Записки научных
семинаров ПОМИ
Том 443, 2016 г.

М. А. Бондаренко, Б. Б. Лурье

УСЛОВИЕ СОГЛАСНОСТИ. ВОЗМОЖНОСТЬ РЕДУКЦИИ К АБЕЛЕВОЙ СИТУАЦИИ.

§1. Предисловие

Условие согласности Фаддеева–Хассе является важным необходимым условием разрешимости задачи погружения. В работах [4–6] его удалось редуцировать к случаю, когда заданная группа является p-группой. Кроме того, когда рассматривается задача погружения над числовыми полями (или, более общо, когда совпадают порядок и показатель в группе Брауэра), условие согласности редуцируется к случаю коммутативного ядра, что серьёзно упрощает его проверку.

В то же время в общей ситуации такая редукция не всегда возможна. Был построен пример для 2-групп (ядром выступала группа кватернионов, а погружаемое поле было квадратичным расширением основного [6]). Однако, специфика 2-группы в этом примере весьма существенна и опирается на одну из теорем Алберта о тензорном произведении алгебр обобщённых кватернионов ([2]). Аналог такой теоремы для циклических пар с p-расширением при нечётном p не доказан и представляет собой очень трудную задачу.

В настоящей работе исследуется условие согласности в проблеме погружения полей с p-группами при нечётном p и некоммутативном ядре. Выяснено, что гипотетическая редукция к абелеву ядру в общем случае неверна, хотя для групп малого порядка справедлива.

Статья представляет собой переработанную дипломную работу первого из соавторов, выполненную под руководством второго.

Авторы выражают признательность А. В. Яковлеву за полезные замечания.

§2. Введение

2.1. Условие согласности. Напомним одну из формулировок условия согласности, которую будем использовать в дальнейшем.

Ключевые слова: задача погружения, условие согласности, некоммутативное ядро.

Пусть K/k – расширение Галуа с группой F и ψ: $G \to F$ – сюръективный гомоморфизм. Скрещенным произведением $G \times K$ группы G с полем K называется алгебра над k, составленная из формальных сумм $\sum\limits_g u_g x_g$, $x_g \in K$, с правилами умножения $u_{g_1} u_{g_2} = u_{g_1 g_2}$ и $x u_g = u_g x^{\psi(g)}$. Эта алгебра содержит в качестве подалгебры алгебру $K[N]$, где $N = \mathrm{Ker}(\psi)$.

Одна из формулировок условия согласности, открытая Д. К. Фаддеевым, состоит в "распадении" скрещенного произведения. Именно, это условие состоит в том, что алгебра $G \times K$ изоморфна алгебре матриц порядка $(F{:}1)$ над некоторой своей подалгеброй.

В дальнейшем предполагается, что характеристика поля k взаимно проста с порядком ядра. В этом случае как групповое кольцо $K[N]$, так и скрещенное произведение $G \times K$ являются полупростыми алгебрами. Соответственно, распадение $G \times K$ равносильно распадению всех его простых компонент. Не ограничивая общности, можно считать, что G является p-группой [4–6], а поле k содержит корни из 1 степени, равной периоду ядра [2].

В качестве ядра N задачи погружения рассмотрим некоммутативную группу порядка p^3 и показателя p. Группа порядка p^3 и показателя p^2 исследуется аналогично. Группа G предполагается p-группой.

В [2] эта задача решена в предположении, что выполнено условие согласности. Заметим, что факторизация по коммутанту ядра приводит к полупрямому расширению (когда G – p-группа), поэтому сопутствующая абелева задача разрешима, и, тем самым, выполнено условие согласности.

2.2. Обозначения. Существуют две группы порядка p^3, при нечётном p, которые задаются образующими и соотношениями как

$$H_1 = \langle \alpha, \beta | \alpha^p = \beta^p = [\alpha, \beta]^p = 1 \rangle$$

и

$$H_2 = \langle \alpha, \beta | \alpha^p = \beta^{p^2} = 1, \alpha^\beta = \alpha\beta^p \rangle.$$

Мы будем обозначать γ образующую центра группы, то есть $\gamma = [\alpha, \beta]$ для H_1 и $\gamma = \beta^{ps}$ для H_2, где s не делится на p и будет выбрано по ситуации. Несложно видеть, что в этих группах центр циклический порядка p и совпадает с коммутантом. Более того, видно, что сопутствующая абелева задача в нашем случае всегда разрешима, поскольку является полупрямой задачей. Поэтому наша цель – лишь построить пример, когда сама задача не согласна.

В работе нас будет интересовать действие элементов G на N. Очевидно, автоморфизмы из G вкладываются в некоторую силовскую p-подгруппу полной группы автоморфизмов $Aut(N)$. В свою очередь, при подходящем выборе образующих в N, автоморфизмы силовской подгруппы описываются так:

для $H_1 =$: $\alpha^g = \alpha\gamma^j$, $\gamma^g = \gamma$, $\beta^g = \beta\alpha^k\gamma^i$.

для H_2: $\alpha^g = \alpha\beta^{pj}$, $\beta^g = \alpha^k\beta^{1+pi}$.

Мы предполагаем, что поле k содержит первообразный корень степени p из 1, который впредь будет обозначаться нами ζ.

Почти все дальнейшие рассуждения будут проводиться для группы H_1, но обозначения специально будут введены таким образом, чтобы те же конструкции проходили и для H_2.

Заметим, что элементы вида $e_k = \frac{\sum_{i=0}^{p-1} \gamma^i\zeta^{ki}}{p}$ являются минимальными центральными идемпотентами алгебры $\Lambda = G \times K$, причём $\gamma e_k = \zeta^{-k}e_k$. Тем самым, алгебры вида Λe_k являются центральными простыми. Как известно, центральная простая алгебра является полной матричной алгеброй над некоторым телом.

§3. Случай $(G : N) = p$

Теорема. *Если $(F : 1) = p$, то для задачи погружения выполнено условие согласности.*

Доказательство. Доказательство проведём для $N = H_1$. Рассмотрим компоненту Λe_k. Очевидно, при $k = 0$ Λe_0 изоморфна $N/N' \times K$, где N' – коммутант, он же – подгруппа, порождённая γ. Заметим, что эта алгебра соответствует полупрямой задаче, а потому для неё не просто существует модуль согласности, но даже решение исходной задачи погружения. При $k \neq 0$ рассмотрим суммы $c_k = \frac{\sum_{i=0}^{p-1} \alpha^i\zeta^{ki}}{p}$. Несложно видеть, что их образы $c_k e_l$ в любой компоненте вида Λe_l являются ортогональными идемпотентами, то есть делителями нуля. Наличие делителей нуля означает, что Λe_k является матричной алгеброй, чего, безусловно, достаточно для нашего доказательства. □

§4. Случай факторгруппы $C_p \times C_p$

Как и ранее, ограничимся случаем $N = H_1$, и пусть F – группа порядка p^2 экспоненты p.

Для любого $\sigma \in G$, как мы показали ранее, при подходящем выборе $\alpha, \beta \in N$ имеют место включения $[\alpha, \sigma] \in \langle\gamma\rangle, [\beta, \sigma] \in \langle\alpha, \gamma\rangle$, где $\gamma = [\alpha, \beta]$. При этом замена $\beta \to \beta\alpha^i$ ничего не меняет.

Лемма. *Прообразы σ, τ образующих группы F можно выбрать таким образом, чтоб выполнялись соотношения:*
(1) $\alpha^\sigma = \alpha^\tau = \alpha, \beta^\sigma = \beta, \beta^\tau = \beta\alpha$, *либо*
(2) $\alpha^\sigma = \alpha^\tau = \alpha, \beta^\sigma = \beta^\tau = \beta$.

Доказательство. Пусть σ_1, τ_1 – произвольные прообразы образующих группы F. Заменой $\sigma_1 \to \sigma_1\beta^i, \tau_1 \to \tau_1\beta^j$ можно добиться того, что новые прообразые σ_2, τ_2 коммутируют с α. Далее, при замене $\sigma_2 \to \sigma_2\tau_2^k$(либо $\tau_2 \to \tau_2\sigma_2^k$) можно получить соотношение $\beta_3^\sigma = \beta\gamma^l$(либо $\beta_3^\tau = \beta\gamma^l$), где $\sigma_3(\tau_3)$ – новые прообразы. Замена $\sigma_3 \to \sigma_4 = \sigma_3\alpha^l$ приводит к равенству $\beta_4^\sigma = \beta$. Если теперь $\beta_3^\tau = \beta\alpha^i\gamma^j$, то при i не делящемся на p положим $\alpha_1 = \alpha^i\gamma^j$, а при делящемся положим $\tau_4 = \tau_3\alpha^{-j}$. Полученные прообразы удовлетворяют нашим условиям. □

Теорема. *Если $F = C_p \times C_p$, то для нашей задачи погружения условие согласности выполнено.*

Доказательство. Пусть $\Lambda = G \times K$ – скрещенное произведение, $e_t = \frac{\sum_{i=0}^{p-1} \gamma^i\zeta^{ti}}{p}$ – центральные идемпотенты. Алгебра Λe_0 распадается(как алгебра, отвечающая факторизации по коммутанту ядра). Рассмотрим простую центральную подалгебру Λe_1, для остальных компонент рассмотрение аналогично (единицу этой алгебры e_1 в дальнейшем будем опускать). Алгебра Λe_1 содержит простую подалгебру, порожденную полем k и элементами α, β. Эта алгебра является матричной, поскольку $(\alpha e_1)^p = \beta e_1)^p = e_1$. Тем самым, $\Lambda e_1 = k(\alpha, \beta) \otimes D$, где D – централизатор нашей подалгебры. D порождён полем K, элементом σ, который коммутирует с α и β, и элементом $\tau_1 = \frac{\sum_{l=0}^{p-1} \beta^{-l}\tau\beta^l}{d}$, где $d \in k^*$, значение которого мы определим позже. Если F редуцирует на ядре внутренние автоморфизмы, достаточно положить $\tau_1 = \tau$.

Тогда

$$\sum_{l=0}^{p-1}\beta^{-l}\tau\beta^{l}=\tau\sum_{l=0}^{p-1}(\tau^{-1}\beta^{-l}\tau)\beta^{l}=\tau\sum_{l=0}^{p-1}(\beta\alpha)^{-l}\beta^{l}$$
$$=\tau\sum_{l=0}^{p-1}\alpha^{-l}\beta^{-l}\gamma^{\frac{-l(l-1)}{2}}\beta^{l}=\tau\sum_{l=0}^{p-1}\alpha^{-l}\zeta^{\frac{l(l-1)}{2}}$$

(так как $\gamma e_1=\zeta^{-1}e_1$).

Рассмотрим сумму $s=\sum\limits_{l=0}^{p-1}\alpha^{-l}\zeta^{\frac{l(l-1)}{2}}\in k(\alpha)$. Кольцо $k(\alpha)$ коммутативно и раскладывается в прямую сумму полей с ортогональными идемпотентами $\epsilon_t=\sum\limits_{l=0}^{p-1}\alpha^{-j}\zeta^{jt}$, причём $\alpha\epsilon_t=\zeta^t\epsilon_t$. Имеем теперь

$$s=\sum_{k=0}^{p-1}s\epsilon_t=\sum_{k=0}^{p-1}\sum_{l=0}^{p-1}\alpha^{-l}\zeta^{\frac{l(l-1)}{2}}\epsilon_t\sum_{k=0}^{p-1}\sum_{l=0}^{p-1}\zeta^{-lt}\zeta^{\frac{l(l-1)}{2}}\epsilon_t$$
$$=\sum_{t=0}^{p-1}\zeta^{\frac{-(t+\frac{1}{2})^2}{2}}\sum_{l=0}^{p-1}\zeta^{\frac{(l-(t+\frac{1}{2}))^2}{2}}\epsilon_t$$

(показатели, разумеется, берутся по $\bmod p$). Внутренняя сумма – это хорошо известная сумма Гаусса, она не зависит от t. Обозначим её d. Имеем теперь $s=d\sum\limits_{t=0}^{p-1}\zeta^{\Gamma_t}\epsilon_t$, где $\Gamma_t=\frac{-(t+\frac{1}{2})^2}{2}$. Взяв $\tau_1=\frac{\tau s}{d}$, получаем $\tau_1=\tau\sum\limits_{t=0}^{p-1}\zeta^{\Gamma_t}\epsilon_k$, откуда $\tau_1^p=\tau^p$ в силу ортогональности ϵ_t.

Очевидно, достаточно найти элемент, равный в степени p единице, поскольку тогда есть делители нуля. Заметим, что $\sigma^p=\gamma^{r_1}$ и $\tau_1^p=\gamma^{r_2}$. Если хотя бы одно из чисел r_1 и r_2 равно 0, искомый элемент – это σ или τ соответственно. Обозначим $f=[\sigma,\tau_1]$. Очевидно, f коммутирует с α и лежит в N, а потому имеет порядок 1 или p. Возьмём произвольные a и b. Рассмотрим элемент $x=\sigma^a\tau_1^b$. Тогда $x^p=\gamma^{ar_1+br_2}f^{\frac{abp(p-1)}{2}}=\gamma^{ar_1+br_2}$. Осталось подобрать a и b таким образом, чтобы $ar_1+br_2=0$. Теорема доказана. □

§5. Пример отсутствия согласности

В этом параграфе строится пример, когда условие согласности нарушается.

Определение. *Пусть k – поле, содержащее первообразный корень ζ степени n из единицы, и заданы элементы $a, b \in k^*$. Символом $k[a, b]$ будем обозначать ассоциативную центральную алгебру размерности n^2 над k с базисом $c^i d^j$ $(i, j = 0, 1, \ldots, n-1)$, где c и d удовлетворяют соотношениям $c^n = a$,$d^n = b$,$c^{-1}dc = d\zeta$. Такая алгебра называется алгеброй обобщённых кватернионов.*

Согласно теореме Хассе, алгебра $k[a, b]$ вполне распадается в том и только в том случае, когда b является нормой элемента из $k(\sqrt[p]{a})$.

Рассмотрим теперь следующую задачу погружения.

Пусть F – расширение ядра H_1 посредством $C_p \times C_p \times C_p$. Именно, пусть σ, τ, ω – представители образующих группы F, удовлетворяющие соотношениям $\alpha^\sigma = \alpha^\tau = \alpha^\omega = \alpha$, $\beta^\sigma = \beta^\tau = \beta^\omega = \beta$,$\sigma^p = \gamma$, $\tau^p = \omega^p = 1$, $[\tau, \omega] = \gamma$, $[\tau, \sigma] = [\omega, \sigma] = 1$. (Таким образом, F индуцирует на ядре внутренние автоморфизмы, что существенно упрощает дальнейшие вычисления.)

В качестве поля k рассмотрим $Q(\zeta, x, y)$, где ζ – первообразный корень степени p из 1, а x и y трансцендентны над Q. Пусть $b \in Q^*$ и не является p-й степенью в $Q(\zeta)$. В качестве поля K рассмотрим $k(\sqrt{x}, \sqrt{y}, \sqrt{b})$ и зададим на K действие элементов из F:

$\sqrt[p]{x}^{\psi(\sigma)} = \sqrt[p]{x}\zeta, \sqrt[p]{b}^{\psi(\tau)} = \sqrt[p]{b}\zeta$ и $\sqrt[p]{y}^{\psi(\omega)} = \sqrt[p]{y}\zeta$, а остальные действия на образующих тривиальны.

Основной целью нашей работы является следующая теорема.

Теорема. *Для построенной задачи погружения условие согласности не выполнено.*

Доказательство. Мы будем рассматривать подалгебры Λe_t. При $t = 0$ получается скрещенное произведение, соответствующее полупрямой задаче, а потому оно является матричной алгеброй нужного порядка. Далее, при $t \neq 0$ мы начнём рассмотрение с подалгебры $k(\alpha, \beta)$. Очевидно, это матричная алгебра, поскольку в ней есть делители нуля, а, исходя из её размерности, это алгебра матриц порядка p над k. Значит, это единичный элемент в группе Брауэра и вопрос сводится к исследованию централизатора, является ли он матричной алгеброй порядка p^2. Централизатор имеет над k размерность p^6. В свою очередь, в этом централизаторе есть матричная подалгебра $k(\tau, \sqrt[p]{b})$, снова единичная в группе Брауэра. Её централизатор $\Lambda_2 = k(\sigma, \sqrt[p]{x}, \sqrt[p]{y}, \omega\sqrt[p]{b}^{-1})$. Осталось показать, что это тело. Заметим, что эта алгебра является тензорным произведением двух кватернионных алгебр: $k[\zeta, x]$ и

$k[y, b^{-1}]$. Докажем, что оба сомножителя суть алгебры с делением. Проверка получается одинаковая, по критерию Хассе, приведём её для первой алгебры: пусть некоторый элемент из $k(\sqrt[p]{\zeta})$ имеет норму x. Рассмотрим его как дробно-рациональную функцию от x с коэффициентами из $Q(\sqrt[p]{\zeta}, y)$. Пусть это $f(x)$. Тогда

$$N(f(x)) = f(x)f(x)^{\sigma} \dots f(x)^{\sigma^{-1}}.$$

Все эти дробно-рациональные функции имеют одинаковую степень, а потому их произведение имеет степень, кратную p как функция от x, то есть не равно x.

Осталось показать, что тензорное произведениет тел $k[\zeta, x]$ и $k[y, b]$ также является телом, то есть не имеет делителей нуля.

Подобные алгебры рассматривались в работе [3] как примеры тел, что натолкнуло авторов на мысль о том, что и данная алгебра – тело.

Для доказательства мы можем воспользоваться теоремой на странице 467 книги [7]:

Теорема. *Пусть D – алгебра с делением над полем F, пусть K/F – циклическое расширение степени n с образующей группы Галуа τ. Если D^K – алгебра с делением (здесь используется обозначение $D^K := D \otimes_F K$), то $A = D^{F(x)} \otimes_{F(x)} (K(x), \tau, x)$ – алгебра с делением над $F(x)$. (Здесь $(K(x), \tau, x)$ – обычное скрещенное произведение, т.е. алгебра, полученная присоединением элемента u_τ к $K(x)$ так, что u_τ коммутирует с K и $u_\tau x^\tau = x u_\tau$, где τ – образующая группы Галуа $K(x)/K$).*

В качестве поля F рассмотрим $F = Q(\zeta, y)$, в качестве K – $F(\sigma)$. Пусть $D = F[y, b]$. Несложно видеть, что в этой ситуации $D^{F(x)} = k[y, b^{-1}]$, а $(K(x), \tau, x) = k[\zeta, x]$. Для применения теоремы осталось показать, что D^F – алгебра с делением.

Лемма. *В обозначениях предыдущего абзаца D^K – алгебра с делением.*

Доказательство. Покажем для этого, что K не вкладывается в D (тогда K– не поле разложения, следовательно, исходя из размерности D над F, D^K – алгебра с делением). Пусть $y_1 = \sqrt[p]{y}$, $b_1 = \sqrt[p]{b^{-1}}$. Ясно, что K не вкладывается в $F(b_1)$, поскольку одно расширение имеет циклическую группу Галуа над F, а другое – нет. Осталось показать, что, если K вкладывается в D, то вкладывается и в $F(b_1)$.

Предположим, что это не так. Рассмотрим σ. Если K не вкладывается в $F(b_1)$, то образ σ в D содержит в своей записи y_1. Рассмотрим образ σ в D как дробно-рациональную функцию от y_1 с коэффициентами из $Q(\zeta, b_1)$, акцентируем внимание на старшей степени. Пусть $\sigma = \frac{ay_1^n+\dots}{by_1^m+\dots}$. Поскольку при возведении в степень p слева и справа получается ζ, то $n = m$. Помимо этого, из формального приравнивания получается, что $(\frac{ay_1^n}{by_1^n})^p = \zeta$. Но $\frac{ay_1^n}{by_1^n} \in Q(\zeta, b_1)$, чего, как уже доказано, быть не может. Таким образом, доказано, что K не содержится в D в качестве подполя. $\square$

Итак, мы можем воспользоваться результатом книги [7].

Замечание. *Построенный пример отнюдь не является минимальным. Можно понизить степень трансцендентности поля k, т.е. рассматривать в качестве поля k поле рациональных функций от одной переменной над полем алгебраических чисел. Но при этом существенно возрастёт объём вычислений и возникают серьёзные технические трудности, которые приходится преодолевать.*

Мы завершили доказательство, ибо компоненты Λe_t алгебры $G \times K$ при $t \neq 0$ не являются матричными алгебрами размерности p^3, а потому $G \times K$ не является матричной алгеброй порядка p^3 над своей подалгеброй.

Таким образом, редукция условия согласности к сопутствующей абелевой задаче в общем случае не имеет места при любом p. $\square$

Литература

1. Б. Н. Делоне, Д. К. Фаддеев, *Исследование по геометрии теории Галуа.* — Мат. сборник **15**, No. 2 (1944), 243–284.
2. В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа*, Наука, 1990.
3. А. В. Прокопчук, С. В. Тихонов, В. И. Янчевский, *Об общих элементах в группах SK_1 для центральных простых алгебр*, Институт математики НАНБ. Вести НАНБ, серия физ.-мат. No. 3 (2008), 35–41.
4. Б. Б. Лурье, *Об условии погружаемости, когда ядро есть неабелева p-группа.* — Мат. заметки **2**, No. 3 (1967), 233–238.
5. Б. Б. Лурье, *Об условии согласности в проблеме погружения.* — Зап. научн. семин. ЛОМИ **71** (1977), 155–162.
6. Б. Б. Лурье, *Условие согласности Фаддеева–Хассе.* — Зап. научн. семин. ПОМИ **272** (2000), 259–273.

7. Р. Пирс, *Ассоциативные алгебры*, Мир, 1986.

Bondarenko M. A., Lur'e B. B. Compatibility condition. The possibility of reduction to commutative situation.

There is an example of the nocompatibility in this paper for the odd case. Kernel and factor-group are p-groups. Besides there are some notes about lower examples for p-groups.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
наб. р. Фонтанки, д. 27,
191023 С.-Петербург, Россия
E-mail: bondarenko.mikh@yandex.ru
E-mail: lurje@pdmi.ras.ru

Поступило 22 декабря 2015 г.