J. Appl. Math. & Informatics Vol. **40***(2022), No. 3 - 4, pp. 765 - 767*
https://doi.org/10.14317/jami.2022.765

THE INVERSE GALOIS PROBLEM

ŁUKASZ MATYSIAK

Abstract. The inverse Galois problem concerns whether or not every finite group appears as the Galois group of some Galois extension of the rational numbers. This problem, first posed in the early 19th century, is unsolved. In other words, we consider a pair - the group G and the field K. The question is whether there is an extension field L of K such that G is the Galois group of L. In this paper we present the proof that any group G is a Galois group of any field extension. In other words, we only consider the group G. And we present the solution to the inverse Galois problem.

AMS Mathematics Subject Classification : 12F12, 11S20.
Key words and phrases : Field extension, finite group, Galois group, inverse Galois problem.

1. Introduction

Some specific field extensions $K \subset L$ are classified as Galois extensions (separable and normal). We call the group of automorphism of such $K \subset L$ the Galois group of $K \subset L$. The inverse Galois problem asks the question whether every finite group is isomorphic to the Galois group of a Galois extension of rational numbers $\mathbb{Q}$.

In this section we discuss some historical (and some modern) results concerning the Inverse Galois Problem. In Galois theory we see many familiar groups arise as automorphism groups of a field L that fix some subfield $K \subset L$. The Inverse Galois problem is concerned with classifying which finite groups can be realized as such automorphism groups. There has been cosiderable progress made on this question when we take the base field K to be $\mathbb{Q}$.

In the 1800's it was shown that the Inverse Galois problem holds for all finite abelian groups ([4]).

Received October 21, 2021. Revised February 18, 2022. Accepted February 24, 2022.

In 1937 Scholz and Reichardt proved that all odd p-groups can be realized as the Galois group of some number field over $\mathbb{Q}$. The proof involved solving special central embedding problems of the form

$$1 \to \mathbb{Z}/p\mathbb{Z} \to \overline{G} \to G \to 1,$$

where G is the Galois group of some number field L over $\mathbb{Q}$, $\mathbb{Z}/p\mathbb{Z}$ is the Galois group of the algebraic closure of L ($\overline{L}$) over L, and, $\overline{G}$ is the Galois group of $\overline{L}$ over $\mathbb{Q}$.

In 1954 Shafarevich showed that every solvable group is a Galois group over $\mathbb{Q}$. There was a flaw pointed out in this proof in 1989, but it was resolved by Shafarevich in the same year ([1], [3]).

The question is still open for non-solvable groups. However, many specific examples of non-solvable groups are known to occur as Galois groups over $\mathbb{Q}$ (ex. all A_n and S_n. This follows by Hilbert's irreducibility theorem which states that if a group G can be recognized as a Galois group of an extension of $\mathbb{Q}(t)$ with basefield $\mathbb{Q}(t)$, then G can also be recognized as a Galois group of a number field over $\mathbb{Q}$.)

For simple groups we know that A_n, $\mathbb{Z}/p\mathbb{Z}$, and 25 of the 26 sporadic simple groups occur as Galois groups over $\mathbb{Q}$. The question of whether simple Lie type groups and/or the last sporadic group M_{23} occur as Galois groups over $\mathbb{Q}$ is still open.

In [2] Dugas and Göbel show that all infinite groups are Galois groups over any field.

2. Main results

Let's start from the following Lemma.

Lemma 2.1. *Let K be a field and G be a finite group of field automorphism of K, then K is a Galois extension of the fixed field K^G with Galois group G, moreover $[K\colon K^G] = |G|$.*

Proof. Pick any $\alpha \in K$ and consider a maximal subset $\{\sigma_1, \ldots, \sigma_n\} \subseteq G$ for which all $\sigma_i\alpha$ are distinct. Now any $\tau \in G$ must permute the $\sigma_i\alpha$ as it is an automorphism and if some $\tau\sigma_i\alpha \neq \sigma_j\alpha$ for all j then we could extend our set of σs by adding this $\tau\sigma_i$.

So α is a root of

$$f_\alpha(X) = \prod_{i=1}^{n}(X - \sigma_i\alpha),$$

note that f_α is fixed by τ by the above. So all the coefficients of f_α are in K^G. By construction f_α is a separable polynomial as the $\sigma_i\alpha$ were chosen distinct, note that f_α also splits into linear factors in K.

The above was for arbitrary $\alpha \in K$ so we have hust shown directly that K is a separable and normal extension of K^G, which is the definition of Galois extension. As every element of K^G is a root of polynomial of degree n we cannot have the extension degree $[K\colon K^G] > n$. But we also have a group of n automorphisms of K that fix K^G so $[K\colon K^G] \geqslant n$ and hence $[K\colon K^G] = n$. □

Theorem 2.2. *Every finite group is a Galois group.*

Proof. Let K be an arbitrary field, G any finite group. Now take $L = K(g'\colon g \in G)$ (i.e. adjoin all elements of G to K as indeterminates, denoted by g'). Now we have a natural action of G on L defined via $h \cdot g' = (hg)'$ and extending K-linearly. Now L and G satisfy Lemma 2.1 and hence $L^G \subset L$ is a Galois extension with Galois group G. □

From Theorem 2.2 we have a Corollary that is commonly known as the Inverse Galois Problem.

Corollary 2.3. *Every finite group is the Galois of Galois extension of* $\mathbb{Q}$.

Proof. It is enough take $K = \mathbb{Q}$. From proof of Theorem 2.2 we have $L^G = \mathbb{Q}$. □

Later a generalization of the Inverse Galois Problem arose, where instead $\mathbb{Q}$ we take any field K. Unfortunately, such a fact does not follow from the proof, because in general the equality $L^G = K$ not holds.

References

1. I.R. Shafarevich, *Construction of fields of algebraic numbers with given solvable Galois group*, Izv. Akad. Nauk SSSR. Ser. Mat. **18** (1954), 525–578.
2. M. Dugas, R. Göbel, *All infinite groups are Galois groups over any field*, Transactions of the American Mathematical Society, **304** (1987).
3. I.R. Shafarevich, *Factors of decreasing central series*, Mat. Zametki (in Russian) **45** (1987), 114–117.
4. H.G.J. Tiesinga, *The inverse Galois problem*, Bachelor Project Mathematics, University of Groningen, 2016.

Łukasz Matysiak received M.Sc. from Kazimierz Wielki University and Ph.D. at Nicolaus Copernicus University. Since 2019 he has been at Kazimierz Wielki University. His research interests include commutative algebra (composites), cryptology, Galois theory, number theory.

Institute of Mathematics, Kazimierz Wielki University, Bydgoszcz 85-090, Poland.
e-mail: lukmat@ukw.edu.pl