перестановок корней многочлена $f_n(x)$ содержит транспозицию. Для этого выражение $P_n(ix)$ для $n = p + 1$ рассмотрим в кольце $\mathbb{Z}[x, i]/(r, i^2 + 1)$. Мы получим, группируя для всех $k \in [7, r - 7] \cap \mathbb{N}$ скобку $ix + k$ со скобкой $ix + r - k$, что многочлен $f_n(x)$ в кольце $\mathbb{F}_r[x]$ примет вид

$$f_n(x) = g(x) f_3(x) = g(x)(21x^2 - 35 \cdot 21x + 84 \cdot 21); \tag{7}$$

параметры p и r подобраны таким образом, что $g(x)$ – сепарабельный многочлен над $\mathbb{F}_r$ степени $n - 3$, причем $\mathbb{F}_r$ – поле разложения многочлена $g(x)$. Так как $(21, r) = 1$, то можно в (7) сократить на 21 и получить многочлен $x^2 - 35x + 84$, дискриминант которого равен 889. По условию 889 не является квадратом в $\mathbb{F}_r$, а потому можно осуществить гензелев подъем разложения (7) в кольцо $\mathbb{Z}_r[x]$; мы получим тем самым, что группа разложения некоторого простого дивизора $\mathfrak{r}$ поля разложения многочлена $f_n(x)$ над $\mathbb{Q}$, лежащего над r, содержит транспозицию. Но в таком случае и $\mathrm{Gal}_{\mathbb{Q}}(f_n)$ также содержит транспозицию.

Теперь убедимся в неприводимости многочлена $f_n(x)$ над $\mathbb{Q}$ в условиях теоремы. Для этого обозначим через $\sigma_{r,t}$ – элементарный симметрический многочлен степени r от набора $[1, t] \cap \mathbb{N}$, а через $s_{r,t}$ – r-ю степенную сумму от набора $[1, t] \cap \mathbb{N}$. В таком случае, используя определение многочлена $f_n(x)$, нетрудно видеть, что

$$f_n(x) = (-1)^{n-1}\sigma_{1,2n}x^{n-1} + (-1)^{n-2}\sigma_{3,2n}x^{n-2} + \ldots + \sigma_{2n-1,2n}. \tag{8}$$

В предположениях теоремы многочлен $f_n(x)$ является многочленом Эйзенштейна относительно простого числа q. Действительно, используя представление (8), нетрудно показать, что все коэффициенты многочлена $f_n(x)$ (кроме старшего) делятся на q^2, старший делится ровно на q, а свободный член в силу условий теоремы делится ровно на q^2: ведь легко видеть, что $\sigma_{q-2,q-1} = (q-1)! \cdot x_q$, а $((q-1)!, q) = 1$.

Делимость всех коэффициентов многочлена $f_n(x)$ (кроме старшего) на q^2 может быть показана с использованием равенства

$$\sigma_{2k-1,q-1} = \frac{1}{(2k-1)!} \cdot \begin{vmatrix} s_{1,q-1} & 1 & 0 & \ldots & 0 \\ s_{2,q-1} & s_{1,q-1} & 2 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_{2k-2,q-1} & s_{2k-3,q-1} & s_{2k-4,q-1} & \ldots & 2k-2 \\ s_{2k-1,q-1} & s_{2k-2,q-1} & s_{2k-3,q-1} & \ldots & s_{1,q-1} \end{vmatrix}, \tag{9}$$

очевидного сравнения $s_{2k,q-1} \equiv 0 (\operatorname{mod} q)$ для всех $k \in [1, (q-3)/2] \cap \mathbb{N}$, а также того факта, что $s_{2k-1,q-1} \equiv 0 (\operatorname{mod} q^2)$ для всех $k \in [2, (q-1)/2] \cap \mathbb{N}$ – последнее нетрудно выводится, например, из свойств чисел Бернулли.

Итак, группа $\mathrm{Gal}_{\mathbb{Q}}(f_n)$ – транзитивная[3] подгруппа подстановок в S_p, содержащая транспозицию. В таком случае хорошо известно, что имеется изоморфизм $\mathrm{Gal}_{\mathbb{Q}}(f_n) \cong S_{n-1}$. □

[3] Ведь многочлен $f_n(x)$ неприводим над $\mathbb{Q}$.

Перечислим все натуральные $n \leqslant 600$, удовлетворяющие условиям теоремы 2:

$$n \in \{8,\, 18,\, 20,\, 30,\, 48,\, 270,\, 338,\, 410,\, 488,\, 558\}. \tag{10}$$

Нетрудно видеть, что условия теоремы 2 оставляют большие вопросы по поводу бесконечности множества натуральных n, для которых имеется равенство $\dim_{\mathbb{Q}} V_B = [n/2]$. Следующая теорема, однако, дает некоторую надежду.

Теорема 3. *Если для почти всех*[4] *простых p из арифметической прогрессии $\{26+69k \mid k \in \mathbb{N}\}$ многочлен $f_{p+1}(x)$ неприводим над $\mathbb{Q}$, то существует бесконечная последовательность натуральных n, для которых имеется вложение $A_{n-1} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_n)$ и, в частности, $\dim_{\mathbb{Q}} V_B = [n/2]$.*

Набросок доказательства. Пусть $p = 26 + 69k$ для некоторого $k \in \mathbb{N}$. Заметим, что $26 = 3 + 23$, $69 = 3 \cdot 23$, и рассмотрим выражение $P_{p+1}(ix)$ в кольце $\mathbb{Z}[x,\, i]/(23,\, i^2+1)$. Заметим, что $2p+2 = 8 + 2 \cdot 23(3k+1)$, а потому в кольце $\mathbb{F}_{23}[x]$ имеется разложение

$$f_{p+1}(x) = -(x^{11}+1)^{2(3k+1)} x^{3k+1} f_4(x). \tag{11}$$

Нетрудно убедиться (например, с помощью Maple; хотя можно использовать и алгоритм Берлекемпа), что многочлен $f_4(x)$ неприводим над $\mathbb{F}_{23}$, а потому в кольце $\mathbb{F}_{23}[x]$ многочлен $f_{p+1}(x)$ разлагается в произведение взаимно простых множителей: $f_4(x)$ и $-(x^{11}+1)^{2(3k+1)} x^{3k+1}$, причем последнее выражение имеет поле разложения $\mathbb{F}_{23}$. Сделав гензелев подъем разложения (11) в кольцо $\mathbb{Z}_{23}[x]$, мы получим, что группа разложения некоторого простого дивизора $\mathfrak{p}_{23}$ поля разложения многочлена $f_{p+1}(x)$ над $\mathbb{Q}$, лежащего над 23, содержит элемент порядка 3. Итак, $3 \mid |\mathrm{Gal}_{\mathbb{Q}}(f_{p+1})|$.

Теперь заметим, что $3 \nmid (p-1)$, ибо $p \equiv 2 (\mathrm{mod}\, 3)$. Если теперь p – такое простое число из условий теоремы, что $f_{p+1}(x)$ неприводим над $\mathbb{Q}$, то группа $\mathrm{Gal}_{\mathbb{Q}}(f_{p+1})$ неразрешима: действительно, в противном случае хорошо известно (см. [3, Гл. 5, п. 23.5, Теорема 23.6]), что она была бы подгруппой голоморфа $Z_p \leftthreetimes Z_{p-1}$, а $3 \mid |\mathrm{Gal}_{\mathbb{Q}}(f_{p+1})|$.

Итак, если p – такое простое число из условий теоремы, что $f_{p+1}(x)$ неприводим над $\mathbb{Q}$, то $\mathrm{Gal}_{\mathbb{Q}}(f_{p+1})$ – неразрешимая транзитивная группа подстановок простой степени. Но тогда эта группа дважды транзитивна в силу классической теоремы Бернсайда (см. [4, Гл. 8, §38]). Наконец, дважды транзитивные неразрешимые группы подстановок простой степени p хорошо известны. Именно, из результата [4, Гл. 8, §38, Теорема 4] мы получаем тогда либо нужное нам вложение $A_p \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_{p+1})$, либо следующие возможности:

1. $p = 11$ и $\mathrm{Gal}_{\mathbb{Q}}(f_n)$ изоморфна либо M_{11}, либо $L_2(11)$;
2. $p = 23$ и $\mathrm{Gal}_{\mathbb{Q}}(f_n)$ изоморфна M_{23};
3. $p = (r^{st}-1)/(r^s-1)$ для некоторого простого r и некоторых натуральных s, t, в этом случае $\mathrm{Gal}_{\mathbb{Q}}(f_n)$ изоморфна некоторой подгруппе в $\mathrm{Aut}(L_t(r^s))$, содержащей $L_t(r^s)$.

Пусть N – достаточно большое натуральное число. Оценим количество чисел множества[5]

$$B = \left\{ \left. \frac{r^{st}-1}{r^s-1} \right| s,\, t \in \mathbb{N} : \, (s,\, t) \neq (1,\, 2),\, t > 1,\, r \in \mathbb{P} \right\}, \tag{12}$$

не превосходящих N.

Мы имеем

$$N \geqslant \frac{r^{st}-1}{r^s-1} > r^{s(t-1)} \geqslant r^2.$$

Но тогда $r < \sqrt{N}$. Далее, так как $r \geqslant 2$, то мы имеем также неравенство $N > 2^{s(t-1)}$, откуда $s(t-1) < \ln N / \ln 2$. Итак, мы получили следующие оценки сверху:

$$r < \sqrt{N}, \quad s < \frac{\ln N}{\ln 2}, \quad t < \frac{\ln N}{\ln 2} + 1.$$

[4] Т.е. кроме, быть может, конечного числа.

[5] Поскольку случай $(s,\, t) = (1,\, 2)$ невозможен по тривиальным причинам.

Но тогда количество элементов множества B, не превосходящих N, заведомо не превосходит величины

$$B_N = \sqrt{N}\frac{\ln N}{\ln 2}\left(\frac{\ln N}{\ln 2}+1\right). \tag{13}$$

С другой стороны, количество простых чисел в арифметической прогрессии $\{26+69k \mid k \in \mathbb{N}\}$ эквивалентно при $N \to +\infty$ величине

$$P_N = \frac{N}{44\ln N}, \tag{14}$$

что сразу вытекает из теоремы Дирихле о простых числах в арифметической прогрессии и асимптотического закона распределения простых чисел. Поскольку $\lim\limits_{N\to+\infty} P_N/B_N = +\infty$, то доказываемое утверждение вытекает из условия на неприводимость многочленов $f_{p+1}(x)$ над $\mathbb{Q}$ для почти всех простых p из арифметической прогрессии $\{26+69k \mid k \in \mathbb{N}\}$. $\square$

К сожалению, неприводимость многочлена $f_n(x)$ над $\mathbb{Q}$ удается пока установить лишь в следующем случае:

Теорема 4. *Пусть число $q > 3$ является простым с условием $x_q \notin q^3\mathbb{Z}_q$, тогда многочлен $f_{(q-1)/2}(x)$ неприводим над $\mathbb{Q}$.*

Используя результат теоремы 4, можно доказать следующее утверждение[6]:

Теорема 5. *Пусть $q \equiv 2 (\mathrm{mod}\, 3)$ – такое нечетное простое число, что многочлен $f_4(x)$ неприводим над $\mathbb{Q}$, а число $p = 3+q+3qk$ также простое для некоторого натурального k. Положим $n = p+1$. Если число $2p+3 = 2n+1$ является простым с условием $x_{2p+3} \notin (2p+3)^3\mathbb{Z}_{2p+3}$, то $A_p \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_n)$, кроме, быть может, случая, когда $p = (r^{st}-1)/(r^s-1)$ для некоторого простого r и некоторых натуральных r, s.*

Нетрудно видеть, что в теореме 5 можно положить $q = 23$ и получить

Следствие 1. *Пусть p – простое число из прогрессии $\{26+69k \mid k \in \mathbb{N}\}$, не представимое в виде $(r^{st}-1)/(r^s-1)$ ни для каких простого r и натуральных s, t. Пусть, далее, число $2p+3$ является простым с условием $x_{2p+3} \notin (2p+3)^3\mathbb{Z}_{2p+3}$. Тогда имеется вложение $A_p \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_{p+1})$ и, в частности, при $n = p+1$ справедливо равенство $\dim_{\mathbb{Q}} V_B = [n/2]$.*

Если все-таки оказалось, что простое p из следствия 1 представляется в виде $(r^{st}-1)/(r^s-1)$ для каких-то простого r и натуральных s, t, то при выполнении остальных условий следствия 1 получается оценка $\dim_{\mathbb{Q}} V_B \geqslant 3$.

Наконец, укажем примеры натуральных n, удовлетворяющих условиям следствия 1.

Теорема 6. *Для натуральных $n \in \{1\,614,\ 34\,503\,270,\ 499\,989\,828\}$ выполнены все условия следствия 1, а потому имеются вложения $A_{n-1} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_n)$. В частности, для рассматриваемых n справедливо равенство $\dim_{\mathbb{Q}} V_B = [n/2]$.*

Следствие 2. *В задаче (1) при $n = 499\,989\,828$ для любого натурального $k \leqslant 249\,994\,914$ существует оптимальное управление (если, конечно, выбрать оператор C согласно теореме 1), проходящее за конечное время половину всюду плотной обмотки k-мерного тора, отвечающей положительному направлению времени.*

2.2 Некоторые замечания

2.2.1 О простых числах Вольстенхольма

Простые числа $q > 3$ со свойством $x_q \in q^3\mathbb{Z}_q$ называются *простыми числами Вольстенхольма* (см. [5]). На сегодняшний день известно лишь два простых числа Вольстенхольма: 16 843 и 2 124 679. Более того, других простых чисел Вольстенхольма на отрезке $[5, 10^9]$ нет (см. [5]). Оценка $k \leqslant 249\,994\,914$ является принципиально неулучшаемой на текущий момент потому, что простое $p = 499\,989\,827$ – максимальное из

[6] К сожалению, более слабое, чем теорема 3.

всех простых чисел, принадлежащих прогрессии $\{26+69k \mid k \in \mathbb{N}\}$, для которого еще $2p+3 < 10^9$ и выполняются остальные условия следствия 1. Разумеется, можно брать простые p из других арифметических прогрессий, перечисленных в теореме 5, но принципиального улучшения оценки из следствия 2 не будет, так как неизвестно распределение простых чисел Вольстенхольма на интервале $(10^9, +\infty)$.

Таким образом, проблема построения в задачах (1) оптимального управления, пробегающего половину всюду плотной обмотки k-мерного тора, отвечающей положительному направлению времени, для сколь угодно большого k, сводится (согласно теореме 3) к следующей проблеме.

Проблема 2. *Можно ли утверждать, что для почти всех простых p из арифметической прогрессии $\{26 + 69k \mid k \in \mathbb{N}\}$ многочлен Зеликина–Локуциевского $f_{p+1}(x)$ неприводим над $\mathbb{Q}$?*

В настоящий момент из результатов по неприводимости многочлена $f_n(x)$ над $\mathbb{Q}$ установлена лишь теорема 4.

2.2.2 О теореме 3

Количество простых чисел в арифметической прогрессии $\{26 + 69k \mid k \in \mathbb{N}\}$, не превосходящих N, эквивалентно при $N \to +\infty$ величине $N/(44 \ln N)$, что вытекает из теоремы Дирихле о простых числах в арифметической прогрессии. В наброске доказательства теоремы 3 показано, что количество простых чисел не выше N, принадлежащих множеству

$$X = \left\{ \frac{r^{st} - 1}{r^t - 1} \middle| r \in \mathbb{P},\, s,\, t \in \mathbb{N} \right\}, \tag{15}$$

оценивается сверху величиной

$$B_N = \sqrt{N} \frac{\ln N}{\ln 2} \left(\frac{\ln N}{\ln 2} + 1 \right). \tag{16}$$

Таким образом, для построения задачи оптимального управления, в которой имеется оптимальное управление, проходящее за конечное время половину всюду плотной обмотки k-мерного тора (отвечающей положительному направлению времени) для любого наперед заданного натурального k, достаточно решить следующую более слабую форму проблемы 2:

Проблема 3. *Количество простых чисел p из арифметической прогрессии $\{26+69k \mid k \in \mathbb{N}\}$, для которых многочлен Зеликина–Локуциевского $f_{p+1}(x)$ приводим над $\mathbb{Q}$, равно $O(B_N)$ при $N \to +\infty$, где величина B_N определена в* (16).

Благодарности

Автор выражает глубокую благодарность акад. РАН д.ф.-м.н. профессору Сергею Владимировичу Конягину, чл.-корр. РАН д.ф.-м.н. профессору Михаилу Ильичу Зеликину, д.ф.-м.н. профессору Вячеславу Александровичу Артамонову и д.ф.-м.н. Льву Вячеславовичу Локуциевскому за полезные консультации и неоценимую моральную поддержку.

Список литературы

[1] M. I. Zelikin, D. D. Kiselev, L. V. Lokutsievskiy. Optimal Control and Galois Theory. *Matem. Sbornik*, 204(11):83-98, 2013 (in Russian). = M. I. Zelikin, D. D. Kiselev, L. V. Lokutsievskiy. Optimal Control and Galois Theory. *Sbornik Mathematics*, 204(11):1624–1638, 2013 (English transl.).

[2] D. D. Kiselev. On the dense winding of the 2-dimensional torus. *Matem. Sbornik*, 207(4):113-122, 2016 (in Russian). = D. D. Kiselev. On the dense winding of the 2-dimensional torus. *Sbornik Mathematics*, 207(4):581-589, 2016 (English transl.).

[3] V. V. Prasolov. *Polynoms.* MCCME, Moscow, 2003 (in Russian). = В.В. Прасолов. *Многочлены.* МЦНМО, Москва, 2003.

[4] D. A. Suprunenko. *Permutation groups.* Nauka i tehnika, Minsk, 1996 (in Russian). = Д.А. Супруненко. *Группы подстановок.* Наука и техника, Минск, 1996.

[5] R. J. McIntosh, E. L. Roettger. A search for Fibonacci–Wieferich and Wolstenholme primes. *Math. Computation*, 76:2087–2094, 2007.

Applications of Galois Theory to Optimal Control

Denis D. Kiselev
Russian Foreign Trade Academy (Moscow, Russia)

Keywords: Galois group, linear independence, dense winding, generalized Fuller optimal control problem.

We investigate linear independence over $\mathbb{Q}$ of elements from some specific $[n/2]$-elementary root subsystem of the polynomial $\mathrm{Im}\,(ix+1)\dots(ix+2n)$. We apply our investigations to the optimal synthesis problem of the generalized Fuller optimal control problem: there exists the generalized Fuller optimal control problem, the optimal control of which runs through the half of the dense winding of k-dimensional torus in finite positive time for arbitrary natural $k \leqslant 249\,994\,914$. Under irreducibility assumption of Zelikin–Lokutsievskiy polynoms over $\mathbb{Q}$ of almost all prime degrees from arithmetic progression $\{26+69k \mid k \in \mathbb{N}\}$ one could assign an arbitrary natural value for k.