МАТЕМАТИКА И МАТЕМАТИЧЕСКО ОБРАЗОВАНИЕ, 2023
MATHEMATICS AND EDUCATION IN MATHEMATICS, 2023
Proceedings of the Fifty Second Spring Conference
of the Union of Bulgarian Mathematicians
Borovetz, April 10–14, 2023

CONTEMPORARY GALOIS THEORY AND ITS CLASSICAL PROBLEMS

Ivo M. Michailov

In this survey we outline the milestones of several classical problems in Galois theory: Noether's problem, the inverse problem and the embedding problem. We demonstrate the connection between these problems in the bigger context of the invariant theory of finite groups. We also point out several new results of the author and his collaborators regarding Noether's problem and the embedding problem.

1. Invariant theory of finite groups. Invariant theory of finite groups has intimate connections with Galois theory. One of the first major results was the main theorem on the symmetric functions that described the invariants of the symmetric group S_n acting on the polynomial ring $K[x_1, \ldots, x_n]$ by permutations of the variables. This theorem appears to have been understood, or at least intuited and used, by Newton, as early as 1665. By the turn of the nineteenth century it was regarded as well known. For Galois himself, it was the essential lemma on which his entire theory rested. However, it was not properly proven or even precisely stated until the nineteenth century.

In the following, K will always denote an infinite field. (Usually, in invariant theory it is assumed that $K = \mathbb{C}$, the field of complex numbers.) Let W be a finite dimensional K-vector space. A function $f : W \to K$ is called polynomial or regular if it is given by a polynomial in the coordinates with respect to a basis of W. It is easy to see that this is independent of the choice of a coordinate system of W. We denote by $K[W]$ the K-algebra of polynomial functions on W which is usually called the coordinate ring of W or the ring of regular functions on W. If $w_1, \ldots, w_n$ is a basis of W and $x_1, \ldots, x_n$ the dual basis of the dual vector space W^* of W, i.e., the coordinate functions, we have $K[W] = K[x_1, \ldots, x_n]$. This is a polynomial ring in the x_i because the field K is infinite. Appart from the common operations addition and multiplication in a ring, $K[W]$ is a linear space over K, since we can multiply the polynomials with scalars from K. Moreover, for any $\alpha \in K, f, g \in K[W]$ the condition $\alpha \cdot (f \cdot g) = (\alpha \cdot f) \cdot g = f \cdot (\alpha \cdot g)$ is satisfied. Such rings are called algebras.

As usual, we denote by $\mathrm{GL}(W)$ the general linear group, i.e., the group of K-linear automorphisms of the K-vector space W. Choosing a basis $(w_1, w_2, \ldots, w_n)$ of W we can identify $\mathrm{GL}(W)$ with the group $\mathrm{GL}_n(K)$ of invertible $n \times n$ matrices with entries in K

This work is partially supported by a project No RD-08-32/17.01.2023 of Shumen University.
2020 Mathematics Subject Classification: 12F12, 13A50, 20D15, 14E08.
Key words: Noether's problem, the embedding problem, Galois group, the inverse problem.

in the usual way: The i-th column of the matrix A corresponding to the automorphism $g \in \mathrm{GL}(W)$ is the coordinate vector of $g(w_i)$ with respect to the chosen basis.

Now assume that there is given a subgroup $G \subset \mathrm{GL}(W)$ or, more generally, a group G together with a linear representation on W, i.e., a group homomorphism $\rho : G \to \mathrm{GL}(W)$. The corresponding linear action of G on W will be denoted by $(\sigma, w) \mapsto \sigma w = \rho(\sigma)w$ ($\sigma \in G, w \in W$), and we will call W a G-module.

Definition 1.1. A function $f \in K[W]$ is called *G-invariant* or shortly *invariant* if $f(\sigma w) = f(w)$ for all $\sigma \in G$ and $w \in W$. The invariants form a subalgebra of $K[W]$ called *invariant ring* and denoted by $K[W]^G$.

There is another way to describe the invariant ring. For this we consider the following linear action of G on the coordinate ring $K[W]$:

$$(\sigma, f) \mapsto \sigma f, \quad \sigma f(w) = f(\sigma^{-1}w), \quad \text{for } \sigma \in G, f \in K[W], w \in W.$$

This is usually called the regular representation of G on the coordinate ring. (The inverse σ^{-1} in this definition is necessary in order to get a left-action on the space of functions.) Clearly, a function f is invariant if and only if it is a fixed point under this action, i.e., $\sigma f = f$ for all $\sigma \in G$. This explains the notation $K[W]^G$ for the ring of invariants.

Example 1.1. Let S_n denote the symmetric group on n letters and let us consider the natural representation of S_n on $W = K^n$ given by $\sigma(e_i) = e_{\sigma(i)}$, or, equivalently,

$$\sigma(x_1, x_2, \ldots, x_n) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, \ldots, , x_{\sigma^{-1}(n)}).$$

The symmetric group S_n acts on the polynomial ring $K[x_1, \ldots, x_n]$, and the invariant functions are the symmetric polynomials:

$$K[x_1, \ldots, x_n]^{S_n} = \{f \mid f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n) \text{ for all } \sigma \in S_n\}.$$

It is well known and classical that every symmetric function can be expressed uniquely as a polynomial in the elementary symmetric functions $\sigma_1, \sigma_2, \ldots, \sigma_n$ (Fundamental Theorem on Symmetric Polynomials). The existence part of the latter theorem can be formulated also as follows:

Theorem 1.1. *The elementary symmetric polynomials $\sigma_1, \sigma_2, \ldots, \sigma_n$ generate the algebra of symmetric polynomials:*

$$K[x_1, \ldots, x_n]^{S_n} = K[\sigma_1, \sigma_2, \ldots, \sigma_n].$$

One of the fundamental problems in Classical Invariant Theory is the following:

Open Problem. *Describe generators and relations for the ring of invariants $K[W]^G$.*

This question goes back to the 19th century and a number of well-known mathematicians of that time have made important contributions: Boole, Sylvester, Cayley, Hermite, Clebsch, Gordan, Capelli, Hilbert.

Example 1.2. Let $C_2 = \{id, \sigma\}$, the cyclic group of order 2, act on the n-dimensional K-vector space W by $\sigma(v) = -v$ (char $K \neq 2$). We are going to determine a system of generators for the ring of invariants $K[W]^{C_2}$. Note first that $f \in K[x_1, \ldots, x_n]$ is invariant under C_2 if and only if $f(x_1, \ldots, x_n) = \sigma f = f(-x_1, \ldots, -x_n)$. Hence the invariants are the polynomials that are sums of monomials of even degree. (Recall that the degree d of the monomial $ax_1^{d_1}x_2^{d_2}\cdots x_n^{d_n}$ is defined as $d = d_1 + d_2 + \cdots + d_n$.) In particular, the monomials $x_1^2, \ldots, x_n^2, x_ix_j$ ($i \neq j$) are invariants. It can be shown that any monomial of even degree is a product of these monomials, so $K[x_1, \ldots, x_n]^{C_2} = K[x_1^2, \ldots, x_n^2, x_ix_j : i \neq j]$.

2. Noether's problem. In 1917, Emmy Noether published a seminal paper [19] on the *inverse Galois problem*. Instead of determining the Galois group of transformations of a given field and its extension, Noether asked whether, given a field and a group, it is always possible to find an extension of the field that has the given group as its Galois group. Noether reduced this to *Noether's problem*, which asks whether the fixed field of a subgroup G of the permutation group S_n acting on the function field $K(x_1, \ldots, x_n)$ is always purely transcendental (i.e. rational) extension of the field K. Recall that a field extension L of K is purely transcendental (or rational) over K if $L \simeq K(x_1, \ldots, x_n)$ over K for some integer n, with $x_1, \ldots, x_n$ algebraically independent over K.

Example 2.1. The symmetric group S_n acts on the function field $K(x_1, \ldots, x_n)$, and the invariant functions are the symmetric functions. According to the Fundamental Theorem on Symmetric Polynomials $K(x_1, \ldots, x_n)^{S_n} = K(\sigma_1, \ldots, \sigma_n)$. The elementary symmetric polynomials are algebraically independent over K, so $K(\sigma_1, \ldots, \sigma_n)$ is purely transcendental over K, i.e., Noether's problem has an affirmative answer for S_n over any field K.

On the other hand, it is known that the answer is 'no' for some G's, even for an algebraically closed K. For most G's, as for example the alternating groups A_n with $n > 5$, the problem remains open for every K. A more general version of Noether's problem asks, in Serre's terminology [1, 33.1], whether the following property holds:

Noe(G/K): There exists a faithful, finite-dimensional, linear K-representation $G \subset GL(V)$ such that the extension $K(V)^G/K$ is rational.

Usually, Noether's problem is formulated in this way: Let G be a finite group and G act on the rational function field $K(x(g) : g \in G)$ by K automorphisms defined by $g \cdot x(h) = x(gh)$ for any $g, h \in G$. Denote by $K(G)$ the fixed field $K(x(g) : g \in G)^G$. *Noether's problem* then asks whether $K(G)$ is rational over K.

Noether's problem for abelian groups was studied extensively by Swan, Voskresenskii, Endo, Miyata and Lenstra, etc. The reader is referred to Swan's paper for a survey of this problem [27]. Fischer's Theorem is a starting point of investigating Noether's problem for finite abelian groups in general.

Theorem 2.1. (Fischer [27, Theorem 6.1]) *Let G be a finite abelian group of exponent e. Assume that* (i) *either char $K = 0$ or char $K > 0$ with char $K \nmid e$, and* (ii) *K contains a primitive e-th root of unity. Then $K(G)$ is rational over K.*

Example 2.2. The cyclic group $C_2 = \{1, g\}$ acts on the function field $K(x_1, x_g)$ by $g : x_1 \mapsto x_g \mapsto x_1$. Define $y_1 = x_1 + x_g, y_2 = x_1 - x_g$. We have that $K(x_1, x_g) = K(y_1, y_2)$ and $g : y_1 \mapsto y_1, y_2 \mapsto -y_2$. It is easy to see now that $K(x_1, x_g)^{C_2} = K(y_1, y_2)^{C_2} = K(y_1, y_2^2)$ is rational over K.

The following theorem of Kang generalizes Fischer's theorem for the metacyclic p-groups.

Theorem 2.2. (Kang [4, Theorem 1.5]) *Let G be a metacyclic p-group with exponent p^e, and let K be any field such that* (i) *char $K = p$, or* (ii) *char $K \neq p$ and K contains a primitive p^e-th root of unity. Then $K(G)$ is rational over K.*

Recently, Michailov gave an affirmative answer to Noether's problem for p-groups having an abelian normal subgroup of index p.

Theorem 2.3. (Michailov [14, Theorem 1.8]) *Let G be a group of order p^n for $n \geq 2$ with an abelian subgroup H of order p^{n-1}, and let G be of exponent p^e. Choose any $\alpha \in G$ such that α generates G/H, i.e., $\alpha \notin H, \alpha^p \in H$. Denote $H(p) = \{h \in H : h^p =$*

$1, h \notin H^p\} \cup \{1\}$, *and assume that* $[H(p), \alpha] \subset H(p)$. *Denote by* $G_{(i)} = [G, G_{(i-1)}]$ *the lower central series for* $i \geq 1$ *and* $G_{(0)} = G$. *Let the* p*-th lower central subgroup* $G_{(p)}$ *be trivial. Assume that* (i) *char* $K = p > 0$, *or* (ii) *char* $K \neq p$ *and* K *contains a primitive* p^e*-th root of unity. Then* $K(G)$ *is rational over* K.

The key idea to prove such results is to find a faithful G-subspace W of the regular representation space $\bigoplus_{g \in G} K \cdot x(g)$ and to show that W^G is rational over K. The subspace W is obtained as an induced representation from H. The list of groups which were investigated regarding Noether's problem is very extensive. We are not aware of a survey or a monograph that covers most of the results obtained in this area. Recently, we have proved the following

Theorem 2.4 ([16, Theorem 1.2])**.** *For any prime* p *let* G *be a* p*-group of nilpotency class* 2, *which has the AEC property (i.e. abelian extension of a cyclic group). Denote by* p^e *the exponent of* G. *Assume that* (i) *char* $K = p > 0$, *or* (ii) *char* $K \neq p$ *and* K *contains a primitive* p^e*-th root of unity. Then* $K(G)$ *is rational over* K.

The latter result can be proven also via the obstructions to the related embedding problem, given in the last section. This shows that there is another connection besides the one discovered by Noether (that the positive solution of Noether's problem always implies a positive solution to the inverse problem). Namely, in this case the knowledge of the obstruction to the related embedding problem can give us an answer when Noether's problem has a positive answer.

3. The inverse problem in Galois theory. The *inverse problem of Galois theory* consists of two parts:

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

2. **Actual construction.** If G is realizable 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 whether all finite groups can be realized over $\mathbb{Q}$ is one of the most challenging problems in mathematics, and it is still unsolved. If Noether's Problem $\mathrm{Noe}(G/\mathbb{Q})$ has an affirmative answer, G can be realised as a Galois group over $\mathbb{Q}$, and in fact over any Hilbertian field of characteristic 0.

In the nineteenth century, the following result was established:

Theorem 3.1 (Kronecker-Weber)**.** *Every algebraic number field whose Galois group over* $\mathbb{Q}$ *is abelian, is a subfield of the cyclotomic field* $\mathbb{Q}(\zeta)$, *where* ζ *is an* n*-th root of unity for some natural number* n.

The latter theorem was first stated by Kronecker (1853) though his argument was not complete for extensions of degree a power of 2. Weber (1886) published a proof, but this had some gaps and errors that were pointed out and corrected by Neumann (1981). The first complete proof was given by Hilbert (1896). The proof can be found in most books on class field theory. In the early 20-th century Hilbert's 12-th problem on the generalization of the Kronecker-Weber Theorem gained popularity. The history of the 12-th problem is explained at lenght in [21].

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 3.2. *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 polynomials with the alternating group A_n as a Galois group were given by Schur [23] in 1930.

The next important step was taken in 1937 by A. Scholz and H. Reichard [22, 20] who proved the following existence result:

Theorem 3.3. *For an odd prime p, every finite p-group occurs as a Galois group over $\mathbb{Q}$.*

The final step concerning solvable groups was taken by Shafarevich [25], although with a mistake relative to the prime 2. 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 [18, Chapter IX].

Theorem 3.4 (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 3.5 (Shih [26])**.** *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 3.6 (Malle & Matzat [7])**.** *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. It should be noted that all these realization results of simple groups were achieved via the rigidity method and the Hilbert Irreducibility Theorem. Extensive surveys of recent developments regarding the classical inverse problem and its related problems can be found for example in the monographs [2, 3, 5, 6, 24, 28].

4. The Fundamental Group of the Punctured Riemann Sphere. In this section we are going to describe the structure of the fundamental group of the punctured Riemann sphere. From its algebraic variant, we can easily obtain a solution of the inverse problem of Galois theory over $\mathbb{C}(t)$. After extension of the fundamental group by complex conjugation one can also derive the solution of the inverse Galois problem over $\mathbb{R}(t)$.

We begin with the Riemann sphere $\mathscr{X} := \hat{\mathbb{C}}$. From this, a set of s points $\mathscr{P} := \{\mathscr{P}_1, \ldots, \mathscr{P}_s\}$ is removed. For any choice of base point $\mathscr{P}_0 \in \mathscr{X} \setminus \mathscr{P}$ the topological fundamental group $\pi_1^{\mathrm{top}}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0)$ relative to $\mathscr{P}_0$ is generated by homotopy classes of nonintersecting loops γ_i from $\mathscr{P}_0$ counterclockwise around $\mathscr{P}_i$ (see Fig. 1).

By stereographic projection the punctured Riemann sphere $\mathscr{X} \setminus \mathscr{P}$ is homeoporhic to the real plane from which $s-1$ points are removed: $\mathscr{X} \setminus \mathscr{P} \simeq \mathbb{R}^2 \setminus \mathscr{Q}$, where $\mathscr{Q} := \{\mathscr{Q}_2, \ldots, \mathscr{Q}_s\}$. From Van Kampen's theorem it follows that the topological fundamental group $\pi_1^{\mathrm{top}}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0)$ is the free group with $s-1$ generators. This can be shown either by induction on the number of points, or by the homotopy equivalence between $\mathbb{R}^2 \setminus \mathscr{Q}$ and the bouquet of $s-1$ circles (i.e. the wedge sum of k circles). Now, we can

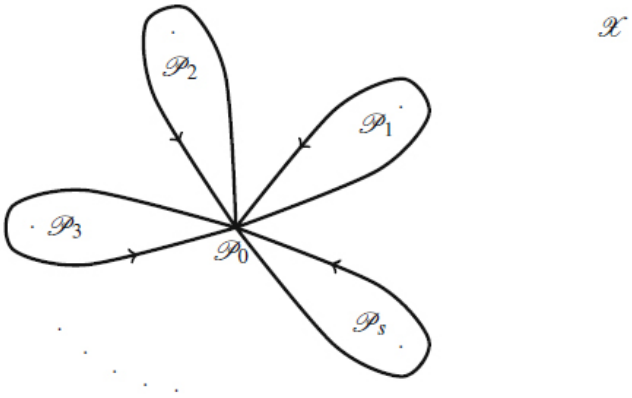

Fig. 1. Generators of $\pi_1^{\mathrm{top}}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0)$

put $\gamma_1 = \left(\prod_{i=2}^{s} \gamma_i\right)^{-1}$ and obtain that the fundamental group $\pi_1^{\mathrm{top}}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0)$ has the following presentation:

$$\pi_1^{\mathrm{top}}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0) = \langle \gamma_1, \gamma_2, \ldots, \gamma_2 | \gamma_1 \gamma_2 \cdots \gamma_s = 1 \rangle.$$

The only continuous automorphism of the field of complex numbers $\mathbb{C}$ is given by complex conjugation, denoted here by ρ. If the set $\mathscr{P}$ introduced previously and the base point $\mathscr{P}_0$ remain stable under ρ, i.e., if $\mathscr{P}^\rho = \mathscr{P}$ and $\mathscr{P}_0^\rho = \mathscr{P}_0$, then ρ acts on $\pi_1^{\mathrm{top}}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0)$. Indeed, assume that $\mathscr{P}$ consists of r pairs of complex conjugate points $\mathscr{P}_1, \ldots, \mathscr{P}_{2r}$ arranged first by decreasing imaginary part and then by decreasing real part (in case of equality of the imaginary parts), and the real points $\mathscr{P}_{2r+1} < \cdots < \mathscr{P}_s$. Choosing the real base point $\mathscr{P}_0 < \mathscr{P}_{2r+1}$ we obtain Fig. 2.

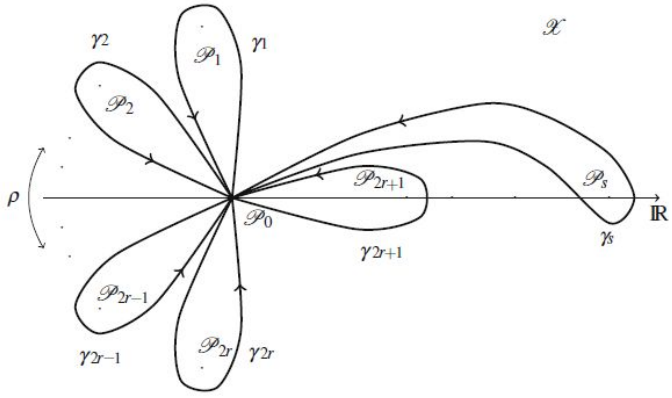

Fig. 2. Action of complex conjugation

With this standard arrangement, the homotopy classes of paths γ_i are sent to γ_{2r+1-i}^{-1} for $i = 1, \ldots, 2r$, and γ_{2r+j} for $j = 1, \ldots, s-2r$ is mapped to

$$\gamma_{2r+1} \cdots \gamma_{2r+j-1} \gamma_{2r+j}^{-1} \gamma_{2r+j-1}^{-1} \cdots \gamma_{2r+1}^{-1}.$$

Therefore ρ acts on the generators of $\pi_1^{\mathrm{top}}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0)$ in this way:

$$(\gamma_1, \ldots, \gamma_s)^\rho = (\gamma_{2r}^{-1}, \ldots, \gamma_1^{-1}, \gamma_{2r+1}^{-1}, \ldots, (\gamma_s^{-1})^{\gamma_{s-1}^{-1} \cdots \gamma_{2r+1}^{-1}}).$$

The topological fundamental group π_1^{top} has an algebraic analogue π_1^{alg}, for which however the convenient visualization as group of homotopy classes of paths is lost. Namely, let $K := \mathbb{C}(\mathscr{X})$ be the function field of $\mathscr{X} = \hat{\mathbb{C}}$, or equivalently of the projective line $\mathbb{P}^1(\mathbb{C})$. Then K is isomorphic to the field of rational functions $\mathbb{C}(t)$ over $\mathbb{C}$. Denote by $\mathbb{P}(K/\mathbb{C})$ the set of prime divisors or equivalently valuation ideals of the function field $K/\mathbb{C}$. Then the set $\mathscr{P} \subset \mathscr{X}$ corresponds to the subset S of primes of $K/\mathbb{C}$ whose valuation ideal has a common zero at one of the points $\mathscr{P}_i$.

Now let $\mathbf{N}_S$ denote the set of all finite Galois extension fields of K, ramified only at prime divisors of S, in a fixed algebraic closure $\tilde{K}$ of K. The union of all $N \in \mathbf{N}_S$ forms the maximal extension field M_S of K (in $\tilde{K}$) unramified outside S. It is again Galois over K, and for $|S| > 1$ finite, the Galois group is obtained as the projective limit of the finite Galois groups $\mathrm{Gal}(N/K)$:

$$\mathrm{Gal}(M_S/K) = \varprojlim (\mathrm{Gal}(N/K))_{N \in \mathbf{N}_S}.$$

This Galois group formally depending on $\hat{K}$ is called the algebraic fundamental group of $\mathscr{X} \setminus \mathscr{P}$:

$$\pi_1^{\mathrm{alg}}(\mathscr{X} \setminus \mathscr{P}) = \pi_1^{\mathrm{alg}}(\mathscr{X} \setminus \mathscr{P}, \hat{K}) := \mathrm{Gal}(M_S/K).$$

For the algebraic fundamental group we get the following profinite version of Riemann's existence theorem:

Theorem 4.1. *The algebraic fundamental group $\pi_1^{alg}(\mathscr{X} \setminus \mathscr{P})$ is isomorphic to the profinite completion of the topological fundamental group $\pi_1^{top}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0)$:*

$$\pi_1^{alg}(\mathscr{X} \setminus \mathscr{P}) \cong \hat{\pi}_1^{top}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0).$$

Moreover for any choice of the base point $\mathscr{P}_0$ there exists a monomorphism

$$\iota : \pi_1^{top}(\mathscr{X} \setminus \mathscr{P}; \mathscr{P}_0) \to \pi_1^{alg}(\mathscr{X} \setminus \mathscr{P}),$$

such that $\pi_1^{alg}(\mathscr{X} \setminus \mathscr{P})$ is generated as topological group by the images of the γ_i (where $\iota(\gamma_i)$ is identified with γ_i):

$$\pi_1^{alg}(\mathscr{X} \setminus \mathscr{P}) = \langle \gamma_1, \ldots, \gamma_s | \gamma_1 \cdots \gamma_s = 1 \rangle\hat{}.$$

Now, let the finite group G be generated by the elements $\sigma_1, \ldots, \sigma_{s-1}, s \geq 2$. Then there exists a continuous epimorphism $\psi : \mathrm{Gal}(M_S/K) \to G$ with $\psi(\gamma_i) = \sigma_i$ for $i = 1, \ldots, s-1$ and $\psi(\gamma_s) = (\sigma_1 \cdots \sigma_{s-1})^{-1}$. The fixed field $N := M_S^{\ker(\psi)}$ now yields a Galois extension of $K = \mathbb{C}(\mathscr{X})$ with $\mathrm{Gal}(N/K) \cong \mathrm{Gal}(M_S/K)/\ker(\psi) \cong G$. This gives a solution of the inverse problem of Galois theory over the field of rational functions $\mathbb{C}(t)$:

Theorem 4.2. *Every finite group occurs as Galois group over $\mathbb{C}(\mathscr{X}) \cong \mathbb{C}(t)$.*

5. The embedding problem in Galois theory. Let k be arbitrary field and let H be a non simple group. Assume that A is a normal subgroup of H. Then the realizability of the quotient group $G = H/A$ as a Galois group over k is a necessary condition for

the realizability of H over k. In this way arises the next generalization of the inverse problem in Galois theory – the embedding problem of fields.

Let K/k be a Galois extension with Galois group G, and let

$$1 \longrightarrow A \longrightarrow H \xrightarrow{\alpha} G \longrightarrow 1, \tag{5.1}$$

be a group extension, i.e., a short exact sequence. Solving *the embedding problem* related to K/k and (5.1) consists of determining whether or not there exists a Galois algebra (called also a *weak* solution) or a Galois extension (called a *proper* solution) L, such that K is contained in L, H is isomorphic to $\mathrm{Gal}(L/k)$, and the homomorphism of restriction to K of the automorphisms from H coincides with α. We denote the so formulated embedding problem by $(K/k, H, A)$. We call the group A the *kernel* of the embedding problem.

A well known criterion for solvability is obtained by using the Galois group Ω_k of the algebraic separable closure $\bar{k}$ over k.

Theorem 5.1 ([2, Theorem 1.15.1])**.** *The embedding problem $(K/k, H, A)$ is weakly solvable if and only if there exists a homomorphism $\delta : \Omega_k \to H$, such that $\alpha \cdot \delta = \varphi$, where $\varphi : \Omega_k \to G$ is the natural epimorphism. The embedding problem is properly solvable if and only if among the homomorphisms δ, there exists an epimorphism.*

Given that the kernel A of the embedding problem is abelian, another well known criterion holds. We can define an G-module structure on A by $a^\rho = \bar{\rho}^{-1} a \bar{\rho}$ ($\bar{\rho}$ is a pre-image of $\rho \in G$ in H).

Corollary 5.2 ([2, Theorem 13.3.2])**.** *Let A be an abelian group and let c be the 2-coclass of the group extension (5.1) in $H^2(G, A)$. Then the embedding problem $(K/k, H, A)$ is weakly solvable if and only if $\inf\limits_{G}^{\Omega_k}(c) = 0$*

Next, let K contain a primitive root of unity of order equal to the order of the kernel A. Then we can define the character group $\hat{A} = \mathrm{Hom}\,(A, K^*)$ and make it an G-module by ${}^\rho\chi(a) = \chi(a^\rho)^{\rho^{-1}}$, for $\chi \in \hat{A}$, $a \in A$, $\rho \in G$.

Let $\mathbb{Z}[\hat{A}]$ be the free abelian group with generators e_χ (for $\chi \in \hat{A}$). We make it an G-module by ${}^\rho e_\chi = e_{{}^\rho\chi}$. Then there exists an exact sequence of G-modules

$$0 \longrightarrow V \longrightarrow \mathbb{Z}[\hat{A}] \xrightarrow{\pi} \hat{A} \longrightarrow 0, \tag{5.2}$$

where π is defined by $\pi(\sum\limits_i k_i e_{\chi_i}) = \prod\limits_i \chi_i^{k_i}$ where $k_i \in \mathbb{Z}$.

We can clearly consider all G-modules as Ω_k-modules. The exact sequence (5.2) then implies the exact sequence

$$0 \longrightarrow A \simeq \mathrm{Hom}(\hat{A}, \bar{k}^\times) \longrightarrow \mathrm{Hom}(\mathbb{Z}[\hat{A}], \bar{k}^\times) \longrightarrow \mathrm{Hom}(V, \bar{k}^\times) \longrightarrow 0.$$

Since $H^1(\Omega_k, \mathrm{Hom}(\mathbb{Z}[\hat{A}], \bar{k}^\times)) = 0$ (see [2, §3.13.3]), we obtain the following exact sequence

$$0 \longrightarrow H^1(\Omega_k, \mathrm{Hom}(V, \bar{k}^\times)) \xrightarrow{\beta} H^2(\Omega_k, A) \xrightarrow{\gamma} H^2(\Omega_k, \mathrm{Hom}(\mathbb{Z}[\hat{A}], \bar{k}^\times)).$$

We call the element $\eta = \gamma\bar{c}$ *the (first) obstruction.* The condition $\eta = 0$ is clearly necessary for the solvability of the embedding problem $(K/k, H, A)$. This is the well-known *compatibility* condition found by Faddeev and Hasse. In general it is not a sufficient condition for solvability. Indeed if we assume that $\eta = 0$, then there appears a second obstruction, namely $\xi \in H^1(\Omega_k, \mathrm{Hom}(V, \bar{k}^\times))$ such that $\beta(\xi) = \bar{c}$. Thus, in order to

obtain a necessary and sufficient condition we must have both $\eta = 0$ and $\xi = 0$. The second obstruction is very hard to calculate explicitly, though. That is why embedding problems for which $H^1(\Omega_k, \mathrm{Hom}(V, \bar{k}^\times)) = 0$ are of special interest. This condition turns out to be fulfilled in a number of cases.

Let us begin with the so called *Brauer problem*. The embedding problem $(K/k, H, A)$ is called *Brauer* if $\hat{A}$ is a trivial G-module. Then we have the well known

Theorem 5.3 ([2, Theorem 3.1])**.** *The compatibility condition for the Brauer problem $(K/k, H, A)$ is necessary and sufficient for its weak solvability.*

Let $q \geq 2$ be a natural number, let k be arbitrary field of characteristic relatively prime to q, containing a primitive qth root of unity ζ, and put $\mu_q = \langle\zeta\rangle$. Let K be a Galois extension of k with Galois group G. Consider the group extension

$$1 \longrightarrow \langle\varepsilon\rangle \longrightarrow H \longrightarrow G \longrightarrow 1, \tag{5.3}$$

where ε is a central element of order q in H. We are going to identify the groups $\langle\varepsilon\rangle$ and μ_q, since they are isomorphic as G-modules.

Assume that $c \in H^2(G, \mu_q)$ is the 2-coclass corresponding to the group extension (5.3). *The obstruction* to the embedding problem $(K/k, H, \mu_q)$ we call the image of c under the inflation map $\inf\limits_{G}^{\Omega_k} : H^2(G, \mu_q) \to H^2(\Omega_k, \mu_q)$.

Note we have the standard isomorphism of $H^2(\Omega_k, \mu_q)$ with the q-torsion in the Brauer group of k induced by applying $H^*(\Omega_k, \cdot)$ to the q-th power exact sequence of Ω_k-modules $1 \longrightarrow \mu_q \longrightarrow \bar{k}^\times \longrightarrow \bar{k}^\times \longrightarrow 1$. In this way, the obstruction equals the equivalence class of the crossed product algebra $(G, K/k, \bar{c})$ for any $\bar{c} \in c$. Hence we may identify the obstruction with a Brauer class in $\mathrm{Br}_q(k)$.

Note that we have an injection $\mu_q \hookrightarrow K^\times$, which induces a homomorphism $\nu : H^2(G, \mu_q) \to H^2(G, K^\times)$. Then the obstruction is equal to $\nu(c)$, since there is an isomorphism between the relative Brauer group $\mathrm{Br}(K/k)$ and the group $H^2(G, K^\times)$.

Clearly, the problem $(K/k, H, \mu_q)$ is Brauer, so from the proof of Theorem 5.3 given in the paper [15] it follows that $H^1(\Omega_k, \mathrm{Hom}(V, \bar{k}^\times)) = 0$. Hence the homomorphism $\gamma : H^2(\Omega_k, A) \to H^2(\Omega_k, \mathrm{Hom}(\mathbb{Z}[\hat{A}], \bar{k}^\times))$ is an injection. Therefore, the problem is solvable if and only if the (first) obstruction is split.

More generally, the following result holds.

Theorem 5.4. *Let c be the 2-coclass in $H^2(G, \mu_q)$, corresponding to the group extension (5.3). Then the embedding problem $(K/k, H, \mu_q)$ is weakly solvable if and only if $\nu(c) = 1$. If μ_q is contained in the Frattini subgroup $\Phi(H)$ of H, then the condition $\nu(c) = 1$ is sufficient also for the proper solvability of the problem $(K/k, H, \mu_q)$ (see [2, §1.6, Cor. 5]).*

Remark. The related terms *weak solvability* and *Galois algebras* were introduced in order to avoid the trouble of describing some very rare exceptions. For example the embedding problem related to the split exact sequence $1 \to C_2 \to C_2 \times C_2 \to C_2 \to 1$ is 'almost' always solvable in term of fields. We need just to suppose that $|k^*/k^{*2}| \geq 4$ so that there exist $a, b \in k$ such that $k(\sqrt{a}, \sqrt{b})$ is a $C_2 \times C_2$ extension. However, formally speaking, it is possible that $|k^*/k^{*2}| < 4$ and then obviously we can not define a $C_2 \times C_2$ extension. We can instead define a Galois algebra with Galois group $C_2 \times C_2$ and say that the problem is always weakly solvable.

The main goal is to decompose the obstruction to any μ_q-embedding problem as

a product of classes of cyclic algebras. We denote by $(a, b; \zeta)_{q,k}$ (or just $(a, b)_q$) the equivalence class of the cyclic algebra which is generated by i_1 and i_2, such that $i_1^q = b, i_2^q = a$ and $i_1 i_2 = \zeta i_2 i_1$. For $q = 2$ we have the quaternion class $(a, b; -1)$, commonly denoted by (a, b). For example, from the well-known Merkurjev-Suslin Theorem [9] it follows that the obstruction to any μ_p-embedding problem is equal to a product of classes of cyclic p-algebras (where p is a prime). The explicit computation of these cyclic p-algebras, however, is not a trivial task.

In 1987 Massy [8] obtained a formula for the decomposition of the obstruction in the case when $F = \mathrm{Gal}(K/k)$ is isomorphic to $(C_p)^n$, the elementary abelian p-group.

We proved similar results for p-groups in [10, 11, 12, 13]. Moreover, we were able to find the obstructions for any group of nilpotency class ≤ 2.

Let $q \geq 2$ and $n_1 \leq n_2 \leq \cdots \leq n_t$ be natural numbers. Let L/K be a $G \simeq \prod_{i=1}^{t} C_{n_i}$ extension. Assume that for all i, K contains a primitive n_i-th root of unity ζ_{n_i} and a primitive q-th root of unity ζ. Let $K_i = K(\sqrt[n_i]{a_i})$ be the subextension corresponding to the factor C_{n_i} for $i = 1, \ldots, t$ and some $a_i \in K^\times$. (That is, K_i is the fixed subfield of $\prod_{j \neq i} C_{n_j}$.) Let σ_i be the generator of C_{n_i} for $i = 1, \ldots, t$. We have that $\sigma_j \sqrt[n_i]{a_i} = \zeta_{n_i}^{\delta_{ij}} \sqrt[n_i]{a_i}$ (δ is the Kronecker delta).

Theorem 5.5 ([17, Theorem 2.3])**.** *Let L/K be a $G \simeq \prod_{i=1}^{t} C_{n_i}$ extension as described above. Let*

$$1 \longrightarrow \mu_q \simeq \langle \zeta \rangle \longrightarrow H \longrightarrow G \simeq \prod_{i=1}^{t} C_{n_i} \longrightarrow 1 \tag{5.4}$$

be a central group extension with cohomology class $\gamma \in H^2(G, \mu_q)$. Let $s_1, \ldots, s_t$ be the pre-images of $\sigma_1, \ldots, \sigma_t$, let $d_{ij} \in \{0, \ldots, q-1\}$ be given by $s_i s_j = \zeta^{d_{ji}} s_j s_i$, and let $s_i^{n_i} = \zeta^{m_i}$ for $i = 1, \ldots, t; m_i \in \{0, \ldots, q-1\}$. Then q divides $d_{ij} n_i$ for all $i, j : j \neq i$, and the obstruction to the weak solvability of the embedding problem $(L/K, H, \mu)$ given by γ is

$$\prod_{i=1}^{t} (a_i, \zeta^{m_i})_{n_i} \cdot \prod_{i<j} (a_j, a_i)_{n_j}^{d_{ij} n_i / q}.$$

If $\zeta \in \langle s_1, \ldots, s_t \rangle$ then the obstruction is for the proper solvability.

REFERENCES

[1] S. Garibaldi, A. Merkurjev, J-P. Serre. Cohomological invariants in Galois cohomology. AMS Univ. Lecture Series vol. **28**, Amer. Math. Soc., Providence, 2003.

[2] V. V. Ishanov, B. B. Lur'e, D. K. Faddeev. The embedding problem in Galois theory. Amer. Math. Soc., Providence, 1997.

[3] C. Jensen, A. Ledet, N. Yui. Generic polynomials: constructive aspects of the inverse Galois problem. Cambridge University Press, 2002.

[4] M. Kang. Noether's problem for metacyclic p-groups. *Adv. Math.*, **203** (2005), 554–567.

[5] A. Ledet. Brauer Type Embedding Problems. Fields Institute Monographs **21**, American Mathematical Society, 2005.

[6] G. Malle, B. H. Matzat. Inverse Galois Theory. Springer Monographs in Mathematics, Springer-Verlag, 1999.

[7] G. Malle, B. H. Matzat. Realisierung von Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$, *Math. Ann.*, **272** (1985), 549–565.

[8] R. Massy. Construction de p-extensions galoisiennes d'un corps de caractéristique différente de p. *J. Algebra*, **109** (1987), 508–535.

[9] 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 (in Russian); English translation in *Math. USSR Izvestiya*, **21** (1983), 307–340.

[10] I. Michailov. Four non-abelian groups of order p^4 as Galois groups. *J. Algebra*, **307** (2007), 287–299.

[11] I. Michailov. On Galois cohomology and realizability of 2-groups as Galois groups. *Cent. Eur. J. Math.*, **9**, no. 2 (2011), 403–419.

[12] I. Michailov. On Galois cohomology and realizability of 2-groups as Galois groups II. *Cent. Eur. J. Math.*, **9**, no. 6 (2011), 1333–1343.

[13] I. Michailov. Galois realizability of groups of orders p^5 and p^6. *Cent. Eur. J. Math.*, **11**, no. 5 (2013), 910–923.

[14] I. Michailov. Noether's problem for abelian extensions of cyclic p-groups. *Pacific J. Math*, **270** (1) (2014), 167–189.

[15] I. Michailov, N. Ziapkov. Embedding obstructions for the generalized quaternion group. *J. Algebra* **226** (2000), 375–389.

[16] I. Michailov, I. Dimitrov, I. Ivanov. Noether's problem for abelian extensions of cyclic p-groups of nilpotency class 2, *C. R. Acad. Bulgare Sci.*, **75**, no 3 (2022), 323–330.

[17] I. Michailov, I. Dimitrov, I. Ivanov. On the embedding problem of central cyclic extensions of abelian groups. *Annual of Konstantin Preslavsky University of Shumen* **XXII C** (2021), 13–21.

[18] J. Neukirch, A. Schmidt, K. Wingberg. Cohomology of number fields. Grundlehren der Mathematischen Wissenschaften, **323**, Springer-Verlag, 2000.

[19] E. Noether. Gleichingen mit vorgeschriebener Gruppe. *Math. Ann.*, **78** (1917), 221–229.

[20] H. Reichardt. Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung. *J. Reine Angew. Math.*, **177** (1937), 1–5.

[21] N. Schappacher. On the History of Hilbert's Twelfth Problem. Societe Mathematique de France, 1998.

[22] A. Scholz. Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I. *Math. Z.*, **42** (1937), 161–188.

[23] I. Schur. Gleichungen ohne Affekt, Sitzungsberichte Akad. Berlin (1930), 443–449.

[24] J.-P. Serre. Topics in Galois Theory'. Research Notes in Mathematics, Jones & Barlett, 1992.

[25] I. R. Shafarevich. Construction of fields of algebraic numbers with given solvable Galois group. *Izv. Aksd. Nauk SSSR, Ser. Mat.* **18** (1954), 525–578 (in Russian).

[26] K.-Y. Shih. On the construction of Galois extensions of function fields and number fields. Math. Ann. **207** (1974), 99–120.

[27] R. Swan. Noether's problem in Galois theory. In: "Emmy Noether in Bryn Mawr", edited by B. Srinivasan and J. Sally, Springer-Verlag, Berlin, 1983.

[28] H. Völklein. Groups as Galois Groups, an Introduction. Cambridge Studies in Advanced Mathematics **53**, Cambridge University Press, 1996.

Ivo M. Michailov
Faculty of Mathematics and Informatics
Konstantin Preslavsky University of Shumen
Universitetska str. 115
9700 Shumen, Bulgaria
e-mail: ivo_michailov@yahoo.com

СЪВРЕМЕННА ТЕОРИЯ НА ГАЛОА И НЕЙНИТЕ КЛАСИЧЕСКИ ЗАДАЧИ

Иво М. Михайлов

В това проучване очертаваме крайъгълните камъни на няколко класически проблема в теорията на Галоа: ньотеровата задача, обратната задача и задачата за вложимост. Демонстрираме връзката между тези проблеми в по-широкия контекст на теория на инвариантите на крайните групи. Също така посочваме няколко нови резултата на автора и неговите сътрудници по отношение на ньотеровата задача и задачата за вложимост.

Ключови думи: Ньотеровата задача, задачата за вложимост, група на Галоа, обратната задача