Publicacions Matemàtiques, Vol 36 (1992), 1053–1073.

ON THE INVERSE PROBLEM OF GALOIS THEORY

NÚRIA VILA

Dedicated to Pere Menal

Abstract

The problem of the construction of number fields with Galois group over $\mathbb{Q}$ a given finite groups has made considerable progress in recent years. The aim of this paper is to survey the current state of this problem, giving the most significant methods developed in connection with it.

The inverse problem of Galois theory asks whether given a field K and a finite group G there exists a polynomial with coefficients in K whose Galois group over K is isomorphic to the given group G. Different aspects of this problem can be pointed out : The existence of solutions, the effective construction of polynomials, the existence of solutions with some additional conditions, and so on. In any case, the answers to these problems are very different according to the prefixed field K. For example, over $\mathbb{C}(T)$ the inverse problem of Galois theory always has an affirmative answer, as a consequence of Riemann's existence theorem. In contrast, it is well-known that over the finite fields, only cyclic groups appear as Galois groups, and also, over the p-adic fields only solvable groups occur as Galois groups.

However, the main problem in this context which is classically known as the inverse problem of Galois theory is to realize any finite group as a Galois group over the rational field $\mathbb{Q}$. In recent years there has been considerable progress in this as yet unsolved problem. The aim of this paper is to survey the current state of this problem, giving the most significant methods developed in connection with it. This paper essentially contains a talk given in the "Seminario de Geometria Algebraica", at the Complutense University of Madrid, in November 1990.

Partially supported by grant PB89-0215 from CICYT

1. Hilbert's Irreducibility Theorem: S_n, A_n

The origin of the questions related to the construction of polynomials with prefixed Galois group can be found in Hilbert. In 1892, in the same paper in which he established his irreducibility theorem, he proved that the symmetric group S_n and the alternating group A_n are Galois group over $\mathbb{Q}(T)$ and over every number field [**Hi**].

Hilbert's irreducibility Theorem. *Let K be a number field. Let $F(T_1,\dots,T_r,X) \in K[T_1,\dots,T_r,X]$ be an irreducible polynomial. There exists infinitely many r-tuples $t=(t_1,\dots,t_r)\in \mathbb{Z}^r$ such that the polynomial*

$$F_t(X) := F(t_1,\dots,t_r,X) \in K[X]$$

is irreducible.

Moreover, there exists infinitely many r-tuples $t=(t_1,\dots,t_r)\in\mathbb{Z}^r$ such that the Galois group of $F(T_1,\dots,T_r,X)$ over $K(T_1,\dots,T_r)$ is isomorphic to the Galois group of $F_t(X)$ over K,

$$\mathrm{Gal}_{K(T_1,\dots,T_r)}(F(T_1,\dots,T_r,X)) \cong \mathrm{Gal}_K(F_t(X)).$$

Applying this result to the general equation of degree n,

$$F(T_1,\dots,T_n,X) = X^n + T_1X^{n-1} + \cdots + T_n$$

we obtain that, for infinitely many values of $t=(t_1,\dots,t_n)\in\mathbb{Z}^n$, the Galois group of $F_t(X)$ over any number field K is

$$\mathrm{Gal}_K(F_t(X)) \cong S_n.$$

Therefore, S_n appears as a Galois group over every number field and in particular over $\mathbb{Q}$. Hilbert also constructed polynomials $F(X,T)$ and $G(X,T)$ with rational coefficients which are irreducible over $\overline{\mathbb{Q}}(T)$ and whose Galois groups over $\mathbb{Q}(T)$ are

$$\mathrm{Gal}_{\mathbb{Q}(T)}(F(X,T)) \cong S_n$$
$$\mathrm{Gal}_{\mathbb{Q}(T)}(G(X,T)) \cong A_n,$$

for all values of n. The splitting fields of these polynomials are regular extensions over $\mathbb{Q}(T)$ (i.e. $\mathbb{Q}$ is algebraically closed in these splitting fields), hence S_n and A_n are Galois groups over $K(T)$, where K is any number field. Therefore, by Hilbert's irreducibility theorem, A_n appears as a Galois group over every number field. Moreover, we have infinitely

many rational polynomials with Galois groups over $\mathbb{Q}$, isomorphic to S_n and to A_n.

From Hilbert's irreducibility theorem, we find that a Galois realization of a finite group G over $\mathbb{Q}(T)$ provides, in fact, a parametric solution over $\mathbb{Q}$. Moreover, if the Galois extension over $\mathbb{Q}(T)$ is regular, we get an affirmative answer for the group G over any number field.

On the other hand, from a geometric point of view, an irreducible polynomial $F(X,T) \in \mathbb{Q}[T,X]$ defines an irreducible projective rational curve C which is a Galois covering of the projective line $\mathbf{P}_1$ over $\mathbb{Q}$. The function field of C is the splitting field N over $\mathbb{Q}(T)$ of $F(X,T)$. Therefore, the curve C is absolutely irreducible if and only if N is a regular extension of $\mathbb{Q}(T)$.

Noether's method. Emmy Noether's idea to construct equations with a prescribed Galois group was to extend Hilbert's method to any finite group G. Let us consider a finite group G acting faithfully on a set of m elements, $G \subset S_m$. Let K be a number field and $L = K(T_1, \ldots, T_m)$. The question is whether the invariant field L^G is a purely transcendental extension of K. An affirmative answer to this question for a given G and K would imply, by Hilbert's irreducibility theorem, that G can be realized as a Galois group over K. Noether proved that this was true for every subgroup of S_4. Later an affirmative answer to Noether's question for some cyclic groups was found. Moreover, by Luroth's theorem every subfield $K \subsetneq L \subset K(T)$ is purely transcendental over K, and by Castelnuovo's theorem, this is also true for $K = \mathbb{C}$ and $m = 2$, but for $m \geq 3$ this conclusion becomes false. This leads to the problem of the construction of unirational varieties which are not rational. However Swan [**Sw 69**] shows that for the cyclic group C_{47} Noether's question has a negative answer. Other examples have been obtained, the simplest one is provided by Lenstra [**Le 74**] for C_8. Still, Noether's method has recently been revitalized. Ekedahl [**Ek 90**] has given a new proof of Hilbert's irreducibility theorem in which it is proved that, although the invariant field K^G is not purely transcendental, it may have sufficiently good properties, in terms of weak approximation of smooth rational varieties, for Hilbert's irreducibility theorem to remain valid and, by specializing, to obtain a Galois extension with a Galois group isomorphic to the given group G.

2. Galois embedding problem I: Solvable groups

Let $1 \longrightarrow A \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$ be an exact sequence of finite groups. Suppose that G is a Galois group over a field K, $G \cong \mathrm{Gal}(L/K)$. The question is whether there exists a Galois extension $\widetilde{L}$ of K such that

$\widetilde{G} \cong \mathrm{Gal}(\widetilde{L}/K)$, $\widetilde{L} \supset L \supset K$ and the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathrm{Gal}(\widetilde{L}/L) & \longrightarrow & \mathrm{Gal}(\widetilde{L}/K) & \longrightarrow & \mathrm{Gal}(L/K) & \longrightarrow & 1 \end{array}$$

is commutative.

In other words, let $G_K = \mathrm{Gal}(\overline{K}/K)$ be the absolute Galois group of K, the Galois extension L/K gives an epimorphism $p : G_K \longrightarrow G$. The Galois embedding problem associated with L/K has a solution if there exists an homomorphism $\tilde{p} : G_K \longrightarrow \widetilde{G}$ such that the diagram

$$\begin{array}{ccccccccc} & & & & & & G_K & & \\ & & & & & \swarrow^{\tilde{p}} & \downarrow{\scriptstyle p} & & \\ 1 & \longrightarrow & A & \longrightarrow & \widetilde{G} & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

is commutative. In fact the homomorphism $\tilde{p}$ defines an algebra which is an extension of K. If the kernel A is an abelian group and K a number field then, if the embedding problem has an algebra solution, it also has a field solution (cf. [**Ik 60**]). Therefore, in this case, the two formulations are equivalent.

It is easy to see that every abelian group appears as a Galois group over $\mathbb{Q}$. Let $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$, let p_i be a prime such that $p_i \equiv 1 \pmod{n_i}$, $1 \leq i \leq n$. Let ζ_i be a primitive p_i-th root of unity, let K_i be the cyclic subfield of the cyclotomic field $\mathbb{Q}(\zeta_i)$ of degree n_i over $\mathbb{Q}$. Then $\mathrm{Gal}(K_i/\mathbb{Q}) \cong \mathbb{Z}/n_i\mathbb{Z}$ and the compositum field $K_1 \cdots K_r$ has Galois group over $\mathbb{Q}$ isomorphic to G, since $K_i \cap K_j = \mathbb{Q}$, for $i \neq j$, $1 \leq i, j \leq n$.

Since a solvable group G admits an abelian tower

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{0\},$$

it may seem to be easy to obtain the solvable case from the abelian one. It is "only" necessary to solve one to one the successive embedding problems! This procedure, however, has a lot of difficulties. In 1954, Šafarevič succeeded to prove that:

Theorem. *Every finite solvable group appears as a Galois group over any number field.*

The proof of this significant result is contained in four interrelated papers [**Ša 54a**], [**Ša 54b**], [**Ša 54c**] and [**Ša 54d**]. The arithmetic

properties of $\mathbb{Q}$ plays an essential roll in Šafarevič's arguments. It should be emphasized that it is not still known if every solvable group appears as a Galois group over $\mathbb{Q}(T)$. The starting point in Šafarevič's research was the works of Scholz [**Sc 37**], and Reichardt [**Re 37**] who, independently, proved

Theorem. *Every ℓ-group appears as Galois group over $\mathbb{Q}$, where ℓ is an odd prime.*

In order to obtain their results, Scholz and Reichardt solve successive Galois embedding problems controlling the ramification of the extension field at each step, for ℓ-groups. Šafarevič reconsiders this result and gives a new proof covering the case $\ell = 2$. He defines the concept of Scholz's extension and introduces arithmetic invariants whose cancelation assures the existence of a solution to the corresponding embedding problem. On the other hand, by Ore's result (cf. [**Su 82**]), it is known that every solvable group G is isomorphic to a quotient of a semidirect product of a solvable group R by a nilpotent group N, with $|R| < |G|$. Let us formulate the following result of Išhanov [**Iš 76**],

Theorem. *Let L/K be a Galois extension of number fields with Galois group G. Let N be a nilpotent group on which G acts. Consider the semidirect product $\widetilde{G} = N : G$. Then, the embedding problem associated to L/K and $\widetilde{G}$ has a solution.*

If this theorem is true, a proof of Šafarevič's theorem can be obtained, by induction on the order of the solvable group G, and using the two above results. It seems that there is a mistake in the proof of Išhanov's theorem, as well as, in the original proof of Šafarevič, concerning the even case; it will be corrected in a forthcoming book [**Iš-Lu-Fa ?**]. However, for the odd case an alternative proof using cohomological techniques has been given by Neukirch [**Ne 79**].

A possible way to realize the non-solvable groups as Galois groups over $\mathbb{Q}$ is, using the classification of finite groups, to realize all the simple groups and to solve all the associated embedding problems. Nevertheless, some families of non-solvable groups appear as Galois group over $\mathbb{Q}$, using arithmetic-geometric methods.

3. Arithmetic-Geometric methods: $\mathrm{GL}_2(p)$, $\mathrm{PGL}_2(p)$, $\mathrm{PSL}_2(p)$

Let E/K be an elliptic curve defined over a field K and $N \geq 1$ an integer. The kernel $E[N]$ of the multiplication by N defines a Galois

extension $K(E[N])/K$ whose Galois group is

$$\mathrm{Gal}(K(E[N])/K) \subset \mathrm{Aut}(E[N]) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Let E_T be a generic elliptic curve over $K = \mathbb{Q}(T)$, for example

$$E_T : y^2 = 4x^3 - Tx - T.$$

It is a classical result (cf. [**We 09**]) that the Galois group of the field F_N generated by the N-division points of E_T over $\mathbb{Q}(T)$ is isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Notice that this is a non regular extension of $\mathbb{Q}(T)$, since the cyclotomic field $\mathbb{Q}(\zeta_N)$ lies in F_N. Nevertheless, we find that $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ appears as a Galois group over $\mathbb{Q}(T)$ and then, by Hilbert's irreducibility theorem, over $\mathbb{Q}$. A related classical result (cf. [**Fr 22**]) is that M_N the field of modular functions with Fourier coefficients in $\mathbb{Q}(\zeta_N)$ is a Galois extension of $\mathbb{Q}(j)$ with Galois group isomorphic to $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. That is, the modular curve $X(N)$ is a Galois covering of $X(1)$ defined over $\mathbb{Q}(\zeta_N)$ whose Galois group is $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. Let

$$G_0 := \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}_{a \in (\mathbb{Z}/N\mathbb{Z})^*} \right\} / \{\pm 1\},$$

it can be proved that the fixed field $M_N^{G_0}$ is the splitting field of the modular polynomial. Hence the Galois group of the modular polynomial over $\mathbb{Q}(j)$ is isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. Therefore, the groups $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ and $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$ are Galois groups over $\mathbb{Q}(T)$.

On the other hand, if $N = p^r$, and p an odd prime, the Galois group of M_{p^r} over $\mathbb{Q}(j, \zeta_{p^r})$ is isomorphic to $\mathrm{PSL}_2(\mathbb{Z}/p^r\mathbb{Z})$. Shih [**Shi 74**], studying coverings associated with some twisted modular curves, found that in fact $\mathrm{PSL}_2(\mathbb{Z}/p^r\mathbb{Z})$ occurs as a Galois group over $\mathbb{Q}(T)$, if 2,3, or 7 is a quadratic non-residue modulo p.

Ribet [**Ri 75**], using modular forms, obtains that $\mathrm{PSL}_2(\mathbf{F}_{p^2})$ appears as a Galois group over $\mathbb{Q}$, for $p \neq 47$ and such that 144169 is a quadratic non-residue modulo p. Using hyperelliptic curves with real multiplication, Mestre [**Me 88**] proves that $\mathrm{PSL}_2(\mathbb{F}_{p^2})$ is a Galois group over $\mathbb{Q}(T)$, if $p \equiv \pm 2 \pmod 5$.

4. Constructive Galois Theory: Simple groups

In the last few years, considerable progress has been made in the realization of simple groups as Galois group of regular extensions over $\mathbb{Q}(T)$

and, consequently, by Hilbert's irreducibility theorem, over every number field. The constructive Galois theory or the rigidity method validates a classical idea: To use the known fact that every finite group is a Galois group of a polymomial with coefficients in $\mathbb{C}(T)$ and impose conditions in order to ensure that the polynomial can be defined over $\mathbb{Q}(T)$. The first results in this direction can be found in papers of Shih **[Shi 74]**, Fried **[Fr 77]** and Belyi **[Be 79]**. The main force behind this method is Matzat, his rechearch has established and developed this theory. Moreover the work of Thompson has contributed to popularizing and simplifying the method. With the constructive Galois theory, many simple groups have been found to be Galois groups of regular extensions of $\mathbb{Q}(T)$.

$\mathbb{C}(T)$: **Riemann surfaces.** By the Riemann existence theorem for compact surfaces, we know that there is a one-to-one correspondence between the finite extensions of $\mathbb{C}(T)$ and the ramified covering of finite degree of the Riemann sphere $\mathbb{P}_1(\mathbb{C})$. Therefore the problem of classifiying finite extensions of $\mathbb{C}(T)$ is reduced to a topological problem with a well known solution. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ be a finite set of points of $\mathbb{P}_1(\mathbb{C})$, there is a one-to-one correspondence between the finite coverings of $\mathbb{P}_1(\mathbb{C})$ unramified outside of S and the finite unramified coverings of the surface $\mathbb{P}_1(\mathbb{C}) \setminus S$. On the other hand, there is a one-to-one correspondence between the finite unramified covering of $\mathbb{P}_1(\mathbb{C}) \setminus S$ and the subgroups of finite index of its fundamental group $\Pi_1(\mathbb{P}_1(\mathbb{C}) \setminus S)$. This fundamental group has r generators with one relation

$$\Pi_1 = \Pi_1(\mathbb{P}_1(\mathbb{C}) \setminus S) = < u_1, \ldots, u_r; u_1 \cdots u_r = 1 > .$$

Let $\mathbb{C}(T)^S$ be the maximal Galois extension of $\mathbb{C}(T)$ unramified outside S, its Galois group over $\mathbb{C}(T)$

$$G^S = \mathrm{Gal}(\mathbb{C}(T)^S/\mathbb{C}(T)) = \widehat{\Pi}_1$$

is the profinite completetion of Π_1. Then G^S is a profinite group with r generators and one relation, the subgroups generated by each generator and their conjugates are the inertia groups of primes of $\mathbb{C}(T)^S$ over the selected primes $\mathfrak{p}_i$, $i = 1, \ldots, r$.

Let G be any finite group; we can always consider r generators $g_1, \ldots, g_r$ of G with the relation $g_1 \cdots g_r = 1$. Then, we can define an epimorphism

$$\psi : G^S \longrightarrow G,$$

by $\psi(u_i) = g_i$. The fixed field $N = (\mathbb{C}(T)^S)^{\ker \psi}$ has a Galois group over $\mathbb{C}(T)$ isomorphic to G

$$\mathrm{Gal}(N/\mathbb{C}(T)) \cong G.$$

The extension $N/\mathbb{C}(T)$ is unramified outside S, since $N \subset \mathbb{C}(T)^S$. Therefore, every finite group G appears as a Galois group of an extension field of $\mathbb{C}(T)$ which is unramified outside a prefixed set of primes. Indeed by Lefschetz's principle these arguments remain true if one replaces $\mathbb{C}$ by any algebraically closed subfield of $\mathbb{C}$, in particular by $\overline{\mathbb{Q}}$. The difficult problem is to descend to $\mathbb{Q}$! It is necessary to impose conditions, "easy" to compute on the presentation of the group, which enable us to ensure that in fact the extension $N/\overline{\mathbb{Q}}(T)$ is $\mathbb{Q}$-defined, that is, $G_{\mathbb{Q}}$-invariant. In other words, that there exists a regular Galois extension $N_0/\mathbb{Q}(T)$ such that $N_0\overline{\mathbb{Q}} = N$ and

$$\mathrm{Gal}(N_0/\mathbb{Q}(T)) \cong \mathrm{Gal}(N/\overline{\mathbb{Q}}(T)) \cong G.$$

This will be achieved by forcing the "rigidity" on the presentation of the group.

Rationality criteria: Rigidity. Let G be a finite group . Let $C_1, \dots, C_r$, $r \geq 3$, be a r-tuple of conjugacy classes of G. Let us denote

$$\overline{A} = \overline{A}(C_1, \dots, C_r) = \{(g_1, \dots, g_r) \in C_1 \times \cdots \times C_r : g_1 \cdots g_r = 1\}$$
$$A = A(C_1, \dots, C_r) = \{(g_1, \dots, g_r) \in \overline{A} : < g_1, \dots, g_r >= G\},$$

clearly $A \subset \overline{A}$ and G operates by conjugacy on A and on $\overline{A}$. We need the following definitions:

The family $(C_1, \dots, C_r)$ is called *rigid* if A is not empty and G operates transitively on A.

The family $(C_1, \dots, C_r)$ is called *strictly rigid* if it is rigid and $\overline{A} = A$.

A conjugacy class C of G is called *rational* over $\mathbb{Q}$ if any irreducible character of G is rational on C, or equivalently if C contains all powers σ^i of $\sigma \in C$, with i relatively prime to the order of σ.

Suppose that a group G, with trivial center $Z(G) = \{1\}$, has a family $(C_1, \dots, C_r)$ rigid with all the C_i rationals. Let $G =< g_1, \dots, g_r >$, $g_i \in C_i$ and $\psi : G^S \longrightarrow G$, $\psi(u_i) = g_i$. Let $N = (\overline{\mathbb{Q}}(T)^S)^{\ker \psi}$, N is a Galois extension of $\overline{\mathbb{Q}}(T)$ with a Galois group isomorphic to G. The main idea is that rational and rigid conditions on the family $(C_1, \dots, C_r)$ imply that $N/\mathbb{Q}(T)$ is normal and the Galois group $\Gamma = \mathrm{Gal}(N/\mathbb{Q}(T))$ contains a complement for G. That is, there exists a subgroup $H \subset \Gamma$ such that $\Gamma = HG$. Therefore the fixed field $N_0 = N^H$ is a Galois extension of $\mathbb{Q}(T)$ with Galois group G, such that $N_0\overline{\mathbb{Q}} = G$. Now, we can establish the rationality theorem following Belyi [**Be 79**], Matzat [**Ma 84**] and Thompson [**Th 84a**].

Theorem. *Let G be a finite group with trivial center, let $C_1, \dots, C_r$, $r \geq 3$ be r conjugacy classes of G such that each C_i is rational over $\mathbb{Q}$*

and $(C_1, \dots, C_r)$ is rigid. Let $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ be a finite set of primes of $\overline{\mathbb{Q}}(T)$ which are $\mathbb{Q}$-defined. There exists a Galois extension $N/\overline{\mathbb{Q}}(T)$ defined over $\mathbb{Q}$ with Galois group G and unramified outside of S.

Corollary. *Every finite simple group with a rigid family of rational conjugacy classes appears as Galois group of a regular extension of $\mathbb{Q}(T)$.*

Note that the condition on the center of the group G, $Z(G) = \{1\}$, is essential for the rationality criterion for the group G.

However, if the rigid conjugacy classes are not rational, the above results remain true if $\mathbb{Q}(T)$ is replaced by $K(T)$, where K denotes a cyclotomic field containing all the entries in the character table of G corresponding to the classes $C_1, \dots, C_r$.

In order to apply this theorem for a particular group G it is necessary to find a family $(C_1, \dots, C_r)$ of rational conjugacy classes which is rigid. It is easy to see that $(C_1, \dots, C_r)$ is rigid if and only if $|A(C_1, \dots, C_r)| = |G|$; and that $(C_1, \dots, C_r)$ is strictly rigid if and only if $|\overline{A}(C_1, \dots, C_r)| = |G|$. On the other hand the cardinality of $\overline{A} = \overline{A}(C_1, \dots, C_r)$ can be computed if the character table of G is known, so we have

$$|\overline{A}| = \frac{|C_1| \cdots |C_r|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(x_1) \cdots \chi(x_r)}{\chi(1)^{r-2}},$$

where $x_i \in C_i$, $i = 1, \dots, r$, and $\mathrm{Irr}(G)$ denotes the set of the complex irreducible characters of G. The rationality of the conjugacy classes can be also checked from the character table of G.

For further variants and refinements of this result see [**Fr 77**], [**Ma 87**], [**Ma 89**] and [**Ma 91**]. It is of considerable interest the study of the Hurwitz braid group actions which enables Matzat [**Ma 91**] to show that, among others, the Mathieu group M_{24} is a Galois group over $\mathbb{Q}$.

Simple groups which are Galois group over $\mathbb{Q}(T)$, by rigidity. The following theorem sumarizes the results of Dentzer, Feit, Fong, Hoyden-Siedersleben, Hunt, Malle, Matzat, Pahlings, Thompson and Zeh-Marschke, concerning the realization of simple groups as Galois groups over $\mathbb{Q}(T)$, using rationality criteria.

Theorem. *The following simple groups appear as Galois groups of a regular extension of $\mathbb{Q}(T)$, using rigidity methods:*

The alternating group, A_n [**Sh 74**], [**Ma 91**].

All the sporadic simple groups, except the Mathieu group M_{23} [**Th 84a**], [**Hoy 85**], [**Ma-Ze 86**]], [**Hu 86**], [**Pa 88**], [**Pa 89**], [**Ma 89**].

The following classical groups of Lie type:

$\mathrm{PSL}_2(p)$,	$p \not\equiv \pm 1 \pmod{24}$	[**Ma 84**]
$\mathrm{PSL}_2(p^2)$,	$p \equiv \pm 2 \pmod 5$	[**Fe 84**]
$\mathrm{PSL}_3(p)$,	$p \equiv 1 \pmod 4$	[**Th 84b**]
$\mathrm{PSU}_3(p)$,	$p \equiv 3 \pmod 4$, $p > 3$; $p \equiv 3, 5 \pmod 7$, $p > 5$	[**Mal 90**]
$\mathrm{PSp}_4(p)$,	$p \equiv \pm 2 \pmod 5$, $p \geq 3$	[**De 89**]
$\mathrm{PSp}_{\ell-1}(2)$,	2 *a primitive root mod. the prime* ℓ	[**Hä ?**]
$\mathrm{PSO}^+_{\ell+1}(2)$,	2 *a primitive root mod. the prime* ℓ	[**Hä ?**]
$\mathrm{PSO}^-_{\ell-1}(2)$,	2 *a primitive root mod. the prime* $\ell \geq 11$	[**Th 84d**]

The following exceptional groups of Lie type:

$G_2(p)$,	$p \geq 5$	[**Fe-Fo 84**] [**Th 84c**]
$F_4(p)$,	$p \equiv \pm 2, \pm 6 \pmod{13}, p \geq 19$	[**Mal 88**]
$E_6(p)$,	$p \equiv 4, 5, 6, 9, 16, 17 \pmod{19}$	[**Mal ?**]
$E_8(p)$,	$p \equiv \pm 3, \pm 7, \pm 9, \pm 10, \pm 11, \pm 12,$ $\pm 13, \pm 14 \pmod{31}, p \geq 131$	[**Mal 88**].

Many more finite simple groups are known to be Galois groups over $\mathbb{Q}^{ab}(T)$, where $\mathbb{Q}^{ab}$ is the maximal abelian extension of $\mathbb{Q}$: All classical simple groups, all sporadic simple groups and most of the exceptional finite simple groups of Lie type also (cf. [**Be 74**], [**Ma 87**], [**Mal 89**]).

Explicit polynomials. Let $L/\mathbb{Q}(T)$ be a finite separable extension of degree n. Let $N/\mathbb{Q}(T)$ be a normal closure of L over $\mathbb{Q}(T)$. The ramification structure of the extension $L/\mathbb{Q}(T)$ can be determined through the disjoint cycle decomposition, as a permutation of n elements, of the generators of the Galois group of $N/\mathbb{Q}(T)$. The genus of the field L can be computed, using Hurwitz's genus formula. If it is zero and L has a prime of degree 1, then L is a rational function field, $L = \mathbb{Q}(x)$. If the ramified primes of $\mathbb{Q}(T)$ are "well" chosen, the relations which satisfy x can also be obtained from the ramification structure. Therefore, a defining equation of the extension $N/\mathbb{Q}(T)$ can be obtained.

As an example, we shall obtain equations realizing S_n, using this method. Let C_1, C_2 and C_3 be the conjugacy classes of the following permutations: $(n\ n-1 \cdots 3\ 2\ 1)$, $(1\ 2 \cdots k)(k+1\ k+2 \cdots n)$ and $(1\ k+1)$. Each conjugacy class C_i is rational and (C_1, C_2, C_3) is a strictly rigid family. Let $\mathfrak{p}_\infty$, $\mathfrak{p}_0$, $\mathfrak{p}_1$ be the primes of $\overline{\mathbb{Q}}(T)$, defined over $\mathbb{Q}$, given by

$$\mathrm{div}(T) = \mathfrak{p}_0/\mathfrak{p}_\infty, \qquad \mathrm{div}(T-1) = \mathfrak{p}_1/\mathfrak{p}_\infty.$$

The cycle decomposition of those generators of S_n implies that the ramification of these primes in L must be

$$\mathfrak{p}_\infty = \mathfrak{P}_\infty^n, \qquad \mathfrak{p}_0 = \mathfrak{P}_{00}^{n-k}\mathfrak{P}_{01}^k, \qquad \mathfrak{p}_1 = \mathfrak{P}_1^2\mathfrak{A},$$

where $\mathfrak{P}_\infty$, $\mathfrak{P}_{00}$, $\mathfrak{P}_{01}$, $\mathfrak{P}_1$ are primes and $\mathfrak{A}$ denotes an ideal of L. An extension field $L/\mathbb{Q}(T)$ of degree n with the above ramification has, by Hurwitz's genus formula, genus zero. Then $L = \mathbb{Q}(x)$ and we can choose x such that

$$\operatorname{div}(x) = \frac{\mathfrak{P}_{00}}{\mathfrak{P}_\infty}, \qquad \operatorname{div}(x-1) = \frac{\mathfrak{P}_1}{\mathfrak{p}_\infty},$$
$$\operatorname{div}(x-a) = \frac{\mathfrak{P}_{01}}{\mathfrak{P}_\infty}, \qquad \operatorname{div}(x^{n-2} + a_{n-3}x^{n-3} + \cdots + a_0) = \frac{\mathfrak{A}}{\mathfrak{P}_\infty^{n-2}}.$$

Therefore we can deduce that the equation

$$F(X,T) = X^{n-k}(X - \frac{n}{n-k})^k - (\frac{-k}{n-k})^k T,$$

defines the extension $L/\mathbb{Q}(T)$ and its Galois group over $\mathbb{Q}(T)$ is isomorphic to S_n,

$$\operatorname{Gal}_{\mathbb{Q}(T)}(F(X,T)) \cong S_n.$$

Let N be the decomposition field of $F(X,T)$ over $\mathbb{Q}(T)$. Let $M = N^{A_n}$ the fixed field by A_n. Studying the ramification of $M/\mathbb{Q}(T)$ and again using Hurwitz's formula, we can find that $M = \mathbb{Q}(y)$. We can compute the defining equation of L/M. Let

$$F_{n,k}(X,T) = \begin{cases} X^n - A(nX - k(n-k)^k, & n \text{ odd} \\ X^n + k^{n-2k}B^{n-k-1}(nX + (n-k)kB)^k, & n \text{ even}, \end{cases}$$

where $A = k^{n-2k}(1 - (-1)^{(n-1)/2}nT^2)$, $B = (-1)^{n/2}k(n-k)T^2 + 1$ and $k \le n/2$, the Galois group of $F_{n,k}(X,T)$ over $\mathbb{Q}(T)$ is isomorphic to A_n (cf. [**Vi 85**]).

Explicit polynomials over $\mathbb{Q}(T)$ and over $\mathbb{Q}$ with prefixed Galois group have also been obtained, using this method, for the following groups:

$\mathrm{PSL}_2(p)$, $p = 7, 11, 13$ [**Mal-Ma 85**]; $\mathrm{SL}_2(8)$ [**Ma 84**]; M_{11}, M_{12} [**Ma-Ze 86**] and M_{22} [**Mal 88**]; all the primitive nonsolvable permutation groups of degree ≤ 15 [**Ma 84**], [**Mal 87**]; $\mathrm{Sp}_6(2)$, $\mathrm{GO}_6^-(2)$, $\mathrm{O}_6^-(2)$ [**Hä ?**].

5. Galois embedding problem II: Extensions of simple groups

Since rationality criteria work for simple groups, but need the condition of trivial center, it seems therefore that the next step, in order to realize finite groups as Galois groups over $\mathbb{Q}$, will be to consider extension groups of simple groups and to study the subsequent Galois embedding problems. Let

$$1 \longrightarrow H \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$$

be an exact sequence of finite groups. The group $\widetilde{G}$ is an extension of H by G, $\widetilde{G} = H \cdot G$. Firstly we analyze the easy cases. Suppose that the exact sequence splits, that is, the extension group is $\widetilde{G} = H \times G$. If the group G occurs as a Galois group of a regular extension L of $\mathbb{Q}(T)$, then, by Galois theory, each Galois extension $N_0/\mathbb{Q}$ with Galois group H, defines a Galois extension $N_0L/\mathbb{Q}(T)$ with Galois group isomorphic to $\widetilde{G}$. Note that the extension field obtained is non-regular. Should the extension group be a wreath product $\widetilde{G} = H \wr G$, an analogous result is valid (cf. [**Ma 87**]). If the extension group is a semidirect product $\widetilde{G} = H : G$, with H a non-trivial abelian group, an analogous result is also valid, since the semidirect product $H : G$ is a quotient of a wreath product $H \wr G$. Let us distinguish two cases for non-split extensions $\widetilde{G} = H \cdot G$.

Case I. H **non-abelian:** $Z(H) = \{1\}$. It is known from group theory that if the extension group $\widetilde{G} = H \cdot G$ has H non-abelian with trivial center then the group $\widetilde{G}$ is isomorphic to a subgroup $U \subset \mathrm{Aut}(H) \times G$ which satisfies

$$U \cap \mathrm{Aut}(H) = \mathrm{Inn}(H)$$
$$\mathrm{pr}_2(U) = G$$

Following Matzat [**Ma 85**], we say that a finite group G has a GAR-realization over $K(T)$ if the following conditions are satisfied:

(G) There exists a regular Galois extension $N/K(T)$ such that $G \cong \mathrm{Gal}(N/K(T))$.

(A) There exists a subgroup $A \subset \mathrm{Aut}(N/K)$ such that $A \cong \mathrm{Aut}(G)$ and $K(T) = N^{\mathrm{Inn}(G)}$.

(R) Each regular extension R/N^A over K with $\overline{K}R = \overline{K}(T)$ is a rational function field over the field K.

Let K be a number field and K_0/K a Galois realization of the group G, $G \cong \mathrm{Gal}(K_0/K)$. Suppose that the group H has a GAR-realization

over $K(T)$, $N/K(T)$, from condition (A) we can consider $L = N^A$. Let $L_0 = K_0 L$ and $N_0 = K_0 L$. By Galois theory, we find that N_0/L is a Galois extension whose Galois group is

$$\mathrm{Gal}(N_0/L) \cong \mathrm{Aut}(H) \times G.$$

On the other hand, $\widetilde{G}$ is isomorphic to a subgroup U of $\mathrm{Gal}(N_0/L)$. The fixed field $M = N_0^U$ is a rational function field over K, by condition (R). Therefore, the extension field N_0/M with Galois group $\widetilde{G}$ provides solutions to the associated Galois embedding problem. Now we can formulate the following result of Matzat [**Ma 85**]

Theorem. *Let K be a number field, H a non-trivial finite group with $Z(H) = \{1\}$ such that it has a GAR-realization over $K(T)$. Then every Galois embedding problem over K with kernel H has an infinite number of solutions.*

As a consequence, if a finite group G has a normal tower

$$G \supset G_0 \supset G_1 \supset \cdots \supset G_n = \{1\}$$

such that G/G_0 occurs as Galois group over a number field K, and G_{i-1}/G_i has a GAR-realization over $K(T)$ for all $i = 1, \ldots, n$, there are an infinite number of Galois extensions over K with Galois group isomorphic to G.

Summarizing the results of Häfner, Folkers, Malle, Matzat and Pahlings, we can establish:

Theorem. *The following simple groups have a GAR-realization over $\mathbb{Q}(T)$:*

The alternating group A_n, $n \neq 6$ [**Ma 85**].

All the sporadic simple groups, except the Mathieu group M_{23} [**Ma 85**], [**Pa 89**].

The following classical groups of Lie type:

$\mathrm{PSL}_2(p)$,	$p \not\equiv \pm 1 \pmod{24}$	[Mal-Ma 85]
$\mathrm{PSL}_3(p)$,	$p \equiv 5 \pmod{12}$	[Th 84b]
$\mathrm{PSU}_3(p)$,	$p \equiv 7 \pmod{12}$, $p \equiv 10, 19 \pmod{21}$,	[Mal 90]
$\mathrm{PSp}_4(p)$,	$p \equiv 13, 17 \pmod{20}$,	[Hä ?]
$\mathrm{PSp}_{\ell-1}(2)$,	2 *a primitive root mod. the prime* $\ell \geq 7$	[Hä ?]
$\mathrm{PSO}^+_{\ell+1}(2)$,	2 *a primitive root mod. the prime* ℓ	
	$\ell \equiv -1 \pmod{4}$, $\ell \geq 11$	[Hä ?]
$\mathrm{PSO}^-_{\ell-1}(2)$,	2 *a primitive root mod. the prime* $\ell \geq 11$	[Th 84d]

The following exceptional groups of Lie type:

$G_2(p)$,	$p \geq 5$	[Ma 87]
$F_4(p)$,	$p \equiv \pm 2, \pm 6 \pmod{13}$, $p \geq 19$	[Mal 88]
$E_6(p)$,	$p \equiv 4, 5, 6, 9, 16, 17 \pmod{19}$	[Mal ?]
$E_8(p)$,	$p \equiv \pm 3, \pm 7, \pm 9, \pm 10, \pm 11, \pm 12,$	
	$\pm 13, \pm 14 \pmod{31}$, $p \geq 131$	[Mal 88].

Case II. H **abelian:** $H \subset Z(\widetilde{G})$. Let

$$1 \longrightarrow H \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1$$

be a central extension of G, $H \subset Z(\widetilde{G})$. These extension groups are on the opposite side. Rigidity requires a trivial center but any finite group $\widetilde{G}$, with $Z(\widetilde{G}) \neq \{1\}$, can be considered as a central extension of the group $G := \widetilde{G}/Z(\widetilde{G})$ which has a non-trivial center. This leads us to the study of the realization of these extensions groups as Galois groups.

Suppose that we know that G is a Galois group over a number field K, $G = \mathrm{Gal}(N/K)$, since in this case the kernel H is an abelian group, the associated Galois embedding problem into $\widetilde{G}$ has a solution if and only if there exists a lifting $\tilde{p} : G_K \longrightarrow \widetilde{G}$ of the projection $p : G_K \longrightarrow G$. On the other hand, $\widetilde{G}$ as an extension group of G defines a cohomological element $c \in H^2(G, H)$. Therefore, there exists a lifting $\tilde{p}$ of p if and only if $\inf(c)=0$. Note that if the extension group splits, then $c = 0$ and $\inf(c) = 0$.

Let G be a perfect group, for example a simple group. There exists an universal central extension of G,

$$1 \longrightarrow H \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1,$$

This extension is characterized by the following universal property: For every central extension of G

$$1 \longrightarrow A \longrightarrow E \longrightarrow G \longrightarrow 1,$$

there exists one and only one homomorphism from $\widetilde{G}$ to E over G. Therefore we can formulate the following reduction theorem.

Theorem. *Let K be a number field and G a perfect group. Suppose that G appears as a Galois group over K, $G = \mathrm{Gal}(N/K)$. If the extension N/K can be embedded into a Galois extension over K with Galois group $\widetilde{G}$, then N/K can be embedded in a Galois extension over K whose Galois group is any central extension of G.*

Consequently the question whether a central extension of a perfect group G occurs as a Galois group is reduced to solve the problem for the universal extension of G. It is known that the kernel of the universal extension of G is the Schur multipliers of G, $H = M(G)$. These groups are well known for the simple groups (cf. [**At 85**]), for example,

$$M(A_n) \cong \mathbb{Z}/2\mathbb{Z}, \quad n \neq 6, 7; \qquad M(A_6) = M(A_7) = \mathbb{Z}/6\mathbb{Z};$$
$$M(M_{11}) = \{1\}, \qquad M(M_{12}) = M(\mathrm{PSL}_2(\mathbb{F}_p)) = \mathbb{Z}/2\mathbb{Z}.$$

We will now make a distintion according to whether the kernel of the embedding problem is $\mathbb{Z}/2\mathbb{Z}$ or not.

Suppose now that $H = \mathbb{Z}/2\mathbb{Z}$, the obstruction to the Galois embedding problem lies, in this case, in the 2-component of the Brauer group of K

$$\inf(c) \in H^2(G_K, \mathbb{Z}/2\mathbb{Z}) = \mathrm{Br}_2(K).$$

Suppose that L/K is a separable extension field of degree n, $\mathrm{car}(K) \neq 2, 3$, such that its normal closure is N/K. Clearly, $G = \mathrm{Gal}(N/K) \subset S_n$. Let $2^- S_n$ be the Schur double cover of S_n such that the transpositions are lifted to elements of order two. Let $\widetilde{G}$ be the inverse image of G in $2^- S_n$, we have

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \widetilde{G} \longrightarrow G \longrightarrow 1,$$

Serre [**Se 84**] has determined the obstruction to this embedding problem:

Theorem.

$$\inf(c) = (2, d_L) + w(L/K),$$

where $w(L/K)$ denotes the Hasse-Witt invariant of the quadratic form $Tr_{L/K}(x^2)$, and d_L its discriminant.

Then, the problem of realizing $\widetilde{G}$ as Galois group over K is reduced to solving the following steps:

a) Find irreducible polynomials $f(X) \in K[X]$ of degree n with Galois groups isomorphic to G.

b) Compute $w(K(\alpha)/K)$, where α is a root of $f(X)$.

c) Impose conditions over $f(X)$ in order to have $w(K(\alpha)/K) = (2, d_{K(\alpha)})$.

The first case studied was $\widetilde{G} = \widetilde{A}_n$, the Schur double cover of A_n. It can be proved [**Vi 84**] that the decomposition field of the previous equations with Galois group A_n over $\mathbb{Q}(T)$ can be embedded into a Galois extension with Galois group $\widetilde{A}_n$, for the following values of n:

$n \equiv 0, 1 \pmod 8$

$n \equiv 2 \pmod 8$ and sum of two squares

$n \equiv 3 \pmod 8$ and sum of three squares, $n = x_1^2 + x_2^2 + x_3^2, (x_1, n) = 1$.

Consequently, any central extension of A_n occurs as a Galois group over any number field, for these values of n. Feit [**Fe 86**], using Laguerre polynomials, proved that $\widetilde{A}_6$ and $\widetilde{A}_7$ are also Galois group over every number field. Mestre [**Me 90**] constructs new realizations of A_n having an associated trace form independently of T such that for $T = 0$, its Hasse-Witt invariant is trivial. Then, for any value of n, $\widetilde{A}_n$ appears as a Galois group over every number field. Summarizing results of Bayer, Feit, Häfner, Llorente, Mestre, Sonn and Vila we can formulate

Theorem. *The following double covers appear as Galois groups over every number field:*

$2\,A_n$, *for all values of* n	[**Vi 84**] [**Me 90**]
$2^+S_n, 2^-S_n$, *for all values of* n,	[**Vi 88**] [**So 89**]
$2\,M_{12}$	[**Ba-Ll-Vi 86**]
$2\,\mathrm{Sp}_6(2)$	[**Hä ?**].

Construction of double covers Galois extension fields have been obtained by Crespo [**Cr 89**], [**Cr 90**], as explicit solutions to embedding problems, for $2.A_n$, 2^+S_n and 2^-S_n.

In the case that the kernel $H \neq \mathbb{Z}/2\mathbb{Z}$, it seems to be simpler to construct extensions with Galois group $\widetilde{G}$. The following idea of Feit (cf. [**Fe 89**]) allows us the use of rigidity methods: if the group G has an outer automorphism ρ which can be extended to $\widetilde{G}$ and acts non trivially on $Z(\widetilde{G})$, then, if the semidirect extension group $\widetilde{G} :< \rho >$ has trivial center, the rationality criteria are applicable. If $N/\mathbb{Q}(T)$ is a Galois extension with Galois group $\widetilde{G} :< \rho >$ and the fixed field $N^{\widetilde{G}}$ is a rational function field, then an extension with Galois group $\widetilde{G}$ over $\mathbb{Q}(T)$ is found. Using these arguments, Feit [**Fe 89**], Malle [**Mal 90**] and Häfner [**Hä ?**] have obtained

Theorem. *The following triple covers appear as Galois groups over every number field:*

$3.A_6,\ 3.A_7,\ 3.M_{22},\ 3.Suz,\ 3.Fi'_{24},\ 3.O'N$	[**Fe 89**]
$SU_3(p),\ p \equiv -1 \pmod 4,\ p > 3;\ p \equiv 3,5 \pmod 7,\ p > 5$	[**Mal 90**]
$3.O_7(3),\ 3.SO_7(3)$	[**Hä ?**].

References

[Atlas 85] CONWAY, J. H., CURTIS, R. T., NORTON, S. P., PARKER, R. A. AND WILSON, R. A., "*Atlas of finite groups*," Oxford, Clarendon Press, 1985.

[Ba-Ll-Vi 86] BAYER, P., LLORENTE, P. AND VILA, N., $\widetilde{M}_{12}$ comme groupe de Galois sur $\mathbb{Q}$, *C. R. Acad. Sc. Paris* **303** (1986), 277–280.

[Be 79] BELYI, G. V., On Galois extensions of a maximal cyclotomic field, *Izv. Akad. Nauk. SSSR Ser. Mat.* **43** (1979), 267–276; *Math. USSR Izv.* **14** (1980), 247–256.

[Cr 89] CRESPO, T., Explicit construction of $\widetilde{A}_n$ type fields, *J. of Algebra* **127** (1989), 425–461.

[Cr 90] CRESPO, T., Explicit construction of $2S_n$ Galois extensions, *J. of Algebra* **129** (1990), 312–319.

[De 89] DENTZER, R., Projektive symplektische Gruppen $PSp_4(p)$ als Galoisgruppen über $\mathbb{Q}(t)$, *Arch. Math.* **53** (1989), 337–346.

[Ek 90] EKEDAHL, T., An effective version of Hilbert's irreducibility theorem, in "*Séminaire de Théorie des Nombres, Paris, 1988-89*," Birkhäuser, 1990, pp. 241-249.

[Fe 84] FEIT, W., Rigidity of $\mathrm{Aut}(PSL_2(p^2))$, $p \equiv \pm 2 \pmod 5$, $p \neq 2$, in "*Proceedings of the Rutgers group theory year, 1983-1984*," Cambridge University Press, Cambridge, 1984, pp. 351–356.

[Fe 86] FEIT, W., $\widetilde{A}_5$ and $\widetilde{A}_7$ are Galois groups over number fields, *J. of Algebra* **104** (1986), 231–260.

[Fe 89] FEIT, W., Some finite groups with nontrivial centers which are Galois groups, in "*Group Theory, Proceedings of the 1987 Singapore Conference*," W. de Gruyter, Berlin-New York, 1989, pp. 87–109.

[Fe-Fo 84] FEIT, W. AND FONG, P., Rational rigidity of $G_2(p)$ for any prime $p > 5$, in "*Proceedings of the Rutgers group theory year, 1983-1984*," Cambridge University Press, Cambridge, 1984, pp. 323–326.

[Fr 28] FRICKE, R., "*Lehrbuch der Algebra III*," Braunschweig, Vieweg, 1928.

[Fri 77] FRIED, M. D., Fields of definition of function fields and Hurwitz families- Groups as Galois group, *Commun. Alg.* **5** (1977), 17–82.

[Hä ?] HÄFNER, F., Einige orthogonale und symplektische Gruppen als Galoisgruppen über $\mathbb{Q}$, (to appear).

[Hi] HILBERT, D., Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, *J. reine angew. Math.* **110** (1892), 104–129.

[Ho 68] HOECHSMANN, K., Zum Einbettungsproblem, *J. reine angew. Math.* **229** (1968), 81–106.

[Hoy 85] HOYDEN-SIEDERSLEBEN, G., Realisierung der Jankogruppen J_1 und J_2 als Galoisgrouppen über $\mathbb{Q}$, *J. Algebra* **97** (1985), 14–22.

[Hu 86] HUNT, D. C., Rational rigidity and the sporadic groups, *J. Algebra* **99** (1986), 577–592.

[Ik 60] IKEDA, M., Zur Existenz eigentlicher galoisscher Körper beim Einbettungsproblem für galoissche Algebren, *Abh. Math. Sem. Univ. Hamburg* **24** (1960), 126–131.

[Iš 76] IŠHANOV, V. V., On the semidirect imbedding problem with nilpotent kernel, *Izv. Akad. Nauk. SSSR Ser. Mat.* **40** (1976); *Math. USSR Izv.* **10** (1976), 1–23.

[Iš-Lu-Fa ?] IŠHANOV, V. V., LURIE, B. B. AND FADDEEV, D. F., "*The embedding problem in Galois theory*," Nauka, Moscou (to appear).

[Le 74] LENSTRA, H. W., Rational functions invariant under a finite abelian group, *Invent. Math.* **25** (1974), 299–325.

[Mal 87] MALLE, G., Polynomials for primitive nonsolvable permutation groups of degree $d \leq 15$, *J. Symb. Comput.* **4** (1987), 83 –92.

[Mal 88a] MALLE, G., Exceptional groups of Lie type as Galois group, *J. reine angew. Math.* **392** (1988), 70–109.

[Mal 88b] MALLE, G., Polynomials with Galois group $\mathrm{Aut}(M_{22})$, M_{22}, and $\mathrm{PSL}_3(\mathbb{F}_4) \cdot 2_2$ over $\mathbb{Q}$, *Math. Comput.* **51** (1988), 764–768.

[Mal 90] MALLE, G., Some unitary groups as Galois groups over $\mathbb{Q}$, *J. Algebra* **131** (1990), 476–482.

[Mal ?] MALLE, G., Disconnected groups of Lie type as Galois groups, (to appear).

[Mal-Ma 85] MALLE, G. AND MATZAT, B. H., Realisierung von Gruppen $\mathrm{PSL}_2(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$, *Math. Ann.* **272** (1985), 549–565.

[Ma 84] MATZAT, B. H., Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe, *J. reine angew. Math* **349** (1984), 179 –220.

[Ma 85] MATZAT, B. H., Zum Einbettungsproblem der algebraischen Zahlentheorie mit nicht abelschem Kern, *Invent. Math.* **80** (1985), 365–374.

[Ma 87] MATZAT, B. H., "*Konstruktive Galoistheorie*," Springer-Verlag, Berlin, 1987.

[Ma 89] MATZAT, B. H., Rationality criteria for Galois extensions, in "*Galois groups over* $\mathbb{Q}$," Springer-Verlag, New York, 1989, pp. 361–383.

[Ma 91] MATZAT, B. H., Zöpfe und Galoissche Gruppen, *J. reine angew. Math.* **420** (1991), 99–159.

[Ma-Ze 86] MATZAT, B. H. AND ZEH-MARSCHKE, A., Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbb{Q}$, *J. Number Theory* **23** (1986), 195–202.

[Me 88] MESTRE, J.-F., Courbes hyperelliptiques à multiplications réelles, *C.R. Acad. Sci. Paris* **307** (1988), 721–724.

[Me 90] MESTRE, J.-F., Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\widetilde{A}_n$, *J. Algebra* **131** (1990), 483–495.

[No 18] NOETHER, E., Gleichungen mit vorgeschriebener Gruppe, *Math. Ann.* **78** (1918), 221–229.

[Pa 88] PAHLINGS, H., Some sporadic groups as Galois groups, *Rend. Sem. Math. Univ. Padova* **79** (1988), 97–107.

[Pa 89] PAHLINGS, H., Some sporadic groups as Galois groups II, *Rend. Sem. Math. Univ. Padova* **82** (1989), 163–171.

[Ri 75] RIBET, K. A., On l-adic representations attached to modular forms, *Invent. Math.* **28** (1975), 245–275.

[Ša 54a] ŠAFAREVIČ, I. R., On the construction of fields with a given Galois group of order l^a, *Izv. Akad. Nauk. SSSR Ser. Mat.* **18** (1954), 216–296; *Amer. Math. Soc. Transl.* **4** (1956), 107–142.

[Ša 54b] ŠAFAREVIČ, I. R., On an existence theorem in the theory of algebraic numbers, *Izv. Akad. Nauk. SSSR Ser. Mat.* **18** (1954), 327–334; *Amer. Math. Soc. Transl.* **4** (1956), 143–151.

[Ša 54c] ŠAFAREVIČ, I. R., On the problem of imbedding fields, *Izv. Akad. Nauk. SSSR Ser. Mat.* **18** (1954), 389–418; *Amer. Math. Soc. Transl.* **4** (1956), 151–183.

[Ša 54d] ŠAFAREVIČ, I. R., Construction of fields of algebraic numbers with given solvable Galois group, *Izv. Akad. Nauk. SSSR Ser. Mat.* **18** (1954), 525–575; *Amer. Math. Soc. Transl.* **4** (1956), 185–237.

[Sc 37] SCHOLZ, A., Konstruktion algebraischer Zahlkörper mit beliebiger Gruppe von Primzahlpotenzordnung I, *Math. Z.* **42** (1937), 161–188.

[Se 84] SERRE, J.-P., L'invariant de Witt de la forme $\mathrm{Tr}(x^2)$, *Comment. Math. Helvetici* **59** (1984), 651–676.

[Se 88] SERRE, J.-P., Groupes de Galois sur $\mathbb{Q}$, Sém. Bourbaki 1987–1988, *Asterisque* **161-162** (1988), 73–85.

[Sh 74] SHIH, K.-Y., On the construction of Galois extensions of function fields and number fields, *Math. Ann.* **207** (1974), 99–120.

[So 89] SONN, J., Central extensions of S_n as Galois group via trinomials, *J. Algebra* **125** (1989), 320–330.

[Su 82] SUZUKI, M., "*Group theory I*," Springer-Verlag, Berlin, 1982.

[Sw 69] SWAN, R. G., Invariant rational functions and a problem of Steenrod, *Invent. Math.* **7** (1969), 148–158.

[Th 84a] THOMPSON, J. G., Some finite groups which appear as $\mathrm{Gal}(L/K)$ where $K \leq \mathbb{Q}(\mu_n)$, *J. Algebra* **89** (1984), 437–499.

[Th 84b] THOMPSON, J. G., PSL_3 as Galois group over $\mathbb{Q}$, in "*Proceedings of the Rutgers group theory year, 1983-1984*," Cambridge University Press, Cambridge, 1984, pp. 309–319.

[Th 84c] THOMPSON, J. G., Primitive roots and rigidity, in "*Proceedings of the Rutgers group theory year, 1983-1984*," Cambridge University Press, Cambridge, 1984, pp. 327–350.

[Th 86] THOMPSON, J. G., Regular Galois extensions of $\mathbb{Q}(x)$, in "*Group theory, Beijing 1984*," Springer-Verlag, Berlin, 1984, pp. 210–220.

[Vi 85] VILA, N., On central extensions of A_n as Galois group over $\mathbb{Q}$, *Arch. Math.* **44** (1985), 424–437.

[Vi 88] VILA, N., On stem extensions of S_n as Galois group over number fields, *J. Algebra* **116** (1988), 251–260.

[Wa 84] WALTER, J. H., Classical groups as Galois groups, in "*Proceedings of the Rutgers group theory year, 1983-1984*," Cambridge

University Press, Cambridge, 1984, pp. 357–383.

[We 08] WEBER, H., "*Lehrbuch der Algebra III*," Vieweg, Braunschweig, 1908.

Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007 Barcelona
SPAIN

Rebut el 7 de Gener de 1992