Math-Net.Ru
Общероссийский математический портал

В. В. Ишханов, Б. Б. Лурье, Задача погружения для числовых полей с некоммутативным ядром порядка p^4, *Алгебра и анализ*, 1990, том 2, выпуск 6, 161–167

https://www.mathnet.ru/aa227

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

Параметры загрузки:
IP: 18.97.9.175
24 мая 2025 г., 20:03:00

© 1990 г.

В.В.Ишханов, Б.Б.Лурье

ЗАДАЧА ПОГРУЖЕНИЯ ДЛЯ ЧИСЛОВЫХ ПОЛЕЙ С НЕКОММУТАТИВНЫМ ЯДРОМ ПОРЯДКА p^4

Рассматриваются условия погружаемости конечного p-расширения числового поля в p-расширение, относительная группа Галуа которого имеет порядок p^4.

1°. В публикуемых в настоящем томе воспоминаниях И.Р.Шафаревича о Дмитрии Константиновиче Фаддееве рассказывается об истории задачи погружения полей и приводится ее формулировка. Мы будем обозначать посредством $(K/k, G, \varphi, B)$ задачу погружения, связанную с точной последовательностью конечных групп

$$1 \longrightarrow B \longrightarrow G \xrightarrow{\varphi} \mathrm{Gal}\ (K/k) \longrightarrow 1.$$

Некоторые аргументы в этом обозначении могут опускаться, если их восстановление очевидно.

Когда ядро B задачи погружения коммутативно, теория имеет законченный характер [1-4]. В [5] исследована задача погружения с некоммутативным ядром порядка p^3. Условия погружения оказались единообразными для всех таких групп (для каждого p имеются две неизоморфные группы порядка p^3).

В последние годы авторы предприняли систематическое исследование задачи погружения с некоммутативным ядром порядка p^4. (Заметим, что существуют десять попарно неизоморфных групп порядка p^4 для любого нечетного p (причем случаи p=3 и p>3 различны), и девять для p=2 (см. [6])). Полностью эта работа еще не завершена, и данная статья представляет собой обзор результатов, полученных к настоящему времени. Две статьи [7,8] с одинаковым названием содержат подробное рассмотрение задачи погружения с двумя различными (неизоморфными) ядрами порядка p^4.

Как и прежде, мы предполагаем дополнительно, что поля k и K, фигурирующие в задаче погружения, - числовые (т.е. локальные поля или поля алгебраических чисел), а группа G (соответственно и $F=\mathrm{Gal}(K/k)$) является p-группой. Кроме того, можно считать, что в поле k содержится первообразный корень ζ_0 степени p из 1 - в противном случае ситуация согласно [9] оказывается проще.

2°. Необходимое условие погружаемости, найденное Д.К.Фаддеевым (и переоткрытое Х.Хассе), носит название условия согласности. Одна из формулировок этого условия следующая (см. также упоминаемую выше статью И.Р.Шафаревича). Пусть $G \times K$ - скрещенное произведение группы G и поля K, т.е. свободный K-модуль с базисом

Ключевые слова: локальное поле, задача погружения, группа Галуа, поле алгебраических чисел, p-расширение, сопутствующая задача, условие согласности, скрещенное произведение.

$\{u_g\}$, $g\in G$, и с умножением, задаваемым формулами $u_{g_1}u_{g_2}=u_{g_1g_2}$, $xu_g=u_gx^{\varphi(g)}$ для $x\in K$. Условие согласности состоит в том, что алгебра $G\times K$ изоморфна матричной алгебре порядка, равного порядку группы $F=\mathrm{Gal}(K/k)$, над своей подалгеброй (в случае абелева ядра B - над своим центром). Для числовых полей это условие редуцируется к условию согласности для абелевой задачи $(K/k,\ G/B',\ \varphi',\ B/B')$, где B' - коммутант группы B, а φ' - естественное отображение $G/B'\longrightarrow G/B$ (см. [10]).

Другие необходимые условия погружаемости представляют собой требования разрешимости так называемых сопутствующих задач. Укажем некоторые способы получения таких задач.

1. Пусть существуют гомоморфизм $\psi:G\longrightarrow G_1$ и эпиморфизм $\varphi_1:G_1\longrightarrow F$, где G_1 - конечная группа, такие, что $\varphi_1\psi=\varphi$. Тогда задача $(K/k,G_1,\varphi_1,B_1)$, где B_1 - ядро φ_1, является сопутствующей для задачи $(K/k,G,\varphi,B)$. Это достаточно ясно, когда ψ - эпиморфизм, поскольку в качестве решения сопутствующей задачи можно взять подполе (подалгебру) элементов из решения L основной задачи, инвариантных относительно ядра отображения $B\longrightarrow B_1$. В общем же случае можно решить задачу $(K/k,G_1,\varphi_1,B_1)$, взяв прямую сумму нескольких таких решений и определенным образом задав на ней автоморфизмы из G_1 (см. [1]).

2. Пусть k_1 - подполе поля K, содержащее поле k, F_1 - группа Галуа расширения K/k_1, т.е. F_1 реализуется как подгруппа группы F. Тогда задача $(K/k_1,G,B)$, где G_1 - прообраз F_1 в G, сопутствует задаче $(K/k,G,B)$, поскольку всякое решение исходной задачи решает и сопутствующую.

3. Пусть K/k - расширение полей алгебраических чисел, $\mathfrak{p}$ - простой дивизор поля k (конечный или бесконечный). Обозначим через $k_\mathfrak{p}$ пополнение поля k в точке $\mathfrak{p}$, и через $K_\mathfrak{p}$ - тензорное произведение $K\otimes k_\mathfrak{p}$. Задача $(K_\mathfrak{p}/k_\mathfrak{p},G,\varphi,B)$ сопутствует исходной. $K_\mathfrak{p}$ не обязано, вообще говоря, быть полем, но всегда является алгеброй Галуа над $k_\mathfrak{p}$ с группой F, и задача в такой постановке осмысленна (см. [3]).

4. **Операция подъема.** Пусть поле K_1 содержит K и нормально над k с группой F_1 (тем самым задан эпиморфизм $\psi:F_1\longrightarrow F$). Обозначим через G_1 произведение групп G и F_1 с отождествленной факторгруппой F; тогда определен эпиморфизм $\varphi_1:G_1\longrightarrow F_1$ с ядром, изоморфным $B=\mathrm{Ker}\ \varphi$. В этой ситуации задачи погружения $(K/k,G,\varphi,B)$ и $(K_1/k,G_1,\varphi_1,B)$ являются эквивалентными, т.е. они разрешимы одновременно, и их решения находятся в биективном соответствии.

Операция подъема позволяет совершить некоторые редукции нашей задачи. Во-первых, мы можем считать, что поле K содержит первообразный корень ζ из 1 степени, равной периоду ядра B. Действительно, если $\zeta\notin K$, возьмем поле $K_1=K(\zeta)$; оно нормально над k, поскольку является композитом K и кругового расширения $k(\zeta)$. Так как согласно допущению, сделанному ранее, корень степени p из 1 содержится в k, группа Галуа $F_1=\mathrm{Gal}(K_1/k)$ является p-группой, и мы можем перейти к эквивалентной задаче погружения $(K_1/k,G_1,\varphi_1,B)$.

Предположим далее, что разрешима сопутствующая задача погружения

$(K/k, G/B_1, B/B_1)$, где B_1 - нормальная в G подгруппа группы B (например, коммутант B), и пусть L - решение этой задачи. Взяв в качестве K_1 само L, если это поле, или его поле-ядро L_0, мы получим посредством подъема эквивалентную задачу погружения $(K_1/k, G, \varphi_1, B)$, где G_1 - произведение групп G и $\mathrm{Gal}(K_1/k)$ с отождествленной фактор-группой F. При этом расширение $1 \to B/B_1 \to G_1/B_1 \to F_1 \to 1$ является уже полупрямым, т.е. систему факторов расширения G_1 посредством $F_1 = \mathrm{Gal}(K_1/k)$ можно выбрать уже в B_1. Иначе говоря, в G_1 существует подгруппа H_1, отображающаяся на F_1 с ядром B_1. Если B_1 содержится в центре группы B, то задание H_1 превращает B в F_1-группу и тем самым определяет гомоморфизм $\theta: F_1 \to \mathrm{Aut}B$, точнее, в силовскую p-подгруппу $\mathrm{Aut}_p B$ группы всех автоморфизмов группы B.

3°. Естественный ход исследования задачи погружения $(K/k, G, \varphi, B)$ следующий. Выберем в B подгруппу A, нормальную в G, так, чтобы сопутствующая задача $(K/k, G/A, B/A)$ была разрешима, и все ее решения имели простое описание. Теперь задача сводится к вопросу о существовании таких решений L этой сопутствующей задачи, для которых разрешима задача погружения $(L/k, G, A)$. Заметим, что эта последняя задача осмысленна, даже когда L не поле, а алгебра Галуа. При этом группу A желательно выбрать так, чтобы условие разрешимости для задачи $(L/k, G, A)$ совпадало с условием согласности, достаточно просто проверяемым. В частности, условие согласности влечет погружаемость, когда A - группа порядка p^2. Однако в этом случае не очень удобно описывать все решения задачи $(K/k, G/A, B/A)$.

Для случая локальных полей и абелева ядра (см. [3]) условие согласности гарантирует погружаемость. Поэтому в этой ситуации удобно рассматривать в качестве A коммутативную подгруппу в B индекса p, нормальную в G (таковая всегда существует, когда порядок B равен p^4). При этом B/A - группа порядка p, и если A содержит систему факторов расширения, то расширение $1 \to B/A \to G/A \to F \to 1$ является прямым, и решения сопутствующей задачи $(K/k, G/A, B/A)$ описываются чрезвычайно просто.

В случае полей алгебраических чисел условие согласности для абелевой задачи $(L/k, G, A)$ не всегда гарантирует погружаемость. Здесь помогает теория, развитая в [4], устанавливающая важное и довольно часто имеющее место условие, при котором согласность влечет разрешимость абелевой задачи. При выполнении этого условия нам достаточно исследовать „второе препятствие" для нашей задачи, т.е. ответить на вопрос, при каких L, решающих задачу $(K/k, G/A, B/A)$, решение L согласно с группой G.

Прежде чем переходить к задачам с конкретными ядрами порядка p^4, отметим результат, легко вытекающий из [5], но не сформулированный там, касающийся задачи погружения с неабелевым ядром порядка p^3. Именно для локальных полей (и p-группы G) задача погружения $(K/k, G, \varphi, B)$ разрешима *всегда* (соответственно автоматически выполняется условие согласности). Если же K и k - поля алгебраических чисел, то нужно исследовать лишь сопутствующую локальную задачу, отвечающую бесконечным дивизорам поля k, т.е. архимедовским пополнениям (и, разумеется, только при $p=2$).

Доказательство содержится в [11].

4°. Пусть B имеет две образующие a, b, причем $a^{p^3}=1$, $b^p=1$, $[a,b]=a^{p^2}$; квадратные скобки означают коммутатор. Это, при $p>2$, - единственная с точностью до изоморфизма, некоммутативная группа периода p^3 и порядка p^4. Задача погружения с таким ядром B исследована в [7]. Здесь получены следующие результаты.

Теорема 4.1. *Для разрешимости задачи погружения $(K/k, G, \varphi, B)$ над локальными полями необходимо и достаточно выполнения условия согласности.*

Теорема 4.2. *Для разрешимости задачи погружения $(K/k, G, \varphi, B)$ над полями алгебраических чисел необходимо и достаточно, чтобы было выполнено условие согласности и (при $p=2$) были разрешимы сопутствующие задачи, отвечающие архимедовским пополнениям.*

5°. Пусть теперь ядро нашей задачи имеет образующие a, b и соотношения $a^{p^2}=1$, $b^p=1$, $c=[a,b]$ - центральный элемент порядка p, отличный от $a^{pt}, t=0,1,\dots,p-1$. Эта задача подробно исследована в [8]. Для этого ядра оказывается, что при факторизации по центру C ядра B расширение $1 \to B/C \to G/C \to F \to 1$ всегда полупрямое, и группа $\mathrm{Aut}_p B$ содержит в качестве подгруппы группу внешних автоморфизмов $\overline{\mathrm{Aut}_p B}$. Поэтому существует гомоморфизм $\theta: F \to \mathrm{Aut}_p B$, как композиция естественного гомоморфизма $\bar\theta: F \to \overline{\mathrm{Aut}_p B}$ и вложения $\overline{\mathrm{Aut}_p B} \to \mathrm{Aut}_p B$. Группа $\overline{\mathrm{Aut}_p B}$ порождается двумя автоморфизмами $\sigma: a \to ab$, $b \to b \pmod{B'}$; $\tau: a \to a$, $b \to a^p b \pmod{B'}$ (B' - коммутант B) и является некоммутативной группой порядка p^3 и периода p при $p>2$ (для $p=2$ это - группа диэдра). Показано, что для числовых полей можно ограничиться исследованием второго препятствия.

Результаты исследования существенно зависят от того, каков образ отображения $\bar\theta: F \to \overline{\mathrm{Aut}_p B}$ и от четности или нечетности p.

Теорема 5.1. *Задача погружения для локальных полей $(K/k, G, \varphi, B)$ при $p=2$ разрешима в том и только в том случае, если для нее выполнено условие согласности. То же верно для нечетного p, если $\bar\theta$ - сюръективен либо порождается элементами τ и $[\sigma,\tau]$.*

Теорема 5.2. *Задача погружения для полей алгебраических чисел $(K/k, G, \varphi, B)$ при $p=2$ разрешима тогда и только тогда, когда выполнено условие согласности и разрешимы сопутствующие задачи, возникающие при архимедовских пополнениях.*

Теорема 5.3. *Пусть $(K/k, G, \varphi, B)$ - задача погружения для полей алгебраических чисел, p - нечетное. Если $\bar\theta$ - сюръективен либо $\mathrm{Im}\,\bar\theta$ не содержит элементов $\sigma^i\tau^j[\sigma,\tau]^k$ при $ij \not\equiv 0 \pmod p$, то для разрешимости этой задачи необходимо и достаточно, чтобы были разрешимы все сопутствующие локальные задачи $(K_{\mathfrak{p}}/k_{\mathfrak{p}}, G, \varphi, B)$ для конечных простых дивизоров $\mathfrak{p}$ поля k.*

Для исключительных случаев построены примеры, показывающие, что эти исключения в формулировках теорем 5.1 и 5.3 существенны. Таким образом, для данного ядра не всегда верен принцип Хассе.

Закономерен вопрос - почему результат для более общего случая (сюръективность

θ) оказывается сильнее, чем для частного? Дело в том, что подполе поля K, отвечающее группе $\mathrm{Ker}\ \theta$ в случае сюръективности, является неабелевым расширением k, и поэтому структурные константы, определяющие это поле, не вполне независимы.

6°. Рассмотрим в качестве группы B группу с образующими a, b, где $a^{p^2}=b^{p^2}=1$, $[a,b]=b^p$ – центральный элемент группы. Здесь группа $\overline{\mathrm{Aut}_p B}$ не вкладывается в группу $\mathrm{Aut}_p B$, имеющую три образующие σ, τ, ω, где $\sigma: a \longrightarrow ab$, $b \longrightarrow b$; $\tau: a \longrightarrow a$, $b \longrightarrow a^p b$; $\omega: a \longrightarrow a$, $b \longrightarrow b^{1+p}$, причем имеют место соотношения $\sigma^{2p}=[\sigma,\tau,\sigma], \tau^p=1$, $\omega^p=1$, $[\sigma,\tau,\tau]=1$, $[\sigma,\omega]=\sigma^p$, $[\tau,\omega]=1$ при p нечетном и $\sigma^2=[\sigma,\omega]$, $\tau^2=1$, $\omega^2=1$, $[\sigma,\tau,\sigma]=1$, $[\sigma,\tau,\tau]=1$, $[\tau,\omega]=1$ для $p=2$ (порядок этой группы p^5). Хотя ω действует как внутренний автоморфизм, индуцированный элементом a, в исследовании задачи его устранить невозможно, сохраняя требование, чтобы G/B' было полупрямым расширением группы B/B'. Это обстоятельство делает выкладки чрезвычайно громоздкими.

Вторая сложность заключается в том, что для абелевой подгруппы $A=\langle a^p, b\rangle$ в качестве ядра, условие согласности не гарантирует погружаемость, когда отображение $\theta: F \longrightarrow \mathrm{Aut}_p B$ не сюръективно, но содержит элементы $\sigma\tau^t$, $t \not\equiv 0 \pmod p$. Поэтому в данном случае приходится решать задачу в два этапа, факторизуя на первом задачу по $A_1=\langle a^p, b^p\rangle$, и соответственно на втором этапе исследуя условие согласности для задачи $(L/k, G, A_1)$, где L – решение полупрямой (а не прямой) задачи $(K/k, G/A_1, B/A_1)$. Полное описание таких решений несколько сложнее, чем для прямой задачи, и на втором этапе это обстоятельство сказывается еще большей громоздкостью. Тем не менее результаты оказываются проще, чем для ядра из предыдущего пункта. Здесь они анонсированы.

Теорема 6.1. *Если для задачи погружения $(K/k, G, \varphi, B)$ над локальными полями при $p>2$ выполнено условие согласности, то она разрешима.*

При $p=2$ этот факт неверен (заметим, что в предыдущем пункте как раз случай $p=2$ был благополучным).

Теорема 6.2. *Задача погружения $(K/k, G, \varphi, B)$ над полями алгебраических чисел при нечетном p разрешима тогда и только тогда, когда разрешима абелева сопутствующая задача $(K/k, G/B', B/B')$.*

Эта формулировка может быть усилена. Именно если $\theta: F \longrightarrow \mathrm{Aut}_p B$ сюръективен или $\mathrm{Im}\theta$ не содержит элемента $\sigma\tau^t (t \not\equiv 0 (\mathrm{mod}\, p))$, то для разрешимости достаточно требовать условия согласности.

Теорема 6.3. *Задача погружения $(K/k, G, \varphi, B)$ над полями алгебраических чисел при $p=2$ разрешима тогда и только тогда, когда разрешимы все сопутствующие локальные задачи $(K_\mathfrak{p}/k_\mathfrak{p}, G, \varphi, B)$, где $\mathfrak{p}$ – простые дивизоры поля k, включая бесконечные.*

Заметим, что проверять разрешимость этих локальных задач нужно в действительности лишь на конечном числе дивизоров $\mathfrak{p}$.

Методика исследования, как и для предыдущих групп, основана на технике теории полей классов [12, 13]. Таким образом, для нашего случая справедлив принцип Хассе.

7°. Рассмотрим теперь ситуации, когда исследование задачи погружения проводится значительно проще. Напомним, что для некоммутативного ядра порядка p^3 задача погружения решается очень легко (см. п. 3°). Значит, если ядро B содержит характеристическую (в p-расширениях) некоммутативную подгруппу B_1 порядка p^3, мы можем свести исследование к задаче $(K/k, G/B_1, B/B_1)$, а второй этап - задача $(L/k, G, B_1)$ решается автоматически (при нечетном p). Укажем случаи, когда такой подход возможен.

1. Пусть группа B имеет три образующие a, b, c, причем $a^{p^2}=b^p=c^p=1$, элемент a - централен, $[b,c]=a^p$, и p - нечетное. Группа $B_1=\langle a^p, b, c\rangle$ - некоммутативная группа периода p, а все остальные элементы B имеют порядок p^2. Поэтому B_1 характеристична, и имеет место результат.

Теорема 7.1. *Задача погружения* $(K/k, G, \varphi, B)$ *для локальных или глобальных числовых полей разрешима в том и только в том случае, когда выполнено условие согласности для сопутствующей задачи* $(K/k, G/B_1, B/B_1)$.

2. Пусть группа B имеет образующие a, b, c, связанные соотношениями $a^{p^2}=b^p=c^p=1$, $[a,b]=1$, $[a,c]=b$, $[b,c]=a^p$ при $p>2$. Для подгруппы $\langle a^p, b, c\rangle=B_1$ справедливы те же соображения, что и для предыдущей группы. Но, кроме того, для каждого $f\in F$ найдется такой прообраз $h\in G$, который коммутирует с b и c, а также оставляет инвариантной циклическую подгруппу $\langle a\rangle$. Множество H таких прообразов есть подгруппа в G и $H\cap B=\langle a^p\rangle=B'$. Значит, расширение $1\to B/B'\to G/B'\to F\to 1$ полупрямое, а расширение $1\to B/B_1\to G/B_1\to F\to 1$ прямое.

Теорема 7.2. *Для указанной группы B задача погружения* $(K/k, G, \varphi, B)$ *в случае числовых полей всегда разрешима.*

Те же соображения применимы к группе B с образующими a, b, c и соотношениями $a^{p^2}=b^p=c^p=1$, $[a,b]=1$, $[a,c]=b$, $[b,c]=a^{pj}$, где j - фиксированный квадратичный невычет по $\mathrm{mod}\,p$, но только при $p>3$ (при $p=3$ группа $B_1=\langle a^p, b, c\rangle$ нехарактеристична в B). Соответственно справедлива и теорема 7.2 применительно к нашей группе.

3. Пусть, наконец, $p=2$ и группа B имеют образующие a, b и соотношения $a^8=b^2=1$, $[a,b]=a^2$. Элементы ba^{ℓ} имеют порядок 2 при четном ℓ и порядок 4 при нечетном. Тем самым группа $B_1=\langle a^2, b\rangle$ - характеристическая подгруппа ядра B и изоморфна группе диэдра. Поэтому задачу погружения $(K/k, G, \varphi, B)$ достаточно исследовать лишь при архимедовских нормированиях поля k, т.е. препятствия могут возникнуть разве лишь, когда $k=\mathbb{R}$ и $K=\mathbb{C}$. Но легко видеть, что все расширения группы B посредством циклической группы порядка 2 полупрямые, так что задача $(\mathbb{C}/\mathbb{R}, \tilde{G}, \tilde{\varphi}, B)$ всегда разрешима, и мы получили теорему.

Теорема 7.3. *Для указанной группы B задача погружения* $(K/k, G, \varphi, B)$ *всегда разрешима.*

Заметим, что как для группы диэдра, так и для данной группы полная группа автоморфизмов является 2-группой. Поэтому здесь является излишним требование, чтобы G сама была 2-группой.

Задачи погружения с не рассмотренными здесь ядрами порядка еще ждут исследования. Мы надеемся, что накопленный экспериментальный материал окажется полезен для каких-то обобщений и гипотез.

Список литературы

[1] Делоне Б.Н., Фаддеев Д.К. Исследования по геометрии теории Галуа // Мат.сб. 1944. Т.15(57), N 2. С.243-276.

[2] Яковлев А.В. Задача погружения полей // Изв.АН СССР. Сер.мат. 1964. Т.28, N 5. С.645-660.

[3] Демушкин С.Н., Шафаревич И.Р. Задача погружения для локальных полей // Изв.АН СССР. Сер.мат. 1959. Т.23, N 6. С.823-840.

[4] Яковлев А.В. Задача погружения для числовых полей // Изв.АН СССР. Сер.мат. 1967. Т.31, N 2. С.211-224.

[5] Лурье Б.Б. К задаче погружения с некоммутативным ядром порядка p^3// Тр.Мат. ин-та АН СССР. 1965. Т.80. С.98-101.

[6] Hölder O. Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4 // Math.Ann. 1893. Bd 43. S.301-412.

[7] Ишханов В.В. О задаче погружения с некоммутативным ядром порядка p^4 // Тр.Мат.ин-та АН СССР. 1990. Т.183. С.116-121.

[8] Ишханов В.В., Лурье Б.Б. О задаче погружения с некоммутативным ядром порядка p^4 // Зап.науч.семинаров ЛОМИ. 1989. Т.175. С.46-52.

[9] Neukirch J. On solvable number fields // Invent.Math. 1979. Vol.53, N 2. P.135-164.

[10] Лурье Б.Б. Об условии согласности в проблеме погружения полей // Зап.науч.семинаров ЛОМИ. 1977. Т.71. С.155-162.

[11] Ишханов В.В., Лурье Б.Б., Фаддеев Д.К. Задача погружения в теории Галуа. М.: Наука, 1990. 272 с.

[12] Artin E., Tate J. Class field theory. Harvard, 1961.

[13] Алгебраическая теория чисел. М.: Мир, 1969. 483 с.

Ленинградское отделение
Математического института им.В.А.Стеклова АН СССР
191011, Ленинград, наб.Фонтанки, д.27

Поступило 5 июня 1990 г.