Алгебра и анализ
Том 30 (2018), № 1

St. Petersburg Math. J.
Vol. 30 (2019), No. 1, Pages 95–102
https://doi.org/10.1090/spmj/1531
Article electronically published on December 5, 2018

ULTRASOLVABLE AND SYLOW EXTENSIONS WITH CYCLIC KERNEL

D. D. KISELEV AND A. V. YAKOVLEV

Abstract. An extension of finite groups is said to be ultrasolvable if there exists a Galois extension of number fields such that its Galois group is a factor group of this group extension and all solutions of the corresponding embedding problem are fields. In the paper, necessary and sufficient conditions of the ultrasolvability of a group extension are obtained for extensions of odd order with cyclic kernel.

§1. Introduction

1.1. The embedding problem for an exact sequence of finite groups

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\varphi} F = \mathrm{Gal}(K/k) \longrightarrow 1$$

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 $\varphi(g)$. For the case of an Abelian kernel, the problem was solved completely in the paper [1], where a solvability criterion was given in homological terms. It turns out that in many cases the search of solutions of the embedding problem in the class of Galois algebras is equivalent to the search of solutions in the class of fields (for example, this is true for extensions of algebraic number fields and a nilpotent kernel, see [2]).

But in some interesting cases one can guarantee *a priori* that all solutions of an embedding problem are fields (as in [3], we say that such embedding problems are *ultrasolvable*). The first nontrivial examples of ultrasolvable embedding problems were constructed in [3, 4]. In connection with the results of [3, 4], one of the authors has formulated the following problem.

Problem 1. Let

$$1 \longrightarrow A \longrightarrow G \xrightarrow{\varphi} F \longrightarrow 1 \tag{1.1}$$

be an extension of finite groups with Abelian kernel A. Under what conditions does there exist a Galois extension of number fields K/k with Galois group F such that the corresponding embedding problem is ultrasolvable?

In the papers [5, 6, 7], Problem 1 was solved for minimal[1] p-extensions of odd order with cyclic kernel and for p-extension of odd order with cyclic kernel and Abelian quotient group.

In this paper we obtain an appropriate generalization of the results of [6, 7] (Theorem 1). Then, using Theorem 1, we completely solve Problem 1 for extensions of odd order with cyclic kernel; this result is the essence of Theorem 2.

2010 *Mathematics Subject Classification.* Primary 12F10; Secondary 12F12, 11R32.
Key words and phrases. Galois algebra, embedding problem, ultrasolvability, Sylow extensions.

[1]See Subsection 1.2.

1.2. Terminology and notation. All groups we consider below are finite if not stated otherwise. Hereinafter, p is always an odd prime integer. We shall say that the extension (1.1) is *ultrasolvable* if for this extension there exists a solution K/k of Problem 1. Assume that the kernel A of the extension (1.1) is an Abelian group. Let p be a prime divisor of the order of the group A. Then we can consider the quotient of the extension (1.1) over the p'-subgroup $A_{p'}$ of A, i.e., the extension

$$1 \longrightarrow A/A_{p'} \longrightarrow G/A_{p'} \xrightarrow{\varphi_{p'}} F \longrightarrow 1, \tag{1.2}$$

where $\varphi_{p'}$ is the epimorphism induced by φ. If in (1.2) p divides $|F|$, then we let F_p be a Sylow p-subgroup of F and G_p the inverse image of F_p under the homomorphism $\varphi_{p'}\colon G/A_{p'} \to F$. If, on the contrary, $p \nmid |F|$, we set $F_p = F$, $G_p = G/A_{p'}$. The extension

$$1 \longrightarrow A/A_{p'} \longrightarrow G_p \xrightarrow{\varphi_{p'}} F_p \longrightarrow 1$$

defined in this way will be called a *p-Sylow subextension* of (1.1).

By a p-local field we mean any finite extension of the field $\mathbb{Q}_p$. We say that k is a local field if k is a p-local field for a prime integer p. By a number field we mean any finite extension of the field $\mathbb{Q}$. For a number field k and its place $\mathfrak{p}$, we denote by $k_\mathfrak{p}$ the $\mathfrak{p}$-adic completion of k. Next, we denote by $\mathcal{O}_k$ the ring of algebraic integers of k, and by $\mathcal{O}_\mathfrak{p}$ the valuation ring of the field $k_\mathfrak{p}$. By $\nu_p(m)$ we denote the exponent of p in the integer m and by ε_m a primitive mth root of unity. If k_1, k_2 are fields of characteristic zero, then $k_1 \cdot k_2$ is the composite of these fields.

Recall some notions that will be important in further considerations. Let $F_1 < F$ be a proper subgroup of the group F from the extension (1.1) and $G_1 < G$ its inverse image under the epimorphism φ. The resulting extension G_1 of F_1 by $A = \ker\varphi$ is called an accompanying extension of the second kind. Now, let A_1 be a proper subgroup of the kernel A of the extension (1.1). Assume that A_1 is a normal subgroup of G; then the epimorphism φ induces an epimorphism $\widehat{\varphi}\colon G/A_1 \to F$ with the kernel A/A_1. The extension obtained in this way is called an accompanying extension of the first kind. In what follows the term "accompanying extensions" is used not only for the accompanying extensions of the first or second kind, but also for their compositions, i.e., extensions of the second kind followed by extensions of the second kind.

We shall call the extension (1.1) *minimal* if (1.1) is not a split extension but all its accompanying extensions are split. Below, by a minimal extension we always mean a minimal p-extension with cyclic kernel.

Let $(K/k, G, \varphi)$ be an embedding problem over a number field k and $\mathfrak{p}$ a place of the field k. Then we can define the $\mathfrak{p}$-localization $(K \otimes_k k_\mathfrak{p}/k_\mathfrak{p}, G, \varphi)$ of the problem $(K/k, G, \varphi)$. If L is a solution of the initial problem, then the Galois algebra $L \otimes_k k_\mathfrak{p}$ is a solution of the $\mathfrak{p}$-local problem $(K \otimes_k k_\mathfrak{p}/k_\mathfrak{p}, G, \varphi)$.

Recall the definition of a Brauer embedding problem. Let $(K/k, G, \varphi)$ be an embedding problem with cyclic kernel A of order m. Assume that the characteristic of the field k does not divide m and that $\varepsilon_m \in K$. The group $\operatorname{Hom}(A, K^*)$ can naturally be made a $\operatorname{Gal}(K/k)$-module:

$$\chi^f(a) = \chi(a^{f^{-1}})^f, \quad \forall \chi \in \operatorname{Hom}(A, K^*), \quad f \in \operatorname{Gal}(K/k), \quad a \in A.$$

The problem $(K/k, G, \varphi)$ is called a Brauer problem if $\chi^f = \chi$ for all $\chi \in \operatorname{Hom}(A, K^*)$ and all $f \in \operatorname{Gal}(K/k)$.

Let $(K/k, G, \varphi)$ be an embedding problem with Abelian kernel A; assume that the characteristic of the field k does not divide the period m of A and that $\varepsilon_m \in K$. Then for any $\chi \in \operatorname{Hom}(A, K^*)$ we can construct the accompanying Brauer embedding problem

$$(K/K_\chi, G_\chi/\ker\chi, \varphi_\chi);$$

here $F_\chi = \mathrm{Gal}(K/K_\chi)$ is the subgroup of all elements of F that act trivially on χ, G_χ is the inverse image of F_χ under φ, and, φ_χ is the epimorphism induced by φ.

Again, let $(K/k, G, \varphi)$ be an embedding problem with Abelian kernel A the period m of which is coprime to the characteristic of the field k, and let[2]

$$\chi \in \mathrm{Hom}(A, K^*)$$

be a homomorphism such that $\chi^f = \chi$ for all $f \in \mathrm{Gal}(K/k)$. The embedding problem $(K/k, G/\ker\chi, \varphi_\chi)$ is called an elementary accompanying Brauer problem (here φ_χ is the epimorphism induced by φ). The well-known Demushkin–Shafarevich theorem (see [8, Chapter 3, §14, Theorem 3.14.1]) states that if k is a local field, then the solvability of all elementary accompanying Brauer problems is necessary and sufficient for the solvability of the initial problem.

Assume that the kernel of the embedding problem $(K/k, G, \varphi)$ is not contained in the Frattini subgroup $\Phi(G)$ of the group G. Then there is a maximal subgroup H of G that does not contain the kernel of the embedding problem; the problem $(K/k, H, \varphi)$ is called a maximal adjoined problem for the problem $(K/k, G, \varphi)$. It is well known (see [3, Theorem 1]) that the problem $(K/k, G, \varphi)$ is ultrasolvable if and only if it has a solution, but all its maximal adjoined problems are unsolvable.

Let L_0/k be a Galois extension of fields with the Galois group G_0. Next, let $i\colon G_0 \to G$ be a monomorphism of finite groups. The group G is the union of right cosets of G_0 in G:

$$G = \bigcup_\rho \rho = \bigcup_\rho G_0\bar\rho,$$

where $\bar\rho$ denotes a representative of a cosets ρ in G; we always assume that $\bar\rho_0 = 1$ for the coset $\rho_0 = G_0$. Recall the construction of the Galois algebra with the Galois group G and the kernel field L_0. As an algebra, L is the direct sum of fields $\bigoplus_\rho L_0E_{\bar\rho}$, where the $E_{\bar\rho}$ are minimal idempotents such that

$$\sum_\rho E_{\bar\rho} = 1.$$

The action of the automorphisms $g \in G$ on L is defined by the formula

$$\Big(\sum_\rho X_{\bar\rho}E_{\bar\rho}\Big)^g = \sum_\rho X_{\bar\rho}^{\bar\rho g\overline{\rho g}^{-1}} E_{\overline{\rho g}}$$

(in particular, $E_{\bar\rho}^g = E_1^{\bar\rho g} = E_1^{\overline{\rho g}}$). Observe that $\bar\rho g$ and $\overline{\rho g}$ belong to the same coset, so that $\bar\rho g\overline{\rho g}^{-1} \in G_0$. It is easily seen that the constructed Galois algebra L over k with the Galois group G and the kernel field L_0 is the induced G-module $\mathrm{ind}_{G_0}^G L_0$.

§2. Galois extensions with prescribed localizations

2.1. Our purpose in this section is to prove the following result, which essentially generalizes Proposition 1 in [9].

Proposition 1. *Let G be a finite group, and let A_i/k_i be Galois algebras with the Galois group G over local fields k_i $(1 \le i \le m)$. Then there exists a Galois extension of the number fields K/k with the Galois group G and distinct places $\mathfrak{p}_1, \dots, \mathfrak{p}_m$ of the field k such that for every i the localization $k_{\mathfrak{p}_i}$ of the field k is isomorphic to k_i and $A_i \cong K \otimes_k k_{\mathfrak{p}_i}$.*

Proof. We start with the following fact, which is well known. But it is difficult to find a suitable reference; that is why we give its proof here.

---

[2]Here it is not required that $\varepsilon_m \in K^*$.

Lemma 1. *There exists a number field $\widetilde{k}$ and its pairwise distinct places $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ such that the localization $\widetilde{k}_{\mathfrak{q}_i}$ of $\widetilde{k}$ is isomorphic to the field k_i for each i, $1 \le i \le m$.*

Proof. It may happen that two or more of the local fields k_i are extensions of the same field $\mathbb{Q}_p$, or even they are isomorphic fields. Let $q_1, \ldots, q_s$ be all prime integers such that each field k_i is a finite extension of one of the fields $\mathbb{Q}_{q_j}$. There exists a number field l with the following property: every of the prime integers q_j completely splits into the product of sufficiently many places such that the decomposition field of each of this places is isomorphic to $\mathbb{Q}_{q_j}$. For example, we can adjoin to $\mathbb{Q}$ the roots of an irreducible polynomial of degree m, which is congruent to the polynomial

$$(x-1)\ldots(x-m)$$

modulo a sufficiently large power of $q_1 \cdot \cdots \cdot q_s$. Then there are pairwise distinct places $\mathfrak{r}_1, \ldots, \mathfrak{r}_m$ of the field l with the following property: if k_i is a finite extension of the field $\mathbb{Q}_{q_j}$, then the field $l_{\mathfrak{r}_i}$ is isomorphic to $\mathbb{Q}_{q_j}$.

For each i, choose an irreducible unitary polynomial $f_i(x)$ with $\mathfrak{r}_i$-adic integer coefficients and such that the field k_i is obtained by adjoining a root of $f_i(x)$ to the field $l_{\mathfrak{r}_i}$. Let $g(x) \in \mathbb{Z}[x]$ be a polynomial of the same degree d_i as the polynomial $f_i(x)$, which is congruent to $f_i(x)$ modulo a sufficiently large power of $\mathfrak{r}_i$ and congruent to $(x-1)\ldots(x-d_i)$ modulo sufficiently large powers of $\mathfrak{r}_j$ for all $j \ne i$. Then the field k_i is obtained by adjoining a root α_i of the polynomial $g_i(x)$ to $l_{\mathfrak{r}_i}$, and this root is contained in all other fields $l_{\mathfrak{r}_j}$, $j \ne i$. The field $\widetilde{k} = l(\alpha_1, \ldots, \alpha_m)$ satisfies all requirements of Lemma 1. □

Let $\widetilde{k}$ be the number field constructed in Lemma 1. We split the rest of the proof into several steps.

Step 1. First, let G be the symmetric group S_n of degree n. Denote by L_i the kernel field of the algebra A_i and by G_i the Galois group of the extension $L_i/\widetilde{k}_{\mathfrak{q}_i}$. Since G_i is a subgroup of the group $G = S_n$, the field L_i is the decomposition field over $\widetilde{k}_{\mathfrak{q}_i}$ of a unitary separable polynomial $f_i(x)$ of degree n with coefficients from the valuation ring $\mathcal{O}_{\mathfrak{q}_i}$ of the local field $\widetilde{k}_{\mathfrak{q}_i}$. The ring $\mathcal{O}_{\widetilde{k}}$ is everywhere dense in $\mathcal{O}_{\mathfrak{q}_i}$ in the $\mathfrak{q}_i$-adic topology. Hence, we may assume without loss of generality that $f_i(x) \in \mathcal{O}_{\widetilde{k}}[x]$ for all i. It is well known (see, e.g., [10, Chapter IV,§3,Theorem 1]) that the decomposition field of the polynomial $f_i(x)$ over $\widetilde{k}_{\mathfrak{q}_i}$ is determined completely by the behavior of $f_i(x)$ in the ring $(\mathcal{O}_{\widetilde{k}}/\mathfrak{q}_i^{N_i})[x]$ for a sufficiently large N_i. More precisely, there is a positive integer N_i such that the following is true: if m is the maximal integer such that $f_i(x)$ decomposes in the ring $(\mathcal{O}_{\widetilde{k}}/\mathfrak{q}_i^{N_i})[x]$ into the product $g_1(x), \ldots, g_m(x)$ of unitary polynomials, then there exist unitary polynomials $G_1(x), \ldots, G_m(x) \in \mathcal{O}_{k_i}[x]$ irreducible over k_i such that

$$f_i(x) = G_1(x) \cdot \cdots \cdot G_m(x)$$

and $G_j(x) \equiv g_j(x) (\mathrm{mod}\, \mathfrak{q}_i^{N_i})$ for all j.

Everywhere below the numbers N_i are chosen so that the above conditions are satisfied.

Fix different places $\mathfrak{r}_1$, $\mathfrak{r}_2$, $\mathfrak{r}_3$ of the field $\widetilde{k}$, distinct from the places $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$. Choose arbitrary unitary polynomials $g_1(x), g_2(x), g_3(x) \in \mathcal{O}_{\widetilde{k}}[x]$ of degree n satisfying the following conditions: $g_1(x)$ is separable and irreducible over the field $\mathcal{O}_{\widetilde{k}}/\mathfrak{r}_1$; $g_2(x)$ is separable over the field $\mathcal{O}_{\widetilde{k}}/\mathfrak{r}_2$ and decomposes into the product of a polynomial of degree $n-1$ and a linear factor; $g_3(x)$ is separable over the field $\mathcal{O}_{\widetilde{k}}/\mathfrak{r}_3$ and decomposes into the product of $n-2$ linear factors and an irreducible quadratic factor. Such choice is possible because of Hensel's lemma and the density of the ring $\mathcal{O}_{\widetilde{k}}$ in the rings $\mathcal{O}_{\mathfrak{r}_1}$, $\mathcal{O}_{\mathfrak{r}_2}$, $\mathcal{O}_{\mathfrak{r}_3}$.

By the Chinese remainder theorem, there exists a polynomial $f(x) \in \mathcal{O}[x]$ of degree n such that

$$f(x) \equiv f_i(x) (\mathrm{mod}\, \mathfrak{q}_i^{N_i}) \quad \text{for all} \quad i \in [1, m] \cap \mathbb{N},$$
$$f(x) \equiv g_j(x) (\mathrm{mod}\, \mathfrak{r}_j) \quad \text{for all} \quad j \in \{1, 2, 3\}.$$

Let K be the decomposition field of the polynomial $f(x)$ over $k = \widetilde{k}$. By our construction, viewed as a permutation group of degree n, the Galois group $\mathrm{Gal}(K/k)$ is a transitive group, it contains a transposition and a cycle of length $n-1$. Hence, $\mathrm{Gal}(K/k) \cong S_n$. Finally, for each $i \in [1, m] \cap \mathbb{N}$ the decomposition group of any place $\mathfrak{B}_i$ of the field K that lies above the place $\mathfrak{p}_i = \mathfrak{q}_i$ is isomorphic to the Galois group of the extension $L_i/\widetilde{k}_{\mathfrak{q}_i}$. Moreover, the integers N_i have been chosen so that for every i the action of the group G_i on the field L_i coincides up to conjugations with the action of the group $\mathrm{Gal}(K/k)$ on the localization $K_{\mathfrak{B}_i}$ of the field K. But we can arrange that those actions be in agreement if we choose another kernel field of the algebra A_i: all kernel fields of a Galois algebra are conjugated. Changing, if necessary, the notation, we may assume that L_i is the required kernel field. Then, by construction, $L_i = K \cdot k_{\mathfrak{p}_i}$ for all i. Hence, the extension K/k satisfies the requirements of Proposition 1 for the case where $G = S_n$. Indeed, the Galois algebra A_i with the Galois group G is determined up to isomorphism by the kernel field with the Galois group G_i and the inclusion $G_i \hookrightarrow G$.

Step 2. Now, let G be an arbitrary finite group. There is an integer n such that G can be imbedded in S_n. Hence, we may assume that G is a subgroup of S_n. Again, let L_i be the kernel field of the Galois algebra A_i and let $G_i = \mathrm{Gal}(L_i/\widetilde{k}_{\mathfrak{q}_i})$. In a standard way, we construct the Galois algebra $B_i/\widetilde{k}_{\mathfrak{q}_i}$ with the kernel field L_i and the Galois group S_n. It suffices to set $B_i = \mathrm{ind}_{G_i}^{S_n} L_i$, where $G_i = \mathrm{Gal}(L_i/\widetilde{k}_{\mathfrak{q}_i}) \leq G \leq S_n$. By Step 1, we can construct a Galois extension $K/\widetilde{k}$ with the group S_n such that the Galois algebra B_i is isomorphic to $K \otimes_{\widetilde{k}} \widetilde{k}_{\mathfrak{q}_i}$ for each $i \in [1, m] \cap \mathbb{N}$.

For every i we choose a place $\mathfrak{B}_i$ of the field K that lies above $\mathfrak{q}_i$; the decomposition group of $\mathfrak{B}_i$ is isomorphic to $\mathrm{Gal}(L_i/\widetilde{k}_{\mathfrak{q}_i})$. But this is the subgroup G_i of G, which in its turn was identified with a permutation group of degree n. Set $k = K^G$; let $\mathfrak{p}_i = \mathcal{O}_k \cap \mathfrak{B}_i$ ($i \in [1, m] \cap \mathbb{N}$). By construction, $\widetilde{k}_{\mathfrak{q}_i} = k_{\mathfrak{p}_i} \cong k_i$ for all $i \in [1, m] \cap \mathbb{N}$, and the Galois algebra A_i is isomorphic to the Galois algebra $K \otimes_k k_{\mathfrak{p}_i}$ because $B_i \cong \mathrm{ind}_{G_i}^{S_n} A_i$. The Galois extension K/k satisfies the requirements of Proposition 1. □

Corollary 1. *Let $\varphi\colon G \to F$ be an epimorphism of finite groups with Abelian kernel, and let $p_1, \ldots, p_m$ be all prime divisors of the order of the group G. For each i, let G_i be a p_i-subgroup of G that contains the p_i-component of the kernel $\ker \varphi$. Denote by F_i the image $\varphi(G_i)$ and by $\varphi_i\colon G_i \to F_i$ the restriction of φ to G_i ($i \in [1, m] \cap \mathbb{N}$). If for every i there exists a Galois extension of local fields K_i/k_i with the Galois group F_i such that the embedding problem $(K_i/k_i, G_i, \varphi_i)$ is ultrasolvable, then there exists a Galois extension K/k of number fields with the Galois group F such that the embedding problem $(K/k, G, \varphi)$ is ultrasolvable.*

Proof. Let L_i/k_i be a solution of the embedding problem $(K_i/k_i, G_i, \varphi_i)$, which exists under the assumptions of Corollary 1, and let A_i/k_i be the Galois algebra with the kernel field L_i for the inclusion $\mathrm{Gal}(L_i/k_i) = G_i \hookrightarrow G$ (simpler, let $A_i = \mathrm{ind}_{G_i}^{G} L_i$ with the structure of an algebra defined in Subsection 1.2). By Proposition 1, there exists a Galois extension of number fields L/k with the Galois group G and distinct places $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ of the field k, such that for each i the localization $k_{\mathfrak{p}_i}$ of k is isomorphic to the field k_i and the kernel field L_i of the algebra A_i is isomorphic to the kernel field of the k_i-algebra $L \otimes_k k_{\mathfrak{p}_i}$, i.e., to the composite $L \cdot k_{\mathfrak{p}_i}$. Let K be the field $L^{\ker \varphi}$; then the embedding problem $(K/k, G, \varphi)$ is solvable by construction: the field L is one of its solutions.

Now, let G' be an arbitrary maximal subgroup of G that does not contain $\ker\varphi$ (if there are no such subgroups, then $\ker\varphi \le \Phi(G)$, and the ultrasolvability of the embedding problem under consideration follows from [8, Chapter 1,§6, Corollary 5]). Then the group G' does not contain the Sylow p_i-subgroup of the kernel $\ker\varphi$ for at least one i. Hence, the subgroup $G_i' = G_i \cap G'$ is a proper subgroup of G_i. On the other hand, $\varphi(G_i') = F_i$; we denote by $\varphi'\colon G' \to F$ and $\varphi_i'\colon G_i' \to F_i$ the restrictions of φ to G' and of φ_i to G_i'. Since the problem $(K_i/k_i, G_i, \varphi_i)$ is ultrasolvable, the problem $(K_i/k_i, G_i', \varphi_i')$ has no solutions because it is an adjoined problem for the problem $(K_i/k_i, G_i, \varphi_i)$. But the problem $(K_i/k_i, G_i', \varphi_i')$ is the localization of the embedding problem that is an accompanying problem for the problem $(K/k, G', \varphi')$; it follows that the problem $(K/k, G', \varphi')$ is unsolvable. Thus, all adjoined embedding problems of the solvable problem $(K/k, G, \varphi)$ are not solvable. By [3, Theorem 1], the problem $(K/k, G, \varphi)$ is ultrasolvable. □

Remark 1. In Corollary 1 it was assumed that the kernel $\operatorname{Ker}\varphi$ is Abelian. We need this only for the problem $(K_i/k_i, G_i', \varphi_i')$ to be the localization of a problem that is **accompanying** for $(K/k, G', \varphi')$.

§3. Application to ultrasolvability problems

3.1. Let

$$1 \longrightarrow A_p \longrightarrow G_p \xrightarrow{\varphi_p} F_p \longrightarrow 1 \tag{3.1}$$

be a p-extension of odd order with cyclic kernel.

Now we formulate some conditions on a p-local field k_p; these conditions will play a key role in the subsequent arguments.

Conditions 1. Let $p^n = |A_p|$. If (3.1) is a central extension, then

$$\varepsilon_{p^{n-1}} \in k_p, \quad \varepsilon_{p^n} \notin k_p.$$

On the contrary, if the group F_p generates a subgroup of $\operatorname{Aut} A_p$ with a generator $a_p \mapsto a_p^{1+p^i}$, $1 \le i < n$, then

$$\varepsilon_{p^i} \in k_p, \quad \text{but} \quad \varepsilon_{p^{i+1}} \notin k_p.$$

Theorem 1. *Let* (1.1) *be a p-extension of odd order with cyclic kernel A and quotient group F. Assume that the extension* (1.1) *does not split but all its accompanying extensions of the second kind split. Then there exists a Galois extension of local fields K/k with the Galois group F such that the corresponding embedding problem $(K/k, G, \varphi)$ is ultrasolvable.*

Proof. In the papers [6, 7] it was proved that every minimal p-extension of odd order with cyclic kernel is ultrasolvable. Recall that, first, the local ultrasolvability of minimal p-extensions was established. Namely, the following statement was proved: if the field k is a finite extension of $\mathbb{Q}_p$ of sufficiently large degree and if Conditions 1 are fulfilled, then it is possible to construct a Galois extension K/k with the Galois group F such that the problem $(K/k, G, \varphi)$ is ultrasolvable. Moreover, the extension K/k constructed in [6, 7] is such that the problem $(K/k, G, \varphi)$ is not a Brauer problem (because $\varepsilon_{|A|} \notin K$), but all its maximal adjoined problems are Brauer problems. Therefore, we may assume without loss of generality that the extension (1.1) is not minimal. In particular, $|A| > p$.

Let $h \in H^2(F, A)$ be the cohomology class that defines the extension (1.1). We assume that the extension (1.1) is not minimal. Therefore, there exists a proper subgroup A_1 of the group A such that the homomorphism of cohomologies [3]

$$H^2(F, A) \to H^2(F, A/A_1)$$

induced by the canonical epimorphism of F-modules $A \to A/A_1$ maps the class h to the class h_1 that corresponds to a minimal extension. We use the fact that any accompanying extension of second kind for the extension (1.1) splits. Thus, the extension

$$1 \longrightarrow A/A_1 \longrightarrow G/A_1 \xrightarrow{\varphi} F = \mathrm{Gal}(K/k) \longrightarrow 1$$

corresponding to h_1 is minimal. Let k be a p-local field of sufficiently large degree over $\mathbb{Q}_p$ such that Conditions 1 are fulfilled. As has been mentioned, we can construct a Galois extension K/k with the Galois group F such that the problem $(K/k, G/A_1, \varphi_1)$ is ultrasolvable; it is not a Brauer embedding problem because $\varepsilon_{|A/A_1|} \notin K$.

We prove that the problem $(K/k, G, \varphi)$ that corresponds to the class h is ultrasolvable. Indeed, since $\varepsilon_{|A/A_1|} \notin K$, all Brauer elementary accompanying problems for the problem $(K/k, G, \varphi)$ are accompanying embedding problems of the first kind for the solvable problem $(K/k, G/A_1, \varphi_1)$. But then from [8, Chapter 3, §14, Theorem 3.14.1] it follows that the problem $(K/k, G, \varphi)$ is solvable (see also [8, Chapter 4, §2]). Finally, any solution L of the problem $(K/k, G, \varphi)$ is a solution of the problem $(L_1/k, G, \varphi_0)$, where φ_0 is the canonical epimorphism and L_1 is an arbitrary solution of the ultrasolvable problem $(K/k, G/A_1, \varphi_1)$. But L_1 is a field and $\ker \varphi_0$ is contained in the Frattini subgroup $\Phi(G)$. Hence, the problem $(L_1/k, G, \varphi_0)$ is ultrasolvable, which means in particular that L is a field. Thus, the problem $(K/k, G, \varphi)$ satisfies all requirements of the theorem that we prove. □

Now we establish the principal result of the paper.

Theorem 2. *Let* (1.1) *be an extension of odd order with cyclic kernel. The extension* (1.1) *is ultrasolvable if and only if all its Sylow subextensions do not split.*

Proof. The necessity part is almost evident. Indeed, let the extension (1.1) be ultrasolvable. This means that there exists a Galois extension of number fields K/k such that the embedding problem $(K/k, G, \varphi)$ for the extension (1.1) is ultrasolvable. But the problem $(K/k, G, \varphi)$ decomposes into the direct product of problems $(K/k, G^{(p)}, \varphi_p)$ where $G^{(p)} = G/A_{p'}$ and $\varphi_p\colon G^{(p)} \to \mathrm{Gal}(K/k)$ is the epimorphism induced by φ. The kernel of the epimorphism φ_p is the Sylow p-subgroup A_p of the group

$$A = \ker \varphi.$$

Any solution L of the problem $(K/k, G, \varphi)$ is the tensor product over K of solutions of problems $(K/k, G^{(p)}, \varphi_p)$. Since a solution of any of these problems is linearly separated from the composite of solutions of all other problems, the problem $(K/k, G, \varphi)$ is ultrasolvable if and only if the problems $(K/k, G^{(p)}, \varphi_p)$ are ultrasolvable for all $p \mid |A|$. In particular, if $(K/k, G, \varphi)$ is ultrasolvable, then none of the problems $(K/k, G^{(p)}, \varphi_p)$ with $p \mid |A|$ is a semidirect problem. But then by the Gaschütz–Faddeev theorem (see [11, Chapter IV, §6, Corollary 4]) all Sylow subextensions of (1.1) do not split.

Assume now that all Sylow subextensions of (1.1) do not split. Let (3.1) be a p-Sylow subextension that corresponds to the cohomology class $h_p \in H^2(F_p, A_p)$. There exists a subgroup F_{1p} of the group F_p such that the restriction h_{1p} of the class h_p to F_{1p} is not trivial, but the restriction of h_p to any proper subgroup of F_{1p} is trivial. By Theorem 1, there is a Galois extension of p-local fields K_p/k_p with the Galois group F_{1p} such that the problem $(K_p/k_p, G_{1p}, \varphi_p)$ with the class h_{1p} is ultrasolvable.

It remains to apply Corollary 1. □

[3]Recall that A is a cyclic p-group.

References

[1] A. V. Yakovlev, *The embedding problem for fields*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), no. 3, 645–660. (Russian) MR0163907

[2] V. V. Išhanov, *The semidirect embedding problem with a nilpotent kernel*, Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), no. 1, 3–25; English transl., Math. USSR-Izv. **10** (1976), no. 1, 1–23. MR0414519

[3] D. D. Kiselev and B. B. Lur′e, *Ultrasolvability and singularity in an 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

[4] D. D. Kiselev, *Examples of embedding problems in which the only solutions are fields*, Uspekhi Mat. Nauk **68** (2013), no. 4, 181–182; English transl., Russian Math. Surveys **68** (2013), no. 4, 776–778. MR3154820

[5] D. D. Kiselev, *On the ultrasolvability of group p-extensions of an abelian group with the help of a cyclic kernel*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **452** (2016), 108–131. (Russian) MR3589286

[6] D. D. Kiselev and I. A. Chubarov, *On the ultrasolvability of some classes of minimal non-semidirected p-extensions with a cyclic kernel for $p > 2$*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **252** (2016), 132–157. (Russian) MR3589287

[7] D. D. Kiselev, *Minimal p-extensions and the embedding problem*, Comm. Algebra, **46** (2018), No. 1, P. 290–321. MR3764864

[8] V. V. Ishkhanov, B. B. Lur′e and D. K. Faddeev, *The embedding problem in Galois theory*, Nauka, Moscow, 1990; English transl., Transl. Math. Monogr., vol. 165, Amer. Math. Soc., Providence, RI, 1997. MR1223544

[9] A. V. Yakovlev, *Ultrasolvable embedding problems for number fields*, Algebra i Analis **27** (2015), no. 6, 260–263; English transl., St. Petersburg. Math. J. **27** (2016), no. 6, 1049–1051. MR3589231

[10] Z. I. Borevich and I. R. Shafarevich, *The theory of numbers*, Nauka, Moscow, 1985; English transl. first eds., Pure Appl. Math., vol. 20, Acad. Press, New York, 1966. MR0816135 (88f:11001)

[11] J. W. S. Cassels and A. Fröhlich (Eds.), *Algebraic number theory*, Acad. Press, London, 1967. MR0215665 (35:6500)

All-Russian Academy of Foreign Trade, the Ministry of Economic Development of RF, ul. Pudovkina 4a, 119285 Moscow, Russia

Email address: denmexmath@yandex.ru

Department of Mathematics and Mechanics, St. Petersburg State University, Universitetsky prospekt 28, Peterhof, St. Petersburg 198504, Russia

Email address: yakovlev.anatoly@gmail.com

Received 25/OCT/2017

Translated by A. V. YAKOVLEV