Записки научных
семинаров ПОМИ
Том 265, 1999 г.

А. А. Яковлева

ОБ ОДНОЙ ЗАДАЧЕ ПОГРУЖЕНИЯ

Многие авторы (см., например, [2] и приведенную там литературу) исследовали возможность погружения расширения Галуа поля рациональных чисел с симметрической группой степени 4 в расширение с нерасщепляемой группой Галуа порядка 48. При этом выяснилось, что невозможность погружения накладывает арифметические ограничения на исходное расширение. Основным аппаратом в этих работах было изучение эллиптических кривых, связанных с расширением. Вместе с тем, еще в 1944 году Д. К. Фаддеев сформулировал условие согласности, которое в данном случае необходимо и достаточно для разрешимости задачи погружения. Целью работы является исследование упомянутых задач погружения в специальном случае с помощью условия согласности. Этот специальный случай также изучался Ф. Кассу-Ногесом, но полученные нами ограничения на арифметические параметры определяющего многочлена более сильные.

Все сведения о задаче погружения, используемые в настоящей работе, можно найти в [1].

Пусть K/k – расширение Галуа и пусть φ – эпиморфизм конечной группы G на группу Галуа $\mathrm{Gal}(K/k)$ расширения K/k. Задача погружения $(K/k, G, \varphi)$ состоит в построении поля L, содержащего K, и такого, что расширение L/k представляет собой расширение Галуа с группой Галуа G, причем для любого автоморфизма $g \in G$ поля L ограничение g на подполе K совпадает с $\varphi(g)$.

Теорема. *Пусть n – нечетное целое число и пусть K – поле разложения многочлена $f(x) = x^4 - 2nx - 1$ над полем рациональных чисел $\mathbb{Q}$. Группа Галуа F расширения $K/\mathbb{Q}$ является симметрической группой S_4. Пусть, далее, G – группа, порожденная элементами s, t, u, связанными соотношениями*

$$s^4 = t^8 = u^3 = 1, \quad s^{-1}ts = t^{-1}, \quad su = u^2 s, \quad tu = u^2 t^2 s,$$

Работа выполнена при финансовой поддержке РФФИ, грант 96-15-96200.

а φ – эпиморфизм φ группы G на $F = S_4$, заданный формулами

$$\varphi(s) = (1,3), \quad \varphi(t) = (1,2,3,4), \quad \varphi(u) = (1,2,3).$$

Если все простые числа, кратность вхождения которых в каноническое разложение числа $16+27n^2$ нечетна, сравнимы с 1, 3 или 5 по модулю 8, то задача погружения $(K/\mathbb{Q}, G, \varphi)$ разрешима.

Доказательство. Пусть a_1, a_2, a_3, a_4 – корни многочлена $f(x)$ в алгебраическом замыкании поля $\mathbb{Q}$. Поле разложения K многочлена $f(x)$ получается присоединением к полю $\mathbb{Q}$ корней a_1, a_2, a_3, a_4. Найдем группу Галуа F поля разложения K многочлена $f(x) = x^4 - 2nx - 1$ над полем рациональных чисел $\mathbb{Q}$. Поскольку n нечетно, многочлен $f(y+1) = y^4 + 4y^3 + 6y^2 + (4-2n)y - 2n$ удовлетворяет требованиям критерия Эйзенштейна и потому неприводим над $\mathbb{Q}$; следовательно, неприводим и многочлен $f(x)$, а это означает, что группа Галуа F поля разложения $K/\mathbb{Q}$ многочлена $f(x)$ действует на множестве корней a_1, a_2, a_3, a_4 этого многочлена транзитивно.

Пусть

$$g(z) = 4z(1+z^2/4) - (2n)^2 = z^3 + 4z - 4n^2$$

– кубическая резольвента многочлена $f(x) = x^4 - 2nx - 1$. Если z – корень $g(z)$, принадлежащий полю $\mathbb{Q}$, то из соотношения $z^3 = 4(n^2 - z)$ следует, что z^3 делится на 4, но не делится на 8, ибо $n^2 - z$ нечетно при четном z (напомним, что число n нечетно). Таким образом, кубический многочлен $g(z)$ не имеет корней в поле $\mathbb{Q}$ и потому неприводим над $\mathbb{Q}$. Корни кубической резольвенты $g(z)$ являются рациональными функциями корней многочлена $f(x)$ (а именно, поскольку коэффициенты при кубе и квадрате неизвестной в многочлене $f(x)$ равны 0, эти корни – квадраты элементов

$$(a_1+a_2-a_3-a_4)/2, \quad (a_1-a_2-a_3+a_4)/2, \quad (a_1-a_2+a_3-a_4)/2),$$

и потому они содержатся в K. Следовательно, степень расширения $K/\mathbb{Q}$ делится на степень неприводимого многочлена $g(z)$, равную 3, а значит, и порядок группы Галуа F делится на 3.

Дискриминант

$$D = \prod_{1 \leqslant i < j \leqslant 4} (a_i - a_j)^2$$

многочлена $f(x)$ совпадает с дискриминантом кубической резольвенты $g(z)$ и равен

$$-108\left(\left(\frac{4}{3}\right)^3+\left(\frac{-4n^2}{2}\right)^2\right)=-3(12n^2)^2\big(1+16/(27n^4)\big).$$

Сравнимое с 1 по модулю 8 (и даже 16) целое 2-адическое число $1+16/(27n^4)$ является квадратом в $\mathbb{Q}_2$, а -3 – не квадрат в $\mathbb{Q}_2$; поэтому D – не квадрат в $\mathbb{Q}_2$, и тем более не квадрат в $\mathbb{Q}$. Значит, $\mathbb{Q}(\sqrt{D})\neq\mathbb{Q}$, откуда следует, что группа Галуа F не содержится в знакопеременной подгруппе A_4 симметрической группы S_4.

Итак, подгруппа F группы S_4 транзитивна, не содержится в A_4 и ее порядок делится на 3; это возможно лишь при $F=S_4$.

Вернемся теперь к нашей задаче погружения. Ее ядро $A=\operatorname{Ker}\varphi$ – циклическая группа порядка 2, состоящая из двух элементов e, t^4. Хорошо известно, что согласность достаточна для разрешимости такой задачи. Напомним, в чем состоит условие согласности. Пусть $c\in H^2(F,A)$ – фундаментальный класс расширения групп $1\to A\to G\xrightarrow{\varphi}F\to 1$, и пусть $\chi:A\to K^*$ – единственный нетривиальный гомоморфизм ядра A в мультипликативную группу поля K, а $\chi^*:H^2(F,A)\to H^2(F,K^*)$ – гомоморфизм групп когомологий, индуцированный χ. Условие согласности для задачи погружения $(K/\mathbb{Q},G,\varphi)$ состоит в обращении в 0 элемента $\chi^*(c)$.

Для полей алгебраических чисел это условие локализуется. Уточним последнее утверждение в применении к нашей задаче. Для простого числа p обозначим через $\widetilde{K}_p$ тензорное произведение $K\otimes_{\mathbb{Q}}\mathbb{Q}_p$, где $\mathbb{Q}_p$ – поле p-адических чисел. Точно так же, обозначим через $\widetilde{K}_\infty$ тензорное произведение над $\mathbb{Q}$ поля K и поля вещественных чисел $\mathbb{R}$. Обозначим через P множество, состоящее из всех простых чисел и символа ∞. Пусть $\mathfrak{C}$ – группа классов иделей поля K, и пусть

$$\alpha_p:K^*\to\widetilde{K}_p^*,\qquad \beta_p:\widetilde{K}_p^*\to\mathfrak{C}$$

– естественные гомоморфизмы, а

$$\alpha_p^*:H^2(F,K^*)\to H^2(F,\widetilde{K}_p^*),\qquad \beta_p^*:H^2(F,\widetilde{K}_p^*)\to H^2(F,\mathfrak{C})$$

– индуцированные ими гомоморфизмы групп когомологий $(p\in P)$. Из теории полей классов известно, что

- все гомоморфизмы β_p^* инъективны;
- для любого элемента $u \in H^2(F, K^*)$ только конечное число из элементов $\alpha_p^*(u)$ нетривиальны, причем сумма (конечная!) всех элементов $\beta_p^* \, \alpha_p^*(u)$ равна 0 (закон взаимности Артина);
- элемент $u \in H^2(F, K^*)$ равен 0 тогда и только тогда, когда $\alpha_p^*(u) = 0$ для всех $p \in P$.

Из этих свойств сразу следует, что для равенства 0 элемента $u \in H^2(F, K^*)$ необходимо, чтобы для всех $p \in P$ выполнялось равенство $\alpha_p^*(u) = 0$, и достаточно, чтобы это равенство выполнялось для всех $p \in P$, кроме одного (например, p_0): из закона взаимности Артина будет следовать тогда, что $\beta_{p_0}^* \alpha_{p_0}^*(u) = 0$ и, поскольку $\beta_{p_0}^*$ – мономорфизм, что и $\alpha_{p_0}^*(u) = 0$.

Таким образом, задача погружения $(K/\mathbb{Q}, G, \varphi)$ разрешима тогда и только тогда, когда $\alpha_p^*(\chi^*(c)) = 0$ для всех $p \in P$, кроме одного, причем этот исключительный дивизор $p_0 \in P$ может быть выбран произвольно.

Дадим теперь другую интерпретацию условия $\alpha_p^*(\chi^*(c)) = 0$. Для простого числа $p \in P$ обозначим через K_p поле разложения многочлена $f(x)$ над полем p-адических чисел $\mathbb{Q}_p$. Группа Галуа F_p расширения $K_p/\mathbb{Q}$ является подгруппой группы Галуа F расширения $K/\mathbb{Q}$; обозначим через G_p полный прообраз $\varphi^{-1}(F_p)$ и через $\varphi_p : G_p \to F_p$ ограничение φ на G_p. Аналогично, обозначим через K_∞ поле разложения многочлена $f(x)$ над полем вещественных чисел $\mathbb{R}$. Группа Галуа F_∞ расширения $K_\infty/\mathbb{R}$ представляет собой подгруппу группы F; обозначим через G_∞ полный прообраз $\varphi^{-1}(F_\infty)$ и через $\varphi_\infty : G_\infty \to F_\infty$ ограничение φ на G_∞. Условие $\alpha_p^*(\chi^*(c)) = 0$, как хорошо известно, равносильно разрешимости задачи погружения $(K_p/\mathbb{Q}_p, G_p, \varphi_p)$ (конечно, при $p = \infty$ здесь через $\mathbb{Q}_\infty$ обозначено поле вещественных чисел $\mathbb{R}$).

Резюмируя сказанное выше, получаем, что задача погружения $(K/\mathbb{Q}, G_p, \varphi)$ разрешима тогда и только тогда, когда имеют решения задачи погружения $(K_p/\mathbb{Q}_p, G_p, \varphi_p)$ для всех $p \in P$, кроме одного дивизора $p_0 \in P$. В качестве этой исключительной точки возьмем $p_0 = 2$ и рассмотрим отдельно каждую из остальных локальных задач погружения.

(1) $p = \infty$. Производная $f'(x) = 4x^3 - 2n$ многочлена $f(x)$ имеет лишь один вещественный корень. Поскольку между двумя веще-

ственными корнями непрерывно дифференцируемой функции $f(x)$ существует хотя бы один корень ее производной, многочлен $f(x)$ имеет не более двух вещественных корней. С другой стороны, $f(-\infty) > 0$, $f(0) = -1 < 0$, $f(\infty) > 0$, и потому непрерывная функция $f(x)$ имеет по крайней мере один положительный и один отрицательный корень. Итак, у многочлена $f(x)$ ровно два вещественных корня и два комплексно сопряженных невещественных корня. Это значит, что поле K_∞ совпадает с $\mathbb{C}$ и что единственный неединичный элемент группы $F_\infty \subset F$ переставляет два корня (например, a_1 и a_2), оставляя неподвижными два других корня. Итак (1,2) – единственная нетривиальная подстановка корней, входящая в группу Галуа F_∞ расширения $K_\infty/\mathbb{R}$. Таким образом, $F_\infty = \{e, (1,2)\} = \{e, \varphi(s)\}$, и группа $G_\infty = \varphi^{-1}(F_\infty)$ раскладывается в прямое произведение ядра гомоморфизма φ и циклической группы порядка 2, порожденной элементом s. Итак, расширение $1 \to \operatorname{Ker}\varphi_\infty \to G_\infty \to F_\infty \to 1$ расщепляется, и задача погружения $(K_\infty/\mathbb{R}, G_\infty, \varphi_\infty)$ разрешима, как всякая расщепляющаяся задача погружения.

В остальных случаях p – нечетное простое число; через $\overline{f}(x)$ мы будем обозначать многочлен $f(x) \pmod p$ над конечным полем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Для целого числа m будем обозначать через $\overline{m}$ класс вычетов m по модулю p.

(2) Многочлен $\overline{f}(x)$ не имеет кратных корней ни в каком расширении поля $\mathbb{F}_p$. В этом случае

$$\overline{f}(x) = (x - \overline{a}_1)(x - \overline{a}_2)(x - \overline{a}_3)(x - \overline{a}_4),$$

где $\overline{a}_1$, $\overline{a}_2$, $\overline{a}_3$, $\overline{a}_4$ – различные элементы некоторого расширения $\mathbb{F}_q$ поля $\mathbb{F}_p$. Пусть $\mathbb{Q}_p^{nr}$ – неразветвленное расширение поля $\mathbb{Q}_p$ с полем вычетов $\mathbb{F}_q$. По лемме Гензеля многочлен $f(x)$ раскладывается над $\mathbb{Q}_p^{nr}$ в произведение линейных многочленов

$$f(x) = (x - a_1)(x - a_2)(x - a_3)(x - a_4).$$

Таким образом, все корни многочлена $f(x)$ содержатся в поле $\mathbb{Q}_p^{nr}$ и потому $K_p = \mathbb{Q}_p(a_1, a_2, a_3, a_4) \subset \mathbb{Q}_p^{nr}$ – неразветвленное расширения поля $\mathbb{Q}_p$. Но хорошо известно, что любая задача погружения для неразветвленного расширения локального поля всегда разрешима.

(3) У многочлена $\overline{f}(x)$ есть кратный корень в некотором расширении поля $\mathbb{F}_p$. Пусть $\overline{a}_1 = \overline{a}_2$ будет этим кратным корнем. Он

является также корнем производной $\overline{f}'(x) = 4x^3 - 2\overline{n}$, а значит, и многочлена $4\overline{f}(x) - x\overline{f}'(x) = -6\overline{n}x - 4$. Отсюда сразу следует, что в рассматриваемом случае $p \neq 3$ и $\overline{n} \neq 0$, причем $\overline{a}_1 = \overline{a}_2 = -2/3\overline{n}$. Вторая производная $\overline{f}''(x) = 12x^2$ имеет лишь корень 0, который не является корнем многочлена $f(x) = x^4 - 2\overline{n}x - 1$; поэтому кратность корня $\overline{a}_1 = \overline{a}_2$ равна в точности 2. Поскольку кратный корень $\overline{a}_1 = -2/3\overline{n}$ многочлена $f(x)$ является и корнем производной $\overline{f}'(x)$, имеем:

$$0 = \overline{f}'(\overline{a}_1) = 4\overline{a}_1^3 - 2\overline{n} = \frac{-2}{27\overline{n}^3}\big(16 + 27\overline{n}^4\big);$$

поэтому в поле $\mathbb{F}_p$ выполняется соотношение $16 + 27\overline{n}^4 = 0$, т.е. p делит число $16 + 27n^4$. По теореме Виета сумма всех корней многочлена $\overline{f}(x) = x^4 - 2\overline{n}x - 1$ равна 0, а их произведение равно -1. Пусть $\overline{a}_3$, $\overline{a}_4$ – оставшиеся (не кратные) корни многочлена $\overline{f}(x)$ в некотором расширении $\mathbb{F}_q$ поля $\mathbb{F}_p$. Тогда

$$\overline{a}_3 + \overline{a}_4 = -(\overline{a}_1 + \overline{a}_2) = 4/3\overline{n} \quad \text{и} \quad \overline{a}_3\overline{a}_4 = -1/\overline{a}_1\overline{a}_2 = -9\overline{n}^2/4;$$

поэтому многочлен $\overline{f}(x)$ следующим образом раскладывается на множители над полем $\mathbb{F}_p$:

$$\overline{f}(x) = \overline{g}(x)\,\overline{h}(x) = \big((x - \overline{a}_1)(x - \overline{a}_2)\big)\big((x - \overline{a}_3)(x - \overline{a}_4)\big) =$$

$$= (x + 2/3\overline{n})^2\left(x^2 - \frac{4}{3\overline{n}}x - \frac{9\overline{n}^2}{4}\right).$$

Выше мы уже отмечали, что кратность корня $-2/3\overline{n}$ в точности равна 2; поэтому многочлены

$$\overline{g}(x) = \left(x + \frac{2}{3\overline{n}}\right)^2 \quad \text{и} \quad \overline{h}(x) = x^2 - \frac{4x}{3\overline{n}} - \frac{9\overline{n}^2}{4}$$

взаимно просты, и по лемме Гензеля многочлен $f(x)$ раскладывается над полем $\mathbb{Q}_p$ в произведение $f(x) = g(x)h(x)$, где

$$g(x)\,(\operatorname{mod} p) = \overline{g}(x), \qquad h(x)\,(\operatorname{mod} p) = \overline{h}(x).$$

Лемма. *Корни a_3, a_4 многочлена $h(x)$ содержатся в некотором неразветвленном расширении поля $\mathbb{Q}_p$. Если $\overline{a}_3, \overline{a}_4 \in \mathbb{F}_p$, то $a_3, a_4 \in \mathbb{Q}_p$.*

Доказательство. Действительно, $\overline{h}(x) = (x - \overline{a}_3)(x - \overline{a}_4)$, где $\overline{a}_3$, $\overline{a}_4$ – различные элементы расширения $\mathbb{F}_q$ поля $\mathbb{F}_p$ (если $\overline{a}_3$, $\overline{a}_4 \in \mathbb{F}_p$, то $\mathbb{F}_q = \mathbb{F}_p$), потому что единственным кратным корнем многочлена $\overline{f}(x)$ является корень $-2/3\overline{\pi}$ многочлена $\overline{g}(x)$. Пусть $\mathbb{Q}_p'$ – неразветвленное расширение поля $\mathbb{Q}_p$ с полем вычетов $\mathbb{F}_q$ (если $\overline{a}_3$, $\overline{a}_4 \in \mathbb{F}_p$, то $\mathbb{Q}_p' = \mathbb{Q}_p$). По лемме Гензеля многочлен $h(x)$ раскладывается над $\mathbb{Q}_p'$ в произведение $h(x) = (x - a_3)(x - a_4)$. Таким образом, корни a_3, a_4 многочлена $h(x)$ принадлежат неразветвленному расширению $\mathbb{Q}_p'$ поля $\mathbb{Q}_p$.

Дальнейшие рассмотрения разбиваются на 3 случая:

(a) корни $\overline{h}(x)$ содержатся в $\mathbb{F}_p$;

(b) корни $\overline{h}(x)$ не содержатся в $\mathbb{F}_p$, но корни многочлена $g(x)$ содержатся в неразветвленном расширении поля $\mathbb{Q}_p$;

(c) корни $\overline{h}(x)$ не содержатся в $\mathbb{F}_p$ и корни многочлена $g(x)$ не содержатся в неразветвленном расширении поля $\mathbb{Q}_p$.

(a) Этот случай аналогичен случаю $p = \infty$. Корни a_3, a_4 принадлежат полю $\mathbb{Q}_p$ по лемме. Если корни a_1, a_2 многочлена $g(x)$ тоже содержатся в $\mathbb{Q}_p$, то $K_p = \mathbb{Q}_p(a_1, a_2, a_3, a_4) = \mathbb{Q}_p$, $\mathbb{F}_p$ – единичная группа, и задача погружения становится тривиальной. Если же a_1, $a_2 \notin \mathbb{Q}_p$, то $(1, 2)$ – единственная нетривиальная подстановка корней, входящая в группу Галуа F_p расширения $K_p/\mathbb{Q}_p$. Таким образом, $F_p = \{e, (1, 2)\} = \{e, \varphi(s)\}$, и группа $G_p = \varphi^{-1}(F_p)$ раскладывается в прямое произведение ядра гомоморфизма φ и циклической группы порядка 2, порожденной элементом s. Итак, расширение $1 \to \operatorname{Ker}\varphi_p \to G_p \to F_p \to 1$ расщепляется, и задача погружения $(K_p/\mathbb{Q}_p, G_p, \varphi_p)$ разрешима, как всякая расщепляющаяся задача погружения.

(b) Этот случай аналогичен случаю (2). Все корни a_1, a_2, a_3, a_4 многочлена $f(x)$ принадлежат неразветвленному расширению поля $\mathbb{Q}_p$. Поэтому $K_p = \mathbb{Q}_p(a_1, a_2, a_3, a_4)$ – неразветвленное расширение $\mathbb{Q}_p$; но любая задача погружения для неразветвленного расширения разрешима.

(c) Это единственный случай, когда задача погружения $(K_p/\mathbb{Q}_p, G_p, \varphi_p)$ не обязательно разрешима. Пусть $g(x) = x^2 + ux + v$; корни трехчлена $g(x)$ считаются по формуле $a_{1,2} = (-u \pm \sqrt{D_1})/2$, где $D_1 = u^2 - 4v$. Элемент D_1, как и любой элемент локального поля $\mathbb{Q}_p$, представляется в виде $D_1 = \varepsilon p^l$, где ε – p-адическая единица. Если число l четно, $l = 2l_1$, то $\mathbb{Q}_p(a_1, a_2) = \mathbb{Q}_p(\sqrt{D_1}) = \mathbb{Q}_p(\sqrt{\varepsilon})$; но при $p \neq 2$ поле, полученное присоединением к полю $\mathbb{Q}_p$ квадратного корня из p-адической единицы, является неразветвленным расширением $\mathbb{Q}_p$, а это противоречит предположению (с). Следовательно, l нечетно. Поскольку классы вычетов $\overline{a}_1 = \overline{a}_2$, $\overline{a}_3$, $\overline{a}_4$ корней многочлена $f(x)$ по модулю p являются тремя различными элементами поля $\mathbb{F}_q$, разности $a_1 - a_3$, $a_1 - a_4$, $a_2 - a_3$, $a_2 - a_4$, $a_3 - a_4$ представляют собой единицы локального поля K_p; поэтому дискриминант

$$\Delta = \left(\prod_{i<j}(a_i - a_j)\right)^2$$

многочлена $f(x)$ раскладывается в произведение $(a_1 - a_2)^2 = D_1 = p^l\varepsilon$ и единицы ε_1, т.е. $\Delta = p^l\varepsilon_2$, где ε_2 – p-адическая единица. Но, как хорошо известно,

$$\Delta = 108\left(\left(\frac{4}{3}\right)^3 + \left(\frac{-4n^2}{2}\right)^2\right) = \frac{16}{27}\left(16 + 27n^4\right).$$

Таким образом, в рассматриваемом случае простое число p входит в разложение числа $16 + 27n^4$ в нечетной степени l. По предположению (с) корни многочлена

$$\overline{h}(x) = x^2 - \frac{4}{3\overline{n}}x - \frac{9\overline{n}^2}{4}$$

не принадлежат полю $\mathbb{F}_p$; это означает, что дискриминант

$$\left(\frac{4}{3\overline{n}}\right)^2 + 4\frac{9\overline{n}^2}{4} = \left(16 + 81\overline{n}^4\right)/(3\overline{n})^2$$

многочлена $\overline{h}(x)$ не является в $\mathbb{F}_p$ квадратом. Но мы уже отмечали, что $16 + 27\overline{n}^4 = 0$; поэтому $-32 = 16 + 81\overline{n}^4 - 3(16 + 27\overline{n}^4)$ – не квадрат в $\mathbb{F}_p$, или, что то же, -2 – не квадрат в $\mathbb{F}_p$. Таким образом, $\left(\frac{-2}{p}\right) = -1$. Но из закона взаимности Гаусса следует, что

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{(p-1)/2}(-1)^{(p^2-1)/8}.$$

Легко проверить, что

$$(-1)^{(p-1)/2}(-1)^{(p^2-1)/8} = -1$$

тогда и только тогда, когда нечетное простое число p имеем вид $8m+5$ или $8m+7$.

Итак, мы доказали, что случай (3c) возможен лишь тогда, когда p имеет вид $8m+5$ или $8m+7$ и входит в дискриминант в нечетной степни. Остается заметить, что при $p = 8m+5$ задача погружения $(K_p/\mathbb{Q}_p, G_p, \varphi_p)$ разрешима. Это легко следует из описания группы Галуа максимального 2-расширения поля $\mathbb{Q}_p$: она порождается двумя элементами g, h, связанными соотношением $g^{-1}hg = h^{p-1}$. Ясно, что эпиморфизм этой группы на элементарную абелеву группу порядка 4 F_p продолжается до эпиморфизма на диэдральную группу G_p.

Литература

1. В. В. Ишханов, Б. Б. Лурье, Д. К. Фаддеев, *Задача погружения в теории Галуа.* Наука, М. (1990).
2. P. Cassou-Nogues, A. Jehanne, *Parité du nombre de classes des s_4-extensions de $\mathbb{Q}$ et courbes elliptiques.* Pré-publication No. 95-10, Université Bordeaux-1 (1995).

Yakovleva A. A. On an embedding problem.

The following theorem is proved. Let n be an odd integer; if all primes which enter in the canonical decomposition of the integer $16+27n^4$ with odd multiplicities have the form $8m+1$, $8m+3$, or $8m+5$, then the decomposition field of the polynomial $f(x) = x^4 - 2nx - 1$ is embeddable into a nonsplit Galois extension of degree 48.

С.-Петербургский государственный горный институт им. Г. В. Плеханова

Поступило 15 декабря 1999 г.