A BRIEF SURVEY ON THE INVERSE GALOIS PROBLEM

Bigyan Adhikari, Tulasi Prasad Nepal*
Central Department of Mathematics, Tribhuvan University, Kritipur, Kathmandu
*Corresponding author: tpnepal1@gmail.com

(Received: October 24, 2021; Revised: March 19, 2022; Accepted: March 27, 2022)

ABSTRACT

Inverse Galois problem (IGP) states whether any finite group is realizable as a Galois group over the field $K$. It is the question of the structure and representation of the Galois group and also questions its epimorphic images. So, it is called an inverse Galois problem. For $K=\mathbb{Q}$ (the field of rational number), it is called a classical inverse Galois problem (CIGP). This paper reviews the positive answer to the classical inverse Galois problem (CIGP) for all finite abelian groups and some finite non-abelian solvable groups. We also discuss this problem (CIGP) for some finite non-solvable groups in this paper. This problem still remains to solve, but if we find the true value of the statement 'All subgroups of order $m$ of the symmetric group $S_m$ for all $m$ are realizable as Galois group over $\mathbb{Q}$' then its truth value gives the answer of CIGP. We check this statement for $m=1,2,3,4$ and 5 in this paper, where we get that this statement is true. If this statement is true, then CIGP has a positive answer. But if this statement is false then CIGP has a negative answer.

Keywords: Abelian group, Galois group, Galois extension, irreducible polynomial, solvable group

INTRODUCTION

Evariste (Adams, 2010) Galois was born on October 25, 1811, in France. He was the first son of Nicholas Gabriel Galois and Adelaide Marie Demante. Evariste Galois was a political activist as well as a mathematician by whom necessary and the sufficient condition for polynomial to be solvable by the radicals had been found. He is known as the creator of Galois theory because he developed basic theory which links group theory and field theory. He did all his remarkable works in the field of mathematics when he was teenager. We have to say with dejection that he passed away at his tender age. One of the disasters in the scientific world was the loss of the great intelligent mathematician Evariste Galois at his tender age. His life was not happy one because his new mathematical concepts were not got liking by anyone during his brief lifetime and he faced rejection everywhere. His theory is one of the revolutionary concepts of mathematics, but his theory was neither accepted nor noticed during his brief life time. So, his struggleful life always motivates us for studying Galois theory.

Inverse Galois problem (Jensen et al., 2002) (IGP) asks us that whether every finite group is realizable as Galois group over the field $K$. On another word, it asks us that if there exists Galois extension $N$ over $K$ such that a finite group $T$ is isomorphic to the Galois group $Ga(N;K)$. It is the question on structural and representation of Galois group and question on its epimorphic images. So, it is called as inverse Galois problem. If we take field $K$ as field of rational number, then IGP is called as classical inverse Galois problem (CIGP). The classical inverse Galois problem developed early in 19th century during studying polynomials and roots.

(Hanlock, 1978; Jensen et al., 2002) Hilbert began systematic study of CIGP and he presented it early in 19th century. It still remains to solve but some of its partial results have been derived. Hilbert firstly stated Hilbert irreducibility theorem and proved it in 1892 A.D. He used this theorem to prove CIGP for all symmetric groups and alternating groups. Thus, he solved classical inverse Galois problem for symmetric groups and alternating groups in 1892 A.D by using of Hilbert irreducibility theorem.

Kronecker firstly stated Kronecker-Weber theorem in 1853 A.D (Washington, 1982). But his proof was incomplete. In 1886 A.D, Weber proved this theorem, but his proof had also some gap. In 1896 A.D, Hilbert proved Kronecker-Weber Theorem. Hence, he proved CIGP for all finite abelian groups.

Shafarevich's theorem (Shafarevich, 1954; Shafarevich, 1989) states that every finite solvable group is realizable as Galois group over $\mathbb{Q}$. Shafarevich proved this theorem in 1954 A.D. But Alexander Schmidt pointed out a gap in his proof which was fixed by Shafarevich in 1989 AD. Hence, he solved classical inverse Galois problem for all finite solvable groups. So, mathematicians started to look over CIGP for finite non-solvable groups where they got positive answer of CIGP for particularly many non-solvable groups such as $A_m, m>4$ and $S_m, m > 4$, Sporadic groups etc. but it remains to know the answer of this CIGP for many finite non-solvable groups such as Mathieu group $M_{23}$.

MATERIALS AND METHODS

Definition 1 (Gallian, 2015) A group $T$ is said to be solvable if $T$ has a series of the subgroups of $T$ i.e. $\{e\} = \ldots \leq H_1 \leq H_2 \leq \ldots \leq H_k = T$ with $H_{i+1}$ being a normal subgroup of $H_i$, and $H_i/H_{i+1}$ being a solvable group for $i = 1, 2, \ldots, k-1$. $T$ is said to be non-solvable if $T$ does not satisfy the Definition 1.
Definition 2 (Gallian, 2015) Let $m$ be a positive integer and for $i = 1, 2, \ldots, k$, $s_i (s_i < m)$ is a positive integer which is relatively prime to $m$. A cyclotomic polynomial $\varphi_m(t)$ of degree $k$ is defined by

$$
\varphi_m(t) = \prod_{i=1}^{k} (t - \kappa^{s_i})
$$

Where $\kappa = e^{2\pi i/m}$

Theorem 3 (Gallian, 2015) Let $y(t) \in \mathbb{I}[t]$. If $y(t)$ be an irreducible over $\mathbb{I}$ then $y(t)$ be an irreducible over $\mathbb{Q}$.

Theorem 4 (Gallian, 2015) Let $\varphi_m(t)$ be any cyclotomic polynomial. Then $\varphi_m(t)$ is irreducible over $\mathbb{I}$.

Theorem 5 (Gallian, 2015) Let $T$ be an abelian group of order $m$. If $d$ divide integer $m$ then there exists subgroup of order $d$.

Theorem 6 (Neukirch, 1999) For every positive integer $m$, there exists infinitely many primes $q$ such that $q \equiv 1 \mod m$.

Definition 7 (Gallian, 2015) Suppose $X$ be a set of $m$ distinct objects. Now, the set of all bijective mappings defined on the set $X$ forms a group under composition of mapping operation ($\circ$). This group is called as finite symmetric group of order $m!$. It is denoted $S_m$.

Definition 8 (Gallian, 2015) The set of all even permutation $\sigma \in S_m$ forms a group under same binary operation as defined in $S_m$. This group is called as alternating group. It is denoted by $\text{A}_m$. Its order is $\frac{m!}{2}$.

Definition 9 (Bhattacharya et al., 1994) The function $\frac{x(s_1, s_2, \ldots, s_m)}{y(s_1, s_2, \ldots, s_m)}$ is called as symmetric function of indeterminates $s_1, s_2, \ldots, s_m$ over $K$ if for all $\sigma \in S_m$, there is $K$-automorphism mapping $\sigma : K(s_1, s_2, \ldots, s_m) \rightarrow K(s_1, s_2, \ldots, s_m)$, $\sigma \in S_m$ such that

$$
\sigma \left( \frac{x(s_1, s_2, \ldots, s_m)}{y(s_1, s_2, \ldots, s_m)} \right) = \frac{x(\sigma(s_1), \sigma(s_2), \ldots, \sigma(s_m))}{y(\sigma(s_1), \sigma(s_2), \ldots, \sigma(s_m))} = x(s_1, s_2, \ldots, s_m)/y(s_1, s_2, \ldots, s_m)
$$

Definition 10 (Bhattacharya et al., 1994) Suppose $c_1$ be the coefficient of term $t^{m-1}$ in the polynomial

$$
x(t) = \prod_{i=1}^{l} (t - s_i)
$$

by $l_i = s_1 + s_2 + \cdots + s_{m_i}$, $l_2 = s_1s_2 + \cdots + s_1s_{m-1}s_{m}$, $\ldots$, $l_m = s_1 \cdots s_{m-1}s_{m}$.

Theorem 11 (Bhattacharya et al., 1994) Let $x(t)$ be a polynomial of some finite degree over field $K$ having $m$ distinct roots in the splitting field $N$. Then, $\text{Ga}(N: K)$ is isomorphic to the subgroup of $S_m$.

Theorem 12 (Bhattacharya et al., 1994) $x(t)$ is separable and irreducible polynomial of degree $m$ over $K$ if and only if Galois group of this polynomial over $K$ is isomorphic to transitive subgroup of $S_m$.

Theorem 13 (Handlock, 1978; Jensen et al., 2002) Let $K$ be the finite extension field of $Q$. Suppose $x(t) \in K(t)[t] = E(t)$ is an irreducible polynomial, with indeterminates $l = (t_1, \ldots, t_m)$. Let $N$ be the splitting field for polynomial $x(t, l) \in K[l]$ then there exist infinitely many $\alpha = (a_1, a_2, \ldots, a_m) \in K^m$ such that the specialization $x(t, \alpha) \in K[t]$ is well defined and irreducible over $K_\alpha$ and can be chosen so that $\text{Ga}(N : E) \cong \text{Ga}(N' : K)$, where $N'$ is the splitting field extension for $x(t, \alpha) \in K[t]$. This theorem is known as Hilbert irreducibility theorem.

Definition 14 (Jensen et al., 2002) Suppose that a polynomial over field $K$ is $x(t) = a_m t^m + a_{m-1} t^{m-1} + \cdots + a_0$ and $x(t) = ma_m t^m - m + a_1$ is the derivative of the given polynomial, then discriminant of polynomial $x(t)$ is given by

$$
disc(x(t)) = \frac{(-1)^{m(m-1)/2} \text{Res}(x(t), x'(t))}{a_m}
$$

where $\text{Res}(x(t), x'(t))$ is resultant of $x(t)$ and $x'(t)$ which is obtained by finding the determinant of Sylvester matrix

$$
\begin{vmatrix}
\alpha_m & \alpha_{m-2} & \cdots & \alpha_2 & \alpha_1 & 0 & \cdots & 0 \\
0 & \alpha_m & \alpha_{m-2} & \cdots & \alpha_2 & \alpha_1 & \cdots & 0 \\
0 & 0 & \alpha_m & \cdots & \alpha_2 & \alpha_1 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\end{vmatrix}
$$

Theorem 15 (Jensen et al., 2002) Suppose $x(t) \in K(t)$ separable polynomial over its splitting field $N$ and degree of polynomial $x(t)$ is $m$ then $\text{Ga}(N : K)$ is the subgroup of $A_m$ iff discriminant of polynomial $x(t)$ is perfect square in $K$.

Fundamental Theorem of Galois Theory 16 (Gallian, 2015) Let us suppose $K$ is a field with characteristics 0 or a finite field. If $N$ be the splitting field for some polynomial $x(t) \in K[t]$. Then the mapping from the set of subfields of $N$ containing $K$ to the set of subgroups of $\text{Ga}(N : K)$ is
given by $M \rightarrow \text{Gal}(N:M)$ is one to one correspondence. For any subfield $M$ of $N$ containing $K$,


b) If $M$ is the splitting field of some polynomial over $K$, then $\text{Gal}(N:M)$ is normal subgroup of $\text{Gal}(N:K)$ and $\text{Gal}(M:K)$ is isomorphic to $\frac{\text{Gal}(N:K)}{\text{Gal}(N:M)}$.

c) $M = \text{Gal}(N:M)$.

d) If $S$ is the subgroup of $\text{Gal}(N:K)$ then $S = \text{Gal}(N:N_k)$.

**Theorem 17** (Gallian, 2015) Every finite group $T$ is isomorphic to the subgroup of symmetric group $S_m$.

**Definition 18** (Griess, 1998) A finite non-abelian simple sporadic group of order 1020960 acts transitively on set of 23 objects is called $M_{23}$.

**Lemma 19** (Gallian, 2015) $\text{Gal}(q(\bar{q})/Q) \cong \mathbb{I}_n$.

**RESULTS**

**Theorem 20** Every group of prime order is realizable as Galois group over the field of rational number.

Proof: Suppose $T$ be a group of prime order $p$. Suppose $a \in T$. By Lagrange theorem, $|a|$ divides $|T|$. So, $|a|$ must be either 1 or $p$. We suppose that $a$ is not identity element. So, $|a| = p$. Hence, $T$ is a cyclic group. So, $T \cong \mathbb{I}_p$. Since $p$ is integer. By theorem 6, there exists prime $q$ such that $q - 1 = p \times m$. Suppose $\kappa$ be the primitive $q^{th}$ root of unity. By theorem 19, Galois group of $q(\bar{q})(t)$ over $Q$ is $\text{Gal}(\mathbb{Q}(\kappa):Q) \cong \mathbb{I}_{q^k}$. Since $q - 1 = p \times m$. By theorem 5, there exists subgroup $S$ of order $m$ of abelian group $\text{Gal}(\mathbb{Q}(\kappa):Q) \cong \mathbb{I}_{q^k}$. By fundamental theorem of Galois theory, there exists an intermediate field $L$ such that $\text{Gal}(L:Q) \cong \frac{\text{Gal}(\mathbb{Q}(\kappa):Q)}{S}$ which is cyclic group of order $p$. Hence $\text{Gal}(L:Q) \cong \mathbb{I}_p \cong T$.

**Theorem 21** (Washington, 1982) Every finite abelian group $T$ is realizable as Galois group over the field of rational number.

Proof: Suppose $T$ be a finite abelian group of order $m$. By fundamental theorem of finite abelian group, $T \cong C_{m_1} \times C_{m_2} \times \ldots \times C_{m_k}$ and $m = m_1 m_2 \ldots m_k$. By theorem 6, for each $m_i$, there exists distinct prime $q_i$ such that $q_i - 1 = m_i d_i$. We know that $\mathbb{I}_{q_i}$ is the cyclic group of order $q_i - 1$. Here $d_i$ divides $q_i - 1$. By theorem 5, there exists subgroup $T_i$ of order $d_i$ of $\mathbb{I}_{q_i}$. Hence $\frac{T_i}{d_i} \cong C_{m_i}$.

Suppose $\kappa_i$ be the primitive $q_i^{th}$ root of unity and set $\kappa = \kappa_1 \kappa_2 \ldots \kappa_k$ then it is primitive $(q_1 q_2 \ldots q_k)^{th}$ root of unity. By theorem 19, $\text{Gal}(\mathbb{Q}(\kappa):Q) \cong \mathbb{I}_{q_i}$. By Chinese remainder theorem, $I_m = I_{m_1 m_2 \ldots m_k} \cong I_{m_1} \times I_{m_2} \times \ldots \times I_{m_k}$ which implies that $I_{q_i} \cong (I_{m_1} \times I_{m_2} \times \ldots \times I_{m_k})^\times \cong I_{q_1}^\times \times I_{q_2}^\times \ldots \times I_{q_k}^\times$. $\text{Gal}(\mathbb{Q}(\kappa):Q) \cong \mathbb{I}_{q_1} \times \mathbb{I}_{q_2} \times \ldots \times \mathbb{I}_{q_k}$ is abelian group of order $(q_1 - 1)(q_2 - 1)(q_k - 1)$. Here $md = (q_1 - 1)(q_2 - 1)(q_k - 1)$. If we have $d_1 d_2 \ldots d_k = d$ then $m_1 m_2 \ldots m_k = m$ and $m_1 d_1 = q_1 - 1$ for each $i$. By theorem 5, there exists subgroup $S$ of order $d$ of $\text{Gal}(\mathbb{Q}(\kappa):Q)$ and by fundamental theorem of Galois theory, there exist fixed field $N$ such that $\text{Gal}(N:Q) \cong \frac{\text{Gal}(\mathbb{Q}(\kappa):Q)}{S}$. Here, we have $\text{Gal}(\mathbb{Q}(\kappa):Q) \cong \mathbb{I}_{q_1} \times \mathbb{I}_{q_2} \times \ldots \times \mathbb{I}_{q_k}$ and $S$ is the normal subgroup of $\text{Gal}(\mathbb{Q}(\kappa):Q)$. So, there exists normal subgroup $T_1 \times T_2 \times \ldots \times T_k$ of $\mathbb{I}_{q_1} \times \mathbb{I}_{q_2} \times \ldots \times \mathbb{I}_{q_k}$ such that $T_1 \times T_2 \times \ldots \times T_k \cong S$ and each $T_i$ is normal subgroup of abelian group $\mathbb{I}_{q_i}$. Now, $\text{Gal}(N:Q) \cong \frac{\text{Gal}(\mathbb{Q}(\kappa):Q)}{S} \cong \frac{\mathbb{I}_{q_1} \times \mathbb{I}_{q_2} \times \ldots \times \mathbb{I}_{q_k}}{T_1 \times T_2 \times \ldots \times T_k} \cong C_{m_1} \times C_{m_2} \times \ldots \times C_{m_k}$. By Proposition 22 It is false that Galois group of every polynomial $y(t) \in \mathbb{Q}[t]$ over $Q$ is abelian group.

Proof: Yes, it is false that Galois group of every polynomial over $Q$ is abelian because there exists some polynomial polynomial over $Q$ whose Galois group over $Q$ is non-abelian. For example, the Galois group of polynomial $y(t) = t^4 + 5$ over $Q$ is $\text{Gal}(\mathbb{Q}(\sqrt[4]{5}):Q) \cong D_8$. Since $D_8$ is not abelian. So, Galois group of $y(t) = t^4 + 5$ over $Q$ is not abelian. Thus, there exists non-abelian Galois group $\text{Gal}(\mathbb{Q}(\sqrt[4]{5}):Q) \cong D_8$. So, it false that Galois group of every polynomial over $Q$ is abelian group.

**Theorem 23** (Shafarevich, 1954) All finite solvable groups are realizable as Galois group over the field of rational number.

Verification: Let's separate all solvable groups into abelian groups and non-abelian solvable groups. By theorem 21, all abelian groups appear as Galois group over the field of rational number. Now, we have to show that all non-abelian solvable groups appear as Galois group over the field of rational number. But here we just verify this theorem for only some non-abelian solvable groups $D_8$ and $S_3$. $S_3$ is nonabelian but it is solvable group because we have $S_3 \subset A_4 \subset \{e\}$, where each composition factor is abelian. Let us take the polynomial $x(t) = t^3 + 2t + 2$. By Eisenstein’s criterion of irreducibility of polynomial, $x(t) = t^3 + 2t + 2$ is irreducible polynomial over $Q$. $x'(t) = 3t^2 + 2$ and its roots are $\pm \frac{\sqrt{3}}{3}$ which are not
roots of polynomial $x(t)$. So, it is separable polynomial of degree 3. By theorem 12, the Galois group of this polynomial over the field of rational number is isomorphic to transitive subgroup of $S_3$. The transitive subgroup of $S_3$ is either $A_3$ or $S_3$. Here, discriminant of this polynomial is 140 which is not perfect square in $\mathbb{Q}$. So, Galois group of this polynomial $x(t) = t^3 + 2t + 2$ over $\mathbb{Q}$ is isomorphic to $S_3$, otherwise it contradicts theorem 15.

Again, $D_8$ is nonabelian. But it is solvable group because we have $D_8 \subset V_4 \subset \{e\}$ where each composition factor $\frac{D_8}{V_4} \cong \mathbb{I}_2$ and $\frac{V_4}{\{e\}} \cong V_4$ are abelian group. The Galois group of polynomial $y(t) = t^4 + 5$ over $\mathbb{Q}$ is $Ga(\mathbb{Q}(2^2, i)) \cong D_8$.

**Proposition 24** It is false that Galois group of every polynomial over $\mathbb{Q}$ is solvable group.

Proof: To prove this, we have to show that there exists at least one polynomial over $\mathbb{Q}$ whose Galois group over $\mathbb{Q}$ is non-solvable group. $S_7$ is non-solvable group because there is normal series of subgroups of $S_7$ i.e., $S_7 \subset A_7 \subset \{e\}$, where composite factor $\frac{A_7}{\{e\}} \cong A_7$ is not abelian. $S_7$ is realizable as Galois group over $\mathbb{Q}$ because the Galois group [see in details in Bhattacharya et al. (1994)] of polynomial $x(t) = t^7 - 10t^5 + 15t + 5$ over $\mathbb{Q}$ is isomorphic to $S_7$ which is not solvable group. Here exists non-solvable Galois group over the field of rational number. Thus, Galois group of some polynomials over $\mathbb{Q}$ are not solvable but all solvable are realizable as Galois group over $\mathbb{Q}$.

**Theorem 25** (Bhattacharya et al., 1994; Handlock, 1978) Every finite symmetric group is realizable as Galois group over the field of rational number.

Proof: Let us construct $x(t, l) = \prod_{i=1}^{m+1}(t - s_i)$, where $l = (l_1, l_2, ... , l_m)$ be the elementary symmetric function in $s_1, s_2, ... , s_m$ over $\mathbb{Q}$. Suppose that $L$ be the set of all elementary symmetric function of $s_1, s_2, ... , s_m$ over $\mathbb{Q}$ and $E$ be the field of rational function which is generated by $l_1, l_2, ... , l_m$ over $\mathbb{Q}$. All elementary symmetric functions $l_i \in L$. So, we get $E \subset L$. Suppose $N$ be the splitting field of polynomial $x(t, l)$ over $E$. Here, $N$ is separable, normal and finite extension over $E$. So, $N$ is Galois extension field over $E$. By fundamental theorem of Galois theory, $[Ga(N:E)] = [N:E]$. By definition of symmetric function, $L$ is fixed field of group $S_m$ where $S_m$ is the group of $\mathbb{Q}$-automorphism mappings defined on $N$. So, $[N:L] \geq [S_m] = m!$. But we have $[N:E] \leq m!$ and $E \subset L$. So, we get $E = L$ and $[N:E] = m!$. Hence, we get $[Ga(N:E)] = [N:E] = m!$. By theorem 11, $Ga(N:E)$ is isomorphic to the subgroup of $S_m$. But we find that $[Ga(N:E)] = m!$. So, we get $Ga(N:E) \cong S_m$. We know that $S_m$ is transitive subgroup of $S_m$. So, $x(t, l)$ is irreducible polynomial over $E$. By Hilbert irreducibility theorem, there exists $a \in \mathbb{Q}^m$ and irreducible polynomial $x(t, a) \in \mathbb{Q}(t)$ such that $Ga(N:E) \cong Ga(N': \mathbb{Q})$ where $N'$ is the splitting field of $x(t, a)$ over $\mathbb{Q}$. Hence, $Ga(N': \mathbb{Q}) \cong S_m$.

**Proposition 26** (Jensen et al., 2002) The discriminant of polynomial $x(t) = t^m + at + a$ over $\mathbb{Q}$ is $(-1)^{\frac{m(m-1)}{2}}a^{m-1}(a(1-m)m^{-1} + m^m)$.

Proof: We have $\det(Syl)$, where we have

$$
\begin{pmatrix}
1 & \ldots & 0 & a & 0 & 0 & 0 & \ldots & 0 \\
0 & 1 & \ldots & 0 & a & 0 & 0 & \ldots & 0 \\
0 & 0 & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots & a \\
0 & 0 & \ldots & 0 & m & 0 & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & m & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & m & 0 \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & m
\end{pmatrix}
$$

Here, we find the determinant of this matrix $Syl$. At first step, we apply $C_m \leftrightarrow C_m - aC_1$ and $C_{m+1} \leftrightarrow C_{m+1} - aC_1$ on determinant matrix of $Syl$. So, we get

$$
\begin{pmatrix}
1 & \ldots & 0 & 0 & a & 0 & a & 0 & 0 \\
0 & 1 & \ldots & 0 & a & 0 & a & 0 & 0 \\
0 & 0 & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots & a \\
0 & 0 & \ldots & 0 & m & 0 & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & m & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & m & 0 \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & m
\end{pmatrix}
$$

then we expand it along $R_1$. So, we get

$$
\begin{pmatrix}
1 & \ldots & 0 & 0 & a & 0 & a & 0 & 0 \\
0 & 1 & \ldots & 0 & a & 0 & a & 0 & 0 \\
0 & 0 & \ddots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\
0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots & a \\
0 & 0 & \ldots & 0 & a & 0 & a & 0 & 0 \\
0 & 0 & \ldots & 0 & m & 0 & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & m & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & m & 0 \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & m
\end{pmatrix}
$$

We do this same process up to $(m-1)^{th}$ step as we did at first step. Now, we get that $\det(Syl) = \begin{vmatrix}
a - ma & -ma & \ldots & 0 & 0 \\
0 & a - ma & -ma & \ldots & 0 \\
0 & 0 & \ddots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots & a - am - am \\
0 & 0 & \ldots & 0 & a & 0 & a & 0 & 0 \\
0 & 0 & \ldots & 0 & m & 0 & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & m & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & m & 0 \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & m
\end{vmatrix}$

We expand it along $C_1$. So, we get

$$
\begin{pmatrix}
a - am & -ma & \ldots & 0 & 0 \\
0 & a - ma & -ma & \ldots & 0 \\
0 & 0 & \ddots & \vdots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & 0 & \ldots & 1 & 0 & 0 & 0 & \ldots & a - am - am \\
0 & 0 & \ldots & 0 & a & 0 & a & 0 & 0 \\
0 & 0 & \ldots & 0 & m & 0 & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & m & \ldots & 0 & a \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & m & 0 \\
0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 & m
\end{pmatrix}
$$

We get $\det(Syl) = (a-am)$.
\[ \det(syl) = a(a - am)^{m-1} + (-1)^{m+1}m(-am)^{m-1} = a^{m-1}(a(1 - m)^{m-1} + m^m) \]

By definition 14, \( \text{disc}(x(t)) = \left(-1\right)\frac{m(m-1)}{2}a^{-m-1}(a(1 - m)^{m-1} + m^m) \).

**Theorem 27** (Jensen et al., 2002) All alternating group are realizable as a Galois group over \( \mathbb{Q} \).

Proof: The Galois group of a polynomial \( x(t, l) = t^m + lt + l \) over \( \mathbb{Q}(l) \) is isomorphic to \( S_m \) [its proof is in (Jensen et al., 2002)]. Suppose \( N \) be the splitting field of this polynomial over \( \mathbb{Q}(l) \). By proposition 26, the discriminant of \( x(t, l) \) is \( \left(-1\right)\frac{m(m-1)}{2}l^{-m-1}(l(1 - m)^{m-1} + m^m) \).

When \( m \) is a positive odd number, \( \sqrt{\text{disc}(x(t, l))} = \frac{m^{-1}}{l^{\frac{1}{2}}} \sqrt{\left(-1\right)\frac{m(m-1)}{2}(l(1 - m)^{m-1} + m^m)} \) and \( l^{\frac{1}{2}} \in \mathbb{Q}(l) \) but \( w = \sqrt{\left(-1\right)\frac{m(m-1)}{2}(l(1 - m)^{m-1} + m^m)} \) \( \notin \mathbb{Q}(l) \). \( \mathbb{Q}(l)(w) = \mathbb{Q}(w) \).

Now, put \( l = \frac{-1}{w^{2m^-2m^m}} \) in \( x(t, l) \).

Thus, we get a polynomial \( x_0(t, w) = t^m + \frac{m(m-1)}{2}w^{2m^m} \) \((t + 1)\) over \( \mathbb{Q}(l) \).

Now, this polynomial is perfect square in \( \mathbb{Q}(w) \). By theorem 15, \( Ga(N; \mathbb{Q}(w)) \) is isomorphic to the subgroup of \( A_m \). We have \( |Ga(N; \mathbb{Q}(l))| = m! \) and \( |Ga(\mathbb{Q}(N); \mathbb{Q}(l))| = 2 \). By fundamental theorem of Galois theory, we get \( \frac{|Ga(N; \mathbb{Q}(w))|}{m!} = |A_m| \). Hence, \( Ga(N; \mathbb{Q}(w)) \cong A_m \).

By Hilbert irreducibility theorem, there exists \( c \in \mathbb{Q} \) such that Galois group \( Ga(N_c; \mathbb{Q}) \) of irreducible polynomial \( x_0(t, c) \) over \( \mathbb{Q} \) is isomorphic to \( A_m \).

When \( m \) is positive even number, \( \sqrt{\text{disc}(x(t, l))} = \frac{m^{-1}}{l^{\frac{1}{2}}} \sqrt{\left(-1\right)\frac{m(m-1)}{2}(l(1 - m)^{m-1} + m^m)} \) and \( l^{\frac{1}{2}} \in \mathbb{Q}(l) \) but \( u = \sqrt{\left(-1\right)\frac{m(m-1)}{2}(l(1 - m)^{m-1} + m^m)} \) \( \notin \mathbb{Q}(l) \).

Now, \( \mathbb{Q}(l)(u) = \mathbb{Q}(u) \). Put \( l = \frac{m^{-1}}{u^{2(1-m)^{m-1}}} \) in \( x(t, l) \) then \( x_0(t, u) = u^m + \frac{m^{m-1}}{u^{(1-m)^{m-1}}} \) \((t + 1)\) is a polynomial over \( \mathbb{Q}(u) \). This discriminant of this polynomial is perfect square in \( \mathbb{Q}(u) \). By theorem 15, its Galois group \( Ga(N; \mathbb{Q}(u)) \) is isomorphic to the subgroup of \( A_m \). We have \( |Ga(N; \mathbb{Q}(l))| = m! \) and \( |Ga(\mathbb{Q}(N); \mathbb{Q}(l))| = 2 \). By fundamental theorem of Galois theory, we get \( |Ga(N; \mathbb{Q}(u))| = \frac{m!}{2} = |A_m| \). Hence, \( Ga(N; \mathbb{Q}(u)) \cong A_m \).

Hence, every alternating group is realizable as Galois group over the field of rational number.

**Statement 28**: All subgroups of order \( m \) of symmetric group \( S_m \) for all \( m \) are realizable as Galois group over the field of rational number.

**Verification**: For \( m = 1 \), it is trivially true.

For \( m = 2 \), subgroup of order 2 of \( S_2 \) is cyclic group of order two. The Galois group of Galois extension \( \mathbb{Q}(2^1) \) over \( \mathbb{Q} \) i.e., \( Ga(\mathbb{Q}(2^1); \mathbb{Q}) \) is isomorphic to cyclic group of order 2. It is true for \( m = 2 \).

For \( m = 3 \), subgroup (having order 3) of symmetric group \( S_3 \) is only one \( A_3 \). Let us take polynomial \( x_1(t) = t^3 - 3t + 1 \) over \( \mathbb{Q} \). By rational root test, its possible rational roots are \( \pm 1 \). But both are not roots of \( x_1(t) \). So, it has not rational root and it is the polynomial of degree 3. So, we get that this polynomial is irreducible over \( \mathbb{Q} \). This polynomial and its first derivative have not any common root. So, it is separable polynomial. The discriminant of this polynomial is 81 which is perfect square in \( \mathbb{Q} \). By theorem 12 and theorem 15, its Galois group over \( \mathbb{Q} \) is isomorphic to \( A_3 \). Thus, it is true for \( m = 3 \).

For \( m = 4 \), subgroups of order 4 of symmetric group \( S_4 \) are following

- \( \{(1), (12)(34), (13)(24), (14)(23)\} \cong V_4 \) is transitive subgroup of \( S_4 \).
- \( \{(1), (12), (34), (12)(34)\} \cong V_4 \), \( \{(1), (13), (24), (13)(24)\} \cong V_4 \) and \( \{(1), (14), (23), (14)(23)\} \cong V_4 \) are non-transitive subgroup of \( S_4 \).
- \( \{(1), (1234), (1432), (13)(24)\} \cong I_4 \), \( \{(1), (1243), (1342), (14)(23)\} \cong I_4 \) and \( \{(1), (1234), (1423), (12)(34)\} \cong I_4 \) are transitive subgroup of \( S_4 \).

Let us take polynomial \( x_2(t) = t^4 - 3t^2 + 4 \) over \( \mathbb{Q} \).
\[ x_2(t) = t^4 - 3t^2 + 4 = (t^2 + \sqrt{7}t + 2)(t^2 - \sqrt{7}t + 2) \]
\[ = (t + (\sqrt{7} + \frac{1}{2}))(t + (\sqrt{7} - \frac{1}{2}))(t - (\sqrt{7} + \frac{1}{2}))(t - (\sqrt{7} - \frac{1}{2})) \]
From this, we find that this polynomial is
separable and irreducible polynomial over \( \mathbb{Q} \), and its splitting field over \( \mathbb{Q} \) is \( \mathbb{Q}(\sqrt[7]{7}, i) \). We can define only four \( \mathbb{Q} \)-automorphism mappings on \( \mathbb{Q}(\sqrt[7]{7}, i) \): i.e.,

\[
\begin{align*}
\sigma: \sqrt[7]{7} & \rightarrow \sqrt[7]{7}, \\
t & \rightarrow -t \\
\tau: \sqrt[7]{7} & \rightarrow -\sqrt[7]{7}, \\
t & \rightarrow t \\
\sigma \circ \tau: \sqrt[7]{7} & \rightarrow -\sqrt[7]{7}, \\
t & \rightarrow -t \\
\text{And } id: \sqrt[7]{7} & \rightarrow \sqrt[7]{7}. \\
t & \rightarrow t
\end{align*}
\]

The Galois group \( Ga(\mathbb{Q}(\sqrt[7]{7}, i)): \mathbb{Q} = \{ \sigma, \tau, \sigma \circ \tau, id \} \) is isomorphic to \( V_4 \). By theorem 12, this Galois group over \( \mathbb{Q} \) is isomorphic to transitive subgroup \( V_4 \) of \( S_4 \). Let us take next another polynomial \( \chi_1(t) = t^4 - 3t^2 + 4 = (t^2 - 2)(t^2 - 3) \) over \( \mathbb{Q} \). This polynomial is reducible polynomial and separable over \( \mathbb{Q} \). The splitting field of this polynomial over \( \mathbb{Q} \) is \( \mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{3}) \). Here, we can define 4 \( \mathbb{Q} \)-automorphism mappings on \( \mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{3}) \), and they are following

\[
\begin{align*}
\sigma': \sqrt[2]{2} & \rightarrow \sqrt[2]{2}, \\
\sqrt[3]{3} & \rightarrow -\sqrt[3]{3} \\
\tau': \sqrt[2]{2} & \rightarrow -\sqrt[2]{2}, \\
\sqrt[3]{3} & \rightarrow \sqrt[3]{3} \\
\sigma' \circ \tau': \sqrt[2]{2} & \rightarrow -\sqrt[2]{2} \text{ and } id': \sqrt[2]{2} \rightarrow \sqrt[2]{2}, \\
\sqrt[3]{3} & \rightarrow \sqrt[3]{3} \quad \sqrt[3]{3} & \rightarrow \sqrt[3]{3}
\end{align*}
\]

By theorem 12 and 11, the Galois group of this polynomial \( Ga(\mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{3}) : \mathbb{Q}) \) is isomorphic to non-transitive subgroup of \( S_4 \) and \( Ga(\mathbb{Q}(\sqrt[2]{2}, \sqrt[3]{3}) : \mathbb{Q}) = \{ id', \sigma', \tau', \sigma' \circ \tau' \} \cong V_4 \). Again, take another polynomial \( \chi_2(t) = t^4 + 4t^2 + 2 \). By Eisenstein’s criterion of irreducibility of polynomial, this polynomial is an irreducible polynomial over \( \mathbb{Q} \). This polynomial and its first derivative have not any common root. So, it is separable polynomial. By theorem 12, its Galois group over the field of rational number is isomorphic to transitive subgroup of \( S_4 \). The resolvent cubic polynomial of \( \chi_4(t) \) is \( t^3 - 4t^2 - 8t + 32 = (t - 4)(t^2 - 8) \). The splitting field of this resolvent cubic polynomial is \( \mathbb{Q}(\sqrt[2]{2}) \) and \( \mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q} = 2 \). So, its Galois group is isomorphic to either \( D_4 \) or \( \mathbb{I}_4 \). But, we have \( \chi_4(t) = (t^2 + 2 - \sqrt[2]{2})(t^2 + 2 + \sqrt[2]{2}) \) which is reducible over \( \mathbb{Q}(\sqrt[2]{2}) \). Hence, its Galois group is isomorphic to \( \mathbb{I}_4 \). Again, it is true for \( m=4 \).

For \( m=5 \), subgroups (having order 5) of \( S_5 \) are following

\[
\begin{align*}
&\{(1),(12345),(13524),(14253),(15432)\} \cong \mathbb{I}_5 \\
&\{(1),(12345),(12534),(15432),(14352)\} \cong \mathbb{I}_5 \\
&\{(1),(12354),(13425),(15432),(15243)\} \cong \mathbb{I}_5 \\
&\{(1),(12435),(14523),(15342),(13254)\} \cong \mathbb{I}_5 \\
&\{(1),(12435),(13425),(13542),(15234)\} \cong \mathbb{I}_5
\end{align*}
\]

It is clear that these all subgroups are cyclic group of order five. Let us take the cyclotomic polynomial \( q_{11}(t) = 1 + t + \cdots + t^{10} \). By theorem 19, \( Ga(q_{11}(t)/\mathbb{Q}) \cong \mathbb{I}_{11} \cong \mathbb{I}_{10} \). We have that \( \mathbb{I}_2 \) is normal subgroup of \( \mathbb{I}_{10} \). Thus, there exists normal subgroup \( S \) of Galois group \( Ga(q_{11}(t)/\mathbb{Q}) \) such that \( S \cong \mathbb{I}_2 \). By fundamental theorem of Galois theory, there is fixed field \( N \) for subgroup \( S \) such that \( Ga(N: \mathbb{Q}) \cong Ga(q_{11}(t)/\mathbb{Q}) \cong \mathbb{I}_{10} \). It is also true for \( m=5 \).

**Proposition 29** \( M_{23} \cong Ga(N: L) \), \( L \) is the fixed field for subgroup \( S \cong M_{23} \) of Galois group \( Ga(N: \mathbb{Q}) \cong S_{23} \).

Proof: By theorem 25, there exists Galois extension \( N \) over \( \mathbb{Q} \) such that \( Ga(N: \mathbb{Q}) \cong S_{23} \). By definition 18, \( M_{23} \) is subgroup of \( S_{23} \). By property of group isomorphism, there exists subgroup \( S \) of \( Ga(N: \mathbb{Q}) \) such that \( S \cong M_{23} \). By fundamental theorem of Galois theory, there exists fixed field \( L \) for subgroup \( S \) of Galois group \( Ga(N: \mathbb{Q}) \) such that \( Ga(N: L) \cong S \cong M_{23} \). Here \( M_{23} \) is realizable as Galois group over the finite extension field \( L \) of \( \mathbb{Q} \). But it still remains to show that \( M_{23} \) is realizable as Galois group over the field of rational number.

If possible, suppose that \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \), for some \( y(t) \in \mathbb{Q}[t] \). By definition 18, \( M_{23} \) is the transitive subgroup of \( S_{23} \). By theorem 12, we get that \( y(t) \) is irreducible and separable polynomial of degree 23 over \( \mathbb{Q} \) which is necessary condition to reach at \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \).

**Is it possible to reach at sufficient condition \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \)?** If we suppose that \( y(t) \) be an irreducible and separable polynomial of degree 23 then we can’t get \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \), for some \( y(t) \in \mathbb{Q}[t] \). For example, the Galois group of \( y(t) = t^m + at + b \) over \( \mathbb{Q}(l) \) is isomorphic to \( S_m \) detail in [Jensen, 2002]. By theorem 13, there exists infinitely many \( a \in \mathbb{Q} \) and the Galois group of \( y(t) = t^m + at + a \) over \( \mathbb{Q} \) is isomorphic to \( S_m \). So, the Galois group of the irreducible and separable polynomial \( y(t) = t^m + 2t + 2 \) over \( \mathbb{Q} \) is isomorphic to \( S_{23} \). Thus, there exists some irreducible
separable polynomial of degree 23 over \( \mathbb{Q} \) whose Galois group over \( \mathbb{Q} \) is not isomorphic to \( M_{23} \). So, by only this much condition on \( y(t) \), we can’t assure that \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \). Now, we have to search also other conditions on \( y(t) \in \mathbb{Q}[t] \) which can assure that \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \).

**DISCUSSION**

The classical inverse Galois problem still remains to be solved. By theorem 17, we get positive answer of CIGP if the statement 28 is true, but we get negative answer of CIGP if the statement 28 is false. We found that statement 28 is true for \( m=1,2,3,4 \) and 5. So, we suppose that statement is true for \( m \leq k \). Now, if we can show that it is also true for \( m = k + 1 \) then by mathematical induction, it is true for all positive integer \( m \). So, we claim that statement 28 has positive answer for all \( m \) and by theorem 17, we get positive of CIGP. But it still remains to show that statement 28 is true for \( m = k + 1 \). On other hand, it is found that all solvable groups are realizable as Galois group over \( \mathbb{Q} \) group over \( \mathbb{Q} \) and also, we got that some non-solvable group such as \( S_m, m \geq 4, A_m, m \geq 4 \) are also realizable as Galois group over \( \mathbb{Q} \). But it remains to know the answer of CIGP for many other non-solvable groups such as \( M_{23} \). We showed that \( M_{23} \) is realizable as Galois group over the finite extension field \( L \) of \( \mathbb{Q} \), but it still remains to show that \( M_{23} \) is realizable as Galois group over \( \mathbb{Q} \). Now, we have to search a polynomial over \( \mathbb{Q} \) whose splitting field is Galois extension over \( \mathbb{Q} \), and its Galois group over \( \mathbb{Q} \) is isomorphic to \( M_{23} \). Here, \( M_{23} \) is transitive subgroup of \( S_{23} \), where \( M_{23} \) acts transitively on the set of 23 objects. So, \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \) implies that \( y(t) \) is an irreducible and separable polynomial of degree 23 over \( \mathbb{Q} \) which is necessary condition to reach at \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \). But if we suppose that \( y(t) \) is an irreducible and separable polynomial of degree 23 over \( \mathbb{Q} \), then by only these conditions on \( y(t) \), we didn’t assure that \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \), for some \( y(t) \in \mathbb{Q}[t] \) because we got some irreducible and separable polynomial of degree 23 whose Galois group over \( \mathbb{Q} \) is not isomorphic to \( M_{23} \). For example, \( y(t) = t^{23} + at + a \), for infinitely many \( a \in \mathbb{Q} \) is an irreducible and separable polynomial of degree 23 whose Galois group over \( \mathbb{Q} \) is isomorphic to \( S_{23} \). Thus, it is clear that we have to search further conditions on \( y(t) \in \mathbb{Q}[t] \) which can assure that \( Ga(y(t)/\mathbb{Q}) \cong M_{23} \).

**CONCLUSIONS**

From above results and discussion, we conclude that classical inverse Galois problem for all finite abelian group, all finite non-abelian solvable groups \( \{D_p, S_5, S_6, \ldots \} \) and many non-solvable group \( \{A_m, m \geq 5, S_m, m \geq 5, \ldots \} \) has positive answer. This paper concludes that \( M_{23} \) is realizable as Galois group over the Galois extension field \( L \) of \( \mathbb{Q} \) but it remains to show that \( M_{23} \) is realizable as Galois group over \( \mathbb{Q} \). So, CIGP still remains to solve for \( M_{23} \).

This paper also concludes that CIGP has only partial results, but we get its full result if we got answer of question “Whether all subgroups of order \( m \) of symmetric group \( S_m \) for all \( m \) are realizable as Galois group over \( \mathbb{Q} \).”

**ACKNOWLEDGEMENTS**

We are very thankful to all our supportive hands and reviewers for their suggestions to increase the quality of the paper.

**AUTHOR CONTRIBUTIONS**

BA contributed to conceptualization, writing original draft, reviewing and editing. TPN contributed supervision, reviewing and editing.

**CONFLICT OF INTERESTS**

The authors declare no conflict of interests.

**DATA AVAILABILITY STATEMENT**

The data that support the findings of this study are available from the corresponding author, upon reasonable request.

**REFERENCES**


