Inverse Galois Problem

Travor Liu, Ruiyang Tang, Siyu Liu

Department of Mathematics
University College London

9 Dec 2024

Table of Contents

Introduction

The inverse Galois problem (IGP) asks whether every finite group occurs as the Galois group of some extension over a particular field.

Definition

Let G be a finite group and K be a field. G is said to be **realizable over** K if there exists some Galois extension L/K for which $G \cong \mathrm{Gal}(L/K)$.

IGP over $\mathbb{Q}$ is an open problem in general, and so we will discuss in details only a few special cases.

Table of Contents

Cyclotomic Extensions

Definition

Let ζ_n be a primitive n-th root of unity. Then $\mathbb{Q}(\zeta_n)$ is the n-th **cyclotomic extension** of $\mathbb{Q}$.

Recall that ζ_n is a primitive n-th root of unity iff

$$\zeta_n = (e^{\frac{2\pi i}{n}})^j \text{ and } \gcd(j, n) = 1.$$

WLOG, let $\zeta_n = e^{\frac{2\pi i}{n}}$. Then:

Proposition

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a Galois extension.

Proof: Notice that $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1 = \prod_{j=1}^{n}(x - \zeta_n^j)$ over $\mathbb{Q}$, so it is separable over $\mathbb{Q}$. $\square$

Cyclotomic Polynomials

Definition

The n-th **cyclotomic polynomial** is

$$\Phi_n(x) = \prod_{\substack{1\le j\le n \\ \gcd(j,n)=1}} (x - \zeta_n^j).$$

Proposition

For all $n \in \mathbb{N}$, $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$.

Proof: Observe that $x^n - 1 = \prod_{d|n} \Phi_d(x)$. By induction and Gauss's lemma, we obtain the desired result. □

Preparation for Proof of the Irreducibility of Φ_n

Theorem (Fermat's Little Theorem)

If p is a prime and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod{p}$.

Theorem (Freshman's dream)

Let R be a commutative ring with prime characteristic p. Then for all $a_1, \ldots, a_m \in R$, we have $\left(\sum_{i=1}^m a_i\right)^p = \sum_{i=1}^m a_i^p$.

Proof: When $m = 2$, we use the binomial theorem to expand $(a_1 + a_2)^p$, and we note that when $s \in \{1, \ldots, p-1\}$, p divides the binomial coefficient $\binom{p}{s}$. The general case follows by induction. □

Preparation for Proof of the Irreducibility of Φ_n (Continued)

Theorem

For any polynomial $f(x) \in \mathbb{F}_p[x]$, we have $f(x^p) = [f(x)]^p$.

Proof: Let $f(x) = \sum_{i=0}^m a_i x^i$. Then

$$[f(x)]^p = \left[\sum_{i=0}^m a_i x^i\right]^p \overset{\text{(i)}}{=} \sum_{i=0}^m a_i^p x^{ip} \overset{\text{(ii)}}{=} \sum_{i=0}^m a_i x^{ip} = f(x^p),$$

where (i) is due to Freshman's dream, and in (ii) we use Fermat's little theorem to conclude that $a_i = a_i^p$ in $\mathbb{F}_p[x]$. $\square$

Sketch Proof of the Irreducibility of Φ_n

Theorem

$\Phi_n(x)$ is irreducible over $\mathbb{Q}$ and $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_n(x)) = \varphi(n)$.

1. Let $p \nmid n$ be a prime and $\Phi_n(x) = m(x)h(x)$, where $m(x) = m_{\zeta_n,\mathbb{Q}}(x)$. Then $\Phi_n(\zeta_n^p) = 0 \implies m(\zeta_n^p) = 0 \vee h(\zeta_n^p) = 0$.
2. Assume $h(\zeta_n^p) = 0$, so $m(x) \mid h(x^p)$.
3. Choose $m_1(x) \mid \overline{m}(x)$ irreducible over $\mathbb{F}_p$, so $m_1(x) \mid \overline{m}(x) \implies m_1(x) \mid \overline{h}(x^p) = [\overline{h}(x)]^p$. Since $\overline{\Phi}(x) = \overline{m}(x)\overline{h}(x)$, $[m_1(x)]^2 \mid \overline{\Phi}(x)$ thus $x^n - 1$ is not separable.
4. Note $\frac{\mathrm{d}}{\mathrm{d}x}(x^n - 1) = nx^{n-1} \neq 0$, the separability of $x^n - 1$ in $\mathbb{F}_p[x]$ is ensured, therefore contradiction reached. We conclude that $m(\zeta_n^p) = 0 \implies m(\zeta_n^j) = 0 \forall j$ coprime to n.
5. Therefore $\Phi_n(x) \mid m(x)$, and by assumption $m(x) \mid \Phi_n(x)$, $m(x) = \Phi_n(x)$. So $\Phi_n(x)$ is the minimal polynimal of ζ_n. □

Galois Group of Cyclotomic Extensions

Proposition

$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*$.

Proof: Since each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ permutes the roots of $\Phi_n(x)$,

$$\sigma(\zeta_n) = \zeta_n^j, \quad \gcd(j, n) = 1.$$

Define the map $f : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ by

$$f : (\sigma : \zeta_n \mapsto \zeta_n^j) \mapsto j,$$

which is an isomorphism. $\square$

IGP for Cyclic Groups over $\mathbb{Q}$

Let $n \in \mathbb{N}$. We want to find $\mathbb{Q} \subseteq L \subseteq \mathbb{C}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong C_n$.

1. If $n+1$ is a prime p, $(\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1} = C_n$. Let $\zeta_p = e^{\frac{2\pi i}{p}}$,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^*.$$

2. If $n+1$ is not a prime, we need:

Theorem (Dirichlet's theorem on arithmetic progressions)

Let $a, m \in \mathbb{Z}$ be coprime. Then $\exists$ infinitely many primes $\equiv a \pmod{m}$.

See proof in MATH0083; it uses analytic number theory.

IGP for Cyclic Groups over $\mathbb{Q}$ (Continued)

Therefore, for any n, choose a prime p with $p \equiv 1 \pmod{n}$.

Proposition

If $n \mid p-1$, then $C_n \leq C_{p-1}$ and $C_n \cong C_{p-1}/C_{(p-1)/n}$.

By the fundamental theorem of Galois theory, there exists $\mathbb{Q} \subseteq L \subseteq \mathbb{Q}(\zeta_p)$ fixed by $C_{(p-1)/n}$, so

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \frac{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/L)} \cong \frac{C_{p-1}}{C_{(p-1)/n}} \cong C_n. \square$$

Thus, the IGP over $\mathbb{Q}$ is solved in the cyclic case.

Lemma A for IGP for Abelian Groups over $\mathbb{Q}$

Lemma (A)

Every finite Abelian group M is a direct product of cyclic groups. That is, there exist $q_1, \ldots, q_m \in \mathbb{N}$ such that $M \cong \prod_{i=1}^{m} C_{q_i}$.

Proof: This is an immediate corollary of the fundamental theorem of finitely generated modules over PIDs. □

Lemma B for IGP for Abelian Groups over $\mathbb{Q}$

Lemma (B)

Let $n_1, \ldots, n_k \in \mathbb{N}$ be pairwise coprime; then we have $(\mathbb{Z}/n_1 \ldots n_k\mathbb{Z})^* \cong \prod_{i=1}^k (\mathbb{Z}/n_i\mathbb{Z})^*$.

Proof: 1) The CRT gives a natural isomorphism $\mathbb{Z}/n_1 \ldots n_k\mathbb{Z} \cong \prod_{i=1}^k \mathbb{Z}/n_i\mathbb{Z}$.

2) $\left(\prod_{i=1}^k R_i\right)^* = \prod_{i=1}^k R_i^*$ holds for any rings $R_1, \ldots, R_k$. □

Theorem (Chinese remainder theorem)

Let $n_1, \ldots, n_k \in \mathbb{N}$ be pairwise coprime. Then the system of congruences

$$x \equiv a_i \pmod{n_i}, \quad i = 1, \ldots, k$$

has a unique solution modulo $n_1 \cdots n_k$.

IGP for Abelian Groups over $\mathbb{Q}$ - Proof

Let $M = \prod_{i=1}^{m} C_{q_i}$. It suffices to show that M is a quotient of some $(\mathbb{Z}/n\mathbb{Z})^*$.

By Dirichlet's theorem on arithmetic progressions, there exist distinct primes $p_1, \ldots, p_m$ such that $p_j \equiv 1 \pmod{q_j}$ for all $j \in \{1, \ldots, m\}$.

It follows that C_{q_j} is a quotient of $(\mathbb{Z}/p_j\mathbb{Z})^*$ for all $j \in \{1, \ldots, m\}$. So we can define the quotient epimorphisms $\kappa_j : (\mathbb{Z}/p_j\mathbb{Z})^* \to C_{q_j}$.

IGP for Abelian Groups over $\mathbb{Q}$ - Proof (Continued)

Set $n = p_1 \dots p_m$ and let $\pi_j : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/p_j\mathbb{Z})^*$ be natural projections (see Lemma B). These are also epimorphisms.

Define

$$f \coloneqq (\kappa_1 \circ \pi_1, \dots, \kappa_m \circ \pi_m) : (\mathbb{Z}/n\mathbb{Z})^* \to \prod_{i=1}^{m} C_{q_i},$$

which composes and glues the individual epimorphisms. f is also an epimorphism, so $M \cong \prod_{i=1}^{m} C_{q_i} \cong (\mathbb{Z}/n\mathbb{Z})^*/\ker(f)$. □

The IGP over $\mathbb{Q}$ is thus solved in the Abelian case.

Recognition Criterion for S_n

Since a field automorphism permutes the roots of polynomials, we may view each Galois group as a subgroup of some S_n.

We establish a sufficient condition for $G \le S_n$ to be S_n.

Definition

Let G act on X. Then the action is **transitive** if

$$\forall a, b \in X, \quad \exists g \in G \quad g \cdot a = b.$$

Theorem (Recognition criterion for S_n)

Let G be a transitive subgroup of S_n containing a transposition and an $(n-1)$-cycle. Then $G = S_n$.

Proof of the Recognition Criterion

Theorem (Recognition criterion for S_n)

Let G be a transitive subgroup of S_n containing a transposition and an $(n-1)$-cycle. Then $G = S_n$.

WLOG assume $\sigma = (2\ 3\ \dots\ n-1)$, $\tau = (u\ v) \in G$. Choose $\theta \in G$ s.t. $\theta(u) = 1$. Let $k = \theta(v)$. Then $k \geq 2$ and

$$\eta := \theta\tau\theta^{-1} = (1\ k) \in G.$$

By conjugating η with σ, we have

$$\forall 2 \leq r \leq n, \quad (1\ r) \in G.$$

Since $(1\ r)(1\ s)(1\ r)^{-1} = (r\ s)$, G contains every transposition, so $G = S_n$. □

IGP for S_n over $\mathbb{Q}$ – Plan

Theorem (Recognition criterion for S_n)

Let G be a transitive subgroup of S_n containing a transposition and an $(n-1)$-cycle. Then $G = S_n$.

By the properties of Galois group, we know that

Theorem (Irreducibility criterion)

Let L/K be a Galois extension with Galois group G. Then $f(x) \in K[x]$ is irreducible if and only if G is transitive on the roots of f.

Task: Find an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree n whose Galois group G contains a transposition and an $(n-1)$-cycle.

Reduction Modulo p

Theorem (mod p test for irreducibility)

Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ and $p \nmid a_n$ be a prime. If the mod p reduction $\overline{f}(x)$ is irreducible over $\mathbb{F}_p$, then $f(x)$ is irreducible over $\mathbb{Q}$.

We also quote a result from algebraic number theory:

Theorem (Dedekind)

If $f(x) \in \mathbb{Z}[x]$ is monic and $\overline{f} = g_1 g_2 \cdots g_k$ for distinct irreducibles $g_1, \ldots, g_k$ of degree $n_1, \ldots, n_k$ in $\mathbb{F}_p[x]$, then $\mathrm{Gal}(f/\mathbb{Q})$ contains an $(n_1, n_2, \ldots, n_k)$-cycle.

See Keith Conrad's article [1] for details.

IGP for S_n over $\mathbb{Q}$ – Proof

Now, let $f(x) \in \mathbb{Z}[x]$ be monic and $G = \mathrm{Gal}(f/\mathbb{Q})$.

Choose irreducible $f_1(x) \in \mathbb{F}_2[x]$ of degree n. By Dedekind's theorem,

$$f \equiv f_1 \pmod 2 \implies G \text{ transitive.}$$

Let $f_2 = g_1 g_2 \in \mathbb{F}_3[x]$ for irreducible quadratic $g_1(x) \in \mathbb{F}_3[x]$ and $g_2(x) \in \mathbb{F}_3[x]$ of degree $n-2$ s.t.

$$g_2(x) = \begin{cases} h(x) & n \text{ odd} \\ xh(x) & n \text{ even} \end{cases}$$

for some irreducible $h(x) \in \mathbb{F}_3[x]$ of odd degree. If $f \equiv f_2 \pmod 3$, then G contains some $(2,k)$-cycle σ for some odd k, so σ^k is a transposition.

IGP for S_n over $\mathbb{Q}$ – Proof (Continued)

Now, we have

$$f \equiv f_1 \pmod 2 \implies G \text{ transitive,} \tag{1}$$

$$f \equiv f_2 \pmod 3 \implies G \text{ contains a transposition.} \tag{2}$$

Let $f_3(x) = xg_3(x) \in \mathbb{F}_5[x]$ for some irreducible $g_3(x) \in \mathbb{F}_5[x]$ of degree $n-1$, so

$$f \equiv f_3 \pmod 5 \implies G \text{ contains an } (n-1)\text{-cycle.} \tag{3}$$

By the CRT, there exists a monic $f(x) \in \mathbb{Z}[x]$ satisfying the conditions (1), (2), and (3), so $G = S_n$. $\square$

Table of Contents

Properties of Finite Fields

In contrast to the case over $\mathbb{Q}$, not every finite group is realizable over any given finite field. We start with some preliminary facts:

Proposition

1. *Every finite field is of order $q = p^n$ for some prime p and some $n \in \mathbb{N}$.*
2. *Conversely, for all prime p and all $n \in \mathbb{N}$, there exists a field of order $q = p^n$, unique up to isomorphism (we denote this field by $\mathbb{F}_q$).*
3. *$\mathbb{F}_q$ precisely contains all the roots of the polynomial $x^q - x \in \mathbb{F}_p[x]$.*

Proof: 1) Consider the following obvious facts.

i. For all prime p, there is exactly one field of order $\mathbb{F}_p$, up to isomorphism.

ii. Every finite field F has characteristic p for some prime p, $\mathbb{F}_p$ is a subfield of F, and $F/\mathbb{F}_p$ is a finite extension. □

Properties of Finite Fields (Continued)

Proof: (Continued)

2) & 3) Let $q = p^n$ and $f(x) = x^q - x \in \mathbb{F}_p[x]$. Let L be a splitting field of $f(x)$ over $\mathbb{F}_p$. It can be proven that the q roots of $f(x)$ in L form a subfield of L. This proves the existence part of 2).

Let F be a field of order q. It can be shown that all its elements are roots of $x^q - x$, so $x^q - x \in \mathbb{F}_p[x]$ splits in F. There cannot be a smaller field in which it splits, so F is a splitting field of $x^q - x$. Recalling that all splitting fields of a polynomial are isomorphic, the uniqueness part of 2) is proven. □

IGP over Finite Fields - Proof

Theorem

A finite group is realizable over any given finite field if and only if it is cyclic.

Proof: Let $q = p^n$ for some prime p, and consider a finite extension $L/\mathbb{F}_q$ of degree $m \in \mathbb{N}$. Of course $L \cong \mathbb{F}_{q^m}$ as extensions of $\mathbb{F}_q$. Consider the function (called **Frobenius endomorphism**)

$$\sigma : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_{q^m}, \; x \mapsto x^q.$$

This is an automorphism of $\mathbb{F}_{q^m}$ partly due to the theorem below:

Theorem (Freshman's dream, general version)

Let R be commutative ring with prime characteristic p; then for all $a, b \in R$ and all $n \in \mathbb{N}$, we have $(a + b)^{p^n} = a^{p^n} + b^{p^n}$.

IGP over Finite Fields - Proof (Continued)

Proof: (Continued)

$\mathbb{F}_{q^m}/\mathbb{F}_q$ is Galois as it is a splitting field of $x^{q^m} - x$ over $\mathbb{F}_q$.

We show that $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$. Since the unit group $\mathbb{F}_q^*$ of $\mathbb{F}_q$ is cyclic, $\mathbb{F}_q^* = \langle \alpha \rangle$, and every non-zero element of $\mathbb{F}_q$ is a power of α. As α is also a root of $x^q - x$, σ fixes α.

Now, we show that $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$ is cyclic. Write $\mathbb{F}_{q^m}^* = \langle \beta \rangle$. Clearly, $\mathbb{F}_{q^m} = \mathbb{F}_q(\beta)$, so σ^k fixes $\mathbb{F}_{q^m}$ iff $\sigma^k(\beta) = \beta$, which happens iff $m \mid k$, so

$$\mathrm{ord}(\sigma) = m = |\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)| = [\mathbb{F}_{q^m} : \mathbb{F}_q],$$

which means that $\mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) = \langle \sigma \rangle \cong C_m$. □

The discussion of the IGP over any finite field is therefore complete.

Table of Contents

Transcendental Extensions

Let L/K be some field extension. Recall that

Definition

An element $\alpha \in L$ is **algebraic** over K if $\exists f(x) \in K[x]$ for which $f(\alpha) = 0$.

We introduce the opposite notion:

Definition

An element $\alpha \in L$ is **transcendental** over K if it is not algebraic. L/K is transcendental if L contains a transcendental element.

e.g. e, π over $\mathbb{Q}$ are transcendental. $\mathbb{Q}(\pi)/\mathbb{Q}$ and $K(t)/K$ are transcendental.

IGP over $\mathbb{C}(t)$

IGP is completely resolved for the case $K = \mathbb{C}(t)$, the complex function field.

Tools: complex analysis, Riemann surfaces, covering maps

Theorem (Riemann's existence theorem, analytic version)

Let S be a compact Riemann surface. For any distinct points $a_1, a_2, \ldots, a_n \in S$ and $c_1, c_2, \ldots, c_n \in \mathbb{C}$, there exists a meromorphic function $f : S \to \mathbb{C}$ such that $f(a_j) = c_j$ for $j = 1, 2, \ldots, n$.

RET establishes a connection between finite extensions over $\mathbb{C}(t)$ and compact Riemann surfaces. See §5-6 of Volklein [4] for details.

IGP over $\mathbb{Q}(t_1, t_2, \ldots, t_n)$

We can relate IGP over the n-variable function field $\mathbb{Q}(t_1, t_2, \ldots, t_n)$ and IGP over $\mathbb{Q}$ via a result of Hilbert:

Theorem (Hilbert's irreducibility theorem)

Let $f(t_1, \ldots, t_n, x_1, \ldots, x_m) \in \mathbb{Q}(t_1, \ldots, t_n)[x]$ be irreducible. Then $\exists$ infinitely many $q_1, q_2, \ldots, q_n \in \mathbb{Q}$ s.t. the specialized polynomial $f(q_1, \ldots, q_n, x_1, \ldots, x_m) \in \mathbb{Q}[x_1, \ldots, x_m]$ is irreducible.

Corollary

If G is realizable over $\mathbb{Q}(t_1, \ldots, t_n)$, then G is realizable over $\mathbb{Q}$.

See §1 of Volklein [4]. This means one can realize every S_n by considering the Galois extension of a general polynomial.

Bibliography

Keith Conrad.
Galois Groups over $\mathbb{Q}$ and Factorizations mod p.
https://kconrad.math.uconn.edu/blurbs/gradnumthy/galois-Q-factor-mod-p.pdf

David S. Dummit and Richard M. Foote (2004).
Abstract Algebra (3rd ed.).
John Wiley & Sons, Inc.

Fariba Ranjbar and Saeed Ranjbar (1979).
Inverse Galois Problem and Significant Methods.
arXiv: 1512.08708

Helmut Voklein (1996).
Groups as Galois Groups: An Introduction.
Cambridge University Press.