The inverse Problem of Galois theory

Christian U. Jensen

København Universitets matematiske Institut
Universitetsparken 5
DK- 2100 København
cujensenmath.ku.dk

The essence of Galois Theory: The systematically developed connection between two seemingly unrelated subjects, the theory of fields and the theory of groups.

More specifically, but in the same line, is the idea of studying a mathematical object by its group of automorphisms, an idea emphasized in Klein's Erlanger Program, which has been accepted as a powerful tool in a great variety of mathematical disciplines.

The Galois Theory of field extensions combines the esthetic appeal of a theory of nearly perfect beauty with the technical development and difficulty that reveal the depth of the theory and that make possible its great usefulness primarily in algebraic number theory and related parts of algebraic geometry.
(From Roger Lyndon in: Encyclopedia of Mathematics and Its Applications)

1 Basic concepts

For the convenience of the reader we start by briefly recalling the basic concepts. All fields in this article are supposed to have characteristic 0, so there will be no problems of separability. (In other words: every finite field extension will be separable.)

If L/K is a field extension $Aut(L/K)$ is defined as the group of all field automorphisms of L that are the identity on K. If K is the fixed field of $Aut(L/K)$, (i.e. no element in $L \setminus K$ is left invariant by all automorphisms of $Aut(L/K)$) then L/K is called a *Galois extension* (or normal extension). If L/K is Galois $Aut(L/K)$ is usually denoted $Gal(L/K)$.

Theorem 1.1. *For a finite extension L/K the following conditions are equivalent:*

i) L/K is a Galois extension.

ii) L is the splitting field over K for a polynomial $f(x)$ in $K[x]$, (i.e., L is a smallest extension of K, in which $f(x)$ splits completely in linear factors.)

iii) Every irreducible polynomial $f(x)$ in $K[x]$ having some root in L splits in linear factors in L.

For the sake of brevity a Galois extension of a field K with Galois group G is called a G-extension of K. If $f(x)$ is a polynomial in $K[x]$ the Galois group of the splitting field of $f(x)$ over K is called the Galois group of $f(x)$. As for the explicit form of the Galois group the following is quite useful.

Theorem 1.2. *If L is the splitting field over a field K of an irreducible polynomial $f(x)$ in $K[x]$ of degree n, then the action of the Galois group $Gal(L/K)$ on the roots of $f(x)$ gives rise to a permutation of these n roots. This yields an isomorphism of $Gal(L/K)$ onto a transitive subgroup of the symmetric group S_n, called the Galois permutation group of $f(x)$.*

Another useful tool in determining Galois groups is the following.

Theorem 1.3. *Let M and L be extension fields of a field K, both of them being contained in a common larger field. If M/K is a finite Galois extension then the compositum ML is a Galois extension of L and $Gal(ML/L) \simeq Gal(M/M \cap L)$. If M and L are finite Galois extensions of K and $M \cap L = K$ then the compositum ML is a finite Galois extension of K and $Gal(ML/K)$ is isomorphic to the direct product $Gal(M/K) \times Gal(L/K)$.*

The *inverse problem of Galois theory* asks whether every finite group can be realized as the Galois group for some Galois extension of the rational number field $\mathbb{Q}$. This problem can also be expressed in terms of permutation groups: Given a transitive subgroup G of the symmetric group S_n, the question is whether there exists an irreducible polynomial $p(x)$ in $\mathbb{Q}[x]$ of degree n, such that G is the Galois permutation group described in Theorem 1.2 with $K = \mathbb{Q}$. Although many families of finite groups can be realized as Galois groups over $\mathbb{Q}$ it is still an open problem whether every finite group is realizable as Galois group over $\mathbb{Q}$. In this article we shall give a survey of some important results on this question. The account we give is by no means complete. It is just our hope to give an impression of the type of results and the type of methods that are used.

The author is grateful to Juliusz Brzezinski and Anders Thorup, who have read the manuscript and made several valuable comments.

2 Some "relatively easy" results

We start by a classical result which basically is just a study of cyclotomic fields, i.e. fields generated by roots of unity.

Theorem 2.1. *Every finite abelian group A appears as a Galois group over $\mathbb{Q}$.*

Proof. (Sketch.) A is a direct product of cyclic groups. We restrict ourselves to prove the theorem for a cyclic group. The proof for general A is slightly more involved but depends on the same ideas.

Consider the cyclic group C_n of order n. By Dirichlet´s theorem concerning prime numbers in arithmetic progressions there exists a prime number p which is $\equiv 1$ modulo n. The Galois group over $\mathbb{Q}$ of the p^{th} cyclotomic field $\mathbb{Q}(\zeta_p)$, ζ_p being a primitive p^{th} root of unity, is cyclic of order $p-1$. Since n divides $p-1$ the Galois group $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ contains a subgroup H such that the quotient $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})/H$ is cyclic of order n. By the main theorem of Galois theory, the fixed field of H will then be a C_n-extension of $\mathbb{Q}$. □

Remark. The realizability of two finite groups G and H as Galois groups over $\mathbb{Q}$ does not automatically imply the realizability of the direct product $G \times H$ as a Galois group over $\mathbb{Q}$. This, of course, holds if the orders $|G|$ and $|H|$ are relatively prime, since in that case the compositum of a G-extension and an H-extension will be a $(G \times H)$-extension. But in general one should be careful: There exist fields K admitting a G-extension and an H-extension, but not a $(G \times H)$-extension. However, from the above theorem 2.1, theorem 1.3 and proposition 2.2 below (for $\mathcal{A}$ being the family of finite abelian groups) it follows that if G is realizable as a Galois group over $\mathbb{Q}$, then so is $G \times A$ for every finite abelian group A.

Proposition 2.2. *Let $\mathcal{A}$ be family of finite groups which is closed under formation of finite direct products. Let K be a field such that any group in $\mathcal{A}$ is a Galois group over K. If L is an arbitrary finite extension of K, then there exists for any $A \in \mathcal{A}$ an A-extension of K whose intersection with L is K.*

Proof. Since all fields in this article have characteristic 0, there is a primitive element for the extension L/K, and hence by a theorem of Artin there are only finitely many fields between L and K. Let t be the number of these fields. Let A be a group in $\mathcal{A}$. The direct product A^{t+1} of $t+1$ copies of A is by assumption realizable as the Galois group of an extension M of K. We can write M as the compositum of $(t+1)$ A-extensions M_i, $1 \leqq i \leqq t+1$, where $M_i \cap M_j = K$ for $i \neq j$. Consider the fields $M_i \cap L$, $1 \leqq i \leqq t+1$. Since there are only t fields between K and L there must be two indices i and j such $i \neq j$ and $M_i \cap L = M_j \cap L$, whence $M_i \cap L = M_j \cap L = M_i \cap L \cap M_j \cap L = M_i \cap M_j \cap L = K \cap L = K$. □

The next two results may at first glance look like being "almost" a solution of the inverse problem of Galois theory.

Theorem 2.3. *For any finite group G there exists an algebraic number field K (i.e. a finite extension of the rational number field $\mathbb{Q}$) that admits a G-extension.*

Proof. (Sketch.) For any odd prime p the polynomial

$$f(x) = (x^2+4)(x-2)(x-4)\cdots(x-2(p-2)) - 2$$

has degree p and is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion applied to the prime number 2. Elementary calculus shows that $f(x)$ has exactly $(p-2)$ real roots. It is a classical result that the splitting field over $\mathbb{Q}$ of an irreducible polynomial in $\mathbb{Q}$ of prime degree p with exactly $p-2$ real roots is Galois over $\mathbb{Q}$ with the

symmetric group S_p as Galois group. Hence the splitting field M of $f(x)$ over $\mathbb{Q}$ is an S_p-extension of $\mathbb{Q}$.

Now for a suitable large prime p the group G sits as a subgroup of S_p. Hence the Galois group of $M/\mathbb{Q}$ contains a copy of G. If K is the corresponding fixed field for G the main theorem of Galois theory implies that M/K is Galois with G as Galois group. □

Remark. The sad thing about the above result is that we have no way of controlling the ground field K, in particular of going down to $\mathbb{Q}$. In some sense the theorem shows that the inverse problem of Galois theory is "just" a problem of descent.

The next result was first proved by E. Fried and J .Kollar [FK], but an error was found in the proof by M. Fried. A relatively elementary proof was given by W.-D. Geyer[Ge]. It will, however, take several pages, so we refrain from giving it here.

Theorem 2.4. *Every finite group is the automorphism group of a finite extension field L of the rational number field $\mathbb{Q}$.*

Remark. The sad thing here is that the field L constructed in this theorem will usually *not* be a Galois extension of $\mathbb{Q}$.

3 Hilbert enters

In some sense the inverse problem of Galois theory is as old as Galois theory itself; however the first systematic attack was made by Hilbert in his famous paper [Hi] in which the principal result was:

Theorem 3.1 (Hilbert's Irreducibility Theorem)**.** *Let $f(x_1, \ldots, x_m, t_1, \ldots, t_n)$ be an irreducible polynomial in $\mathbb{Q}[x_1, \ldots, x_m, t_1, \ldots, t_n]$. Then there exist infinitely many n-tuples $(q_1, \ldots, q_n)$ of rational numbers such that the specialized polynomial $f(x_1, \ldots, x_m, q_1, \ldots, q_n)$ is either a constant in $\mathbb{Q}$ or irreducible viewed as a polynomial in $\mathbb{Q}[x_1, \ldots, x_m]$.*

The proof is by no means easy. A relatively accessible proof can be found in Hadlock[Ha]. Hilbert's Irreducibility Theorem has a very important application in inverse Galois theory:

Theorem 3.2. *Let $\mathbb{Q}(t_1, \ldots, t_n)$ be a purely transcendental extension of $\mathbb{Q}$, i.e. the field of rational functions in n independent variables $t_1, \ldots, t_n$. If $f(x, t_1, \ldots, t_n)$ is a polynomial in x over the field $\mathbb{Q}(t_1, \ldots, t_n)$ with Galois group G, then there exist infinitely many n-tuples $(q_1, \ldots, q_n)$ of rational numbers such that G is the Galois group over $\mathbb{Q}$ of the specialized polynomial $f(x, q_1, \ldots, q_n)$. In particular, if a finite group G can be realized as a Galois group over $\mathbb{Q}(t_1, \ldots t_n)$ then G can also be realized as a Galois group over $\mathbb{Q}$.*

We omit the proof which may take a few pages. The usefulness of the above theorem lies in the fact that it is much easier to realize a group as a Galois group over the function field $\mathbb{Q}(t_1, \ldots, t_n)$ than over $\mathbb{Q}$: there is much more space and freedom to operate in the function field. Here are two examples:

By the general polynomial of degree n we mean the polynomial

$$f(x, t_1, \ldots, t_n) = x^n + t_1 x^{n-1} + \cdots + t_{n-1} x + t_n$$

viewed as a polynomial in x with coefficients in the rational function field $\mathbb{Q}(t_1, \ldots, t_n)$ in n independent variables $t_1, \ldots t_n$. It can shown (e.g. using the theory of symmetric polynomials) that the splitting field of $f(x, t_1, \ldots, t_n)$ over $\mathbb{Q}(t_1, \ldots, t_n)$ is a Galois extension of $\mathbb{Q}(t_1, \ldots, t_n)$ with the symmetric group S_n as Galois group. Theorem 3.2 thus implies that S_n can also be realized as a Galois group over $\mathbb{Q}$.

In the same paper Hilbert showed that also the alternating group A_n can be realized as a Galois group over $\mathbb{Q}(t_1, \ldots, t_n)$.(This is much harder than in the S_n-case.) Thereby one obtains a realization of A_n over $\mathbb{Q}$.

However, there is one defect in the above strategy: Both theorem 3.1. and theorem 3.2. are merely existence theorems and do not yield explicit Galois realizations of the desired groups. One can find explicit polynomials over the function field whose splitting field has the prescribed group as Galois group, but usually not an explicit specialization to $\mathbb{Q}$ with the same Galois group.

For instance, let $P_n(t, x)$ be the following polynomial:

$$P_n(t, x) = \begin{cases} x^n + ((-1)^{(n-1)/2} n t^2 - 1)(nx + n - 1) \text{ for odd } n \\ x^n + n x^{n-1} + (-1)^{n/2} t^2 + (n-1)^{n-1} \text{ for even } n. \end{cases}$$

The splitting field of $P_n(t, x)$ viewed as a polynomial in x over $\mathbb{Q}(t)$ is an A_n-extension of $\mathbb{Q}(t)$. So there exist infinitely many rational numbers q such that the splitting field of $P(q, x)$ over $\mathbb{Q}$ is an A_n-extension. But the theory does not tell us, how to find such q's explicitly. The above results hold for a larger class of fields:

Definition. A field K is called *Hilbertian* if the assertion of Theorem 3.1 remains true when $\mathbb{Q}$ is replaced by K.

Thus the symmetric groups S_n and the alternating groups A_n are realizable as Galois groups over any Hilbertian field.

Examples. Every algebraic number field of finite degree is Hilbertian. For every field K the field of all rational functions over K is Hilbertian. An algebraically closed field (for instance the field $\mathbb{C}$ of complex numbers) is not Hilbertian. Similarly, the field $\mathbb{R}$ of real numbers and the $p-$adic number fields are not Hilbertian.

4 Emmy Noether and others enter

Let G be a subgroup of the symmetric group S_n. Viewed as a group of permutations of n independent variables $t_1, \ldots, t_n$ it gives rise to a group of automorphisms of

the rational function field $\mathbb{Q}(t_1,\ldots,t_n)$. More precisely, if σ is a permutation in G the corresponding automorphism $\bar{\sigma}$ of $\mathbb{Q}(t_1,\ldots,t_n)$ is defined by

$$\bar{\sigma}(f(t_1,\ldots,t_n) = f(t_{\sigma(1)},\ldots,t_{\sigma(n)})$$

where $f(t_1,\ldots,t_n)$ is a rational function in $\mathbb{Q}(t_1,\ldots,t_n)$.

If $\mathcal{F}(G)$ is the fixed field of G then $\mathbb{Q}(t_1,\ldots,t_n)$ is a Galois extension of $\mathcal{F}(G)$ with Galois group G. Emmy Noether raised the following question:

(NP)"*Noether´s Problem*": Is $\mathcal{F}(G)$ isomorphic to the field of rational functions over $\mathbb{Q}$ in n independent variables?

If the answer is " yes", then Theorem 3.2 implies that G is realizable as a Galois group over $\mathbb{Q}$. It will have many other consequences which we shall mention later.

In the case, where $G = S_n$ the answer to (NP) is clearly "yes". Indeed, the fixed field $\mathcal{F}(S_n)$ is just the field of the rational functions of the n elementary symmetric polynomials in $t_1,\ldots,t_n$. For the alternating groups A_n the question is much harder: it is known that the answer to (NP) is affirmative, if $n \leqq 5$, but the answer is not known for any $n > 5$. In the 1920's and 1930's (NP) was answered in the affirmative for several groups of "small" orders. However, already in the case where G is the cyclic group order 3 acting on $\mathbb{Q}(t_1,t_2,t_3)$ by cyclic permutation of the variables it is not trivial to prove that the fixed field is generated by 3 rational functions in $\mathbb{Q}(t_1,t_2,t_3)$. The fixed field is $\mathbb{Q}(T_1,T_2,T_3)$ where

$$T_1 = t_1+t_2+t_3,\ \ T_2 = A(t_1,t_2,t_3)/C(t_1,t_2,t_3),\ \ T_3 = B(t_1,t_2,t_3/C(t_1,t_2,t_3),$$

and

$$A(t_1,t_2,t_3) = 3t_1^2t_2+3t_2^2t_3+3t_3^2t_1-t_1^3-t_2^3-t_3^3-6t_1t_2t_3,$$

$$B(t_1,t_2,t_3) = 3t_1t_2^2+3t_2t_3^2+3t_3t_1^2-t_1^3-t_2^3-t_3^3-6t_1t_2t_3,$$

$$C(t_1,t_2,t_3) = t_1^2+t_2^2+t_3^2-t_1t_2-t_2t_3-t_3t_1.$$

In 1925 Ph. Furtwängler [Fu] proved that (NP) could be answered in the affirmative for all solvable transitive subgroups of S_p, p being a prime $\leqq 11$. He noticed that his method did not work for $p = 47$. For some time a (positive) solution of (NP) was considered to be the "right" way to solve the inverse problem of Galois theory. Therefore, it came as a surprise that in 1969 R.Swan [Sw] and independently V.E. Voskresenskii [Vo] proved that for G equal to the cyclic group C_{47} of order 47 the answer to (NP) is "no". However, the fact that C_{47} can be realized as a Galois group over $\mathbb{Q}$ is, of course, a consequence of theorem 2.1. But the example showed that Noether's approach could not lead to a solution of the inverse problem of Galois theory. For a full list of all references in this area the paper by H. Lenstra [Le] is recommended. Here is also a complete classification of the abelian groups for which (NP) has a negative answer and it is shown that the cyclic group of order 8 is the smallest one.

5 Solvable groups and embedding problems

For a long time it was an open problem whether every finite solvable group could be realized as a Galois group over $\mathbb{Q}$. Since every solvable group has a normal series with abelian quotients and (theorem 2.1) every abelian group is Galois group over $\mathbb{Q}$, it may seem surprising that the realizability of solvable groups could be so hard. However, here it should be taken in consideration that there exist fields K such that any finite abelian group appears as Galois group over K, but no non-abelian group does. To be more specific, one has to study "embedding problems": Let L/K be a finite Galois extension with Galois group G and let $\pi : H \to G$ be a surjective homomorphism of the finite group H onto G. One then asks whether there exists a Galois extension M/K, M containing L and with $Gal(M/K) \simeq H$ such that the restriction map $Res : Gal(M/K) \to Gal(L/K) = G$ corresponds to π, i.e. such that $Res = \pi \circ \phi$ for some isomorphism $\phi : Gal(M/K) \to H$. This is called the *embedding problem* given by L/K and π. In case of an affirmative answer we say that M/K is a solution to the embedding problem. We illustrate the above by two examples.

Examples. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{2})$ and π the canonical homorphism for the cyclic group C_4 of order 4 onto the cyclic group C_2 of order 2. The correponding embedding problem has a solution with $M = \mathbb{Q}(\sqrt{2+\sqrt{2}})$.

However, with the same K but $L = \mathbb{Q}(\sqrt{-1})$ and the same π it is just an exercise in Galois theory to see that the corresponding embedding problem has no solution.

Some important embedding problems are solvable. Let G be the Galois group of a finite Galois extension L/K and let A be a finite group, on which G acts, i.e. there is given a homomorphism $\alpha : G \to Aut(A)$. One can then define the semi-direct product $A \rtimes G$ as the set of all pairs (a, g) with the group composition

$$(a_1, g_1)(a_2, g_2) = (a_1 \alpha_{g_1}(a_2), g_1 g_2).$$

This gives rise to a short exact sequence

$$1 \to A \underset{i}{\to\to} A \rtimes G \underset{\pi}{\to\to} G \to 1,$$

where i is the injective map sending a to $(a, 1)$, π is the surjective mapping sending (a, g) to g and the kernel of π equals the image of i. One can then consider the embedding problem with $H = A \rtimes G$ and the π as above.

The following result is basically due to M. Ikeda (Cf.[JLY] p. 108).

Theorem 5.1. *Let K be a Hilbertian field (e.g. $\mathbb{Q}$) and let L/K be a Galois extension with G as Galois group. Let A be an abelian group on which G acts. Then the above embedding problem has a solution, that is, there is an $(A \rtimes G)$-extension of K having L as its G-subextension.*

A very special case is the following. Let K be $\mathbb{Q}$, and L an extension of degree 2, i.e. $L = \mathbb{Q}(\sqrt{q})$, where q is a rational number which is not a square. Let A be

the cyclic group C_n of order n and let the non-trivial element in $Gal(\mathbb{Q}(\sqrt{q})/\mathbb{Q})$ act on C_n by sending each element in C_n to its inverse. Then the corresponding semi-direct product is the dihedral group D_n of order $2n$. The theorem then says that $L = \mathbb{Q}(\sqrt{q})$ can be embedded in a D_n extension. In particular, every dihedral group is realizable as a Galois group over $\mathbb{Q}$.

As for the realizability of solvable groups the first general step was taken in 1937 by Reichardt[Re] and Scholz[Sco], who considered the case of p-groups, i.e. groups whose order is a power of a prime p. By solving successive embedding problems controlling ramifications such that obstructions were eliminated they managed to prove that for any odd prime p every p-group appears a Galois group over $\mathbb{Q}$. Shafarevich succeeded in extending this result to the case $p = 2$ and finally in 1954 [Sha] obtained the celebrated theorem that every finite solvable group can be realized as Galois group over $\mathbb{Q}$. The proof was extremely complicated and had several inaccuracies. The first complete proof, correct in all details, was given in the book [NSW]

6 Generic polynomials and regular extensions

Instead of just knowing that a finite group G can be realized as a Galois group over $\mathbb{Q}$ it would be desirable to get some kind of "universal parametrization" of all G-extensions of $\mathbb{Q}$. To put the question more precisely the following concept is introduced.

Definition. Let $P(t_1, \ldots, t_n)(x)$ be a monic polynomial in $\mathbb{Q}(t_1, \ldots, t_n)[x]$, where $t_1, \ldots, t_n$ and x are independent variables and let G be a finite group. $P(t_1, \ldots, t_n)(x)$ is called a generic polynomial for the group G, if the following two conditions are satisfied:

(i) for every field K the splitting field of $P(t_1, \ldots, t_n)(x)$ over $K(t_1, \ldots, t_n)$ is a G-extension of $K(t_1, \ldots, t_n)$,

(ii) for every field K every G-extension of K is the splitting field over K for $P(a_1, \ldots, a_n)(x)$ for a suitable n-tuple $(a_1, \ldots, a_n) \in K^n$.

The variables $t_1, \ldots, t_n$ are called the parameters.

If there is a G-generic polynomial of the finite group G (with unspecified n), then theorem 3.2 implies that G is realizable as a Galois group over $\mathbb{Q}$ and actually over any Hilbertian field. It can be proved that if (NP) has a positive solution for a group G then there exists a G-generic polynomial, but the converse is false. As mentioned earlier (NP) has a negative answer if G is cyclic of order 47, but by the following result of Lenstra there exists generic polynomial for the cyclic group of order 47.

Theorem 6.1. *There exist G-generic polynomials for a finite abelian group G if and only if G has no element of order 8.*

The theorem shows, in particular, that already for the cyclic group of order 8, the answer to (NP) is negative. As for dihedral groups less information is available.

For the dihedral group D_q of order $2q$, q being an odd number, there exist generic polynomials, but if q is even there are - so far - only fragmentary results. For a group which admits generic polynomials it is often quite cumbersome to find them explicitly. Here are some examples.

The construction in the proof that a positive answer to (NP) for a group G implies the existence of a G-generic polynomial usually leads to complicated polynomials with more parameters than necessary. For instance, for S_3 and the cyclic group of order 3 one would get 3 parameters. By alternative methods one gets much simpler generic polynomials with just one parameter. Indeed, x^3+tx+t is generic for S_3 and $x^3-tx^2+(t-3)x+1$ is generic for the cyclic group of order 3. (See e.g. [Se] pp. 1-2 or [JLY], p. 30.) For the cyclic group of order 5 there exists a generic polynomial with 2 parameters and it can be shown that there is no generic polynomial with only one parameter.

Both the condition that (NP) has a positive solution for G and the condition that there exists a G-generic polynomial are quite strong. There is a weaker condition that is almost as good and for which no group is known for which it does not hold.

Definition. Let $t_1,\dots,t_n$ be indeterminates and G a finite group. A G-extension M of $\mathbb{Q}(t_1,\dots,t_n)$ is called *regular* if $\mathbb{Q}$ is relatively algebraically closed in M, i.e. if no element in $M\setminus\mathbb{Q}$ is algebraic over $\mathbb{Q}$. We often say that M is a regular G-extension over $\mathbb{Q}$.

The existence of a G-generic polynomial implies the existence of a regular G-extension:

Theorem 6.2. *Let $f(t_1,\dots,t_n,x)\in\mathbb{Q}(t_1,\dots,t_n)[x]$ be a G-generic polynomial. Then the splitting field of $f(t_1,\dots,t_n)(x)$ over $\mathbb{Q}(t_1,\dots,t_n)$ is a regular G-extension over $\mathbb{Q}$.*

We omit the proof. Hence for a finite group G we have the following implications:

(NP) has a positive answer for G $\Rightarrow$ there exists a G-generic polynomial $\Rightarrow$ there exists a G-regular extension over $\mathbb{Q}$ $\Rightarrow$ there exists a G-extension of $\mathbb{Q}$.

Here the first two implications are strict: there exists a generic polynomial for the cyclic group C_{47} of order 47, but Noethers problem has a negative answer for C_{47}. Furthermore for the cyclic group C_8 of order 8, there exists a regular C_8-extension of $\mathbb{Q}$, but (by theorem 6.1) no generic C_8-polynomial. It is an open question whether the third implication can be reversed: There is a conjecture that this implication actually is an equivalence. The following two theorems are stability results for regular extensions.

Theorem 6.3. *If G is a finite group for which there is a regular G-extension over $\mathbb{Q}$, then for an arbitrary field K there exists a regular G-extension over K, i.e. there exists a G-extension M of a rational function field $K(t_1,\dots,t_n)$ such that K is relatively algebraically closed in M.*

Theorem 6.4. *If G and H are finite groups such that there exists a G-regular extension and an H-regular extension of $\mathbb{Q}$, then there also exists a $(G\times H)$-regular extension of $\mathbb{Q}$.*

Remark. Theorem 5.1 and theorem 3.2 (with $\mathbb{Q}$ replaced by a Hilbertian field) show that if a group G can be realized as Galois group for a regular extension over $\mathbb{Q}$ then G can be realized as a Galois group over any Hilbertian field.

Theorem 5.4 implies that if G and H are finite groups such that there exist regular G- and regular H-extensions over $\mathbb{Q}$, then there exists a regular $(G \times H)$-extension over $\mathbb{Q}$, in particular $G \times H$ is realizable as a Galois group over $\mathbb{Q}$ (Cf. also the remark after theorem 1.1.) Combining the above results it follows that for a finite group G the existence of a G-regular extension over $\mathbb{Q}$ implies the existence of infinitely many distinct G-extensions of any Hilbertian field. Therefore, the existence of a regular G-extension of $\mathbb{Q}$ yields considerably more information than the existence of just a G-extension does. It is known that every finite abelian group is realizable as Galois group for regular extension of $\mathbb{Q}$. So are many dihedral groups, for instance, the dihedral group D_q of order $2q$ for every odd q. However, it is still unknown whether every finite solvable group can appear as Galois group for a regular extension over $\mathbb{Q}$, in particular, it is unknown if every finite solvable group is realizable as Galois group over every Hilbertian field. Clearly every symmetric group S_n is realizable as Galois group of regular extension over $\mathbb{Q}$. So is every alternating group A_n. Indeed, the splitting field over $\mathbb{Q}(t)$ for the polynomial $P_n(t, x)$ in section 3 is a regular A_n-extension of $\mathbb{Q}(t)$.

In the last decades large classes of linear groups and non-abelian simple groups have been realized as Galois groups of regular extensions over $\mathbb{Q}$. We briefly recall the definitions. For a commutative ring R the special linear group $SL_n(R)$ of degree n is the group of all $(n \times n)$ matrices with entries in R having determinant 1. The projective special linear group $PSL_n(R)$ of degree n is the quotient of $SL_n(R)$ with respect to its centre. If R is a field it is a classical result that $PSL_n(R)$ is a non-abelian simple group except for the case where $n = 2$ and R is a field with 2 or 3 elements. By arithmetic-geometric methods, e.g. by use of elliptic curves and modular forms, several of the above groups (for $n = 2$) have been realized as Galois groups of regular extensions of $\mathbb{Q}$. To give just one example, Shih [Shi] proved in 1974 that $PSL_2(\mathbb{F}_p)$[1] is realizable as Galois group for a regular extension of $\mathbb{Q}$ provided p is a prime number for which 2, 3 or 7 is a quadratic non-residue modulo p.

It is well known that every finite group is realizable as a Galois group of the splitting field over $\overline{\mathbb{Q}}(t)$ for a polynomial with coefficients in $\overline{\mathbb{Q}}(t)$ where $\overline{\mathbb{Q}}$ is the field of all algebraic numbers. The problem is to obtain conditions which ensure that the polynomial can be defined over $\mathbb{Q}$. Certain very technical "rigidity" conditions on the group G imply that G can be realized as Galois group of a regular extensions of $\mathbb{Q}(t)$. A large class of simple groups can in this way be realized as Galois groups of a regular extension of $\mathbb{Q}(t)$, for instance all the sporadic simple groups except the Mathieu group M_{23}, (but including the monster group!) and many classical groups of Lie type and some exceptional groups of Lie type. For a full account of these results we refer to the monograph [MM].

[1] If p is a prime number $\mathbb{F}_{p^n}$ denotes the field with p^n elements

7 Explicit examples

The previous sections mainly dealt with the mere existence of polynomials whose splitting fields had some prescribed Galois groups. Hilbert proved that all symmetric groups S_n and all alternating groups A_n can be realized as Galois groups over $\mathbb{Q}$. However, he gave no explicit numerical examples. Issai Schur (1930-31)[Scu] gave some explicit examples. The Galois group of the splitting field over $\mathbb{Q}$ for the n-th Laguerre polynomial

$$L_n(x) = \frac{e^x}{n!}\frac{d^n(x^n e^{-x})}{dx^n} = 1 - \binom{n}{1}\frac{x}{1!} + \binom{n}{2}\frac{x^2}{2!} - \cdots + (-1)^n\frac{x^n}{n!}$$

is the symmetric group S_n. He also proved that the Galois group of the splitting field over $\mathbb{Q}$ for the polynomial

$$E_n(x) = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$$

is A_n for $n \equiv 0 \bmod 4$ and S_n for $n \not\equiv 0 \bmod 4$.

In some sense "most" polynomials of degree n in $\mathbb{Q}[x]$ have S_n as Galois group. To be more precise: let $g(n,t)$ be the number of monic polynomials in $\mathbb{Z}[x]$ of degree n such that the absolute value of each coefficient is $\leqq t$. Let $h(n,t)$ be the number of the above polynomials whose Galois group over $\mathbb{Q}$ is S_n. By a famous result of van der Waerden[Wa] the quotient $h(n,t)/g(n,t)$ converges to 1 as $t \to \infty$. So to realize that the Galois group of some polynomial is a symmetric group, is from a "statistical" point of view not surprising, but the actual verification may require some effort. The simplest example of a polynomial of degree n such that the Galois group over $\mathbb{Q}$ - for every n - is S_n is $x^n - x - 1$. The proof that this holds for all n depends on non-trivial results from algebraic number theory.

As mentioned in section 6 Shih[Shi] proved in 1974 that $PSL_2(\mathbb{F}_p)$ is realizable as the Galois group of a regular extension of $\mathbb{Q}$ if 2, 3 or 7 is a quadratic non-residue modulo p. This, in particular, applies to $PSL_2(\mathbb{F}_7)$. This group has order 168 and is the smallest simple group which is neither cyclic nor an alternating group. Until 1970 $PSL_2(\mathbb{F}_7)$ was the smallest simple group that has not been realized as a Galois group over $\mathbb{Q}$. In the search for a septimic polynomial with this group as a Galois group mathematicians from Karlsruhe University applied a "trial and error" method, i.e. thousands of septimic polynomials were computer tested and finally the polynomial $T(x) = x^7 - 3x + 7$ was found to be a good candidate: it is irreducible, has exactly 3 real roots and the discriminant is the square of rational number. Hence from knowledge of the transitive subgroups of S_7 it follows that the Galois group of $T(x)$ is either the alternating group A_7 or $PSL(2,\mathbb{F}_7)$. But it was then a hard task to rule out A_7, before $PSL(2,\mathbb{F}_7)$ was proved to be the Galois group of $T(x)$ over $\mathbb{Q}$. To-day computer programs have been developed which in a few seconds can compute Galois groups of irreducible polynomials over $\mathbb{Q}$ of degree $\leqq 11$.

For an irreducible polynomial $p(x) \in \mathbb{Q}[x]$ the Galois permutation group over $\mathbb{Q}$ is a transitive subgroup of S_n (cf. theorem 1.2). This group is determined up to

conjugacy. The transitive subgroups of S_n, $n \leqq 12$, have been classified up to conjugacy. All these groups appear as permutation Galois groups of *explicitly known* polynomials in $\mathbb{Q}[x]$. A complete list of these polynomials can be found in [MM]. At the moment it is difficult to say which is the smallest group that so far has not been realized as Galois group over $\mathbb{Q}$. But it *seems* that it might be a certain extension of the group $PSL_2(\mathbb{F}_{16})$ of degree 2, which has order 8160.

8 Concluding Remarks

If K is a field such that every finite group is realizable as a Galois group over K then it is easy to see that every finite group is realizable as a Galois group over any finite field extension L of K. (Use e.g. theorem 1.3 and proposition 2.2.) In particular, if the inverse problem of Galois theory has a positive solution, then every finite group appears as a Galois group over every algebraic number field of finite degree.

However, there exists a finite field extension L/K such that every finite group is a Galois group over L but not every finite group is a Galois group over K. An amusing example of this phenomenon is due to Florian Pop [Po]. Recall that an algebraic number α is called totally real, if α and all its conjugates are real, in other words, if all the roots of α´s minimal polynomial over $\mathbb{Q}$ are real. The totally real algebraic numbers form a subfield $\mathbb{Q}_{tr}$ of the field, $\overline{\mathbb{Q}}$ of all algebraic numbers. Not every finite group is realizable as a Galois group over $\mathbb{Q}_{tr}$, for instance no group of odd order (> 1) is realizable; more precisely, the only groups that are realizable as Galois groups over $\mathbb{Q}_{tr}$ are the groups which can be generated by involutions (i.e. the elements of order 2). However, over the field $\mathbb{Q}_{tr}(\sqrt{-1})$, which has degree 2 over $\mathbb{Q}_{tr}$, every finite group is realizable as a Galois group!

Taking into account that the finite simple groups are the building blocks for all finite groups the natural strategy concerning the inverse problem of Galois theory has been to start by realizing the simple groups as Galois groups and then gradually building up bigger Galois extensions. So far many simple groups have been realized as Galois groups over $\mathbb{Q}$. One might think that if a large family of simple groups have been realized as Galois groups over $\mathbb{Q}$ then the remaining simple groups would follow automatically. But this is not the case. Indeed, if we divide the family of finite simple groups arbitrarily into disjoint classes $\mathcal{A}$ and $\mathcal{B}$, then there exists a field K such that every group in $\mathcal{A}$ is realizable as a Galois group over K while no group in $\mathcal{B}$ is. Similarly, even if one had realized all finite simple groups as Galois groups over $\mathbb{Q}$ the remaining finite groups would not follow automatically. Actually, even "worse" things can happen. By the length of a finite group G we mean the length of one (and then of any) composition series of G. Then for any positive integer t there exists a field K_t such that every group of length $\leqq t$ appears as a Galois group over K_t, but there exists a group of length $t+1$ that does not appear a Galois group over K_t. So roughly speaking there is no easy short cut to the solution of the inverse problem of Galois theory.

References

[FK] E. Fried& J. Kollár,*Automorphism groups of Algebraic Number Fields*, Math.Z. **163** (1978), 121-123.

[Fu] Ph. Furtwängler, *Über Minimalbasen für Körper rationaler Funktionen*, S.B.Akad. Wiss.Wien **134**(1925),69-80.

[Ge] W.-D. Geyer, *Jede endliche Gruppe ist Automorphismengruppe einer endlichen Erweiterung $K/\mathbb{Q}$*, Arch.Math.(Basel),**41**(1983),139-142.

[Ha] C.R.Hadlock, *Field Theory and its classical Problems*, Carus Mathematical monographs 19, Mathematical Association of America, 1978.

[Hi] D. Hilbert,*Über die Irreducibilität ganzer rationalen Funktionen mit ganzzahligen Coefficienten*,J.reine Angew. Math.**110** (1892),104-129.

[JLY] C. U.Jensen, A.Ledet & N. Yui,*Generic Polynomials.Constructive Aspects of the inverse Galois Problem*, Mathematical Sciences Research Institute Publications, 45, Cambridge University Press, 2002.

[Le] H. W. Lenstra, *Rational Functions invariant under a finite abelian Group*, Invent.Math. **25**(1974), 299-325.

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

[NSW] J. Neukirch, A.Schmidt & K.Wingberg, *Cohomology of Number Fields*, Grundlehren der Mathematischen Wissenschaften 323, Springer-Verlag, 2000.

[Po] H. Pop, *Embedding Problems over large Fields*, Ann.of Math. **144**(1996),1-34.

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

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

[Scu] I. Schur, *Gleichungen ohne Affekt*, Gesammelte Abhandlungen, Vol. III, nr. 67,(1930), 191 -197.

[Se] J.-P.Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Jones & Bartlett, 1992.

[Sha] I. R. Shafarevich,*Construction of Fields with given solvable Galois group*, Izv.

[Shi] K.-Y. Shih, *On the Construction of Galois Extensions of Function Fields and Number Fields*, Math.Ann.**207**(1974),99-120.

[Sw] R.G.Swan, *Invariant rational Functions and a Problem of Steenrod*, Invent.Math. **7**(1969), 148-158.

[Vo] V. E. Voskresenskii, *On the question of the structure of the subfield of invariants of a cyclic group of automorphisms of the field $\mathbb{Q}(x_1, \ldots, x_n)$*, Izv. Akad.Nauk SSSR, Ser.Mat.(1970), 366-375.

[Wa] B.L.van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math.Ann.**109** (1933), 13-16.