Записки научных
семинаров ПОМИ
Том 272, 2000 г.

Б. Б. Лурье

УСЛОВИЕ СОГЛАСНОСТИ ФАДДЕЕВА–ХАССЕ В ПРОБЛЕМЕ ПОГРУЖЕНИЯ ПОЛЕЙ

Условие согласности впервые появилось в работе [1] как необходимое условие разрешимости задачи погружения. Д. К. Фаддеев дает там три его эквивалентные формулировки и находит важные частные случаи, когда оно обеспечивает погружаемость. Другую формулировку этого условия (при коммутативном ядре) открыл Х. Хассе ([2]). Он предположил, что это условие является для погружаемости и достаточным. Эту гипотезу в 1954 опровергли Д. К Фаддеев и И. Р. Шафаревич ([3, 4]), построив совершенно различные контрпримеры.*

В дальнейшем условие согласности (в иной терминологии – первое препятствие) играло важную роль в работах С. П. Демушкина и И. Р. Шафаревича ([5, 6]). В [5] доказано, что для задачи погружения с локальными полями при абелевом ядре это условие гарантирует погружаемость. В [6] исследуется "второе препятствие", т.е. некоторое дополнительное необходимое (но не достаточное) условие погружаемости для полей алгебраических чисел (при абелевом ядре).

Полностью задачу погружения с абелевым ядром решил А. В. Яковлев. В [7] найдено дополнительное условие погружаемости, которое при выполнении условия согласности не только необходимо, но и достаточно для погружаемости. В [8] задача погружения специализируется для числовых полей и оказывается, что во многих важных случаях дополнительное условие погружаемости несущественно, т.е. условия погружаемости и согласности совпадают. Условие согласности играет важную роль также в исследованиях А. В. Яковлева по изучению группы Галуа алгебраического замыкания локальных полей ([9]) и по

Работа выполнена при финансовой поддержке фонда РФФИ (грант No. 00-01-00116а).

*Гипотеза Хассе выглядит очень правдоподобно. Д. К. Фаддеев рассказывал, что одно время тоже верил в ее справедливость, но поостерегся выдвинуть ее в печати.

обратной задаче теории Галуа ([10]), где вводится класс универсально согласных полей.

Указанные работы прояснили суть условия согласности и его роль в задаче погружения в случае коммутативного ядра. В этом случае условие согласности сравнительно легко проверяется и достаточно сильное.

Сложнее, естественно, обстоит дело в случае задачи погружения с неабелевым ядром. Условие согласности при неабелевом ядре, как правило, более слабое, но его непосредственная проверка значительно труднее.

Удовлетворительный ответ на вопрос, что представляет собой условие согласности, содержится в настоящей статье, представляющей завершающий этап исследования по данной проблематике.

В работе [11] доказана редукционная теорема, позволяющая сводить условие согласности при p-ядре к случаю, когда и погружаемое поле является p-расширением основного. Важный результат содержится в работе [12], где условие согласности для числовых полей при неабелевом ядре сводится к проверке этого условия для абелева ядра (полученного факторизацией ядра по коммутанту). При этом для общих (не числовых) полей этот результат неверен.

Возникла гипотеза, что условие согласности в произвольном случае эквивалентно условию согласности с p-группами. В работе [13] эта гипотеза доказана для многих частных случаев. Полное доказательство публикуется здесь впервые.

Мне приятно отметить, что интерес к данной проблематике был стимулирован беседами с А. В. Яковлевым, и он всегда проявлял живой интерес к моим исследованиям.

§1. Постановка задачи и необходимые определения

Задаче погружения посвящена книга [14]. Одна из ее глав состоит в подробном исследовании условия согласности. Здесь дается лишь конспективное изложение, дающее возможность автономного чтения статьи.

Пусть задано (конечное) расширение Галуа K/k полей с группой Галуа F и определен эпиморфизм φ конечной группы G на F с ядром A. Задача погружения (записываемая $(K/k, G, \varphi)$) состоит в нахождении поля (алгебры Галуа) L, содержащего поле K и имеющего группу G над k, такого, что автоморфизмы $g \in G$, ограниченные на K, совпадают с автоморфизмами $\varphi(g) \in F = \mathrm{Gal}\,(K/k)$. Вместо явной конструкции поля (алгебры) L частно ограничиваются условиями существования такого расширения. $A = \operatorname{Ker}\varphi$ называется ядром задачи погружения. Как известно, поле (алгебра) L, если оно существует, обладает A-нормальным базисом над K (и G-нормальным базисом над k).

Ослабим теперь требования к искомому объекту L. Будем называть *модулем согласности* для нашей задачи погружения $(K/k, G, \varphi)$ линейное пространство P над K, содержащее K, на котором действуют k-автоморфизмы $g \in G$ такие, что $g|_K$ совпадает с $\varphi(g) \in \mathrm{Gal}\,(K/k)$, и P обладает A-нормальным базисом над K, т.е. $P = \oplus_{a \in A} K \mathrm{v}^{a}$, где $\mathrm{v} \in P$. Условие существования такого модуля согласности P называется *условием согласности*. Если задача погружения имеет решение L, то L и является таким модулем согласности. Поэтому условие согласности необходимо для существования решения задачи погружения (погружаемости).

Определим теперь для поля K и группы G скрещенное произведение $G \times K$, играющее ключевую роль в работе.

Пусть, как и прежде, K/k – расширение Галуа, и задано отображение $\varphi : G \to \mathrm{Gal}\,(K/k)$. Построим алгебру над K с базисом $\{u_g\}$, занумерованным элементами $g \in G$ и с умножением $u_g x \cdot u_h y = u_{gh} x^{\varphi(h)} y$, где $g, h \in G$, $x, y \in K$. Такая алгебра называется скрещенным произведением группы G и поля K и обозначается $G \times K$. Когда φ – изоморфизм, получаем классическое скрещенное произведение с единичными факторами, которое, как известно, изоморфно матричной алгебре над полем k порядка, равного $[K : k]$. Кроме того, алгебра $G \times K$ содержит подалгебру, натянутую на элементы u_a, $a \in A = \operatorname{Ker}\varphi$, которая является групповой алгеброй $K[A]$. Элементы $g \in G$ действуют как автоморфизмы на $K[A]$ посредством сопряжения.

Алгебра $G \times K$ – ассоциативная конечномерная алгебра. Она является полупростой в том и только в том случае, когда полупроста групповая алгебра $K[A]$, т.е. когда характеристика поля k не делит порядок группы A.

Дадим еще одно определение. Для задачи погружения $(K/k, G, \varphi)$ будем называть *системой согласности* набор элементов $l_g \in K[A]$, $g \in G$, для которых

1) $l_{g_1 g_2} = l_{g_1}^{g_2} l_{g_2}$ $(g_1, g_2 \in G)$

2) $l_a = u_a^{-1}$ для $a \in A$.

Эти равенства показывают, что l_g – обратимые элементы $K[A]$ (т.к. $l_{g^{-1}}^g l_g = u_1$ – единица алгебры) и тем самым l_g – одномерный коцикл на G со значениями в мультипликативной группе $K[A]$.

Теорема 1.1 (впервые доказана в [1], см. также [14]). *Для задачи погружения $(K/k, G, \varphi)$ следующие условия эквивалентны:*

1. *Существует модуль согласности.*
2. *Существует система согласности.*
3. *Скрещенное произведение $G \times K$ изоморфно алгебре матриц порядка $(K : k)$ над некоторой своей подалгеброй.*

Тем самым, каждое из этих условий может служить формулировкой условия согласности. Заметим, что проверка условия (3) проще, чем проверка других условий, а импликации (3)$\Longrightarrow$(1) или (3)$\Longrightarrow$(2) опираются на теорему Крулля–Шмидта и поэтому не всегда конструктивны.

Рассмотрим теперь случай коммутативного ядра A. Расширение G в этом случае определяется, как известно, каноническим классом из $H^2(F, A)$ (представитель которого – коцикл расширения). При наличии системы согласности этот элемент из $H^2(F, A)$ распадается в $H^2(F, (K[A])^*)$. Верно и обратное – если коцикл расширения есть кограница в $(K[A])^*$, существует система согласности для нашей задачи погружения. Это – еще одна формулировка условия согласности (приведенные рассуждения справедливы и для некоммутативного ядра; однако в этом случае когомологии не образуют группу, и A не является F-модулем).

Условие согласности в форме Хассе требует дополнительных определений.

§2. Сопутствующие, равносильные и присоединенные задачи

Задачу погружения $(K_1/k_1, G_1, \varphi_1)$ называют *сопутствующей* для задачи $(K/k, G, \varphi)$, если разрешимость первой необходима для разрешимости второй. Рассмотрим некоторые приемы, приводящие к сопутствующим задачам.

1. Пусть задача погружения связана с точной последовательностью групп

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

и A_0 – подгруппа A, нормальная в G. Тогда определен эпиморфизм $\varphi_1 : G/A_0 \longrightarrow F$ с ядром A/A_0, и с задачей погружения $(K/k, G, \varphi)$ можно связать задачу погружения $(K/k, G_1, \varphi_1)$. Ясно, что решение L задачи $(K/k, G, \varphi)$ порождает решение L^{A/A_0} задачи погружения $(K/k, G_1, \varphi_1)$ так что она – сопутствующая для исходной. Такую задачу называют *сопутствующей первого рода.*

В частности, если A_0 – коммутант ядра A, получают *сопутствующую абелеву* задачу погружения.

Можно несколько обобщить понятие сопутствующей задачи первого рода. Именно, пусть ψ – произвольный морфизм (не обязательно сюръективный) $G \longrightarrow G_1$ такой, что $\varphi_1\psi = \varphi$ (где φ_1 – эпиморфизм $G_1 \longrightarrow F$). Разрешимость задачи погружения $(K/k, G, \varphi)$ гарантирует в этом случае по-прежнему разрешимость задачи $(K/k, G_1, \varphi_1)$, если искать решение в классе алгебр Галуа ([14], гл. 1). Морфизм ψ является композицией сюръективного морфизма $G \longrightarrow \operatorname{Im}\psi$ и инъективного $\operatorname{Im}\psi \longrightarrow G_1$.

2. Зададим в $F = \operatorname{Gal}(K/k)$ подгруппу F_1. Определим G_1 как полный прообраз φ в G. Обозначим через φ_1 ограничение φ на G_1 и через k_1 – подполе поля K, отвечающее подгруппе F_1. Задача погружения $(K/k_1, G_1, \varphi_1)$, очевидно, разрешима, если разрешима исходная задача $(K/k, G, \varphi)$. Задача погружения $(K/k_1, G_1, \varphi_1)$ называется *сопутствующей задачей второго рода* для исходной.

Можно рассмотреть композицию двух таких процедур (сперва сопутствующую задачу второго, а затем первого рода). Так получается смешанная сопутствующая задача погружения.

3. Пусть K/k – расширение Галуа полей алгебраических чисел с группой Галуа F, и $\mathfrak{p}$ – простой дивизор поля k. Обозначим через $k_\mathfrak{p}$ пополнение поля k по дивизору $\mathfrak{p}$, а через $K_\mathfrak{p}$ – тензорное произведение $K \otimes_k k_\mathfrak{p}$. $K_\mathfrak{p}$ может не быть полем (если продолжение $\mathfrak{p}$ на K не единственно), но является алгеброй Галуа, а над алгеброй Галуа задача погружения также может быть поставлена. Полученная задача $(K_\mathfrak{p}/k_\mathfrak{p}, G, \varphi)$ называется *локальной сопутствующей* задачей погружения для исходной.

Рассмотрим теперь процедуру подъема. Пусть задача погружения связана с точной последовательностью

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

где $F = \operatorname{Gal}(K/k)$, и задано расширение Галуа L/k с группой H, содержащее K. Тем самым, определено сюръективное отображение $\psi : H \longrightarrow F$. Рассмотрим прямое произведение $\overline{G}$ групп G и H с объединенной факторгруппой F (т.е. множество пар (g, h), где $g \in G$, $h \in H$, $\varphi g = \psi h$). Имеет место коммутативная диаграмма с точными строками (здесь $B = \operatorname{Ker} \psi$)

$$\begin{tikzcd}
 & & 1 \arrow[d] & 1 \arrow[d] & \\
 & & B \arrow[r, phantom, "="] \arrow[d] & B \arrow[d] & \\
1 \arrow[r] & A \arrow[r] \arrow[d, equal] & \bar{G} \arrow[r, "\bar{\varphi}"] \arrow[d, "\bar{\psi}"'] & H \arrow[r] \arrow[d, "\psi"] & 1 \\
1 \arrow[r] & A \arrow[r] & G \arrow[r, "\varphi"] \arrow[d] & H \arrow[r] \arrow[d] & 1. \\
 & & 1 & 1 &
\end{tikzcd}$$

Говорят, что задача погружения $(L/k, \overline{G}, \bar{\varphi})$ получена из задачи $(K/k, G, \varphi)$ *подъемом* до L.

Обратная процедура называется спуском. Она возможна, если в G содержится нормальная подгруппа B, чье пересечение с ядром A тривиально. Тогда $\varphi(B) \approx B = \operatorname{Gal}(K/K_1)$, где K_1 – расширение Галуа k с группой $F_1 = F/B$, и можно рассмотреть задачу погружения $(K_1/k, G/B, \varphi_1)$, где φ_1 индуцировано отображением φ.

Задача погружения, полученная из исходной посредством подъема (спуска), эквивалентна исходной, т.е. они разрешимы (неразрешимы) одновременно (см. [14], гл. 1, §13).

Введем теперь понятие присоединенной задачи погружения. Пусть, как и прежде, задача погружения связана с точной последовательностью

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

и в G задана подгруппа G_1, отображающаяся на F при морфизме φ. Обозначим через φ_1 ограничение φ на G_1 и через A_1 ядро φ_1 (т.е. $A_1 = A \cap G_1$). Задача погружения $(K/k, G_1, \varphi_1)$ называется *присоединенной задачей погружения* для задачи $(K/k, G, \varphi)$.

Как мы видели, задача $(K/k, G, \varphi)$ – сопутствующая для задачи $(K/k, G_1, \varphi_1)$. Поэтому разрешимость задачи $(K/k, G_1, \varphi_1)$ гарантирует разрешимость $(K/k, G, \varphi)$, т.е. погружаемость присоединенной задачи погружения *достаточна* для погружаемости исходной.

Рассмотрим важный частный случай присоединенной задачи погружения. Пусть K/k является p-расширением. Рассмотрим в G силовскую p-подгруппу G_p (напомним, что она определена с точностью до сопряженности). Полученная присоединенная задача $(K/k, G_p)$ называется *силовской присоединенной задачей погружения*.

Теорема 2.1. *Условие согласности для всех указанных сопутствующих задач погружения – необходимое условие согласности в исходной задаче. Условия согласности для задач, полученных посредством подъема (спуска) эквивалентны. Условие согласности для присоединенной задачи погружения достаточно для согласности в исходной задаче.*

Доказательство см. в [14]. Заметим, что содержательным здесь является лишь доказательство выполнения условия согласности при спуске. Все остальные доказательства совершенно элементарны.

§3. Условие согласности в форме Хассе

Введем понятие брауэровской задачи погружения. Пусть ядро A задачи погружения – циклическая группа порядка n, характеристика поля k не делит n, и поле K содержит первообразный корень степени n из 1 (этого всегда можно добиться посредством подъема к круговому расширению поля K). Тогда определен инъективный морфизм $\chi : A \longrightarrow K^*$. Задача погружения называется в этом случае *брауэровской*, если морфизм χ является F-операторным, т.е. $\chi(a^f) = (\chi(a))^f$ для любых $a \in A$, $f \in F$).

Теорема Брауэра (см. [14], гл. 3, §1) утверждает, что такая задача погружения разрешима в том и только в том случае, если для нее выполнено условие согласности. Более того, по системе согласности конструируются все решения брауэровской задачи погружения.

Пусть теперь ядро A – произвольная абелева группа, характеристика поля k не делит порядок A, и поле K содержит первообразный корень из 1 степени, равной показателю A. Группа $\hat{A} = \mathrm{Hom}(A, K^*)$ в этом случае абстрактно изоморфна A. Рассмотрим произвольный характер $\chi \in \hat{A}$. Обозначим через F_χ подгруппу группы F, для элементов которой $\chi^f = \chi$, т.е. верны равенства $\chi(a^f) = (\chi(a))^f$ $(a \in A)$, через k_χ – подполе поля K, отвечающее подгруппе F_χ, через A_χ ядро χ, через G_χ – полный прообраз F_χ в G. Тогда имеется точная последовательность

$$1 \longrightarrow A/A_\chi \longrightarrow G_\chi/A_\chi \xrightarrow{\varphi_\chi} F_\chi \longrightarrow 1$$

и задача погружения $(K/k_\chi, G_\chi/A_\chi, \varphi_\chi)$ является брауэровской (A/A_χ – циклическая, ибо вкладывается в K^*).

Теорема 3.1 (Хассе). *Для того, чтобы при указанных предположениях выполнялось условие согласности для задачи погружения* $(K/k, G, \varphi)$ *необходимо и достаточно, чтобы для любого* $\chi \in \hat{A} = \mathrm{Hom}(A, K^*)$ *выполнялось условие согласности для брауэровских задач* $(K/k_\chi, G_\chi/A_\chi, \varphi_\chi)$.

(Доказательство см. в [14], гл. 3, §3.)

Разумеется, достаточно проверять условие согласности не для всех характеров χ, а лишь для образующих группы $\hat{A}$.

Таким образом, для абелева ядра получаем еще одну форму условия согласности – разрешимость всех сопутствующих брауэровских задач (когда поле K содержит корень из 1 достаточно высокой степени). Это и есть условие согласности в форме Хассе.

Итак, в случае абелева ядра проверка условия согласности выглядит довольно просто.

§4. Строение скрещенного произведения

Здесь излагаются результаты статьи [12] (см. также [14], гл. 2, §§8, 9).

Строение алгебры $G \times K$ тесно связано со строением групповой алгебры $K[A]$, где A – ядро отображения $\varphi : G \longrightarrow F = \mathrm{Gal}(K/k)$. Будем считать, что характеристика поля k не делит порядок A, и поле K содержит первообразный корень из 1 степени, равной показателю A. Этого всегда можно добиться процедурой подъема. Тогда все неприводимые представления $K[A]$ абсолютно неприводимы (иначе говоря, алгебра $K[A]$ – прямая сумма матричных алгебр над K).

Пусть μ – неприводимое представление $K[A]$ и e – соответствующий идемпотент, d – степень представления. Идемпотент e не всегда центральный в скрещенном произведении $G \times K$. Пусть G_e – централизатор идемпотента e в группе G (при этом, разумеется, $A \subset G_e$). Центральным в $G \times K$ будет идемпотент $E = \sum_\rho e^{\bar{\rho}}$, где $\{\rho\}$ – смежные классы G по G_e, а $\bar{\rho}$ – их представители в G. Обозначим $F_e = \varphi(G_e) \subset F$, пусть k_e – подполе K, принадлежащее подгруппе F_e. Алгебра $(G \times K)E$ – неприводимая компонента скрещенного произведения. Легко проверяется, что $(G \times K)E$ – матричная алгебра над алгеброй $(G_e \times K)e$, определенной над полем k_e, порядка $[G : G_e]$. Таким образом, осталось исследовать структуру простых алгебр $(G_e \times K)e$.

Теорема 4.1. *Существует двумерный коцикл $c_{f_1,f_2} \in Z^2(F_e, K^*)$ такой, что алгебра $(G_e \times K)e$ – матричная порядка d над скрещенным произведением поля K и группы $F_e = \mathrm{Gal}(K/k_e)$ с системой факторов c_{f_1,f_2}. Когда μ – одномерное представление, в качестве c_{f_1,f_2} можно взять $\mu(h_{f_1,f_2})$, где h – коцикл расширения $1 \longrightarrow A/A' \longrightarrow G/A' \longrightarrow F_e \longrightarrow 1$ (A' – коммутант A).*

С каждым неприводимым представлением μ степени $d > 1$ можно связать одномерное представление μ_0 – определитель матрицы порядка d, задаваемой представлением μ.

Теорема 4.2. *В приведенных обозначениях коцикл $c^d_{f_1,f_2} \in Z^2(F_e, K^*)$ гомологичен коциклу $\mu_0(h_{f_1,f_2})$, где $h_{f_1,f_2} \in Z^2(F_e, A/A')$ – ограничение коцикла расширения $1 \longrightarrow A/A' \longrightarrow G/A' \longrightarrow F \longrightarrow 1$ на F_e.*

Заметим, что коцикл c_{f_1,f_2} может быть непосредственно вычислен по модулю леммы Шура ([16]).

Теоремы 4.1 и 4.2 доказаны в [12], см. также [14], гл. 2.

Из теоремы 4.1 вытекает следующий важный критерий условия согласности: для каждого неприводимого представления алгебры $K[A]$ степени d с идемпотентом e скрещенное произведение поля K и группы F_e с системой факторов c_{f_1,f_2} должно быть изоморфно алгебре матриц порядка $|F_e|/\delta$, где δ – наибольший общий делитель d и $|F_e|$, над некоторой подалгеброй.

Для произвольной простой центральной алгебры Λ над полем k можно определить две арифметические характеристики: индекс Λ как корень квадратный из размерности содержащегося в Λ тела (над которым Λ – матричная алгебра) и показатель алгебры Λ в группе Брауэра $\mathrm{Br}k$ (т.е. наименьшее натуральное число l, для которого тензорная l-ая степень Λ – матричная над k). Ясно, что показатель алгебры всегда является делителем индекса. Но в некоторых важных частных случаях показатель и индекс алгебры совпадают. В частности, это имеет место для локальных полей и полей алгебраических чисел. Из теоремы 4.2 следует, что для таких полей из распадения коцикла $\mu_0(h_{f_1,f_2})$ вытекает, что индекс алгебры $(G_e \times K)e$ является делителем степени представления d. Тем самым, справедлива следующая теорема.

Теорема 4.3. *Пусть поле k таково, что для него и его конечных расширений показатель и индекс простых центральных алгебр над k совпадают. Тогда условие согласности для задачи погружения $(K/k, G, \varphi)$ равносильно условию согласности для сопутствующей абелевой задачи $(K/k, G/A', \varphi')$, где A' – коммутант группы A.*

Таким образом, для числовых полей условие согласности достаточно проверять лишь для абелева ядра. Однако в случае произвольных полей этот факт неверен, и имеется соответствующий пример, когда ядро – группа кватернионов ([14]).

§5. Редукция к p-расширениям

Покажем, что условие согласности достаточно проверять лишь для случая, когда погружаемое поле является p-расширением основного. Никаких ограничений на поля при этом не накладывается. Теорема эта для случая, когда ядро является p-группой, доказана в [12], см. также [14], гл. 2, §4. На общий случай она переносится без труда.

Пусть S – множество всех простых делителей порядка группы $F = \mathrm{Gal}\,(K/k)$. Для каждого $p \in S$ определим силовскую подгруппу F_p и ее полный прообраз $G_{(p)}$ в G. Обозначим через k_p подполе поля K, принадлежащее F_p. Задача погружения $(K/k, G_{(p)}, \varphi_{(p)})$, где $\varphi(p)$ – ограничение φ на $G_{(p)}$, является, как мы видели, сопутствующей второго рода для исходной задачи $(K/k, G, \varphi)$.

Теорема 5.1. *Для согласности в задаче погружения $(K/k, G, \varphi)$ необходимо и достаточно, чтобы выполнялись условия согласности для задач $(K/k_p, G_{(p)}, \varphi_{(p)})$ для всех $p \in S$.*

Необходимость очевидна. Пусть теперь условие согласности выполняется для всех сопутствующих задач $(K/k, G_{(p)}, \varphi_{(p)})$. Это значит, что скрещенные произведения $G_{(p)} \times K$ изоморфны каждая алгебре матриц порядка $|F_p|$ над своей подалгеброй. Но тогда и скрещенное произведение $G \times K$ изоморфно алгебре матриц порядка $|F_p|$ над некоторой подалгеброй. Осталось воспользоваться тем, что алгебра, одновременно представимая как матричная взаимно простых порядков, является алгеброй матриц порядка, равного их произведению (см. [14], дополнение, §1). Таким образом, алгебра $G \times K$ является матричной порядка $\prod_{p\in S}|F_p| = |F|$ над своей подалгеброй, а это и есть одна из формулировок условия согласности для задачи $(K/k, G, \varphi)$.

На самом деле, достаточно рассматривать лишь те $p \in S$, которые делят порядок ядра A. Действительно, пусть $q \in S$, $q \nmid |A|$. Рассмотрим силовскую q-подгруппу G_q группы G. На G_q отображение φ инъективно, и $\varphi(G_q) = F_q$. Но тогда $G_q \times K \approx F_q \times K$ изоморфно алгебре матриц порядка $|F_q|$ над k_q. Тем самым, для таких q условие согласности для сопутствующих задач всегда выполнено.

§6. Редукция к p-группам

Результаты данного параграфа ранее не публиковались, хотя в [13] была сформулирована гипотеза и доказаны некоторые частные результаты.

Согласно теореме 5.1, условие согласности достаточно исследовать, когда K/k является p-расширением, т.е. когда $F = \mathrm{Gal}(K/k)$ – p-группа. Это и будем предполагать.

Пусть G_p – силовская p-подгруппа группы G. Имеет место точная последовательность конечных p-групп

$$1 \longrightarrow A_p \longrightarrow G_p \xrightarrow{\varphi_p} F \longrightarrow 1,$$

где φ_p – ограничение φ на G_p, $A_p = \mathrm{Ker}\,\varphi_p$ – одна из силовских подгрупп ядра A.

Рассмотрим задачу погружения $(K/k, G_p, \varphi_p)$. Это присоединенная задача погружения, т.е. ее разрешимость (согласность) влечет разрешимость (согласность) исходной задачи (K, k, G, φ). В [15] показано, что силовская присоединенная задача погружения эквивалентна исходной в смысле разрешимости, когда A_p – абелева группа. Однако, в общем случае, это неверно даже для локальных полей.

В [13] была высказана гипотеза, что условия согласности для исходной и присоединенной силовской задачи эквивалентны. Докажем эту гипотезу.

Основная Лемма. *Пусть Λ – конечномерная ассоциативная алгебра с 1 над полем k, Γ – ее подалгебра, содержащая 1, и Λ – свободный Γ-модуль, размерности m. Если Λ – алгебра матриц порядка*

q над некоторой своей подалгеброй, и числа m, q взаимно просты, то и Γ – алгебра матриц порядка q над своей подалгеброй.

Доказательство. Поскольку Λ – свободный Γ-модуль, имеем разложение $\Lambda = \Gamma v_1 \oplus \Gamma v_2 \oplus \dots \Gamma v_m$ в прямую сумму левых Γ-модулей ранга 1. Можно считать, что $v_1 = 1$.

С другой стороны, мы имеем разложение

$$\Lambda = \Lambda\varepsilon_{11} \oplus \Lambda\varepsilon_{22} \oplus \dots \oplus \Lambda\varepsilon_{qq},$$

где ε_{ii} – диагональные матричные единицы. Слагаемые $\Lambda\varepsilon_{ii}$ – левые Λ-модули, а потому и левые Γ-модули. Таким образом, алгебра Λ двумя способами раскладывается в прямую сумму изоморфных друг другу слагаемых.

Разложим Γ в прямую сумму неразложимых левых Γ-модулей

$$\Gamma = \Gamma v_1 = s_1 P_1 \oplus s_2 P_2 \oplus \dots \oplus s_k P_k,$$

где P_i $(i = 1, \dots, k)$ – неразложимые попарно неизоморфные левые Γ-модули, а s_i – кратности их вхождения в Γv_1.

Так как все Γv_j $(j = 1, \dots, m)$ изоморфны между собой, получаем разложение

$$\Lambda = ms_1 P_1 \oplus ms_2 P_2 \oplus \dots \oplus ms_k P_k. \qquad (*)$$

Аналогично представим $\Lambda\varepsilon_{11}$ в виде прямой суммы неразложимых левых Γ-модулей:

$$\Lambda\varepsilon_{11} = t_1 Q_1 \oplus t_2 Q_2 \oplus \dots \oplus t_l Q_l,$$

где все Q_i $(i = 1, \dots, l)$ попарно неизоморфны, а t_i – кратности их вхождения в $\Lambda\varepsilon_{11}$. Тогда имеем

$$\Lambda = qt_1 Q_1 \oplus qt_2 Q_2 \oplus \dots \oplus qt_l Q_l. \qquad (**)$$

Разложения $(*)$ и $(**)$ – два разложения одного и того же Γ-модуля Λ в прямую сумму неразложимых левых Γ-модулей. По теореме Крулля–Шмидта эти разложения эквивалентны. Значит, $k = l$ и посредством перенумерации можно добиться того, что $P_1 \approx Q_1$, $P_2 \approx Q_2$, $P_k \approx Q_k = Q_l$. Тем самым, имеем равенства $qt_1 = ms_1$, $qt_2 = ms_2, \dots qt_k = ms_k$. Так как q и m взаимно просты, все s_i делятся на q, $s_i = qr_i$, откуда получаем изоморфизм

$$\Gamma = \Gamma v_1 \approx qr_1 P_1 \oplus qr_2 P_2 \oplus \dots \oplus qr_k P_k.$$

Обозначим через Δ левый Γ-модуль, изоморфный прямой сумме $\Gamma_1 P_1 \oplus r_2 P_2 \oplus \ldots \oplus r_k P_k$. Тогда $\Lambda \approx \Delta_1 \oplus \Delta_2 \oplus \ldots \oplus \Delta_q$, где все Δ_i – попарно изоморфные левые Γ-идеалы. Как известно, Λ в этом случае является матричной алгеброй порядка q над своей подалгеброй (см. [14], Дополнение, теорема Д.1.2). Лемма доказана.

Теперь гипотеза доказывается элементарно.

Теорема 6.1. *Рассмотрим задачу погружения $(K/k, G, \varphi)$, где K/k – p-расширение, и присоединенную силовскую задачу $(K/k, G_p, \varphi_p)$. Условия согласности для этих задач эквивалентны.*

Доказательство. Пусть условие согласности выполнено для задачи $(K/k, G, \varphi)$. Рассмотрим алгебры $\Lambda = G \times K$ и $\Gamma = G_p \times K$ над k. Алгебра Λ является свободным Γ-модулем (в качестве базиса можно взять $\{u_{\bar\rho}\}$, где ρ – смежные классы разложения G по G_p, а $\bar\rho$ – их представители в G). Алгебра Λ является матричной алгеброй примарного порядка $q = (K : k)$ над своей подалгеброй, а размерность Λ над Γ взаимно проста с q. Тем самым, все предположения основной Леммы выполнены. Поэтому $\Gamma = G_p \times K$ – алгебра матриц порядка $q = (K : k)$ над своей подалгеброй, и для задачи $(K/k, G_p, \varphi_p)$ выполнено условие согласности.

Теоремы 5.1 и 6.1 позволяют сводить проверку условия согласности к p-группам.

Следствие. *Пусть задача погружения $(K/k, G, \varphi)$ связана с точной последовательностью конечных групп $1 \longrightarrow A \longrightarrow G \xrightarrow{\varphi} F \longrightarrow 1$.*

Рассмотрим множество S простых чисел p, делящих как порядок A, так и порядок F. Условие согласности для задачи $(K/k, G, \varphi)$ выполняется в том и только в том случае, если оно выполняется для всех задач $(K/k_p, G_p, \varphi_p)$, $p \in S$, где G_p – силовская p-подгруппа группы G, а k_p принадлежит в K подгруппе $\varphi(G_p)$.

Литература

1. Б. Н. Делоне, Д. К. Фаддеев, *Исследования по геометрии теории Галуа.* — Матем. сб. **15(57), No. 2** (1944), 243–284.
2. H. Hasse, *Existenz und Mannigfaltigkeit Abelscher Algebren mit vorgegebener Galoisgruppe über einem Teilkörper des Grundkörpers.* — Math. Nachr. (1948) **Bd1**, No. **1**, 40–61; No. 4, 213–217.
3. Д. К. Фаддеев, *Об одной гипотезе Хассе.* — Докл. АН СССР **94, No. 6** (1954), 1013–1016.

4. И. Р. Шафаревич, *О задаче погружения полей.* — Докл. АН СССР **95, No. 3** (1954), 459–461.
5. С. П. Демушкин, И. Р. Шафаревич, *Задача погружения для локальных полей.* — Изв. АН СССР, сер. матем. **23, No. 6** (1959), 823–840.
6. С. П. Демушкин, И. Р. Шафаревич, *Второе препятствие для задачи погружения полей алгебраических чисел.* — Изв. АН СССР, сер. матем.. **26**, No. 6 (1962), 911–924.
7. А. В. Яковлев, *Задача погружения полей.* — Изв. АН СССР, сер. матем., **28, No. 3** (1964), 645–660.
8. В. А. Яковлев, *Задача погружения для числовых полей.* — Изв. АН СССР, сер. матем., **31**, No. **2** (1967), 211–224.
9. А. В. Яковлев, *Группа Галуа алгебраического замыкания локального поля.* — Изв. АН СССР, сер. матем. **32**, No. **6** (1968), 1283–1322.
10. Н. П. Зяпков, А. В. Яковлев, *Универсально согласные расширения Галуа.* — Зап. научн. семин. ЛОМИ **71** (1977), 133–152.
11. Б. Б. Лурье, *Об условиях погружаемости, когда ядро есть неабелева p-группа.* — Матем. заметки **2** No. **3** (1967), 106–114.
12. Б. Б. Лурье, *Об условии согласности в проблеме погружения полей.* — Зап. научн. семин. ЛОМИ **71** (1977), 155–162.
13. В. В. Ишханов, Б. Б. Лурье, *Условие согласности для задачи погружения с p-расширением.* — Зап. научн. семин. ПОМИ **236** (1997), 100–105.
14. В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа.* М., Наука, 1990, 272 с Перевод: V. V. Ishkhanov, B. B. Lur'e, and D. K. Faddeev *The embedding problem in Galous theory.* Transl. Math. Monogr., **165**, Amer. Soc., Providance, RI, 1997, 184 p.
15. В. В. Ишханов, Б. Б. Лурье, *Задача погружения над p-расширением.* — Алгебра и Анализ **9** вып. 4 (1997), 87–97.
16. Ч. Кэртис, И. Райнер, *Теория представлений конечных групп и ассоциативных алгебр.* М., Наука, 1969, 669 с.

Lur'e B. The Faddeev–Hasse compatibility condition in the field embedding problem.

The compatibility condition is an important condition for the solvability of the embedding problem. In the present paper, this condition is reduced to a considerably simple situation. New results and the history of the problem are given.

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

Поступило 29 июня 2000 г.