Записки научных
семинаров ПОМИ
Том 319, 2004 г.

А. В. Яковлев

ЕЩЕ О ПОГРУЖЕНИИ ЦИКЛИЧЕСКИХ РАСШИРЕНИЙ В ЦИКЛИЧЕСКИЕ

Пусть k_1/k – циклическое расширение Галуа, и пусть φ – эпиморфизм циклической группы порядка m на группу Галуа расширения k_1/k. Мы говорим, что расширение k_1/k m-погружаемо (m-согласно), если задача погружения $(k_1/k, \varphi)$ имеет решение (соответственно, если для этой задачи погружения выполнено условие согласности).

Этой задаче была посвящена работа автора [1], в которой найдены необходимые и достаточные условия погружаемости квадратичного расширения в циклическое расширение степени 2^n. Однако, там не исследовались связи между условиями согласности и погружаемости. Для полей алгебраических чисел частично эти связи выяснены в работе [4], которая в значительной степени стимулировала написание настоящей статьи.

Теорема 1. *Пусть k – поле, характеристика которого не равна 2, и пусть $n \geqslant 3$. Далее, пусть $K_0 = k(\sqrt{-1})$, $K = k(\sqrt[2^n]{1})$, и пусть F и F_0 – группы Галуа расширений K/k и K/K_0. Пусть $b \in K_0$ – такой элемент, что элемент $a = \mathrm{Nm}_{K_0/k}\, b \in k$ не является квадратом. Обозначим через $x, y \in H^0(F_0, K^*)$ классы элементов a, b по модулю $\mathrm{Nm}_{K/K_0}(K^*)$. Предположим, что группа F не циклическая. Тогда:*

1. *расширение $k(\sqrt{a})/k$ 2^n-погружаемо тогда и только тогда, когда в группе $H^0(F_0, K^*)$ существует такой элемент z, что элемент $y + 2z \in H^0(F_0, K^*)$ инвариантен относительно группы F;*
2. *расширение $K_0(\sqrt{a})/K_0$ 2^n-погружаемо тогда и только тогда, когда $x \in 2H^0(F_0, K^*)$;*
3. *расширение $k(\sqrt{a})/k$ 2^n-согласно тогда и только тогда, когда расширение $K_0(\sqrt{a})/K_0$ 2^n-погружаемо*

(для групп когомологий мы используем аддитивную запись).

Доказательство. Утверждения (1) и (2) – просто переформулировки утверждений (d) и (c) теоремы из работы [1]. Перед тем, как доказывать утверждение (3), сделаем три простых наблюдения.

– Условие согласности необходимо и достаточно для разрешимости задачи погружения расширения $K_0(\sqrt{a})/K_0$ в циклическое расширение порядка 2^n. Действительно, группа Галуа расширения $K_0(\sqrt{a}, \sqrt[2^n]{1})/K_0$ действует на группе характеров ядра этой задачи посредством циклической факторгруппы, и наше утверждение следует из одного из результатов работы [2].

– Задача погружения расширения $k(\sqrt{a})/k$ в циклическое расширение порядка 4 разрешима, потому что $a = \mathrm{Nm}_{K_0/k}(b)$ (см. случай (b) теоремы из [1]).

– Условие согласности эквивалентно разрешимости всех сопровождающих брауэровских задач погружения.

Для доказательства утверждения (3) остается заметить, что любая сопровождающая брауэровская задача для задачи погружения расширения $k(\sqrt{a})/k$ в циклическое расширение порядка 2^n является или задачей погружения расширения $k(\sqrt{a})/k$ в циклическое расширение порядка 4, или сопровождающей задачей для задачи погружения расширения $K_0(\sqrt{a})/K_0$ в циклическое расширение порядка 2^n.

Обозначим для краткости группу $H^0(F_0, K^*)$ через A; эта группа является F-модулем, на котором группа F_0 действует тривиально. Поэтому мы можем рассматривать A как модуль над циклической группой F/F_0 порядка 2. Обозначим через τ элемент, порождающий эту группу.

Следствие 1. *Пусть A_0 – подгруппа группы A, состоящая из всех τ-инвариантных элементов, и пусть B – множество всех элементов $u \in A$, таких что $(\tau+1)u \in 2A$. Если $B \neq A_0+2A$, то существует квадратичное расширение $k(\sqrt{a})$ поля k, которое 2^n-согласно, но не 2^n-погружаемо.*

Замечание. Очевидно, что $B \supseteq A_0 + 2A$.

Доказательство. Пусть $y \in B$, $y \notin A_0 + 2A$, и пусть $b \in K_0$ – любой элемент, класс вычетов которого по модулю Nm_{K/K_0} равен $y \in A = H^0(F_0, K^*)$. Тогда $x = (1+\tau)y \in (1+\tau)B \subseteq 2A$ является классом вычетов элемента $a = b^{1+\tau} \in k$ по модулю Nm_{K/K_0}. Поскольку $x \in 2H^0(F_0, K^*)$, а множество $y + 2H^0(F_0, K^*)$ не содержит ни одного τ-инвариантного элемента, из теоремы 1 следует, что расширение $k(\sqrt{a})/k$ 2^n-согласно, но не 2^n-погружаемо.

Теорема 2. *Пусть в обозначениях и предположениях теоремы* 1 *поле* k *является полем алгебраических чисел. Если порядок группы* F_0 *не меньше* 4 *и* $H^3(F, K^*) \neq 0$, *то существует* 2^n*-согласное, но не* 2^n*-погружаемое квадратичное расширение* $k(\sqrt{a})$ *поля* k.

Доказательство. Обозначим через $\mathfrak{J}$, $\mathfrak{C}$ группу иделей и группу классов иделей поля K. Последовательность τ-модулей

$$H^{-1}(F_0, \mathfrak{C}) \longrightarrow H^0(F_0, K^*) \longrightarrow H^0(F_0, \mathfrak{J}) \xrightarrow{\alpha} H^0(F_0, \mathfrak{C})$$

точна. Но $H^{-1}(F_0, \mathfrak{C}) = 0$, потому что группа F_0 циклическая; следовательно, $A = H^0(F_0, K^*) = \operatorname{Ker} \alpha$. Теория полей классов позволяет явно описать модули $H^0(F_0, \mathfrak{J})$, $H^0(F_0, \mathfrak{C})$ и гомоморфизм α.

Пусть P – множество всех простых дивизоров поля k; для каждого $\mathfrak{p} \in P$ обозначим через $F_\mathfrak{p} \subseteq F$ группу разложения любого простого дивизора поля K, делящего $\mathfrak{p}$. Пусть m – порядок группы F_0, $m_\mathfrak{p}$ – порядок пересечения $F_0 \cap F_\mathfrak{p}$, и пусть $q_\mathfrak{p} = m/m_\mathfrak{p}$ ($\mathfrak{p} \in P$). Модуль $H^0(F_0, \mathfrak{C})$ порождается единственным элементом e, а модуль $H^0(F_0, \mathfrak{J})$ порождается элементами $e_\mathfrak{p}$, $\mathfrak{p} \in P$; эти порождающие элементы связаны определяющими соотношениями

$$me = 0, \quad m_\mathfrak{p} e_\mathfrak{p} = 0 \ \text{ для всех } \mathfrak{p} \in P; \quad \tau e = e;$$
$$\text{если } \ F_\mathfrak{p} \nsubseteq F_0, \text{ то } \tau e_\mathfrak{p} = e_\mathfrak{p},$$

и гомоморфизм α задается формулой $\alpha(e_\mathfrak{p}) = q_\mathfrak{p} e$.

Если $H^3(F, K^*) \neq 0$, то $F_\mathfrak{p} \neq F$ для всех $\mathfrak{p} \in P$; следовательно, для каждого $\mathfrak{p}$ или $\tau e_\mathfrak{p} \neq e_\mathfrak{p}$, или $m_\mathfrak{p}$ является собственным делителем m. Это значит, что $\alpha(2z) \in 4H^0(F_0, \mathfrak{C})$ для всех тех $z \in H^0(F_0, \mathfrak{J})$, для которых элементы $2z$ инвариантны относительно τ. Но каждая циклическая подгруппа группы F является группой разложения некоторого простого дивизора поля K. Следовательно, существует дивизор $\mathfrak{q} \in P$, такой что $F_\mathfrak{q} = F_0$; тогда $m_\mathfrak{q} = m$, и $\alpha(e_\mathfrak{q}) = e$. Элемент $y = (\tau - 1)e_\mathfrak{q}$ содержится в $\operatorname{Ker} \alpha = A$, и $(1 + \tau)y = 0 \in 2A$. Если $z \in A$ – такой элемент, что элемент $y + 2z$ инвариантен относительно τ, то элемент $2(z - e_\mathfrak{q}) = y + 2z - (1 + \tau)e_\mathfrak{q} \in H^0(F^0, \mathfrak{J})$ тоже инвариантен относительно τ, и $\alpha(2(z - e_\mathfrak{q})) = -2e \notin 4H^0(F_0, \mathfrak{C})$, что невозможно. Таким образом, ни один из элементов множества $y + 2A$ не является τ-инвариантным. По следствию 1, существует 2^n-согласное, но не 2^n-погружаемое квадратичное расширение $k(\sqrt{a})$ поля k.

Теорема 3. *Пусть в обозначениях и предположениях теоремы* 1 *поле* k *является полем алгебраических чисел,* $H^3(F,K^*) \neq 0$ *и* $n=3$. *Если расширение* $k(\sqrt{a})/k$ 8-*погружаемо, то существуют такие элементы* $c \in k$, $u \in K$, *что* $a = c^2 \operatorname{Nm}_{K/k} u$.

Доказательство. Поле K получается присоединением к полю k первообразного корня восьмой степени из единицы ζ. Его группа Галуа – нециклическая группа порядка 4, порожденная автоморфизмами σ, τ, такими что $\zeta^\tau = \zeta^{-1}$, $\zeta^\sigma = \zeta^5$. По теореме Гильберта 90 F-модуль K^* когомологически тривиален в размерности 1. Поэтому по теореме 2 из работы [3] F-модуль K^* когомологически эквивалентен прямой сумме модулей, каждый из которых или изоморфен целочисленному групповому кольцу некоторой факторгруппы группы F (таких факторгрупп пять), или изоморфен $I \otimes I$, где I – ядро канонического эпиморфизма $\mathbb{Z}[F] \to \mathbb{Z}$. Если $H^3(F,K^*) \neq 0$, то все группы разложения дивизоров поля K являются собственными подгруппами F, и потому вторая группа когомологий K^*, которая изоморфно вкладывается во вторую группу когомологий группы иделей, не содержит элементов порядка 4. Поскольку $H^2(F, I\otimes I)$ – циклическая группа порядка 4, группа K^* когомологически эквивалентна прямой сумме модулей, каждый из которых изоморфен целочисленному групповому кольцу одной из пяти факторгрупп группы F. Отсюда следует, что в предположениях теоремы 3 $H^{-1}(F,K^*) = 0$.

По теореме из [1], если расширение $k(\sqrt{a})/k$ 8-погружаемо, то существуют такие элементы $b_1 \in K_0$, $v \in K$, что $b_1^{\tau+1} = a$, $b_1^{\tau-1} = v^{1+\sigma}$. Отсюда следует, что $\operatorname{Nm}_{K_0/k} v = v^{(\sigma+1)(\tau+1)} = (b_1^{\tau-1})^{\tau+1} = 1$, и, поскольку $H^{-1}(F,K^*) = 0$, найдутся элементы $u, w \in K$, такие что $v = u^{\tau-1}w^{\sigma-1}$. Тогда $b_1^{\tau-1} = v^{\sigma+1} = u^{(\sigma+1)(\tau-1)}$. Следовательно, элемент $c = b_1/u^{\sigma+1}$ инвариантен относительно τ. С другой стороны, элемент c инвариантен относительно σ, потому что инвариантны относительно σ элементы b_1 и $u^{\sigma+1}$. Значит, $c \in k$, и $a = b_1^{\tau+1} = (cu^{\sigma+1})^{\tau+1} = c^2 \operatorname{Nm}_{K/k} u$.

Следствие 2. *Пусть* K – *поле, полученное присоединением всех корней* 8-*ой степени из* 1 *к полю алгебраических чисел* k, *и пусть* F – *группа Галуа расширения* K/k. *Если* $H^3(F,K^*) \neq 0$, *то существует элемент* $a \in \operatorname{Nm}_{K/k}(K^*)$, *такой что расширение* $k(\sqrt{a})/k$ 16-*согласно, но не* 16-*погружаемо.*

Доказательство. Пусть $K_1 \supset K$ – поле, полученное присоединением первообразного корня 16-й степени из 1, и пусть F_1 – группа Галуа расширения K_1/k. Поскольку $H^3(F, K^*) \neq 0$, очевидно, что и $H^3(F_1, K_1^*) \neq 0$. По теореме 2 существует 16-согласное, но не 16-погружаемое квадратичное расширение $k(\sqrt{a_1})$ поля k. Это расширение 8-согласно, и, поскольку ядро задачи погружения квадратичного расширения в циклическое расширение порядка 8 – циклическая группа порядка 4, оно 8-погружаемо. По теореме 3 существуют элементы $c \in k$, $u \in K$, такие что $a_1 = c^2 \operatorname{Nm}_{K/k} u$. Пусть $a = \operatorname{Nm}_{K/k} u$; тогда квадратичное расширение $k(\sqrt{a}) = k(\sqrt{a_1})$ поля k 16-согласно, но не 16-погружаемо.

Высказывалось предположение, что, при выполнении условия согласности, принадлежность элемента a группе норм из поля корней 2^{n-1}-й степени из 1 достаточна для 2^n-погружаемости расширения $k(\sqrt{a})/k$. Как мы только что увидели, это не так уже в случае, когда k – поле алгебраических чисел, а $n = 4$. Укажем теперь необходимые и достаточные условия 2^n-погружаемости 2^n-согласного квадратичного расширения.

Теорема 4. *Пусть $n \geqslant 4$ и пусть K_1, K – поля, полученные присоединением всех корней 2^n-ой степени из 1 и 2^{n-1}-ой степени из 1 к полю k, а $K_0 = k(\sqrt{-1})$. Предположим, что группа Галуа расширения K/k не циклическая. Пусть, далее, $k(\sqrt{a})/k$ – 2^n-согласное квадратичное расширение; тогда по теореме 1 существуют такие элементы $u \in K_0$, $v \in K_1$, что $a = u^2 \operatorname{Nm}_{K_1/K_0} v$. Для того, чтобы расширение $k(\sqrt{a})/k$ было 2^n-погружаемым, необходимо и достаточно, чтобы произведение $a \operatorname{Nm}_{K_0/k}(1/u)$ принадлежало группе норм $\operatorname{Nm}_{K/k} K^*$.*

Доказательство.

Достаточность. Поскольку расширение $k(\sqrt{a})/k$ является 2^n-согласным, а потому и 4-согласным, а значит, и 4-погружаемым, существует такой элемент $b \in K_0$, что $a = \operatorname{Nm}_{K_0/k} b$. Пусть $r = (K : K_0)$; тогда группа Галуа расширения K_1/k порождается двумя элементами σ, τ, связанными определяющими соотношениями $\tau^2 = \sigma^{2r} = 1$, $\sigma\tau = \tau\sigma$; при этом σ порождает группу Галуа расширения K_1/K_0, поле K является подполем поля K_1, принадлежащим подгруппе, порожденной σ^r, а ограничение τ на K_0 порождает группу Галуа расширения K_0/k.

Пусть $w \in K$ – такой элемент, что $a \operatorname{Nm}_{K_0/k}(1/u) = \operatorname{Nm}_{K/k} w$.

Тогда

$$(b/u)^{1+\tau} = a\,\mathrm{Nm}_{K_0/k}(1/u) = w^{(1+\sigma+\ldots+\sigma^{r-1})(1+\tau)},$$

и по теореме Гильберта 90 найдется такой элемент $u_1 \in K_0$, что

$$b/u = u_1^{\tau-1} w^{1+\sigma+\ldots+\sigma^{r-1}}.$$

Мы получаем теперь, что

$$a/b^2 = (u/b)^2\,\mathrm{Nm}_{K_1/K_0} v = (u_1^{1-\tau})^2 (w^{2(1+\sigma+\ldots+\sigma^{r-1})})^{-1}\,\mathrm{Nm}_{K_1/K_0} v = \\ = (u_1^{1-\tau})^2\,\mathrm{Nm}_{K_1/K_0}(v/w),$$

а это как раз и есть достаточное условие 2^n-погружаемости из [1].

Необходимость. Если расширение $k(\sqrt{a})/k$ 2^n-погружаемо, то по теореме из [1] найдутся такие элементы $u_1 \in K_0$, $v_1 \in K_1$, что $a = (bu_1^{1-\tau})^2\,\mathrm{Nm}_{K_1/K_0} v_1$. Тогда

$$\left(\frac{bu_1^{1-\tau} v_1^{1+\sigma+\ldots+\sigma^{r-1}}}{uv^{1+\sigma+\ldots+\sigma^{r-1}}}\right)^{1+\sigma^r} = \frac{(bu_1^{1-\tau})^2\,\mathrm{Nm}_{K_1/K_0} v_1}{u^2\,\mathrm{Nm}_{K_1/K_0} v} = a/a = 1,$$

и по теореме Гильберта 90 существует такой элемент $w \in K_1$, что

$$bu_1^{1-\tau}/u = w^{1-\sigma^r}(v^{1+\sigma+\ldots+\sigma^{r-1}})/(v_1^{1+\sigma+\ldots+\sigma^{r-1}}) = v_2^{1+\sigma+\ldots+\sigma^{r-1}},$$

где $v_2 = w^{1-\sigma} v/v_1$. Поскольку $bu_1^{1-\tau}/u \in K_0$, элемент $bu_1^{1-\tau}/u$ инвариантен относительно σ, и потому $v_2^{1-\sigma^r} = (v_2^{1+\sigma+\ldots+\sigma^{r-1}})^{1-\sigma} = (bu_1^{1-\tau}/u)^{1-\sigma} = 1$. Следовательно, элемент v_2 принадлежит подполю K поля K_1. Теперь мы получаем:

$$a\,\mathrm{Nm}_{K_0/k}(1/u) = (bu_1^{1-\tau}/u)^{1+\tau} = v_2^{(1+\sigma+\ldots+\sigma^{r-1})(1+\tau)} = \mathrm{Nm}_{K/k} v_2.$$

Литература

1. А. В. Яковлев, *Погружение циклического расширения в циклическое.* — Зап. научн. семин. ПОМИ **265** (1999), 306–313.
2. А. В. Яковлев, *Задача погружения полей.* — Известия АН СССР, сер. матем. **28**, № 3 (1964), 645–660.
3. А. А. Яковлева, *Модули с тривиальными 1-когомологиями.* — Алгебра и Анализ **12**, № 3 (2000), 201–222.

4. В. В. Ишханов, Б. Б. Лурье, *Об одной задаче погружения с циклическим ядром.* — Зап. научн. семин. ПОМИ **305** (2003), 144–152.

Yakovlev A. V. More about the embedding of a cyclic extension into a cyclic extension.

The connections between the concordance condition and the solvability of the problem of embedding of a cyclic Galois extension into another cyclic Galois extension are investigated.

Санкт-Петербургский
государственный университет
E-mail: yakovlev@yak.pdmi.ras.ru

Поступило 1 октября 2004 г.