Алгебра и анализ
Том 27 (2015), № 6

St. Petersburg Math. J.
Vol. 27 (2016), No. 6, Pages 1049–1051
http://dx.doi.org/10.1090/spmj/1435
Article electronically published on September 30, 2016

ULTRASOLVABLE EMBEDDING PROBLEMS FOR NUMBER FIELDS

A. V. YAKOVLEV

Dedicated to Sergeĭ Vladimirovich Vostokov on the occasion of his anniversary

Abstract. It is proved that the existence of an ultrasolvable embedding problem $(K/k, \varphi)$ for finite extensions of the field of p-adic numbers implies the existence of an ultrasolvable embedding problem $(K/k, \varphi)$ for finite extensions of the field of rational numbers.

Let K/k be a finite Galois extension with the Galois group F, and let $\varphi\colon G \to F$ be an epimorphism of finite groups. The embedding problem $(K/k, \varphi)$ consists of construction of a Galois algebra L/k with the Galois group G such that $L \supset K$ and the restriction of any automorphism $g \in G = \mathrm{Gal}(L/k)$ to K coincides with $\varphi(g)$. Let $G_0 \neq G$ be a subgroup of G such that $\varphi(G_0) = F$, and let φ_0 be the restriction of φ to G_0. We say that the embedding problem $(K/k, \varphi_0)$ is *adjoined* to the initial embedding problem. An embedding problem is said to be *ultrasolvable* (see [3]) if it has a solution, but all problems adjoined to it are unsolvable. In other words, this means that the problem has a solution, and all of its solutions are fields. Below p is always a prime integer, and $\mathbb{Q}$ and $\mathbb{Q}_p$ are the fields of rational and p-adic numbers. Our purpose in this paper is to prove the following theorem.

Theorem 1. *Let $\varphi\colon G \to F$ be an epimorphism of finite groups. If there exist finite extensions $\widetilde{k} \subset \widetilde{K}$ of the field $\mathbb{Q}_p$ such that $\widetilde{K}/\widetilde{k}$ is a Galois extension with the Galois group F and the embedding problem $(\widetilde{K}/\widetilde{k}, \varphi)$ is ultrasolvable, then there exist finite extensions $k \subset K$ of the field $\mathbb{Q}$, such that K/k is a Galois extension with the Galois group F and the embedding problem $(K/k, \varphi)$ is ultrasolvable.*

Lemma. *Let $\widetilde{k}$ be a finite extension of the field $\mathbb{Q}_p$, and let $\widetilde{L}$ be its finite Galois extension with the Galois group G. Then there exist finite extensions $k \subset \widetilde{k}$, $L \subset \widetilde{L}$ of the field $\mathbb{Q}$ such that $L\widetilde{k} = \widetilde{L}$, L is a normal extension of the field k, and restriction to L of the automorphisms belonging to the Galois group G of the extension $\widetilde{L}/\widetilde{k}$ determines an isomorphism onto the Galois group of the extension L/k.*

Proof. Let k' and L' denote the fields of all algebraic numbers contained respectively in $\widetilde{k}$ and in $\widetilde{L}$. Obviously, L'/k' is a Galois extension with the Galois group G. Let $\alpha \in L'$ be an element that generates this extension, and let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n$ be the irreducible polynomial with the coefficients $a_i \in k'$ such that α is a root of $f(x)$ (of course, $n = (L' : k') = (\widetilde{L} : \widetilde{k})$). The elements $1, \alpha, \dots, \alpha^{n-1}$ form a basis of L' over k'; for each $g \in G$ the element α^g is contained in L'; consequently, it can be represented in the form

$$\alpha^g = b_{g.0} + b_{g,1}\alpha + \cdots + b_{g,n-1}\alpha^{n-1}, \quad b_{g,j} \in k'.$$

2010 *Mathematics Subject Classification.* Primary 11S20; Secondary 11R32.
Key words and phrases. Galois group, embedding problem.

Let k be the field obtained by adjoining all coefficients $a_i, b_{g,i}$ $(0 \le i < n,\ g \in G)$ to the field $\mathbb{Q}$. The field k is finite over $\mathbb{Q}$ because we have adjoined only finitely many algebraic numbers to $\mathbb{Q}$. Next, set $L = k(\alpha)$; by construction we have $k \subset k' \subset \widetilde{k}$, $L\widetilde{k} = \widetilde{k}(\alpha) = \widetilde{L}$. The number α is a root of the irreducible polynomial $f(x) \in k[x]$ (it is irreducible even over $\widetilde{k}$), and all the other roots α^g of this polynomial can be represented as polynomials in α with coefficients from k; therefore, all roots are contained in L. Thus, the extension L/k is a normal extension, and it is obvious that the restrictions to L of the automorphisms belonging to the Galois group G of the extension $\widetilde{L}/\widetilde{k}$ constitute the Galois group of the extension L/k. □

Proof of Theorem 1. Let $\widetilde{L}$ be a solution of the problem $(\widetilde{K}/\widetilde{k}, \varphi)$, and let L/k be the Galois extension of number fields with the Galois group G that was constructed in the lemma. Let $K = \widetilde{K} \cap L = L^{\operatorname{Ker}\varphi}$. Then K/k is the extension with the Galois group F, and the embedding problem $(K/k, \varphi)$ is solvable (for example, the field L is a solution of this problem). But all embedding problems adjoined to this problem are unsolvable because they do not become solvable even if we extend the ground field k up to the field $\widetilde{k}$. □

To illustrate the applications of Theorem 1, consider two examples of local ultrasolvable embedding problems, due to D. D. Kiselev. The following notation will be used till the end of the paper:

• p is a prime integer, $n \ge 1$ if p is odd and $n \ge 2$ if $p = 2$;

• G_1 is the group generated by a, b with the defining relations $a^{p^{n+1}} = [a, b] = e$, $b^{p^{n+1}} = a^{p^n}$;

• G_2 is the group generated by a, b, c with the defining relations $a^{p^{n+1}} = b^p = c^p = [a, b] = [a, c] = a^{p^n}[b, c] = e$;

• F_i are the quotient groups of the groups G_i by the subgroups generated by a, and $\varphi_i\colon G_i \to F_i$ are the canonical epimorphisms of the groups onto the quotient groups $(i = 1, 2)$.

Next, let k be a finite extension of the field $\mathbb{Q}_p$ that contains a primitive p^nth, but not p^{n+1}th root of unity. The Galois group D of the maximal p-extension M of the field k is generated as pro-p-group by the elements $x_1, x_2, \dots, x_m$ with the only defining relation

$$x_1^{p^n}[x_1, x_2][x_3, x_4] \dots [x_{m-1}, x_m] = e,$$

where $m = (k : \mathbb{Q}_p) + 2$ is an even integer (see [1, 2]). Let $\Psi_i\colon D \to G_i$ be epimorphisms given by the formulas

$$\Psi_1(x_1) = ab^p, \quad \Psi_1(x_2) = b, \quad \Psi_1(x_i) = e \ \text{ if } \ i \ne 1, 2;$$
$$\Psi_2(x_1) = a, \quad \Psi_2(x_3) = b, \quad \Psi_2(x_4) = c, \quad \Psi_2(x_i) = e \ \text{ if } \ i \ne 1, 3, 4.$$

Set $\Phi_i = \varphi_i\Psi_i$; let L_i, K_i be the subfields of the field M belonging to the subgroups $\operatorname{Ker}\Psi_i$, $\operatorname{Ker}\Phi_i$ of the Galois group D of the extension M/k. Then the L_i/k are Galois extensions with the Galois groups G_i, and the K_i/k are Galois extensions with the Galois groups F_i. Obviously, the embedding problems $(K_i/k, \varphi_i)$ are solvable: the fields L_i are their solutions.

We show that these embedding problems are ultrasolvable. If this is not the case, then for $i = 1$ or for $i = 2$ there is a solution of the problem $(K_i/k, \varphi_i)$ that is not a field. Then there is a homomorphism $\Psi_i'\colon D \to G_i$ such that $\varphi_i\Psi_i' = \Phi_i$ and the image of Ψ_i' is not equal to G_i. We show that in both cases this assumption implies the wrong statement $e \ne e$. First, let $i = 1$. Then $\Psi_1'(x_1) = a^s b^p$, $\Psi_1'(x_2) = a^t b$, and the homomorphism Ψ_1' sends all commutators $[x_1, x_2], \dots, [x_{m-1}, x_m]$ to e (here and below s, t, u, v are some

integers). The image of Ψ_1' contains $a^s b^p$ and $a^t b$; it follows that if p does not divide s, then this image coincides with the entire group G_1. Hence, $s = up$, and we have

$$e = \Psi_1'(x_1^{p^n}[x_1, x_2] \dots [x_{m-1}, x_m]) = (a^{p^{n+1}})^u b^{p^{n+1}} = b^{p^{n+1}} = a^{p^n} \neq e.$$

Now, let $i = 2$. Then $\Psi_2'(x_1) = a^s$, $\Psi_2'(x_3) = a^t b$, $\Psi_2'(x_4) = a^v c$, and the homomorphism Ψ_2' sends all commutators $[x_1, x_2], [x_5, x_6], \dots, [x_{m-1}, x_m]$ to e. The image of Ψ_2' contains a^s, $a^t b$, and $a^v c$; it follows that if p does not divide s, then this image coincides with the entire group G_2. Hence, $s = up$, and we have

$$e = \Psi_2'(x_1^{p^n}[x_1, x_2] \dots [x_{m-1}, x_m]) = (a^{p^{n+1}})^u [a^t b, a^v c] = [b, c] \neq e.$$

Due to Theorem 1, from these examples of local ultrasolvable embedding problems it follows immediately that the corresponding examples can be constructed also for global fields.

Theorem 2. *There exist finite extensions k_1, k_2 of the field $\mathbb{Q}$, a Galois extension K_1/k_1 with the Galois group F_1, and a Galois extension K_2/k_2 with the Galois group F_2 such that the embedding problems $(K_1/k_1, \varphi_1)$ and $(K_2/k_2, \varphi_2)$ are ultrasolvable.*

References

[1] S. P. Demuškin, *The group of maximal p-extension of a local fields*, Izv. Akad. Nauk SSSR Ser. Mat. **25** (1961), no. 3, 329–346. (Russian) MR0123565

[2] ———, *On 2-extensions of a local field*, Sibirsk. Mat. Zh. **4** (1963), no. 4, 991–955. (Russian)

[3] D. D. Kiselev and B. B. Lur′e, *Ultrasolvability and singularity in the embedding problem*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **414** (2013), 113–126; English transl., J. Math. Sci. (N.Y.) **199** (2014), no. 3, 306–312. MR3470598

Department of Mathematics and Mechanics, St. Petersburg State University, Universitetskaya ul. 28, Stary Petergof, St. Petersburg 198504, Russia

E-mail address: yakovlev.anatoly@gmail.com

Received 1/OCT/2015

Translated by THE AUTHOR