Записки научных
семинаров ПОМИ
Том 375, 2010 г.

А. В. Яковлев

О ЗАДАЧЕ ПОГРУЖЕНИЯ ЧИСЛОВЫХ ПОЛЕЙ В СЛУЧАЕ ЭЛЕМЕНТАРНОГО АБЕЛЕВА ЯДРА

Пусть K/k – конечное расширение Галуа с группой Галуа F, и пусть φ – эпиморфизм конечной группы G на группу F. Мы обозначаем через $(K/k, \varphi)$ следующую задачу погружения: построить поле $L \supseteq K$, которое является расширением Галуа поля k с группой Галуа G, причем ограничение любого автоморфизма $g \in G = \mathrm{Gal}\,(L/k)$ на подполе K совпадает с автоморфизмом $\varphi(g) \in F = \mathrm{Gal}\,(K/k)$.

Замечание 1. Обычно требуется существование алгебры Галуа L, решающей задачу погружения, а не обязательно поля. Однако, здесь мы рассматриваем только задачи погружения с абелевыми ядрами для числовых полей, а в этом случае, как показал Д. К. Фаддеев в [1], обе формулировки задачи погружения равносильны.

Необходимым условием существования решения задачи погружения является условие согласности, открытое Д. К. Фаддеевым [1] и переоткрытое Х. Хассе [2]. Поскольку нам не понадобится использовать явную форму этого условия, мы не будем напоминать здесь, в чем оно состоит. Напомним только, что это условие не является достаточным для разрешимости задачи погружения, даже если ядро $A = \mathrm{Ker}\,\varphi$ задачи погружения является абелевой группой.

Дополнительное условие погружаемости в случае абелева ядра было найдено в [3–5]. Здесь мы ограничимся одним следствием из этого условия, которое показывает, что в некоторых ситуациях согласность достаточна для погружаемости. Но сначала зафиксируем обозначения, которые будут действовать до конца работы:

K – *поле, содержащее первообразный корень степени* n *из* 1;
k – *такое подполе* K, *что* K/k – *конечное расширение Галуа*;
$F = \mathrm{Gal}\,(K/k)$;
$\varphi : G \to F = \mathrm{Gal}\,(K/k)$ – *групповой эпиморфизм, ядро которого* A – *конечная абелева группа экспоненты* n;

Ключевые слова: группа Галуа, числовые поля.

$\overline{A} = \mathrm{Hom}\,(A, K^*)$ – *группа характеров группы* A*, превращенная в* G*-модуль по следующему правилу*

$$\chi^g(a) = (\chi(gag^{-1}))^{\varphi(g)} \quad \text{для любых} \quad \chi \in \overline{A}, \quad g \in G, \quad a \in A;$$

$G_0 \supseteq A$ – *нормальная подгруппа группы* G*, состоящая из всех элементов группы* G*, действующих тривиально на* $\overline{A}$;

$F_0 = \varphi(G_0)$, $\overline{F} = F/F_0$, $\overline{K} = K^{F_0}$ – *подполе* K*, состоящее из всех* F_0*-инвариантных элементов.*

Ясно, что $\overline{K}/k$ – расширение Галуа с группой Галуа $\overline{F}$, и что группа $\overline{F}$ естественно отождествляется с подгруппой группы автоморфизмов $\mathrm{Aut}\,(\overline{A})$ группы $\overline{A}$, так что $\overline{A}$ может рассматриваться как $\overline{F}$-модуль. Ниже мы всегда рассматриваем $\overline{F}$ как подгруппу $\mathrm{Aut}\,(\overline{A})$.

В [5] было найдено дополнительное (при выполненной согласности) условие погружаемости для числовых полей; к сожалению, в формулировке этого условия участвовал неканонический изоморфизм. Но здесь нам не понадобится общий результат, и мы будем использовать только следующее непосредственное следствие из него.

Теорема 1. *Пусть в предыдущих обозначениях* K *– поле алгебраических чисел (т.е. конечное расширение поля рациональных чисел). Пусть* Π *– множество всех простых дивизоров поля* $\overline{K}$*, и для любого простого дивизора* $\mathfrak{P} \in \Pi$ *пусть* $\overline{F}_{\mathfrak{P}} \subset \overline{F} = \mathrm{Gal}\,(\overline{K}/k)$ *– группа разложения* $\mathfrak{P}$ *в расширении* $\overline{K}/k$*. Если для задачи погружения* $(K/k, \varphi)$ *выполнено условие согласности, и если пересечение ядер всех гомоморфизмов ограничения*

$$r_{\mathfrak{P}} : H^1(\overline{F}, \overline{A}) \to H^1(\overline{F}_{\mathfrak{P}}, \overline{A}) \quad (\mathfrak{P} \in \Pi)$$

состоит только из 0*, то эта задача погружения разрешима.*

Если группа $\overline{F}$ циклическая, то согласность достаточна для разрешимости задачи погружения для любых полей, а не только полей алгебраических чисел (см.[4]). Грубо говоря, согласность достаточна для погружаемости, если $\overline{F}$ – небольшая подгруппа группы $\mathrm{Aut}\,(\overline{A})$. Однако, в случае числовых полей согласность иногда оказывается достаточной для погружаемости и для очень больших групп $\overline{F}$.

В настоящей работе мы рассматриваем задачу погружения для числовых полей в случае, когда ядром задачи является элементарная абелева группа. Прежде, чем сформулировать основной результат, дадим одно определение. Пусть p – простое число. Всякая элементарная абелева p-группа B является векторным пространством над полем из p-элементов $\mathbb{F}_p$. Автоморфизм ε группы B будем называть элементарным автоморфизмом по отношению к базису $b_1, \ldots, b_n$ этой группы, если существуют такие индексы $1 \leqslant i < j \leqslant n$, что действие ε на базисных элементах задается формулами

$$\varepsilon(b_i) = b_i + b_j, \quad \varepsilon(b_q) = b_q \quad \text{при} \quad q \neq i.$$

Теорема 2. *Пусть K/k – расширение Галуа с группой Галуа F, и пусть $\varphi : G \to F$ – эпиморфизм, ядро которого A – конечная элементарная абелева p-группа, где p – некоторое простое число. Если K – поле алгебраических чисел, содержащее первообразный корень степени p из 1, а в группе $\overline{A}$ есть такой базис, что силовская p-подгруппа группы $\overline{F}$ порождается элементарными по отношению к этому базису автоморфизмами группы $\overline{A}$, то согласность достаточна для разрешимости задачи погружения $(K/k, \varphi)$.*

Доказательство. Пусть $G_p \supseteq A$ – силовская p-подгруппа группы G, $F_p = \varphi(G_p)$, $k_p = K^{F_p}$ – подполе K, состоящее из всех F_p-инвариантных элементов, $\varphi_p : G_p \to F_p = \mathrm{Gal}\,(K/k_p)$ – индуцированный φ эпиморфизм. По теореме Кохендорфера – Фаддеева разрешимость задачи погружения $(K/k_p, \varphi_p)$ влечет разрешимость задачи $(K/k, \varphi)$. Поэтому достаточно доказать теорему в предположении, что G является p-группой; тогда p-группой будет и группа $\overline{F}$.

Согласно теореме 1, для доказательства теоремы 2 нам достаточно показать, что справедливо следующее утверждение: любой одномерный коцикл l_σ группы $\overline{F}$ в $\overline{F}$-модуле $\overline{A}$, ограничения которого на группы разложения всех простых дивизоров поля $\overline{K}$ распадаются, и сам распадается. Но все циклические подгруппы группы $\overline{F} = \mathrm{Gal}\,(\overline{K}/k)$ являются группами разложения некоторых простых дивизоров поля $\overline{K}$, поэтому теорема 2 сразу вытекает из следующей леммы.

Лемма. *Пусть p – простое число, B – элементарная абелева p-группа, $b_1, \ldots, b_n$ – базис группы B, и пусть S – подгруппа группы* $\mathrm{Aut}\,(B)$*, порожденная элементарными по отношению к базису $b_1, \ldots, b_n$ автоморфизмами. Если l_σ – такой одномерный коцикл группы S со значениями в S-модуле B, что его ограничения на все циклические подгруппы группы S распадаются, то и сам коцикл l_σ распадается.*

Доказательство леммы. Для $1 \leqslant i < j \leqslant n$ обозначим через ε_{ij} элементарный автоморфизм группы B, действующий по правилу

$$\varepsilon_{ij}(b_i) = b_i + b_j, \quad \varepsilon_{ij}(b_q) = b_q \quad \text{при} \quad q \neq i.$$

Обозначим через J множество всех пар (i, j), таких что $1 \leqslant i < j \leqslant n$. По условию леммы, существует такое подмножество J_0 множества J, что автоморфизмы ε_{ij}, $(i, j) \in J_0$, порождают группу S.

Распадение ограничения коцикла l_σ на циклическую подгруппу группы S, порожденную элементом ε_{ij}, $(i, j) \in J_0$, означает, что $l_{\varepsilon_{ij}} \in (\varepsilon_{ij} - 1)B$. Но из описания действия элементарного автоморфизма ε_{ij} на базисе $b_1, \dots, b_n$ видно, что $(\varepsilon_{ij} - 1)B$ является одномерным подпространством B, порожденным элементом b_j, так что существует такой элемент $x_{ij} \in \mathbb{F}_p$, что $l_{\varepsilon_{ij}} = x_{ij} b_j$.

Покажем, что если пары (i, j) и (i, q) принадлежат J, то $x_{ij} = x_{iq}$. Заметим сначала, что

$$\varepsilon_{ij}\varepsilon_{iq}(b_i) = \varepsilon_{ij}(b_i + b_q) = b_i + b_j + b_q, \quad \varepsilon_{ij}\varepsilon_{iq}(b_r) = b_r \quad \text{при} \quad r \neq i,$$

поэтому $(\varepsilon_{ij}\varepsilon_{iq} - 1)B$ – одномерное подпространство B, порожденное элементом $b_j + b_q$. Ограничение коцикла l_σ на циклическую подгруппу группы S, порожденную произведением $\varepsilon_{ij}\varepsilon_{iq}$, распадается; следовательно, $l_{\varepsilon_{ij}\varepsilon_{iq}} \in (\varepsilon_{ij}\varepsilon_{iq} - 1)B$, и потому $l_{\varepsilon_{ij}\varepsilon_{iq}} = z b_j + z b_q$ для некоторого $z \in \mathbb{F}_p$. С другой стороны,

$$l_{\varepsilon_{ij}\varepsilon_{iq}} = l_{\varepsilon_{ij}} + \varepsilon_{ij} l_{\varepsilon_{iq}} = x_{ij} b_j + \varepsilon_{ij} \cdot x_{iq} b_q = x_{ij} b_j + x_{iq} b_q,$$

так что $z b_j + z b_q = x_{ij} b_j + x_{iq} b_q$, откуда следует, что $x_{ij} = z = x_{iq}$; это мы и хотели показать.

Обозначим через I множество всех тех индексов i, для которых есть такой индекс j, что $(i, j) \in J_0$. Для каждого $i \in I$ пусть y_i – общее значение чисел x_{ij} для всех j, таких что $(i, j) \in J_0$. Таким образом, если $(i, j) \in J_0$, то $l_{\varepsilon_{ij}} = y_i b_j$. Положим $c = \sum_{i \in I} y_i b_i$; тогда для любой пары индексов $(i, j) \in J_0$ будет

$$(\varepsilon_{ij} - 1)c = \sum_{q \in I} y_q (\varepsilon_{ij} - 1) b_q = y_i b_j = l_{\varepsilon_{ij}}.$$

Все значения одномерного коцикла l_σ полностью определяются его значениями на образующих ε_{ij}, $(i, j) \in J_0$; отсюда следует, что соотношение $(\sigma - 1)c = l_\sigma$ выполняется для всех $\sigma \in S$, а это и значит, что коцикл l_σ распадается. Лемма доказана; вместе с ней доказана и теорема 2.

Хорошо известно, что если B – элементарная абелева p-группа, то для любой силовской p-подгруппы группы $\mathrm{Aut}\,(B)$ есть такой базис группы B, что эта силовская подгруппа порождается всеми элементарными по отношению к этому базису автоморфизмами. Поэтому следующее утверждение является частным случаем теоремы 2.

Теорема 3. *Пусть K/k – расширение Галуа с группой Галуа F, и пусть $\varphi : G \to F$ – эпиморфизм, ядро которого A – конечная элементарная абелева p-группа, где p – некоторое простое число. Если K – поле алгебраических чисел, содержащее первообразный корень степени p из 1, а группа $\overline{F}$ содержит силовскую p-подгруппу группы $\mathrm{Aut}\,(\overline{A})$, то согласность достаточна для разрешимости задачи погружения $(K/k, \varphi)$.*

Еще одним следствием теоремы 2 является

Теорема 4. *Пусть p – простое число, K/k – расширение Галуа с группой Галуа F, и пусть $\varphi : G \to F$ – эпиморфизм, ядро которого A – элементарная абелева группа типа (p,p,p). Если K – поле алгебраических чисел, не обязательно содержащее первообразный корень степени p из 1, то согласность достаточна для разрешимости задачи погружения $(K/k, \varphi)$.*

Доказательство. Если поле K не содержит нетривиальных корней p-й степени из 1, то согласность всегда достаточна для задачи погружения числовых полей с ядром, являющимся абелевой p-группой (см. [5]). Пусть теперь поле K содержит первообразный корень из 1 степени p; тогда можно воспользоваться теоремой 2. Силовская p-подгруппа $\overline{F}_p$ группы $\overline{F}$ вкладывается в некоторую силовскую подгруппу P группы $\mathrm{Aut}\,(\overline{A})$, и в $\overline{A}$ есть такой базис b_1, b_2, b_3, что группа P порождается элементарными по отношению к этому базису автоморфизмами ε_{12}, ε_{13}, ε_{23}. У группы P всего две нециклических собственных подгруппы: одна из них порождена автоморфизмами ε_{12}, ε_{13}, а вторая – автоморфизмами ε_{13}, ε_{23}. Таким образом, подгруппа $\overline{F}_p$ группы P либо циклическая, либо порождается элементарными по отношению к базису b_1, b_2, b_3 автоморфизмами. Во втором случае согласность достаточна для разрешимости задачи погружения по теореме 2. Если же группа $\overline{F}_p$ циклическая, то, как уже отмечалось выше, согласность достаточна для погружаемости для любых полей и для любых абелевых ядер.

Замечание 2. В своей дипломной работе (не опубликовано) я нашел необходимое и достаточное дополнительное условие погруженния (при выполненной согласности) для случая абелева ядра типа (p,p,p); это условие состоит в том, что некоторый элемент поля k должен представляться в виде произведения норм элементов из двух подполей поля $\overline{K}$. Как мы видим, для числовых полей дополнительное условие исчезает, а примеров нечисловых полей, для которых дополнительное условие не выполняется, у меня нет. Поэтому остается открытым вопрос о достаточности согласности для погружаемости в случае, когда ядро задачи погружения – абелева группа типа (p,p,p).

Литература

1. Б. Н. Делоне, Д. К. Фаддеев, *Исследования по геометрии теории Галуа.* — Мат. сб. **15(57)** (1944), No. 2, 243–284.
2. H. Hasse, *Existenz und Mannigfaltigkeit Abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers.* — Math. Nachr. **1** (1948), No. 1, 40–61, No. 4, 213–217.
3. А. В. Яковлев, *Задача погружения полей.* — ДАН СССР **150** (1963), No. 5, 1009–1011.
4. А. В. Яковлев, *Задача погружения полей.* — Изв. АН СССР, сер. мат. **28** (1964), No. 3, 645–660.
5. А. В. Яковлев, *Задача погружения для числовых полей.* — Изв. АН СССР, сер. мат. **31** (1967), No. 2, 211–224.

Yakovlev A. V. On the embedding problem for number fields in the case of elementary abelian kernel.

The Galois embedding problem is considered in the case of number fields and elementary abelian kernel. New cases are discovered in which the concordance condition is sufficient for the existence of a solution of the embedding problem. In particular, it is true when the order of the kernel is the cube of a prime integer.

С.-Петербургский
государственный университет
Университетский пр. 28, Петродворец,
198504 Санкт-Петербург, Россия
E-mail: yakovlev.anatoly@gmail.com

Поступило 14 декабря 2009 г.