The Inverse Galois Problem

Alissa Furet

Dalhousie University
February 9^{th}, 2022

DEFINITIONS

Galois Extension

An algebraic extension $\mathbb{F} \subset \mathbb{E}$ is Galois if it is splitting and separable.

Galois Group

If $\mathbb{F} \subset \mathbb{E}$ is galois, then $\mathrm{Aut}(\mathbb{E} / \mathbb{F})$ is the Galois group of $\mathbb{F} \subset \mathbb{E}$.

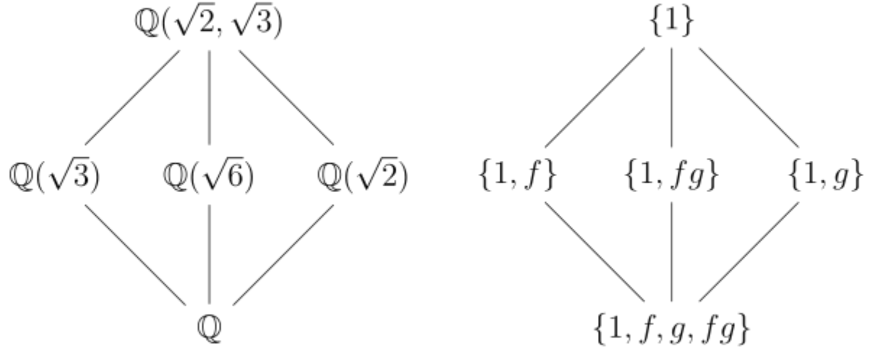
Where

$$\mathrm{Aut}(\mathbb{E} / \mathbb{F}) = \{ \text{ all automorphisms } \alpha : \mathbb{E} \to \mathbb{E} \text{ such that } \alpha(x) = x \;\; \forall x \in \mathbb{F} \}$$

MOTIVATION

Galois Theory

Provides a connection between field theory and group theory



We can reduce certain problems in field theory to group theory, which is often simpler.

Fields ⇒ Groups

What about going the other direction?

Groups ⇒ Fields

The Inverse Galois Problem

SOLVED

Is every finite group the Galois group of some Galois extension?

UNSOLVED

Is every finite group the Galois group of some Galois extension of the rational numbers $\mathbb{Q}$?

Is every finite group G the Galois group of some Galois extension?

$G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ for some extension $\mathbb{F} \subset \mathbb{E}$

YES!

Let's construct a Galois extension $\mathbb{F} \subset \mathbb{E}$ for an arbitrary finite group G such that G = Gal($\mathbb{E}/\mathbb{F}$)

Lemma 1

Every finite group is contained in S_p for a large enough prime p where S_p is the symmetric group over p elements.

Lemma 2

Every irreducible polynomial in $\mathbb{Q}[x]$ of degree p having exactly p - 2 real roots has S_p as a Galois group over $\mathbb{Q}$.

Lemma 3

For any positive integer n, there is an irreducible polynomial in $\mathbb{Q}[x]$ of degree n having exactly n - 2 real roots.

Back to our problem

Let’s find some extension $\mathbb{F} \subset \mathbb{E}$ such that

$$G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$$

for some arbitrary finite group G.

Proof

Let G be a finite group of order n.

Embed G in S_p . (Lemma 1)

Let f be an irreducible polynomial in $\mathbb{Q}[x]$ of degree p with exactly p - 2 roots. (Lemma 3)

Let $\mathbb{E}$ be the splitting field of f over $\mathbb{Q}$. Then $\mathbb{E}$ has Galois group S_p over $\mathbb{Q}$. (Lemma 2)

Let $\mathbb{F} = \mathbb{E}^G$, the fixed field of G.

Conclusion

By the Fundamental Theorem of Galois Theory,

$$\mathbb{F} = \mathbb{E}^G \subset \mathbb{E} \text{ is a Galois extension with Galois group } G \leq S_p$$

$$G = \mathrm{Gal}(\mathbb{E}/\mathbb{F})$$

Can we just extend this proof to $\mathbb{F} = \mathbb{Q}$?

No!

If $\mathbb{F} = \mathbb{Q}$, then

$$\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = S_p \neq G$$

This is an <u>example</u> of a finite group being the Galois group of some Galois extension of the rational numbers $\mathbb{Q}$.

$\longrightarrow$ does not hold for any arbitrary finite group G

Is every finite group G the Galois group of some Galois extension of the rational numbers $\mathbb{Q}$?

$G = \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ for some extension $\mathbb{Q} \subset \mathbb{E}$

This problem, first posed in the 19th century, is **unsolved**.

We can derive some partial results.

First approach

Hilbert (1892)

Used the Irreducibility Theorem to show:

There exists infinitely many Galois extensions $\mathbb{Q} \subset \mathbb{E}$ and $\mathbb{Q}[x_1, \dots, x_n] \subset \mathbb{E}$ with Galois groups corresponding to the <u>symmetric</u> S_n or <u>alternating</u> group A_n .

Cyclic groups

Let’s construct a Galois extension $\mathbb{Q} \subset \mathbb{E}$ for $\mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{R}$,

such that $\mathbb{Z}/n\mathbb{Z} = \mathrm{Gal}(\mathbb{E}/\mathbb{Q})$

Cyclotomic Extensions

(Dummit and Foote, 13.4)

Useful definitions.

A primitive p^{th} root of unity, μ, is any complex number that yields 1 when raised to some positive integer power p

$$\mathbb{Z}/p\mathbb{Z} \cong \mu_p$$

Choose a prime p such that $p \equiv 1 \pmod{n}$ (Dirichlet's Theorem)

Let $\mathbb{Q}(\mu)$ be the subfield of $\mathbb{Q}$ generated by μ, a primitive p^{th} root of unity.

Then $\mathbb{Q}(\mu)$ is the splitting field for $f(x) = x^p - 1$ over $\mathbb{Q}$

So, $Gal(\mathbb{Q}(\mu)/\mathbb{Q})$ is cyclic of order $p - 1$

Let $H \subset \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})$ be a cyclic subgroup of order $(p - 1) / n$

By the Fundamental Theorem of Galois Theory,

$\mathbb{Q} \subset \mathbb{Q}(\mu)^H$ is a Galois extension with Galois group $\mathbb{Z}/n\mathbb{Z}$

$$\mathbb{Z}/n\mathbb{Z} = \mathrm{Gal}(\mathbb{Q}(\mu)^H/\mathbb{Q})$$

Finite abelian groups

Theorem

Every finite abelian group A is isomorphic to the Galois group Gal($\mathbb{E}/\mathbb{Q}$) for some Galois extension $\mathbb{Q} \subset \mathbb{E}$.

We’ve constructed the Galois extension $\mathbb{Q}(\mu)^H \subset \mathbb{Q}$ such that $\mathbb{Z}/n\mathbb{Z} = \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}(\mu)^H)$.

There exist an abelian group $A \cong \mathrm{Gal}(\mathbb{Q}(\mu)^H/\mathbb{Q})$.

→ This method can be extended to abelian groups

Worked Example: $n = 3$

Choose $p = 7$ such that $7 \equiv 1 \pmod 3$ (Dirichlet's Theorem)

Let $\mathbb{Q}(\mu)$ be the subfield of $\mathbb{Q}$ generated by μ, a primitive 7^{th} root of unity.

Then $\mathbb{Q}(\mu)$ is the splitting field for $f(x) = x^7 - 1$ over $\mathbb{Q}$

So, $\mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})$ is cyclic of order $7 - 1 = 6$

Let $H \subset \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q})$ be a cyclic subgroup of order (7 - 1)/3 = 3.

Let $H = \{ 1, \eta^3 \}$, where η is the generator of H which sends $\mu \mapsto \mu^3$.

By the Fundamental Theorem of Galois Theory,

$\mathbb{Q}(\mu)^H \subset \mathbb{Q}$ is a Galois extension with Galois group $\mathbb{Z}/3\mathbb{Z}$

$$\mathbb{Z}/3\mathbb{Z} = \mathrm{Gal}(\mathbb{Q}/\mathbb{Q}(\mu)^H)$$

SUMMARY

<table>
<tr><th>SOLVED</th><th>UNSOLVED</th></tr>
<tr><td>Is every finite group the Galois group of some Galois extension?</td><td>Is every finite group the Galois group of some Galois extension of the rational numbers $\mathbb{Q}$?</td></tr>
<tr><td rowspan="4">We constructed a Galois extension $\mathbb{E}^G \subset \mathbb{E}$ for an arbitrary finite group G such that $G = \mathrm{Gal}(\mathbb{E}/\mathbb{E}^G)$ by embedding G into S_p</td><td>Symmetric group</td></tr>
<tr><td>Alternating group</td></tr>
<tr><td>Cyclic groups</td></tr>
<tr><td>Abelian Groups</td></tr>
</table>

References

- Dummit, D. S., & Foote, R. M. (2004). *Abstract algebra*. John Wiley & Sons.
- Hungerford, T. W. (1980). *Algebra*. Springer.
- Malle, G., & Matzat, B. H. (1999). *Inverse galois theory*. Springer.
- Wikimedia Foundation. (2021, November 14). *Inverse galois problem*. Wikipedia. Retrieved February 1, 2022, from https://en.wikipedia.org/wiki/Inverse_Galois_problem
- Wikimedia Foundation. (2022, January 15). *Dirichlet's theorem on arithmetic progressions*. Wikipedia. Retrieved February 1, 2022, from https://en.wikipedia.org/wiki/Dirichlet%27s_theorem_on_arithmetic_progressions
- M TurgeonM Turgeon 9, Qiaochu YuanQiaochu Yuan 355k4141 gold badges758758 silver badges11291129 bronze badges, & ViperRobKViperRobK 15511 silver badge44 bronze badges. (1960, August 1). *Is every Group A Galois group?* Mathematics Stack Exchange. Retrieved February 1, 2022, from https://math.stackexchange.com/questions/188882/is-every-group-a-galois-group
- *My brain is open*. Every finite group is a Galois group · My Brain is Open. (n.d.). Retrieved February 1, 2022, from https://alexjbest.github.io/blog/maths/2017/05/02/every-group-is-a-galois-group.html
- user140776user140776 1, & Qiaochu YuanQiaochu Yuan 355k4141 gold badges758758 silver badges11291129 bronze badges. (1964, May 1). *Every finite group is isomorphic to the Galois group of some polynomial*. Mathematics Stack Exchange. Retrieved February 1, 2022, from https://math.stackexchange.com/questions/1778949/every-finite-group-is-isomorphic-to-the-galois-group-of-some-polynomial
- Zywina, D. (2015). The inverse Galois problem for PSL2(FP). *Duke Mathematical Journal*, *164*(12). https://doi.org/10.1215/00127094-3129271
- *The inverse Galois problem*. (n.d.). Retrieved February 1, 2022, from https://fse.studenttheses.ub.rug.nl/14148/1/thesisclassic.pdf

Thank you!

Alissa Furet

Dalhousie University
February 9th, 2022