S. P. Demushkin

1962

SovietRxiv

Abstract

Full Text

S. P. Demushkin

THE EMBEDDING PROBLEM FOR FIELDS OF ALGEBRAIC NUMBERS

(Presented by Academician I. M. Vinogradov on 25 XII 1961)

The embedding problem $(k/\Omega, G, \varphi)$ is considered in the formulation and under the assumptions of the paper ([1]); in particular, it is assumed that G is a p-group. It is also assumed that k is a field of algebraic numbers of finite degree.

As is known, a solution of the embedding problem can be constructed by successive p-steps, which correspond to choosing invariant subgroups of index p, p^2, and so on in the kernel. These successive solutions must be chosen so that the compatibility condition is preserved at each stage. Suppose that $r-1$ steps can be carried out in the embedding problem in such a way that the compatibility condition is preserved. Denote the field obtained in this way by $k^{(r-1)}$. Let us determine the conditions under which it is possible to carry out r steps in the embedding problem while preserving the compatibility condition.

For this purpose consider the embedding problem

$$\overline{P}_{r-1}(k^{(r-1)}/\Omega,\, G/A_r,\, \overline{\varphi}_{r-1}),$$

where A_r is the invariant subgroup corresponding to the r-th step. The embedding problem $\overline{P}_{r-1}$ is solvable, since for the problem

$$P_{r-1} = (k^{(r-1)}/\Omega,\, G,\, \varphi_{r-1})$$

the compatibility condition is satisfied, and the problem $\overline{P}_{r-1}$ accompanies it. Let k_r' be a solution of the problem $\overline{P}_{r-1}$. For the problem $(k_r'/\Omega, G, \varphi_r)$, compatibility is determined by the algebras $C_{\chi_i^{(r)}}$ defined by the characters $\chi_i^{(r)}$ of the group A_r. These algebras, by virtue of the choice of $k^{(r-1)}$, will be cyclic. Let $\mathfrak{p}$ be a prime divisor of the field Ω and $\mathfrak{P}_{ij}$ its divisors in the field $k_{\chi_i^{(r)}}$. Take an arbitrary set of integers

$$c' = \{c_{ij}'^{(\mathfrak{p})}\}$$

and form the function

$$J(c') = \prod_{\mathfrak{p},i,j} \mu_{\mathfrak{P}_{ij}}(C_{\chi_i^{(r)}})^{c_{ij}'^{(\mathfrak{p})}}.$$

Here $\mu_{\mathfrak{P}_{ij}}(C_{\chi_i^{(r)}})$ is the invariant of the algebra $C_{\chi_i^{(r)}}$ at the point $\mathfrak{P}_{ij}$ in multiplicative form. This product is meaningful, since only for a finite number of divisors $\mathfrak{P}_{ij}$ is the invariant

$$\mu_{\mathfrak{P}_{ij}}(C_{\chi_i^{(r)}}) \neq 1.$$

The function $J(c')$ is some p-th root of unity; generally speaking, it depends on the choice of the fields $k^{(r-1)}$ and k'_r. We are interested in those

$$c = \{c_{ij}^{(\mathfrak{p})}\}$$

for which $J(c)$ does not depend on the choice of the fields $k^{(r-1)}$ and k'_r. Clearly, if c has this property, then so does

$$c + pc_1, \qquad pc_1 = \{pc_{ij}^{(\mathfrak{p})}\},$$

since always $J(c' + pc'_1) = J(c')$. Denote by H the group $(c)/(pc)$, where (c) is the group generated by the elements c.

Theorem. The group H is finite. In order that there exist a solution of the embedding problem $(k/\Omega, G/A_r, \varphi_r)$, a field $k^{(r)}$ such that for the embedding problem

$$P_r = (k^{(r)}/\Omega,\, G,\, \varphi_r)$$

the compatibility condition is satisfied, it is necessary and sufficient that all $J(c)$, $c \in H$, be equal to unity.

Proof. If the field $k^{(r)}$ is such that for the embedding problem P_r the compatibility condition is satisfied, then, taking as k'_r the field $k^{(r)}$, we shall have

$$C_{\chi_i^{(r)}} \sim 1$$

for all $\chi_i^{(r)}$. Therefore $J(c) = 1$ for every $c \in H$. Thus the necessity of the condition of the theorem is proved.

We now show that there are only finitely many elements c. Indeed, fix the field $k^{(r-1)}$ and vary the field k'_r. This means that we consider the first step for the embedding problem P_{r-1}. As shown in ([2]), to each element $c \in H$ one can put in correspondence a number

a_c from Ω such that $\Omega(\sqrt[p]{a_c}) \subset k^{(r-1)}$. Since all the algebras under consideration will in our case be defined over subfields of the field k, in fact we shall have $\Omega(\sqrt[p]{a_c}) \subset k$. This number is determined up to p-th powers. But, up to p-th powers, there are only finitely many of the numbers a_c; therefore there will also be only finitely many elements c.

Let now all $J(c)$, $c \in H$, be equal to 1. We shall prove by induction that then there exists a field $k^{(r)}$ such that, for the problem P_r, the compatibility condition is satisfied. For $r = 1$ the proof of this assertion was given in ([2]). Suppose that the assertion is true for $r - 1$. Fix in $k^{(r-1)}$ a subfield $k^{(1)}$, and within these limits we shall vary the fields $k^{(r-1)}$ and k'_r. By the choice of

$k^{(1)}$, for the embedding problem P_1 the compatibility condition is satisfied. For such a problem, the possibility of finding a field $k^{(r)}$ compatible with P_r means the possibility of carrying out $r-1$ steps while preserving the compatibility condition. A necessary and sufficient condition for this is the reduction to 1 of all $J(c)$ which do not depend on $k^{(r-1)}$ and k'_r ($k^{(r-1)}$ must, of course, contain $k^{(1)}$). To reduce such $J(c)$ to 1 we have only one possibility: to vary the field $k^{(1)}$. Let us see how $J(c)$ depends on the field

$$k^{(1)} = k(\sqrt[n]{\mu_1 m_1}), \quad m_1 \in \Omega$$

(on m_1 there are also imposed certain conditions, invariant, however, with respect to multiplication). To this end, decompose the algebra $C_{x_i^{(r)}}$ into a product of two algebras:

$$C_{x_i^{(r)}} \sim \overline{C}_{x_i^{(r)}} \otimes \widetilde{C}_{x_i^{(r)}},$$

where $\overline{C}_{x_i^{(r)}}$ is some fixed algebra of the type $C_{x_i^{(r)}}$, and $\widetilde{C}_{x_i^{(r)}}$ is the algebra computed for the split group extension. The function $J(c)$ will therefore be represented in the form of a product

$$J(c) = \overline{J}(c)\,\widetilde{J}(c).$$

Since $J(c)$ does not depend on the choice of the fields $k^{(r-1)}$ ($k^{(r-1)} \supset k^{(1)}$) and k'_r, it follows that $\widetilde{J}(c)$ does not depend on such a choice. Applying to the algebra $\widetilde{C}_{x_i^{(r)}}$ the generalization of Theorem 2 from ([1]) on multiplication of algebras, we obtain that $\widetilde{J}(c)$ depends on m_1 multiplicatively. Let us write this dependence explicitly:

$$J(c) = \overline{J}(c)\,\widetilde{J}(c, m_1).$$

We need to achieve that $J(c) = 1$. There are only finitely many such $\overline{J}(c)$. Let these be $J(c_1), J(c_2), \dots, J(c_t)$. It is necessary, therefore, that the equations

$$\overline{J}(c_i)\,\widetilde{J}(c_i, m_1) = 1$$

be solvable, or

$$\widetilde{J}(c_i, m_1) = \overline{J}(c_i)^{-1}.$$

We shall show that, under our assumptions, this system of equations is solvable. Indeed, the solvability condition for such a system of equations is the following property: if

$$\prod_i \widetilde{J}(c_i, m_i)^{a_i} = 1$$

for all m_i, for some set of integers a_i, then it must be that

$$\prod_i \overline{J}(c_i)^{-a_i} = 1,$$

or

$$\prod_i \overline{J}(c_i)^{a_i} = 1.$$

Suppose

$$\prod_i \widetilde{J}(c_i, m_1)^{a_i} = 1.$$

This means that

$$\widetilde{J}(c) = \prod_i \widetilde{J}(c_i, m_1)^{a_i} = 1,$$

where

$$c \approx \prod_i c_i^{a_i}$$

(equality up to p-th powers), does not depend on the choice of the fields $k^{(r-1)}$ and k_r'. Since

$$J(c) = \overline{J}(c)\,\widetilde{J}(c),$$

it follows that $J(c)$ also does not depend on the choice of $k^{(r-1)}$ and k_r'. The latter means that, by the condition of the theorem, it must be that $J(c) = 1$; then

$$J(c) = \overline{J}(c)\,\widetilde{J}(c) = 1.$$

The theorem is proved.

Mathematical Institute named after V. A. Steklov
Academy of Sciences of the USSR

Received
25 XII 1961

REFERENCES

1. S. P. Demushkin, I. R. Shafarevich, *Izv. AN SSSR, ser. matem.*, **23**, 823 (1959).

2. S. P. Demushkin, I. R. Shafarevich, *Izv. AN SSSR, ser. matem.*, **26**, No. 6 (1962).

Note: Figure translations are in progress. See original paper for figures.