Inverse Galois Problem

Jia-Hao Liang

Instructor: Olivier Fouquet
Coaches: Estelle Basset and Arthur Gerard

20th August 2024

Table of Contents

Introduction to Galois Theory

- $K := \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is the smallest field containing $\alpha_1, \ldots, \alpha_n$, and $\mathbb{Q}$.
- $Aut_{\mathbb{Q}}K$ is the automorphism group that fixes $\mathbb{Q}$.

- Galois extension:

$K/\mathbb{Q}$ is Galois

1. $\iff$ $\alpha_1, \alpha_2, \ldots, \alpha_n$ are all the roots of $P \in \mathbb{Q}[x]$
(The roots, all the roots, nothing but the roots)
2. $\iff$ $|Aut_{\mathbb{Q}}K| = [K : Q]$ (Things move around a lot)

- Galois correspondence:

Subextension$\longleftrightarrow$Subgroup

Introduction

The $Inverse\ Galois\ Problem$ over $\mathbb{Q}$ for a group G asks whether a finite group G is the Galois group of a field extension of $\mathbb{Q}$.

- Object: Field extension, Minimal polynomial, Automorphism group
- Main interest: Find the field extension
- Procedure

Introduction

Procedure:

- Step 1: Construct the extension
- Step 2: Prove that the extension is Galois
  1. Method 1: Roots, all the roots, nothing but the roots
  2. Method 2: Degree = Order
- Step 3: Show the Automorphism group is equal to the given group

Problem 1

Statement 1

Show that $\mathbb{Z}/n\mathbb{Z}$ for all $2 \leq n \leq 12$ is the Galois group of a field extension over $\mathbb{Q}$.

Solution to Problem 1

Main Idea

1. $\mathbb{Z}/(p-1)\mathbb{Z} \simeq (\mathbb{Z}/p\mathbb{Z})^*$ for p a prime
2. Cyclotomic field

Notation

Denote a primitive n-th root of unity as ζ_n.

Definition

Cyclotomic field is a field $K_n = \mathbb{Q}(\zeta_n)$ obtained from the field $\mathbb{Q}$ of rational numbers by adjoining ζ_n, where n is a natural number.

Solution to Problem 1

Solution

We divide the problem into two cases

$$\begin{cases} n = 2, 4, 6, 10, 12 & n + 1 \text{ is a prime number} \\ n = 3, 5, 7, 8, 9, 11 & n + 1 \text{ is a composite number} \end{cases}$$

Solution to Problem 1

Easy case: When $n+1$ is a prime number $(n = 2, 4, 6, 10, 12)$

- Step 1: Consider $\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}$.
- Step 2: Consider the minimal polynomial of ζ_{n+1} : $\mu_{\zeta_{n+1}} = \sum_{i=1}^{n} x^n$
  Then, by "the roots, all the roots, nothing but the roots",
  $\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}$ is Galois.
- Step 3: Consider the automorphism $f : \zeta_{n+1} \mapsto \zeta_{n+1}^a$.
  $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta_{n+1}) \simeq (\mathbb{Z}/(n+1)\mathbb{Z})^* \simeq \mathbb{Z}/n\mathbb{Z}$.

Solution to Problem 1

Easy case: When $n+1$ is a prime number $(n = 2, 4, 6, 10, 12)$

- Step 1: Consider $\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}$.
- Step 2: Consider the minimal polynomial of ζ_{n+1} : $\mu_{\zeta_{n+1}} = \sum_{i=1}^{n} x^n$
  Then, by "the roots, all the roots, nothing but the roots", $\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}$ is Galois.
- Step 3: Consider the automorphism $f : \zeta_{n+1} \mapsto \zeta_{n+1}^a$.
  $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta_{n+1}) \simeq (\mathbb{Z}/(n+1)\mathbb{Z})^* \simeq \mathbb{Z}/n\mathbb{Z}$.

Solution to Problem 1

Easy case: When $n+1$ is a prime number $(n = 2, 4, 6, 10, 12)$

- Step 1: Consider $\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}$.
- Step 2: Consider the minimal polynomial of ζ_{n+1} : $\mu_{\zeta_{n+1}} = \sum_{i=1}^{n} x^n$
  Then, by "the roots, all the roots, nothing but the roots",
  $\mathbb{Q}(\zeta_{n+1})/\mathbb{Q}$ is Galois.
- Step 3: Consider the automorphism $f : \zeta_{n+1} \mapsto \zeta_{n+1}^a$.
  $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta_{n+1}) \simeq (\mathbb{Z}/(n+1)\mathbb{Z})^* \simeq \mathbb{Z}/n\mathbb{Z}$.

Solution to Problem 1

Hard case: When $n+1$ is a composite

Dirichlet's Theorem: For given $n \in \mathbb{N}$, exist prime $p = kn+1 (k \in \mathbb{N})$

Main idea: Effect of Automorphism
$g : \zeta_p^{a^i b^j} \longmapsto \zeta_p^{a^{i+u} b^{j+v}}$

- Step 1: $L := \mathbb{Q}(\zeta_p^{a^0 b^0} + \ldots + \zeta_p^{a^0 b^{k-1}})$ with $<g> = (\mathbb{Z}/p\mathbb{Z})^*, a = g^k, b = g^n$ of degree n by applying automorphism on it.

$$\begin{array}{c} \mathbb{Q}(\zeta_p) \\ \Big| \, k \\ L \\ \Big| \, n \\ \mathbb{Q} \end{array}$$

$$\begin{matrix} \zeta_p^{a^0 b^0} & \zeta_p^{a^0 b^1} & \cdot & \zeta_p^{a^0 b^{k-1}} \\ \zeta_p^{a^1 b^0} & \ddots & & \vdots \\ \vdots & & \cdot & \vdots \\ \zeta_p^{a^{n-1} b^0} & \cdots & \cdot & \zeta_p^{a^{n-1} b^{k-1}} \end{matrix}$$

Diagram of unit roots

Solution to Problem 1

Hard case: When $n+1$ is a composite or arbitrary

- Step 2: Consider the polynomial $\prod_{i=0}^{n-1}(x-r_i), r_i := \zeta_p^{a^ib^0} + \ldots + \zeta_p^{a^ib^{k-1}}$.
  It is the minimal polynomial since it is invariant under $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta_p)$.
  Define $f : \zeta_p \longmapsto \zeta_p^{a^ub^0}$.
- Step 3: $Aut_{\mathbb{Q}}L \simeq \mathbb{Z}/n\mathbb{Z}$.

$$\begin{array}{cccc} \zeta_p^{a^0b^0} & \zeta_p^{a^0b^1} & \cdots & \zeta_p^{a^0b^{k-1}} \\ \zeta_p^{a^1b^0} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \zeta_p^{a^{n-1}b^0} & \cdots & \cdots & \zeta_p^{a^{n-1}b^{k-1}} \end{array}$$

Diagram of unit roots

Solution to Problem 1

Hard case: When $n+1$ is a composite or arbitrary

- Step 2: Consider the polynomial $\prod_{i=0}^{n-1}(x-r_i), r_i := \zeta_p^{a^i b^0} + \ldots + \zeta_p^{a^i b^{k-1}}$.
  It is the minimal polynomial since it is invariant under $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta_p)$.
  Define $f : \zeta_p \longmapsto \zeta_p^{a^u b^0}$.
- Step 3: $Aut_{\mathbb{Q}}L \simeq \mathbb{Z}/n\mathbb{Z}$.

$$\begin{array}{cccc}
\zeta_p^{a^0 b^0} & \zeta_p^{a^0 b^1} & \cdots & \zeta_p^{a^0 b^{k-1}} \\
\zeta_p^{a^1 b^0} & \ddots & & \vdots \\
\vdots & & \ddots & \vdots \\
\zeta_p^{a^{n-1} b^0} & \cdots & \cdots & \zeta_p^{a^{n-1} b^{k-1}}
\end{array}$$

Diagram of unit roots

Problem 2

Statement 2

Let $P \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p with exactly $p-2$ real roots in $\mathbb{C}$. Show that the Galois group of the smallest subfield of $\mathbb{C}$ containing the roots of P has Galois $\mathfrak{S}_p$. Find a concrete extension with Galois group $\mathfrak{S}_5$.

Analysis

1. The smallest subfield is $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_p)$.
2. Since automorphism sends root to root, so $Aut_{\mathbb{Q}}K \subset \mathfrak{S}_p$.

Problem 2

Statement 2

Let $P \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p with exactly $p-2$ real roots in $\mathbb{C}$. Show that the Galois group of the smallest subfield of $\mathbb{C}$ containing the roots of P has Galois $\mathfrak{S}_p$. Find a concrete extension with Galois group $\mathfrak{S}_5$.

Analysis

1. The smallest subfield is $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_p)$.
2. Since automorphism sends root to root, so $Aut_{\mathbb{Q}} K \subset \mathfrak{S}_p$.

Problem 2

Analysis

3. It suffices to find a 'swap' element f and a cyclic permutation g by considering $g^i f g^{-i}$ for $1 \leq i \leq n$.

WLOG, let the cyclic permutation g be $(1, 2, \ldots, n) \overset{g}{\mapsto} (2, 3 \ldots, 1)$, and the 'swap' element f be $(1, 2) \overset{f}{\mapsto} (2, 1)$.

$$g^i f g^{-i} : (1, \ldots, i+1, i+2 \ldots, n) \xmapsto{g^{-i}} (n-i+1, \ldots, 1, 2, \ldots, n-i) \overset{f}{\mapsto}$$
$$(n-i+1, \ldots, 2, 1, \ldots, n-i) \xmapsto{g^i} (1, \ldots, i+2, i+1, \ldots, n)$$

Solution to Problem 2

Proof

Now we consider the field extension
$\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset K$

By the Spyglass Property
$[K:\mathbb{Q}(\alpha_1)] \times [\mathbb{Q}(\alpha_1):\mathbb{Q}] = [K:\mathbb{Q}] \implies p\Big|[K:\mathbb{Q}]$

By "The roots, all the roots, nothing but the roots",
$[K:\mathbb{Q}]$ is Galois. So from "Things move around a lot",
$[K:\mathbb{Q}] = |Aut_{\mathbb{Q}}K| \implies p\Big|\,|Aut_{\mathbb{Q}}K|$

$$
\begin{tikzcd}
K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_p) \arrow[d, dash] \\
\mathbb{Q}(\alpha_1) \arrow[d, dash, "p"'] \\
\mathbb{Q}
\end{tikzcd}
$$

Solution to Problem 2

Theorem (Cauchy)

Let G be a finite group and p be a prime factor of $|G|$. Then G contains an element of order p. Equivalently, G contains a subgroup of order p.

Proof

By Cauchy's theorem, because $p \big| \, |Aut_{\mathbb{Q}}K|$, so $\exists g \in Aut_{\mathbb{Q}}K \subset \mathfrak{S}_p$ s.t. g has order p.
The action g is a cyclic permutation of the roots.

Also, consider $f := \alpha_i \longmapsto \overline{\alpha_i}$, the conjugate action. $f \in Aut_{\mathbb{Q}}K$ and it swaps imaginary roots.

$$\begin{tikzcd}[arrows=dash]
K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_p) \arrow[d] \\
\mathbb{Q}(\alpha_1) \arrow[d, "p"'] \\
\mathbb{Q}
\end{tikzcd}$$

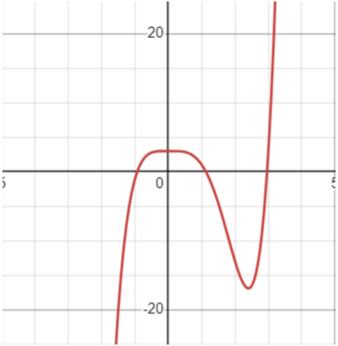
Solution to Problem 2

Example

Consider the roots $\alpha_1, \ldots, \alpha_5$ of the polynomial
$P = x^5 - 3x^4 + 3 \in \mathbb{Q}[x]$
By Eisenstein's Criterion, P is irreducible over $\mathbb{Q}$.
Because $\frac{d}{dx}(x^5 - 3x^4 + 3) = 5x^4 - 12x^3$,

-1	$(-\infty, 0)$	0	$(0, \frac{12}{5})$	$\frac{12}{5}$	$(\frac{12}{5}, +\infty)$	3
< 0	$\nearrow$	> 0	$\searrow$	< 0	$\nearrow$	> 0

By Intermediate Value Theorem, there are 3 real roots,
so $Aut_{\mathbb{Q}}\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = \mathfrak{S}_5$



Problem 3

Statement

Show that all groups of order 8 are Galois groups over $\mathbb{Q}$

Analysis

We know that there are only 5 groups of order 8:

$$\underbrace{\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}_{Abelian}, \underbrace{D_8, \quad Q_8}_{Non-Abelian}$$

Solution to Problem 3

Solution

The Abelian groups are:

1. $\mathbb{Z}/8\mathbb{Z}$
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
3. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

For 1, $\mathbb{Z}/8\mathbb{Z}$ is Galois as shown in Problem 1.
For 2, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \simeq (\mathbb{Z}/15\mathbb{Z})^* \simeq Gal\left(\mathbb{Q}(\zeta_{15})/\mathbb{Q}\right)$
For 3, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq Gal\left(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}\right)$

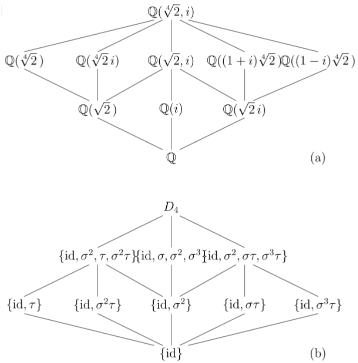
Solution to Problem 3

Definition of D_8

$$D_8 := \langle a, b : a^4 = b^2 = e, aba = b^{-1} \rangle$$

D_8

- Step 1: Consider $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$
- Step 2: Consider $x^4 - 2$. By "The roots, all the roots, nothing but the roots", this is Galois.
- Step 3: Consider $\sigma : \sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $\tau : \tau(i) = -i$. Then, $\sigma\tau\sigma = \tau^{-1}$



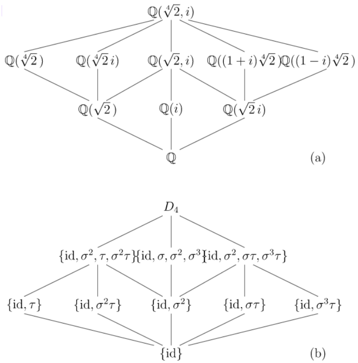
Solution to Problem 3

Definition of D_8

$D_8 := \langle a, b : a^4 = b^2 = e, aba = b^{-1} \rangle$

D_8

- Step 1: Consider $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$
- Step 2: Consider $x^4 - 2$. By "The roots, all the roots, nothing but the roots", this is Galois.
- Step 3: Consider $\sigma : \sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $\tau : \tau(i) = -i$. Then, $\sigma\tau\sigma = \tau^{-1}$



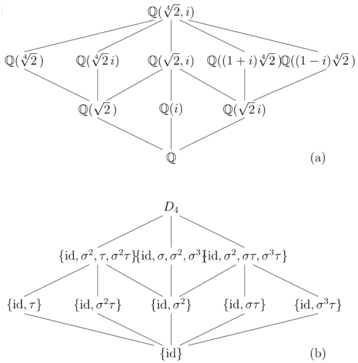
Solution to Problem 3

Definition of D_8

$$D_8 := \langle a, b : a^4 = b^2 = e, aba = b^{-1} \rangle$$

D_8

- Step 1: Consider $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2})$
- Step 2: Consider $x^4 - 2$. By "The roots, all the roots, nothing but the roots", this is Galois.
- Step 3: Consider $\sigma : \sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $\tau : \tau(i) = -i$. Then, $\sigma\tau\sigma = \tau^{-1}$



Solution to Problem 3

Definition of Q_8

$\langle a, b : a^4 = e, a^2 = b^2, ba = ab^3 \rangle$

$$
\begin{tikzcd}
& Q_8 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle a \rangle \arrow[dr, dash] & \langle b \rangle \arrow[d, dash] & \langle ab \rangle \arrow[dl, dash] \\
& \langle -1 \rangle \arrow[d, dash] & \\
& \{Id\} &
\end{tikzcd}
$$

Solution to Problem 3

Q_8

- Step 1: Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and then $L = K\left(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right)$
  Then, $[L : \mathbb{Q}] = 8$ by the Spyglass Property.
- Step 2: Consider

$$P(x) = \prod_{\epsilon_1, \epsilon_2 \in \pm 1} (x - (2 + \epsilon_1\sqrt{2})(3 + \epsilon_2\sqrt{3}))$$

Then, $P(x^2)$ is the minimal polynomial of $\sqrt{(2+\sqrt{2})(3+\sqrt{3})}$

Solution to Problem 3

Q_8

- Step 1: Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and then $L = K\left(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right)$
  Then, $[L : \mathbb{Q}] = 8$ by the Spyglass Property.
- Step 2: Consider

$$P(x) = \prod_{\epsilon_1, \epsilon_2 \in \pm 1} (x - (2 + \epsilon_1\sqrt{2})(3 + \epsilon_2\sqrt{3}))$$

Then, $P(x^2)$ is the minimal polynomial of $\sqrt{(2+\sqrt{2})(3+\sqrt{3})}$

Solution to Problem 3

Q_8

- Step 2(Cont.): Consider
$$\tau : \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2-\sqrt{2})(3+\sqrt{3})} \implies \sqrt{2} \mapsto -\sqrt{2}.$$
$$\sigma : \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2+\sqrt{2})(3-\sqrt{3})} \implies \sqrt{3} \mapsto -\sqrt{3}.$$
- Step 3:
Then we can check that $\sigma\tau = \tau\sigma^3$, where τ and σ has order 4, and $\tau\sigma \neq \sigma\tau \implies Aut_{\mathbb{Q}}L$ is not Abelian, so $Aut_{\mathbb{Q}}L \simeq Q_8$

Solution to Problem 3

Q_8

- Step 2(Cont.): Consider
$$\tau : \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2-\sqrt{2})(3+\sqrt{3})} \implies \sqrt{2} \mapsto -\sqrt{2}.$$
$$\sigma : \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2+\sqrt{2})(3-\sqrt{3})} \implies \sqrt{3} \mapsto -\sqrt{3}.$$

- Step 3:
Then we can check that $\sigma\tau = \tau\sigma^3$, where τ and σ has order 4, and $\tau\sigma \neq \sigma\tau \implies Aut_{\mathbb{Q}}L$ is not Abelian, so $Aut_{\mathbb{Q}}L \simeq Q_8$

Solution to Problem 3

Lattice for Q_8

$$\begin{tikzcd}
 & Q_8 \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle a \rangle \arrow[dr, dash] & \langle b \rangle \arrow[d, dash] & \langle ab \rangle \arrow[dl, dash] \\
 & \langle -1 \rangle \arrow[d, dash] & \\
 & \{Id\} &
\end{tikzcd}$$

Lattice for $L/\mathbb{Q}$

$$\begin{tikzcd}
 & L = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right) \arrow[d, dash] & \\
 & K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{6}) \arrow[d, dash] & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Thank You for your Attention!