В. В. Ишханов, Б. Б. Лурье, О задаче погружения над p-расширением,
Алгебра и анализ, 1997, том 9, выпуск 4, 87–97

https://www.mathnet.ru/aa809

Алгебра и анализ
Том 9 (1997), вып. 4

О ЗАДАЧЕ ПОГРУЖЕНИЯ НАД P-РАСШИРЕНИЕМ

© В. В. Ишханов, Б. Б. Лурье

В работе исследована связь произвольной задачи погружения, заданной над p-расширением полей, и присоединенной задачи, связанной с p-расширениями. Особо исследован случай, когда ядро задачи погружения изоморфно знакопеременной группе шести элементов, а также некоторый более широкий класс задач. Доказано, что для задачи погружения с группой диэдра в качестве ядра справедлив аналог теоремы Кохендорфера–Фаддеева.

§1. Об эквивалентности двух задач погружения

1°. Рассмотрим задачу погружения, связанную с точной последовательностью конечных групп

$$1 \to B \to G \xrightarrow{\varphi} F \to 1, \tag{1}$$

где F является p-группой и реализована как группа Галуа p-расширения полей K/k. Группа G не предполагается p-группой. С этой задачей можно связать другую задачу погружения, определенную p-расширением групп

$$1 \to B_p \to G_p \xrightarrow{\varphi_p} F \to 1, \tag{2}$$

где G_p — силовская p-подгруппа группы G, φ_p — ограничение φ на G_p, $B_p = B \cap G_p$ — силовская p-подгруппа группы B. Выбор силовской подгруппы G_p не однозначен, но все получающиеся задачи погружения эквивалентны.

Ясно, что исследование задачи (2) проще, чем исследование задачи (1). В то же время разрешимость задачи (2) гарантирует разрешимость и (1) (в смысле алгебр Галуа). Более общо, имеет место следующее утверждение.

Предложение 1. *Пусть задана точная коммутативная диаграмма конечных групп*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & A_1 & \longrightarrow & G_1 & \xrightarrow{\varphi_1} & F & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle\mu} & & \| & & \\
1 & \longrightarrow & A_2 & \longrightarrow & G_2 & \xrightarrow{\varphi_2} & F & \longrightarrow & 1
\end{array}$$

Ключевые слова: задача погружения, сопутствующие задачи, дедукционные теоремы.
Работа выполнена при частичной поддержке РФФИ, проект № 96-01-00854.

и пусть F реализуется как группа Галуа расширения K/k. Если разрешима задача погружения, связанная с верхней строкой диаграммы, то разрешима и задача погружения, связанная с ее нижней строкой.

Доказательство. Пусть L_1 — решение задачи погружения, связанной с последовательностью
$$1 \to A_1 \to G_1 \xrightarrow{\varphi_1} F = \mathrm{Gal}(K/k) \to 1.$$

Рассмотрим коммутативную диаграмму

$$\begin{tikzcd}
 & & 1 \arrow[d] & 1 \arrow[d] & \\
 & & A_1 \arrow[r, equal] \arrow[d] & A_1 \arrow[d] & \\
1 \arrow[r] & A_2 \arrow[r] \arrow[d, equal] & \bar{G} \arrow[r] \arrow[d] & G_1{=}\mathrm{Gal}(L_1)/k \arrow[r] \arrow[d, "\varphi_1"] & 1 \\
1 \arrow[r] & A_2 \arrow[r] & G_2 \arrow[r, "\varphi_2"] \arrow[d] & F = \mathrm{Gal}(K/k) \arrow[r] \arrow[d] & 1 \\
 & & 1 & 1 &
\end{tikzcd}$$

Здесь $\overline{G}$ — прямое произведение групп G_1 и G_2 с отождествленной фактор-группой F (т.е. множество пар (g_1, g_2), где $\varphi_1 g_1 = \varphi_2 g_2$). Поскольку существует морфизм $\mu\colon G_1 \to G_2$, для которого $\varphi_2\mu = \varphi_1$, существует и вложение $\bar{\mu}\colon G_1 \to \overline{G}$ (именно, $\mu g_1 = (g_1, \mu g_1) \in \overline{G}$), а значит, $\overline{G}$ — полупрямое расширение A_2 посредством G_1. Поэтому задача погружения $(L_1/k, \overline{G})$ разрешима ([1, гл.1]). Но тогда разрешима и задача погружения $(K/k, G_2)$, полученная спуском полупрямой задачи погружения.

Доказанное предложение позволяет дать расширительное толкование понятию сопутствующей задачи погружения первого рода. Именно, будем говорить, что задача погружения $(K/k, G_2, \varphi_2)$ является сопутствующей первого рода для задачи $(K/k, G_1, \varphi_1)$, если существует морфизм (не обязательно сюръективный) $\mu\colon G_1 \to G_2$, для которого $\varphi_2\mu = \varphi_1$.

2°. Итак, разрешимость присоединенной задачи погружения, связанной с последовательностью (2), достаточна для разрешимости задачи погружения (1) (когда F является p-группой). Поставим вопрос: не являются ли эти задачи эквивалентными. В общем случае ответ отрицательный (см. ниже), но в ряде случаев эти задачи действительно эквивалентны.

Теорема 1. *Пусть силовская подгруппа B_p ядра B коммутативна. Тогда задачи погружения $(K/k, G, \varphi, B)$ и $(K/k, G_p, \varphi_p, B_p)$ эквивалентны.*

Доказательство является прямым следствием теоретико-групповой леммы.

Лемма. *Если силовская подгруппа ядра абелева, то существует морфизм $\lambda\colon G \to G_p$, для которого $\varphi_p\lambda = \varphi$.*

Доказательство. Рассмотрим коммутативную диаграмму

$$\begin{tikzcd}
 & & 1 \arrow[d] & 1 \arrow[d] & \\
 & & B \arrow[r, equal] \arrow[d] & B \arrow[d] & \\
1 \arrow[r] & B_p \arrow[r] \arrow[d, equal] & \bar{G} \arrow[r, "\bar{\varphi}"] \arrow[d] & G \arrow[r] \arrow[d, "\varphi"] & 1 \\
1 \arrow[r] & B_p \arrow[r] & G_p \arrow[r, "\varphi_p"] \arrow[d] & F \arrow[r] \arrow[d] & 1 \\
 & & 1 & 1 &
\end{tikzcd}$$

где $\bar{G}$ — прямое произведение G и G_p с отождествленной факторгруппой F. Для последовательности

$$1 \to B_p \to \bar{G} \xrightarrow{\bar{\varphi}} G \to 1$$

возьмем силовское подрасширение

$$1 \to B_p \to (\bar{G})_p \to G_p \to 1.$$

Это — полупрямое расширение групп, так как пары $(g_p, g_p) \in (\bar{G})_p$, очевидно, образуют группу, изоморфную G_p. Но тогда, согласно теореме Гашюца ([1, гл. 3]; [2, IV, 6)], полупрямым является и само расширение

$$1 \to B_p \to \bar{G} \to G \to 1,$$

т.е. существует вложение $\bar{\lambda}\colon G \to \bar{G}$, причем $\bar{\varphi}\bar{\lambda} = Id$. Тем самым существует и морфизм $\lambda\colon G \to G_p$, для которого $\varphi_p\lambda = \varphi$. Лемма доказана.

Заметим, что для произвольной последовательности

$$1 \to B \to G \to F \to 1,$$

где G — p-группа, точно так же доказывается, что существует морфизм $G \to G_p/B'_p$, где B'_p — коммутант B_p.

Теорема 1 следует теперь из доказанной леммы, так как решение задачи погружения $(K/k, G_p, \varphi_p)$ получается спуском из произвольного решения задачи погружения $(L/k, \bar{G}, \bar{\varphi})$, где L — решение задачи погружения (1), а задача $(L/k, \bar{G}, \bar{\varphi})$ — полупрямая и поэтому разрешима.

Замечание. Теорему Гашюца правильнее называть теоремой Гашюца–Фаддеева. Д. К. Фаддеев получил ее в начале пятидесятых годов при доказательстве ее аналога в теории погружения (теоремы Кохендерфера–Фаддеева), применив оригинальную конструкцию, эквивалентную гомоморфизму коограничения. Эта конструкция впервые была опубликована в [3] (см. также [1, гл.3]).

3°. Построим пример, показывающий, что в случае некоммутативной силовской подгруппы B_p ядра B условия погружаемости для задач (1) и (2) не всегда совпадают. В качестве присоединенной силовской задачи погружения (2) используем пример из [1, гл. 4, §1].

Именно, пусть k — конечное расширение поля p-адических чисел $\mathbb{Q}_p$ (p - нечетное), содержащее первообразный корень ζ степени p из 1, но не содержащее $\sqrt[p]{\zeta}$. Группа $k^*/(k^*)^p$ изоморфна в этом случае линейному пространству размерности $\nu = n+2$ над полем из p элементов, где $n = (k : \mathbb{Q}_p)$. Соответственно группа Галуа максимального p-расширения поля k — про- p-группа с ν образующими $s_1, \ldots, s_\nu$ и одним соотношением типа $s_2^p[s_1, s_2][s_3, s_4] \ldots [s_{\nu-1}, s_\nu] = 1$ (см. [4]).

Пусть поле K получено из k присоединением всех корней степени p из k^*, т.е. $K = k(\sqrt[p]{a_1}, \sqrt[p]{a_2}, \ldots \sqrt[p]{a_\nu})$, где элементы $a_1, a_2, \ldots a_\nu \in k^*$ выбраны так, что мультипликативные символы Гильберта равны ζ на парах $(a_1, a_2), (a_3, a_4), \ldots (a_{\nu-1}, a_\nu)$ и тривиальны в остальных случаях. Соответственно $F = \mathrm{Gal}(K/k)$ — элементарная абелева p-группа с образующими $f_1, f_2, \ldots f_\nu$ (образами элементов $s_1, s_2, \ldots, s_\nu$).

В качестве G_p возьмем p-группу с образующими $g_1, g_2, \ldots g_\nu, \beta$, где $\beta^p = 1$, $g_1^p = g_2^p = \cdots = g_\nu^p = \gamma$, $\gamma^p = 1$; пусть коммутаторы $[\beta, g_i] = \alpha_i$ $(i = 1, 2, \ldots \nu)$ все различны и имеют порядок p, а $[g_i, g_j] = 1$ для любых i, j. Элементы α_i также коммутируют с g_j и друг с другом, а $[\alpha_i, \beta] = \gamma$ для всех α_i. Зададим эпиморфизм $\varphi_p \colon G_p \to F$ по правилу: $\varphi_p(g_i) = f_i$, $\varphi_p(\alpha_j) = 1$, $\varphi_p(\beta) = 1$. Тогда ядро φ_p — это группа B_p, порожденная элементами $\alpha_1, \alpha_2, \ldots \alpha_\nu, \beta$. В [1, гл. 4, 1.4] показано, что задача погружения $(K/k, G_p, \varphi_p, B_p)$ неразрешима.

Определим теперь группу G как полупрямое расширение своей нормальной подгруппы G_p посредством группы порядка 2, порожденной элементом δ. Действие δ на G_p определим по правилам: $\beta^\delta = \beta^{-1}$, $g_i^\delta = \beta^{-1} g_i \beta = g_i \alpha_i^{-1}$. Ясно, что δ определяет на G_p автоморфизм второго порядка, при этом $\gamma^\delta = (g_i^p)^\delta = \gamma$, $\alpha_i^\delta = (\beta^{-1} g_i^{-1} \beta g_i)^\delta = \beta \alpha_i g_i^{-1} \beta^{-1} g_i \alpha_i^{-1} = \beta \beta^{-1} g_i^{-1} \beta g_i g_i^{-1} \beta^{-1} g_i \alpha_i^{-1} = \alpha_i^{-1}$. Поскольку $g_i^{-1} \delta g_i = \delta \beta^{-1} g_i^{-1} \beta g_i = \delta \alpha_i$, подгруппа B, порожденная B_p и элементом δ, нормальна в G, и имеет место точная последовательность групп

$$1 \to B \to G \xrightarrow{\varphi} F \to 1,$$

где $\varphi(\delta) = 1$, $\varphi(\tau) = \varphi_p(\tau)$ для $\tau \in G_p$.

Рассмотрим задачу погружения

$$(K/k, G, \varphi, B). \tag{1}$$

Присоединенная силовская задача

$$(K/k, G_p, \varphi_p, B_p), \tag{2}$$

как сказано выше, неразрешима.

Теорема 2. *Построенная задача погружения* (1) — *разрешима.*

Доказательство. Обозначим через A подгруппу ядра B, порожденную элементами $\alpha_1, \ldots, \alpha_\nu$ и $\gamma = g_i^p$. Групповое расширение

$$1 \to B/A \to G/A \to F \to 1 \tag{3}$$

прямое, поэтому всякое решение задачи погружения, связанной с последовательностью (3), имеет вид $L_1 = K \otimes_k K_1$, где K_1 — расширение поля k с группой Галуа B/A.

Группа B/A порождена образующими $\bar\beta$, $\bar\delta$ с соотношениями $\bar\beta^p = 1$, $\bar\delta^2 = 1$, $\bar\delta\bar\beta\bar\delta = \bar\beta^{-1}$, т.е. является группой диэдра порядка $2p$. Построим расширение K_1/k с группой Галуа B/A.

Возьмем элемент $c \in k^*$, не являющийся квадратом в k. В квадратичном расширении $k(\sqrt{c})$ выберем элемент v с нормой 1 (для этого, согласно теореме Гильберта-90, необходимо и достаточно, чтобы было $v = w\bar{w}^{-1}$, где $w \in k(\sqrt{c})$, $\bar{w}$ — сопряженный элемент; если при этом $w = x + y\sqrt{c}$, где $x \neq 0$, $y \neq 0$, то $v \notin k$). Присоединив к $k(\sqrt{c})$ элемент θ такой, что $\theta^p = v$, получим поле K_1, нормальное над k с группой диэдра; автоморфизмы $\bar\beta$ и $\bar\delta$ действуют в K_1 по формулам: $\theta^{\bar\beta} = \theta\zeta$, $\theta^{\bar\delta} = \theta^{-1}$, $\sqrt{c}^{\bar\beta} = \sqrt{c}$, $\sqrt{c}^{\bar\delta} = -\sqrt{c}$. Легко показать, что таким образом получается всякое расширение поля k (содержащего $\sqrt[p]{1}$) с группой диэдра, но нам этот факт не понадобится. Заметим, что если $v \notin k$, полученное расширение K_1 является полем. Соответственно полем будет и $L_1 = K \otimes_k K_1$.

Рассмотрим задачу погружения, связанную с последовательностью

$$1 \to A \to G \to \mathrm{Gal}(L_1/k) \to 1. \tag{4}$$

Так как ядро этой задачи — абелева группа, справедлива теорема Кохендерфера-Фаддеева, т.е. задача (4) редуцируется к задаче погружения с p-группами

$$1 \to A \to G_p \to \mathrm{Gal}(L_1/k(\sqrt{c})) \to 1. \tag{5}$$

Покажем, что задача (5) разрешима. Так как L_1 — поле, то согласно теореме Демушкина-Шафаревича ([5], см. также [1, 3.14]), для этого достаточно проверить условия согласности для всех сопутствующих центральных брауэровских задач, т.е. для задач, связанных с последовательностями

$$1 \to A/\operatorname{Ker}\chi \to G_p/\operatorname{Ker}\chi \to H = \mathrm{Gal}(L_1/k(\sqrt{c})) \to 1,$$

где $\chi \in \mathrm{Hom}_H(A, L_1^*)$. Поскольку A — группа экспоненты p, то $\mathrm{Hom}(A, L_1^*) = \mathrm{Hom}(A, k^*)$, а значит, $\chi(\alpha_i\gamma) = \chi(\alpha_i^{\beta}) = \chi(\alpha_i)^{\beta} = \chi(\alpha_i)$, откуда $\chi(\gamma) = 1$ для всех $\chi \in \mathrm{Hom}_H(A, L_1^*)$.

Поэтому задача погружения (5) редуцируется к задаче, связанной с последовательностью

$$1 \to A/C \to G_p/C \to (L_1/k(\sqrt{c})) \to 1, \tag{6}$$

где C — подгруппа, порожденная центральным элементом γ.

Ядро задачи (6) — прямое произведение циклических подгрупп порядка p, порожденных каждая элементом $\bar\alpha_i$ (где $\bar\alpha_i$ — образ α_i в A/C) и нормальных в G_p/C. Значит, задача (6) разрешима тогда и только тогда, когда разрешимы все сопутствующие задачи, полученные факторизациями по подгруппам $\tilde{A}_i = \langle\bar\alpha_1, \dots \bar\alpha_{i-1}, \bar\alpha_{i+1}, \dots, \alpha_\nu\rangle$. Покажем, что все они разрешимы.

Рассмотрим одну из таких задач, связанную с точной последовательностью

$$1 \to A/\tilde{A}_i \to G_p/\tilde{A}_i \to H = \mathrm{Gal}(L_1/k(\sqrt{c})) \to 1. \tag{7i}$$

В группе $G_p/\tilde{A}_i$ содержится подгруппа, порожденная образами элементов $g_1, \dots, g_{i-1}, g_{i+1}, \dots, g_\nu$ в $G_p/\tilde{A}_i$, нормальная в $G_p/\tilde{A}_i$ и не содержащая неединичных элементов ядра. Посредством спуска по этой подгруппе задача погружения (7i) редуцируется к задаче погружения, связанной с последовательностью

$$1 \to A/\hat{A}_i \to T_i \to \mathrm{Gal}(k(\sqrt[p]{c}, \theta\sqrt[p]{a_i})/k(\sqrt[p]{c})) \to 1, \tag{8i}$$

где T_i — некоммутативная группа порядка p^3 и экспоненты p.

Условие погружения для такой брауэровской задачи хорошо известно. Оно состоит в том, что символ норменного вычета (a_i, θ^p) должен быть тривиален над $k(\sqrt{c})$. Но, по построению, $\theta^p = v \in k(\sqrt{c})$. Значит, $(a_i, \theta^p)_{k(\sqrt{c})} = (a_i, v)_{k(\sqrt{c})} = (a_i, N_{k(\sqrt{c})/k} v)_k = (a_i, 1)_k = 1$.

Таким образом, все задачи (8i) разрешимы. Значит, разрешима и задача погружения (4), а всякое ее решение является и решением задачи (1). Теорема доказана.

Напомним, что присоединенная задача погружения (2) неразрешима.

§2. Задача погружения с ядром, изоморфным группе диэдра

В теории погружения с коммутативным ядром важную роль играет редукционная теорема Кохендерфера–Фаддеева. Именно, задача погружения, связанная с последовательностью конечных групп

$$1 \to A \to G \xrightarrow{\varphi} F \to 1,$$

где A — коммутативная p-группа, а F реализована как группа Галуа расширения K/k, редуцируется к своей сопутствующей задаче второго рода, связанной последовательностью

$$1 \to A \to G_p \to F_p \to 1,$$

где G_p — силовская p-подгруппа группы $G, F_p = \varphi(G_p)$ и является группой Галуа расширения K/k_p, где k_p — подполе поля K, отвечающее подгруппе F_p.

Для некоммутативного ядра, являющегося p-группой, такой редукции, в общем случае, нет ([1, гл. 5, §2]). Покажем, однако, что аналог теоремы Кохендерфера–Фаддеева справедлив в случае, когда ядро является группой диэдра восьмого порядка.

Итак, пусть задача погружения связана с последовательностью конечных групп

$$1 \to D \to G \to F \to 1, \tag{1}$$

где D порождена элементами α, β с соотношениями $\alpha^4 = 1$, $\beta^2 = 1$, $\beta\alpha\beta = \alpha^{-1}$, $F = \mathrm{Gal}(K/k)$, G и F не предполагаются 2-группами, характеристика поля k отлична от 2. Группа автоморфизмов ядра D является 2-группой, а группа внешних автоморфизмов — циклическая группа порядка 2. Будем считать, что группа F содержит нетривиальный внешний автоморфизм ядра (в противном случае исследование значительно проще). Тогда подполе поля K, отвечающее подгруппе F_0 элементов группы F, чьи прообразы действуют на D как внутренние автоморфизмы, является квадратичным расширением $k(\sqrt{c})$ поля k, и элемент $c \in k^*$ определен с точностью до квадратов.

Условия погружаемости для задачи погружения с ядром D известны ([1, гл. 5, §1]; см. также[6]). Напомним их.

1. Для задачи (1) выполнено условие согласности. В этом случае определена алгебра обобщенных кватернионов P размерности 4 над полем k (со структурными константами $a, b \in k^*$).

2. Указанный элемент c должен быть приведенной нормой кватерниона из P (т.е. должно быть разрешимо уравнение $c = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2$, $x_i \in k$).

Теперь перейдем к нашей редукционной теореме.

Теорема 3. *Пусть определена задача погружения* (1) *с группой диэдра восьмого порядка в качестве ядра. Для ее разрешимости необходимо и достаточно чтобы была разрешима сопутствующая силовская задача второго рода, т.е. задача, связанная с последовательностью*

$$1 \to D \to G_2 \to F_2 = \mathrm{Gal}(K/k_2) \to 1, \tag{2}$$

где $k_2 = K^{F_2}$.

Доказательство. Ясно, что доказывать надо лишь достаточность. Пусть задача (2) — разрешима. В частности, для нее выполнено условие согласности. Тем самым, выполнено условие согласности и для задачи (1) (см.[1, гл. 2, §4]).

Ясно, что определенный выше элемент c для обеих задач (1) и (2) может быть выбран одним и тем же и принадлежать полю k. Покажем, что и элементы a, b могут быть выбраны для обеих задач одними и теми же (и принадлежащими k).

Пусть $\{l_g\}$, $g \in G$ — система согласности для задачи (1), т.е. l_g — одномерный мультипликативный коцикл из $Z^1(G,(K[D])^*)$, для которого $l_\gamma = \gamma^{-1}$ для $\gamma \in D$ ([1], 2, 7). В скрещенном произведении $G \times K$ элементы $u_g l_g$ образуют группу, изоморфную группе F. Поэтому подалгебра M, порожденная этими элементами и полем k, является матричной. Указанная выше алгебра P является централизатором алгебры ME ($E = \frac{1-\alpha^2}{2}$ — центральный идемпотент) в алгебре $(G \times K)E$. Значит, элементы алгебры обобщенных кватернионов P коммутируют со всеми элементами поля K, а потому принадлежат компоненте группового кольца $K[B]E$. Поэтому $a = \xi^p$, $b = \eta^p$, где $\xi, \eta \in K[B]E$, коммутируют со всеми $u_g l_g E$ и антикоммутируют между собой.

Для силовской задачи (2) возьмем в качестве системы согласности ограничение lg на G_2. Тогда алгебра P_2 является подалгеброй в $K[B]E$, и построенные выше ξ, η порождают ее над K_2. Значит, P_2 — алгебра обобщенных кватернионов над k_2 со структурными константами a, b.

Итак, разрешимость задачи (1) означает, что существуют x_1, x_2, x_3, $x_4 \in k$, решающие уравнение

$$c = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2. \tag{$*$}$$

Соответственно разрешимость задачи (2) означает представимость элемента c в виде

$$c = y_1^2 - ay_2^2 - by_3^2 + aby_4^2, \tag{$**$}$$

где y_1, y_2, y_3, $y_4 \in k_2$.

Эти условия можно переформулировать иначе. Квадратичная форма

$$z_1^2 - az_2^2 - bz_3^2 + abz_4^2 - cz_0^2$$

должна быть изотропна над k (условие $*$) или над k_2 (условие $**$) (если $z_0 = 0$, то форма от четырех переменных изотропна, а потому представляет любой элемент поля).

Напомним, что k_2 — подполе поля k, отвечающее подгруппе F_2, и потому имеет над k нечетную степень.

Для окончания доказательства осталось воспользоваться теоремой Шпрингера (см.[7]): если квадратичная форма с коэффициентами из поля k изотропна над расширением поля k нечетной степени, то она изотропна над самим k.

§3. Задача погружения с ядром $\mathfrak{A}_6$

В статье [8] было показано, что задача погружения с ядром $\mathfrak{A}_n$ (знакопеременная группа n элементов) всегда разрешима при $n > 3$, $n \neq 6$. Доказательство базировалось на том, что для знакопеременной неабелевой ($n > 3$) группы полной группой автоморфизмов является (при $n \neq 6$) симметрическая группа $\mathfrak{S}_n$, а она — полупрямое расширение $\mathfrak{A}_n$ посредством любой транспозиции. Однако на симметрической группе $\mathfrak{S}_6$ (а тем самым, и на $\mathfrak{A}_6$) действуют внешние автоморфизмы, переводящие всякий двучленный цикл в произведение трех независимых двучленных циклов (и соответственно, трехчленный цикл из $\mathfrak{A}_6$ в произведение двух независимых трехчленных циклов).

В настоящем параграфе полностью исследован этот исключительный случай. Получены также и другие результаты.

Напомним, что когда ядро задачи погружения имеет единичный центр, в качестве группы G можно рассматривать группу автоморфизмов ядра или ее подгруппу ([8]). Это объясняется тем, что произвольное расширение с таким ядром допускает спуск по централизатору ядра ([1, гл. 1, §3]).

1°. Группа внешних автоморфизмов группы $\mathfrak{S}_6$ имеет порядок 2. Зададим действие внешнего автоморфизма σ на пяти двучленных циклах $\mathfrak{S}_6$ (разумеется, выбор σ неоднозначен): $(12)^\sigma = (12)(34)(56)$; $(13)^\sigma = (13)(25)(46)$; $(14)^\sigma = (14)(26)(35)$; $(15)^\sigma = (15)(24)(36)$; $(16)^\sigma = (16)(23)(45)$.

Этими формулами автоморфизм σ полностью определен, так как всякая подстановка из $\mathfrak{S}_6$ порождается указанными транспозициями. Например, $(23)^\sigma = ((12)(13)(23))^\sigma = (16)(24)(35)$. Имеем далее: $(24)^\sigma = (15)(23)(46)$; $(25)^\sigma = (13)(26)(45)$; $(26)^\sigma = (14)(25)(36)$; $(34)^\sigma = (12)(36)(45)$; $(35)^\sigma = (14)(23)(56)$; $(36)^\sigma = (15)(26)(34)$; $(45)^\sigma = (16)(25)(34)$; $(46)^\sigma = (13)(24)(56)$; $(56)^\sigma = (12)(35)(46)$.

Легко проверяется, что выбранный автоморфизм σ является инволюцией, т.е. $\sigma^2 = 1$. Поэтому $\operatorname{Aut} \mathfrak{S}_6$ — полупрямое расширение $\mathfrak{S}_6$. На $\mathfrak{A}_6$ группу внешних автоморфизмов представляют автоморфизм σ, произвольная транспозиция τ и $\sigma\tau$. Следовательно, группа внешних автоморфизмов $\operatorname{Aut}\mathfrak{A}_6/\mathfrak{A}_6$ — четверная группа.

Выделим какую-либо силовскую 2-подгруппу в $\operatorname{Aut}\mathfrak{A}_6$. Именно, пусть

$$\alpha = (16)(2435) \in \mathfrak{A}_6, \beta = (16)(23) \in \mathfrak{A}_6, \tau = (16) \in \mathfrak{S}_6$$

и указанный автоморфизм σ. Нетрудно проверить соотношения: $\alpha^4 = 1$, $\beta^2 = 1$, $\beta^{-1}\alpha\beta = \alpha^{-1}$; $\tau^2 = 1$, $\alpha^\tau = \alpha$, $\beta^\tau = \beta$; $\sigma^2 = 1$, $\alpha^\sigma = \alpha^{-1}$, $\beta^\sigma = \beta\alpha$, $\sigma^{-1}\tau\sigma = \tau\alpha^2$.

Таким образом, группа G_2 (силовская 2-подгруппа группы $\operatorname{Aut}\mathfrak{A}_6 = \operatorname{Aut}\mathfrak{S}_6$) имеет порядок 32 и порождена указанными элементами α, β, τ, σ. Пересечение $D = G_2 \cap \mathfrak{A}_6$ образована элементами α, β и изоморфна группе диэдра восьмого порядка.

Итак, рассмотрим две задачи погружения, связанные с последовательностями групп

$$1 \to \mathfrak{A}_6 \to G \xrightarrow{\varphi} F \to 1, \tag{1}$$

$$1 \to D \to H \xrightarrow{\varphi_2} F \to 1, \tag{2}$$

где $G = \operatorname{Aut}\mathfrak{A}_6$, H — ее силовская 2-подгруппа, D — группа диэдра, F — четверная группа. Пусть $F = \operatorname{Gal}(K/k)$, где K получено из k присоединением двух квадратных радикалов: $K = k(\sqrt{m_1}, \sqrt{m_2})$. Будем считать, что $m_1, m_2 \in k$ выбраны так, чтобы элементы σ, τ (точнее, их образы в F) действуют на них по правилу: $\sqrt{m_1}^\sigma = -\sqrt{m_1}$, $\sqrt{m_1}^\tau = \sqrt{m_1}$, $\sqrt{m_2}^\sigma = \sqrt{m_2}$, $\sqrt{m_2}^\tau = -\sqrt{m_2}$.

Покажем сперва, что задача погружения (2) разрешима не всегда. Для этого вычислим элементы c, a, b из предыдущего параграфа для нашей задачи.

Поле $k(\sqrt{c})$ принадлежит в K подгруппе F_0, действующей на ядре как внутренние автоморфизмы. Поскольку в нашем случае F_0 порождается образом элемента τ, $k(\sqrt{c}) = k(\sqrt{m_1})$, и поэтому можно считать, что $c = m_1$.

Рассмотрим скрещенное произведение $H \times K$ и его простую компоненту $(H \times K)E$, где $E = \frac{1-\alpha^2}{2}$. Алгебра $(H \times K)E$ имеет над k размерность 64 и раскладывается в тензорное произведение над k трех коммутирующих алгебр: $k(\alpha E, \beta E)$, $k(\sqrt{m_2}; \tau E)$, $k(\sqrt{m_1}, \sigma\beta(1+\alpha)\sqrt{m_2}E)$. Первые две подалгебры — матричные, поэтому для задачи (2) выполнено условие согласности. Третья подалгебра — алгебра обобщенных кватернионов со структурными константами m_1, $2m_2$. Поэтому можно считать, что $a = m_1$, $b = 2m_2$ (разумеется, можно выбрать коммутирующие подалгебры по другому, так, чтобы нематричная подалгебра содержалась в групповом кольце, но она будет изоморфна указанной).

Таким образом, разрешимость задачи (2) равносильна представимости m_1 квадратичной формой

$$m_1 = x_0^2 - m_1 x_1^2 - 2m_2 x_2^2 + 2m_1 m_2 x_3^2$$

над полем k. Ясно, что такое представление не всегда возможно (например, когда k вкладывается в $\mathbb{R}$, а m_1, m_2 — отрицательные). Поэтому вопрос об эквивалентности задач (1) и (2) содержателен.

Теорема 4. *Задача погружения* (1) *разрешима тогда и только тогда, когда разрешима присоединенная задача погружения* (2).

Доказательство. Нам надо доказать, что из разрешимости задачи (1) следует разрешимость задачи (2).

Пусть L — решение задачи (1). L может быть как полем, так и алгеброй Галуа. Поднимем задачу погружения (2) до L, т.е. рассмотрим задачу погружения, связанную с последовательностью групп

$$1 \to D \to \bar{H} \xrightarrow{\varphi_3} G \to 1, \tag{3}$$

где $\bar{H}$ — произведение групп H и G с отождествленной факторгруппой F, а $G = \mathrm{Gal}(L/k)$. Задача (3) эквивалентна задаче погружения (2).

Пусть L' — поле-ядро алгебры L (если L — поле, то $L' = L$), а G' — группа Галуа расширения L'/k. Тогда G' — подгруппа группы G, и задача погружения (3) равносильна задаче погружения над полем, отвечающей последовательности

$$1 \to D \to \bar{H}' \xrightarrow{\varphi_4} G' \to 1, \tag{4}$$

где $\bar{H}'$ — образ G' в $\bar{H}$.

Согласно теореме 3, задача погружения (4) равносильна силовской задаче погружения (5), отвечающей последовательности

$$1 \to D \to \bar{H}'_2 \xrightarrow{\varphi_5} G'_2 \to 1, \tag{5}$$

где $\bar{H}'_2$ и G'_2 — силовские 2-подгруппы $\bar{H}'$ и G' соответственно.

Группа $\bar{H}'_2$ — произведение групп H и G'_2 с отождествленной факторгруппой F. Поскольку G' — подгруппа группы G, G'_2 — подгруппа силовской 2-подгруппы группы G, а поэтому вкладывается в группу $H = G_2$. Тем самым групповое расширение (5) — полупрямое. Значит, задача погружения (5) разрешима. Соответственно разрешимы и эквивалентные ей задачи погружения (4), (3) и (2). Теорема доказана.

Замечание. Групповое расширение (3)

$$1 \to D \to \bar{H} \xrightarrow{\varphi_3} G \to 1$$

довольно примечательно. Его силовская часть

$$1 \to D \to \bar{H}_2 \to H \to 1,$$

как показано выше, расщепляется. Покажем, что само расширение (3) не расщепляется. Предположим противное. Тогда существует отображение $\lambda\colon G \to H$, такое, что $\varphi_2\lambda = \varphi_1$. Тем самым, задан морфизм $\lambda_0\colon \mathfrak{A}_6 \to D$. Но группа $\mathfrak{A}_6$ — простая, поэтому $\operatorname{Ker}\lambda_0 = \mathfrak{A}_6$ и отображение λ_0 — тривиальное. Но тогда морфизм λ определяет вложение F в H, т.е. расширение (2) — полупрямое, что неверно.

Хорошо известно, что теорема Гашюца не переносится на случай неабелева ядра. Для группы кватернионов соответствующий пример доставляет группа порядка 48. Но для группы диэдра таких примеров еще не было, и возможно, что построенное расширение (3) в этом смысле минимально.

Заметим также, что задача погружения (3) дает еще один пример универсально разрешимой задачи погружения (см. [9]).

2°. Группа $\mathfrak{A}_6$ уникальна в классе знакопеременных групп, однако другое ее представление позволяет перенести полученный результат на более широкий класс групп. Заметим для этого, что $\mathfrak{A}_6$ изоморфна $PSL(2,9)$ ([10, с.10]).

На группе $PSL(2,9)$ внешние автоморфизмы τ и σ имеют более понятную природу. Именно, автоморфизм τ — это автоморфизм Фробениуса $x \to x^3$, примененный ко всем элементам матрицы. Представителем автоморфизма σ может служить сопряжение на $PSL(2,9)$ посредством матрицы из $GL(2,9)$, не являющееся внутренним сопряжением (т.е. ее определитель — не квадрат в $GF(9)$).

Эти соображения позволяют перенести результат данного параграфа на другие группы. Именно, рассмотрим группу $PSL(2,p^2)$, где $p \equiv \pm 3 \pmod 8$ — простое число.

Группа внешних автоморфизмов $PSL(2,p^2)$ также является четверной группой, порожденной на $PSL(2,p^2)$ автоморфизмом Фробениуса и внешним сопряжением [11, §10]. Силовская 2-подгруппа $PSL(2,p^2)$ является группой диэдра восьмого порядка при $p \equiv \pm 3 \pmod 8$. Тем самым на этот класс групп дословно переносятся все рассуждения настоящего параграфа, и мы получили теорему.

Теорема 5. *Пусть B — группа $PSL(2,p^2)$ при $p \equiv \pm 3 \pmod 8$. Задача погружения с ядром B равносильна присоединенной 2-силовской задаче.*

Авторы выражают благодарность В. М. Цветкову за полезные обсуждения.

Список литературы

[1] Ишханов В. В., Лурье Б. Б., Фаддеев Д. К., *Задача погружения в теории Галуа*, Наука, Гл. ред. физ.-мат. лит., М., 1990.
[2] Касселс Дж., Фрёлих А. (ред.), *Алгебраическая теория чисел*, Мир, М., 1969.
[3] Зяпков Н. П., Яковлев А. В., *Универсально согласные расширения Галуа*, Зап. науч. семин. ЛОМИ **71** (1977), 133–152.
[4] Демушкин С. П., *Группа максимального p-расширения локального поля*, Изв. АН СССР. Сер. мат. **25** (1961), № 3, 329–346.
[5] Демушкин С. П., Шафаревич И. Р., *Задача погружения для локальных полей*, Изв. АН СССР. Сер. мат. **23** (1959), № 6, 823–840.
[6] Лурье Б. Б., *К задаче погружения с некоммутативным ядром порядка p^3*, Тр. Мат. ин-та АН СССР **80** (1965), 98–101.
[7] Lam T. Y., *The algebraic theory of quadratic forms*, W. A. Benjamin, Inc., Reading, MA, 1973.
[8] Лурье Б. Б., *К задаче погружения с ядром без центра*, Изв. АН СССР. Сер. мат. **28** (1964), № 5, 1135–1138.
[9] Лурье Б. Б., *Об универсально разрешимых задачах погружения*, Тр. Мат. ин-та АН СССР **183** (1990), 121–126.
[10] Gorenstein D., Lyons R., Solomon R., *The classification of the finite simple groups*, Math. Surveys Monogr., vol. 40.1, Amer. Math. Soc., Providence, RI, 1994.
[11] Стейнберг Р., *Лекции о группах Шевалле*, Мир, М., 1975.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
191011, Санкт-Петербург, наб. р. Фонтанки, 27
Россия

Поступило 4 марта 1997 г.