МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА

*На правах рукописи*

**Киселев Денис Дмитриевич**

# Ультраразрешимые накрытия и смежные вопросы теории Галуа

Специальность 01.01.06 – математическая логика, алгебра и теория чисел

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
доктора физико-математических наук

Москва — 2018

Работа выполнена на кафедре высшей алгебры механико-математического факультета МГУ имени М.В. Ломоносова.

Официальные оппоненты: **Кузьмин Леонид Викторович**,
доктор физико-математических наук,
НИЦ "Курчатовский институт",
ИИТ, начальник лаборатории.

**Востоков Сергей Владимирович**,
доктор физико-математических наук, профессор
ФГБОУ ВО "Санкт-Петербургский государственный университет",
математико-механических факультет,
заведующий кафедрой.

**Шабат Георгий Борисович**,
доктор физико-математических наук, профессор,
ФГБОУ ВО "Российский государственный гуманитарный университет", институт лингвистики,
кафедра математики, логики и интеллектуальных систем в гуманитарной сфере, профессор.

Защита диссертации состоится «30» ноября 2018 г. в 16 ч. 45 мин. на заседании диссертационного совета МГУ.01.17 Московского государственного университета имени М. В. Ломоносова по адресу: 119234, Москва, ГСП-1, Ленинские горы, д. 1, МГУ имени М. В. Ломоносова, механико-математический факультет, аудитория 14-08

E-mail: msu.01.17@mail.ru

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки МГУ имени М. В. Ломоносова (Ломоносовский просп., д. 27) и на сайте ИАС «ИСТИНА»:

https://www.istina.msu.ru/dissertations/143663993

Автореферат разослан «28» сентября 2018 г.

Ученый секретарь
диссертационного совета
МГУ.01.17 при МГУ
доктор физико-математических наук,
чл.-корр. РАН

А. И. Шафаревич

# Общая характеристика работы

## Актуальность темы

Диссертация посвящена исследованию ряда трудных вопросов теории Галуа (как классической, так и обратной задаче), теории представлений конечных групп (индекс Шура), построению явных вложений конечных абелевых $p$-групп в группу Дженнингса $\mathcal{J}(\mathbb{F}_p)$.

Одним из возможных подходов к решению обратной задачи теории Галуа – построение расширений Галуа поля рациональных чисел с наперед заданной группой Галуа – была и остается задача погружения. Задача погружения, ассоциированная точной последовательностью конечных групп,

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\varphi} F = \mathrm{Gal}(K/k) \longrightarrow 1,$$

состоит в том, чтобы построить $k$-алгебру Галуа $L$ с группой $G$, содержащую поле $K$, таким образом, чтобы эпиморфизм ограничения автоморфизмов $L$ на $K$ совпадал бы с $\varphi$. У истоков задачи погружения стояли А. Шольц, Х. Райхард и Д. К. Фаддеев. А. Шольц[1] решил задачу погружения (в смысле полей) для полей алгебраических чисел в случае, когда группа $G$ есть полупрямое произведение $F \leftthreetimes A$ с абелевым ядром $A$, что в конечном счете позволило ему[2] решить обратную задачу теории Галуа для $p$-групп нечетного порядка над полем $\mathbb{Q}$. Более простыми средствами этот результат был независимо установлен Х. Райхардом[3]. Д. К. Фаддеев в своей совместной с Б. Н. Делоне фундаментальной работе[4] ввели понятие алгебры Галуа на основе элегантного геометрического подхода, что позволило в дальнейшем решать задачу погружения с абелевым ядром с привлечением гомологических методов. Было установлено важнейшее необходимое условие разрешимости задачи погружения – условие согласности, которое состояло в "аддитивной" разрешимости задачи, т.е. в качестве "решения" допускались не только алгебры Галуа, но и так называемые модули согласности: $G$-модули со структурой конечномерного векторного пространства над $K$, обладающие $A$-нормальным базисом над $K$. При этом $A$ не обязательно абелева группа. Д. К. Фаддеев[5] дает критерии существования таких модулей согласности. Один из них состоит в следующем. Рассмотрим скрещенное произведение $G \times K$, т.е. $k$-алгебру, составленную из сумм вида

[1] A. Scholtz, "Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoischer Gruppe", *Math. Z.*, **30**, (1929), 332–356.

[2] A. Scholtz, "Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung", *Math. Z.*, **42**, (1936), 161–188.

[3] H. Reichardt, "Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung", *J. reine angew. Math.*, **177**, (1937), 1–5.

[4] Б. Н. Делоне, Д. К. Фаддеев, "Исследования по геометрии теории Галуа", *Матем. сб.*, **15:2**, (1944), 243–284.

[5] Там же.

$\sum_{g\in G} u_g x_g$, где $x_g \in K$, с правилами умножения $u_{g_1}u_{g_2} = u_{g_1g_2}$ и $xu_g = u_g x^{\varphi(g)}$ при $x \in K$, а $g \in G$. Существование модуля согласности оказалось равносильно изоморфизму скрещенного произведения $G \times K$ алгебре матриц порядка $|F|$ над некоторой подалгеброй. В той же работе[6] показано, что условие согласности достаточно для разрешимости задачи погружения в смысле алгебр Галуа в случае, если ядро является циклической группой, порядок которой не делится на 8; при доказательстве использовалось утверждение, сводящее решение задач погружения с абелевым ядром к случаю, когда ядро является $p$-группой. Независимо это позднее было установлено Р. Кохердорфером[7]. Кроме того, без всяких ограничений (в отличие от работы А. Шольца[8]) была показана равносильность решения задачи погружения с абелевым ядром над полями алгебраических чисел в смысле полей и в смысле алгебр Галуа, делающая таким образом условие согласности чрезвычайно полезным инструментом в исследовании обратной задачи теории Галуа. Дальнейшие исследования в области обратной задачи теории Галуа были проведены в цикле работ И. Р. Шафаревича[9][10][11][12], где была решена обратная задача теории Галуа для полей алгебраических чисел и разрешимых групп. Отметим, что полупрямая задача погружения числовых полей с нильпотентным ядром была решена В. В. Ишхановым[13].

В[14] задача погружения с абелевым ядром была решена А. В. Яковлевым в гомологических терминах. Выяснилось, в частности, что если факторгруппа действует на ядре как циклическая группа автоморфизмов, а примитивный корень степени периода ядра лежит в $K$, то выполнения условия согласности Фаддеева-Хассе достаточно для разрешимости задачи погружения. В работе[15] задача погружения с абелевым ядром решается для числовых полей и оказывается, что в широком классе случаев дополнительное условие погружаемости несущественно: если, например, тривиально пересечение ядер го-

[6]Там же.

[7]R. Kochendörffer, "Zwei Reduktionssätze zum Einbettungsproblem für Abelsche Algebren", *Math. Nachr.*, **10:1-2**, (1953), 75–84.

[8]A. Scholtz, "Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoischer Gruppe", *Math. Z.*, **30**, (1929), 332–356.

[9]И. Р. Шафаревич, "О построении полей с заданной группой Галуа порядка $l^\alpha$", *Изв. АН СССР, сер. матем.*, **18:3**, (1954), 261–296.

[10]И. Р. Шафаревич, "Об одной теореме существования в теории алгебраических чисел", *Изв. АН СССР, сер. матем.*, **18:4**, (1954), 327–334.

[11]И. Р. Шафаревич, "О задаче погружения полей", *Изв. АН СССР, сер. матем.*, **18:5**, (1954), 389–418.

[12]И. Р. Шафаревич, "Построение полей алгебраических чисел с заданной разрешимой группой Галуа", *Изв. АН СССР, сер. матем.*, **18:6**, (1954), 525–578.

[13]В. В. Ишханов, "О полупрямой задаче погружения с нильпотентным ядром", *Изв. АН СССР, сер. матем.*, **40:1**, (1976), 3–25.

[14]А. В. Яковлев, "Задача погружения полей", *ДАН СССР*, **150:5**, (1964), 1009–1011.

[15]А. В. Яковлев, "Задача погружения для числовых полей", *Изв. АН СССР. Сер. матем.*, **31:2**, (1967), 211–224.

моморфизмов ограничения вида $r_{\mathfrak{p}}\colon H^2(F, \widehat{A}) \to H^2(F_{\mathfrak{p}}, \widehat{A})$, где $F$ – группа Галуа расширения числовых полей $K/k$ с условием $\varepsilon_n \in K$ ($n$ – период абелева ядра $A$), $\widehat{A} = \mathrm{Hom}(A, K^*)$, а $F_{\mathfrak{p}}$ – группа разложения точки $\mathfrak{p}$ поля $k$ в $K$, то дополнительное условие погружаемости несущественно. Это позволило в[16] решить обратную задачу теории Галуа для разрешимых групп над числовыми полями практически без использования арифметики полей алгебраических чисел (в отличие от работы[17] и[18]), а только используя теорему Д. К. Фаддеева-А. Шольца о разрешимости в смысле полей полупрямой задачи погружения числовых полей с абелевым ядром (см.[19]).

Мы видим, таким образом, что для решения задачи погружения в смысле полей необходимо сначала решить такую же задачу в смысле алгебр Галуа, а потом преодолеть ряд технических условий для доказательства разрешимости такой задачи в смысле полей (что особенно важно для обратной задачи теории Галуа). Отметим, что эти технические условия особенно существенны в случае, когда задача погружения ставится над локальными полями[20]: если задача погружения $p$-расширения $K/k$ $p$-локальных полей разрешима в смысле алгебр Галуа, то из-за конечности факторгруппы $k^*/k^{*p}$ вполне возможно, что не удастся найти решение этой же задачи в смысле полей. Систематические исследования разрешимости задачи погружения над локальными полями в собственном смысле[21] были проделаны Б. Б. Лурье (см.[22]). Поэтому особенно интересен случай, когда априори можно гарантировать, что все решения задачи погружения окажутся полями (такие задачи мы в дальнейшем называем *ультраразрешимыми*). Простейшее условие таково: ядро задачи погружения лежит в группе Фраттини накрывающей группы (см.[23]). Первые нетривиальные примеры (когда указанное условие на группу Фраттини не выполняется) были построены в[24][25]. В связи с работой[26] А. В. Яковлев поставил следующую проблему.

---

[16] А. В. Яковлев, "Расширения Галуа с разрешимой группой", *Тр. МИАН*, **183**, (1990), 204–215.

[17] И. Р. Шафаревич, "Построение полей алгебраических чисел с заданной разрешимой группой Галуа", *Изв. АН СССР, сер. матем.*, **18:6**, (1954), 525–578.

[18] В. В. Ишханов, "О полупрямой задаче погружения с нильпотентным ядром", *Изв. АН СССР, сер. матем.*, **40:1**, (1976), 3–25.

[19] A. Scholtz, "Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoischer Gruppe", *Math. Z.*, **30**, (1929), 332–356.

[20] В данном случае конечными расширениями поля $\mathbb{Q}_p$.

[21] Т.е. когда решение ищется в классе полей.

[22] В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, "*Задача погружения в теории Галуа*, М. Наука, 1990, Гл. 4.

[23] Там же, Гл. 1, §6, Следствие 5.

[24] Д. Д. Киселев, "Примеры задач погружения, у которых решения только поля", *УМН*, **68:4**, (2013), 181–182.

[25] Д. Д. Киселев, Б. Б. Лурье, "Ультраразрешимость и сингулярность в проблеме погружения", *Зап. научн. сем. ПОМИ*, **414**, (2013), 113–126.

[26] Там же.

**Проблема** (А. В. Яковлев). *Пусть*

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\varphi} F \longrightarrow 1$$

*– расширение конечных групп с абелевым ядром $A$. При каких условиях существует расширение Галуа числовых полей $K/k$ с группой $F$, такое что получившаяся задача погружения ультраразрешима?*

Глава 1 целиком посвящена результатам диссертанта по проблеме Яковлева, которую удалось решить для широкого класса групповых расширений (в частности, полностью для расширений нечетного порядка с циклическим ядром). Таким образом, актуальность главы 1 не вызывает сомнений.

В теории представлений конечных групп весьма интересна и актуальна проблема оценки индекса Шура неприводимых комплексных характеров над полем рациональных чисел. Данная проблема имеет довольно длинную историю. Упомянем результаты О. Шиллинга[27][28] и П. Рокетта[29][30], в которых показано, что индекс Шура любого неприводимого комплексного характера конечной $p$-группы при $p > 2$ над полем рациональных чисел равен 1; в случае $p = 2$ имеется неулучшаемая оценка $m_{\mathbb{Q}}(\chi) \mid 2$. Далее, в работе Д. М. Голдшмидта-И. М. Айзекса[31] данный результат получил объяснение: если $n$ – экспонента группы $G$, а $\chi \in \operatorname{Irr} G$ – неприводимый комплексный характер, то представление с характером $\chi$ реализуется в любом поле $k$, содержащем $\mathbb{Q}(\chi)$, таком что $\operatorname{Gal}(k(\varepsilon_n)/k)$ – циклическая группа нечетного порядка. В работах Б. Фейна[32][33] данный результат был обобщен на случай, когда $\operatorname{Gal}(k(\varepsilon_n)/k)$ – циклическая группа не обязательно нечетного порядка; при этом необходимо наложить дополнительное условие: уравнение $-1 = u^2 + v^2$ разрешимо в поле $k$. Естественно поставить вопрос о поиске равномерных наилучших оценок индекса Шура неприводимых комплексных характеров конечных групп на определенных классах конечных групп. В главе 2 строятся наилучшие оценки индекса Шура неприводимых комплексных характеров конечных групп на классе всех конечных групп порядка $n$ (класс $G_{\mathrm{ord}}(n)$) и на классе всех конечных групп заданной экспоненты (класс $G_{\exp}(n)$) – эти результаты многократно усиливают известные результаты Б. Фейна-Т. Ямады[34].

[27] O. F. G. Schilling, "Über die Darstellungen endlicher Gruppen", *J. für Math.*, **174**, (1936), 188.

[28] O. F. G. Schilling, "*The theory of valuations*", Amer. Math. Soc. (N.Y.), New York, 1950.

[29] P. Roquette, "Arithmetische Untersuchung des Charakterringes einer endlichen Gruppe", *J. für Math.*, **190**, (1952), 148–168.

[30] P. Roquette, "Realisierung von Darstellungen endlicher nilpotenter Gruppen", *Arch. der Math.*, **9**, (1958), 241–250.

[31] D. M. Goldschmidt, I. M. Isaacs, "Schur indices in finite groups", *J. Algebra*, **33**, (1975), 191–199.

[32] B. Fein, D. Gordon, J. Smith,"On the representation of -1 as sum of two squares in an algebraic number field", *J. Number Theory*, **3**, (1971), 310–315.

[33] B. Fein, "Schur indices and sums of squares", *Proc. Ams. Math. Soc.*, **51:1**, (1975), 31–34.

[34] T. Yamada, "*The Schur Subgroup of the Brauer Group*", Berlin, Springer-Verlag, 1974, Ch. 9, theorem 9.1.

Пусть задана конечная группа $G$ экспоненты $n$ и ее неприводимый комплексный характер $\chi$ с индексом Шура $m \geqslant 3$ над полем $\mathbb{Q}$. Б. Фейн в своей работе[35] впервые построил пример, когда для произвольного поля $L$ в башне $\mathbb{Q}(\chi) \subset L \subset \mathbb{Q}(\varepsilon_n)$, такого что $(L : \mathbb{Q}(\chi)) = m$, тем не менее выполнено $m_L(\chi) \neq 1$. Он же показал, что для случая $n = p^\alpha q^\beta$ таких примеров построить нельзя[36]. Позднее Р. Моллин[37] и Е. Шпигель совместно с А. Трояном[38] построили ряд достаточных признаков того, что указанное поле $L$ все-таки обладает свойством $m_L(\chi) = 1$. Однако, их достаточные условия невозможно проверить, если не известны значения характера $\chi$. Например, пусть $r$ – минимальное натуральное число, такое что $\mathbb{Q}(\chi) \subseteq \mathbb{Q}(\varepsilon_r)$, а $h(\mathbb{Q}(\chi))$ – число классов поля $\mathbb{Q}(\chi)$, тогда одним из достаточных условий будет такое[39]

$$(m_{\mathbb{Q}}(\chi),\, (\mathbb{Q}(\varepsilon_r) : \mathbb{Q}(\chi)),\, h(\mathbb{Q}(\chi))) = 1.$$

П. Шмид в своей замечательной работе[40] определил так называемые группы Шура типа $G(p^a,\, q)$ и $G(p^a,\, q,\, r)$ а также пять исключительных типов групп Шура. Эти группы обладают таким свойством: пусть для данной конечной группы $G$ $p$-компонента $m_{\mathbb{Q}}(\chi)_p$ индекса Шура неприводимого комплексного характера $\chi$ над полем $\mathbb{Q}$ равна $p^a \geqslant 2$. Тогда в группе $G$ существует секция $H$, изоморфная одной из групп Шура[41], и неприводимый комплексный характер $\psi \in \operatorname{Irr} H$ с условием $m_{\mathbb{Q}}(\chi)_p = m_{\mathbb{Q}}(\psi)$; при этом $H$ является с точностью до изоморфизма одной из исключительных групп Шура в том и только в том случае, когда $p^a = 2$, и $\varepsilon_4 \notin \mathbb{Q}(\chi)$ (см.[42]). Используя группы Шура, мы даем обобщение результата Б. Фейна на случай, когда $n$ не обязательно делится только на два различных простых числа.

Хорошо известно, что если индекс Шура неприводимого комплексного характера $\chi$ конечной группы $G$ относительно поля алгебраических чисел $k$ равен $m$, то можно найти циклическое расширение $K/k(\chi)$ степени $m$, такое что $m_K(\chi) = 1$. Этот результат составляет содержание известной теоремы Грюнвальда-Ванга[43]. Пусть $K/k(\chi)$ – циклическое расширение полей алгебраических чисел степени $\widetilde{m}$, где $\widetilde{m} \mid m$. Мы изучаем достаточные условия того, что найдется циклическое расширение $L/k(\chi)$ степени $m$, причем, во-первых, $K \subseteq L$, а, во-вторых, $m_L(\chi) = 1$.

---

[35] B. Fein, "Minimal spliting fields for group representations", *Pacific J. Math.*, **51:2**, (1974), 427–431.

[36] Там же, Theorem.

[37] R. Mollin, "Splitting fields and group characters", *J. Reine Angew. Math.*, **315**, (1980), 107–114.

[38] E. Spiegel, A. Trojan, "Minimal splitting fields in cyclotomic extensions", *Proc. Ams. Math. Soc.*, **87:1**, (1983), 33–37.

[39] Там же, Corollary 6.

[40] P. Schmid, "Schur Indices and Schur Groups", *J. Algebra*, **169**, (1994), 226–247.

[41] Там же, 1. Introduction.

[42] Там же, 6. Conclusion, (6.1).

[43] I. Reiner, "*Maximal orders*", London Math. Soc. Monogr. (N.S.), **28**, Oxford Univ. Press, Oxford, 2003, Theorem (32.18).

Пусть $k$ – коммутативное кольцо с единицей. Рассмотрим множество $\mathcal{J}(k)$ формальных степенных рядов относительно переменной $x$ с коэффициентами в кольце $k$, причем коэффициент при $x$ ряда $f(x) \in \mathcal{J}(k)$ равен единице. На множестве $\mathcal{J}(k)$ можно ввести бинарную операцию: по определению $(f * g)(x) = f(g(x))$; такое определение корректно, так как ряд $g(x) \in \mathcal{J}(k)$ не содержит свободного члена. Впервые ряды такого вида рассмотрел Дженнингс, который в своей работе[44] установил, что относительно так введенной операции $\mathcal{J}(k)$ становится группой, а также показал ряд общих (не зависящих от выбора коммутативного кольца $k$ с единицей) свойств.

В случае $k = \mathbb{F}_p$ группа $\mathcal{J}(\mathbb{F}_p)$ обладает рядом интересных свойств, самым важным из которых, по-видимому, является универсальность: любая про-$p$-группа не более чем счетного ранга изоморфно вкладывается в $\mathcal{J}(\mathbb{F}_p)$. Этот результат был впервые установлен Р. Каминой[45]. Из этого результата следует, что произвольная конечная $p$-группа допускает изоморфное вложение в группу $\mathcal{J}(\mathbb{F}_p)$. Однако, доказательство наличия такого вложения даже для абелевых $p$-групп весьма далеко от конструктивного. И. К. Бабенко в своем обзоре[46] отмечает, что даже явные вложения групп $Z_{p^2}$ и $Z_p \times Z_p$ в $\mathcal{J}(\mathbb{F}_p)$ неизвестны! В тоже время вложение группы $Z_p$ в $\mathcal{J}(\mathbb{F}_p)$ строится очевидным образом: надо взять ряд $f(x) = x/(1-x)$, который имеет порядок $p$. В главе 3 мы строим явные вложения произвольной конечной абелевой $p$-группы в $\mathcal{J}(\mathbb{F}_p)$. Также вполне естественно в связи с проблемой Яковлева сформулировать *задачу вложения*, которая в частном случае решается в главе 3. Учитывая упомянутый обзор И. К. Бабенко, актуальность главы 3 не вызывает сомнений.

Наконец, в классической теории Галуа вполне естественно ставить вопросы о линейной независимости над основным полем собственного подмножества корней некоторого сепарабельного многочлена. Примечательно, что такие вопросы (вполне естественные для теории Галуа) находят применение в теории оптимального синтеза траекторий задач оптимального управления. Актуальность таких задач не вызывает сомнения; например, в работе[47] ставится гипотеза 1 (которую мы в дальнейшем называем проблемой М. И. Зеликина-Л. В. Локуциевского) о линейной независимости над $\mathbb{Q}$ некоторой подсистемы корней вполне определенного многочлена с целыми коэффициентами: линейная независимость таких корней позволяет строить траектории оптимального управления, проходящие за конечное время всюду плотную обмотку тора

[44] S. A. Jennings, "Substitution groups of formal power series", *Canad. J. Math.*, **6**, (1954), 325–340.

[45] R. Camina, "Subgroups of the Nottingham group", *J. Algebra*, **196:1**, (1997), 101–113, Corollary 2.

[46] И. К. Бабенко, "Алгебра, геометрия и топология группы подстановок формальных степенных рядов", *УМН*, **68:1**, (2013), 3–76, Замечание 4.11.

[47] М. И. Зеликин, Л. В. Локуциевский, Р. Хильдебранд, "Геометрия окрестностей особых экстремалей в задачах с многомерным управлением", *Тр. МИАН*, **277**, (2012), 74–90.

достаточно высокой размерности. Таким образом, актуальность понимания структуры оптимального синтеза в таких задачах для прикладных исследований (и, как следствие, актуальность исследования с помощью теории Галуа линейной независимости корней многочленов) не вызывает сомнения. Этим вопросам посвящена глава 4.

### Цель работы

Целью диссертации является:

1. решение проблемы А. В. Яковлева, посвященной характеризации ультраразрешимых групповых расширений, для групповых расширений нечетного порядка с циклическим ядром (полностью) а также в достаточно широких классах групповых расширений четного порядка с циклическим ядром;

2. выяснение того, что локально-глобальный принцип А. В. Яковлева не является необходимым для ультраразрешимости $p$-расширений;

3. построение неполупрямых $p$-расширений с абелевым нециклическим ядром, для которых проблема А. В. Яковлева решается отрицательно;

4. получение наилучших равномерных оценок индекса Шура неприводимых комплексных характеров конечных групп порядка $n$ (класс $G_{\mathrm{ord}}(n)$), конечных групп заданной экспоненты $n$ (класс $G_{\exp}(n)$) над полем $\mathbb{Q}$;

5. построение явных вложений конечных абелевых $p$-групп в группу Дженнингса $\mathcal{J}(\mathbb{F}_p)$, дающих ответ на вопрос И. К. Бабенко;

6. отыскание критерия разрешимости уравнения $x^{p^m} = y_0$ в группе $\mathcal{J}(\mathbb{F}_p)$ при заданных натуральном $m$ и элементе $y_0 \in \mathcal{J}(\mathbb{F}_p)$ порядка $p$;

7. сведе́ние проблемы Зеликина-Локуциевского к неприводимости над $\mathbb{Q}$ многочлена $f_{p+1}(x)$ для почти всех простых $p$, решение ее для ряда[48] натуральных $n$ и, как следствие, построение в обобщенной задаче Фуллера решений с управлением, проходящим за конечное время всюду плотную обмотку $k$-мерного тора для любого натурального $k \leqslant 249\,998\,919$ (отметим, что такая оценка на текущий момент принципиально неулучшаема);

8. доказательство существования для любого $n > 3$ не менее двух элементов "критического" множества корней многочлена Зеликина-Локуциевского, линейно независимых над $\mathbb{Q}$ и, как следствие, построение в обобщенной задаче Фуллера для любого $n > 3$ решений с управлением, проходящим за конечное время всюду плотную обмотку 2-мерного тора;

[48] Предположительно бесконечного.

9. доказательство неприводимости многочленов $f_{(q-1)/2}$ степени $(q-3)/2$ над $\mathbb{Q}$ для всех простых $q > 3$ с дополнительным условием на число Бернулли: $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$; вычисление группы Галуа многочлена $f_n(x)$ над $\mathbb{Q}$ при условии, что для $n > 4$ числа $p = n-1$, $q = 2n+1$, $r = 2n+7$ являются простыми, 889 не квадрат по модулю $r$, а $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$;

10. доказательство вложения $A_{n-1} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_n)$ при условии, что числа $p = n-1$, $q = 2n+1$ являются простыми, причем $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$, а $p$ принадлежит арифметической прогрессии $\{26 + 69k \mid k \in \mathbb{N}\}$ и не представимо в виде дроби $(r^{st}-1)/(r^s-1)$ ни для какого простого $r$ и натуральных $s$, $t$.

### Методы исследования

В работе использованы методы алгебраической теории чисел, элементарной теории чисел, локальной теории полей классов, теории Галуа, теории погружения, гомологической теории, теории представлений конечных групп, классификации конечных простых групп, теории индекса Шура, аналитической теории чисел.

### Научная новизна

Все результаты диссертации являются новыми и состоят в следующем:

1. решена проблема А. В. Яковлева, посвященная характеризации ультраразрешимых групповых расширений, для групповых расширений нечетного порядка с циклическим ядром (полностью) а также в достаточно широких классах групповых расширений четного порядка с циклическим ядром;

2. выяснено, что локально-глобальный принцип А. В. Яковлева не является необходимым для ультраразрешимости $p$-расширений;

3. построены неполупрямые $p$-расширения с абелевым нециклическим ядром, для которых проблема А. В. Яковлева решается отрицательно;

4. получены наилучшие равномерные оценки индекса Шура неприводимых комплексных характеров конечных групп порядка $n$ (класс $G_{\mathrm{ord}}(n)$), конечных групп заданной экспоненты $n$ (класс $G_{\exp}(n)$) над полем $\mathbb{Q}$;

5. построены явные вложения конечных абелевых $p$-групп в группу Дженнингса $\mathcal{J}(\mathbb{F}_p)$, дающие ответ на вопрос И. К. Бабенко;

6. найден критерий разрешимости уравнения $x^{p^m} = y_0$ в группе $\mathcal{J}(\mathbb{F}_p)$ при заданных натуральном $m$ и элементе $y_0 \in \mathcal{J}(\mathbb{F}_p)$ порядка $p$;

7. проблема Зеликина-Локуциевского сведена к вопросу о неприводимости над $\mathbb{Q}$ многочлена $f_{p+1}(x)$ для почти всех простых $p$, решена проблема Зеликина-Локуциевского для ряда[49] натуральных $n$ и, как следствие, в обобщенной задаче Фуллера построены решения с управлением, проходящим за конечное время всюду плотную обмотку $k$-мерного тора для любого натурального $k \leqslant 249\,998\,919$ (отметим, что такая оценка на текущий момент принципиально неулучшаема);

8. доказано существование для любого $n > 3$ не менее двух элементов "критического" множества корней многочлена Зеликина-Локуциевского, линейно независимых над $\mathbb{Q}$ и, как следствие, в обобщенной задаче Фуллера для любого $n > 3$ построены решения с управлением, проходящим за конечное время всюду плотную обмотку 2-мерного тора;

9. доказана неприводимость многочленов Зеликина-Локуциевского степени $(q-3)/2$ над $\mathbb{Q}$ для всех простых $q > 3$ с дополнительным условием на число Бернулли: $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$; вычислена группа Галуа многочлена $f_n(x)$ над $\mathbb{Q}$ при условии, что для $n > 4$ числа $p = n-1$, $q = 2n+1$, $r = 2n+7$ являются простыми, 889 не квадрат по модулю $r$, а $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$;

10. доказано вложение $A_{n-1} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_n)$ при условии, что числа $p = n-1$, $q = 2n+1$ являются простыми, причем $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$, а $p$ принадлежит арифметической прогрессии $\{26 + 69k \mid k \in \mathbb{N}\}$ и не представимо в виде дроби $(r^{st}-1)/(r^s-1)$ ни для какого простого $r$ и натуральных $s$, $t$.

### Апробация работы

Результаты диссертации докладывались на следующих научных семинарах.

Механико-математический факультет МГУ:

1. Научно-исследовательский семинар кафедры высшей алгебры (2013–2018 гг., неоднократно);

2. Избранные вопросы алгебры (2013–2018 гг., неоднократно);

3. Геометрическая теория оптимального управления (14 октября 2012 г., 01 ноября 2016 г.);

[49] Предположительно бесконечного.

4. Научно-исследовательский семинар им. П. С. Александрова (20 февраля 2014 г.);

5. Теория групп (17 февраля 2017 г.);

6. Московский семинар по теории чисел (10 марта 2017 г.).

Математический институт им. В. А. Стеклова:

1. Современные проблемы теории чисел (23 апреля 2015 г., 22 сентября 2016 г.);

2. Семинар по арифметической геометрии (20 марта 2017 г.).

Санкт-Петербургское отделение математического института им. В. А. Стеклова:

1. Общеинститутский математический семинар (20 февраля 2017 г.);

2. Городской алгебраический семинар им. Д. К. Фаддеева (20 февраля 2017 г.).

Результаты диссертации докладывались на следующих российских и международных конференциях.

1. Алгебраический коллоквиум, посв. 85-летию чл.-корр. РАН проф. А. И. Кострикина и 90-летию проф. Л. А. Скорнякова (Москва, МГУ, 17 февраля 2014 г.);

2. Международная конференция “Алгебра и комбинаторика”, посвященная 60-летию чл.-корр. РАН проф. А. А. Махнева (Екатеринбург, ИММ УРО РАН, 03 июня – 07 июня 2013 г.);

3. VI школа-конференция “Алгебры Ли, алгебраические группы и теория инвариантов” (Москва, МГУ, 30 января – 04 февраля 2017 г.);

4. Международная школа-конференция “Современные проблемы математики” (Екатеринбург, ИММ УРО РАН, 05 февраля – 11 февраля 2017 г.);

5. Международная конференция “Математическая теория оптимального управления”, посвященная 90-летию академика Р. В. Гамкрелидзе (Москва, МИАН, 01 июня – 02 июня 2017 г.);

6. Международная алгебраическая конференция, посвященная 110-летию со дня рождения профессора А. Г. Куроша (Москва, МГУ, 23 мая – 25 мая 2018 г.).

### Публикации

По теме диссертации опубликовано 16 работ в ведущих российских и зарубежных журналах перечня RSCI WebOfScience, WebOfScience, Scopus: все работы, опубликованные в русскоязычных журналах, входят в перечень RSCI WebOfScience; все переводные версии опубликованных работ а также все англоязычные работы входят в Scopus; в WebOfSicence входят все переводные версии опубликованных работ (за исключением [2], [6], [8], [10] и [13]) а также англоязычные работы [15] и [16]. Без соавторов опубликовано 12 работ.

### Теоретическая и практическая ценность работы

Диссертация имеет теоретический характер. Ее результаты могут найти применение в теории погружения, теории Галуа, теории представлений конечных групп, теории оптимального управления.

### Структура и объем диссертации

Диссертация состоит из введения, 4 глав и заключения. Главы подразделяются на разделы и пункты. Все результаты глав 1–4 получены диссертантом самостоятельно.

Диссертация написана на 201 странице. Список литературы состоит из 101 наименования.

## Краткое содержание работы

**Во введении** обосновывается актуальность темы диссертации, кратко излагаются история вопроса и основные результаты диссертанта, даются сведения о публикациях диссертанта по теме диссертации, о структуре и апробации работы.

**В главе 1** исследуется проблема А. В. Яковлева о характеризации ультраразрешимых групповых расширений.

**Проблема** (1.1). *Пусть*

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\varphi} F \longrightarrow 1 \tag{1.1}$$

*– расширение конечных групп с абелевым ядром $A$. При каких условиях существует расширение Галуа числовых полей $K/k$ с группой $F$, такое что получившаяся задача погружения ультраразрешима?*

Предположим, что $A$ – циклическая $p$-группа с порождающим элементом $a$ порядка $p^n$ для некоторого $n \geqslant 2$. Пусть $F$ – некоторая $p$-группа. Превратим $A$ в $F$-модуль с помощью гомоморфизма $\gamma\colon F \to \operatorname{Aut} A$. Вложение $F$-модулей $\Phi(A) \hookrightarrow A$ индуцирует гомоморфизм когомологий $\alpha\colon H^2(F, \Phi(A)) \to H^2(F, A)$. В 1.2.3 дается в удобных для дальнейшего терминах описание ядра $\ker\alpha$. Для этого по группе $F$ строится абелева $p$-группу $F_0$ с тем же числом образующих, что и $F$. При этом действие группы $F_0$ на $A$ будет "таким же" как и действие $F$. Более точно это выражено в условиях 1.1.

**Условия** (1.1)**.** Пусть $F = \ker\gamma$. В таком случае в качестве $F_0$ рассмотрим элементарную абелеву группу ранга $d(F)$; при этом определен естественный эпиморфизм $\theta\colon F \to F_0$. Группу $A$ можно рассматривать как тривиальный $F_0$-модуль.

Пусть $F$ действует на $A$ нетривиально. Тогда существует элемент $f_1 \in F$, такой что $\gamma(f_1)$ порождает $\operatorname{im}\gamma$. При этом без ограничения общности $a^{f_1} = a^{1+p^i}$ для некоторого $i \in [1, n-1] \cap \mathbb{N}$. В качестве группы $F_0$ в этом случае возьмем абелеву группу с образующими $f_1^0, \ldots, f_{d(F)}^0$, причем $f_1^0$ имеет такой же порядок как и $\gamma(f_1)$, а образующие[50] $f_2^0, \ldots, f_{d(F)}^0$ являются элементами порядка $p$. На $A$ можно ввести структуру $F_0$-модуля, положив $a^{f_1^0} = a^{f_1}$ и $a^{f_r^0} = a$ для всех $r > 1$. В силу леммы 1.3 элемент $f_1$ можно дополнить (если $d(F) > 1$) до системы образующих $\{f_r\}_{r=1}^{d(F)}$ группы $F$ таким образом, что $a^{f_r} = a$ для всех $r > 1$. Ясно, что соответствие $f_r \mapsto f_r^0$ корректно продолжается до эпиморфизма $\theta\colon F \to F_0$.

Эпиморфизм $\theta$ из условий 1.1 позволяет корректно определить гомоморфизмы[51] $\lambda_1\colon H^2(F_0, \Phi(A)) \to H^2(F, \Phi(A))$, $\lambda_2\colon H^2(F_0, A) \to H^2(F, A)$. При этом следующая диаграмма

$$\begin{array}{ccc} H^2(F, \Phi(A)) & \xrightarrow{\alpha} & H^2(F, A) \\ {\scriptstyle\lambda_1}\uparrow & & {\scriptstyle\lambda_2}\uparrow \\ H^2(F_0, \Phi(A)) & \xrightarrow{\beta} & H^2(F_0, A), \end{array} \tag{1.5}$$

где горизонтальные стрелки – гомоморфизмы, индуцированные модульным вложением $\Phi(A) \hookrightarrow A$, является коммутативной. Далее, искомое описание строится с помощью лемм 1.5, 1.6 и описании ядра $\ker\beta$ нижней строки диаграммы (1.5), указанном в леммах 1.7 и 1.8.

**Лемма** (1.5)**.** *Гомоморфизм $\lambda_1$ диаграммы (1.5) индуцирует эпиморфизм ядер $\lambda_1\colon \ker\beta \to \ker\alpha$.*

[50] Если, конечно, $d(F) > 1$.

[51] Ясно, что $\Phi(A)$ является как $F$- так и $F_0$-подмодулем модуля $A$: ведь $A$ – циклическая $p$ группа.

**Лемма** (1.6). *Пусть* $(K_0/k,\, G_0,\, \varphi_0)$ *– ультраразрешимая задача погружения с циклическим ядром* $A$*, причем* $G_0$ *– p-группа, а* $F_0 = \mathrm{Gal}(K_0/k)$*. Сделаем подъем до задачи* $(K/k,\, G,\, \varphi)$*, где* $G$ *– p-группа, а* $F = \mathrm{Gal}(K/k)$*. Если* $d(F_0) = d(F) < d(G_0)$*, то задача* $(K/k,\, G,\, \varphi)$ *ультраразрешима.*

**Лемма** (1.7). *Ядро* $\ker\beta$ *из диаграммы (1.5) порождается при* $i < n$ *следующими расширениями*

$$\begin{aligned} X_1 = \langle d,\, c_1, \ldots,\, c_{d(F)} \mid d^{p^{n-1}} = 1,\, c_1^{p^{n-i}} = d^{p^{n-i-1}},\, c_r^p = 1 \,\forall\, r > 1, \\ [c_s,\, c_t] = 1 \,\forall\, s < t,\, d^{c_1} = d^{1+p^i},\, d^{c_r} = d \,\forall\, r > 1\rangle, \\ X_r = \langle d,\, c_1, \ldots,\, c_{d(F)} \mid d^{p^{n-1}} = 1,\, c_1^{p^{n-i}} = 1,\, c_s^p = 1 \,\forall\, 1 < s \neq r,\, c_r^p = d, \\ [c_1,\, c_r] = d^{-p^{i-1}},\, [c_s,\, c_t] = 1 \,\forall\, s < t : (s,\, t) \neq (1,\, r), \\ d^{c_1} = d^{1+p^i},\, d^{c_s} = d \,\forall\, s > 1\rangle \,\forall\, r > 1. \end{aligned} \tag{1.7}$$

**Лемма** (1.8). *Ядро* $\ker\beta$ *из диаграммы (1.5) порождается при* $i = n$ *следующими расширениями*

$$\begin{aligned} X_1 = \langle d,\, c_1, \ldots,\, c_{d(F)} \mid d^{p^{n-1}} = 1,\, c_1^p = d,\, c_r^p = 1 \,\forall\, r > 1, \\ [c_s,\, c_t] = 1 \,\forall\, s < t,\, d^{c_r} = d \,\forall\, r > 1\rangle, \\ X_r = \langle d,\, c_1, \ldots,\, c_{d(F)} \mid d^{p^{n-1}} = 1,\, c_1^p = 1,\, c_s^p = 1 \,\forall\, 1 < s \neq r,\, c_r^p = d, \\ [c_s,\, c_t] = 1 \,\forall\, s < t,\, d^{c_s} = d \,\forall\, s > 1\rangle \,\forall\, r > 1. \end{aligned} \tag{1.8}$$

Пусть $F$ и $A$ – $p$-группы, причем $A$ циклическая порядка $p^n$, на которой введена структура $F$-модуля. Рассмотрим нетривиальный класс $h \in H^2(F,\, A)$. Предположим, что задан такой эпиморфизм $\theta\colon F \to F_1$, что, во-первых, $A$ – тривиальный $\ker\theta$-модуль, а, во-вторых, подъем некоторого класса $h_1 \in H^2(F_1,\, A)$ в группу $H^2(F,\, A)$, индуцированный эпиморфизмом $\theta$, дает класс $h$. Предположим, наконец, что $d(F_1) = d(F)$; кроме того будем считать, что группа $F_1$ реализована как группа Галуа расширения локальных полей $K_1/k$. В таком случае класс $h_1$ порождает некоторую задачу погружения $(K_1/k,\, G_1,\, \varphi_1)$.

Пусть расширение $K_1/k$ таково, что задача $(K_1/k,\, G_1,\, \varphi_1)$ ультраразрешима. В таком случае в силу $d(F_1) = d(F)$ и леммы 1.6 если задача $(K_1/k,\, F,\, \theta)$ разрешима, то любое ее решение $K$ задает ультраразрешимую задачу погружения $(K/k,\, G,\, \varphi)$ с классом $h$.

Конкретизируем условия разрешимости задачи $(K_1/k,\, F,\, \theta)$. В силу результатов[52] и[53] для разрешимости такой задачи необходима и достаточна разрешимость всех элементарных сопутствующих брауэровских задач, отвечающих $F$-операторным характерам ядра $\ker\theta$. Будем считать, что $\varepsilon_{p^n} \notin K_1$. В

[52] В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа*, М. Наука, 1990, Гл. 4, §1, Теорема 4.1.2.

[53] Там же, Гл. 3, §14, Теорема 3.14.1.

таком случае все такие задачи имеют циклическое ядро порядка $p^j$, причем $j < n$. Ясно, что любой класс $h_\chi \in H^2(F_1, \langle\varepsilon_{p^j}\rangle)$, отвечающий такой задаче, определяет расширение $F_1$ до $F_\chi$ с помощью $\langle\varepsilon_{p^j}\rangle$, причем $F_\chi$ – гомоморфный образ группы $F$. В 1.2.4 определяется понятие "плохого класса".

**Определение** (1.1). Класс $\widehat{h} \in H^2(F_1, \langle\varepsilon_{p^j}\rangle)$ будем называть "плохим" для $h$, если он определяет такое расширение $F_1$ до $\widehat{F}$ с помощью $\langle\varepsilon_{p^j}\rangle$, что подъем класса $h_1$ в группу $H^2(\widehat{F}, A)$, индуцированный эпиморфизмом $\theta$, задает тривиальное расширение.

Доказывается лемма 1.9, используемая в 1.3.4 и 1.3.5.

**Лемма** (1.9). *Рассмотрим классы*

$$\{h_{\chi,j} \in H^2(F_1, \langle\varepsilon_{p^j}\rangle) \mid \chi \in \mathrm{Hom}_F(\ker\theta, \langle\varepsilon_{p^j}\rangle)\}_{j=1}^{j_0},$$

*определяющие всевозможные элементарные сопутствующие брауэровские задачи для* $(K_1/k, F, \theta)$. *Образы данных классов в группе* $H^2(F_1, \langle\varepsilon_{p^{j_0}}\rangle)$ *при гомоморфизме, индуцированном вложением* $\langle\varepsilon_{p^j}\rangle$ *в* $\langle\varepsilon_{p^{j_0}}\rangle$, *порождают подгруппу, не содержащую плохих для* $h$ *элементов.*

В 1.2.5 дается в удовлетворительных терминах решение задачи погружения с ядром порядка $p$ для $p > 2$. Именно, предложение 1.1 обобщает на случай $p > 2$ результат А. Ледета[54], доказанный им при $p = 2$. Рассмотрим некоторое групповое расширение

$$1 \longrightarrow \langle\varepsilon_p\rangle \longrightarrow \widehat{H} \xrightarrow{\pi} X \times Y \longrightarrow 1. \tag{1.14}$$

**Предложение** (1.1). *Пусть (1.14) – неполупрямое расширение с классом* $h \in H^2(X \times Y, \langle\varepsilon_p\rangle)$. *Пусть* $K_X/k$ *и* $K_Y/k$ *– расширения Галуа*[55] *с группами* $X$ *и* $Y$ *соответственно. Пусть* $\{x_r\}_{r=1}^{d(X)}$, $\{y_r\}_{r=1}^{d(Y)}$ *– соответственно образующие групп* $X$ *и* $Y$. *Выберем* $a_1, \ldots, a_{d(X)}$ *и* $b_1, \ldots, b_{d(Y)}$ *из* $k^* \setminus k^{*p}$ *таким образом, чтобы* $\sqrt[p]{a_i} \in K_X$ *для всех* $i$, *а* $\sqrt[p]{b_j} \in K_Y$ *для всех* $j$, *причем*

$$\sqrt[p]{a_i}^{x_r} = \varepsilon_p^{\delta_{ri}}\sqrt[p]{a_i}, \qquad \sqrt[p]{b_j}^{y_l} = \varepsilon_p^{\delta_{lj}}\sqrt[p]{b_j}.$$

*Выберем прообразы* $\overline{x}_1, \ldots, \overline{x}_{d(X)}$, $\overline{y}_1, \ldots, \overline{y}_{d(Y)}$ *для элементов* $x_1, \ldots, x_{d(X)}$ *и* $y_1, \ldots, y_{d(Y)}$ *относительно эпиморфизма* $\pi$; *при этом для всех* $i$, $j$ *выполнено* $[\overline{x}_i, \overline{y}_j] = \varepsilon_p^{d_{ij}}$. *Тогда для* $K = K_X \otimes_k K_Y$ *задача погружения* $(K/k, H, \pi)$ *разрешима тогда и только тогда, когда в* $B(k)$

$$[K_X, X, \mathrm{res}_{X\times Y\to X} h][K_Y, Y, \mathrm{res}_{X\times Y\to Y} h]\prod_{i,j} k[a_i, b_j]^{d_{ij}} \sim 1.$$

[54] A. Ledet, On 2-groups as Galois groups, *Canad. J. Math.*, **47:6**, (1995), 1253–1273, Theorem 2.4.

[55] Линейно разделенные над $k$; при этом мы предполагаем $\varepsilon_p \in k$.

В 1.2.6 мы решаем с помощью предложения 1.1 задачи погружения, связанные с расширениями из ядра $\ker\beta$ диаграммы (1.5).

В разделе 1.3 рассматриваются $p$-расширения с циклическим ядром, обладающие свойством минимальности. При этом существенно используется результат В. В. Ишханова и Б Б. Лурье[56] и результат Б. Б. Лурье[57]. В 1.3.1, 1.3.2 и 1.3.3 исследуется случай минимальных $p$-расширений нечетного порядка с $d(F) = 2$. Мы используем локальную теорию полей классов и описание группы Галуа максимального $p$-расширения локального поля, полученное С. П. Демушкиным[58].

**Теорема** (1.1). *Пусть (1.1) – минимальное $p$-расширение, у которого $d(F) = 2$, тогда (1.1) ультраразрешимо.*

В 1.3.4 и 1.3.5 исследуется ультраразрешимость $p$-расширений нечетного порядка с циклическим ядром и $d(F) > 2$ со свойством минимальности. Ключевую роль при этом играет лемма 1.9. Исследование проходит по той же схеме, что в случае $d(F) = 2$, однако становится существенно более сложным.

В теореме 1.2 (случай $d(F) = 2$ получается из теоремы 1.1) устанавливается ультраразрешимость произвольного минимального $p$-расширения нечетного порядка с циклическим ядром.

**Теорема** (1.2). *Пусть (1.1) – минимальное $p$-расширение с циклическим ядром, тогда (1.1) ультраразрешимо.*

В 1.3.6 даются некоторые обобщения теоремы 1.2 на случай минимальных 2-расширений.

**Условия** (1.4). Пусть (1.1) – минимальное 2-расширение с циклическим ядром порядка $2^n$ для $n \geqslant 3$ с порождающим элементом $a$. Группа автоморфизмов $\operatorname{Aut} A$ в этом случае порождается элементами $\sigma$, $\tau$, причем

$$a^\sigma = a^5,\ a^\tau = a^{-1}.$$

Пусть либо $A$ является тривиальным $F$-модулем, либо действие $F$ на $A$ определяется гомоморфизмом $\gamma\colon F \to \operatorname{Aut} A$, образ которого является подгруппой в группе $\langle\sigma\rangle$.

**Следствие** (1.2). *Пусть (1.1) – минимальное 2-расширение с циклическим ядром $A$ и факторгруппой $F$, причем выполнены условия 1.4. Тогда (1.1) ультраразрешимо.*

---

[56] В. В. Ишханов, Б. Б. Лурье, Универсально разрешимые задачи погружения с циклическим ядром, *Зап. научн. сем. ПОМИ*, **265**, (1999), 189–197, Лемма.

[57] В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа*, М. Наука, 1990, Гл. 4, §1, Теорема 4.1.2.

[58] С. П. Демушкин, Группа максимального $p$-расширения локального поля, *Изв. АН СССР, сер. матем.*, **25:3**, (1961), 329–346, Теорема.

В разделе 1.4 результаты раздела 1.3 обобщаются с $p$-расширений на расширения нечетного порядка с циклическим ядром. Именно, для таких расширений получается полное решение проблемы 1.1 в теореме 1.7.

**Теорема** (1.7)**.** *Пусть (1.1) — расширение нечетного порядка с циклическим ядром $A$. Расширение (1.1) ультраразрешимо тогда и только тогда, когда все его $p$-силовские подрасширения для всех $p \mid |A|$ не являются полупрямыми.*

Данный результат основывается на результатах раздела 1.3 и теореме 1.6.

**Теорема** (1.6)**.** *Пусть (1.1) — неполупрямое $p$-расширение нечетного порядка с циклическим ядром $A$ и факторгруппой $F$. Пусть любое сопутствующее расширение второго рода к (1.1) уже является полупрямым. Тогда существует расширение Галуа локальных полей $K/k$ с группой Галуа $F$, такое что задача погружения $(K/k, G, \varphi)$, соответствующая расширению (1.1) ультраразрешима.*

Используя результаты теоремы 1.4, следствия 1.2 и пункта 1.4.2, в теореме 1.13 (надлежащим образом обобщающей теорему 1.7) дается решение проблемы А. В. Яковлева для достаточно широкого класса 2-расширений с циклическим ядром.

**Теорема** (1.13)**.** *Пусть (1.1) – 2-расширение с циклическим ядром, определяемое классом $h \in H^2(F, A)$. Пусть существует подгруппа $F_1$ группы $F$, удовлетворяющая одному из следующих условий:*

1. *либо $F_1$ циклическая, а ограничение $h_1 \in H^2(F_1, A)$ класса $h$ не является обобщенно-кватернионным (кроме случаев $|A| \in \{4, 8\}$);*
2. *либо ограничение $h_1 \in H^2(F_1, A)$ класса $h$ определяет минимальное расширение, а $F_1$-модульное действие на $A$ определяется условиями 1.4.*

*Тогда расширение (1.1) ультраразрешимо.*

Раздел 1.5 посвящен исследованию условий ультраразрешимости кватернионных расширений. До сих пор результаты по проблеме 1.1 (т.е. результаты раздела 1.4, кроме теоремы 1.5) использовали построение ультраразрешимых задач погружения над локальными полями по расширению (1.1) и последующее применение[59] вместе с[60]. Данные результаты составляют так называемый *локально-глобальный* принцип в теории ультраразрешимости: если ультраразрешимость расширения удалось показать в локальных полях, то

[59] А. В. Яковлев, Ультраразрешимые задачи погружения для числовых полей, *Алгебра и анализ*, **27:6**, (2015), 260–263, Теорема 1.

[60] Д. Д. Киселев, А. В. Яковлев, Ультраразрешимые и силовские расширения с циклическим ядром, *Алгебра и анализ*, **30:1**, (2018), 128–138, Предложение 1.

отсюда вытекает ультраразрешимость в числовых полях, т.е. ультраразрешимость расширения в смысле проблемы 1.1. Естественно возникает следующий вопрос: *пусть имеется ультраразрешимое $p$-расширение, будет ли оно ультраразрешимым в локальных полях?* В 1.5.1 мы выясняем условия согласности Д. К. Фаддеева-Х. Хассе для задачи погружения, связанной с обобщенно-кватернионным расширением

$$1 \longrightarrow \langle a\rangle \longrightarrow \langle a,\, b \mid a^{2^n}=1,\, b^2=a^{2^{n-1}},\, a^b=a^{-1}\rangle \xrightarrow{\varphi} \langle f\rangle, \qquad (1.101)$$

где[61] $\varphi(b)=f$, $\varphi(a)=1$. В 1.5.2 мы исследуем ультраразрешимость кватернионного расширения с циклическим ядром порядка 8. Наконец, в 1.5.3 мы исследуем ультраразрешимость кватернионного расширения с циклическим ядром порядка 16. Указанный результат составляет содержание теоремы 1.10.

**Теорема** (1.10). *Задача погружения (1.101) при $k=\mathbb{Q}$, $d=7$, $n=4$ является ультраразрешимой.*

**Следствие** (1.4). *Расширение (1.1), соответствующее задаче (1.101) при $n=4$, является ультраразрешимым, но не является ультраразрешимым ни в каких локальных полях.*

Следствие (1.4) дает отрицательный пример к локально-глобальному принципу в теории ультраразрешимости. В 1.5.4 мы показываем, что группа порядка 2 ультраразрешимо накрывается группой обобщенных кватернионов порядка 16 с помощью группы $Q_8$. Именно, рассмотрим задачу погружения $(K/k,\, Q_{16},\, \varphi,\, Q_8)$, где $Q_{16}$ задана в (1.101) для $n=3$, а $Q_8$ вложена в $Q_{16}$ как нормальная подгруппа, порожденная элементами $a^2$, $b$. При этом $\varphi(b)=1$, а $\varphi(a)$ порождает группу $\mathrm{Gal}(K/k)$.

**Теорема** (1.11). *Задача $(K/k,\, Q_{16},\, \varphi,\, Q_8)$ при $k=\mathbb{Q}$, а $K=k(\sqrt{7})$ является ультраразрешимой.*

В разделе 1.6 рассматриваются $p$-расширения с абелевым нециклическим ядром. Показывается принципиальное отличие от случая $p$-расширений с циклическим ядром. Именно, на основе конструкции Б. Б. Лурье универсально разрешимых неполупрямых групповых расширений (см.[62]) и конструкции Д. К. Фаддеева (см.[63]) отображения перенесения устанавливается теорема 1.14.

[61] $f$ – порождающий элемент группы $\mathrm{Gal}(k(\sqrt{d})/k)$.

[62] Б. Б. Лурье, Об универсально разрешимых задачах погружения, *Тр. МИАН*, **183**, (1990), 121–126, Теорема 1.

[63] В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа*, М. Наука, 1990, Гл. 3, §7.

**Теорема** (1.14). *Для любой конечной $p$-группы нечетного порядка $\widetilde{F}$ существует неполупрямое $p$-расширение с абелевым ядром и $\widetilde{F}$ в качестве факторгруппы, которое не является ультраразрешимым.*

Наконец, в разделе 1.7 ставится *задача вложения*, в некотором смысле двойственная задаче погружения. Именно, пусть $\varphi\colon X \to Y$ – заданный мономорфизм конечных $p$-групп, а $\psi\colon X \to \operatorname{Aut} K$ – заданное вложение $X$ в группу автоморфизмов некоторого поля $K$. При каких условиях существует гомоморфизм $\omega\colon Y \to \operatorname{Aut} K$, делающий следующую диаграмму

$$\begin{array}{ccccc} 1 & \longrightarrow & X & \xrightarrow{\varphi} & Y \\ & & {\scriptstyle\psi}\big\downarrow & & {\scriptstyle\omega}\big\downarrow \\ & & \operatorname{Aut} K & = & \operatorname{Aut} K \end{array} \tag{1.117}$$

коммутативной? Ясно, что задача вложения в некотором смысле двойственна задаче погружения, но намного более сложна: во-первых, инъективные объекты устроены сложнее проективных, во-вторых, если $K$ – числовое поле, то группа $\operatorname{Aut} K$ конечна, что затрудняет использование $\operatorname{Aut} K$ как некоего "универсального объекта". Изучение задачи вложения может дать альтернативный подход к проблеме А. В. Яковлева на основе индуктивных рассуждений с использованием результатов раздела 1.3 и локально-глобального принципа в теории ультраразрешимости (см.[64] а также[65]). В одном частном случае изучение условий разрешимости задачи вложения проводится в разделе 3.3 (см. теорему 3.2).

**В главе 2** строятся наилучшие равномерные оценки индекса Шура над полем $\mathbb{Q}$ неприводимых комплексных характеров конечных групп на классах групп заданного конечного порядка $n$ (класс $G_{\mathrm{ord}}(n)$) и групп заданной экспоненты $n$ (класс $G_{\exp}(n)$). В разделе 2.1 дается описание главы и используемых обозначений (см. п. 2.1.3).

В разделе 2.2 строятся функции $\psi$ и $\gamma$ (описание данных функций дано в 2.2.2), удовлетворяющие свойству: для любой группы $G \in G_{\mathrm{ord}}(n)$ и любого $\chi \in \operatorname{Irr} G$ выполнено $m_{\mathbb{Q}}(\chi) \mid \psi(n)$, причем указанная оценка является наилучшей на классе $G_{\mathrm{ord}}(n)$; для любой группы $G \in G_{\exp}(n)$ и любого $\chi \in \operatorname{Irr} G$ выполнено $m_{\mathbb{Q}}(\chi) \mid \gamma(n)$, причем указанная оценка является наилучшей на классе $G_{\exp}(n)$. Данный результат составляет содержание теоремы 2.1.

Пусть задано натуральное число $n$, тогда имеется разложение $n = p_1^{k_1} \dots p_s^{k_s}$ на простые множители, причем $p_1 < p_2 < \dots < p_s$. Определим функцию $\psi\colon \mathbb{N} \to \mathbb{N}$ следующим образом:

[64] А. В. Яковлев, Ультраразрешимые задачи погружения для числовых полей, *Алгебра и анализ*, **27:6**, (2015), 260–263, Теорема 1.

[65] Д. Д. Киселев, А. В. Яковлев, Ультраразрешимые и силовские расширения с циклическим ядром, *Алгебра и анализ*, **30:1**, (2018), 128–138, Предложение 1.

1. $\psi(1) := 1$ (при этом, естественно, $s = 0$); если $s = 1$, $p_1 = 2$, $k_1 \geqslant 3$, то положим $\psi(n) := 2$; если $s = 1$, $p_1 > 2$ либо $s = 1$, $p_1 = 2$, $k_1 \leqslant 2$, то полагаем $\psi(n) := 1$;

2. Пусть $s \geqslant 2$. Для каждого $i \in \overline{1,\, s}$ положим

$$\psi_1^{(p_i)}(n) := \max\{p_i^r \mid 2r \leqslant k_i,\, \exists\, j \in \overline{1,\, s} \setminus \{i\} : \\ p_j \equiv 1 (\mathrm{mod}\, p_i^r),\, p_i^r (p_j - 1)_{p_i} \leqslant p_i^{k_i}\}.$$

   Если максимум берется по пустому множеству, то полагаем

$$\psi_1^{(p_i)}(n) := \begin{cases} 1, & \text{при } p_i \neq 2, \\ 2, & \text{при } p_i = 2,\, k_i \geqslant 3, \\ 1, & \text{при } p_i = 2,\, k_i \leqslant 2. \end{cases}$$

   В случае $s = 2$ полагаем $\psi_2^{(p^i)}(n) := 1$.

3. Пусть $s \geqslant 3$. Для каждого $i \in \overline{1,\, s}$ положим

$$\psi_2^{(p_i)}(n) := \max\{p_i^r \mid 3r \leqslant k_i,\, \exists\, j_1,\, j_2 \in \overline{1,\, s} \setminus \{i\} : \\ j_1 \neq j_2,\ p_{j_1} \equiv 1 (\mathrm{mod}\, p_i^r),\, p_{j_2} \equiv 1 (\mathrm{mod}\, p_i^r), \\ \max\{|p_{j_1} \bmod p_{j_2}|_{p_i},\, |p_{j_2} \bmod p_{j_1}|_{p_i}\} \geqslant p_i^r\}.$$

   Если максимум в берется по пустому множеству, то полагаем

$$\psi_2^{(p_i)}(n) := \begin{cases} 1, & \text{при } p_i \neq 2, \\ 2, & \text{при } p_i = 2,\, k_i \geqslant 3, \\ 1, & \text{при } p_i = 2,\, k_i \leqslant 2. \end{cases}$$

4. Если $\psi(n)$ еще не было определено, то $\psi(n) := \prod\limits_{i=1}^{s} \max\{\psi_1^{(p_i)}(n),\, \psi_2^{(p_i)}(n)\}$.

Аналогичным образом определяется функция $\gamma\colon \mathbb{N} \to \mathbb{N}$.

1. $\gamma(1) := 1$ (при этом, естественно, $s = 0$); если $s = 1$, $p_1 = 2$, $k_1 \geqslant 2$, то положим $\gamma(n) := 2$; если $s = 1$, $p_1 > 2$ либо $s = 1$, $p_1 = 2$, $k_1 = 1$, то полагаем $\gamma(n) := 1$;

2. Пусть $s \geqslant 2$. Для каждого $i \in \overline{1,\, s}$ положим

$$\gamma_1^{(p_i)}(n) := \max\{p_i^r \mid 2r \leqslant k_i,\, \exists\, j \in \overline{1,\, s} \setminus \{i\} : \\ p_j \equiv 1 (\mathrm{mod}\, p_i^r),\, p_i^r (p_j - 1)_{p_i} \leqslant p_i^{k_i}\}.$$

Если максимум в берется по пустому множеству, то полагаем

$$\gamma_1^{(p_i)}(n) := \begin{cases} 1, & \text{при } p_i \neq 2, \\ 2, & \text{при } p_i = 2,\ k_i \geqslant 2, \\ 1, & \text{при } p_i = 2,\ k_i = 1. \end{cases}$$

В случае $s = 2$ полагаем $\gamma_2^{(p^i)}(n) := 1$.

3. Пусть $s \geqslant 3$. Если $p_1 = 2$, то положим $f_n(p_1) := k_1 - 1$. Для $p_1 \neq 2$ полагаем $f_n(p_1) := k_1$. Для $i \in \overline{2,\, s}$ полагаем $f_n(p_i) := k_i$. Для каждого $i \in \overline{1,\, s}$ положим

$$\gamma_2^{(p_i)}(n) := \max\{p_i^r \mid r \leqslant f_n(p_i),\, \exists\, j_1,\, j_2 \in \overline{1,\, s} \setminus \{i\} : \\ j_1 \neq j_2,\ p_{j_1} \equiv 1 (\mathrm{mod}\, p_i^r),\, p_{j_2} \equiv 1 (\mathrm{mod}\, p_i^r), \\ \max\{|p_{j_1} \bmod p_{j_2}|_{p_i},\, |p_{j_2} \bmod p_{j_1}|_{p_i}\} \geqslant p_i^r\}.$$

Если максимум в берется по пустому множеству, то полагаем

$$\gamma_2^{(p_i)}(n) := \begin{cases} 1, & \text{при } p_i \neq 2, \\ 2, & \text{при } p_i = 2,\ k_i \geqslant 2, \\ 1, & \text{при } p_i = 2,\ k_i = 1. \end{cases}$$

4. Если $\gamma(n)$ еще не было определено, то $\gamma(n) := \prod\limits_{i=1}^{s} \max\{\gamma_1^{(p_i)}(n),\, \gamma_2^{(p_i)}(n)\}$.

**Теорема** (2.1). *Пусть $n$ – произвольное натуральное число. Для любой группы $G \in \mathfrak{G}_{\mathrm{ord}}(n)$ и любого характера $\chi \in \mathrm{Irr}\, G$ справедлива оптимальная оценка $m_{\mathbb{Q}}(\chi) \mid \psi(n)$. Для любой конечной группы $G \in \mathfrak{G}_{exp}(n)$ и любого характера $\chi \in \mathrm{Irr}\, G$ справедлива оптимальная оценка $m_{\mathbb{Q}}(\chi) \mid \gamma(n)$.*

В разделе 2.3 рассматриваются вопросы реализуемости неприводимых комплексных представлений конечных групп в минимальном расширении поля рациональных чисел. Более точно, дано неприводимое комплексное представление группы $G$ с характером $\chi \in \mathrm{Irr}\, G$ и $\mathbb{Q}$-индексом Шура $m_{\mathbb{Q}}(\chi)$, при каких условиях указанное представление реализуется над полем $K$, степень которого над $\mathbb{Q}(\chi)$ равна $m_{\mathbb{Q}}(\chi)$? В 2.3.1 дается обобщение результата Б. Фейна[66] о том, что если $n = p^\alpha q^\beta$ для некоторых простых $p \neq q$, то ответ на вопрос о реализуемости положителен.

**Теорема** (2.2). *Пусть конечная группа $G$ экспоненты $n$ такова, что для любого простого $p \mid n$ существует не более одного простого $q \mid n$ такого*

[66] B. Fein, Minimal spliting fields for group representations, *Pacific J. Math.*, **51:2**, (1974), 427–431, Theorem.

*что* $p \mid (q-1)$. *Тогда для произвольного неприводимого характера* $\chi \in \operatorname{Irr} G$ *с индексом Шура* $m_{\mathbb{Q}}(\chi) = m$, *удовлетворяющим условию* $m_2 \in \mathbb{Z}_{\geqslant 4} \cup \{1\}$, *существует поле* $L$ *в башне* $\mathbb{Q}(\chi) \subseteq L \subseteq \mathbb{Q}(\varepsilon_n)$, *такое что* $(L : \mathbb{Q}(\chi)) = m$, *причем* $m_L(\chi) = 1$.

Наконец, в 2.3.2 усиливается хорошо известная теорема Грюнвальда-Ванга о существовании циклического поля разложения для центрально-простой конечномерной алгебры над числовым полем. Указанное обобщение опирается на результат В. В. Ишханова[67], где в когомологических терминах найдено необходимое и достаточное условие существования у разрешимой задачи погружения с абелевым ядром над числовыми полями решения, имеющего заданное локальное поведение в конечном числе точек основного поля. Именно, мы исследуем, при каких достаточных условиях неприводимое представление конечной группы $G$ с характером $\chi \in \operatorname{Irr} G$ и индексом Шура $m_k(\chi) = m > 1$ над полем алгебраических чисел $k$ реализуется в поле $L$ степени $m$ над $k(\chi)$, причем таком, что $L/k(\chi)$ – циклическое расширение Галуа, содержащее заданное циклическое подрасширение $K/k(\chi)$ степени $\widetilde{m} \mid m$.

Рассмотрим задачу погружения заданного циклического расширения Галуа $K/k(\chi)$ с группой $F$ порядка $\widetilde{m}$ в расширение с циклической группой Галуа $H$ порядка $m$ или, кратко, задачу $(K/k(\chi),\, H,\, \varphi)$, где $\varphi\colon H \to F$ – естественный эпиморфизм. Для каждого простого $p \mid m$, такого что $m_{k(\chi)\cdot\mathbb{Q}_p}(\chi) = m^{(p)} \neq 1$ выберем произвольным образом простую точку $\mathfrak{p}$ поля $k(\chi)$, лежащую над ним. Заметим, что вообще говоря алгебра Галуа $K \otimes_{k(\chi)} k(\chi)_{\mathfrak{p}}$ не является полем, но в любом случае определено поле-ядро $K_{\mathfrak{p}}$, являющееся расширением Галуа поля $k(\chi)_{\mathfrak{p}}$ с группой Галуа $F_{\mathfrak{p}}$, допускающей вложение в $F = \operatorname{Gal}(K/k(\chi)) \cong \operatorname{Gal}(K \otimes_{k(\chi)} k(\chi)_{\mathfrak{p}}/k(\chi)_{\mathfrak{p}})$. Пусть $H_{\mathfrak{p}}$ – полный прообраз подгруппы $F_{\mathfrak{p}}$ в группе $H$ при эпиморфизме $\varphi_{\mathfrak{p}}$. Очевидно, что для существования поля $L$ степени $m$ над $k(\chi)$, такого что $m_L(\chi) = 1$, причем решающего задачу $(K/k(\chi),\, H,\, \varphi)$, необходимо выполнение условия

$$m^{(p)} \mid |H_{\mathfrak{p}}| \,\forall\, p :\ m^{(p)} \neq 1. \tag{2.3}$$

Пусть для краткости $n := m/\widetilde{m}$.

**Теорема** (2.3). *Пусть циклическое расширение Галуа* $K/k(\chi)$ *таково, что*

$$\pi(\widetilde{m}) = \pi(n) = \pi\left(\frac{|H_{\mathfrak{p}}|}{n}\right).$$

*Тогда для существования поля* $L$ *степени* $m$, *содержащего* $K$ *в качестве подполя и имеющего над* $k(\chi)$ *циклическую группу Галуа со свойством* $m_L(\chi) =$

[67] В. В. Ишханов, Задача погружения с данными локализациями, *Изв. АН СССР. Сер. матем.*, **39:3**, (1975), 512–522, Теорема 1.

1, *необходимо и достаточно, чтобы, помимо условия (2.3), образ класса* $c \in H^2(\mathrm{Gal}(K/k(\chi)), \langle\varepsilon_n\rangle)$, *соответствующего расширению группы* $F$ *до* $H$ *с помощью* $\ker\varphi$, *в группе* $H^2(\mathrm{Gal}(K/k(\chi)), K^*)$ *при отображении, индуцированном вложением* $\varepsilon_n \hookrightarrow K^*$, *являлся нулевым.*

**В главе 3** исследуются вложения конечных абелевых $p$-групп в группу Дженнингса $\mathcal{J}(\mathbb{F}_p)$. Пусть $k$ – коммутативное кольцо с единицей. Рассмотрим множество $\mathcal{J}(k)$ формальных степенных рядов относительно переменной $x$ с коэффициентами в кольце $k$, причем коэффициент при $x$ ряда $f(x) \in \mathcal{J}(k)$ равен единице. Более формально,

$$\mathcal{J}(k) = \{f(x) \in k[[x]] \mid f(x) = x + \sum_{n=2}^{\infty} a_n x^n\}. \tag{3.1}$$

На множестве $\mathcal{J}(k)$ можно ввести бинарную операцию: по определению $(f * g)(x) = f(g(x))$; такое определение корректно, так как ряд $g(x) \in \mathcal{J}(k)$ не содержит свободного члена.

В разделе 3.2 дается ответ на вопрос И. К. Бабенко[68] о построении явных вложений конечных абелевых $p$-групп в группу $\mathcal{J}(\mathbb{F}_p)$. Такое вложение строится в теореме 3.1, причем термин “явный” понимается в смысле замечания 3.1: сколь угодно далекие частичные суммы рядов, отвечающих порождающим элементам заданной конечной абелевой $p$-группы, вычисляются за конечное число шагов.

Рассмотрим многочлен $f(x) = x^p + tx$ как элемент кольца $\mathbb{F}_p[t][x]$. Нетрудно заметить, что множества $W_{f,n}$ корней $n$-й итерации многочлена $f(x)$ в фиксированном алгебраическом замыкании $\overline{\mathbb{F}_p((t))}$ поля $\mathbb{F}_p((t))$ вложены друг в друга: $W_{f,n} \subset W_{f,n+1}$ для любого натурального $n$. Если положить $k_n := \mathbb{F}_p((t))(W_{f,n})$ для $n \in \mathbb{N}$, а $k_0 := \mathbb{F}_p((t))$, то расширение $k_n/k_0$ является вполне разветвленным расширением Галуа степени $(p-1)p^{n-1}$ с абелевой группой Галуа, изоморфной группе обратимых элементов кольца $\mathbb{F}_p[[t]]/(t^n)$. При этом если $t_n$ – корень многочлена $f^{(n)}(x)$, являющийся униформизирующей поля $k_n$, то элемент $t_{n-1} = f(t_n)$ – униформизирующая поля $k_{n-1}$ при $n > 1$. Также $t = -(f^{n-1}(t_n))^{p-1}$. Положим

$$W_{f,\infty} := \bigcup_{n=1}^{\infty} W_{f,n}; \qquad k_\infty := k_0(W_{f,\infty}).$$

Для каждого $a \in \mathbb{F}_p[[t]]^*$ существует и притом единственный формальный ряд

[68] И. К. Бабенко, Алгебра, геометрия и топология группы подстановок формальных степенных рядов, *УМН*, **68:1**, (2013), 3–76, Замечание 4.11.

$[a]_f(x) \in \mathbb{F}_p[[t]][[x]]$, обладающий свойствами

$$[a]_f(x) \equiv ax (\mathrm{mod}\, \mathrm{deg} \geqslant 2),$$
$$f([a]_f(x)) = [a]_f(f(x)).$$

Для $u \in \mathbb{F}_p[[t]]^*$ символ Артина $\theta(u) = (u,\, k_\infty/k_0)$ задается явно:

$$y^{\theta(u)} := [u^{-1}]_f(y),\ \forall\, y \in W_{f,\infty}.$$

**Лемма** (3.1). *Пусть* $h(t) \in \mathbb{F}_p[[t]]^*$, $f(x) = x^p + tx$. *Тогда* $[h(t)]_f(x) = h(t)x + \sum_{n=1}^{\infty} a_{p^n}(t)x^{p^n}$, *где*

$$a_{p^{n+1}}(t) := \frac{a_{p^n}(t)^p - a_{p^n}(t)}{t^{p^n} - t},\ n \in \mathbb{N}; \qquad a_p(t) := \frac{h(t)^p - h(t)}{t^p - t}.$$

Пусть по-прежнему $k_0 = \mathbb{F}_p((t))$, $k_n = k_0(W_{f,n})$, а $t_i$ – такой простой элемент поля $k_i$, что $t_i = f(t_{i+1})$ для $i \in [1,\, n-1] \cap \mathbb{N}$. Тогда $t = -t_1^{p-1} = -(f^{(n-1)}(t_n))^{p-1}$.

**Лемма** (3.2). *Элемент* $t$ *явно выражается в виде степенного ряда относительно переменной* $t_n$ *в смысле замечания 3.1.*

Фиксируем локальное поле $k_0 = \mathbb{F}_p((t))$ и рассмотрим расширение Любина-Тейта $k_n/k$, где $k_n = k_0(W_{f,n})$ с группой Галуа, изоморфной $(\mathbb{F}_p[[t]]/(t^n))^*$, а $n = p^m$ для некоторого достаточно большого натурального $m \equiv 0 (\mathrm{mod}\, 2)$ (позднее мы конкретизируем выбор $m$). Рассмотрим следующий набор элементов группы $(\mathbb{F}_p[[t]]/(t^n))^*$:

$$g_1 = 1 + t_p + t^{p+1},\ g_2 = 1 + t^{p^2} + t^{p^2+1}, \ldots,\ g_{\frac{m}{2}} = 1 + t^{p^{\frac{m}{2}}} + t^{p^{\frac{m}{2}}+1}. \qquad (3.5)$$

Элементы $g_1, \ldots, g_{m/2}$ в (3.5) записаны, разумеется, по модулю соотношения $t^n = 0$.

**Лемма** (3.3). *Элементы* $g_1, \ldots, g_{m/2}$ *порождают с точностью до изоморфизма группу* $Z_{p^{m-1}} \times Z_{p^{m-2}} \times \ldots \times Z_{p^{m-m/2}}$.

Пусть дана произвольная конечная абелева $p$-группа $A \cong Z_{p^{r_1}} \times \ldots \times Z_{p^{r_s}}$, где $1 \leqslant r_1 \leqslant \ldots \leqslant r_s$. Тогда группа $A$ допускает вложение в группу $(\mathbb{F}_p[[t]]/(t^n))^*$ при $n = p^m$ и $m \geqslant \max\{2s,\, 2r_s\}$, $m \equiv 0 (\mathrm{mod}\, 2)$. В самом деле, согласно лемме 3.3 элементы $g_1, \ldots, g_{m/2}$ из (3.5) порождают в $(\mathbb{F}_p[[t]]/(t^n))^*$ подгруппу, изоморфную $Z_{p^{m-1}} \times Z_{p^{m-2}} \times \ldots \times Z_{p^{m-m/2}}$. Группа $A$ вкладывается в группу $\langle g_1, \ldots, g_{m/2} \rangle$ и, тем самым, в группу $(\mathbb{F}_p[[t]]/(t^n))^*$, причем если $a_1, \ldots, a_s$ – образующие группы $A$, то можно считать $a_i = g_i^{p^{m-i-r_i}}$ для всех $i$.

Расширение $\mathbb{F}_p((t))(W_{f,n})/\mathbb{F}_p((t))$ имеет группу Галуа $(\mathbb{F}_p[[t]]/(t^n))^*$. Такое расширение вполне разветвлено, поэтому если $t_n$ – униформизирующая поля

$\mathbb{F}_p((t))(W_{f,n})$, то $\mathbb{F}_p((t))(W_{f,n}) = \mathbb{F}_p((t_n))$. Заметим, что элементы $g_1, \ldots, g_{m/2}$ из (3.5) действуют на униформизирующую $t_n$ следующим образом: $t_n^{g_i} := [g_i]_f(t_n)$. Леммы 3.1 и 3.2 дают таким образом искомое конструктивное описание группы $A$ как подгруппы в $\mathcal{J}(\mathbb{F}_p)$.

**Теорема** (3.1). *Любая конечная абелева $p$-группа вкладывается в $\mathcal{J}(\mathbb{F}_p)$, причем искомое вложение допускает явное описание.*

Для элемента порядка 4 явное вложение в $\mathcal{J}(\mathbb{F}_2)$ может быть выписано в виде формулы, что и сделано в 3.2.2. Именно, пусть $g(x) \in \mathcal{J}(\mathbb{F}_2)$ определено следующим образом:

$$g(x) = (1+y)x + x^2, \tag{3.8}$$

а $y$ определяется формулой

$$y = \sum_{k=4}^{\infty} a_k x^k,$$

$$\begin{cases} a_5 = 0,\ a_4 = 1, & \\ a_k = a_{k-2}, & k \in \{6,\ 7,\ 8\}, \\ a_k = a_{k-2} + a_{(k-2)/2}, & k \geqslant 10,\ k \equiv 0 (\mathrm{mod}\, 2), \\ a_k = a_{k-2} + a_{(k-1)/2}, & k \geqslant 9,\ k \not\equiv 0 (\mathrm{mod}\, 2). \end{cases} \tag{3.9}$$

Степенной ряд $g(x)$, определяемый формулами (3.8) и (3.9), задает в $\mathcal{J}(\mathbb{F}_2)$ элемент порядка 4, что вытекает из лемм 3.1 и 3.2.

Наконец, в разделе 3.3 мы возвращаемся к задаче вложения, определенной в разделе 1.7. Именно, пусть $y_0 \in \mathcal{J}(\mathbb{F}_p)$ – заданный элемент порядка $p$. Фиксируем $m \in \mathbb{N}$. При каких необходимых и достаточных условиях в группе $\mathcal{J}(\mathbb{F}_p)$ разрешимо уравнение $x^{p^m} = y_0$? Указанная задача может быть сформулирована в терминах задачи вложения (1.117) с $K = \mathbb{F}_p((t))$, $X = Z_p$, $Y = Z_{p^{m+1}}$. Всюду далее $U_j = 1 + t^j \mathbb{F}_p[[t]]$ для $j \in \mathbb{N}$.

Пусть $G$ – циклическая $p$-группа порядка $p^m$ с образующей $\gamma$. Как было отмечено, вложение $G \hookrightarrow \mathcal{J}(\mathbb{F}_p)$ определяет эпиморфизм $\varkappa$ и обратно. Обозначим через $G_j$ подгруппу в $G$, порожденную элементом $\gamma^{p^j}$. Для каждого $j \in [0,\ m-1] \cap \mathbb{Z}$ определено число $r_j \in \mathbb{N}$ со свойством: $\varkappa(U_{r_j}) = G_j$, а $\varkappa(U_{r_j+1}) = G_{j+1}$. Иными словами, эпиморфизм $\varkappa$ определяет последовательность $\{r_j\}_{j=0}^{m-1}$, которую мы будем называть *ветвлением* эпиморфизма $\varkappa$.

**Лемма** (3.4). *Последовательность $\{r_j\}_{j=0}^{m-1} \subset \mathbb{N}$ тогда и только тогда является ветвлением, когда $(r_0,\ p) = 1$, $r_j \geqslant p r_{j-1}$ для всех $j$, причем если $r_j > p r_{j-1}$, то дополнительно $p \nmid r_j$.*

Для каждого элемента $g \in \mathcal{J}(\mathbb{F}_p)$ порядка $p^m$ можно определить *последовательность глубин* $\{d_j\}_{j=0}^{m-1} \subset \mathbb{N}$ следующим образом: $d_j = \nu_t(t^{g^{p^j}} - t) - 1$.

Рассмотрим для последовательности глубин $\{d_j\}_{j=0}^{m-1}$ функцию $\varphi\colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}$, определенную следующим образом:

$$\varphi(u) = \begin{cases} \frac{1}{p^t}(u - d_{t-1}) + \sum\limits_{j=1}^{t-1} \frac{1}{p^j}(d_j - d_{j-1}) + d_0, & d_{t-1} \leqslant u \leqslant d_t; \\ u, & 0 \leqslant u \leqslant d_0; \\ \frac{1}{p^m}(u - d_{m-1}) + \sum\limits_{j=1}^{m-1} \frac{1}{p^j}(d_j - d_{j-1}) + d_0, & d_{m-1} \leqslant u, \end{cases} \tag{3.10}$$

где, конечно, $t \leqslant m - 1$.

**Лемма** (3.5). *Последовательность $\{d_j\}_{j=0}^{m-1} \subset \mathbb{N}$ тогда и только тогда является последовательностью глубин некоторого элемента $g \in \mathcal{J}(\mathbb{F}_p)$ порядка $p^m$, когда*

$$d_{j-1} = d_{j-2} + p^{j-1}(p-1)\varphi(d_{j-2}) + p^{j-1}u_{j-2} \quad \forall\, j \in [2,\, m] \cap \mathbb{N}, \tag{3.11}$$

*причем $(d_0,\, p) = 1$; для каждого $j \in [2,\, m] \cap \mathbb{N}$ число $u_{j-2} \in \mathbb{Z}_{\geqslant 0}$ а также если $u_{j-2} > 0$ для какого-то $j \in [2,\, m] \cap \mathbb{N}$, то $(u_{j-2},\, p) = 1$.*

**Теорема** (3.2). *Пусть $y_0 \in \mathcal{J}(\mathbb{F}_p)$ – фиксированный элемент порядка $p$. Фиксируем $m \in \mathbb{N}$, тогда в группе $\mathcal{J}(\mathbb{F}_p)$ уравнение $x^{p^m} = y_0$ разрешимо тогда и только тогда когда существует последовательность глубин $\{d_j\}_{j=0}^{m}$, у которого $d_m$ – глубина элемента $y_0$.*

Лемма 3.5 и теорема 3.2 решают в простых арифметических терминах задачу вложения (1.117) с $K = \mathbb{F}_p((t))$, $X = Z_p$, $Y = Z_{p^{m+1}}$.

**В главе 4** исследуется проблема Зеликина-Локуциевского[69]. Определим $[n/2]$-элементное множество $B$ следующими формулами.

Пусть $n$ четно. Тогда положим $B = \{v_k\}_{k=1}^{[n/2]} \subset \mathbb{R}_{>0}$, где $v_k$ – единственный действительный корень уравнения

$$\sum_{s=1}^{2n} \operatorname{arctg} \frac{x}{s} = (2k-1)\pi. \tag{4.2}$$

Пусть $n$ нечетно. Тогда положим $B = \{v_k\}_{k=1}^{[n/2]} \subset \mathbb{R}_{>0}$, где $v_k$ – единственный действительный корень уравнения

$$\sum_{s=1}^{2n} \operatorname{arctg} \frac{x}{s} = 2k\pi. \tag{4.3}$$

[69] М. И. Зеликин, Л. В. Локуциевский, Р. Хильдебранд, Геометрия окрестностей особых экстремалей в задачах с многомерным управлением, *Тр. МИАН*, **277**, (2012), 74–90, Гипотеза 1.

**Проблема** (4.1). *Верно ли, что все элементы множества $B$ линейно независимы над $\mathbb{Q}$?*

В 4.1.1 поясняется важность данного вопроса для теории оптимального синтеза в многомерной обобщенной задаче Фуллера (4.1). Именно, рассмотрим оптимизационную задачу

$$J(x) = \int_0^{+\infty} \langle x, Cx \rangle \, dt \to \min \tag{4.1}$$

на траекториях управляемой системы

$$\begin{aligned} &x^{(n)} = u, \quad |u| \leq 1, \quad x(t) \in V, \quad u(t) \in U = V \quad \forall\, t \in [0, +\infty); \\ &x^{(k)}(0) = x_k^0, \; 0 \leqslant k \leq n-1. \end{aligned}$$

Здесь $V$ – конечномерное евклидово пространство достаточно высокой размерности со скалярным произведением $\langle \cdot, \cdot \rangle$, а $C$ – некоторый самосопряженный линейный оператор. Функция $x(t)$ считается абсолютно непрерывной вместе со своими $2n-1$ производными. Управление $u(t) \in L_1(0; +\infty)$ – измеримая функция. Было установлено[70], что в задаче (4.1) существует оптимальное управление, проходящее за конечное время всюду плотную обмотку $k$-мерного тора при $k \leqslant [n/2]$, если некоторые $k$ элементов множества $B$ линейно независимы над полем $\mathbb{Q}$, а оператор $C$ выбран подходящим образом[71]. Определим многочлен $f_n(x) \in \mathbb{Z}[x]$ степени $n-1$ формулой

$$x f_n(x^2) = \operatorname{Im} \prod_{j=1}^{2n} (ix + j). \tag{4.4}$$

В разделе 4.2 приводятся редукции проблемы 4.1 к вопросам теории Галуа. Именно, в 4.2.1 устанавливается лемма 4.1 и следствие 4.1, которые сводят проблему 4.1 к вопросу о вложимости знакопеременной группы степени $n-1$ в группу Галуа над $\mathbb{Q}$ многочлена $f_n(x)$ степени $n-1$, определенного в (4.4) и (4.5).

**Лемма** (4.1). *Пусть $a(x) \in k[x]$ – сепарабельный многочлен степени $n-1$, где $n \in \mathbb{Z}_{\geqslant 5}$. Пусть далее $A_{n-1} \hookrightarrow \operatorname{Gal}_k(a)$. В этом случае любые $\left[\frac{n}{2}\right]$ корня многочлена $A(x) := a(x^2)$, квадраты которых попарно различны, линейно независимы над $k$.*

**Следствие** (4.1). *Пусть $n \in \mathbb{Z}_{\geqslant 5}$ таково, что $A_{n-1} \hookrightarrow \operatorname{Gal}_{\mathbb{Q}}(f_n)$. Тогда все элементы множества $B$, определенного в (4.2) и (4.3), линейно независимы над $\mathbb{Q}$. В частности, для таких $n$ проблема 4.1 решается положительно.*

[70] М. И. Зеликин, Д. Д. Киселев, Л. В. Локуциевский, Оптимальное управление и теория Галуа, *Матем. сб.*, **204:11**, (2013), 83–98.

[71] Там же, Теорема 3.

Результаты пункта 4.2.2 направлены на получение информации о группе Галуа $\mathrm{Gal}_{\mathbb{Q}}(f_n)$: в теореме 4.1 устанавливается при некоторых ограничениях неприводимость многочлена $f_n(x)$ над $\mathbb{Q}$.

**Теорема** (4.1). *Пусть $n > 1$ – такое натуральное число, что число $q = 2n + 1$ является простым с условием $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$, тогда многочлен $f_n(x)$ неприводим над $\mathbb{Q}$.*

В теореме 4.2 при условии неприводимости многочлена $f_{p+1}(x)$ для некоторых простых $p$ специального вида устанавливается 2-транзитивность группы $\mathrm{Gal}_{\mathbb{Q}}(f_{p+1})$.

**Теорема** (4.2). *Пусть $q \equiv 2 (\mathrm{mod}\, 3)$ – такое нечетное простое число, что многочлен $f_4(x)$ неприводим над $\mathbb{Q}$, а $p = 3 + q + 3qk$ – простое число для некоторого натурального $k$. Если многочлен $f_{p+1}(x)$ неприводим над $\mathbb{Q}$, то группа $\mathrm{Gal}_{\mathbb{Q}}(f_{p+1})$ как группа перестановок корней является неразрешимой дважды транзитивной группой.*

В теореме 4.3 строится бесконечная последовательность натуральных $n$, для которых группа $\mathrm{Gal}_{\mathbb{Q}}(f_n)$ содержит транспозицию.

**Теорема** (4.3). *Пусть $n > 4$ – такое натуральное число, что число $r = 2n + 7$ является простым, причем выполнено дополнительное условие на квадратичный символ Лежандра*

$$\left(\frac{889}{r}\right) = -1, \tag{4.28}$$

*тогда группа $\mathrm{Gal}_{\mathbb{Q}}(f_n)$ как группа подстановок корней многочлена $f_n(x)$ содержит транспозицию. Более того, таких простых чисел $r$ существует бесконечно много.*

Объединяя теорему 4.1 и теорему 4.2, получаем набор условий на $n$, при выполнении которых проблема 4.1 решается положительно.

**Теорема** (4.4). *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 $k$. Если число $2p+3$ является простым с условием $B_{2p} \not\equiv 0 (\mathrm{mod}\, 2p+3)$, то $A_p \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_{p+1})$, кроме, быть может, случая когда $p = (r^{st} - 1)/(r^s - 1)$ для некоторого простого $r$ и некоторых натуральных $r$, $s$.*

Наконец, в разделе 4.3 результаты раздела 4.2 применяются для получения количественных результатов по проблеме 4.1. В 4.3.1 в теоремах 4.6 и 4.7 для

любого $n > 3$ показывается, что по крайней мере два элемента множества $B$ линейно независимы над $\mathbb{Q}$.

В 4.3.2 из теоремы 4.4 извлекается ряд следствий, посвященных существованию в задаче (4.1) решения, управление которого за конечное время проходит всюду плотную обмотку тора более высокой размерности, чем 2.

**Следствие** (4.5). *Пусть $q \equiv 2 (\mathrm{mod}\, 3)$ – такое нечетное простое число, что многочлен $f_4(x)$ неприводим над $\mathbb{F}_q$, а число $p = 3 + q + 3qk$ также простое для некоторого натурального $k$. Если число $2p+3$ является простым с условием $B_{2p} \not\equiv 0 (\mathrm{mod}\, 2p+3)$, и если $p$ не представимо в виде $(r^{st}-1)/(r^s-1)$ ни для какого простого $r$ и натуральных $s$, $t$, то все элементы множества $B$, определенного условиями (4.2) и (4.3), линейно независимы над $\mathbb{Q}$. В частности, для таких $n = p + 1$ проблема 4.1 решается положительно.*

**Теорема** (4.8). *Пусть $n > 4$ – такое натуральное число, что числа $p = n-1$, $q = 2n + 1$, $r = 2n + 7$ являются простыми, причем для $r$ выполнено условие (4.28), а для $q$ – условие $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$. Тогда имеет место изоморфизм $\mathrm{Gal}_{\mathbb{Q}}(f_n) \cong S_p$.*

Теорема 4.4 иллюстрируется следующими примерами: при

$$n \in \{1614,\, 34\,503\,270,\, 499\,989\,828,\, 499\,997\,838\}$$

справедливы вложения $A_{n-1} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_n)$, в частности, проблема 4.1 решается положительно для таких $n$. Отметим, что число $n = 499\,997\,838$ является максимальным известным на данный момент числом, для которого получено положительное решение проблемы 4.1.

Также рассматривается пример на применение теоремы 4.8: перечислены все натуральные $n \leqslant 600$, удовлетворяющие условиям теоремы 4.8, для которых, как следствие, проблема 4.1 решается положительно. Все такие натуральные $n$ имеют следующий вид:

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

## Заключение

Все результаты диссертации являются новыми и состоят в следующем:

1. решена проблема А. В. Яковлева, посвященная характеризации ультраразрешимых групповых расширений, для групповых расширений нечетного порядка с циклическим ядром (полностью) а также в достаточно широких классах групповых расширений четного порядка с циклическим ядром;

2. выяснено, что локально-глобальный принцип А. В. Яковлева не является необходимым для ультраразрешимости $p$-расширений;

3. построены неполупрямые $p$-расширения с абелевым нециклическим ядром, для которых проблема А. В. Яковлева решается отрицательно;

4. получены наилучшие равномерные оценки индекса Шура неприводимых комплексных характеров конечных групп порядка $n$ (класс $G_{\mathrm{ord}}(n)$), конечных групп заданной экспоненты $n$ (класс $G_{\exp}(n)$) над полем $\mathbb{Q}$;

5. построены явные вложения конечных абелевых $p$-групп в группу Дженнингса $\mathcal{J}(\mathbb{F}_p)$, дающие ответ на вопрос И. К. Бабенко;

6. найден критерий разрешимости уравнения $x^{p^m} = y_0$ в группе $\mathcal{J}(\mathbb{F}_p)$ при заданных натуральном $m$ и элементе $y_0 \in \mathcal{J}(\mathbb{F}_p)$ порядка $p$;

7. проблема Зеликина-Локуциевского сведена к вопросу о неприводимости над $\mathbb{Q}$ многочлена $f_{p+1}(x)$ для почти всех простых $p$, решена проблема Зеликина-Локуциевского для ряда[72] натуральных $n$ и, как следствие, в обобщенной задаче Фуллера построены решения с управлением, проходящим за конечное время всюду плотную обмотку $k$-мерного тора для любого натурального $k \leqslant 249\,998\,919$ (отметим, что такая оценка на текущий момент принципиально неулучшаема);

8. доказано существование для любого $n > 3$ не менее двух элементов "критического" множества корней многочлена Зеликина-Локуциевского, линейно независимых над $\mathbb{Q}$ и, как следствие, в обобщенной задаче Фуллера для любого $n > 3$ построены решения с управлением, проходящим за конечное время всюду плотную обмотку 2-мерного тора;

9. доказана неприводимость многочленов Зеликина-Локуциевского степени $(q-3)/2$ над $\mathbb{Q}$ для всех простых $q > 3$ с дополнительным условием на число Бернулли: $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$; вычислена группа Галуа многочлена $f_n(x)$ над $\mathbb{Q}$ при условии, что для $n > 4$ числа $p = n-1$, $q = 2n+1$, $r = 2n+7$ являются простыми, 889 не квадрат по модулю $r$, а $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$;

10. доказано вложение $A_{n-1} \hookrightarrow \mathrm{Gal}_{\mathbb{Q}}(f_n)$ при условии, что числа $p = n-1$, $q = 2n+1$ являются простыми, причем $B_{q-3} \not\equiv 0 (\mathrm{mod}\, q)$, а $p$ принадлежит арифметической прогрессии $\{26 + 69k \mid k \in \mathbb{N}\}$ и не представимо в виде дроби $(r^{st}-1)/(r^s-1)$ ни для какого простого $r$ и натуральных $s$, $t$.

[72] Предположительно бесконечного.

## Благодарности

Диссертант благодарит д.ф.-м.н. проф. В. А. Артамонова, д.ф.-м.н. проф. А. В. Яковлева, д.ф.-м.н. доц. Б. Б. Лурье, д.ф.-м.н. проф. чл.-корр. РАН М. И. Зеликина, д.ф.-м.н. Л. В. Локуциевского, к.ф.-м.н. доц. И. А. Чубарова за неоднократную помощь и поддержку в процессе написания диссертации.

## Работы автора по теме диссертации

[1] М. И. Зеликин, Д. Д. Киселев, Л. В. Локуциевский, "Оптимальное управление и теория Галуа", *Матем. сборник*, **204**:11 (2013), 83–98; *Sbornik Math.*, **204**:11 (2013), 1624–1638.
В работе [1] Д. Д. Киселеву принадлежит доказательство гипотезы 1 для всех $4 < q < 17$ а также теоремы 4 и 5.

[2] Д. Д. Киселев, И. А. Чубаров, "Об ультраразрешимости некоторых классов минимальных неполупрямых $p$-расширений с циклическим ядром для $p > 2$", *Записки научн. сем. ПОМИ*, **452** (2016), 132–157; *Journal of Math. Sciences (N. Y.)*, **232**:5 (2018), 677–692.
В работе [2] Д. Д. Киселеву принадлежит основная теорема 1.

[3] Д. Д. Киселев, А. В. Яковлев, "Ультраразрешимые и силовские расширения с циклическим ядром", *Алгебра и анализ*, **30**:1 (2018), 128–138.
В работе [3] Д. Д. Киселеву принадлежат теорема 1 и основной результат работы – теорема 2.

[4] Д. Д. Киселев, "Оптимальные оценки индекса Шура и реализуемость представлений", *Матем. сборник*, **205**:4 (2014), 69–78; *Sbornik Math.*, **205**:4 (2014), 522–531.

[5] Д. Д. Киселев, "Явные вложения конечных абелевых $p$-групп в группу $\mathcal{J}(\mathbb{F}_p)$", *Матем. заметки*, **97**:1 (2015), 74–79; *Math. Notes*, **97**:1 (2015), 63–68.

[6] Д. Д. Киселев, "Ультраразрешимые накрытия группы $Z_2$ группами $Z_8$, $Z_{16}$ и $Q_8$", *Зап. научн. сем. ПОМИ*, **435** (2015), 47–72; *Journal of Math. Sciences (N. Y.)*, **219**:4 (2016), 523–538.

[7] Д. Д. Киселев, "О всюду плотной обмотке 2-мерного тора", *Матем. сборник*, **207**:4 (2016), 113–122; *Sbornik Math.*, **207**:4 (2016), 581–589.

[8] Д. Д. Киселев, "Об ультраразрешимости групповых $p$-расширений абелевой группы с помощью циклического ядра", *Зап. научн. сем. ПОМИ*, **452** (2016), 108–131; *Journal of Math. Sciences (N. Y.)*, **232**:5 (2018), 662–676.

[9] Д. Д. Киселев, "Об ультраразрешимых задачах погружения с циклическим ядром", *Успехи мат. наук*, **71**:6 (2016), 165–166; *Russian Math. Surveys*, **71**:6 (2016), 1149–1151.

[10] Д. Д. Киселев, "Метациклические 2-расширения с циклическим ядром и вопросы ультраразрешимости", *Зап. научн. сем. ПОМИ*, **460** (2017), 114–133.

[11] Д. Д. Киселев, "Теория Галуа, классификация конечных простых групп и всюду плотная обмотка тора", *Матем. сборник*, **209**:6 (2018), 65–74; *Sbornik Math.*, **209**:6 (2018), 840–849.

[12] Д. Д. Киселев, "Ультраразрешимые накрытия некоторых нильпотентных групп циклической группой над числовыми полями и смежные вопросы", *Изв. РАН. Сер. матем.*, **82**:3 (2018), 69–89; *Izv. Math.*, **82**:3 (2018), 512–531.

[13] Д. Д. Киселев, "Оптимальное управление, всюду плотная обмотка тора и простые числа Вольстенхольма", *Вестник МГУ. Сер. 1. Матем. Мех.*, **73**:4 (2018), 60–62; *Moscow Univ. Math. Bull.*, **73**:4 (2018), 162–163.

[14] D. D. Kiselev, "Applications of Galois Theory to Optimal Control", *CEUR Workshop Proceedings*, **1897** (2017), 50–56; Scopus: 85029102049.

[15] D. D. Kiselev, "Minimal $p$-extensions and the embedding problem", *Comm. Algebra*, **46**:1 (2018), 290–321.

[16] S. I. Bogataya, S. A. Bogatyi, D. D. Kiselev, "Powers of elements of the series substitution group $\mathcal{J}(\mathbb{Z}_2)$", *Topology and its applications*, **201** (2016), 29–56.
В работе [16] Д. Д. Киселеву принадлежит параграф §6 ([16, 6. Elements of finite order]), содержащий ответ на вопрос И. К. Бабенко о построении явных элементов конечного $p$-примарного порядка в группе $\mathcal{J}(\mathbb{F}_p)$.