Записки научных
семинаров ПОМИ
Том 349, 2007 г.

В. В. Ишханов, Б. Б. Лурье

О ЗАДАЧЕ ПОГРУЖЕНИЯ С ЯДРОМ $\mathrm{PSL}\,(2, p^2)$

В работе [1] авторы исследовали задачу погружения с ядром $\mathfrak{A}_6$ (знакопеременная группа шести элементов). Эта группа изоморфна $\mathrm{PSL}\,(2,9)$, и это позволило дословно перенести полученный результат на задачи погружения с ядром $\mathrm{PSL}\,(2,p^2)$, где $p \equiv \pm 3 (\mathrm{mod}\, 8)$.

В настоящей работе решается задача погружения с ядром $\mathrm{PSL}\,(2,p^2)$ при произвольном нечетном простом p, заданная над полями алгебраических чисел.

1°. Пусть $B = \mathrm{PSL}\,(2,p^2)$ (проективная специальная линейная группа над полем из p^2 элементов) и задана точная последовательность конечных групп

$$1 \to B \to G \xrightarrow{\varphi} F \to 1.$$

Как известно, $\mathrm{PSL}\,(2,p^2)$ является простой группой и тем более имеет единичный центр. Поэтому в качестве группы G достаточно рассматривать группу автоморфизмов ядра (см. [2]), что мы в дальнейшем и предполагаем. Группа внешних автоморфизмов нашего ядра $\mathrm{PSL}\,(2,p^2)$ достаточно бедна – на прообразах из $\mathrm{SL}\,(2,p^2)$ она порождена автоморфизмом Фробениуса (т.е. возведением всех элементов матрицы в p-ю степень) и сопряжением посредством матрицы из $\mathrm{GL}\,(2,p^2)$, чей определитель не является квадратом (см. [3]).

Таким образом, группа внешних автоморфизмов ядра является четверной группой.

Зафиксируем какую-либо силовскую 2-подгруппу G_2 группы G (разумеется, все они сопряжены).

Порядок группы $B = \mathrm{PSL}\,(2,p^2)$ равен $\frac{1}{2}(p^2+1)(p^4-p^2)$, поэтому силовская 2-подгруппа ядра имеет порядок q, равный максимальной степени двойки, делящей p^2-1. Иначе говоря, $q = 8$ при

Работа выполнена при финансовой поддержке фонда РФФИ, грант 06-01-00741а.

$p \equiv \pm 3 (\operatorname{mod} 8)$, $q = 16$ при $p \equiv \pm 7 (\operatorname{mod} 16)$ и т.д. Соответственно, порядок группы $G_2 = (\operatorname{Aut} B)_2$ равен $4q$.

Обозначим через α образ матрицы $\begin{pmatrix} w & 0 \\ 0 & w^{-1} \end{pmatrix}$, где w – какой-либо элемент максимального 2-порядка в поле $\mathfrak{F} = \mathrm{GF}(p^2)$. Таким образом $w = v^m$, где v – образующая циклической группы $\mathfrak{F}^*$, а m – максимальный нечетный делитель числа $p^2 - 1$. Поскольку $w^{q/2} = -1$, элемент α имеет в $\mathrm{PSL}(2, p^2)$ порядок $q/2$. Через β обозначим образ матрицы $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, так что $\beta^2 = 1$. Ясно, что $\beta^{-1}\alpha\beta$ равно образу матрицы $\begin{pmatrix} -w^{-1} & 0 \\ 0 & -w \end{pmatrix}$, т.е. $\beta^{-1}\alpha\beta = \alpha^{-1}$. Таким образом, группа $D = B_2$ есть обобщенная группа диэдра порядка $2 \cdot \frac{q}{2}$.

Ясно, что автоморфизм Фробениуса Φ коммутирует с β. Если $p \equiv 1 (\operatorname{mod} 4)$, выбранный элемент $w \in F$ отображается автоморфизмом Φ в $-w$, поскольку w^2 принадлежит полю из p элементов; тогда Φ коммутирует и с α.

Пусть теперь $p \equiv -1 (\operatorname{mod} 4)$. В этом случае число m (максимальный нечетный делитель числа $p^2 - 1$) делится на $\frac{p-1}{2}$, поэтому $m(p+1)$ делится на $\frac{p^2-1}{2}$ (и не делится на $p^2 - 1$). Значит, $w^{p+1} = v^{m(p+1)} = -1$. Поэтому $w^p = -w^{-1}$ и $\alpha^{\Phi} = \alpha^{-1}$.

Обозначив через τ автоморфизм Φ при $p \equiv 1 (\operatorname{mod} 4)$ и композицию Φ и β при $p = -1(\operatorname{mod} 4)$, получаем: $\tau^2 = 1$, $\alpha^\tau = \alpha$, $\beta^\tau = \beta$.

Пусть теперь σ – сопряжение на $\mathrm{GL}(2, p^2)$, задаваемое матрицей $\begin{pmatrix} 0 & w \\ 1 & 0 \end{pmatrix}$. Определитель этой матрицы – не квадрат в $\mathfrak{F}$, и σ определяет внешний автоморфизм на $\mathrm{PSL}(2, p^2) = B$. Так как квадрат матрицы $\begin{pmatrix} 0 & w \\ 1 & 0 \end{pmatrix}$ является скалярной матрицей, имеем $\sigma^2 = 1$. Несложный подсчет показывает, что

$$\alpha^\sigma = \alpha^{-1}, \quad \beta^\sigma = \beta\alpha^{-1}.$$

На 2-группе $D = B_2$ коммутатор $[\sigma, \tau]$ действует тривиально. Но произвольная матрица $\begin{pmatrix} x & y \\ z & t \end{pmatrix}$ при действии коммутатора $[\sigma, \tau]$ переходит в матрицу $\begin{pmatrix} x & -y \\ -z & t \end{pmatrix}$ (это проверяется прямым счетом; при этом надо учитывать, что $c^p = c$ при $p \equiv 1 (\operatorname{mod} 4)$ и $c^{p+1} = -1$ при $p \equiv -1 (\operatorname{mod} 4)$). Таким образом, в группе $\operatorname{Aut}\mathrm{PSL}(2, p^2)$ – это автоморфизм, индуцированный матрицей $\begin{pmatrix} i & -0 \\ 0 & -i \end{pmatrix}$, где $i \in \mathfrak{F}$, $i^2 = -1$. Таким образом, коммутатор $[\sigma, \tau]$ равен $\alpha^{q/4}$.

Итак, обозначив $q = 2^{n+1}$ для группы D и ее расширения G_2, имеем следующие соотношения:

$$\alpha^{2^n} = 1, \quad \beta^2 = 1, \quad \alpha^\beta = \alpha^{-1}, \quad \tau^2 = 1, \quad \alpha^\tau = \alpha,$$
$$\beta^\tau = \beta, \quad \sigma^2 = 1, \quad \alpha^\sigma = \alpha^{-1}, \quad \beta^\sigma = \beta\alpha^{-1}, \quad \tau^\sigma = \tau\alpha^{2^{n-1}}.$$

Рассмотрим задачу погружения, связанную с последовательностью

$$1 \to B = \mathrm{PSL}\,(2, p^2) \to G = \mathrm{Aut}\, B \xrightarrow{\varphi} F = \mathrm{Gal}\,(K/k) \to 1, \qquad (1)$$

и присоединенную силовскую задачу

$$1 \to D = B_2 \to G_2 \xrightarrow{\varphi_2} F = \mathrm{Gal}\,(K/k) \to 1. \qquad (2)$$

Как было показано ранее, K – расширение поля k с группой Клейна: $K = k(\sqrt{c}, \sqrt{d})$, где c, $d \in k^*$. Действие $\mathrm{Gal}\,(K/k)$ зададим формулами

$$\sqrt{c}^{\,\sigma} = -\sqrt{c}, \quad \sqrt{c}^{\,\tau} = \sqrt{c}, \quad \sqrt{d}^{\,\sigma} = \sqrt{d}, \quad \sqrt{d}^{\,2} = -\sqrt{d}.$$

Как известно, разрешимость присоединенной задачи (2) гарантирует разрешимость и задачи (1).

2°. Будем решать задачу (2) в два этапа.

Обозначим через A циклическую подгруппу D, порожденную элементом α. Ясно, что G_2/A – прямое расширение D/A посредством F, поэтому всякое решение сопутствующей задачи $(K/k, G_2/A, \overline{\varphi})$ имеет вид $L = K(\sqrt{x})$, где $x \in K^*$ и $\sqrt{x}^{\,\beta} = -\sqrt{x}$, $\sqrt{x}^{\,\sigma} = \sqrt{x}^{\,\tau} = \sqrt{x}$. Чтобы была разрешима задача (2), нужно найти такое $x \in k^*$, для которого разрешима задача погружения, связанная с последовательностью групп

$$1 \to A \to G_2 \xrightarrow{\varphi_3} \mathrm{Gal}\,(L/k) \to 1. \qquad (3)$$

Вычислим "второе препятствие" для задачи (2), т.е. условия, при которых выполняется условие согласности для задачи (3).

Групповая алгебра $K[A]$ содержит следующие идемпотенты, центральные в скрещенном произведении $G \times L$:

$$E_0 = \frac{1+\alpha^{2^{n-1}}}{2} \cdot \frac{1+\alpha^{2^{n-2}}}{2} \cdots \frac{1+\alpha}{2},$$

$$E_1 = \frac{1+\alpha^{2^{n-1}}}{2} \cdot \frac{1+\alpha^{2^{n-2}}}{2} \cdots \frac{1+\alpha^2}{2}\ \frac{1-\alpha}{2},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$E_j = \frac{1+\alpha^{2^{n-1}}}{2} \cdots \frac{1+\alpha^{2^{j+1}}}{2} \cdot \frac{1-\alpha^{2^j}}{2},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$E_{n-2} = \frac{1+\alpha^{2^{n-1}}}{2}\ \frac{1-\alpha^{2^{n-2}}}{2},$$

$$E_{n-1} = \frac{1-\alpha^{2^{n-1}}}{2}.$$

Все эти идемпотенты ортогональны друг другу, а их сумма равна 1. Рассмотрим алгебры $\Lambda_j = (G \times L)E_j$ и найдем центр каждой из этих алгебр. Для Λ_0 и Λ_1 центром служит поле k. Центром алгебры Λ_2 является $k(\alpha^2\sqrt{cx}\, E_2) \approx k(\sqrt{-cx})$. Центр алгебры Λ_3 порожден над k элементами $\alpha^4\sqrt{cx}\, E_3$, $(\alpha+\alpha^{-1})E_3$, т.е. изоморфен $k(\sqrt{-cx}, \sqrt{2})$. Соответственно, центр алгебры Λ_j порожден над k элементами

$$\alpha^{2^{j-1}}\sqrt{cx}\, E_j, \quad (\alpha+\alpha^{-1})E_j, \quad (\alpha^2+\alpha^{-2})E_j, \dots, (\alpha^{2^{j-3}}+\alpha^{-2^{j-3}})E_j.$$

Рассмотрим последовательность

$$\theta_2 = 0, \quad \theta_3 = \sqrt{2}, \quad \theta_4 = \sqrt{2+\sqrt{2}}, \dots, \theta_{j+1} = \sqrt{2+\theta_j}.$$

Тогда центр алгебры Λ_j при $j \geqslant 2$ изоморфен $k(\sqrt{-cx}, \theta_j)$ (числа θ_j могут быть представлены как $\theta_j = 2\cos\frac{\pi}{2^{j-1}}$; соответственно $k(\theta_j, \sqrt{-1})$ содержит первообразный корень из 1 степени 2^j).

Пусть $H = \{g \in G_2 : (\alpha^g = \alpha, \beta^g = \beta)$ или $(\alpha^g = \alpha^{-1}, \beta^g = \beta\alpha^{-1})\}$ – подгруппа группы G_2. Ясно, что $\varphi(H) = F$ и $H_1 \cap D = \langle\, \alpha^{2^{n-1}} \,\rangle$.

Скрещенное произведение $(H \times K)E_j$ является классическим скрещенным произведением поля K и его группы Галуа F. Для $j = 0, 1, \dots, n-2$ система факторов в этом скрещенном произведении единичная (так как $\sigma^2 = \tau^2 = 1$, $[\sigma, \tau] = \alpha^{2^{n-1}}$), поэтому все алгебры $(H \times K)E_j$ – матричные. При $j = n-1$ $(H \times K)E_{n-1}$ является тензорным произведением матричной алгебры $k(\tau, \sqrt{d})$ и кватернионной алгебры $k(\sigma\sqrt{d}, \sqrt{c})$ со структурными константами c, d. Иначе говоря $(H \times K)E_{n-1}$ подобна (в группе Брауэра) алгебре $k[c,d]$.

Централизатор алгебры $(H \times K)E_j$ в алгебре $\Lambda_j = (G \times L)E_j$ порожден указанным выше центром и парой антикоммутирующих элементов $\sqrt{x}\,E_j$, $(\beta + \beta\alpha^{-1})E_j$. Поскольку

$$(\beta + \beta\alpha^{-1})^2 E_j = (2 + \alpha + \alpha^{-1})E_j \quad \text{и} \quad (\alpha + \alpha^{-1})E_j = \theta_j E_j,$$

этот централизатор изоморфен $k(\sqrt{-cx}, \theta_j)[2+\theta_j, x]$ (алгебра кватернионов с константами $2 + \theta_j, x$ над центром). Здесь $j = 2, \ldots, n-1$. Кроме того, алгебра Λ_0 – матричная; алгебра Λ_1 изоморфна тензорному произведению $(H \times K)E_1$ и алгебры $k(\beta\sqrt{c}\,E_1, \sqrt{x}\,E_1)$, т.е. подобна алгебре $k[c,x]$.

Как известно, условие согласности для задачи погружения (в данном случае, для задачи (3)) состоит в том, что алгебра $G \times L$ изоморфна алгебре матриц порядка $(L:k)$ над своей подалгеброй (см. [4]). Таким образом, для задачи (3) условие согласности состоит в том, что являются матричными следующие алгебры:

$$\begin{array}{l} k[c,x] \\ k(\sqrt{-cx})\ [2,x] \\ \ldots\ldots\ldots\ldots\ldots \\ k(\sqrt{-cx}, \theta_j)[2+\theta_j, x] \quad (j = 2,3,\ldots,n-2) \\ \ldots\ldots\ldots\ldots\ldots \\ k(\sqrt{-cx}, \theta_{n-1})[2+\theta_{n-1}, x]\ [c,d]. \end{array}$$

В нахождении такого $x \in k^*$ и состоит “второе препятствие” для задачи (2).

При $n = 2$ (т.е. когда $p \equiv \pm 3 (\mathrm{mod}\ 8)$), наши условия имеют вид: $k[c,x]$ и $k(\sqrt{-cx})\,[c,d]$ – матричные алгебры. Условие погружения в этом случае состоит в том, что c является нормой кватерниона из $k[c,d]$ (см. [1, 4]). При $n \geqslant 3$ должны быть матричными по крайней мере три алгебры. Можно показать, что при $n \geqslant 3$ достаточно ограничиться рассмотрением трех алгебр – первой и двух последних из указанных. Но этот факт нам не потребуется.

3°. Пусть теперь K/k – расширение числовых полей. В этой ситуации условие согласности равносильно этому условию для всех сопутствующих локальных задач погружения $(K_\mathfrak{p}/k_\mathfrak{p}, G_2, \varphi_\mathfrak{p})$, где $\mathfrak{p}$ – произвольный простой дивизор поля k (включая и бесконечные точки), $k_\mathfrak{p}$ – пополнение поля k в точке $\mathfrak{p}$, $K_\mathfrak{p} \otimes_k k_\mathfrak{p}$ (см. [4, 5]). При этом, разумеется, достаточно рассматривать лишь критические для нашей ситуации точки поля k, т.е. делители чисел c, d, 2, x и бесконечные точки.

Однако, если ядро – циклическая 2-группа порядка 8 или больше, условие согласности не гарантирует погружаемости. Дополнительное условие, гарантирующее погружаемость, сформулируем в форме Демушкина–Шафаревича (см. [5]).

Присоединим к полю K первообразный корень ζ из 1 степени, равной порядку A, т.е. 2^n. Обозначим $\overline{K} = K(\zeta)$, $\overline{L} = L(\zeta) = \overline{K}(\sqrt{x})$, $\overline{F} - \mathrm{Gal}\,(\overline{K}/k)$, $\overline{G}_2$ – произведение групп G_2 и $\overline{F}$ с объединенной факторгруппой F. Ядро эпиморфизма $\overline{F} \to F$ имеет в общем случае две образующие γ, δ, которые действуют на корне ζ по правилам $\zeta^\gamma = \zeta^{-1}$, $\zeta^\delta = \zeta^5$ (при этом γ и δ содержатся в центре группы $\overline{G}_2$).

Задача (3) равносильна задаче (4) $(\overline{L}/k, \overline{G}_2, \varphi_4)$, заданной последовательностью

$$1 \to A \to \overline{G}_2 \xrightarrow{\varphi_4} F^* = \mathrm{Gal}\,(\overline{L}/k) \to 1, \tag{4}$$

поскольку получена из задачи (3) подъемом. Для этих задач также эквивалентны и условия согласности (см. [4]). Группа F^* – прямое произведение групп $\overline{F}$ и D/A.

Пусть $\widehat{A} = \mathrm{Hom}\,(A, \overline{K}^*)$ – группа характеров A, $\widetilde{F}$ – группа автоморфизмов ядра. Обозначим через F_0 подгруппу группы F^*, элементы которой действуют на A тривиально, тогда $\widetilde{F} \approx F^*/F_0$. Группа $\widetilde{A}$ превращается в F^*-операторную, если определить характер χ^f $(\chi \in \widehat{A}, f \in F^*)$ по правилу $\chi^f(\alpha) = (\chi(\alpha^{f^{-1}}))^f$. Группа $\widetilde{F}$ порождается образами β_1 и δ_1 автоморфизмов β и δ соответственно (поскольку γ действует на A так же, как β). Через L_0 обозначим поле $\overline{L}^{F_0}$. Будем считать, что поле k не содержит ни $\sqrt{-1}$, ни $\theta_n = 2\cos\frac{\pi}{2^{n-1}}$, так что элементы γ, δ реально присутствуют в нашем исследовании – в противном случае рассмотрение выглядит проще.

Найдем поле L_0. Группа F_0 содержит элементы τ, $\sigma\beta$ и $\gamma\beta$. Кроме того, F_0 может содержать элемент δ в какой-либо степени, но само δ в F_0 не содержится. Поэтому L_0 порождено над k числами $\sqrt{c}\cdot\sqrt{x}\sqrt{-1}=\sqrt{-cx}$ и θ_n, т.е. $L_0=k(\sqrt{-cx},\theta_n)$.

Согласно [5], для разрешимости задачи (4) (помимо согласности) достаточно, чтобы была единичной группа когомологий $H^3(\widetilde{F},L_0^*)$ (напомним, что $\widetilde{F}=F^*/F_0=\mathrm{Gal}(L_0/k)$).

Порядок группы $H^3(\widetilde{F},L_0^*)$ равен частному от деления порядка $\widetilde{F}$ на наименьшее общее кратное порядков групп разложения для всех конечных точек поля k. Таким образом, задача (4) разрешима, если существует такой элемент $x\in k^*$ и такая точка $\mathfrak{p}$ поля k, что группа разложения в этой точке совпадает с $\widetilde{F}$ (и, разумеется, выполняется условие согласности для (4)). Группа разложения в точке $\mathfrak{p}$ совпадает с $\widetilde{F}$, когда $(L_0)_\mathfrak{p}=L_0\otimes_k k_\mathfrak{p}$ остается полем.

4°. **Теорема 1.** *Задача погружения* (2) *разрешима тогда и только тогда, когда разрешимы сопутствующие локальные задачи, отвечающие бесконечным точкам поля k.*

Доказательство. Необходимость очевидна. Будем доказывать достаточность. В соответствии с программой, намеченной ранее, нам нужно найти такой элемент $x\in k^*$, что выполняются следующие условия:

1) $k[c,x]$ – матричная алгебра,
2) $k(\sqrt{-cx},\theta_j)[2+\theta_j,\,x]$ – матричные алгебры ($j=0,1,\ldots,n-2$),
3) $k(\sqrt{-cx},\theta_{n-1})[2+\theta_{n-1},x]\otimes[c,d]$ – матричная алгебра,
4) существует конечная точка $\mathfrak{p}$ поля k, для которой $L_0\otimes_k k_\mathfrak{p}=k(\sqrt{-cx},\theta_n)\otimes_k k_\mathfrak{p}$ остается полем.

Домножив элементы c, d на квадраты, добьемся того, что они – целые элементы поля k. Пусть l – такое число, что $\theta_2=0,\ldots,\theta_l\in k$, но $\theta_{l+1}\notin k$ (ясно, что $0\leqslant l\leqslant n-1$). Обозначим через S_1 множество конечных точек поля k, делящих 2, c или d, а через S_2 – множество бесконечных точек (т.е. архимедовых нормирований) поля k. Определим локальное поведение $x_\mathfrak{p}$ элемента x в этих точках.

1. Пусть $\mathfrak{p}\mid\theta_l$, причем $-c$ – не квадрат в $k_\mathfrak{p}$ и $(2+\theta_l)(-c)$ – не квадрат в $k_\mathfrak{p}$. Положим тогда $x_\mathfrak{p}=1$. Тогда алгебра $k_\mathfrak{p}[c,x_\mathfrak{p}]$ распадается, т.к. $x_\mathfrak{p}=1$, остальные алгебры распадаются, т.к. определены над $k_\mathfrak{p}(\theta_j)$, а $k_\mathfrak{p}(\sqrt{-cx_\mathfrak{p}})$ – квадратичное расширение $k_\mathfrak{p}$. Покажем, что $k_\mathfrak{p}(\sqrt{-cx_\mathfrak{p}},\theta_n)$ является полем.

Действительно, $k_{\mathfrak p}(\theta_n)$ – поле, поскольку $\mathfrak p \mid \theta_l$ и уже $k_{\mathfrak p}(\theta_l)$ – поле. Осталось доказать, что $\sqrt{-cx_{\mathfrak p}} = \sqrt{-c}$ не содержится в $k_{\mathfrak p}(\theta_n)$. Предположим противное. Тогда $\sqrt{-c} \in k_{\mathfrak p}(\theta_{l+1})$. Значит, $-c = (u + v\theta_{l+1})^2$, где u, $v \in k_{\mathfrak p}$: отсюда $uv = 0$ и либо $-c = u^2$, либо $-c = (v\theta_{l+1})^2 = v^2(2+\theta_l)$ в противоречии с предположением.

2. Пусть $\mathfrak p \mid \theta_l$, причем $-c$ – не квадрат в $k_{\mathfrak p}$, но $(2+\theta_l)(-c)$ – квадрат в $k_{\mathfrak p}$. Положим в этом случае $x_{\mathfrak p} = 1 + (2+\theta_l)\pi^2$, где π – простой элемент $k_{\mathfrak p}$. Тогда $-cx_{\mathfrak p} \equiv 2 + \theta_l (\operatorname{mod} \pi^2)$, значит, $-cx_{\mathfrak p}$ – не квадрат в $k_{\mathfrak p}$ и, по построению, $k_{\mathfrak p}[c, x_{\mathfrak p}]$ – матричная алгебра. Как и ранее, предположение $\sqrt{-cx_{\mathfrak p}} \in k_{\mathfrak p}(\theta_n)$ приводит к тому, что либо $-cx_{\mathfrak p}$ является квадратом в $k_{\mathfrak p}$, либо $-cx_{\mathfrak p} = v^2(2+\theta_l)$, где $v \in k_{\mathfrak p}$. И то и другое невозможно, поскольку $x_{\mathfrak p} = 1 + (2+\theta_l)\pi^2$ – не квадрат в $k_{\mathfrak p}$. Таким образом, и в этом случае все требования к локальному поведению $x_{\mathfrak p}$ выполнены.

3. Пусть $\mathfrak p \mid \theta_l$, причем $-c$ – квадрат в $k_{\mathfrak p}$ (т.е. мы вправе считать $c = -1$). Положим в этом случае $x_{\mathfrak p} = 1 + \pi^2$, где π – простой элемент поля $k_{\mathfrak p}$. Докажем, что $x_{\mathfrak p}$ нельзя представить в виде $(2+\theta_l)v^2$ $(v \in k_{\mathfrak p})$ – проверка всех остальных требований к $x_{\mathfrak p}$ очевидна. Пусть $x_{\mathfrak p} = 1 + \pi^2 = (2+\theta_l)v^2$. Рассмотрим абсолютную норму (над $\mathbb{Q}_2$) для этого равенства. Ясно, что норма числа $2+\theta_l$ равна 2, поэтому указанное равенство невозможно.

4. Пусть $\mathfrak p \nmid \theta_l$, но $\mathfrak p \mid 2$. Положим в этом случае $x_{\mathfrak p} = 1$, если $-c$ – не квадрат в $k_{\mathfrak p}$. Если же $-c$ – квадрат в $k_{\mathfrak p}$, то выберем $x_{\mathfrak p} \in k_{\mathfrak p}$ так, чтобы $x_{\mathfrak p}$ не было квадратом, но было суммой двух квадратов в $k_{\mathfrak p}$. Тогда условие согласности (т.е. первые три условия) в точке $\mathfrak p$ выполняются.

5. Пусть $\mathfrak p \nmid 2$, но $\mathfrak p \mid c$. Положим $x_{\mathfrak p} = 1$. Тогда $k_{\mathfrak p}(\sqrt{-cx_{\mathfrak p}}) = k_{\mathfrak p}(-c)$ – квадратичное расширение поля $k_{\mathfrak p}$, поэтому условие согласности в точке $\mathfrak p$ выполнено.

6. Пусть $\mathfrak p \nmid 2$, $\mathfrak p \nmid c$, $\mathfrak p \mid d$. В этом случае c – единица в $k_{\mathfrak p}$. Выберем в качестве $x_{\mathfrak p}$ единицу поля $k_{\mathfrak p}$ такую, что $-cx_{\mathfrak p}$ – не квадрат в $k_{\mathfrak p}$. Алгебра $k_{\mathfrak p}[c, x_{\mathfrak p}]$ распадается, т.к. c, $x_{\mathfrak p}$ – локальные единицы, а остальные алгебры распадаются, поскольку определены над $k_{\mathfrak p}$.

7. Пусть теперь $\mathfrak p \in S_2$, т.е. бесконечная точка поля k. Если при вложении k в $\mathbb{R}$, отвечающем нормированию $\mathfrak p$, элементы c и d оказываются отрицательными, то локальная сопутствующая задача погружения неразрешима. В самом деле, условие $k_{\mathfrak p}[c, x]$

означает в этом случае, что $x_{\mathfrak{p}} > 0$, но тогда $\mathbb{R}(\sqrt{-cx}) = \mathbb{R}$ и $\mathbb{R}[c,d]$ есть тело кватернионов, и задача неразрешима. Но это противоречит условию теоремы. Когда c или d положительны при вложении k в $\mathbb{R}$ (отвечающем точке $\mathfrak{p}$), положим $x_{\mathfrak{p}} > 0$.

Итак, для любого $\mathfrak{p} \in S_1 \cup S_2$ мы нашли элементы $x_{\mathfrak{p}} \in k_{\mathfrak{p}}$ такие, что все локальные задачи погружения, отвечающие этим точкам, разрешимы.

В соответствии с теоремой Чеботарева о плотности, существует простой элемент x поля k, чье локальное поведение в точках $\mathfrak{p} \in S_1 \cup S_2$ совпадает с $x_{\mathfrak{p}}$ (с точностью до локальных квадратов). Обозначим $\mathfrak{q} = (x)$ – главный дивизор простого числа x. Докажем, что элемент x – искомый, т.е. решает задачу (4), а соответственно, задачи (3) и (2).

Поскольку для $\mathfrak{p} \notin S_1 \cup S_2 \cup \{\mathfrak{q}\}$ элементы c, d, x, θ_j, $2\cdot\theta_j$ являются единицами поля $k_{\mathfrak{p}}$, условие согласности для соответствующей локальной задачи выполнено, осталось проверить его для единственной точки $\mathfrak{q}$. Алгебры $k_{\mathfrak{q}}(\sqrt{-cx}, \theta_j)\ [2+\theta_j, x]\ (j < n-1)$, а также $k_{\mathfrak{q}}(-cx, \theta_{n-1})\ [2+\theta_{n-1}, x]\ [c,d]$ распадаются, поскольку $k_{\mathfrak{q}}(\sqrt{-cx})$ – квадратичное расширение $k_{\mathfrak{q}}$. Осталось проверить распадение алгебры $k_{\mathfrak{q}}[c,x]$. Но для всех точек $\mathfrak{p}$ (конечных и бесконечных), отличных от $\mathfrak{q}$, алгебры $k_{\mathfrak{p}}[c,x]$ распадаются. Значит, по закону взаимности, распадается и алгебра $k_{\mathfrak{q}}[c,x]$.

Таким образом, для задач погружения (3) и (4) выполняется глобальное условие согласности. Кроме того, для $\mathfrak{p} \mid \theta_l$ группа разложения (по построению) совпадает с $\widetilde{F}$, а значит, группа когомологий $H^3(\widetilde{F}, L_0)$ тривиальна. Теорема доказана. □

Замечание. Как видно из доказательства, задача (2) неразрешима тогда и только тогда, когда существует вложение поля k в $\mathbb{R}$, при котором оба элемента c, d отрицательны.

Соответственно, для разрешимости задачи (2) достаточно, чтобы числа c или d были тотально положительны. Задача (2) разрешима также, если число $c\,d$ тотально отрицательно.

5°. Вернемся к исходной задаче (1) с ядром $B = \mathrm{PSL}\,(2, p^2)$.

Теорема 2. *Задача погружения с ядром* $\mathrm{PSL}\,(2, p^2)$ *над числовыми полями разрешима тогда и только тогда, когда разрешима отвечающая ей присоединенная* 2*-задача, или, что то же самое, разрешимы сопутствующие локальные задачи в бесконечных точках.*

Доказательство. Разрешимость присоединенной задачи погружения достаточна для разрешимости исходной.

Пусть присоединенная силовская 2-задача (с ядром, изоморфным обобщенной группе диэдра) неразрешима. Это означает, что существует вложение k в $\mathbb{R}$, при котором указанные элементы c, d – оба отрицательны. Но тогда поле K превращается в алгебру Галуа, изоморфную прямой сумме двух полей комплексных чисел с идемпотентами

$$e_1 = \frac{1 + \frac{\sqrt{c}\sqrt{d}}{\sqrt{|c|\,|d|}}}{2}, \quad e_2 = \frac{1 - \frac{\sqrt{c}\sqrt{d}}{\sqrt{|c|\,|d|}}}{2}.$$

Подгруппа группы F, оставляющая инвариантными эти идемпотенты, порождена элементом $\sigma\tau$. Соответственно, локальная задача погружения, отвечающая данной бесконечной точке, равносильна задаче погружения расширения $\mathbb{C}/\mathbb{R}$ в группу, порожденную ядром и автоморфизмом $\sigma\tau$. Поскольку прообраз автоморфизма $\sigma\tau$ в этой группе не может иметь порядок 2 (иначе это реализовалось бы в силовской подгруппе), расширение $\mathrm{PSL}\,(2, p^2)$ посредством автоморфизма $(\sigma\tau)$ – не полупрямое. Но задача над алгебраическим замкнутым полем разрешима лишь тогда, когда она полупрямая. Следовательно, при $c < 0$, $d < 0$ задача (1) неразрешима. Теорема доказана. $\square$

Литература

1. В. В. Ишханов, Б. Б. Лурье, *Задача погружения над p-расширением.* — Алгебра и анализ **9**, No. 4 (1997), 87–97.
2. Б. Б. Лурье, *К задаче погружения с ядром без центра.* — Изв. АН СССР, Сер. мат. **28**, No. 5 (1964), 1135–1138.
3. Р. Стейнберг, *Лекции о группах Шевалле.* Мир, М., 1975.
4. В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа.* Наука, М., 1990.
5. С. П. Демушкин, И. Р. Шафаревич, *Второе препятствие для задачи погружения полей алгебраических чисел.* — Изв. АН СССР, Сер. мат. **26**, No. 6 (1962), 911–914.
6. С. П. Демушкин, И. Р. Шафаревич, *Задача погружения для локальных полей.* — Изв. АН СССР, Сер. мат. **23**, No. 6 (1959), 823–840.

Ishkhanov V. V., Lur'e B. B. The embedding problem with kernel $\mathrm{PSL}\,(2, p^2)$.

The embedding problem of number fields is considered. It is proved that it is solvable if and only if all the associated local problems at the infinite points are solvable. It is also proved that the solvability of an adjoint with Sylow 2-group is equivalent to the solvability of the original problem.

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

Поступило 10 ноября 2007 г.