Записки научных
семинаров ПОМИ
Том 305, 2003 г.

В. В. Ишханов, Б. Б. Лурье

ОБ ОДНОЙ ЗАДАЧЕ ПОГРУЖЕНИЯ С ЦИКЛИЧЕСКИМ ЯДРОМ

Интерес к довольно частной задаче, ставшей предметом нашего исследования, инициирован работой [1]. Там показано, что разрешимость в радикалах неприводимого уравнения простой степени p влечет разрешимость задачи погружения квадратичного расширения основного поля в расширение с циклической 2-группой Галуа, именно, степень искомого расширения является максимальной степенью двойки, делящей $p-1$.

Задача погружения с ядром, являющимся циклической 2-группой, исследовалась неоднократно (см. [2–5]). Как известно, условие согласности Фаддеева–Хассе для такой задачи не гарантирует погружаемости, если порядок ядра больше 4. Найдены и дополнительные условия погружения. В этой работе мы рассмотрим задачу погружения с циклической 2-группой для числовых полей и найдем условие погружения в терминах норменных отображений. Далее, в качестве следствия, рассмотрим подобную задачу над полем рациональных чисел Q.

§1. Редукция исходной задачи погружения

Пусть k – поле алгебраических чисел, причем $\sqrt{-1} \notin k$, $\sqrt{2} \notin k$, $\sqrt{-2} \notin k$, $K = k(\sqrt{m})$ – квадратичное расширение поля k с группой Галуа F и

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

расширение циклических 2-групп, где G – циклическая группа порядка 2^n. Возникает задача погружения $(K/k, G, \varphi)$, состоящая в построении расширения L с группой автоморфизмов G над полем k, причем $K \subset L$ и ограничение автоморфизма $g \in G$ на поле

Работа выполнена при поддержке фонда РФФИ, грант 03-01-00633а, 03-01-00349 и Программы 2003 г. фундаментальных исследований Президиума РАН "Исследования в фундаментальных областях современной математики".

K совпадает с $\varphi(g)$. Если $n \leqslant 3$, то ядро задачи погружения меньше или равно 4 и в этом случае задача погружения разрешима, если выполнено условие согласности. Поэтому в дальнейшем будем считать, что $n > 3$.

Пусть G_1 – циклическая группа порядка 16 и

$1 \to A_1 \to G_1 \xrightarrow{\varphi_1} F \to 1$ – групповое расширение, полученное факторизацией ядра A по подгруппе порядка 2^{n-4}. Тогда мы имеем сопутствующую задачу погружения

$$(K/k, G_1, \varphi_1). \tag{2}$$

Теорема 1. *Если выполнено условие согласности для задачи* (1), *то разрешимость задачи* (2) *влечет разрешимость задачи* (1).

Доказательство. Пусть $\bar{k}$ – максимальное алгебраическое расширение поля k с группой Галуа $\overline{F}$, f и f_1 – классы когомологий из группы $H^2(F, A)$ и $H^2(F, A_1)$, соответствующие расширениям G и G_1.

Пусть λ – гомоморфизм подъема $H^2(F, A) \to H^2(\overline{F}, A)$ и λ_1 – гомоморфизм подъема $H^2(F, A_1) \to H^2(\overline{F}, A_1)$. Рассмотрим коммутативную диаграмму

$$\begin{array}{ccc}
H^2(\overline{F}, A) & \xrightarrow{\beta} & H^2(\overline{F}, A_1) \\
\downarrow{\scriptstyle\alpha} & & \downarrow{\scriptstyle\alpha_1} \\
\sum\limits_{\mathfrak{p}} H^2(\overline{F}_{\mathfrak{p}}, A) & \xrightarrow{\delta} & \sum\limits_{\mathfrak{p}} H^2(\overline{F}_{\mathfrak{p}}, A_1),
\end{array}$$

где $\mathfrak{p}$ – простой дивизор поля k, $\overline{F}_{\mathfrak{p}}$ – группа Галуа максимального алгебраического расширения пополнения $k_{\mathfrak{p}}$ поля k в точке $\mathfrak{p}$. Гомоморфизмы β и δ индуцированы гомоморфизмом $A \to A_1$.

Разрешимость задачи (1) означает, что $\lambda f = 0$, а разрешимость задачи (2), что $\lambda_1 f_1 = 0$. Выполнение условия согласности для задачи (1) означает, что $\alpha\lambda f = 0$. Таким образом, нам достаточно показать, что гомоморфизм β индуцирует мономорфизм $\operatorname{Ker}\alpha \to \operatorname{Ker}\alpha_1$.

Пусть $\bar{k}^*$ – мультипликативная группа поля $\bar{k}$, $\hat{A} = \operatorname{Hom}(A, \bar{k}^*)$ и $\hat{A}_1 = \operatorname{Hom}(A_1, \bar{k}^*)$. Согласно двойственности Тейта [7] ядра отображений α и α_1 двойствены ядрам отображений

$$H^1(\overline{F},\hat{A}) \to \prod_{\mathfrak{p}} H^1(\overline{F}_{\mathfrak{p}},\hat{A}) \quad \text{и} \quad H^1(\overline{F},\hat{A}_1) \to \prod_{\mathfrak{p}} H^1(\overline{F}_{\mathfrak{p}},\hat{A}_1)$$

соответственно (аналогичный результат доказан А. В. Яковлевым в [5]).

Рассмотрим коммутативную диаграмму

$$\begin{array}{ccc} H^1(\overline{F},\hat{A}) & \xrightarrow{\bar{\alpha}} & \prod_{\mathfrak{p}} H^1(\overline{F}_{\mathfrak{p}},\hat{A}) \\ \uparrow{\scriptstyle \bar{\beta}} & & \uparrow{\scriptstyle \bar{\delta}} \\ H^1(\overline{F},\hat{A}_1) & \xrightarrow{\bar{\alpha}_1} & \prod_{\mathfrak{p}} H^1(\overline{F}_{\mathfrak{p}},\hat{A}_1) \end{array}$$

Согласно двойственности Тейта нам достаточно показать, что гомоморфизм $\bar{\beta}$ инъективен на ядре отображения $\bar{\alpha}_1$. Покажем это.

Пусть $x \in H^1(\overline{F},\hat{A}_1)$, $\bar{\alpha}_1 x = 0$ и $\bar{\beta}x = 0$. Обозначим через $\overline{F}_0$ подгруппу в $\overline{F}$, состоящую из элементов, действующих тривиально на $\hat{A}$ и через H обозначим фактор группу $\overline{F}/\overline{F}_0$. Ограничение x на подгруппу $H^1(\overline{F}_0,\hat{A}_1)$ тривиально, так как отображение $H^1(\overline{F}_0,\hat{A}_1) \to \prod_{\mathfrak{p}} H^1(\overline{F}_{0\mathfrak{p}},\hat{A}_1)$ инъективно (здесь $\overline{F}_{0\mathfrak{p}}$ – соответствующие локальные группы).

Подгруппа $\overline{F}_0$ соответствует подполю K_0, полученному из k присоединением всех корней из 1 степени 2^n. Таким образом, группа H – это абелева группа с двумя образующими τ и γ и соотношениями $\tau^{2^{n-2}} = 1$, $\gamma^2 = 1$. Если ζ_n – первообразный корень из 1 степени 2^n, то можно считать, что автоморфизмы τ и γ выбраны так, что действуют на ζ_n следующим образом:

$$\zeta_n^\tau = \zeta_n^5, \quad \zeta_n^\gamma = \zeta_n^{-1}.$$

Как было замечено, ограничение элемента x на $H^1(\overline{F}_0,\hat{A}_1)$ тривиально, следовательно, существует $x_1 \in H^1(H,\hat{A}_1)$, отображающийся в x при гомоморфизме подъема $H^1(H,\hat{A}_1) \to H^1(\overline{F},\hat{A}_1)$. Заметим, что ограничение x_1 на группу $H^1(\{\tau\},\hat{A}_1)$ тривиально, т.к. существует аналогичная локальная подгруппа. Следовательно, x_1 получается подъемом элемента из группы $H^1(H/\{\tau\},\hat{A}_1^{\{\tau\}})$. Группа $H/\{\tau\}$ – циклическая группа второго порядка, а группа

$\hat{A}_1^{\{\tau\}}$ – циклическая группа порядка 4, состоящего из характеров группы A_1 со значениями в группе корней четвертой степени из 1. Аналогичным образом устроена и группа $H^1(H/\{\tau\}, \hat{A}^{\{\tau\}})$. При выполнении условия согласности для задачи (1), и следовательно, и для задачи (2), дополнительное условие погружения для задач (1) и (2) соответствует тривиальному характеру группы $H^1(H/\{\tau\}, \mu_4)$, где μ_4 – группа корней четвертой степени из 1. Следовательно, дополнительные условия для задач (1) и (2) совпадают. Теорема доказана.

Замечание. Условие $\sqrt{-1}$, $\sqrt{2}$, $\sqrt{-2} \notin k$ не ослабляет рассматриваемую задачу. Если $\sqrt{-1} \in k$, то группа H – циклична, следовательно, условие согласности достаточно для разрешимости задачи погружения. Если $\sqrt{2} \in k$ или $\sqrt{-2} \in k$, то в этом случае нужно делать редукцию к группе более высокого порядка чем 16, но и в этом случае группа Галуа корней из 1, которые нужно присоединить к полю k, имеют порядок 4.

§2. Решение редуцированной задачи

В настоящем параграфе мы рассмотрим задачу погружения квадратичного расширения $k(\sqrt{m})$ поля k в циклическое расширение степени 16. Будем по-прежнему предполагать, что $\sqrt{-1}$, $\sqrt{2}$, $\sqrt{-2} \notin k$. Пусть $k_1 = k(\sqrt{-1})$,$k_2 = k(\sqrt{-1}, \sqrt{-2})$, и k_3 – поля, полученные из k присоединением первообразных корней из 1 соответственно четвертой, восьмой и шестнадцатой степени. Группа Галуа Γ расширения k_3/k имеет две образующие σ и τ, причем $\sigma^4 = 1$, $\tau^2 = 1$ и действие автоморфизмов σ и τ в расширении k_3/k определяется следующими формулами:

$$\zeta_{16}^{\sigma} = \zeta_{16}^{5}, \quad \zeta_{16}^{\tau} = \zeta_{16}^{-1}.$$

Заметим, что $\mu \in k_3^*$ определяет циклическую алгебру Галуа над полем k шестнадцатой степени, если $\mu^{\sigma-5} = A_1^{16}$ и $\mu^{\tau+1} = A_2^{16}$, где $A_1, A_2 \in k_3^*$. Действительно, k-алгебра $k_3(\sqrt[16]{\mu})$ имеет группу автоморфизмов $\{\alpha\} \times \Gamma$, где $\{\alpha\}$ – циклическая группа порядка 16 с образующим элементом α и действие α на $\sqrt[16]{\mu}$ задается следующим образом: $\sqrt[16]{\mu}^{\alpha-1} = \zeta_{16}$. Тогда $\sqrt[16]{\mu}^{\alpha\tau} = (\sqrt[16]{\mu}\zeta_{16})^{\tau} = \sqrt[16]{\mu^{-1}}A_2\zeta_{16}^{-1}$. С другой стороны, $\sqrt[16]{\mu}^{\tau\alpha} = (\sqrt[16]{\mu}^{-1}A_2)^{\alpha} = \sqrt[16]{\mu}^{-1}\zeta_{16}^{-1}A_2$. Аналогично проверяется, что автоморфизмы α и σ коммутируют между собой. Таким образом,

$k_3(\sqrt[16]{\mu})$ – алгебра Галуа над k с группой $\{\alpha\}\times\Gamma$. Подалгебра L, соответствующая подгруппе Γ, является алгеброй Галуа шестнадцатой степени над k. Ясно, что L является расширением поля k, если $\mu = m\mu_1^2$, $\mu_1 \in k_3$. Можно показать, что для расширений четвертой степени элемент μ выбирается в поле k_1, а для расширений восьмой степени – в поле k_2.

Теорема 2. *Пусть $(k(\sqrt{m})/k, G, \varphi)$ – задача погружения полей алгебраических чисел, где G – циклическая группа порядка 16, и пусть для рассматриваемой задачи погружения выполнено условие согласности. Если $H^3(\Gamma_2, k_2^*) = 0$, где Γ_2 – группа Галуа расширения k_2/k, то задача погружения разрешима. Если $H^3(\Gamma_2, k_2^*) \neq 0$, то для разрешимости задачи необходимо и достаточно, чтобы m было нормой в расширении k_2/k.*

Доказательство. Если $H^3(\Gamma_2, k_2^*) = 0$, то задача погружения разрешима (см. [3, 6]).

Предположим, что задача погружения разрешима и $H^3(\Gamma_2, k_2^*) \neq 0$. Для каждого простого дивизора $\mathfrak{p}$ поля k через $n_\mathfrak{p}$ обозначим число простых дивизоров поля k_2, делящих $\mathfrak{p}$. Известно, что порядок группы $H^3(\Gamma_2, k_2^*)$ – это наибольший общий делитель чисел $n_\mathfrak{p}$, следовательно, если группа $H^3(\Gamma_2, k_2^*) \neq 0$, то ее порядок равен 2. Условие согласности состоит в распадении кватернионных алгебр $[m,-1]$, $[m,2]$ и $[m,\zeta_8]$ над полями k, k_1 и k_2 соответственно. Покажем, что m является локальной нормой в расширении k_2/k. Действительно, если $\sqrt{-1} \in k_\mathfrak{p}$, то m является нормой в $k_p(\sqrt{2})/k_\mathfrak{p}$, так как распадается алгебра $[2,m]$ над полем $k(\sqrt{-1})$. Если $\sqrt{2}$ или $\sqrt{-2}$ содержится в $k_\mathfrak{p}$, то m является локальной нормой, так как алгебра $[m,-1]$ распадается над полем k.

Пусть $M_1 \in k_1^*$ и $N_{k_1/k}M_1 = m$, тогда элемент $mM_1^{-2} \in k_1^*$ задает циклическое расширение K_1 степени 4 над полем k, так как $(mM_1^{-2})^\tau = m\ M_1^{-2\tau} = m^{-1}M_1^2$.

Покажем, что поле K_1 погружается в циклическое расширение восьмой степени. Для этого покажем, что для всех простых точек $\mathfrak{p}$ поля k алгебра $K_{1\mathfrak{p}}$ погружается в циклическую алгебру Галуа степени 8. Пусть группа разложения дивизора $\mathfrak{p}$ – циклическая группа порядка 2 с образующим элементом σ, и пусть $M_{3\mathfrak{p}} \in k_{2\mathfrak{p}}^*$ со свойством $N_{k_{2\mathfrak{p}}/k_{1\mathfrak{p}}}M_{3\mathfrak{p}} = m$. Положим $\mu_\mathfrak{p} = mM_1^{-2}M_{3\mathfrak{p}}^4$. Тогда $\mu_\mathfrak{p}^{\sigma-5} = m^{-4}M_1^8M_{3\mathfrak{p}}^{4(\sigma-5)}$ – есть 8-я степень в $k_{2\mathfrak{p}}^*$. В остальных случаях в качестве $\mu_\mathfrak{p}$ можно взять mM_1^{-2}. Таким образом, расширение K_1/k погружается в циклическое расширение восьмой степени. Искомое расширение K_2 существует, так как оно является решением задачи погружения с циклическим ядром порядка 2, при этом все сопутствующие локальные задачи разрешимы. Таким образом, расширение четвертой степени, соответствующее элементу $\mu = mM_1^{-2}z^2$, где $z \in k^*$, погружается в циклическое расширение степени 8, если алгебра $[z, -1]$ распадается над полем k.

Рассмотрим задачу погружения циклического расширения, соответствующего элементу $mM_1^{-2}z^2$ в циклическое расширение степени 16. Так как ее ядро имеет порядок 4, то для ее разрешимости необходимо и достаточно выполнения условия согласности. Оно заключается в разрешимости всех сопутствующих брауэровских задач, причем в данном случае достаточно рассматривать две из них. Первая задача соответствует характеру со значениями в группе корней второй степени из единицы и является задачей погружения циклического расширения четвертой степени в циклическое расширение степени 8. Заметим, что эта задача была решена ранее и условием ее разрешимости является распадение алгебры $[z, -1]$ над полем k. Вторая задача определена над полем $k(\sqrt{-1})$. Она разрешима, если распадается алгебра $[mM_1^{-2}z^2, i]$ экспоненты 4 над полем $k(\sqrt{-1})$. Таким образом, препятствие состоит в распадении произведения трех алгебр $C_4(m, i)$, $[M_1, 2]$, $[m_2, 2]$ над полем $k(i)$, где первая алгебра – циклическая порядка 4 с инвариантами m, i, а последние две – это алгебры кватернионов.

Рассмотрим инварианты алгебры $C_4(m, i)$. Если $\mathfrak{p}$ – точка поля k и $\mathfrak{p} \nmid 2$, то алгебра $C_4(m, i)$ распадается соответствующим локальным полем, так как выполнено условие согласности. Кроме того, выполнение условия согласности влечет распадение алгебры $C_4(m, i)$ над локальным полем, если $\mathfrak{p}|2$ и $\sqrt{-1} \notin k_\mathfrak{p}$ (в этом случае $\sqrt{2} \in k_\mathfrak{p}(\sqrt{-1})$). Следовательно, остается рассмотреть случай, когда $\mathfrak{p}|2$, $\sqrt{-1} \in k_\mathfrak{p}$ и $\sqrt{2} \notin k_\mathfrak{p}$. В этом случае инвариант алгебры $C_4(m, i)$ может быть равен -1, но число таких точек должно быть четно. Тогда существует число $m_1 \in k^*$ такое, что алгебры $C_4(m, i)$ и $(m_1, 2)$ подобны (вторая алгебра есть алгебра кватернионов) над полем $k(i)$, и кроме того, алгебра $C_4(mm_1^2, i)$ распадается над полем $k(i)$ и условие погружения рассматриваемой задачи состоит в распадении алгебры кватернионов $[M_1zm_1, 2]$ над полем $k(i)$. Распадение последней алгебры означает, что M_1zm_1 является нормой в расширении $k(\sqrt{-1}, \sqrt{2})/k(\sqrt{-1})$, что эквивалентно тому, что m является нормой в расширении $k(\sqrt{-1}, \sqrt{2})/k$. Теорема доказана.

§3. Необходимое условие разрешимости в радикалах уравнения простой степени

Пусть $f(x) = 0$ – неприводимое уравнение простой степени q с коэффициентами из поля k. Если это уравнение разрешимо в радикалах, то, как показано в [1], разрешима задача погружения $(k(\sqrt{d})/k, G, \varphi)$, где d – дискриминант рассматриваемого уравнения, а G – циклическая 2-группа, порядок которой равен максимальной степени двойки 2^n, делящей $q-1$. При $q \equiv -1 \pmod 4$ задача погружения бессодержательна, так как ее ядро – единичное. Поэтому далее мы будем считать, что $q \equiv 1 \pmod 4$. Найдем условия погружения для рассматриваемой задачи в случае, когда поле k есть поле рациональных чисел Q. В этом случае условие согласности достаточно для погружения, так как группа $H^3(H, k_0^\varphi) = 0$, где k_0 – круговое расширение поля Q, полученное присоединением корней степени 2^n из 1, и H – группа Галуа расширения k_0/Q (см. [6]). Найдем условие согласности в арифметических терминах. Итак, рассматриваем задачу погружения $(Q\sqrt{d})/Q, G, \varphi)$, где d – бесквадратное целое число, а G – циклическая 2-группа порядка 2^n.

Теорема 3. *Условие согласности, и следовательно, условие погружения для задачи $(Q(\sqrt{d})/Q, G, \varphi)$ состоит в следующем*

а) *d – положительное число,*

б) *для любого нечетного простого $p|d$ имеем $p \equiv 1 \pmod{2^n}$.*

Доказательство. Условие а) очевидно, так как в случае отрицательного d расширение $Q(\sqrt{d})$ нельзя погрузить в расширение с циклической группой порядка 4 (мы считаем, что $p \equiv 1 \pmod 4$).

Рассмотрим условие б). Условие согласности равносильно погружаемости всех сопутствующих локальных задач $(Q_p(\sqrt{d})/Q_p, G, \varphi)$. Если $p|d$, $p \equiv -1 \pmod 4$, то неразрешима уже задача погружения квадратичного расширения $Q(\sqrt{d})$ в циклическое расширение степени 4 (так как в этом случае d не является суммой двух квадратов в Q_p). Поэтому мы вправе считать, что все нечетные простые делители d имеют вид $4m+1$. Соответственно, дискриминант расширения $Q(\sqrt{d})/Q$ равен d.

1. Пусть $p \nmid d$, тогда p не делит дискриминант расширения $Q(\sqrt{d})/Q$. В этом случае $Q_p(\sqrt{d})/Q_p$ является либо неразветвленным расширением степени 2, либо прямой суммой двух экземпляров Q_p. В обоих случаях $Q_p(\sqrt{d})/Q_p$ – неразветвленная алгебра Галуа и такая задача всегда разрешима (см. лемму 3.14 [7]).

2. Пусть $p=2$ и $2|d$, тогда $d=2m$, где $m>0$ и $m\equiv 1 \pmod 4$. В этом случае расширение $Q_2(\sqrt{d})$ погружается в циклическое 2-расширение любой степени.

3. Пусть p – нечетное, $p|d$ и $p\equiv 1 \pmod 4$. В этом случае условие существования циклического расширения степени 2^n равносильно тому, что поле Q_p содержит первообразные корни из 1 степени 2^n, что эквивалентно тому, что $p\equiv 1 \pmod{2^n}$. Теорема доказана.

Литература

1. Б. Б.Лурье, *Критерий неразрешимости в радикалах уравнения простой степени.* — ДАН, **388**, No. 4 (2003), 447–448.
2. Д. К. Фаддеев, *Об одной гипотезе Хассе.* — ДАН СССР, **94**, No. 6 (1954), 1013–1016.
3. Д. К. Фаддеев, Р. А. Шмидт, *Условие погружения для циклической группы восьмого порядка.* — Вестник ЛГУ, **19**, No. 4, 36–42.
4. Р. А. Шмидт, А. В. Яковлев, *Условие погружаемости в случае циклического нормального делителя порядка* 2^n. — Вестник ЛГУ, **13**, No. 3 (1963), 137–139.
5. А. В. Яковлев, *Задача погружения для числовых полей.* — Изв. АН СССР. Сер. мат. **31**, No. 2 (1967), 211–224.
6. С. П. Демушкин, И. Р. Шафаревич, *Второе препятствие для задачи погружения полей алгебраических чисел.* — Изв. АН СССР. Сер. мат., **26**, No. 6 (1962), 911–924.
7. В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа.* Наука, М. (1990), 269 с.

V. V. Ishkhanov and B. B Lur'e. Some field embedding problem with cyclic kernel.

The problem of embedding a quadratic extension of a number field into an extension with a cyclic 2-group is studied. A reduction theorem showing that, under the compatibility condition, an additional condition of embedding consists of the solvability of the problem with cyclic kernel of order 16 (of course, the degree of the desired field is no less than 16.) An

additional condition of the embedding into a field of degree 16 is found; namely, the number generating the given quadratic extension must be a norm in the cyclotomic field containing the primitive roots of unity of eight degree. For Q, the condition of embedding is easier: all odd prime divisors of the generating element must be congruent with 1 modulo the order of the extension group. In addition, the quadratic extension must be real.

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

Поступило 1 декабря 2003 г.