МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2008
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2008
Proceedings of the Thirty Seventh Spring Conference of
the Union of Bulgarian Mathematicians
Borovetz, April 2–6, 2008

THE INVERSE PROBLEM OF GALOIS THEORY*

Ivo M. Michailov, Nikola P. Ziapkov

In this survey we outline the milestones of the Inverse Problem of Galois theory historically up to the present time. We summarize as well the contribution of the authors to the Galois Embedding Problem, which is the most natural approach to the the Inverse Problem in the case of non-simple groups.

1. Introduction. Let G be a finite group, and let K be a field. The Inverse Problem of Galois Theory consists of two parts:

i: **Existence.** Determine whether there exists a Galois extension M/K such that the Galois group $\mathrm{Gal}(M/K)$ is isomorphic to G.

ii: **Actual construction.** If G is realisable as a Galois group over K, construct explicitly either Galois extensions or polynomials over K having G as a Galois group.

The classical Inverse Problem of Galois Theory is the existence problem for the field $K = \mathbb{Q}$ of rational numbers. The question of whether all finite groups can be realized over $\mathbb{Q}$ is one of the most challenging problems in mathematics, and it is still unsolved. In this connection, an especially interesting version of the Inverse Problem concerns regular extensions: Let $\mathbf{t} = (t_1, t_2, \ldots, t_n)$ be indeterminates. A finite Galois extension $\mathbb{M}/\mathbb{Q}(\mathbf{t})$ is called *regular*, if $\mathbb{Q}$ is relatively algebraically closed in $\mathbb{M}$, i.e., if every element in $\mathbb{M} \setminus \mathbb{Q}$ is transcedental over $\mathbb{Q}$. **The Regular Inverse Galois Problem** asks: Is every finite group realisable as the Galois group of a regular extension of $\mathbb{Q}(\mathbf{t})$? Whenever we have a regular Galois extension $\mathbb{M}/\mathbb{Q}(\mathbf{t})$, by the Hilbert Irreducibility Theorem there is a 'specialization' $M/\mathbb{Q}$ with the same Galois group. Moreover, we get such specialized extensions M/K over any Hilbertian field in characteristic 0.

The above Inverse Problems have been solved in the affirmative in some cases, e.g.:

(1) If $K = \mathbb{C}(t)$, where t is an indeterminate, then any finite group G occurs as a Galois group over K. This follows basically from the Riemann Existence Theorem. More generally, the absolute Galois group of the function field $K(t)$ is free pro-finite with infinitely many generators, whenever K is algebraically closed, cf. [2].

(2) If $K = \mathbb{F}_q$ is a finite field, then the Galois group of every polynomial over K is a cyclic group.

(3) If K is a $\mathfrak{p}$-adic field, then any polynomial over K is solvable.

*This work is partially supported by project N 8/2007 of Shumen University.
2000 Mathematics Subject Classification: Primary 12F12, secondary 12F10.
Key words: Inverse Galois theory, embedding problem.

There are several monographs devoted to the Inverse Problems, and containing an extensive survey, e.g. [14, 43, 39, 4]. In the following section we briefly discuss some of the most significant results in this area.

2. Milestones of the Inverse Problem. In the early nineteenth century, the following result was established:

Theorem 2.1 (Kronecker-Weber)**.** *Any finite abelian group G occurs as a Galois group over $\mathbb{Q}$. Furthermore, G can be realized as the Galois group of a subfield of the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is an n-th root of unity for some natural number n.*

The proof can be found in most books on class field theory.

The first systematic study of the Inverse Galois Problem started with Hilbert in 1892. Hilbert used his Irreducibility Theorem to establish the following result:

Theorem 2.2. *For any $n \geq 1$, the symmetric group S_n and the alternating group A_n occur as Galois groups over $\mathbb{Q}$.*

The first explicit examples of ploynomials with the alternating group A_n as a Galois group were given by Schur [36] in 1930.

In 1916, E. Noether [33] raised the following question:

THE NOETHER PROBLEM. *Let $M = \mathbb{Q}(t_1, \ldots, t_n)$ be the field of rational functions in n indeterminates. The symmetric group S_n of degree n acts on M by permuting the indeterminates. Let G be a transitive subgroup of S_n, and let $K = M^G$ be the subfield of G-invariant rational functions of M. Is K a rational extension of $\mathbb{Q}$? I.e., is K isomorphic to a field of rational functions over $\mathbb{Q}$?*

If the Noether Problem has an affirmative answer, then G can be realised as a Galois group over $\mathbb{Q}$, and in fact over any Hilbertian field of characteristic 0.

The next important step was taken in 1937 by A. Scholz and H. Reichard [37, 35] who proved the following existence result:

Theorem 2.3. *For an odd prime p, every finite p-group occurs as a Galois group over $\mathbb{Q}$.*

It is not known whether there is a regular Galois extension of $\mathbb{Q}(t)$ with Galois group G for an arbitrary p-group G.

The final step concerning solvable groups was done by Shafarevich [40], although with a gap when the prime 2 divides the order of the group. In the notes appended to his Collected papers, p. 752, Shafarevich sketches a method to correct this. For a full correct proof, the reader is referred to the book by Neukirch, Schmidt and Wingberg [34, Chapter IX].

Theorem 2.4 (Shafarevich)**.** *Every solvable group occurs as a Galois group over $\mathbb{Q}$.*

Of the finite simple groups, the projective groups $\mathrm{PSL}(2, p)$ for some odd primes p were among the first to be realized. The existence was established by Shih in 1974 and later polynomials were constructed by Malle and Matzat:

Theorem 2.5 (Shih [41])**.** *Let p be an odd prime such that either $2, 3$ or 7 is a quadratic non-residue modulo p. Then $\mathrm{PSL}(2, p)$ occurs as a Galois group over $\mathbb{Q}$.*

Theorem 2.6 (Malle & Matzat [13]). *Let p be an odd prime with $p \not\equiv \pm 1 \pmod{24}$. Then explicit families of polynomials over $\mathbb{Q}(t)$ with Galois group $\mathrm{PSL}(2,p)$ can be constructed.*

For the 26 sporadic simple groups, all but possibly one, namely, the Mathieu group $\mathbf{M}_{23}$, have been shown to occur as Galois groups over $\mathbb{Q}$ by Matzat and his collaborators.

The Fischer-Griess group M, known as the "Monster", is the largest of the sporadic simple groups. Its order is

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

In 1984, Thompson succeeded in proving the following existence theorem:

Theorem 2.7 (Thompson [42]). *The monster group occurs as a Galois group over $\mathbb{Q}$.*

For the proof of the latter Theorem, however, one is forced to rely upon the classification theorem for the finite simple groups. (Some doubts remain as to whether a proof of the classification theorem, spread over 500-odd articles, is complete and correct, not to mention that the part on "quasi-thin" groups has never been published.)

Later several families of simple linear groups were realized as Galois groups over $\mathbb{Q}$ (see [14]).

It should be noted that all these realization results of simple groups were achieved via the rigidity method and the Hilbert Irreducibility Theorem. For a detailed exposition of this approach, the readers are referred to the books [14, 39].

Another noteworthy approach to the Inverse Problem, applicable for specific non-simple groups, is based on trace forms, i.e., quadratic forms of the type $x \mapsto \mathrm{Tr}_{L/K}(x^2)$ defined on a field extension L/K. Given a finite Galois extension M/K with Galois group G, we can consider G as a transitive subgroup of the symmetric group S_n for some natural number n. Let $\widetilde{S}_n$ be the *stem cover* of S_n, i.e., the *double cover*

$$1 \to \{\pm 1\} \to \widetilde{S}_n \to S_n \to 1$$

in which transpositions lift to elements of order 2, and products of two disjoint transpositions lift to elements of order 4. Then we get a double cover $\widetilde{G}$ of G, and we can ask: Can M/K be extended to a $\widetilde{G}$-extension F/K? The answer to this question involves the study of trace forms, and have been used by Mestre [17] and others to realise stem covers of alternating groups as regular extensions over $\mathbb{Q}$. Serre [38] studied the trace form $\mathrm{Tr}_{L/K}(x^2)$ in detail. This approach is sometimes applied to other groups, e.g. 2-groups, in connection with the orthogonal Galois representations and Clifford groups.

Recently, there has been developed plenty of computational methods, aided by a computer, determining the Galois groups of polynomials over $\mathbb{Q}$. Some of these results are published in Journal of Symbolic Computation, Volume 30, Issue 6 (Dec. 2000) "Algorithmic methods in Galois Theory", see e.g. [6], where Kluners and Malle show that every transitive group of degree up to 15 is realisable as a Galois group over $\mathbb{Q}$. In another paper by the same authors [7] is announced the creation of a database for number fields. It encompasses roughly 100 000 polynomials generating distinct number fields over the rationals of degrees up to 15. The database contains polynomials for all transitive permutation groups up to that degree, and is accessed via the computer algebra system Kant. In the same paper is published a result by Serre, which states that if *every* finite group is realisable as a Galois group over $\mathbb{Q}$, then it is in fact possible to realise them inside $\mathbb{R}$. The applications of this result could lead potentially to a negative answer to

the classical Inverse Galois Problem, if, for example, one discovers a group which does not posses a real field that realises it over $\mathbb{Q}$. That is another reason for the interest in the explicit construction of all fields that realise a given group as a Galois group. Such a negative result, however, is extremely difficult to discover. In fact, the only negative result regarding realisability over $\mathbb{Q}$ (with an extra condition) known to us is due to Jan Brinkuis:

Theorem 2.8 (Brinkuis, [1]). *There is no Galois extension of $\mathbb{Q}$ with cyclic Galois group of odd prime power order which has a normal integral basis over any proper intermediate field.*

3. The Embedding Problem. Let K/k be a Galois extension with Galois group F, and let

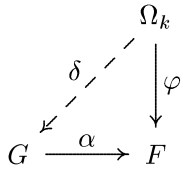
$$1 \to A \to G \xrightarrow{\alpha} F \to 1, \tag{3.1}$$

be a finite group extension. Then *the embedding problem* $(K/k, G, A)$ consists in determining whether there exists a Galois algebra (called also a *weak* solution), or a Galois extension (called a *proper* solution) L/k, such that $K \subset L$, $G \cong \mathrm{Gal}(L/k)$ and the homomorphism of restriction to K of the automorphisms from G coincides with α. The notion of Galois algebra was invented independently by Faddeev and Hasse as a generalization of the Galois extension, which makes amends for the possible lack of Galois extensions solving the split embedding problems. The group A is called *the kernel* of the embedding problem.

Thus, the embedding problem becomes the main tool of investigations of the realisability of a given group G over arbitrary fields. Today, the theory of embedding problems is so developed, that one can deem it as an independent branch of Galois theory. For a deeper acquaintance with the embedding problems and Galois algebras we refer the reader to the excellent monograph [3].

A well known criterion for solvability is obtained by using the Galois group Ω_k of the separable closure k_s over k.

Theorem 3.1 [3, Th. 1.15.1]. *The embedding problem $(K/k, G, A)$ is weakly solvable iff there exists a homomorphism $\delta : \Omega_k \to G$, such that the diagram*



is commutative, where φ is the natural epimorphism. The embedding problem is properly solvable iff among the homomorphisms $\Omega_k \to G$, such that the above diagram is commutative, there exists an epimorphism.

Given that the kernel A of the embedding problem is abelian, another well known criterion holds.

Corollary 3.2 [3, Th. 13.3.2]. *Let A be an abelian group and let c be the 2-coclass of the group extension* (3.1) *in $H^2(F, A)$. Then the embedding problem $(K/k, G, A)$ is weakly solvable iff $\inf_F^{\Omega_k}(c) = 0$, where $\inf_F^{\Omega_k} : H^2(F, A) \to H^2(\Omega_k, A)$ is the inflation map.*

Yakovlev further invented cohomological exact sequences in order to replace the splitting condition $\inf_F^{\Omega_k}(c) = 0$ with two conditions, one of which is equivalent to the famous compatibility condition found by Faddeev and Hasse (see [44, 3]).

We give now one of its forms, when $A = \ker \alpha$ is abelian, and the field K contains all roots of unity of degree equal to the period of A. The kernel A becomes an F-module in natural way: for $f \in F$ and $a \in A$, we set $a^f = \overline{f}^{-1} a \overline{f}$, where $\overline{f}$ is arbitrary pre-image of f in G. For any homomorphism $\chi : A \to K^*$ we denote by F_χ the subgroup of F, containing all $f \in F$ such that $\chi(a^f) = [\chi(a)]^f$, and by G_χ the pre-image of F_χ in G. Next, pick an element $c_\chi \in H^2(F_\chi, A)$, related to the exact sequence

$$1 \to A \to G_\chi \xrightarrow{\alpha} F_\chi \to 1. \tag{3.2}$$

Then, the compatibility condition, which is necessary for the solvability of the embedding problem, states: For every homomorphism $\chi : A \to K^*$, the image of the element c_χ under the map $H^2(F_\chi, A) \to H^2(F_\chi, K^*)$, induced by χ, is equal to 1.

In [49] A. Yakovlev and N. Ziapkov introduced a new type of fields – *universally compatible fields*. Namely, we say that the Galois extension K/k is universally compatible of period q, if the field K contains a primitive root of unity ξ of degree q, and for all subgroups F_0 of F, the homomorphisms $H^2(F_0, \langle\xi\rangle) \to H^2(F_0, K^*)$, induced by the inclusion $\langle\xi\rangle \hookrightarrow K^*$, are zero. Yakovlev and Ziapkov established the following results.

Theorem 3.3 [49]**.** *The extension K/k, containing a primitive root of unity of degree q, is universally compatible of period q if and only if the compatibility condition holds for all embedding problems $(K/k, G, A)$ with abelian kernel A of period q.*

Theorem 3.4 [49]**.** *Let K/k be a Galois extension with Galois group F, such that K contains a primitive root of unity of degree q. Let $\varphi : S \to F$ be an epimorphism, where S is a free group, put $R = \ker \varphi$, and let $G = S/[R, R]R^q$. Then K/k is universally compatible of period q if and only if the compatibility condition is fulfilled for the embedding problem $(K/k, G, A)$, where A is the kernel of the epimorphism $\alpha : G \to F$, induced by φ.*

In this way, according to the latter theorem, it suffices to verify the compatibility condition for only one problem, rather than for all embedding problems with abelian kernel of period q. In [46] Ziapkov shows that the universally compatible extensions can be reduced to p-extensions.

The next step is to consider universally compatible extensions which do not possess a primitive p-th root of unity. The Galois extension K/k, not having a primitive p-th root of unity (p is a prime), we call universally compatible of period p^n, if the field K_1, obtained from K by adjoining a primitive p^n-th root of unity, is universally compatible of period p^n. More generally, if K/k does not possess primitive roots of unity of degree $p_1, p_2, \ldots, p_m$ for distinct primes p_i, then we call it universally compatible of period $p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}$ if it is universally compatible for all periods $p_1, p_2, \ldots, p_m$. The following results from [49] yield the solution of the Inverse Problem over algebraic number fields for all groups of odd order. (Another proof of this theorem can be found in the paper by Neukirch [33].)

Theorem 3.5. *Let $p_1, p_2, \ldots, p_m$ be different odd primes, and set $q = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}$. Further, let K be an extension of $\mathbb{Q}$ of odd degree, and let K/k be universally compatible of period q. Then for all embedding problems $(K/k, G, A)$ with kernel A (not necessarily*

abelian) of period dividing q, there exists a proper solution.

Theorem 3.6. *For every odd $q = p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}$ there exists a universally compatible Galois extension of period q over $\mathbb{Q}$.*

Corollary 3.7. *For every group G of odd order, and for every algebraic number field K, there exists a Galois extension L/K with Galois group G.*

In [49] a special type of universally compatible extensions is also defined: The Galois extension K/k is called *universally embeddable* of period q, if all embedding problems $(K/k, G, A)$ with abelian kernel of period q are solvable.

Now, let K/k be a finite Galois extension of local fields, and let K contain a primitive root of unity of degree q. According to [3], the compatibility condition for local fields is also a sufficient condition for solvability of an embedding problem with abelian kernel. Therefore, if K/k is universally compatible then it is also universally embeddable. It follows from Kochendörffer reduction theorems that when the kernel is abelian, we can reduce arbitrary embedding problem to a p-group embedding problem. Ziapkov investigated this problem in [45]:

Theorem 3.8 [45]**.** *Let K/k be a universally embeddable extension of local fields of period $q = p^n$ with Galois group F, and let K contain a primitive root of unity of degree q. Let also $\alpha_1 : F_1 \to F$ be an epimorphism of finite p-groups with kernel an elementary abelian p-group, where F_1 and F have the same number of generators. Then there exists a universally embeddable extension of period q, which is a solution of the embedding problem $(K/k, F_1, \ker \alpha_1)$.*

In [47, 48], Ziapkov gives more necessary and sufficient conditions about the universally embeddable extensions.

When dealing with embedding problems, it is often useful to simplify the matters by constructing equivalent or attendant (called also associate) embedding problems, which are related to 'smaller' group extensions (i.e., the groups have smaller orders). The papers [28, 30] contain such results.

Since the compatibility condition is not always sufficient, Yakovlev [44, 3] proposed an additional condition (as we mentioned above), so that the compatibility condition to be satisfied. This purely homological approach was extended by us in [29], where we found the connection between the obstructions (the elements attached to the two conditions) of the original embedding problem and the associated embedding problems of the first and second kind. The obstructions are interpreted as elements of the groups H^1, H^2, Ext^1 and Ext^2. This brought a number of new results and new proofs of well-known facts, e.g. the second Kochendörffer reduction theorem, which states that every embedding problem can be reduced to an equivalent embedding problem for p-groups.

The realisability of p-groups as Galois groups is a quite common topic in many recent papers, especially for $p = 2$. Apart from the almost folklore results regarding small 2-groups (e.g., the cyclic group C_4 of order 4, the dihedral and quaternion groups of order 8), the first significant advance about the realisability of 2-groups as Galois groups was made in the nineties of the 20th century in the works of Kiming and Ledet [5, 8]. Kiming used explicit cohomology to obtain necessary and sufficient conditions for realisability of some groups of order 16, and also described the Galois extensions that realised them. His method, however, utilizes a huge amount of explicit cohomological calculations and

leads to very complicated conditions. Ledet was the first to make a complete study of the realisability of all groups of order 16 by applying more refined cohomology and the theory of quaternion algebras as well. He obtained quite clear and easy to apply obstructions in terms of quaternion algebras, which made possible to develop the theory of 2-groups as Galois groups into much bigger depths. This was the main topic of Michailov's dissertation [18]. Most of Michailov's results concerning groups of order 16 over arbitrary, rational and local fields are published in the papers [31, 20, 21]. The embedding of biquadratic extensions of the type $\mathbb{Q}(p,q)$ for arbitrary primes p and q into fields that realise groups of order 16 was the main topic of [20], where the quaternion algebras are transformed into diophantine equations, and which in turn are solved by the means of congruences and quadratic residues. Michailov also used in [21] the description of the relative Brauer groups over local fields to calculate the quaternion algebras, participating in the obstructions.

The explicit description of all Galois extensions that realise small 2-groups by the means of quadratic forms is another important contribution of Ledet in [10, 11, 12]. His method, however, is working only if the obstruction is equivalent to a product of two quaternion algebras, and it is impossible to apply it to the quaternion group of order 16, whose obstruction is a product of three quaternion algebras. Michailov succeeded in extending Ledet's results to be applicable for the mentioned group in [22], unfortunately not in the general case, but with some extra conditions on the field properties.

Ledet also suggested in [9] a way of computing the obstructions to embedding problems with kernel 4 which are applied to the quaternion, dihedral and quasidihedral (known also as semidihedral) groups of order 32. His results were generalized by Michailov in [19, 25] and applied to the quaternion (Q_{2^n}), dihedral (D_{2^n}), semidihedral (SD_{2^n}) and modular (M_{2^n}) groups of order 2^n for arbitrary $n \geq 4$. Although Ledet's proof of the main theorem in [9] can not be generalized, Michailov applied other cohomological methods to make such a generalization for an arbitrary cyclic kernel. We shall describe now the main points of this generalization.

Assume again that we have an embedding problem $(K/k, G, A)$ with an abelian kernel A, and define the homomorphisms e and f from $F = \mathrm{Gal}(K/k)$ in $\{+1, -1\}$ by: ${}^{\sigma}a = \bar{\sigma}^{-1}a\bar{\sigma} = a^{e_\sigma}$ and $\sigma i = i^{f_\sigma}$ for $\sigma \in F, a \in A$ and $i = \sqrt{-1} \in K$. In [19, 25] the following results are proved.

Theorem 3.9. *Let K/k be a finite Galois extension with Galois group F, and let $\zeta \in K$ be a primitive 2^nth root of unity $(n > 1)$. Consider the group extension*

$$1 \to C_{2^n} \to G \underset{\pi}{\to} F \to 1,$$

such that $e_\sigma, f_\sigma \in \{+1, -1\}$ for all $\sigma \in F$. Let k_1 be the fixed field of $N = \mathrm{Ker}g$. Then the embedding problem $(K/k, G, C_{2^n})$ is solvable, if and only if the embedding problems $(K/k_1, \pi^{-1}(N), \mu_{2^n})$ and $(K/k, G/C_{2^{n-1}}, \mu_2)$ are solvable.

Corollary 3.10. *Let K/k be a finite Galois extension with Galois group F, and let ζ be a primitive 2^nth root of unity $(n > 1)$, such that $\zeta + \zeta^{-1} \in k, i(\zeta - \zeta^{-1}) \in k$ and $i \notin K$. Let*

$$1 \to C_{2^n} \to G \underset{\pi}{\to} F \to 1$$

be a group extension. Extend the elements $\sigma \in F$ to $K(i)$ by $\sigma i = i$, and let κ be the generator of $\mathrm{Gal}(K(i)/K)$. Let $k(\sqrt{b})$ be the fixed field of $N = \mathrm{Ker}g$ and $k_1 = k(i\sqrt{b})$.

Then $\mathrm{Gal}(K(i)/k_1) \cong F$*, and the embedding problem* $(K/k, G, C_{2^n})$ *is solvable, if and only if the embedding problems* $(K(i)/k_1, G, \mu_{2^n})$ *and* $(K/k, G/C_{2^{n-1}}, \mu_2)$ *are solvable.*

With the aid of the latter two results, Michailov managed to calculate the obstructions of embedding problems, which are not Brauer. The obstruction of the Brauer problem, however, requires a 'brute force' calculations in the related crossed product algebras. We give now the description of the obstructions of the Brauer problems related to the quaternion, dihedral and semidihedral 2-groups.

Let K/k be a D_8 extension, let $\zeta \in K$ be a primitive 2^n-th root of unity, such that $\zeta \notin k, \zeta + \zeta^{-1} \in k$ and $i(\zeta - \zeta^{-1}) \in k$. Then $K/k = k(\sqrt[4]{a}, i)$ for some $a \in k \setminus k^2$, and D_8 is generated by elements σ and τ, given by:

$$\sigma : \sqrt[4]{a} \mapsto i\sqrt[4]{a}, i \mapsto i;\ \tau : \sqrt[4]{a} \mapsto \sqrt[4]{a}, i \mapsto -i.$$

Assume that G is a group generated by elements s and t, such that s is of order $2^{n+2}, t^2 = \varepsilon_1$ and $ts = \varepsilon_2 s^{-1}t$, where $\varepsilon_1^2 = \varepsilon_2^2 = 1$. Since $ts^4 = s^{-4}t$, we can put $s^4 = \zeta$, and get the group extension

$$1 \to \mu_{2^n} \underset{\zeta \mapsto s^4}{\to} G \underset{\substack{s \mapsto \sigma \\ t \mapsto \tau}}{\to} D_8 \to 1, \tag{3.3}$$

where we identify the cyclic group $\langle s^4 \rangle$ with the group of 2^n-th roots of unity μ_{2^n}. Therefore we have $s^4 = \zeta, t^2 = \varepsilon_1$ and $ts = \varepsilon_2 \zeta^{-1} s^3 t$, where $\varepsilon_1, \varepsilon_2 \in \{+1, -1\}$. The group G has an element of order 2^{n+2}, hence G is isomorphic either to the dihedral, semidihedral or quaternion group of order 2^{n+3}.

Theorem 3.11 [19, Th. 3.2]**.** *For the solvability of the embedding problem* $(K/k, G, \mu_{2^n})$ *for* $n \geq 1$*, it is necessary that there exists* $\alpha_1 \in k^*$ *and* $\beta_1 \in k$*, such that* $\alpha_1^2 + a\beta_1^2 = 2 - \zeta - \zeta^{-1}$*. In that case the obstruction to the embedding problem* $(K/k, G, \mu_{2^n})$ *is*

$$(-1, \varepsilon_1)(2 + \zeta + \zeta^{-1}, \alpha_1\beta_1)\left(a, \varepsilon_2\alpha_1\left(2\alpha_1 - \frac{\zeta - \zeta^{-1}}{i}\right)\right) \in \mathrm{Br}(k).$$

In [24] Michailov studied the groups of order 32 as Galois groups over arbitrary fields of characteristic $\neq 2$. With the aid of the computer algebra GAP 3+, Michailov calculated the obstructions to the solvability of embedding problems with kernels 2 or 4, related to those groups of order 32, for which previously nothing or little was known from Galois theory perspective. In some cases there is given a description of the Galois extensions that realise the groups under consideration, and also some new automatic realisability results, i.e., when from the realisability of a given group follows the realisability of another group.

As for the p-groups for p-odd, the matter is more complicated, because of the much heavier calculations in the crossed product algebras. On the other hand, the p-cyclic algebras are a very good replacement of the quaternion algebras, so there is a hope that one can calculate the obstructions as products of p-cyclic classes in the Brauer group. This approach was used by Michailov in [23], and can be briefly described as follows:

Let p be a prime. Assume that F is arbitrary field of characteristic not equal to$p$, containing the full group of p-th roots of unity $\mu_p = \langle \zeta \rangle$, where ζ is a fixed primitive p-th root of unity. When $p = 2$, the 2-nd root of unity -1 is, of course, always in F. Next, consider a central embedding problem with cyclic kernel C_p of order p. Since the kernel lies in the centre of the given group G, we can identify C_p with μ_p. In this way, we can link the solvability of the embedding problem to an element in $\mathrm{Br}_p(F)$ – the p-torsion

of the Brauer group, called *the obstruction*, which is the crossed product algebra related to the embedding problem with kernel μ_p. Then the embedding problem is solvable if and only if the obstruction is split in $\mathrm{Br}_p(F)$. If $p = 2$, then by Merkurjev theorem [15] it follows that the obstruction, as a class in the Brauer group, is equal to a product of classes of quaternion algebras. Merkurjev theorem, however, does not give explicit formulae. This is one of the key issues in the considerations of small 2-groups. If p is odd, then Merkurjev's proof can not be generalized, but nevertheless the generalization is true, which is the well-known Merkurjev-Suslin theorem, see [16].

According to a special case of this theorem, every class in $\mathrm{Br}_p(F)$ is equal to a product of p-cyclic algebras. We denote the equivalence class of the p-cyclic algebra (called sometimes generalized quaternion algebra) by $(a, b; \zeta)$, which is generated by i_1 and i_2, such that $i_1^p = b, i_2^p = a$ and $i_1 i_2 = \zeta i_2 i_1$. For $p = 2$ we have the quaternion class $(a, b; -1)$, commonly denoted by (a, b). The following Theorem gives us a formula for the obstruction of an embedding problem related to a group extension of a group having a direct factor the cyclic group of order p. In spite of the differences between the properties of the p-cyclic algebras for p–odd and for $p = 2$, we are able to unite both of the variants:

Theorem 3.12 [23, Th. 2.1], [25, Th. 4.1]**.** *Let $\mathcal{H}$ be a p-group and let*

$$1 \to \mu_p \cong \langle \zeta \rangle \to \mathcal{G} \underset{\pi}{\to} \mathcal{H} \times C_p \to 1 \tag{3.4}$$

be a non-split central group extension with characteristic 2-coclass $\gamma \in H^2(\mathcal{H} \times C_p, \mu_p)$. Let $\sigma_1, \sigma_2, \ldots, \sigma_m$ be a minimal generating set for the maximal elementary abelian factor group of $\mathcal{H}$; and let τ be the generator of the direct factor C_p. Finally, let $s_1, s_2, \ldots, s_m, t \in \mathcal{G}$ be the pre-images of $\sigma_1, \sigma_2, \ldots, \sigma_m, \tau$, such that $t^p = \zeta^j$ and $ts_i = \zeta^{d_i} s_i t$, where $i \in \{1, 2, \ldots, m\}; j, d_i \in \{0, 1, \ldots, p-1\}$.

Let K/F be a Galois extension with Galois group $\mathcal{H}$ and let $L/F = K(\sqrt[p]{b})/F$ be a Galois extension with Galois group $\mathcal{H} \times C_p$ ($b \in F^\times \setminus F^{\times p}$). Choose $a_1, a_2, \ldots, a_m \in F^\times$ such that $\sigma_k \sqrt[p]{a_i} = \zeta^{\delta_{ik}} \sqrt[p]{a_i}$ (δ_{ik} is the Kronecker delta). Then the obstruction to the embedding problem given by L/F and the group extension (3.4) *is*

$$[K, \mathcal{H}, \mathrm{res}_{\mathcal{H}} \gamma](b, \zeta^j \prod_{i=1}^{m} a_i^{d_i}; \zeta).$$

With the aid of the latter criterion, Michailov calculated in [23] the obstructions for embedding problems related to four non-abelian groups of order p^4 and the two non-abelian groups of order p^3. This enabled him to describe the Galois extensions that realise these groups, and to find automatic realisations between them. Finally, the circle of p-groups, whose obstructions can be calculated will be significantly broadened in Michailov's future publications [26, 27] by the means of the transfer (corestriction) map, Kummer theory, and some other 'ad-hoc' cohomological criteria.

REFERENCES

[1] J. Brinkhuis. Normal integral bases and embedding problems, *Math. Ann.*, **264** (1983), 537–543.

[2] D. Harbater. Fundamental groups and embedding problems in characteristic p. Recent Developments in the Inverse Galois Problem (Seattle, WA, 1993), Contemp. Math. vol. **186** (1995), 353–369.

[3] V. V. Ishanov, B. B. Lur'e, D. K. Faddeev. The embedding problem in Galois theory. Amer. Math. Soc., Providence, 1997.
[4] C. Jensen, A. Ledet, N. Yui. Generic polynomials: constructive aspects of the inverse Galois problem. Cambridge University Press, 2002.
[5] I. Kiming. Explicit classifications of some 2-extensions of a field of characteristic different from 2. *Canad. J. Math.* **42** (1990), 825–855.
[6] J. Klüners, G. Malle. Explicit Galois Realization of Transitive Groups of Degree up to 15. *J. Symbolic Computation*, **30** (2000), 675–716.
[7] J. Klüners, G. Malle. A database for field extensions of the rationals. *LMS J. Comput. Math.*, **4** (2001), 182-–196.
[8] A. Ledet. On 2-groups as Galois groups. *Canad. J. Math.*, **47** (1995), 1253–1273.
[9] A. Ledet. Embedding problems with cyclic kernel of order 4. *Israel J. Math.*, **106** (1998), 109–131.
[10] A. Ledet. Generic polynomials for quasi-dihedral, dihedral and modular extensions of order 16, *Proc. AMS* **128** (2000), 2213–2222.
[11] A. Ledet. Generic polynomials for $Q_8-, QC-$, and $QQ-$ extensions. *J. Algebra*, **237** (2001), 1–13.
[12] A. Ledet. Embedding problems and equivalence of quadratic forms. *Math. Scand.*, **88** (2001), 279–302.
[13] G. Malle, B. H. Matzat. Realisierung von Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$m *Math. Ann.*, **272** (1985), 549–565.
[14] G. Malle, B. H. Matzat. Inverse Galois Theorym Springer Monographs in Mathematics, Springer-Verlag, 1999.
[15] A. S. Merkurjev. On the norm residue symbol of degree 2. *Dokl. Akad. Nauk SSSR*, **261** (1981), 542–547; English transl. *Soviet Math. Dokl.* **24** (1981).
[16] A. S. Merkurjev, A. A. Suslin. K-Cohomology of Severi-Brauer Varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR*, Ser. Mat. **46** (1982), 1011–1046; English transl. *Math. USSR Izvestiya* **21** (1983), 307–340.
[17] J.-F. Mestre. Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\widetilde{A}_n$, *J. Algebra* **131** (1990), 483–495.
[18] I. Michailov. 2-groups as Galois groups. Ph.D. Dissertation, Sofia, 2000 (in Bulgarian).
[19] I. Michailov. Embedding obstructions for the dihedral, semidihedral and quaternion 2-groups. *J. Algebra*, **245** (2001), 355–369.
[20] I. Michailov. Some groups of orders 8 and 16 as Galois groups over $\mathbb{Q}$. *Math. Balk. New Series*, **17** (2003), Fasc. 1–2, 155–170.
[21] I. Michailov. Some groups of orders 8 and 16 as Galois groups over the p-adic number field. *Math. Balk. New Series*, **19** (2005), Fasc. 3–4, 367–383.
[22] I. Michailov. Quaternion extensions of order 16. *Serdica Math. J.* **31** (2005), 217-228.
[23] I. Michailov. Four non-abelian groups of order p^4 as Galois groups. *J. Algebra*, **307** (2007), 287–299.
[24] I. Michailov. Groups of order 32 as Galois groups. *Serdica Math. J.*, **33** (2007), 1–34.
[25] I. Michailov. Embedding obstructions for the cyclic and modular 2-groups, *Math. Balk. New Series*, to appear.
[26] I. Michailov. Modular p-extensions and applications to the obstruction theory (in preparation).
[27] I. Michailov. On Galois cohomology and realizability of 2-groups as Galois groups (in preparation).
[28] I. Michailov, N.Ziapkov. Attendant embedding problems. *Compt. Rend. Acad. Bulg. Sci.*, **53** No 7 (2000), 9–12.

[29] I. Michailov, N.Ziapkov. Embedding obstructions for the generalized quaternion group, *J. Algebra* **226** (2000), 375–389.
[30] I. Michailov, N.Ziapkov. On equivalent embedding problems. *Compt. Rend. Acad. Bulg. Sci.*, **53** No 8 (2000), 9–12.
[31] I. Michailov, N.Ziapkov. Embedding problems with Galois groups of order 16. *Math. Balk. New Series*, **15** (2001), Fasc. 1–2, 99–108.
[32] E. Noether. Gleichingen mit vorgeschriebener Gruppe. *Math. Ann.*, **78** (1916), 221–229.
[33] J. Neukirch. On Solvable number fields. *Invest. Math.*, **53** (1979), 135–164.
[34] J. Neukirch, A. Schmidt, K. Wingberg. Cohomology of number fields. Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, 2000.
[35] H. Reichardt. Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung. *J. Reine Angew. Math.*, **177** (1937), 1–5.
[36] I. Shur. Gleichungen ohne Affekt. Sitzungsberichte Akad. Berlin, 1930, 443–449.
[37] A. Scholz. Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I. *Math. Z.*, **42** (1937), 161-188.
[38] J.-P. Serre. L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$. *Comm. Math. Helv.*, **59** (1984), 651–676.
[39] J.-P. Serre. Topics in Galois Theory. Research Notes in Mathematics, Jones & Barlett, 1992.
[40] I. R. Shafarevich. Construction of fields of algevraic numbers with given solvable Galois group. *Izv. Aksd. Nauk SSSR, Ser. Mat.* **18** (1954), 525–578 (in Russian).
[41] K.-Y. Shih. On the construction of Galois extensions of function fields and number fields. Math. Ann. **207** (1974), 99–120.
[42] J. G. Thompson. Some finite groups which appear as $\mathrm{Gal}(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$. *J. Algebra*, **89** (1984), 437–499.
[43] H. Völklein. Groups as Galois Groups, an Introduction. Cambridge Studies in Advanced Mathematics 53, Cambridge University Press, 1996.
[44] A. V. Yakovlev. The embedding problem for fields. *Izv. AN SSSR Ser. Mat.*, **28** No 3 (1964), 645–660 (in Russian).
[45] N. P. Ziapkov. Embedding conditions for universally compatible extensions of local fields. *Math. and Math. Education*, **7** (1978), 339–345 (in Russian).
[46] N. P. Ziapkov. Reduction theorems for universally compatible fields. *Pliska Bulg. Math. Stud.*, **2** (1981), 124–129 (in Russian).
[47] N. P. Ziapkov. Universally embeddable Galois extensions (in Russian). *Pliska Bulg. Math. Stud.*, **2** (1981), 153–156.
[48] N. P. Ziapkov. Embedding of a universally embeddable extension into a universally embeddable extension. *Serdica Math. J.*, **7** (1981), 207–210 (in Russian).
[49] N. P. Ziapkov, A. V. Yakovlev. Universally compatible Galois extensions. *Zap. N. Sem. POMI*, **71** (1977), 133-152 (in Russian).

Ivo M. Michailov, Nikola P. Ziapkov
Faculty of Mathematics and Informatics
Constantin Preslavski University
9712 Shumen, Bulgaria
e-mail: ivo_michailov@yahoo.com, ziapkov2000@yahoo.co.uk

ОБРАТНА ЗАДАЧА НА ТЕОРИЯ НА ГАЛОА

Иво Михайлов, Никола Зяпков

В тази обзорна статия откроваме в исторически план най-важните постижения отнасящи се до Обратната Задача в теорията на Галоа до наши дни. Също така резюмираме приноса на авторите към Задачата за Вложимост в теорията на Галоа, която се явява най-естественият подход към Обратната Задача в случаите на групи, които не са прости.