# Inverse Galois Problem

Jia-Hao Liang

October 15th, 2024

## Abstract

Since the introduction of Galois Theory by the French mathematician Évariste Galois in the early 19th century, the links between groups and field extensions have been discovered. In Galois Theory, the fundamental theorem — Galois correspondence — states that a field extension that is "Galois," meaning that it satisfies one of the equivalent crucial properties of Galois Theory, can be associated with a field in such a way that the lattice of subfields and the lattice of subgroups will be exact inverses of each other. In Galois Theory, our aim is to study fields, but we use Galois correspondence to instead study the groups, which simplifies the task.

Conversely, the Inverse Galois Problem takes an opposite approach: to find the field extension corresponding to a given group. The Inverse Galois Problem remains an unsolved challenge in mathematics, as the ultimate goal is to demonstrate that all groups have a corresponding field extension. In the article below, we employ elementary methods to deduce specific conclusions in Inverse Galois Theory. While not completely solved, this article presents methods to establish correspondences for groups such as cyclic and permutation groups.

**Keywords**: Inverse Galois Problem, Galois Theory, Permutation Groups, Cyclic Groups, Groups of Order 8, Field Extension, Automorphism, Minimal Polynomial.

# Contents

# 1 Introduction

## 1.1 Galois Theory

Galois theory, contributed by Évariste Galois, establishes a crucial link between field theory and group theory. Through the fundamental theorem of Galois theory, specific issues in field theory can be streamlined into group theory, thereby simplifying comprehension and analysis.

## 1.2 Galois Extension

**Lemma 1 (Primitive Element Theorem)** *Consider $K \subset L \subset \mathbb{C}$ and $L/K$ is a finite field extension($dim_K L < +\infty$). Then $\exists \alpha \in L$ such that $L = K(\alpha)$. We call $\alpha$ a primitive element.*

Let $L/\mathbb{Q}$ be a finite extension. $K \subset L$. By the Primitive Element Theorem, $\exists \alpha \in L$ such that $L = K(\alpha)$. We say that $L/\mathbb{Q}$ is Galois if and only if one of the following equivalent statements holds:

1. $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where $\alpha_i$ are all the roots of $P \in K[x]$
(Crucial property number 0: The roots, all the roots, nothing but the roots)
2. $|Aut_{\mathbb{Q}} K| = [K : \mathbb{Q}]$
(Crucial property number 1: Things move around a lot)
3. $L^{Aut_K L} = K$
(Crucial property number 2: Things that don't move are rare)
4. $\forall \beta \in L, \mu_\beta = \prod_{\beta' \in \mathcal{O}} (x - \beta) \in K[x]$
(Crucial property number 3: One in, all in)

## 1.3 Galois Correspondence

**Lemma 2 (Fundamental theorem of Galois theory)** *Suppose $L/K$ is Galois. Then there are two groups*

$$\mathcal{G} : \{K \subset F \subset L\} \longrightarrow \{H \in Gal(L/K) | H \ \textit{a subgroup}\}$$
$$F \longmapsto Aut_F L$$

$$\mathcal{E} : \{H \ \textit{subgroup of} \ Gal(L/K)\} \longrightarrow \{K \subset F \subset L\}$$
$$H \longmapsto L^H$$

*These 2 maps are bijections inverse of each other and such that if $H_1 \subset H_2$ then $\mathcal{E}(H_2) \subset \mathcal{E}(H_1)$ and if $F_1 \subset F_2$, $\mathcal{G}(F_2) \subset \mathcal{G}(F_1)$*

### 1.4 Inverse Galois Problem

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 $\mathbb{Q}$.

To find the field extension that corresponds to our desired group $G$, we will follow a procedure of three steps.

1. Construct a field extension
2. Prove that the field extension that we constructed is Galois. We can do this by using any of the 4 equivalent crucial properties of Galois theory
3. Show the Automorphism group that corresponds to the constructed field is equal to the desired group $G$

## 2 Permutation Groups

**Lemma 3** *$\forall n \in \mathbb{N}$, $\exists P(x)$ an irreducible polynomial over $\mathbb{Q}$ of degree $n$ with n-2 real roots and 2 imaginary roots.*

*Proof.* For a prime p, define the polynomial $f(x)$ of degree $n$ as

$$f(x) = (x^2 + m)\prod_{i=1}^{n-2}(x - \beta_i) \in \mathbb{Z}[x]$$

where $m > 0, 0 < \beta_1 < \beta_2 < \ldots < \beta_{n-2} < p, (\beta_1, \ldots, \beta_{n-2}) \in \mathbb{Z}^{n-2}$.

$f(x)$ has $n - 2$ real roots $\beta_1, \ldots, \beta_{n-2}$, and 2 imaginary roots $\beta_{n-1} = i\sqrt{m}, \beta_n = -i\sqrt{m}$. Now consider

$$g(x) = f(x) + \frac{1}{r}x^n$$

where $\exists r$ such that $p||r, m \wedge r = 1$, and $r$ sufficiently large such that $g(x)$ also has $n - 2$ real roots $\alpha_1, \ldots, \alpha_{n-2}$, and 2 imaginary roots $\alpha_{n-1}, \alpha_n$, and $\forall 1 \leq i \leq n-2, i \in \mathbb{Z}$. Define $P(x)$ as

$$P(x) = rg(x) = rf(x) + x^n = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_o$$

By this definition, the roots of $P(x)$ are also $\alpha_1, \ldots, \alpha_n$. $c_n = r + 1$, so $p \nmid c_n$. Also $\forall 0 \leq i \leq n-1, i \in \mathbb{Z}$, $p|r, r|c_i$ so $p|c_i$. Lastly, $c_0 = mr\prod_{i=1}^{n-2}\beta_i$, and $m \wedge r = 1, \beta_i \wedge r = 1$, so $p^2 \nmid c_0$

**Lemma 4 (Eisenstein's Criterion)** [1] *For a polynomial $P(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_o$, if $\exists p$ a prime such that the following three conditions apply:*

1. $\forall 0 \leq i \leq n-1, i \in \mathbb{Z}, p | c_i$
2. $p \nmid c_n$
3. $p^2 \nmid c_0$

*Then $P(x)$ is irreducible over $\mathbb{R}$*

By Eisenstein's criterion, because $p \nmid c_n, p|c_i, p^2 \nmid c_0$, so $P(x)$ is a irreducible polynomial over $\mathbb{Q}$.

Therefore, $\exists P(x) \in \mathbb{Z}[x]$ which is an irreducible polynomial over $\mathbb{R}$ of degree $n$ with $n-2$ real roots $\alpha_1, \ldots, \alpha_{n-2}$ and 2 imaginary roots $\alpha_{n-1}, \alpha_n$.

Now, consider the smallest field $K$ containing all the roots of the polynomial $P(x)$ that has degree $p$ a prime. Because $K$ must contain $\mathbb{Q}$ and all the roots, so $K = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_p)$.

**Theorem 5** *$Gal(K/\mathbb{Q}) = \mathfrak{S}_p$ for $p$ a prime*

*Proof.* By *Crucial Property Number 0 of Galois Theory*, the finite extension $K/\mathbb{Q}$ is Galois because $\alpha_1, \ldots, \alpha_n$ are all the roots of $P(x) \in \mathbb{Q}[x]$. Consider the field extension $\mathbb{Q} \subset \mathbb{Q}(\alpha_1) \subset K$

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

The diagram of the field extension

Because $P(\alpha_1) = 0$ and $P(x)$ is irreducible in $\mathbb{Q}$, so $\mu_{\mathbb{Q}}(x) = P(x)$, so by definition the degree of the field extension $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = deg(\mu_{\mathbb{Q}}(x)) = p$.

**Lemma 6 (Spyglass Property)** [2] *Given three fields $K \subset L \subset M, [M : K] = [M : L] \times [L : K]$*

By the Spyglass Property, $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha_1)] \times [\mathbb{Q}(\alpha_1) : \mathbb{Q}]$, so $p \big| [K : \mathbb{Q}]$.

Because $K/\mathbb{Q}$ is Galois, so from *Crucial Property Number 2 of Galois Theory*, $[K : \mathbb{Q}] = |Aut_{\mathbb{Q}} K|$, so $p \big| \, |Aut_{\mathbb{Q}} K|$.

**Lemma 7 (Cauchy theorem in Group theory)** [3] *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 $p$.*

By Cauchy theorem, because $p\big|\,|Aut_{\mathbb{Q}}K|$, so $\exists g \in Aut_{\mathbb{Q}}K$ such that the action $g$ has order $p$. Because $Aut_{\mathbb{Q}}K \subset \mathfrak{S}_p$, so $g \subset \mathfrak{S}_p$. Therefore, the action $g$ within the permutation group is a cyclic permutation of the roots.

Also, consider the conjugate action $f \coloneqq \alpha_i \longmapsto \overline{\alpha_i}$. The action $f$ swaps the imaginary roots, and by definition $f \subset Aut_{\mathbb{Q}}K$.

Now, we have found two actions within $Aut_{\mathbb{Q}}K$. The conjugate action $f$ and the cyclic permutation action $g$. Consider the composed action $g^ifg^{-i}$ for $1 \leq i \leq p$.

Without lost of generality, let the cyclic permutation action $g$ be $(\alpha_1, \alpha_2, \dots, \alpha_p) \overset{g}{\mapsto}$ $(\alpha_2, \alpha_3, \dots, \alpha_1)$, and the conjugate action $h$ be $(\alpha_x, \alpha_y) \overset{h}{\mapsto} (\alpha_y, \alpha_x)$ with $x < y$. Notice that $(y-x) \wedge p = 1$, so by Bezout's Theorem, $\exists (r_1, r_2) \in \mathbb{Z}^2$ such that $(y-x)r_1 + pr_2 = 1$, and hence we get $x + (y-x)r_1 = x + 1 - pr_2$. Therefore, the action $f^{'} = (hg^{y-x})^{r_1-1}h(g^{x-y}h)^{r_1-1}$ will be $(\alpha_x, \alpha_{x+1}) \overset{f^{'}}{\longmapsto} (\alpha_{x+1}, \alpha_x)$. Then, consider the action $f = g^{x-1}f^{'}g^{1-x}$. This action will be $(\alpha_1, \alpha_2) \overset{f}{\mapsto} (\alpha_2, \alpha_1)$.

Now, with actions $f, g$, we consider this composed action
$g^ifg^{-i} : (\alpha_1, \dots, \alpha_{i+1}, \alpha_{i+2} \dots, \alpha_p) \overset{g^{-i}}{\longmapsto} (\alpha_{p-i+1}, \dots, \alpha_1, \alpha_2, \dots, \alpha_{p-i})$
$\overset{f}{\mapsto} (\alpha_{p-i+1}, \dots, \alpha_2, \alpha_1, \dots, \alpha_{p-i}) \overset{g^i}{\longmapsto} (\alpha_1, \dots, \alpha_{i+2}, \alpha_{i+1}, \dots, \alpha_p)$

Therefore, by composing $f$ and $g$, we can swap any two adjacent roots. By composing this again, we can swap any two roots. Therefore, $\mathfrak{S}_p \subset Aut_{\mathbb{Q}}K$. Also, because $Aut_{\mathbb{Q}}K \subset \mathfrak{S}_p$ as mentioned before, so $\mathfrak{S}_p = Aut_{\mathbb{Q}}K$.

Since $K/\mathbb{Q}$ is Galois, so by definition $Gal(K/\mathbb{Q}) = Aut_{\mathbb{Q}}K$. Therefore, $Gal(K/\mathbb{Q}) = \mathfrak{S}_p$.

# 3 Cyclic Groups

**Theorem 8** *$\mathbb{Z}/n\mathbb{Z}$ is the Galois group of a field extension over $\mathbb{Q}$.*

*Proof.* We will consider the easy case, that $p$ is a prime number. Firstly, we deduce the following lemma.

**Lemma 9** *$\mu_{\zeta_p} = x^{p-1} + x^{p-2} + \cdots + 1 \equiv \Phi_p(x)$.*

*Proof.* Firstly, $\zeta_p$ is a root of above, since $\zeta_p$ is a root of $\dfrac{x^p - 1}{x - 1}$.Then, we prove this is minimal.

Notice that $\Phi_p(x+1) = \dfrac{(x+1)^p - 1}{x} = x^{p-1} + \dbinom{p}{1} x^{p-2} + \cdots + \dbinom{p}{p-1}$, by Eisenstein's Criterion, $\Phi_p(x+1)$ is irreducible over $\mathbb{Q}$. Therefore $\Phi_p(x)$ is irreducible over $\mathbb{Q}$, thus minimal.

**Theorem 10** *For any prime number $p$, $\mathbb{Z}_{p-1}$ is Galois.*

*Proof.* Let $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ be the field extension. Then it is of degree $p-1$ since the minimal polynomial $\mu_{\zeta_p} = x^{p-1} + x^{p-2} + \cdots + 1$ is of degree $p-1$ by Lemma 9.

By the property of a field, we have that $\zeta_p \in \mathbb{Q}(\zeta_p)$, thus $\zeta_p^i \in \mathbb{Q}(\zeta_p)$, $i = 1, \cdots, p-1$. So we can write $\mathbb{Q}_{\zeta_p}$ as $\mathbb{Q}(\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1})$ while $\zeta_p^i$ ( $i = 1, \cdots, p-1$ ) are the all roots of $\Phi_p$. Therefore, $\mathbb{Q}(\zeta_p)$ is Galois.

Now we will prove that $Aut_{\mathbb{Q}}\mathbb{Q}(\zeta_p) \simeq \mathbb{Z}_{p-1}$. Let $f$ be a mapping from $\mathbb{Z}_{p-1}$ to $Aut_{\mathbb{Q}}(\zeta_p)$, such that $f(k) = g_k$, and $g_k$ is a mapping such that $g_k(\zeta_p^{2^i}) = \zeta_p^{2^{i+k}}$. It is well defined since every element in $\mathbb{Q}(\zeta_p)$ can be written as $P(\zeta_p)$ with $P \in \mathbb{Z}[x]$ and $degP \leq p-1$. Thus, $a \in \mathbb{Q}(\zeta_p)$ implies that

$$a = x_0 + x_1\zeta_p^{2^1} + x_2\zeta_p^{2^2} + \cdots + x_{p-1}\zeta_p^{2^{p-1}},$$

$$g_k(a) = x_0 + x_1\zeta_p^{2^{1+k}} + \cdots + x_{p-1}\zeta_p^{2^{p-1+k}},$$

and
$$g_k^{-1}(a) = x_0 + x_1\zeta_p^{2^{1-k}} + \cdots + x_{p-1}\zeta_p^{2^{p-1-k}}.$$

Therefore, $g_k$ is an automorphism.

If there exists integers $i,\ j$, such that $g_i = g_k$, then $g_i(\zeta_p) = g_j(\zeta_p)$. That is $\zeta_p^{2^i} = \zeta_p^{2^j}$, thus $\zeta_p^{2^i - 2^j} = 1$. By the definition of $\zeta_p$, $2^i \equiv 2^j \pmod{p}$. Thus we can get by Fermat's Theorem, $i \equiv j \pmod{p-1}$. This implies that $p-1 \mid i-j$. Notice that $|i-j| < p-1$, so $i = j$. Therefore, $g_k$ is injective.

Now we have $p-1 = |\mathbb{Z}_{p-1}| \leq |Aut_{\mathbb{Q}}(\zeta_p)|$. On the other hand, $|Aut_{\mathbb{Q}}(\zeta_p)| \leq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$. That is $p-1 = |\mathbb{Z}_{p-1}| \leq |Aut_{\mathbb{Q}}(\zeta_p)| \leq [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$, thus they are all equal, so $f$ is a bijection.

By the definition, we can get $f(g_k \cdot g_j) = f(g_k) \cdot f(g_j)$. Therefore $Aut_{\mathbb{Q}}(\zeta_k) \simeq \mathbb{Z}_{p-1}$, that is $\mathbb{Z}_{p-1}$ is Galois.

To solve the general case, $\forall n \in \mathbb{Z}$, we consider the subextension of $\mathbb{Q}(\zeta_p)$ where $p$ is a prime with the form $p = kn + 1$.

**Lemma 11 (Dirichlet's Theorem)** [4] *Let $a, k \in Z$, with $(a, k) = 1$. Then there are infinitely many prime numbers in the sequence of integers $a, a+k, a+2k, \cdots, a+nk, \cdots$ for $k \in \mathbb{N}$.*

**Lemma 12** *For a given integer $n$, there exist integers $p$ and $k$, such that* $\gcd(k, n) = 1$ *and $p$ is a prime with the form $p = kn + 1$.*

*Proof.* Consider the sequence $a_t = tn^2 + n + 1$ for positive integers $t$. Notice that $\gcd(n^2, n+1) = 1$, thus by Dirichlet's Theorem, there exists an integer $t$ such that $p = tn^2 + n + 1$ is a prime(Notice that this is the case when in Dirichlet's Theorem, $a = 1$). Let $k = tn+1$, then we have $p = tn^2+n+1 = (tn+1)n+1 = kn+1$, $\gcd(k,n) = \gcd(tn+1,n) = \gcd(1,n) = 1$. Therefore the Lemma is proved.

**Lemma 13** *Let* $p,\ k$ *be two positive integers that satisfy* $\gcd(p,k) = 1$*,* $a_1,\ a_2 \in [0, p-1]$*,* $b_1,\ b_2 \in [0, k-1]$*. Define* $f(a,b) = bp + ak$*. We have that for* $(a_1, b_1) \neq (a_2, b_2)$*,* $f(a_1, b_1) \not\equiv f(a_2, b_2) \pmod{pk}$*.*

*Proof.* We will prove by contradiction. Suppose $f(a_1, b_1) \equiv f(a_2, b_2)$ (mod $pk$), i.e. $a_1 k + b_1 p \equiv a_2 k + b_2 k \pmod{pk}$, so $pk \mid (a_1 - a_2)k + (b_1 - b_2)p$. Since $\gcd(k,p) = 1$, $p \mid (a_1 - a_2)k$, thus $p \mid (a_1 - a_2)$. Notice that $a_1,\ a_2 \in [0, p-1]$, we have $a_1 = a_2$.

Similarly, we can have $b_1 = b_2$. Therefore $(a_1, b_1) = (a_2, b_2)$, a contradiction. This Lemma is proved. We follow the definition of $f$ and $g_i$ as before.

**Claim 14** *For any* $m \in \mathbb{N}$*, there exists unique* $(i,j)$*, such that* $g_m = g_k^i \cdot g_n^j$*.*

*Proof.* It is to prove that $g_m(\zeta_p) = g_k^i \cdot g_n^j(\zeta_p)$, i.e. $\zeta_p^{2^m} = g_k^i \cdot g_n^{j-1}(\zeta_p^{2^n}) = g_k^i(\zeta_p^{2^{j\cdot n}}) = \zeta_p^{2^{i\cdot k + j \cdot n}}$.

Since $\gcd(k,n) = 1$, according to the Lemma, we have $(i,j)$ is unique. That is to say, by considering the table below:

$$\begin{array}{cccc}
\zeta_p^{2^{0\cdot k+0\cdot n}} & \zeta_p^{2^{0\cdot k+1\cdot n}} & \cdots & \zeta_p^{2^{0\cdot k+(k-1)\cdot n}} \\
\cdots & \cdots & \cdots & \cdots \\
\zeta_p^{2^{(n-1)\cdot k+0\cdot n}} & \cdots & \cdots & \zeta_p^{2^{(n-1)\cdot k+(k-1)\cdot n}}
\end{array}$$

Applying $g_m \in Aut_{\mathbb{Q}}\mathbb{Q}(\zeta_p)$ to the table above. Any two unit roots in the same column or in the same row are still in the same column or row.

**Define** $r_i = \zeta_p^{2^{ik+0\cdot n}} + \zeta_p^{2^{ik+1\cdot n}} + \cdots + \zeta_p^{2^{ik+(k-1)\cdot n}}$, $i = 0, 1, 2 \cdots, n-1$.

**Claim 15** $P(x) = \prod\limits_{i=0}^{n-1}(x - r_i) \in Q[x]$.

*Proof.* Notice that $g_n(r_i) = r_i$, and $g_k$ is a bijection from $\{r_i \mid i = 0, 1, \cdots, n-1\}$ to itself. Thus for any $m \in \mathbb{N}$,

$$\begin{aligned}
g_m(P(x)) &= g_k^i \cdot g_n^j(P(x)) = g_k^i \cdot g_n^j(\prod_{i=0}^{n-1}(x - r_i)) \\
&= g_k^i(\prod_{i=0}^{n-1}(x - r_i)) = \prod_{i=0}^{n-1}(x - r_i).
\end{aligned}$$

Knowing that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is Galois, thus $\mathbb{Q}(\zeta_p)^{Aut_{\mathbb{Q}}\mathbb{Q}(\zeta_p)} = \mathbb{Q}$.

Since $g_m(P(x)) = P(x)$, any coefficient of $P(x)$ is an element of $\mathbb{Q}(\zeta_p)^{Aut_{\mathbb{Q}}\mathbb{Q}(\zeta_p)}$, consequently an element of $Q$.

Therefore $P(x) \in \mathbb{Q}[x]$.

**Claim 16** *For $i \neq j$, $r_i \neq r_j$.*

*Proof.* Since $\{\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}\}$ are basis of $\mathbb{Q}(\zeta_p)$, $\{\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}\}$ are linearly independent. Thus for $i \neq j$, $r_i \neq r_j$, otherwise $\zeta_p^{2^{i\cdot k+0\cdot n}}, \zeta_p^{2^{i\cdot k+1\cdot n}}, \cdots, \zeta_p^{2^{i\cdot k+(k-1)\cdot n}}, \zeta_p^{2^{j\cdot k+0\cdot n}}, \zeta_p^{2^{j\cdot k+1\cdot n}}, \cdots, \zeta_p^{2^{j\cdot k+(k-1)\cdot n}}$ are linearly dependent, which leads to a contradiction.

**Claim 17** *$\mathbb{Q}(r_0, r_1, \cdots, r_{n-1})/\mathbb{Q}$ is Galois.*

*Proof.* From the above two claims, we have that $P(x) = \prod_{i=0}^{n-1}(x - r_i)$ has no multiple roots. In other words, $\mathbb{Q}(r_0, r_1, \cdots, r_{n-1})$ is the splitting field of a separable polynomial $P(x)$ with coefficients in $\mathbb{Q}$. Therefore $\mathbb{Q}(r_0, r_1, \cdots, r_{n-1})/\mathbb{Q}$ is Galois.

**Claim 18** *$[K : \mathbb{Q}] = n$, where $K := \mathbb{Q}(r_0, r_1, \cdots, r_{n-1})$.*

*Proof.* Since $K/\mathbb{Q}$ is Galois, $[K : \mathbb{Q}] = |Aut_{\mathbb{Q}}K|$. Using the definition, we have $I = g_k^0, g_k, g_k^2, \cdots, g_k^{n-1}$ are different members of $Aut_{\mathbb{Q}}K$. They are different because $g_k^i(r_0) = r_i$ and $r_i \neq r_j$ for $i \neq j$,

$$|Aut_{\mathbb{Q}}K| \geq n \tag{1}$$

On the other hand, $I = g_n^0, g_n, g_n^2, \cdots, g_n^{k-1}$ are different members of $Aut_K\mathbb{Q}(\zeta_p)$, since $g_n^i(r_j) = r_j$ for any $i = 0, 1, \cdots, k-1$ and $j = 0, 1, \cdots, n-1$. Also, $g_n^i(\zeta_p) = \zeta_p^{2^{i\cdot n}}$ for $i = 0, 1, \cdots, k-1$, thus $g_n^i$ $(i = 0, 1, \cdots, k-1)$ differ. Therefore,

$$|Aut_K\mathbb{Q}(\zeta_p)| \geq n \tag{2}$$

Since $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_p)$ and $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ is a Galois extension. Thus $K \subset \mathbb{Q}(\zeta_p)$ is a Galois extension, meaning $[\mathbb{Q}(\zeta_p) : K] = |Aut_k\mathbb{Q}(\zeta_p)|$.

By the spyglass property and (1),(2), we can show that $nk = p-1 = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = [\mathbb{Q}(\zeta_p) : K] \cdot [K : \mathbb{Q}] = |Aut_k\mathbb{Q}(\zeta_p)| \cdot |Aut_{\mathbb{Q}}K| \geq nk$, thus the inequation is taken as equal, that is $[K : \mathbb{Q}] = n$.

**Claim 19** *$Aut_{\mathbb{Q}}K \simeq \mathbb{Z}_n$.*

*Proof.* From the proof of the previous claim, we have $Aut_{\mathbb{Q}}K = \{Id, g_k, g_k^2, \cdots, g_k^{n-1}\}$ is cyclic. So clearly $Aut_{\mathbb{Q}}K \simeq \mathbb{Z}_n$.

From the claims above, we conclude that for any given $n \in \mathbb{N}$, we can find a field $K$ such that $\mathbb{Q} \subset K$ is a Galois extension and $Aut_{\mathbb{Q}}K \simeq \mathbb{Z}_n$.

# 4 The 5 Groups of order 8

**Theorem 20** [5] *All groups of order* 8 *are Galois groups over* $\mathbb{Q}$

*Proof.* We know that there are only 5 groups of order 8. We will divide them into abelian and non-abelian groups, and prove that they are all Galois.

## 4.1 Abelian groups

The Abelian groups are:

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

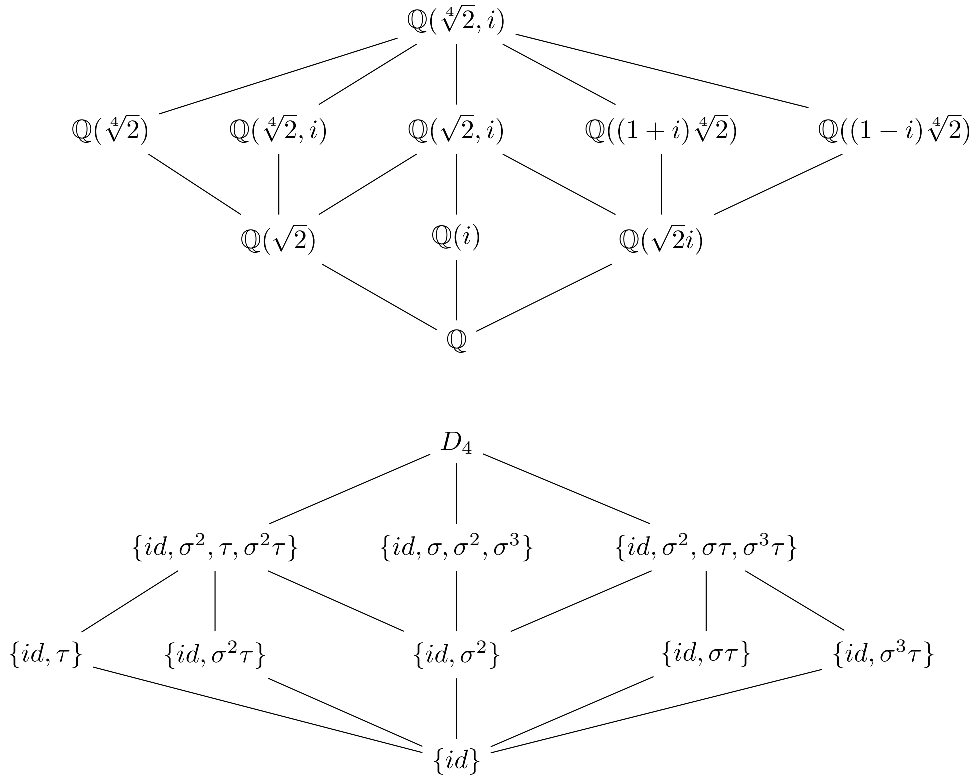
For 1, $\mathbb{Z}/8\mathbb{Z}$ is Galois as shown in Theorem 8.
For 2, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \simeq (\mathbb{Z}/15\mathbb{Z})^* \simeq Gal\,(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$.
For 3, $\mathbb{Z}/2\mathbb{Z}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

## 4.2 Non-abelian groups

The non-abelian groups are:

1. $D_8 \coloneqq \langle \sigma, \tau : \sigma^4 = \tau^2 = e, \sigma\tau\sigma = \tau^{-1} \rangle$
2. $Q_8 \coloneqq \langle \sigma, \tau : \sigma^4 = e, \sigma^2 = \tau^2, \tau\sigma = \sigma\tau^3 \rangle$

For $D_8$, we consider the field extension $\mathbb{Q}(\sqrt[4]{2}, i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i)$. Because all the solutions and only the solutions of the minimal polynomial $x^4 - 2$ are included in the field, so by Crucial Property Number 0 of Galois Theory(The roots, all the roots, nothing but the roots), $\mathbb{Q}(\sqrt[4]{2}, i)$ is Galois. Lastly, consider all the automorphisms of the field, which are $\sigma : \sigma(\sqrt[4]{2}) = i\sqrt[4]{2}$ and $\tau : \tau(i) = -i$. Because $\sigma\tau\sigma = \tau^{-1}$, so by definition $Gal(\mathbb{Q}(\sqrt[4]{2}, i)/\mathbb{Q}) = D_8$.


$\mathbb{Q}(\sqrt[4]{2}, i)$
$\mathbb{Q}(\sqrt[4]{2})$
$\mathbb{Q}(\sqrt[4]{2}, i)$
$\mathbb{Q}(\sqrt{2}, i)$
$\mathbb{Q}((1+i)\sqrt[4]{2})$
$\mathbb{Q}((1-i)\sqrt[4]{2})$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(i)$
$\mathbb{Q}(\sqrt{2}i)$
$\mathbb{Q}$
$D_4$
$\{id, \sigma^2, \tau, \sigma^2\tau\}$
$\{id, \sigma, \sigma^2, \sigma^3\}$
$\{id, \sigma^2, \sigma\tau, \sigma^3\tau\}$
$\{id, \tau\}$
$\{id, \sigma^2\tau\}$
$\{id, \sigma^2\}$
$\{id, \sigma\tau\}$
$\{id, \sigma^3\tau\}$
$\{id\}$

The field extension and corresponding group diagram of $D_8$. Notice that the correspondence is flipped upside down.

For $Q_8$, Consider the field extension $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and $L = K\left(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right)$.

**Claim 21** $[L : \mathbb{Q}] = 8$

*Proof.* By the spyglass property, $[L : \mathbb{Q}] = [L : K] \times [K : \mathbb{Q}]$. Also, we know that $[K : \mathbb{Q}] = 4$ since the minimal polynomial is $(x^2 - 2)(x^2 - 3)$.

To compute $[L : K]$, we first notice that $P(x) = x^2 - (2+\sqrt{2})(3+\sqrt{3}) \in K[x]$ and $P\left(\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right) = 0$. Therefore, the degree of the extension $[L : K]$ will be at most 2. We now will show that the degree is indeed 2 by counterproof.

If the degree is 1, then $\mu(x) = x - \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \in K[x]$, so $\sqrt{(2+\sqrt{2})(3+\sqrt{3})} \in K$. Then, $\sqrt{(2+\sqrt{2})(3+\sqrt{3})} = a + b\sqrt{3}$ where $(a, b) \in \mathbb{Q}^2(\sqrt{2})$. Squaring both sides, we deduce

$$\begin{aligned}(2+\sqrt{2})(3+\sqrt{3}) &= a^2 + 2\sqrt{3}ab + 3b^2 \\ \sqrt{3}(2+\sqrt{2}) + 6 + 3\sqrt{2} &= a^2 + 2\sqrt{3}ab + 3b^2 \\ \sqrt{3}(2+\sqrt{2} - 2ab) &= a^2 + 3b^2 - 6 - 3\sqrt{2} \\ \sqrt{3} &= \frac{a^2 + 3b^2 - 6 - 3\sqrt{2}}{2+\sqrt{2} - 2ab}\end{aligned}$$

Notice that $\frac{a^2 + 3b^2 - 6 - 3\sqrt{2}}{2+\sqrt{2} - 2ab} \in \mathbb{Q}(\sqrt{2})$, which implies that $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, a false statement. We have reached a contradiction, so the assumption is wrong, and hence the degree of $[L : K]$ is 2. By the spyglass property, $[L : \mathbb{Q}] = [L : K] \times [K : \mathbb{Q}] = 2 \times 4 = 8$.

**Claim 22** $P(x) = \prod_{\epsilon_1, \epsilon_2 \in \pm 1} (x - (2 + \epsilon_1\sqrt{2})(3 + \epsilon_2\sqrt{3})) \in \mathbb{Q}[x]$

*Proof.* By Crucial Property Number 0 of Galois Theory (The roots, all the roots, nothing but the roots), $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is a Galois extension. By Crucial Property Number 2 of Galois Theory (Things that don't move are rare), this implies that $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3})} = \mathbb{Q}$.

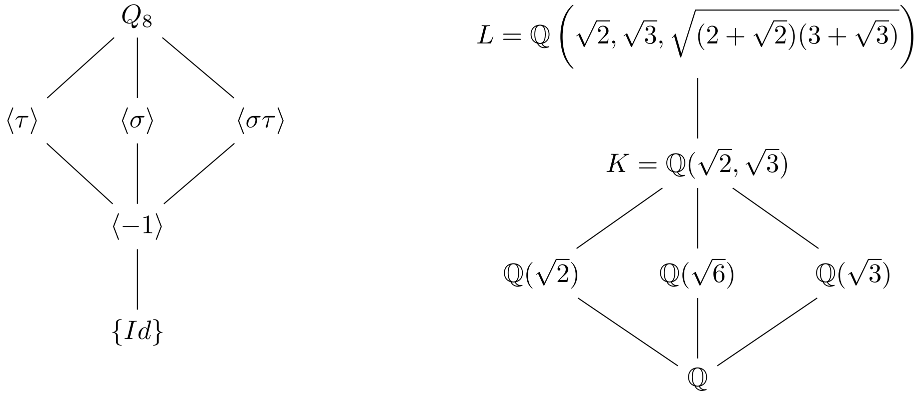
We know that $Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{Id, g_1, g_2, g_1g_2\}$ where $g_1 : \sqrt{2} \mapsto -\sqrt{2}, g_2 : \sqrt{3} \mapsto -\sqrt{3}$. Also, $\alpha \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ will have the form $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ where $(a, b, c, d) \in \mathbb{Q}^4$. Then, $g_1(\alpha) = a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}, g_2(\alpha) = a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}$. Notice that $g_1(P(x)) = g_2(P(x)) = P(x)$, which implies that its coefficients are in $\mathbb{Q}(\sqrt{2}, \sqrt{3})^{Aut_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3})} = \mathbb{Q}$.

Consider

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

Then, $P(x^2)$ is the minimal polynomial of $\sqrt{(2+\sqrt{2})(3+\sqrt{3})}$ over $\mathbb{Q}$. By Crucial Property Number 0 of Galois Theory (The roots, all the roots, nothing but the roots), this extension is Galois.

Consider the automorphisms $\tau : \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$ and $\sigma : \sqrt{(2+\sqrt{2})(3+\sqrt{3})} \mapsto \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$. Then we can check that $\sigma\tau = \tau\sigma^3$, where $\tau$ and $\sigma$ has order 4, and also it is not abelian, that is to say $\tau\sigma \neq \sigma\tau$. Therefore, by definition, $Gal\left(\mathbb{Q}\left(\sqrt{2}, \sqrt{3}, \sqrt{(2+\sqrt{2})(3+\sqrt{3})}\right)/\mathbb{Q}\right) \simeq Q_8$.



The field extension and corresponding group diagram of $Q_8$. Similarly, notice that the correspondence is flipped upside down.

## 5 Conclusion

Although the Inverse Galois Problem is still an open problem in Mathematics, in this article we have proved that some groups have a corresponding field extension. We can do this by using the three steps as stated above. Firstly, construct a field extension. Secondly, prove that the field extension is Galois. Lastly, show that the automorphism group is isomorphic to the desired group.

## 6 Acknowledgements

We would like to extend our deepest gratitude to our professor, **Dr. Olivier Fouquet** from the Université de Franche-Comté, for teaching us the course on Algebra and Number Theory at Yau Mathcamp 2024 with such enthusiasm, thoroughness, and engaging teaching methods. Our heartfelt appreciation also goes out to our coaches, **Estelle Basset** and **Arthur Gerald**, as well as to the Yau Mathcamp organizers, **Shing-Tung Yau** and **Bong Lian**. The support and guidance of these individuals were indispensable for our work.

# References

[1] Ben Lynn, Eisenstein's Irreducibility, Stanford University.

[2] Samuel Moy, An Introduction to the Theory of Field Extensions, University of Chicago.

[3] Keith Conrad, Proof of Cauchy's Theorem, University of Connecticut.

[4] Ang Li, Dirichlet's Theorem About Primes in Arithmetic Progressions, University of Chicago.

[5] Ben Lynn, Groups Up To Order Eight, Stanford University.