С. П. Демушкин, И. Р. Шафаревич, Второе препятствие для задачи погружения полей алгебраических чисел,
Изв. АН СССР. Сер. матем., 1962, том 26, выпуск 6, 911–924

ИЗВЕСТИЯ АКАДЕМИИ НАУК СССР
Серия математическая
26 (1962), 911—924

С. П. ДЕМУШКИН и И. Р. ШАФАРЕВИЧ

ВТОРОЕ ПРЕПЯТСТВИЕ ДЛЯ ЗАДАЧИ ПОГРУЖЕНИЯ ПОЛЕЙ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

В работе исследуется задача погружения полей алгебраических чисел в поля с большей группой Галуа. Вычисляется второе препятствие к разрешимости задачи погружения.

Рассматривается задача погружения нормального над Ω поля k с группой F в большее поле K с группой G над Ω, причем поле K должно быть таким, чтобы естественный гомоморфизм

$$G = \mathfrak{G}(K/\Omega) \to \mathfrak{G}(k/\Omega) = F$$

группы Галуа поля на группу Галуа подполя совпадал с предписанным гомоморфизмом $\varphi : G \to F$. Такую задачу погружения будем записывать в виде $(k/\Omega, G, \varphi)$. Как и в работе [1], будем считать, что ядро A гомоморфизма $\varphi : G \to F$ есть абелева группа и что корни степени m (период группы A) из единицы содержатся в k. Кроме того, так как задача погружения редуцируется к задаче погружения с p-группами [см. [3]], то мы всюду будем предполагать, что G — p-группа.

Некоторые необходимые условия для разрешимости задачи погружения, условия согласности, были открыты Д. К. Фаддеевым [4].

В удобной для нас форме они приведены в работе [1]. Мы эти условия называем первым препятствием. Далее всюду предполагается, что первое препятствие для задачи $(k/\Omega, G, \varphi)$ исчезает.

Задачу погружения мы решаем последовательными шагами. В A выбираем F-инвариантный ряд

$$A \supset A_1 \supset \ldots \supset A_i \supset \ldots \supset 1$$

с $[A_i : A_{i+1}] = p$ (так как G — p-группа, то такой ряд выбрать можно). Затем решаем задачу $(k/\Omega, G/A_1, \varphi)$, которая разрешима, так как является сопутствующей для задачи $(k/\Omega, G, \varphi)$. Пусть k^1 — решение задачи $(k/\Omega, G/A_1, \varphi)$. Спрашивается, когда поле k^1 можно выбрать так, что для задачи $(k^1/\Omega, G, \varphi_1)$ первое препятствие исчезает? Инварианты, которые дают ответ на этот вопрос, мы называем вторым препятствием для задачи погружения. В неявном виде второе препятствие дано в работе [1]. В настоящей работе второе препятствие находится для случая, когда k — поле алгебраических чисел.

§ 1. Задача согласования циклических алгебр; построение инвариантов

Так как все результаты, о которых будет идти речь в дальнейшем, относятся к случаю, когда погружаемое поле k является полем алгебраических чисел, то мы и будем предполагать с самого начала, что k — именно такое поле. Нас будет интересовать второе препятствие для задачи погружения, т. е. инварианты, позволяющие ответить на вопрос, когда существует такое решение k^1 задачи погружения $(k/\Omega, G/A_1, \bar{\varphi})$, что для задачи $(k^1/\Omega, G, \varphi_1)$ исчезает первое препятствие. Как известно из работы [1], второе препятствие определяется набором циклических алгебр над подполями поля k, задаваемых характерами группы A_1. Для нас не будет важна эта зависимость циклических алгебр от характеров группы A_1, поэтому в обозначениях алгебр мы исключаем их зависимость от характеров.

Итак, пусть задано конечное число циклических алгебр

$$C_i = (\alpha_i, \beta_i)_{k_i} \qquad (k_i \subset k).$$

Спрашивается, когда в поле Ω существует такое число m, что все алгебры C_i представляются в виде $C_i \approx (\alpha_i, m)_{k_i}$ для всех i? Если такое число существует, то второе препятствие исчезает; если числа m не существует, то второе препятствие не исчезает.

Мы видим, что задача отыскания второго препятствия для задачи погружения сводится к некоторой задаче о циклических алгебрах. Последней задачей мы и будем заниматься. Сформулируем ее.

Задача согласования циклических алгебр. Задано конечное число алгебраических p-расширений $\{k_i\}$ поля алгебраических чисел Ω и над каждым таким полем k_i задана циклическая алгебра $C_i = (\alpha_i, \beta_i)_{k_i}$ степени p. Каковы условия того, что все алгебры C_i одновременно представляются в виде

$$C_i \approx (\alpha_i, m)_{k_i}, \quad m \in \Omega?$$

Необходимые условия для разрешимости задачи согласования циклических алгебр легко указать. Это локальные условия: для любого простого дивизора $\mathfrak{p}$ поля Ω должно существовать такое число $m_\mathfrak{p} \in \Omega_\mathfrak{p}$ ($\Omega_\mathfrak{p}$ — замыкание Ω по $\mathfrak{p}$), что

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i}\right)_{k_i} = \left(\frac{\alpha_i, m_\mathfrak{p}}{\mathfrak{P}_i}\right)_{k_i}$$

для всех i и всех делителей $\mathfrak{P}_i$ дивизора $\mathfrak{p}$ в поле k_i. Здесь, как и в дальнейшем,

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i}\right)_{k_i}$$

обозначает символ норменного вычета в точке $\mathfrak{P}_i$.

ЛЕММА 1. *Для циклических алгебр* $\{C_i\}$, *возникших из задачи погружения, выполняются локальные условия для их согласования.*

Доказательство. Пусть $(k/\Omega, G, \varphi)$ — задача погружения, из которой возникают алгебры $\{C_i\}$, $\mathfrak{p}$ — простой дивизор поля Ω, $\mathfrak{P}_i$ — его делители в поле k_i. Нам нужно доказать существование такого числа $m_\mathfrak{p} \in \Omega_\mathfrak{p}$, что

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i}\right)_{k_i} = \left(\frac{\alpha_i, m_\mathfrak{p}}{\mathfrak{P}_i}\right)_{k_i}$$

для всех i и $\mathfrak{P}_i \mid \mathfrak{p}$, если алгебры $\{C_i\}$ возникли из задачи погружения. Выясним сначала, что означают локальные условия для алгебр $\{C_i\}$ с точки зрения задач погружения. Мы утверждаем, что локальные условия эквивалентны тому, что для задачи погружения $P_\mathfrak{p} = (k_\mathfrak{p}/\Omega_\mathfrak{p}, G, \varphi)$, где $k_\mathfrak{p}$ — алгебра, получающаяся из k/Ω расширением Ω до $\Omega_\mathfrak{p}$, исчезает второе препятствие.

Действительно, из исчезновения первого препятствия для задачи погружения $P = (k/\Omega, G, \varphi)$ следует исчезновение его для задачи $P_\mathfrak{p}$. Алгебры C_i $(P_\mathfrak{p})$ эквивалентны алгебрам $(\alpha_i, \beta_i)_{k_{i\mathfrak{p}}}$, так как переход от задачи P к задаче $P_\mathfrak{p}$ получается расширением Ω до $\Omega_\mathfrak{p}$. Если для задачи $P_\mathfrak{p}$ исчезает второе препятствие, то существует такое число $m_\mathfrak{p} \in \Omega_\mathfrak{p}$, что все алгебры C_i $(P_\mathfrak{p})$ представляются в виде

$$C_i\,(P_\mathfrak{p}) \approx (\alpha_i, m_\mathfrak{p})_{k_{i\mathfrak{p}}}.$$

Остается заметить, что распадение алгебры над центром, являющимся прямой суммой подалгебр (в нашем случае подполей), эквивалентно тому, что распадаются компоненты алгебры над соответствующими компонентами центра. Так как $k_{i\mathfrak{p}}$ является прямой суммой полей $k_{i\mathfrak{P}_i}$, то представление

$$(\alpha_i, \beta_i)_{k_{i\mathfrak{p}}} \approx (\alpha_i, m_\mathfrak{p})_{k_{i\mathfrak{p}}}$$

эквивалентно тому, что

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i}\right)_{k_i} = \left(\frac{\alpha_i, m_\mathfrak{p}}{\mathfrak{P}_i}\right)_{k_i}$$

для всех i и $\mathfrak{P}_i \mid \mathfrak{p}$.

Следовательно, для доказательства леммы достаточно показать, что для задачи погружения $P_\mathfrak{p}$ исчезает второе препятствие. Мы покажем больше, а именно, что задача погружения $P_\mathfrak{p}$ разрешима. Таким образом, речь идет о доказательстве следующего утверждения: для разрешимости задачи погружения $(k/\Omega, G, \varphi)$, где Ω — локальное поле и k — алгебра, достаточно исчезновения первого препятствия. Применить здесь прямо теорему 4 работы [1] нельзя, так как там все рассуждения велись для случая, когда k — поле.

Пусть

$$k = \sum k e^{\sigma_j}$$

— разложение алгебры k в прямую сумму полей ke^{σ_j} и H — подгруппа F, действующая в нормальном поле $\varkappa = ke$. Тогда имеет место разложение

$$F = \sum H\sigma_j.$$

Рассмотрим задачу погружения $(\varkappa/\Omega, \varphi^{-1}H, \varphi)$. Для такой задачи первое препятствие исчезает, поэтому она разрешима по основной теореме работы ([1]). Пусть $\mathcal{K}$ — решение этой задачи. Рассмотрим алгебру

$$K = \sum \mathcal{K} e^{\bar{\sigma}_j},$$

являющуюся прямой суммой алгебр, изоморфных $\mathcal{K}$. Здесь $\bar{\sigma}_j$ — прообразы элементов σ_j в G. Группа G представляется в виде

$$G = \sum \varphi^{-1}H\bar{\sigma}_j.$$

Определим действие элементов группы G в K по формуле:

$$(\alpha e^{\bar{\sigma}_j})^{h\bar{\sigma}_i} = \alpha^{h_1} e^{\bar{\sigma}_l},$$

если

$$\bar{\sigma}_j h \bar{\sigma}_i = h_1 \bar{\sigma}_l.$$

Легко видеть, что получающееся представление будет регулярным и что алгебра K является решением задачи погружения $(k/\Omega, G, \varphi)$.

Лемма доказана.

Ввиду леммы 1, для нахождения второго препятствия в задаче погружения нам достаточно ответить на следующий вопрос. Пусть для системы C_i циклических алгебр выполнены локальные условия для их согласования; когда систему алгебр C_i можно согласовать? К этому вопросу мы и переходим.

Рассмотрим в поле Ω совокупность чисел b, обладающих свойством: для любого простого дивизора $\mathfrak{p}$ из Ω число b в $\Omega_\mathfrak{p}$ представляется в виде

$$b = \prod_{i,\ \mathfrak{P}_i \mid \mathfrak{p}} (N_{\mathfrak{P}_i}\alpha_i)^{b_{\mathfrak{P}_i}} \lambda^p, \tag{1}$$

где $N_{\mathfrak{P}_i}$ — норма из поля $k_i\mathfrak{P}_i$ в поле $\Omega_\mathfrak{p}$, $b_{\mathfrak{P}_i}$ — некоторые целые числа и $\lambda \in \Omega_\mathfrak{p}$.

Числа b с таким свойством будем называть корневыми. Произведение двух корневых чисел снова будет корневым числом.

Отметим, что корневыми будут, например, все нормы $N_{k_i|\Omega}\alpha_i$, так как такая норма всегда разлагается в произведение локальных норм.

Пусть $\{b\}$ — подгруппа мультипликативной группы поля Ω, порожденная корневыми числами b.

ЛЕММА 2. *Фактор-группа* $\{b\}/\Omega^{*p}$ *конечна.*

Доказательство. Рассмотрим нормальную оболочку полей k_i $(\sqrt[p]{\alpha_i})$. Пусть это будет поле k'. Оно будет конечным расширением поля Ω, так как число алгебр C_i конечно.

Для доказательства леммы достаточно показать, что

$$\Omega(\sqrt[p]{b}) \subset k'.$$

В свою очередь, для доказательства последнего включения достаточно установить, что любой простой дивизор $\mathfrak{p}$ из Ω, полностью разлагающийся в k', полностью разлагается в $\Omega(\sqrt[p]{b})$. Покажем, что для такого дивизора $\mathfrak{p}$ число b является p-й степенью в $\Omega_{\mathfrak{p}}$. Действительно, α_i являются p-ми степенями в $k_i\mathfrak{P}_i$:

$$\alpha_i = A_i^p, \quad A_i \in k_i\mathfrak{P}_i,$$

поэтому

$$b = \prod_{i,\ \mathfrak{P}_i|\mathfrak{p}} (N_{\mathfrak{P}_i}\alpha_i)^{b\mathfrak{P}_i} \lambda^p = \Big[\prod_{i,\ \mathfrak{P}_i|\mathfrak{p}} (N_{\mathfrak{P}_i}A_i)^{b\mathfrak{P}_i}\lambda\Big]^p.$$

Лемма доказана.

Каждому корневому числу b поставим в соответствие выражение:

$$I(b) = \prod_{\mathfrak{p},\ i,\ \mathfrak{P}_i|\mathfrak{p}} \left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i}\right)_{k_i}^{b\mathfrak{P}_i},$$

где $b_{\mathfrak{P}_i}$ получаются из представления (1).

Функции $I(b)$ будем называть корневыми для задачи согласования циклических алгебр $\{C_i\}$.

ЛЕММА 3. *Если циклические алгебры $\{C_i\}$ удовлетворяют локальным условиям для их согласования, то корневая функция $I(b)$ не зависит от способа представления числа b в виде* (1).

Доказательство. Пусть имеются два представления числа b:

$$b = \prod_{i,\ \mathfrak{P}_i|\mathfrak{p}} (N_{\mathfrak{P}_i}\alpha_i)^{b\mathfrak{P}_i} \lambda_{\mathfrak{p}}^p$$

и

$$b = \prod_{i,\ \mathfrak{P}_i|\mathfrak{p}} (N_{\mathfrak{P}_i}\alpha_i)^{b'\mathfrak{P}_i} \lambda_{\mathfrak{p}}'^p.$$

Тогда

$$1 = \prod_{i,\ \mathfrak{P}_i|\mathfrak{p}} (N_{\mathfrak{P}_i}\alpha_i)^{b\mathfrak{P}_i - b'\mathfrak{P}_i} (\lambda_a/\lambda_{\mathfrak{p}}')^p$$

и достаточно показать, что $I(1) = 1$ для любого представления единицы.

Пусть

$$1 = \prod_{i,\ \mathfrak{P}_i|\mathfrak{p}} (N_{\mathfrak{P}_i}\alpha_i)^{n\mathfrak{P}_i} \nu_{\mathfrak{p}}^n.$$

Тогда, используя основные свойства символа норменного вычета и то, что алгебры $\{C_i\}$ удовлетворяют локальным условиям для их согласова-

ния, получаем:

$$I(1) = \prod_{\mathfrak{p},\, i\mathfrak{P}_i|\mathfrak{p}} \left(\frac{\alpha_i,\, \beta_i}{\mathfrak{P}_i}\right)_{k_i}^{n\mathfrak{P}_i} = \prod_{\mathfrak{p},\, i,\, \mathfrak{P}_i|\mathfrak{p}} \left(\frac{\alpha_i,\, m_{\mathfrak{p}}}{\mathfrak{P}_i}\right)_{k_i}^{n\mathfrak{P}_i} =$$

$$= \prod_{\mathfrak{p},\, i,\, \mathfrak{P}_i \,|\, \mathfrak{p}} \left(\frac{N_{\mathfrak{P}_i}\alpha_i,\, m_{\mathfrak{p}}}{\mathfrak{p}}\right)_{\Omega}^{n\mathfrak{P}_i} = \left(\frac{\prod\limits_{i,\, \mathfrak{P}_i \,|\, \mathfrak{p}} (N_{\mathfrak{P}_i}\alpha_i)^{n\mathfrak{P}_i},\, m_{\mathfrak{p}}}{\mathfrak{p}}\right)_{\Omega} = \prod_{\mathfrak{p}} \left(\frac{v_{\mathfrak{p}}^{-p},\, m_{\mathfrak{p}}}{\mathfrak{p}}\right)_{\Omega} = 1.$$

Лемма доказана.

Так как значение $I(b)$ зависит лишь от класса, в который попадает b в $\{b\}/\Omega^{*p}$, то корневых функций имеется только конечное число. Легко проверить, что относительно корневых чисел корневые функции ведут себя мультипликативно, т. е.

$$I(b_1 b_2) = I(b_1)\, I(b_2).$$

§ 2. Основные теоремы

ТЕОРЕМА 1. *Для разрешимости задачи согласования циклических алгебр, удовлетворяющих локальным условиям, необходимо и достаточно обращение в* 1 *всех корневых функций.*

Доказательство. Пусть задача согласования циклических алгебр разрешима, т. е.

$$\left(\frac{\alpha_i,\, \beta_i}{\mathfrak{P}_i}\right)_{k_i} = \left(\frac{\alpha_i,\, m}{\mathfrak{P}_i}\right)_{k_i}, \quad m \in \Omega,$$

при всех i и $\mathfrak{P}_i \,|\, \mathfrak{p}$ в k_i, и $I(b)$ — корневая функция:

$$I(b) = \prod_{\mathfrak{p},\, i,\, \mathfrak{P}_i \,|\, \mathfrak{p}} \left(\frac{\alpha_i,\, \beta_i}{\mathfrak{P}_i}\right)_{k_i}^{b\mathfrak{P}_i},$$

$$b = \prod_{i,\, \mathfrak{P}_i \,|\, \mathfrak{p}} (N_{\mathfrak{P}_i}\alpha_i)^{b\mathfrak{P}_i}\, \lambda_{\mathfrak{p}}^{p}.$$

Тогда, используя основные свойства символа норменного вычета, получаем:

$$I(b) = \prod_{\mathfrak{p},\, i,\, \mathfrak{P}_i \,|\, \mathfrak{p}} \left(\frac{\alpha_i,\, \beta_i}{\mathfrak{P}_i}\right)_{k_i}^{b\mathfrak{P}_i} = \prod_{\mathfrak{p},\, i,\, \mathfrak{P}_i \,|\, \mathfrak{p}} \left(\frac{\alpha_i,\, m}{\mathfrak{P}_i}\right)_{k_i}^{b\mathfrak{P}_i} =$$

$$= \prod_{\mathfrak{p},\, i,\, \mathfrak{P}_i \,|\, \mathfrak{p}} \left(\frac{N_{\mathfrak{P}_i}\alpha_i,\, m}{\mathfrak{p}}\right)_{\Omega}^{b\mathfrak{P}_i} = \prod_{\mathfrak{p}} \left(\frac{\prod\limits_{i,\, \mathfrak{P}_i \,|\, \mathfrak{p}} (N_{\mathfrak{P}_i}\alpha_i)^{b\mathfrak{P}_i},\, m}{\mathfrak{p}}\right)_{\Omega} =$$

$$= \prod_{\mathfrak{p}} \left(\frac{b\lambda_{\mathfrak{p}}^{-p},\, m}{\mathfrak{p}}\right) = \prod_{\mathfrak{p}} \left(\frac{b,\, m}{\mathfrak{p}}\right)_{\Omega} = 1.$$

Таким образом, необходимость условия теоремы доказана. Переходим к доказательству его достаточности.

Пусть $\mathfrak{M}$ — подгруппа идеальных элементов $m = \{m_\mathfrak{p}\}$, для которых

$$\left(\frac{\alpha_i, m_\mathfrak{p}}{\mathfrak{P}_i}\right)_{k_i} = 1$$

при всех i и $\mathfrak{P}_i \mid \mathfrak{p}$. Рассмотрим также подгруппу $\mathfrak{N} = \mathfrak{M}\, m$, $m \in \Omega$. По условию теоремы, существует идеальный элемент

$$\overline{m_0} = \{m_{0\mathfrak{p}}\},$$

для которого

$$\left(\frac{\alpha_i, \beta_i}{\mathfrak{P}_i}\right)_{k_i} = \left(\frac{\alpha_i, m_{0\mathfrak{p}}}{\mathfrak{P}_i}\right)_{k_i}$$

при всех i и $\mathfrak{P}_i \mid \mathfrak{p}$. Для доказательства теоремы нужно, следовательно, показать, что $\overline{m_0} \in \mathfrak{N}$.

Заметим, что подгруппа $\mathfrak{N}$ является допустимой подгруппой [см. (2)]. Для того чтобы убедиться в этом, обозначим через S конечное множество дивизоров в Ω, являющихся либо делителями p, либо такими, что их делители в k_i разветвляются в k_i $(\sqrt[p]{\alpha_i})$. Тогда $\mathfrak{N}$ будет содержать множество идеальных элементов A_S (группа A_S определяется как множество идеальных элементов $\overline{n} = \{n_\mathfrak{p}\}$, для которых $n_\mathfrak{p} = 1$, если $\mathfrak{p} \in S$, и $n_\mathfrak{p}$ — $\mathfrak{p}$-адическая единица, если $\mathfrak{p} \notin S$).

Допустимая подгруппа характеризуется тем, что все ее элементы ортогональны к некоторой конечной совокупности чисел из Ω [см. (2)]. Пусть $b_1, b_2, \ldots, b_r$ — такие числа для $\mathfrak{N}$. Покажем, что они являются корневыми числами. Для этого в качестве $\overline{m} = \{m_\mathfrak{p}\}$ возьмем элемент, для которого $m_\mathfrak{p}$ произвольно при фиксированном $\mathfrak{p}$ и $m_\mathfrak{q} = 1$ при $\mathfrak{q} \neq \mathfrak{p}$. Тогда условие

$$\left(\frac{\alpha_i, m_\mathfrak{p}}{\mathfrak{P}_i}\right)_{k_i} = 1$$

для всех i и $\mathfrak{P}_i|\mathfrak{p}$ будет означать, что

$$(N_{\mathfrak{P}_i}, \alpha_i m_\mathfrak{p})_{\Omega_\mathfrak{p}} \approx 1,$$

т. е. что $m_\mathfrak{p}$ ортогонально конечной совокупности чисел из $\Omega_\mathfrak{p}$. Для числа же b_l должно быть

$$[b_l, \overline{m}] = 1,$$

т. е.

$$(b_l, m_\mathfrak{p})_{\Omega_\mathfrak{p}} \approx 1.$$

Так как ортогональное дополнение к ортогональному дополнению совпадает с первоначальной группой, то

$$b_l = \prod_{i,\ \mathfrak{P}_i \mid \mathfrak{p}} (N_{\mathfrak{P}_i} \alpha_i)^{b_{\mathfrak{P}_i}} \lambda_\mathfrak{p}^p.$$

Поэтому числа $b_1, b_2, \ldots, b_r$ корневые.

Чтобы закончить доказательство теоремы, достаточно показать, что элемент $\overline{m}_0 = \{m_{0\mathfrak{p}}\}$ ортогонален ко всем корневым числам. Пусть

$$b = \prod_{i,\, \mathfrak{P}_i | \mathfrak{p}} (N_{\mathfrak{P}_i} \alpha_i)^{b_{\mathfrak{P}_i}} \lambda_{\mathfrak{p}}^{p}, \quad \lambda_{\mathfrak{p}} \in \Omega_{\mathfrak{p}}.$$

Тогда имеем:

$$[b, \overline{m}_0] = \prod_{\mathfrak{p}} \left(\frac{b,\, m_{0\mathfrak{p}}}{\mathfrak{p}}\right)_{\Omega} = \prod_{\mathfrak{p}} \left(\frac{\prod\limits_{i,\, \mathfrak{P}_i | \mathfrak{p}} (N_{\mathfrak{P}_i} \alpha_i)^{b_{\mathfrak{P}_i}} \lambda_{\mathfrak{p}}^{p},\, m_{0\mathfrak{p}}}{\mathfrak{p}} \right)_{\Omega} =$$

$$= \prod_{\mathfrak{p},\, i,\, \mathfrak{P}_i | \mathfrak{p}} \left(\frac{N_{\mathfrak{P}_i} \alpha_i,\, m_{0\mathfrak{p}}}{\mathfrak{p}}\right)_{\Omega}^{b_{\mathfrak{P}_i}} = \prod_{\mathfrak{p},\, i,\, \mathfrak{P}_i | \mathfrak{p}} \left(\frac{\alpha_i,\, m_{0\mathfrak{p}}}{\mathfrak{P}_i}\right)_{k_i}^{b_{\mathfrak{P}_i}} =$$

$$= \prod_{\mathfrak{p},\, i,\, \mathfrak{P}_i | \mathfrak{p}} \left(\frac{\alpha_i,\, \beta_i}{\mathfrak{P}_i}\right)_{k_i}^{b_{\mathfrak{P}_i}} = I(b) = 1$$

(по условию). Теорема доказана.

Пусть, как и прежде, k' обозначает нормальную над Ω оболочку полей k_i $(\sqrt[p]{\alpha_i})$. Обозначим через $g(\mathfrak{p})$, где $\mathfrak{p}$ — простой дивизор в Ω, число делителей $\mathfrak{p}$ в поле k'.

ТЕОРЕМА 2. *Если общий наибольший делитель чисел* $g(\mathfrak{p})$, $\mathfrak{p} \in \Omega$, *равен единице, то циклические алгебры* $\{C_i\}$, *которые удовлетворяют локальным условиям, всегда можно согласовать.*

Для доказательства теоремы достаточно показать, что все корневые выражения в указанном случае равны 1. Так как мы рассматриваем задачу согласования циклических алгебр C_i над полями k_i, являющимися p-расширениями поля Ω, то и k' будет p-расширением Ω. Поэтому из того, что общий наибольший делитель чисел $g(\mathfrak{p})$ равен единице, следует, что существует простой дивизор $\mathfrak{p}_0$ поля Ω, для которого $g(\mathfrak{p}_0) = 1$, т. е. $\mathfrak{p}_0$ имеет лишь один делитель $\mathfrak{P}_0$ в k'.

Пусть b — корневое число. Докажем, что $I(b) = 1$. Для этого рассмотрим равенство (1), определяющее число b в точке $\mathfrak{p}_0$:

$$b = \prod_{i,\, \mathfrak{P}_{0i} | \mathfrak{p}_0} (N_{\mathfrak{P}_{0i}} \alpha_i)^{b_{\mathfrak{P}_{0i}}} \lambda_0^{p}, \quad \lambda_0 \in \Omega_{\mathfrak{p}_0}.$$

Так как у $\mathfrak{p}_0$ имеется единственный делитель в k', то делитель $\mathfrak{P}_{0i}$ в поле k_i тоже будет один. Кроме того, группа разложения дивизора $\mathfrak{P}_0$ будет совпадать со всей группой $\mathfrak{G}(k'/\Omega)$ и локальные нормы $N_{\mathfrak{P}_{0i}}$ будут совпадать с обычными нормами из полей k_i в Ω. Поэтому в точке $\mathfrak{p}_0$ мы получаем равенство:

$$b = \prod_i (N_{k_i | \Omega} \alpha_i)^{n_i} \lambda_0^{p}$$

(числа $b_{\mathfrak{P}_{0i}}$ обозначены здесь через n_i). Рассмотрим число b из основного поля:

$$b' = b \Big/ \prod_i (N_{k_i|\Omega}\alpha_i)^{n_i}.$$

Оно является корневым, так как все числа $N_{k_i|\Omega}\,\alpha_i$ корневые. Число b является p-й степенью в $\Omega_{\mathfrak{p}_0}$:

$$b' = \lambda_0^p.$$

Покажем, что оно является p-й степенью и в Ω. Действительно, пусть $b' \neq u^p$, $u \in \Omega$. Тогда поле $\Omega\,(\sqrt[p]{b'})$ будет промежуточным между Ω и k' (из доказательства леммы 2 следует, что $\Omega\,(\sqrt[p]{b'})$ является подполем поля k'):

$$\Omega \in \Omega\,(\sqrt[p]{b'}) \subset k'.$$

Перейдя в этой цепочке полей к замыканию по $\mathfrak{P}_0$, получим:

$$\Omega_{\mathfrak{p}_0} = \Omega\,(\sqrt[p]{b'})_{\mathfrak{p}_0} \subset k'_{\mathfrak{P}_0},$$

что противоречит тому, что

$$[k'_{\mathfrak{P}_0} : \Omega_{\mathfrak{p}_0}] = [k' : \Omega]$$

при $g\,(\mathfrak{p}_0) = 1$. Следовательно,

$$b' = u^p, \quad u \in \Omega.$$

Но u^p является корневым числом, для которого $I\,(u^p) = 1$. Поэтому

$$I\,(b) = \prod_i I\,(N_{k_i|\Omega}\,\alpha_i)^{n_i},$$

и достаточно проверить, что

$$I\,(N_{k_i|\Omega}\,\alpha_i) = 1.$$

Напишем для этого разложение $N_{k_i|\Omega}\,\alpha_i$ в произведение локальных норм:

$$N_{k_i|\Omega}\,\alpha_i = \prod_{\mathfrak{P}_i|\mathfrak{p}} N_{\mathfrak{P}_i}\alpha_i.$$

Значит, $b_{\mathfrak{P}_i} = 1$, $b_{\mathfrak{P}_j} = 0$ для $j \neq i$. В таком случае

$$I\,(N_{k_i|\Omega}\,\alpha_i) = \prod_{\mathfrak{p},\, j,\, \mathfrak{P}_j|\mathfrak{p}} \left(\frac{\alpha_j,\, \beta_j}{\mathfrak{P}_j}\right)_{k_j}^{b_{\mathfrak{P}_j}} = \prod_{\mathfrak{p},\, \mathfrak{P}_i|\mathfrak{p}} \left(\frac{\alpha_i,\, \beta_i}{\mathfrak{P}_i}\right)_{k_i} = 1$$

(по закону взаимности). Теорема доказана.

Следствие 1. *Если трехмерная группа когомологий*

$$H^3\,(\mathfrak{G}\,(k'/\Omega),\, k'^*) = 1,$$

то алгебры $\{C_i\}$, *удовлетворяющие локальным условиям, всегда можно согласовать.*

Для доказательства достаточно заметить, что для полей алгебраических чисел трехмерная группа когомологий является циклической и порядок ее равен наибольшему общему делителю чисел $g\,(\mathfrak{p})$, $\mathfrak{p} \in \Omega$.

Следствие 2. *Если поле k' циклическое над Ω, то алгебры $\{C_i\}$, удовлетворяющие локальным условиям, всегда можно согласовать.*

Для доказательства достаточно заметить, что в случае, когда поле k' циклическое над Ω, трехмерная группа когомологий $H^3(\mathfrak{G}(k'/\Omega), k'^*)$ будет единичной или что по закону плотностей Чеботарева в Ω существует простой дивизор $\mathfrak{p}$, принадлежащий образующему элементу группы $\mathfrak{G}(k'/\Omega)$, а тогда для такого $\mathfrak{p}$ имеем:

$$g(\mathfrak{p}) = 1.$$

Приведем результаты, относящиеся к задаче погружения $(k/\Omega, G, \varphi)$ поля алгебраических чисел k, непосредственно вытекающие из теоремы 2 и ее следствий.

Пусть дана группа характеров $\mathfrak{A}$ нормального делителя A в задаче погружения. Тогда фактор-группа F естественно отображается в группу автоморфизмов группы $\mathfrak{A}$. Обозначим через F' ядро этого отображения, через k' — подполе, принадлежащее F' в k, через $g(\mathfrak{p})$ — число делителей в k' простого дивизора $\mathfrak{p}$ в Ω.

ТЕОРЕМА 3. *Если общий наибольший делитель чисел $g(\mathfrak{p})$, $\mathfrak{p} \in \Omega$, равен 1, то исчезновение первого препятствия для задачи погружения $(k/\Omega, G, \varphi)$ поля алгебраических чисел k достаточно для ее разрешимости.*

Для доказательства достаточно заметить, что при переходе к задаче погружения $(k^1/\Omega, G, \varphi_1)$ условие теоремы сохраняется.

Следствие 1. *Если трехмерная группа когомологий*

$$H^3(F/F', k'^*) = 1,$$

то исчезновение первого препятствия для задачи погружения $(k/\Omega, G, \varphi)$ поля алгебраических чисел k достаточно для ее разрешимости.

Следствие 2. *Если фактор-группа F индуцирует в группе характеров нормального делителя циклическую группу автоморфизмов, то исчезновение первого препятствия для задачи погружения $(k/\Omega, G, \varphi)$ поля алгебраических чисел k достаточно для ее разрешимости.*

С помощью результатов работы ([3]) легко получить, что теорема 3 и следствия из нее будут справедливы и для случая, когда G не является p-группой.

Замечание. Хотя доказательства следствий 1 и 2 арифметические, формулировка их чисто алгебраическая. Интересно было бы выяснить, не справедливы ли эти следствия для произвольного поля k. Гипотеза о том, что это имеет место, подтверждается случаем, когда k — локальное поле. В этом случае трехмерных гомологий нет и, действительно, исчезновение первого препятствия достаточно для погружаемости.

§ 3. Пример

Рассмотрим пример на вычисление второго препятствия (этот пример взят из работы ([5])).

Пусть нормальный делитель A в задаче погружения $(k/\Omega, G, \varphi)$ — циклическая группа восьмого порядка: $A = \{\alpha\}$. Мы можем предполагать, что любой дивизор $\mathfrak{p}$ из Ω имеет в поле k', которое было определено

в предыдущем параграфе, либо два, либо четыре делителя (см. теорему 3). Это, в частности, означает, что фактор-группа F индуцирует в группе характеров группы A нециклическую группу автоморфизмов. Но группа автоморфизмов группы A является произведением двух циклических групп второго порядка. Следовательно, группа F должна порождать всю эту группу автоморфизмов и поэтому поле k' имеет вид:

$$k' = \Omega\ (\sqrt{a},\ \sqrt{b}).$$

Сделаем в задаче погружения $(k/\Omega,\ G,\ \varphi)$ первый шаг. Нормальным делителем после первого шага будет

$$A_1 = \{\alpha^2\}.$$

У него имеются два существенных для нас характера χ_1 и χ_2:

$$\chi_1(\alpha^2) = -1,$$
$$\chi_2(\alpha^2) = i.$$

Пусть x_1 и x_2 — продолжения характеров χ_1 и χ_2 на A. Ясно, что всегда

$$F_{x_2} \subset F_{\chi_2},$$
$$F_{x_1} \subset F_{\chi_1} = F,$$
$$F_{\chi_2} \subset F_{\chi_1} = F, \quad F_{x_2} \subset F_{x_1}$$

и что индексы всех написанных подгрупп равны либо 1, либо 2. Нетрудно проверить, что в рассматриваемом случае все эти индексы равны 2. Будем считать, что

$$k_{x_1} = \Omega\ (\sqrt{a}) \quad [k_{x_2} = \Omega\ (\sqrt{a},\ \sqrt{b})],$$
$$k_{\chi_2} = \Omega\ (\sqrt{a}) \quad [k_{\chi_1} = \Omega\,].$$

Поэтому

$$\alpha_{x_2} = b,$$
$$\alpha_{x_1} = a.$$

Число a будет корневым, но второго препятствия оно дать не может, так как является нормой от $\alpha_{x_1} = a$.

Докажем, что число b тоже будет корневым. Для этого нужно, чтобы

$$b \approx a^{i_\mathfrak{p}} \prod_{\mathfrak{P}_i \mid \mathfrak{p}} (N_{\mathfrak{P}_i} b)^{i_{\mathfrak{P}_i}} \text{ в } \Omega_\mathfrak{p}. \tag{2}$$

Знак $\approx$ означает 2-равенство, т. е. равенство с точностью до квадратов. Так как норма $N_{\mathfrak{P}_i} b$ всегда будет равна b или b^2 независимо от делителя $\mathfrak{P}_i$ дивизора $\mathfrak{p}$, то мы будем брать в 2-равенстве (2) только один из делителей дивизора $\mathfrak{p}$:

$$b \approx a^{i_\mathfrak{p}} N_\mathfrak{p} b^{j_\mathfrak{p}} \tag{2'}$$

($N_\mathfrak{p} b$ обозначает здесь норму $N_{\mathfrak{P}_i} b$ для одного из делителей $\mathfrak{P}_i$ дивизора $\mathfrak{p}$). Если $a \approx 1$ в $\Omega_\mathfrak{p}$, то

$$N_\mathfrak{p} b = b$$

и поэтому в 2-равенстве (2′) нужно взять $i_\mathfrak{p} = 0$, $j_\mathfrak{p} = 1$. Если $a \not\approx 1$ в $\Omega_\mathfrak{p}$, то

$$N_\mathfrak{p} b = b^2 \approx 1.$$

Поэтому при $b \approx 1$ нужно взять $i_\mathfrak{p} = 0$, а при $b \not\approx 1$ должно быть $b \approx a$ $(i_\mathfrak{p} = 1)$, т. е. $ab \approx 1$. Последнее соотношение выполняется, так как в противном случае степень $[\Omega_\mathfrak{p}(\sqrt{a}, \sqrt{b}) : \Omega_\mathfrak{p}]$ была бы равна 4, а это означало бы, что у $\mathfrak{p}$ в поле k' имеется только один делитель.

Следовательно, мы получаем такое представление числа b в виде (2′):

1) $b \approx 1$ в $\Omega_\mathfrak{p}$; $i_\mathfrak{p} = 0$, $j_\mathfrak{p} = 0$;

2) $b \not\approx 1$, но $a \approx 1$ в $\Omega_\mathfrak{p}$; $i_\mathfrak{p} = 0$, $j_\mathfrak{p} = 1$;

3) $b \not\approx 1$ и $a \not\approx 1$ в $\Omega_\mathfrak{p}$; $i_\mathfrak{p} = 1$, $j_\mathfrak{p} = 0$.

Так как мы предполагаем, что первое препятствие для нашей задачи исчезает, то алгебры C_{χ_1} и C_{χ_2} будут иметь вид:

$$C_{\chi_1} \approx (a, \beta_{\chi_1})_\Omega,$$
$$C_{\chi_2} \approx (b, \beta_{\chi_2})_{\Omega(\sqrt{a})}.$$

Значит, корневая функция $I(b)$ представляется следующим образом:

$$I(b) = \prod_\mathfrak{p} \left(\frac{a, \beta_{\chi_1}}{\mathfrak{p}}\right)^{i_\mathfrak{p}} \prod_\mathfrak{p} \left(\frac{b, \beta_{\chi_2}}{\mathfrak{p}}\right)^{j_\mathfrak{p}}_{\Omega(\sqrt{a})}.$$

Здесь через

$$\left(\frac{b, \beta_{\chi_2}}{\mathfrak{p}}\right)_{\Omega(\sqrt{a})}$$

обозначен символ норменного вычета

$$\left(\frac{b, \beta_{\chi_2}}{\mathfrak{P}_i}\right)_{\Omega(\sqrt{a})}$$

для одного из делителей $\mathfrak{P}_i$ дивизора $\mathfrak{p}$.

Рассмотрим теперь числовой пример. Пусть погружаемое поле $k = R(\sqrt{c}, \sqrt{2}, i)$, где R — поле рациональных чисел. Группа Галуа F поля k/R является прямым произведением групп

$$F_1 = \mathfrak{G}(k_1/R), \quad k_1 = R(\sqrt{c}),$$

и

$$F_2 = \mathfrak{G}(k_2/R), \quad k_2 = R(\sqrt{2}, i).$$

Пусть $G = G_1 \times F_2$, где

$$G_1 = \{\alpha, \beta;\ \alpha^8 = 1, \beta^2 = \alpha^4,\ \beta^{-1}\alpha\beta = \alpha^7\}$$

и $\varphi: G \to \mathfrak{G}(k/R)$ — гомоморфное отображение группы G на $\mathfrak{G}(k/R)$, задаваемое таким образом: $\varphi(\alpha) = 1$, $\varphi(\beta)$ — образующий элемент группы F_1 и φ на F_2 является изоморфизмом. Тогда мы имеем задачу погружения $(k/R, G, \varphi)$ с циклическим нормальным делителем восьмого порядка, порождаемым элементом α. Поле k содержит корни восьмой степени из единицы, так как $\sqrt{2} \in k$ и $i \in k$.

Необходимым и достаточным условием исчезновения первого препятствия для такой задачи является распадение циклической алгебры

$$C_0 = (-1, -1)_{R(\sqrt{-c}, \sqrt{2})}.$$

Распадение алгебры C_0 означает, что в поле $R(\sqrt{-c}, \sqrt{2})$ разрешимо уравнение

$$x^2 + y^2 + z^2 = 0.$$

Поле k' будет в данном случае равно $R(\sqrt{-c}, \sqrt{2})$, причем

$$k_{\chi_1} = R(\sqrt{-c}).$$

Для того чтобы в поле $R(\sqrt{-c}, \sqrt{2})$ не исчезал трехмерный коцикл (чтобы число 2 было корневым), должно выполняться такое условие: если $-c \not\equiv 1$ в R_p, то либо $2 \approx 1$, либо $-2c \approx 1$ в R_p. Для задачи, которую мы сейчас рассматриваем, алгебры C_{χ_1} и C_{χ_2}, получающиеся после первого шага (построения поля $k^1 = R(\sqrt{\mu}, \sqrt{c}, \sqrt{2}, i)$, где μ — произвольное число из R), будут иметь вид:

$$C_{\chi_1} \approx (\mu, -c)_R;$$

$$C_{\chi_2} \approx (2, \mu)_{R\sqrt{-c}} \otimes (-1, -1)_{R(\sqrt{-c})}.$$

Значит, корневая функция $I(2)$ будет выражаться следующим образом:

$$I(2) = \prod_p \left(\frac{\mu, -c}{p}\right)_R^{i_p} \prod_p \left(\frac{2, \mu}{p}\right)_{R(\sqrt{-c})}^{j_p} \prod_p \left(\frac{-1, -1}{p}\right)_{R\sqrt{-c})}^{j_p}.$$

Мы знаем, что корневая функция не зависит от числа μ, поэтому в выражении $I(2)$ можно взять $\mu = 1$. Кроме того,

$$\left(\frac{-1, -1}{p}\right)_{R(\sqrt{-c})} = 1$$

для всех $p \neq 2$. Поэтому

$$I(2) = \prod_p \left(\frac{1, -c}{p}\right)_R^{i_p} \prod_p \left(\frac{(2,1}{p}\right)_{R(\sqrt{-c})}^{j_p} \left(\frac{-1, -1}{2}\right)_{R(\sqrt{-c})}^{j_2} = \left(\frac{-1,-1}{2}\right)_{R(\sqrt{-c})}^{j_2}.$$

Для того чтобы не исчезало второе препятствие, необходимо и достаточно выполнение следующих условий:

$$\left(\frac{-1, -1}{2}\right)_{R(\sqrt{-c})} = -1 \quad \text{и} \quad j_2 = 1.$$

Покажем, что если за c взять любое произведение простых чисел вида $16n + 7$, то для задачи погружения $(k/R, G, \varphi)$ будут выполнены все перечисленные выше условия.

Для такой задачи первое препятствие исчезает, так как $-c \equiv 1 \pmod 8$, $-c$ является квадратом в R_2 и уравнение $x^2 + y^2 + z^2 = 0$ разрешимо в $R_2(\sqrt{2})$. Решением последнего уравнения будут, например,

$$x = -1 + \sqrt{-c} + (1 + (\sqrt{-c})\sqrt{2},$$

$$y = -1 - \sqrt{-c} + (-1 + \sqrt{-c})\sqrt{2},$$

$$z = \sqrt{6(c-1)}.$$

Легко видеть, что корень из числа $6(c-1)$ извлекается.

Далее, выполняется условие того, что степень

$$[R_p(\sqrt{-c}, \sqrt{2}) : R_p] < 4$$

для любого простого числа p. В самом деле, если $p = 2$, то $-c \approx 1$ в R_2; если $p|c$, то $\left(\frac{2}{p}\right) = 1$ и $2 \approx 1$ в R_p; если $p \neq 2$, не делит c и

$$\left(\frac{2}{p}\right) = -1, \quad \left(\frac{-c}{p}\right) = -1,$$

то

$$\left(\frac{-2c}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-c}{p}\right) = 1$$

и $-2c \approx 1$ в R_p.

В то же время уравнение $x^2 + y^2 + z^2 = 0$ неразрешимо в R_2. Это означает, что

$$\left(\frac{-1, -1}{2}\right)_{R_2} = -1.$$

Кроме того, $j_2 = 1$, так как $2 \not\approx 1$ в R_2 и $-c \approx 1$ в R_2.

Таким образом, для задачи погружения $(R(\sqrt{c}, \sqrt{2}, i)/R, G, \varphi)$ при условии, что c имеет лишь простые делители вида $16n + 7$, второе препятствие не исчезает. Следовательно, эта задача погружения неразрешима.

Поступило
1.VIII.1961

ЛИТЕРАТУРА

[1] Демушкин С. П. и Шафаревич И. Р., Задача погружения для локальных полей, Известия Ак. наук СССР, серия матем., 23 (1959), 823—840.
[2] Вейль Г., Алгебраическая теория чисел, ИЛ, М., 1947.
[3] Kochendörffer R., Zwei Reduktionssätze zum Einbettungsproblem für Abelsche Algebren, Math. Nachr., 10, № 1—2 (1953), 75—84.
[4] Делоне Б. Н. и Фаддеев Д. К., Исследования по геометрии теории Галуа, Матем. сборн., 15 (57):2 (1944), 243—276.
[5] Фаддеев Д. К., Об одной гипотезе Хассе, Доклады Ак. наук СССР, 94, № 6 (1954), 1013—1016.