В. В. Ишханов, Б. Б. Лурье, Универсально разрешимые задачи погружения с циклическим ядром,
Зап. научн. сем. ПОМИ, 1999, том 265, 189–197

Записки научных
семинаров ПОМИ
Том 265, 1999 г.

В. В. Ишханов, Б. Б. Лурье

УНИВЕРСАЛЬНО РАЗРЕШИМЫЕ ЗАДАЧИ ПОГРУЖЕНИЯ С ЦИКЛИЧЕСКИМ ЯДРОМ

Пусть $1 \to A \to G \xrightarrow{\varphi} F \to 1$ – точная последовательность конечных групп. Говорят, что она определяет универсально разрешимую задачу погружения, если задачи погружения, связанные с этой последовательностью, разрешимы для любой пары полей K/k, где K – расширение Галуа поля k с группой Галуа F. Понятие универсально разрешимых задач погружения введено в [1]. Разрешимость задачи погружения понимается в широком смысле, т.е. решение может быть алгеброй Галуа. Соответственно, и сама задача погружения может ставиться не обязательно над полем, но и над алгеброй Галуа K над k ([2]).

Как показано в [1], класс универсально разрешимых расширений шире класса полупрямых расширений. Именно, для любой группы F, имеющей порядок больше 2, существует расширение с факторгруппой F, являющееся универсально разрешимым, но не полупрямым. Это наблюдение дало возможность Ж.-П. Серру ввести понятие "ничтожных" когомологий [3].

В [1] показано также, что для ядра A, имеющего порядок p, класс универсально разрешимых и класс полупрямых расширений совпадают. Более того, эти классы совпадают, даже если K/k – расширение локальных полей нулевой характеристики.

Докажем вспомогательное теоретико-групповое утверждение.

Лемма. *Пусть*

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

– расширение конечных p-групп нечетного порядка, A – циклическая группа, а группа F не является циклической. Кроме того, пусть для любой собственной подгруппы F_1группы F найдется изоморфная ей подгруппа $\bar{F}_1$ в G и $\varphi(\bar{F}_1) = F_1$. Тогда в группе G существует нормальная подгруппа $\bar{H}$ такая, что $\bar{H} \cap A = 1$ и фактор группа $G/\bar{H}$ – расширение вида

$$1 \to A \to G/\bar{H} \to F_0 \to 1,$$

где F_0 – абелева группа с двумя образующими.

Доказательство. Пусть A имеет порядок p^n и a – образующий элемент группы A. Обозначим через F_2 подгруппу группы F, состоящую из элементов, тривиально действующих на ядро A. Если само F действует тривиально на A, то в качестве F_2 возьмем любую подгруппу индекса p. Тогда F/F_2 – циклическая группа, порядок которой делит p^{n-1}. Обозначим через σ_0 такой образующий элемент группы F/F_2, что действие σ_0 на A определяется формулой $a^{\sigma_0} = a^{1+p^i}$. В случае тривиального действия F на A в качестве образующей группы F/F_2 выберем любой нетривиальный элемент.

Пусть σ – некоторый прообраз элемента σ_0 в группе F. Так как F не является циклической группой, то в F существует такой элемент τ, который является одной из образующих группы F и, кроме того, отображается в единицу при естественном гомоморфизме $F \to F/F_2$. Дополним элементы σ, τ до системы образующих $\sigma, \tau, \tau_3, \tau_4, \ldots, \tau_d$ группы F. Рассмотрим подгруппу F_3, порожденную подгруппой Фраттини группы F и элементами $\sigma, \tau_3, \tau_4, \ldots, \tau_d$. Ясно, что F_3 – нормальный делитель в F индекса p. Обозначим через G_3 полный прообраз относительно φ группы F_3 в G. Тогда G_3 – полупрямое расширение подгруппы A с помощью F_3.

Положим $F_1 = F_2 \cap F_3$, и пусть G_1 – прообраз F_1 в G_3, тогда G_1 – прямое произведение подгруппы A и подгруппы $\bar{H}$, изоморфной F_1. Покажем, что $\bar{H}$ – искомый нормальный делитель в G. Заметим, что произвольный элемент $g \in G$ можно представить в виде $g = \bar{\sigma}^i \bar{\tau}^j h$, где $h \in G_1$, а $\bar{\sigma}$, $\bar{\tau}$ – прообразы в G элементов σ, τ соответственно. Следовательно, достаточно проверить, что для любого $\bar{h} \in \bar{H}$ выполняются условия $\bar{\sigma}^{-1}\bar{h}\bar{\sigma} \in \bar{H}$ и $\bar{\tau}^{-1}\bar{h}\bar{\tau} \in \bar{H}$. Заметим, что первое условие выполняется по построению группы G_3.

Если $\bar{\tau}^{-1}\bar{h}\bar{\tau} \notin \bar{H}$, то $\bar{\tau}^{-1}\bar{h}\bar{\tau} = \bar{h}'a'$, где $\bar{h}' \in \bar{H}$, $a' \in A$. Так как элемент $\bar{\tau}$ перестановочен с элементами подгруппы A, то расширение A с помощью F_2 не является прямым, что противоречит условию леммы.

Данная лемма обобщает предложение 1 из [1]. Докажем теперь основной результат настоящей работы.

Теорема. *Пусть универсально погружаемое расширение связано с* *точной последовательностью конечных групп*

$$1 \to A \to G \to F \to 1,$$

где A – циклическая группа нечетного порядка. Тогда групповое расширение является полупрямым.

Доказательство. Поскольку свойство универсальной разрешимости наследуется при переходе к сопутствующим задачам, достаточно считать G p-группой.

Предположим, что утверждение теоремы не верно. Рассмотрим минимальный контрпример, т.е. такую задачу, для которой всякая сопутствующая задача уже является полупрямой. Таким образом, мы рассматриваем универсально разрешимую задачу погружения, связанную с точной последовательностью p-групп

$$1 \to A \to G \to F \to 1,$$

причем G не является полупрямым расширением, но расширения, получаемые из G факторизацией по подгруппе ядра A и заменой группы F на ее собственную подгруппу, являются полупрямыми. Следовательно, мы можем считать, что значения коцикла $\bar{h} \in Z^2(F, A)$, класс которого h определяет расширение G, находятся в подгруппе A_0 группы A, состоящей из элементов периода p.

Пусть A имеет порядок p^n и a – образующий элемент группы A. Рассмотрим сначала случай, когда группа F циклична. Пусть σ – образующий элемент группы F и действие F на A определяется формулой $a^\sigma = a^{1+p^i}$. В силу минимальности контрпримера F имеет порядок p^n и расширение G – это группа с двумя образующими a, $\bar{\sigma}$ и соотношениями $a^{p^n} = 1$, $\bar{\sigma}^{p^n} = a^{p^{n-1}}$, $[a, \bar{\sigma}] = a^{p^i}$ (квадратные скобки здесь и далее означают коммутатор). Определим $\varphi : G \to F$, положив $\varphi(a) = 1$, $\varphi(\bar{\sigma}) = \sigma$.

Пусть k – локальное поле с полем вычетов, отличным от p, содержащее первообразный корень степени p^i из 1 и не содержащее первообразного корня степени p^{i+1} из 1. Группа Галуа $\bar{F}$ максимального p-расширения поля k имеет две образующие g_1, g_2 и соотношение $[g_1, g_2]g_2^{p^i} = 1$ (см. [4], гл. II, §5).

Зададим расширение K/k гомоморфизмом $\mu : \bar{F} \to F$, который определяется формулами $\mu(g_1) = \sigma$, $\mu(g_2) = \sigma^{p^{n-i}}$. Заметим, что задача погружения $(K/k, G, A)$ разрешима, если существует гомоморфизм $\nu : \bar{F} \to G$ такой, что треугольник

$$\begin{array}{ccc} \bar{F} & \xrightarrow{\nu} & G \\ & \searrow \mu & \downarrow \varphi \\ & & F \end{array}$$

коммутативен. Предположим, что ν существует, и пусть $\nu(g_1) = \bar{\sigma}a^u$, $\nu(g_2) = \bar{\sigma}^{p^{n-1}}a^v$. Тогда

$$[\nu(g_1), \nu(g_2)]\nu(g_2^{p_2^i}) = [\bar{\sigma}a^u, \bar{\sigma}^{p^{n-i}}a^v](\bar{\sigma}^{p^{n-i}}a^v)^{p^i} =$$

$$= [\bar{\sigma}, a^v][a^u, \bar{\sigma}^{p^{n-i}}]\bar{\sigma}^{p^n}a^{vp^i} = a^{-vp^i} \cdot a^{p^{n-1}}a^{vp^i} = a^{p^{n-1}} \neq 1.$$

Следовательно, гомоморфизм ν не существует и задача погружения $(K/k, G, A)$ неразрешима.

Пусть теперь группа F не является циклической, расширение G – минимальный контрпример к утверждению теоремы и $h \in H^2(F, A)$ – соответствующий расширению G класс когомологий. По лемме в группе G существует подгруппа $\bar{H}$, с помощью которой можно осуществить спуск рассматриваемой задачи (см. [2], гл. I, §13) к задаче, связанной с расширением

$$1 \to A \to G_0 \to F_0 \to 1,$$

где F_0 – абелева группа с двумя образующими.

Заметим, что элемент $h_0 \in H^2(F_0, A)$, соответствующий расширению G_0, при подъеме $H^2(F_0, A) \to H^2(F, A)$ отображается в элемент h.

В зависимости от действия группы F, а следовательно, и F_0 на ядре A возможны три различных случая:

1) элементы группы F_0 тривиально действуют на A,

2) действие группы F_0 на A определяется формулами $a^{\sigma_0} = a^{1+p}$, $a^{\tau_0} = a$,

3) действие определяется формулами

$$a^{\sigma_0} = a^{1+p^i}, \quad a^{\tau_0} = a, \quad i > 1$$

(здесь τ_0 – образ τ в группе F_0).

I. Рассмотрим первый случай. Из доказательства леммы следует, что в этом случае можно считать F_0 абелевой группой с двумя образующими σ_0, τ_0 порядка p. Пусть расширение G_0 – группа с тремя образующими $\bar\sigma_0, \bar\tau_0, a$ и соотношениями

$$a^{p^n}=1,\ \bar\sigma_0^p=a^{up^{n-1}},\ \bar\tau_0^p=a^{vp^{n-1}}, [\bar\sigma_0,\bar\tau_0]=\bar a^{wp^{n-1}},$$

$$[\bar\sigma_0,a]=1,\quad [\bar\tau_0,a]=1$$

(u, v, w – целые числа).

Заметим, что можно выбрать образующие $\bar\sigma_0'$ и $\bar\tau_0'$ так, чтобы соотношения имели вид

$$a^{p^n}=1,\ \bar\sigma'^p_0=1,\ \bar\tau'^p_0=1,\ [\bar\sigma_0',\bar\tau_0']=a^{p^{n-1}},$$

$$[\bar\sigma_0',a]=1,\quad [\bar\tau_0',a]=1.$$

Возьмем в качестве k локальное поле, являющееся расширением поля p-адических чисел достаточно высокой степени, и пусть k содержит первообразный корень ζ_n из 1 степени p^n и не содержит первообразного корня степени p^{n+1} из 1. Пусть $K_0=k(\sqrt[p]{m_1},\sqrt[p]{m_2})$, где $m_1, m_2\in k^*$. Мы пока не будем фиксировать значения элементов m_1 и m_2, предположим лишь, что поле K_0 не содержит $\sqrt[p]{\zeta_n}$. Группа F_0 является группой Галуа расширения K_0/k, если положить

$$\sqrt[p]{m_1}^{\sigma_0'-1}=\zeta_1,\qquad \sqrt[p]{m_1}^{\tau_0'-1}=1$$

$$\sqrt[p]{m_2}^{\sigma_0'-1}=1,\qquad \sqrt[p]{m_1}^{\tau_0'-1}=\zeta_1,$$

где $\zeta_1=\zeta_n^{p^{n-1}}$.

Покажем теперь, что элементы m_1, m_2 можно выбрать так, что расширение K_0/k погружается в расширение K/k с группой Галуа F, но задача погружения $(K_0/k, G_0, A)$ является неразрешимой.

Рассмотрим условие разрешимости для задачи $(K_0/k, G_0, A)$. Так как задача является брауэровской, то для ее разрешимости необходимо и достаточно выполнения условия согласности Фаддеева–Хассе, которое в данном случае эквивалентно распадению скрещенного произведения $G_0\times K_0$ (см. [2], гл. II). Алгебра $G_0\times K_0$ является полупростой и определена над полем k. Ее компоненты соответствуют характерам группы A. Так как h принимает значения в подгруппе элементов порядка p, то достаточно рассмотреть характер χ такой, что $\chi(a)=\zeta_n$.

Пусть $e_\chi = \sum_{i=0}^{p^n-1}\chi(a^{-i})a^i$ – идемпотент алгебры $G_0 \times K_0$. Тогда компонента $(G_0 \times K_0)e_\chi$ – прямое произведение алгебр, порождаемых коммутирующими парами элементов $(\sigma_0', \sqrt[p]{m_1})$ и $(\tau_0' \sqrt[p]{m_1}, \sqrt[p]{m_2})$, т.е. $(G_0 \times K_0)e_\chi$ является произведением алгебр обобщенных кватернионов $[1, m_1]\cdot[m_1, m_2]_k$, которое эквивалентно алгебре $[m_1, m_2]_k$. Поскольку k – локальное поле, то распадение алгебры $[m_1, m_2]$ над полем k эквивалентно равенству единице символа Гильберта p-ой степени (m_1, m_2).

Условие погружения поля K_0 в поле K в случае, когда поле k имеет достаточно высокую степень над полем p-адических чисел, состоит в выполнении условия согласности (см. [2], гл. IV, §2). Условие согласности эквивалентно разрешимости всех сопутствующих брауэровских задач, период ядра которых делит p^n.

Пусть $(K_0/k, F_\chi, B)$ – одна из таких задач, где F_χ порождена элементами $\widetilde{\sigma}$, $\widetilde{\tau}$, b и соотношениями $b^{p^i} = 1$, $\widetilde{\sigma}^p = b^u$, $\widetilde{\tau}^p = b^v$, $[\widetilde{\sigma}, \widetilde{\tau}] = b^{wp^{i-1}}$, $[b, \widetilde{\sigma}] = 1$, $[b, \widetilde{\tau}] = 1$. Заметим, что по выбору K_0 показатель $i \leqslant n$. Гомоморфизм $\Psi : F_\chi \to F_0$ задается формулами $\Psi(b) = 1$, $\Psi(\widetilde{\sigma}) = \sigma_0$, $\Psi(\widetilde{\tau}) = \tau_0$. Заметим, что если $i < n$, то $w = 0$. Действительно, если $i < n$ и $w \neq 0$, то подъем

$$H^2(F_0, A) \to H^2(F_\chi, A)$$

аннулирует элемент h_0, следовательно, элемент h в этом случае нулевой (группа F_χ является гомоморфным образом группы F).

Если $i = n$, то F_χ является расширением вида

$$1 \to B \to F_\chi \to F_0 \to 1,$$

где B – циклическая группа порядка p^n с образующей b и F_0 действует на B тривиально. Любое расширение рассматриваемого вида соответствует элементу из группы $H^2(F_0, B)$, которая является элементарной абелевой группой с тремя образующими c_1, c_2, c_3. Образующей c_1 соответствует расширение, порождаемое элементами $\bar{\sigma}_1$, $\bar{\tau}_1$ с помощью соотношений $\bar{\sigma}_1^p = b$, $\bar{\tau}_1^p = 1$, $[\bar{\sigma}_1, \bar{\tau}_1] = 1$. Образующей c_2 соответствует расширение с образующими $\bar{\sigma}_2$, $\bar{\tau}_2$ и соотношениями $\bar{\sigma}_2^p = 1$, $\bar{\tau}_2^p = b$, $[\bar{\sigma}_2, \bar{\tau}_2] = 1$. И наконец, образующей c_3 соответствует расширение с образующими $\bar{\sigma}_3$, $\bar{\tau}_3$ и соотношениями $\bar{\sigma}_3^p = 1$, $\bar{\tau}_3^p = 1$, $[\bar{\sigma}_3, \bar{\tau}_3] = b^{p^{n-1}}$.

Заметим, что элемент h_0 не распадается в $H^2(F_\chi, A)$, если все рассматриваемые брауэровские задачи порождают в $H^2(F_0, B)$

подгруппу, не содержащую элемент c_3. Таким образом, классы когомологий, соответствующие группам F_χ всех рассматриваемых брауэровских задач, должны находиться в одной из максимальных подгрупп группы $H^2(F_0, B)$, не содержащих элемент c_3.

Заменяя в случае необходимости образующие группы F_0, можно показать, что все рассматриваемые группы F_χ являются гомоморфным образом группы с двумя образующими $\widetilde{\sigma}$, $\widetilde{\tau}$ и соотношениями либо $\widetilde{\sigma}^{p^{n+1}} = 1$, $[\widetilde{\sigma}, \widetilde{\tau}]\widetilde{\tau}^{p^n} = 1$, либо $\widetilde{\sigma}^{p^{n+1}} = 1$, $\widetilde{\tau}^{p^{n+1}} = 1$.

Условиями погружения поля K_0 в расширение с одной из указанных групп является в первом случае

$$\begin{cases} (m_1, \zeta_n) = 1 \\ (\zeta_n m_1, m_2) = 1 \end{cases}$$

и

$$\begin{cases} (m_1, \zeta_n) = 1, \\ (m_2, \zeta_n) = 1 \end{cases}$$

– во втором. Напомним, что для неразрешимости задачи $(K_0/k, G_0, A)$ необходимо и достаточно условия $(m_1, m_2) \neq 1$. Ясно, что в локальном поле k числа m_1, m_2 с нужными свойствами выбрать можно. Таким образом, мы показали, что в рассматриваемом случае задача погружения не является универсально разрешимой, т.е., предположение о нетривиальности группового расширения в минимальном контрпримере оказалось неверным.

II. Рассмотрим теперь второй случай, т.е. когда $a^{\sigma_0} = a^{1+p}$, $a^{\tau_0} = a$. По-прежнему, будем считать, что k – локальное поле достаточно высокой степени над полем p-адических чисел. Кроме того, поле k содержит первообразный корень степени p из 1 и не содержит первообразного корня степени p^2 из 1. Пусть ζ_n – первообразный корень степени p^n из 1 и $\zeta_1 = \zeta_n^{p^{n-1}}$. Положим $K_0 = k(\zeta_n, \sqrt[p]{m})$, где $m \in k^*$. Расширение K_0/k имеет группу F_0 в качестве группы Галуа, причем

$$\zeta_n^{\sigma_0} = \zeta_n^{1+p}, \quad \zeta_n^{\tau_0} = \zeta_n$$
$$\sqrt[p]{m}^{\sigma_0} = \sqrt[p]{m}, \quad \sqrt[p]{m}^{\tau_0} = \sqrt[p]{m}\,\zeta_1.$$

Заметим, что группа $H^2(F_0, A)$ имеет порядок p. Групповые расширения G_0, соответствующие нетривиальным элементам, имеют три образующие $a, \bar{\sigma}_0, \bar{\tau}_0$ и соотношения $a^{p^n} = 1$, $\bar{\sigma}_0^{p^{n-2}} = 1$, $\bar{\tau}_0^p = 1$, $[\bar{\sigma}_0, \bar{\tau}_0] = a^{vp^{n-1}}$, $[\bar{\sigma}_0, a] = a^{-p}$, $[\bar{\tau}_0, a] = 1$, где $v \equiv 0 \pmod p$.

Выберем элемент $m \in k^*$, определяющий расширение K_0/k так, чтобы K_0/k погружалось бы в расширение K/k с группой Галуа F и, кроме того, задача погружения $(K_0/k, G_0, A)$ была бы неразрешимой.

Заметим, что для разрешимости задачи погружения $(K_0/k, G_0, A)$ необходимо и достаточно равенства единице символа Гильберта (ζ_n, m).

Рассмотрим теперь условие погружения поля K_0 в поле K с группой Галуа F. Как было замечено выше, такое погружение возможно, если разрешимы все сопутствующие брауэровские задачи погружения, причем порядок ядра p^i таких задач делит p^n.

Если $i = n$, то все сопутствующие брауэровские задачи погружения будут тривиальными. При $1 < i < n$ достаточно рассмотреть задачи, у которых группа F_χ имеет три образующие $\widetilde{\sigma}$, $\widetilde{\tau}$, b и соотношения $\widetilde{\sigma}^{p^{n-1}} = b^{p^{i-1}}$, $\widetilde{\tau}^p = 1$, $[\widetilde{\sigma}, \widetilde{\tau}] = 1$, $[b, \widetilde{\sigma}] = b^p$, $[b, \widetilde{\tau}] = 1$. Ясно, что задача погружения $(K_0/k, F_\chi, B)$ разрешима, так как она является подъемом задачи $(k(\zeta_n)/k, \widetilde{F}, B)$, где $\widetilde{F}$ – группа с образующими $b, \widetilde{\sigma}$ и соотношениями $b^{p^i} = 1$, $\widetilde{\sigma}^{p^{n-1}} = b^{p^{i-1}}$, $[b, \widetilde{\sigma}] = b^p$.

При $i = 1$, рассуждая также, как и в предыдущем случае при $i = n$, можно показать, что все рассматриваемые брауэровские задачи будут разрешимы, если поле K_0 погружается в расширение с группой $\widetilde{F}$, порожденной элементами $\widetilde{\sigma}$, $\widetilde{\tau}$ с помощью соотношений $\widetilde{\sigma}^{p^n} = 1$, $[\widetilde{\sigma}, \widetilde{\tau}]\widetilde{\tau}^p = 1$. При этом гомоморфизм $\widetilde{\Psi} : \widetilde{F} \to F_0$ задается формулами $\widetilde{\Psi}(\widetilde{\sigma}) = \sigma_0$, $\widetilde{\Psi}(\widetilde{\tau}) = \tau_0$. Заметим, что задача погружения $(K_0/k, \widetilde{F}, \widetilde{\Psi})$ разрешима при любом выборе элемента m. Таким образом, при любом выборе m расширение K_0/k погружается в расширение K/k с группой Галуа F. Нам остается выбрать m так, чтобы символ (m, ζ_1) был бы отличен от единицы, при этом задача погружения $(K/k, G, A)$ является неразрешимой. Следовательно, и в этом случае предположение о нетривиальности группового расширения в минимальном контрпримере оказалось неверным.

III. Третий случай рассматривается аналогично. Теорема доказана.

Следствие. *Пусть* $1 \to A \to G \xrightarrow{\varphi} F \to 1$ *и* $1 \to B \to H \xrightarrow{\Psi} F \to 1$ – *два расширения конечных групп, причем* A – *циклическая группа нечетного порядка. Если для любого расширения локальных полей* K/k

с группой Галуа F разрешимость задачи погружения $(K/k, G, \varphi)$ следует из разрешимости задачи погружения $(K/k, H, \Psi)$, то существует гомоморфизм $\mu : H \to G$, для которого треугольник

$$
\begin{array}{ccc}
H & \xrightarrow{\mu} & G \\
& \Psi \searrow \quad \swarrow \varphi & \\
& F &
\end{array}
$$

коммутативен. В частности, если обе задачи эквивалентны для любого расширения локальных полей K/k, то эквивалентны и групповые расширения.

Доказательство. Рассмотрим групповое расширение $1 \to A \to G * H \to H \to 1$, где $G * H$ – произведение групп G и H с отождествленной факторгруппой F. Для всякого расширения L/k с группой Галуа H разрешима задача погружения $(K/k, H, \Psi)$, а значит, и $(K/k, G, \varphi)$. Тем самым, указанное расширение является универсальным. По доказанной теореме оно полупрямое, т.е. существует дополнение H в $G * H$, а это и означает существование искомого гомоморфизма μ.

Данное следствие показывает, что в наших условиях набор препятствий в задаче погружения определяет групповое расширение.

Литература

1. Б. Б. Лурье, *Об универсально разрешимых задачах погружения.* Труды МИАН, **CLXXXIII(183)** (1990), 121–126.
2. В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа.* М., Наука, 1990, 270 сс.
3. J.-P. Serre, *Cohomologie négligeable.* Algèbre et géométrie. Résumé des Cours et Travaux. Paris, College de France, 1993-94.
4. Ж.-П. Серр, *Когомологии Галуа.* М. Мир, 1968, 208 сс.

Ishkhanov V. V. and Lur'e B. B. The universally solvable embedding problem with cyclic kernel.

It is proved that the universally solvable embedding problem with cyclic kernel of odd order is semidirect.

Санкт-Петербургское отделение
Математического института
им. В. А. Стеклова РАН

Поступило 20 декабря 1999 г.