УДК 512.54 Вестник СПбГУ. Сер. 1. Т. 1 (59). 2014. Вып. 2

О ПОГРУЖЕНИИ УНИВЕРСАЛЬНО СОГЛАСНОГО 2-РАСШИРЕНИЯ В УНИВЕРСАЛЬНО СОГЛАСНОЕ

А. В. Яковлев

Санкт-Петербургский государственный университет,
Российская Федерация, 199034, Санкт-Петербург, Университетская наб., 7/9

Расширение Галуа называется универсально согласным периода q если для любой задачи погружения этого расширения с абелевым ядром периода q выполняется условие согласности. Пусть K — такое универсально согласное периода 2^{n+1} расширение поля алгебраических чисел k, что 2 полностью раскладывается в K, и пусть $(K/k, \varphi)$ — некоторая задача погружения с абелевым ядром порядка 2. Доказывается, что (при некоторых теоретико-групповых ограничениях) существует универсально согласное периода 2^n решение этой задачи погружения. Библиогр. 6 назв.

Ключевые слова: группа Галуа, задача погружения, условие согласности.

1. Введение. Понятие универсально согласного расширения Галуа было введено в [1]. Там же было показано, что при помощи универсально согласных расширений можно легко строить расширения Галуа числовых полей с предписанной группой Галуа нечетного порядка. Ключевым моментом, обеспечивающим возможность такого построения, является следующий результат, доказанный в [1]: если p — нечетное простое число, и универсально согласное p-расширение числовых полей не содержит первообразный корень степени p из 1, то это расширение может быть погружено в строго большее универсально согласное p-расширение. Целью настоящей работы является доказательство того, что при некоторых ограничениях аналогичный результат верен и для 2-расширений.

В этом параграфе мы напомним некоторые определения и факты, относящиеся к задаче погружения полей и содержащиеся в книге [2]. Пусть K/k — конечное расширение Галуа или алгебра Галуа с группой Галуа F, и пусть φ — эпиморфизм конечной группы G на группу F. Мы обозначаем через $(K/k, G, \varphi)$ или, короче, через $(K/k, \varphi)$ следующую задачу, называемую задачей погружения: построить алгебру Галуа L/k с группой Галуа G, такую что $K \subseteq L$ и что ограничение любого автоморфизма $g \in G = \mathrm{Gal}(L/k)$ на K совпадает с автоморфизмом $\varphi(g) \in F$ алгебры Галуа K. Ядро эпиморфизма φ называется ядром задачи погружения $(K/k, \varphi)$.

Одно необходимое, но не достаточное условие разрешимости задачи погружения — условие согласности — было найдено Д. К. Фаддеевым в работе [3]. Мы не формулируем его здесь; одна из формулировок этого условия для случая полей алгебраических чисел (который только и интересует нас в этой статье) будет приведена ниже.

Приведем три конструкции, позволяющие, исходя из задачи погружения и дополнительной информации, строить другие задачи погружения. Прежде чем сделать это, напомним, что расширение группы — это пара (G, θ), состоящая из группы G и эпиморфизма $\theta : G \to F$. Если $A = \mathrm{Ker}\theta$ — абелева группа, то на A естественным образом определена структура F-модуля, и расширение групп (G, θ) вполне определяется классом когомологий $x \in H^2(F, A)$.

Первая из этих конструкций — перенесение задачи погружения. Пусть (K/k) — расширение Галуа с группой Галуа F, F_0 — подгруппа F, $\varphi_0 : G_0 \to F_0$ — эпиморфизм групп с конечным абелевым ядром A_0. Пусть $x \in H^2(F_0, A_0)$ — класс когомологий, отвечающий расширению (G_0, φ_0). Группа $A = \mathbb{Z}[F] \otimes_{F_0} A_0$ является левым F-модулем, и хорошо известно (см., например, [4]), что существует канонический изоморфизм

$$t_{F_0}^F : H^2(F_0, A_0) \to H^2(F, \mathbb{Z}[F] \otimes_{F_0} A_0) = H^2(F, A).$$

Пусть

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

— расширение групп, отвечающее классу когомологий $t_{F_0}^F(x) \in H^2(F, A)$. Оно называется перенесением исходного расширения с подгруппы F_0 на всю группу F, а задача погружения $(K/k, \varphi)$ называется перенесением задачи $(K/K^{F_0}, \varphi_0)$ на расширение K/k. Ещё раз отметим, что ядром перенесения является группа $\mathbb{Z}[F] \otimes_{F_0} A_0$.

Предложение 1. *Задача погружения $(K/K^{F_0}, \varphi_0)$ и её перенесение $(K/k, \varphi)$ эквивалентны: первая задача разрешима тогда и только тогда, когда разрешима вторая задача, а условие согласности для первой задачи выполняется тогда и только тогда, когда оно выполняется для второй задачи.*

Вторая конструкция — подъем задачи погружения. Пусть K/k — расширение Галуа с группой Галуа F, H — нормальная подгруппа F, $\bar{K} = K^H$, $\bar{F} = F/H = \mathrm{Gal}(\bar{K}/k)$, $\pi : F \to \bar{F}$ — канонический эпиморфизм на факторгруппу. Далее, пусть $\bar{\varphi}$ — эпиморфизм конечной группы $\bar{G}$ на $\bar{F}$, $G = F \times_{\bar{F}} \bar{G}$ — прямое произведение с объединенной факторгруппой $\bar{F}$ (то есть подгруппа прямого произведения $F \times \bar{G}$, состоящая из таких пар $(f, \bar{g})$, что $\pi(f) = \bar{\varphi}(\bar{g})$), $\varphi : G \to F$ — эпиморфизм групп, сопоставляющий паре $(f, \bar{g}) \in G$ её первую компоненту f.

Предложение 2. *Задачи погружения $(\bar{K}/k, \bar{\varphi})$ и $(K/k, \varphi)$ эквивалентны: первая задача разрешима тогда и только тогда, когда разрешима вторая задача, а условие согласности для первой задачи выполняется тогда и только тогда, когда оно выполняется для второй задачи.*

Наконец, определим произведение задач погружения. Пусть K/k — расширение Галуа с группой Галуа F, и пусть $\varphi_i : G_i \to F$ — эпиморфизмы конечных групп на группу F $(i = 1, 2, \ldots, n)$. Далее, пусть $G = G_1 \times_F \ldots_F \times G_n$ — прямое произведения групп G_i с объединенной факторгруппой F (то есть подгруппа прямого произведения $G_1 \times \ldots \times G_n$, состоящая из таких элементов $(g_1, \ldots, g_n)$, что $\varphi_1(g_1) = \ldots = \varphi_n(g_n)$), и $\varphi : G \to F$ — эпиморфизм, сопоставляющий элементу $(g_1, \ldots, g_n) \in G$ элемент $\varphi_1(g_1) = \ldots = \varphi_n(g_n) \in F$. Расширение (G, φ) называется произведением расширений (G_i, φ_i), а задача погружения $(K/k, \varphi)$ называется произведением задач $(K/k, \varphi_i)$; её ядро — прямое произведение ядер перемножаемых задач.

Предложение 3. *Задача погружения $(K/k, \varphi)$ разрешима тогда и только тогда, когда разрешимы все задачи погружения $(K/k, \varphi_i)$.*

2. Достаточное условие цикличности групп ветвления. Пусть U — группа с двумя образующими u, v, связанными соотношениями $u^2 = v^4 = 1$, $u^{-1}vu = v^3$, а U_1 — абелева группа с двумя образующими u_1, v_1, связанными соотношениями $u_1^2 = v_1^4 = 1$. Далее, пусть K/k — нециклическое расширение Галуа степени 4, а h_1, h_2 — порождающие элементы его группы Галуа. Обозначим через $\delta : U \to \mathrm{Gal}(K/k)$, $\delta_1, \delta_2 : U_1 \to \mathrm{Gal}(K/k)$ эпиморфизмы, задаваемые формулами

$$\delta_0(u) = \delta_1(u_1) = \delta_2(v_1) = h_1, \quad \delta_0(v) = \delta_1(v_1) = \delta_2(u_1) = h_2.$$

Лемма 1. *Если разрешимы все три задачи погружения $(K/k, \delta_0)$, $(K/k, \delta_1)$, $(K/k, \delta_2)$, то группы разложения всех простых дивизоров поля K, не делящих 2, являются циклическими группами.*

Доказательство. Пусть L_0, L_1, L_2 — какие-то решения этих трёх задач. Их композит $L = L_0L_1L_2$ — расширение Галуа поля k, причем группа $G' = \mathrm{Gal}(L/K)$ является подгруппой Фраттини группы $G = \mathrm{Gal}(L/k)$ и представляет собой прямое произведение трёх циклических групп порядка 2.

Пусть теперь $\mathfrak{P}$ — простой дивизор поля K, не делящий 2, $\mathfrak{p}$ — делящийся на него простой дивизор поля k, $K_{\mathfrak{P}}$ и $k_{\mathfrak{p}}$ — $\mathfrak{P}$-адическое пополнение поля K и $\mathfrak{p}$-адическое пополнение поля k. Если группа разложения дивизора $\mathfrak{P}$ не циклическая, то $\mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}}) = \mathrm{Gal}(K/k)$ — нециклическая группа порядка 4. Тензорное произведение $\bar{L} = L \otimes_k K_{\mathfrak{P}}$ является алгеброй Галуа с группой Галуа G над полем $k_{\mathfrak{p}}$. Поскольку $K_{\mathfrak{P}}$ — поле, а группа Галуа H расширения $\bar{L}/K_{\mathfrak{P}}$ является подгруппой Фраттини группы $G = \mathrm{Gal}(\bar{L}/k_{\mathfrak{p}})$, алгебра $\bar{L}$ тоже является полем. Таким образом, мы построили расширение Галуа $\bar{L}$ локального поля $K_{\mathfrak{P}}$ с нечетной характеристикой поля вычетов, группа Галуа которого является прямым произведением трёх циклических групп порядка 2. Но это невозможно, так как любое 2-расширение локального поля с нечетной характеристикой поля вычетов не имеет высшего ветвления, а группа Галуа любого расширения без высшего ветвления порождается не более чем двумя элементами. □

Предложение 4. *Пусть K'/k — расширение числовых полей, группа Галуа F' которого — 2-группа, A — её нормальная подгруппа порядка 2, $K = K'^A$ — подполе K, принадлежащее A. Предположим, что выполняются следующие условия:*

(1) *группы разложения всех простых дивизоров поля K, не делящих 2, циклические;*

(2) *расширение K'/k погружается в такое расширение Галуа L_2/k, что $\mathrm{Gal}(L_2/K)$ — циклическая группа порядка 4, содержащаяся в центре группы $\mathrm{Gal}(L_2/k)$;*

(3) *для любой циклической подгруппы C группы $F = \mathrm{Gal}(K/k)$ расширение K/K^C погружается в строго большее циклическое 2-расширение;*

(4) *для любой подгруппы H группы $F = \mathrm{Gal}(K/k)$, такой что $\alpha^{-1}(H)$ нециклическая группа порядка 4, расширение K'/K^H погружается в расширение Галуа L с группой Галуа U, причем канонический эпиморфизм $U = \mathrm{Gal}(L/K_0) \to \mathrm{Gal}(K'/K_0)$ отображает элемент v в единственный неединичный элемент группы A.*

Тогда группы разложения всех простых дивизоров поля K', не делящих 2, циклические.

Доказательство. Обозначим через α канонический эпиморфизм группы $\mathrm{Gal}(K'/k)$ на группу $\mathrm{Gal}(K/k)$. Предположим, что группа разложения D некоторого простого дивизора $\mathfrak{P}_1$ поля K', не делящего 2, не является циклической. Группа $C = \alpha(D)$ является группой разложения простого дивизора $\mathfrak{P}$ поля K, делящегося на $\mathfrak{P}_1$; поэтому по предположению предложения группа C циклическая, и следовательно, нециклическая группа D раскладывается в прямое произведение группы, изоморфной C, и группы $\mathrm{Gal}(K'/k)$ порядка 2. Следовательно, в группе D есть нециклическая подгруппа V порядка 4, содержащая $\mathrm{Gal}(K'/K)$. Пусть $K_0 = K'^V = K^{\alpha(V)}$. Для расширения K'/K_0 группа V будет группой разложения простого дивизора $\mathfrak{P}_1$ поля K'. Но это невозможно, потому что расширение K'/K_0 удовлетворяет всем условиям леммы

1. Действительно, указанные в пунктах (2), (4) поля L_2, L решают задачи погружения $(K'/K_0, \delta_2)$ и $(K'/K_0, \delta)$, а по условию (3) расширение K/K_0 погружается в циклическое расширение степени L'_1 степени 4, так что $L_1 = L'_1 K'$ — решение задачи $(K'/K_0, \delta_1)$. Полученное противоречие доказывает, что группы разложения всех простых дивизоров поля K', не делящих 2, циклические. $\square$

3. Условие согласности для числовых полей. Пусть k — поле алгебраических чисел, K — его конечное расширение Галуа, $F = \mathrm{Gal}(K/k)$, $\varphi : G \to F$ — эпиморфизм конечной группы G на F с абелевым ядром A. Для простого дивизора $\mathfrak{P}$ поля K мы используем следующие обозначения:

$F_{\mathfrak{P}} \leq F$ — группа разложения дивизора $\mathfrak{P}$;

$G_{\mathfrak{P}} = \varphi^{-1} F_{\mathfrak{P}}$;

$\varphi_{\mathfrak{P}} : G_{\mathfrak{P}} \to F_{\mathfrak{P}}$ — эпиморфизм, индуцированный гомоморфизмом φ;

$\mathfrak{p}$ — простой дивизор поля k, делящийся на $\mathfrak{P}$;

$K_{\mathfrak{P}}$ и $k_{\mathfrak{p}}$ — $\mathfrak{P}$-адическое пополнение поля K и $\mathfrak{p}$-адическое пополнение поля k.

Расширение $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ является расширением Галуа с группой Галуа $F_{\mathfrak{P}}$. Одна из форм условия согласности для задачи погружения $(K/k, G, \varphi)$ с абелевым ядром состоит в следующем: для каждого простого дивизора $\mathfrak{P}$ поля K задача погружения $(K_{\mathfrak{P}}/k_{\mathfrak{p}}, G_{\mathfrak{P}}, \varphi_{\mathfrak{P}})$ разрешима. Но для разрешимости этой задачи достаточно (но не необходимо), чтобы была разрешима задача погружения $(K/K^{F_{\mathfrak{P}}}, G_{\mathfrak{P}}, \varphi_{\mathfrak{P}})$. Таким образом, мы получаем следующее достаточное условие согласности для задачи $(K/k, \varphi)$:

Предложение 5. *Если для каждого простого дивизора $\mathfrak{P}$ поля K задача погружения $(K/K^{F_{\mathfrak{P}}}, G_{\mathfrak{P}}, \varphi_{\mathfrak{P}})$ разрешима, то для задачи погружения $(K/k, G, \varphi)$ выполнено условие согласности.*

Следствие. *Если группы разложения всех простых дивизоров поля K циклические, то для выполнения условия согласности для задачи $(K/k, \varphi)$ достаточно (но, вообще говоря, не необходимо), чтобы для любой циклической подгруппы C группы F циклическое расширение K/K^C погружалось в циклическое расширение степени $m|C|$, где m — период группы* $\mathrm{Ker}\varphi$, *а $|C|$ — порядок циклической группы C.*

Доказательство. Пусть выполнено условие следствия и пусть $F_{\mathfrak{P}} = C$ — циклическая группа разложения простого дивизора $\mathfrak{P}$ поля K. Выберем элемент f, порождающий циклическую группу C; пусть g — какой-то элемент из G, такой что $\varphi(g) = f$, и пусть D — циклическая подгруппа G, порожденная g. Ограничение φ_D гомоморфизма φ на D является эпиморфизмом D на C. Поскольку, очевидно, порядок D делит $m|C|$, задача погружения $(K/K^C, D, \varphi_D)$ разрешима по условию следствия. Но тогда разрешима и задача

$$(K/K^C, \varphi^{-1}(C), \varphi_{\varphi^{-1}(C)}) = (K/K^{F_{\mathfrak{P}}}, G_{\mathfrak{P}}, \varphi_{\mathfrak{P}}).$$

Это верно для всех простых дивизоров поля K, поэтому по предложению 5 для задачи $(K/k, \varphi)$ выполнено условие согласности. $\square$

4. Универсально согласные расширения. Расширение Галуа K/k называется универсально согласным периода N, если условие согласности выполняется для всех задач погружения $(K/k, \varphi)$ с абелевым ядром $\mathrm{Ker}\varphi$ периода N.

Замечание 1. *Наше определение немного отличается от определения из работы [1]. Там определение было дано для случая, когда поле K содержит первообразный корень ζ степени N из 1. Заметим, что если расширение K/k универсально согласно в смысле определения, которое мы используем здесь, то совсем не обязательно, чтобы расширение $K(\zeta)/k$ было универсально согласным, так как далеко не всякая задача погружения для расширения $K(\zeta)/k$ происходит из задачи погружения для расширения K/k.*

Предложение 6. *Пусть K/k — универсально согласное расширение Галуа периода N, $k_1, \bar{K}$ — подполя K, содержащие k, причем $\bar{K}/k$ — расширение Галуа. Тогда K/k_1, $\bar{K}/k$ — универсально согласные расширения Галуа периода N.*

Доказательство. Пусть $(K/k_1, \varphi_1)$, $(\bar{K}/k, \bar{\varphi})$ — задачи погружения с абелевыми ядрами периода N. Тогда перенесение первой и подъем второй задач до задач погружения для расширения K/k тоже являются задачами погружения на расширение K/k с абелевыми ядрами периода N; поскольку расширение K/k универсально согласно периода N, для обеих этих задач выполнено условие согласности. Тогда по предложению 1 условие согласности выполнено для задачи $(K/k_1, \varphi_1)$, а по предложению 2 — для задачи $(\bar{K}/k, \bar{\varphi})$. □

В дальнейшем мы будем интересоваться только универсально согласными расширениями числовых полей.

Лемма 2. *Пусть k — поле алгебраических чисел, и пусть K/k — расширение Галуа, группа Галуа F которого является 2-группой. Если расширение K/k универсально согласно периода 2^m, $m \geq 1$, то группы разложения всех простых дивизоров поля K, не делящих 2, являются циклическими группами.*

Доказательство. Пусть $H \leq F$ — нециклическая группа разложения некоторого простого дивизора $\mathfrak{P}$ поля K, не делящего 2, и пусть $\Phi = H^2[H,H]$ — подгруппа Фраттини группы H. Тогда группа Галуа H/Φ расширения K^Φ/K^H — нециклическая группа порядка 4, и она является группой разложения простого дивизора $\mathfrak{p}$ поля K^Φ, делящегося на $\mathfrak{P}$. По предложению 6 расширение K/K^H универсально согласно периода 2^m; тогда по тому же утверждению универсально согласно периода 2^m и расширение K^Φ/K^H. Но оно не является даже универсально согласным периода 2. Действительно, пусть условие согласности выполняется для всех трех задач погружения расширения K^Φ/K^H с циклическим ядром порядка 2, указанных в формулировке леммы 1. Тогда эти задачи были бы разрешимы, как и любые задачи погружения с ядром простого порядка, и по лемме 1 группы разложения всех простых дивизоров поля K^Φ, не делящих 2, были бы циклическими. □

5. Погружение универсально согласного расширения в универсально согласное. Пусть F — 2-группа, и пусть (F', α) — расширение группы F с ядром порядка 2. Пусть $F_1, \ldots, F_r$ — все циклические подгруппы группы F, полные прообразы $\alpha^{-1}F_i$ которых — тоже циклические группы. Далее, пусть X — группа всех гомоморфизмов из F в двухэлементную группу $\{\pm 1\}$, ядра которых содержат все подгруппы F_i. Мы будем говорить, что для расширения групп (F, α) выполнено условие $\mathcal{E}_n$, если для любого гомоморфизма $\chi \in \mathrm{X}$ существует расширение (P_χ, γ_χ) группы F', такое что

(1) ядро γ_χ содержится в центре группы P_χ;

(2) элемент $f \in F$ действует тривиально на (автоматически абелевом) ядре C_χ расширения $(P_\chi, \alpha\gamma_\chi)$ группы F тогда и только тогда, когда $\chi(f) = 1$;

(3) период группы $\mathrm{Ker}\gamma_\chi$ делит 2^n;

(4) для гомоморфизма χ_0, отображающего всю группу F в 1, группа P_{χ_0} — циклическая группа порядка 4.

Теорема 1. *Пусть k — поле алгебраических чисел, а K/k — 2-расширение Галуа с группой Галуа F, универсально согласное периода 2^{n+1}. Далее, пусть $\alpha : F' \to F$ — эпиморфизм групп с ядром D порядка 2. Если 2 полностью раскладывается в K, и если для расширения групп (F, α) выполнено условие $\mathcal{E}_n$, то существует такое решение K' задачи погружения $(K/k, \alpha)$, что расширение K'/k универсально согласно периода 2^n.*

Доказательство. Мы построим некоторую задачу погружения, в любом решении которой содержится поле K', удовлетворяющее требованиям теоремы. Сначала построим несколько вспомогательных расширений группы F'. Пусть $F_1, \ldots, F_r$ — все подгруппы группы F, такие что для любого i полный прообраз $\alpha^{-1}F_i$ — циклическая группа, а $H_1, \ldots, H_l$ — все подгруппы порядка 2 группы F, не содержащиеся ни в одной из групп F_i.

(1) Для каждого i, $1 \le i \le r$, пусть ε_i — эпиморфизм циклической группы $\bar{F}_i$ порядка $2^{n+1}|F_i|$ на циклическую группу $\alpha^{-1}(F_i)$. Пусть $G_i \xrightarrow{\alpha_i} F'$ — перенесение расширения $(\bar{F}_i, \varepsilon_i)$ на всю группу F'. Обозначим через A_i ядро произведения $\alpha\alpha_i$.

(2) Пусть, как и в § 2, U — группа порядка 8 с образующими u, v, связанными соотношениями $u^{-1}vu = v^3$, $u^2 = v^4 = 1$. Для каждого j, $1 \le j \le l$, обозначим через $\delta_j : U \to \alpha^{-1}(H)$ эпиморфизм, такой что $\delta_j(v)$ — единственный неединичный элемент ядра $\mathrm{Ker}\alpha$, а $\delta_j(u) \notin \mathrm{Ker}\alpha$. Пусть $U_j \xrightarrow{\beta_j} F'$ — перенесение расширения (U, δ_j) на всю группу F'. Обозначим через B_i ядро произведения $\alpha\beta_j$.

(3) Поскольку выполняется условие $\mathcal{E}_n$, для каждого характера $\chi : F \to \{\pm 1\}$, ядро которого содержит все группы F_i, существует расширение (P_χ, γ_χ), удовлетворяющее описанным выше условиям; выше мы уже ввели для ядра гомоморфизма $\alpha\gamma_\chi$ обозначение C_χ.

Пусть теперь (G, φ') — произведение всех расширений (G_i, α_i), (U_j, β_j), (P_χ, γ_χ) группы F', и пусть $\varphi = \alpha\varphi'$. Обозначим через M', M ядра гомоморфизмов φ', φ. Теорема сразу вытекает из следующих утверждений.

Предложение 7. *Задача погружения $(K/k, G, \varphi)$ разрешима.*

Предложение 8. *Если L — решение задачи погружения $(K/k, G, \varphi)$, то $L^{M'}/k$ — универсально согласное периода 2^n решение задачи $(K/k, \alpha)$.*

□

6. Доказательство предложения 8. Обозначим поле $L^{M'}$ через K'; поле L является решением задачи погружения $(K'/k, \varphi')$, которая является произведением задач $(K'/k, \alpha_i)$, $(K'/k, \beta_j)$, $(K'/k, \gamma_\chi)$. По предложению 3 тогда разрешимы все задачи-«сомножители». В частности, для любого j разрешима задача $(K'/k, U_j, \beta_j)$, которая является перенесением задачи $(K'/K^{H_j}, V, \delta_j)$; по предложению 1 задача $(K'/K^{H_j}, V, \delta_j)$ тоже разрешима. Поскольку $H_1, \ldots, H_l$ — все подгруппы группы F, полные прообразы которых в F' — нециклические группы порядка 4, для расширения K'/k выполнено условие (4) предложения 4. Задача $(K'/k, \gamma_{\chi_0})$ тоже разрешима, а это означает выполнение условия (2) предложения 4. Условия (1) и (3) этого предложения выполняются для расширения K'/k, потому что K/k — универсально согласное расширение. Таким образом, расширение K'/k удовлетворяет всем требованиям предложения 4, и по этому предложению группы разложения всех дивизоров поля K', не делящих 2, циклические. Группы разложения делителей 2 являются подгруппами циклической группы второго порядка $\mathrm{Gal}(K'/K)$ и потому тоже циклические.

Пусть C — циклическая подгруппа группы F'. Если $C \supseteq \mathrm{Ker}\alpha$, то $C = \alpha^{-1}(F_i)$ для некоторого i, $1 \leq i \leq r$. Задача погружения расширения K'/K'^C в циклическое расширение порядка $2^n|C|$ разрешима, потому что разрешима являющаяся её перенесением на расширение (K'/k) задача $(K'/k, \alpha_i)$. Если же C не содержит $\mathrm{Ker}\alpha$, то группа $\alpha(C)$ изоморфна C. Для задачи погружения расширения $K/K^{\alpha(C)}$ в циклическое расширение степени $2^n|\alpha(C)| = 2^n|C|$ выполнено условие согласности, потому что K/k — универсально согласное расширение периода 2^{n+1}. В [5] доказано, что если 2 полностью раскладывается в погружаемом поле K, то согласность достаточна для разрешимости задачи с циклическим ядром. Поэтому существует такое поле $L \supset K$, что $L/K^{\alpha(C)}$ — циклическое расширение степени $2^n|C|$. Но тогда LK'/K'^C — тоже циклическое расширение степени $2^n|C|$. Итак, для любой циклической подгруппы C группы F' расширение K'/K'^C погружается в циклическое расширение степени $2^n|C|$. По следствию предложения 5 условие согласности выполняется для любой задачи погружения $(K'/k, \psi)$ с абелевым ядром периода 2^n, то есть расширение K'/k универсально согласно периода 2^n.

7. Доказательство предложения 7. Присоединим к полю K первообразный корень ζ степени 2^{n+1} из 1. Поскольку 2 полностью раскладывается в K, группа Галуа $\bar{F}$ расширения $K(\zeta)/k$ является прямым произведением группы $F = \mathrm{Gal}(K/k)$ и группы $S = \mathrm{Gal}(k(\zeta)/k)$. Последняя группа порождается двумя автоморфизмами s, t, отображающими ζ соответственно в ζ^{-1} и ζ^5. Обозначим через $\bar{G}$ прямое произведение $S \times G$, а через $\bar{\varphi}$ — эпиморфизм

$$1 \times \varphi : \bar{G} = S \times G \to S \times F = \bar{F}.$$

Хорошо известно (см. [2]), что задачи погружения $(K/k, \varphi)$ и $(K(\zeta)/k, \bar{\varphi})$ равносильны, поэтому достаточно доказать разрешимость второй задачи. Ядро обеих задач $\widetilde{M}$ — абелева группа периода 2^{n+1}; расширение K/k универсально согласно периода 2^{n+1}, поэтому для первой, а значит, и для второй задач погружения выполнено условие согласности. Дополнительное условие, гарантирующее существование решения для согласной задачи, было найдено в [6]; нам достаточно будет воспользоваться лишь следствием этого условия, которое в нашей ситуации принимает такой вид.

Предложение 9. *Пусть M — группа характеров ядра $\widetilde{M}$ задачи погружения $(K(\zeta)/k, \bar{\varphi})$, рассматриваемая как модуль над группой Галуа $\bar{F}$ расширения $K(\zeta)/k$. Пусть Π — множество всех простых дивизоров поля $K(\zeta)$; для любого дивизора $\mathfrak{P} \in \Pi$ обозначим через $\bar{F}_{\mathfrak{P}} \subset \bar{F}$ его группу разложения. Если условие согласности выполняется для задачи погружения $(K(\zeta)/k, \bar{\varphi})$ и если пересечение ядер всех гомоморфизмов ограничения*

$$r_{\mathfrak{P}} : H^1(\bar{F}, M) \to H^1(\bar{F}_{\mathfrak{P}}, M) \qquad (\mathfrak{P} \in \Pi)$$

является нулевой подгруппой группы когомологий $H^1(\bar{F}, M)$, то задача погружения $(K_1/k, \varphi_1)$ разрешима.

Всякая циклическая подгруппа группы Галуа является группой разложения некоторого простого дивизора. При наших предположениях группой разложения любого дивизора поля $K(\zeta)$, делящего 2, является группа $S = \mathrm{Gal}(k(\zeta)/k)$. Поэтому для доказательства предложения 7 достаточно доказать следующее утверждение.

Лемма 3 (**основная лемма**). *Если $x \in H^1(\bar{F}, M)$ — такой класс одномерных когомологий, что расщепляются его ограничения на S и на все циклические подгруппы группы F, то и сам класс x расщепляется.*

Доказательство этой леммы будет дано в следующем параграфе. А этот параграф мы завершим описанием $\bar{F}$-модуля M. Сначала выясним, как устроен F-модуль $\widetilde{M}$. Расширение (G, φ) является прямым произведением расширений (G_i, α_i), (U_j, β_j), (P_χ, γ_χ) группы F', то есть прямым произведением групп G_i, U_j, P_χ с объединенной факторгруппой F'. Поэтому $\widetilde{M} = \mathrm{Ker}\alpha\varphi$ — прямое произведение модулей $\widetilde{A}_i = \mathrm{Ker}\alpha\alpha_i$, $\widetilde{B}_j = \mathrm{Ker}\alpha\beta_j$, $\widetilde{C}_\chi = \mathrm{Ker}\alpha\gamma_\chi$ с объединенным фактормодулем $\mathrm{Ker}\alpha = \mathrm{Gal}(K'k)$. Группа S действует на $\widetilde{M}$ тривиально. Модуль $\widetilde{A}_i$ содержит подмодуль $\mathrm{Ker}\alpha_i$, изоморфный $(\mathbb{Z}/2^n\mathbb{Z})[F/F_i]$, фактормодуль по которому является группой порядка 2, и содержит элемент порядка 2^{n+1}, на который группа F_i действует тривиально. Модуль $\widetilde{B}_j$ содержит подмодуль $\mathrm{Ker}\beta_j$, изоморфный $(\mathbb{Z}/2\mathbb{Z})[F/H_j]$, фактормодуль по которому является группой порядка 2, и содержит H_j-инвариантную циклическую подгруппу порядка 4, на которой единственный неединичный элемент h_j группы H_j действует как возведение в третью степень. На модуле $\widetilde{C}_\chi$ ядро χ действует тривиально, но при $\chi \neq \chi_0$ вся группа F действует на нем нетривиально; при этом $\widetilde{C}_\chi$ содержит подмодуль $\mathrm{Ker}\gamma_\chi$ индекса 2, состоящий из F-инвариантных элементов.

Из этого описания модулей $\widetilde{M}$, $\widetilde{A}_i$, $\widetilde{B}_j$, $\widetilde{C}_\chi$ получается следующее описание их аддитивно записанных групп характеров M, A_i, B_j, C_χ.

Лемма 4. *Модули A_i, B_j — циклические $\mathbb{Z}[F]$-модули с образующими a_i, b_j и определяющими соотношениями*

$$
\begin{aligned}
2^{n+1}a_i = 0, \quad 2^n(f-1)a_i = 0, \quad f'a_i = a_i \quad &\text{для всех } f \in F,\ f' \in F_i, \\
4b_j = 0, \quad 2(f-1)b_j = 0, \quad h_j b_j = -b_j \quad &\text{для всех } f \in F.
\end{aligned}
$$

Модуль C_{χ_0} представляет собой циклическую группу порядка 4 с образующей c_{χ_0}, действие F на которую тривиально. При $\chi \neq \chi_0$ элемент $f \in F$ действует на C_χ тривиально тогда и только тогда, когда $\chi(f) = 1$; при этом существует элемент $c_\chi \in C_\chi$, такой что группа F действует тривиально на c_χ и на фактормодуле $\bar{C}_\chi = C_\chi/\langle c_\chi \rangle$. Модуль M как F-модуль является прямой суммой всех модулей A_i, B_j, C_χ с объединенным подмодулем

$$D = \langle 2^n a_i \rangle = \langle 2b_j \rangle = \langle 2c_{\chi_0} \rangle = \langle c_\chi \rangle \quad (\chi \neq \chi_0).$$

Группа S действует на модуле M нетривиально: элемент s действует как умножение на -1, а элемент t — как умножение на 5.

8. Доказательство основной леммы. Как мы знаем из леммы 4, модуль M — прямая сумма модулей A_i, B_j, C_χ с объединенным подмодулем. Пусть ν — канонический эпиморфизм на M прямой суммы

$$\bigoplus_{i=1}^{r} A_i \oplus \bigoplus_{j=1}^{l} B_j \oplus \bigoplus_{\chi\in\mathrm{X}} C_\chi.$$

Модуль M содержит подмодуль

$$D = 2^n\nu(A_i) = 2\nu(B_j) = 2\nu C_{\chi_0} = \nu(\langle c_\chi\rangle) \quad (\chi \neq \chi_0),$$

являющийся циклической группой порядка 2 с тривиальным действием операторов из $\bar{F}$, а фактормодуль M/C раскладывается в прямую сумму модулей $\bar{A}_i = \nu(A_i)$, $\bar{B}_j = \nu(B_j)$, $\bar{C}_\chi = \nu(C_\chi)$. Обозначим через

$$\xi : H^1(\bar{F}, D) \to H^1(\bar{F}, M), \qquad \rho : H^1(\bar{F}, M) \to H^1(\bar{F}, M/D)$$

гомоморфизмы групп когомологий, индуцированные вложением $D \to M$ и проекцией $M \to M/D$.

Лемма 5. *Пусть l_g $(g \in \bar{F})$ — 1-коцикл группы $\bar{F}$ со значениями в $\bar{F}$-модуле M/D, ограничения которого на группу S и на все циклические подгруппы группы F расщепляются. Тогда и коцикл l_g расщепляется.*

Доказательство. Модуль M/D — прямая сумма модулей $\bar{A}_i$, $\bar{B}_j$, $\bar{C}_\chi$; поэтому достаточно доказать утверждение для каждого из этих слагаемых. Оно очевидно для модулей $\bar{C}_\chi$. Действительно, если $f \in F$ и расщепляется ограничение коцикла l_f на циклическую группу, порожденную f, то существует элемент $z \in \bar{C}_\chi$, такой что $l_f = (f-1)z$. Но группа F действует на $\bar{C}_\chi$ тривиально, так что $l_f = (f-1)z = 0$. Далее, ограничение l_g на S расщепляется, так что существует элемент $u \in \bar{C}_\chi$, такой что $(s-1)u = l_s$, $(t-1)u = l_t$. Остается заметить, что и $(f-1)u = 0 = l_f$ для всех $f \in F$.

Докажем теперь утверждение для модулей $\bar{A}_i$ и $\bar{B}_j$. Как F-модуль каждый из этих модулей изоморфен модулю вида $R(F/H)$, где H — некоторая циклическая подгруппа F, а R — кольцо вычетов по модулю 2^n в случае модуля $\bar{A}_i$ и по модулю 2 в случае модуля $\bar{B}_j$. Пусть

$$r : H^1(F, R(F/H)) \to H^1(H, R(F/H))$$

— гомоморфизм ограничения. Как H-модуль R выделяется прямым слагаемым в $R(F/H)$; пусть $\theta : H^1(H, R(F/H)) \to H^1(H, R)$ — гомоморфизм групп когомологий, индуцированный проекцией $R(F/H)$ на это прямое слагаемое. Пусть $y \in H^1(F, R(F/H))$ — класс ограничения коцикла l_g на F. Поскольку H — циклическая группа, $ry = 0$; тогда $\theta ry = 0$. Но хорошо известно (см., например, [4]), что композиция θr является изоморфизмом; поэтому $y = 0$. Таким образом, ограничение коцикла l_g на F расщепляется, то есть найдется элемент $u \in R(F/H)$, такой что $l_f = fu - u$ для всех $f \in F$. Заменим коцикл l_g на гомологичный ему коцикл $l'_g = l_g - gu + u$; тогда $l'_f = 0$ для всех $f \in F$. Поскольку $s'f = fs'$ для всех $s' \in S$, $f \in F$, мы находим, что

$$fl'_{s'} = l'_f + fl'_{s'} = l'_{fs'} = l'_{s'f} = l'_{s'} + s'l'_f = l'_{s'}.$$

Таким образом, все элементы $l'_{s'}$ принадлежат группе $(R(F/H))^F$ F-инвариантных элементов модуля $R(F/H)$. Группа $(R(F/H))^F$ — прямое слагаемое группы, а потому и S-модуля $R(F/H)$. Ограничение $l'_{s'}$ коцикла l'_g на S расщепляется в $R(F/H)$; поэтому $l'_{s'}$ расщепляется уже в S-прямом слагаемом $(R(F/H))^F$ модуля $R(F/H)$, то есть существует элемент $v \in (R(F/H))^F$, такой что $l'_{s'} = s'v - v$ для всех $s' \in S$. Следовательно, для любого элемента $s'f \in SF = \bar{F}$

$$\begin{aligned} l_{s'f} &= l'_{s'f} + s'fu - u = l'_{s'} + s'l'_f + s'fu - u = s'v - v + s'fu - u = \\ &= s'fv - v + s'fu - u = s'f(u+v) - (u+v). \end{aligned}$$

□

Лемма 6. *Если f — элемент одной из групп F_i, то $D \cap (f-1)M = 0$.*

Доказательство. Более того,

$$\nu^{-1}(D) \cap (f-1)\left(\bigoplus_{i=1}^{r} A_i \oplus \bigoplus_{j=1}^{l} B_j \oplus \bigoplus_{\chi \in \mathrm{X}} C_\chi\right) = 0.$$

Действительно,

$$\nu^{-1}(D) \subseteq \bigoplus_{i=1}^{r} \langle 2^n a_i \rangle \oplus \bigoplus_{j=1}^{l} \langle 2b_j \rangle \oplus \bigoplus_{\chi \neq \chi_0} \langle c_\chi \rangle \oplus \langle 2c_{\chi_0} \rangle,$$

так что достаточно показать, что

$$2^n a_i \notin (f-1)A_i, \quad 2b_j \notin (f-1)B_j, \quad c_\chi \notin (f-1)C_\chi.$$

Но это так и есть. В самом деле, элемент $2^n a_i$ не принадлежит даже модулю IM, где I — идеал группового кольца $\mathbb{Z}[F]$, порожденного всеми элементами $f' - 1$, $f' \in F$. Далее, $(f-1)C_\chi = 0$, так как f принадлежит одной из групп F_i, а все эти группы содержатся в ядре χ. Остается рассмотреть случай модуля B_j. При наших предположениях в модуле B_j, рассматриваемом как F_i-модуль и тем более как $\langle f \rangle$-модуль, подмодуль, порожденный b_j, выделяется прямым слагаемым, причем фактормодуль этого слагаемого по $\langle 2b_j \rangle$ — свободный $R[\langle f \rangle]$-модуль. Поэтому если u — ненулевой элемент из этого прямого слагаемого, который под действием $f-1$ попадает в $\langle 2b_j \rangle$, то или $u \in \langle 2b_j \rangle$, или $u = (1 + f + \ldots + f^{h-1})b_j$, где h — порядок элемента f. В обоих случаях $(f-1)u = 0$. □

Мы можем теперь завершить доказательство леммы 3. Последовательность

$$H^1(\bar{F}, D) \xrightarrow{\xi} H^1(\bar{F}, M) \xrightarrow{\rho} H^1(\bar{F}, M/D)$$

точна. По предположению леммы ограничения x на группу S и на все циклические подгруппы группы F расщепляются в M. Это же верно и для коцикла ρx, и из леммы 5 следует, что $\rho x = 0$; поэтому $x \in \mathrm{Im}\xi$, а это означает, что в классе когомологий $x \in H^1(\bar{F}, M)$ есть такой коцикл m_g, что $m_g \in D$ для всех $g \in \bar{F}$. Пусть $f \in F$; поскольку ограничение m_g на циклическую группу, порожденную f, расщепляется, найдется такой элемент $u \in M$, что $m_f = (f-1)u$. Таким образом, $m_f \in D \cap (f-1)M = 0$, и значит, $m_f = 0$ для всех $f \in F$. Далее, ограничение m_g на S расщепляется, то есть существует элемент $v \in M$, такой что $m_s = (s-1)v = -2v$, $m_t = (t-1)v = 4v$. Но $2D = 0$, поэтому $4v = -2(s-1)v = -2m_s = 0$. Если $2v = 0$, то $l_s = l_t = 0$ и тогда $l_g = 0$ для всех $g \in SF = \bar{F}$. Если же $2v \neq 0$, то $0 \neq 2v = -(s-1)v = m_s \in D$, и $2v = 2c_{\chi_0}$, поскольку $2c_{\chi_0}$ — единственный ненулевой элемент в D. В этом случае

$$m_s = 2v = (s-1)c_{\chi_0}, \quad m_t = 0 = (t-1)c_{\chi_0},$$
$$m_f = 0 = (t-1)c_{\chi_0} \;\text{ для всех }\; f \in F.$$

Основная лемма доказана. Вместе с ней доказаны предложение 7 и теорема.

Литература

1. *Зяпков Н. П., Яковлев А. В.* Универсально согласные расширения Галуа // Записки научных семинаров ЛОМИ. Т. 71. 1977. С. 133–152.
2. *Ишханов В. В, Лурье Б. Б., Фаддеев Д. К.* Задача погруюения в теории Галуа. М.: Наука. Гл. ред. физ.-мат. лит., 1990. 269 с.
3. *Делоне Б. Н., Фаддеев Д. К.* Исследования по геометрии теории Галуа // Мат. сб. Т. 15(57). 1944, №2. С. 243–284.
4. *Cartan H., Eilenberg S.* Homological algebra. Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 1999. With an appendix by David A. Buchsbaum. Reprint of the 1956 original.
5. *Яковлев А. В.* О задаче погружения с циклическим ядром для числовых полей // Записки научных семинаров ПОМИ. Т. 400. 2012. С. 209–215.
6. *Яковлев А. В.* Задача погружения для числовых полей // Изв. АН СССР. Сер. мат. Т. 31. 1967, №2.

Статья поступила в редакцию 26 декабря 2013 г.

Сведения об авторах

Яковлев Анатолий Владимирович — доктор физико-математических наук, профессор; yakovlev.anatoly@gmail.com

ON THE EMBEDDING OF A UNIVERSALLY CONSISTENT 2-EXTENSION IN A UNIVERSALLY CONSISTENT EXTENSION

Anatoly V. Yakovlev

St.Petersburg State University, Universitetskaya nab., 7/9, St.Petersburg, 199034, Russian Federation; yakovlev.anatoly@gmail.com

A Galois extension is called universally consistent of the period q, if for any problem of embedding of this extension with an abelian kernel of the period q the consistency condition holds. Let K be a universally consistent extension of the period 2^{n+1} of an algebraic number field k, such that 2 completely splits in K, and let $(K/k, \varphi)$ be an embedding problem with the cyclic kernel of order 2. It is proved that (under some group-theoretical restrictions) there exists a solution of this embedding problem which is universally consistent of the period 2^n. Refs 6.

Keywords: Galois group, Galois embedding problem, consistency condition.