# Galois Theory and the Insolvability of the Quintic

Joshua Guo
Andrew Lee
Karthik Seetharaman
Mentor: Chun Hong Lo

May 22, 2022

# Summary

# Introducing Fields

The central concept of Galois theory is a field:

# Introducing Fields

The central concept of Galois theory is a field:

### Definition

A **field** is a set $F$, endowed with addition $(+)$ and multiplication $(\cdot)$ for which the following "field axioms" hold:

1. Multiplication and addition are associative $(a + (b + c) = (a + b) + c$ for $a, b, c \in F)$ and commutative $(a + b = b + a$ for $a, b \in F)$.

# Introducing Fields

The central concept of Galois theory is a field:

### Definition

A **field** is a set $F$, endowed with addition $(+)$ and multiplication $(\cdot)$ for which the following "field axioms" hold:

1. Multiplication and addition are associative $(a + (b + c) = (a + b) + c$ for $a, b, c \in F)$ and commutative $(a + b = b + a$ for $a, b \in F)$.
2. There exists an additive identity $0 \in F$ and a multiplicative identity $1 \in F$. These are distinct.

# Introducing Fields

The central concept of Galois theory is a field:

### Definition

A **field** is a set $F$, endowed with addition $(+)$ and multiplication $(\cdot)$ for which the following "field axioms" hold:

1. Multiplication and addition are associative $(a + (b + c) = (a + b) + c$ for $a, b, c \in F)$ and commutative $(a + b = b + a$ for $a, b \in F)$.
2. There exists an additive identity $0 \in F$ and a multiplicative identity $1 \in F$. These are distinct.
3. For all $a \in F$, there exists $-a \in F$ such that $a + (-a) = 0$.

# Introducing Fields

The central concept of Galois theory is a field:

**Definition**

A **field** is a set $F$, endowed with addition $(+)$ and multiplication $(\cdot)$ for which the following "field axioms" hold:

1. Multiplication and addition are associative $(a+(b+c)=(a+b)+c$ for $a,b,c\in F)$ and commutative $(a+b=b+a$ for $a,b\in F)$.
2. There exists an additive identity $0\in F$ and a multiplicative identity $1\in F$. These are distinct.
3. For all $a\in F$, there exists $-a\in F$ such that $a+(-a)=0$.
4. For all $a\neq 0\in F$, there exists $\frac{1}{a}\in F$ such that $a\cdot\frac{1}{a}=1$.

# Introducing Fields

The central concept of Galois theory is a field:

### Definition

A **field** is a set $F$, endowed with addition $(+)$ and multiplication $(\cdot)$ for which the following "field axioms" hold:

1. Multiplication and addition are associative $(a + (b + c) = (a + b) + c$ for $a, b, c \in F)$ and commutative $(a + b = b + a$ for $a, b \in F)$.
2. There exists an additive identity $0 \in F$ and a multiplicative identity $1 \in F$. These are distinct.
3. For all $a \in F$, there exists $-a \in F$ such that $a + (-a) = 0$.
4. For all $a \neq 0 \in F$, there exists $\frac{1}{a} \in F$ such that $a \cdot \frac{1}{a} = 1$.
5. $a \cdot (b + c) = a \cdot b + a \cdot c$ for $a, b, c \in F$.

# Examples of Fields

**Example**

- $\mathbb{Q}$
- $\mathbb{R}$
- $\mathbb{C}$
- $\mathbb{Z}/p\mathbb{Z}$
- $\mathbb{Q}(i)$

In this presentation, we only work with subfields of $\mathbb{C}$.

# Field Extensions

**Definition**

If $K \subset L$ are fields, then $L/K$ is a **field extension**. $K$ is called a subfield of $L$ and $L$ is called an extension of $K$.

# Field Extensions

**Definition**

If $K \subset L$ are fields, then $L/K$ is a **field extension**. $K$ is called a subfield of $L$ and $L$ is called an extension of $K$.

We are particularly interested in field extensions of the form $K(a_1, a_2, \ldots, a_n)$, which we define to be the smallest field containing $K, a_1, a_2, \ldots, a_n$.

# Field Extensions

**Definition**

If $K \subset L$ are fields, then $L/K$ is a **field extension**. $K$ is called a subfield of $L$ and $L$ is called an extension of $K$.

We are particularly interested in field extensions of the form $K(a_1, a_2, \ldots, a_n)$, which we define to be the smallest field containing $K, a_1, a_2, \ldots, a_n$.

**Example**

1. $\mathbb{Q}(i)$
2. $\mathbb{R}(i) = \mathbb{C}$
3. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

# Splitting Fields

**Definition**

We say a polynomial $f \in K[x]$ **splits** over the field $L$ if all of its roots lie in $L$.

# Splitting Fields

**Definition**

We say a polynomial $f \in K[x]$ **splits** over the field $L$ if all of its roots lie in $L$.

**Definition**

We say $L$ is a **splitting field** for $f(x)$ over $K$ if $L$ if $f(x)$ splits over $L$ and $L$ is the smallest such field. If

$$f(x) = c(x - a_1)(x - a_2)\cdots(x - a_n), a_i \in L,$$

then this is equivalent to $L = K(a_1, a_2, \ldots, a_n)$.

# Splitting Fields

**Definition**

We say a polynomial $f \in K[x]$ **splits** over the field $L$ if all of its roots lie in $L$.

**Definition**

We say $L$ is a **splitting field** for $f(x)$ over $K$ if $L$ if $f(x)$ splits over $L$ and $L$ is the smallest such field. If

$$f(x) = c(x - a_1)(x - a_2) \cdots (x - a_n), a_i \in L,$$

then this is equivalent to $L = K(a_1, a_2, \ldots, a_n)$.

**Example**

The polynomial $f(x) = x^3 - 2$ does not split in $\mathbb{R}$ since it has two complex roots. Its splitting field is $\mathbb{Q}(e^{\frac{2\pi i}{3}}), \sqrt[3]{2})$.

# Normal Extensions

### Definition

An extension $L/K$ is **normal** if, for all irreducible polynomials $p \in K[x]$, if $p$ has one root in $L$, then $p$ has all its roots in $L$.

# Normal Extensions

### Definition

An extension $L/K$ is **normal** if, for all irreducible polynomials $p \in K[x]$, if $p$ has one root in $L$, then $p$ has all its roots in $L$.

### Theorem

*An extension $L/K$ is normal if and only if there exists some polynomial $p \in K[x]$ such that $L$ is the splitting field for $p$ over $K$.*

# Normal Extensions

### Definition

An extension $L/K$ is **normal** if, for all irreducible polynomials $p \in K[x]$, if $p$ has one root in $L$, then $p$ has all its roots in $L$.

### Theorem

*An extension $L/K$ is normal if and only if there exists some polynomial $p \in K[x]$ such that $L$ is the splitting field for $p$ over $K$.*

### Example

1. $\mathbb{C}$ is a normal extension of $\mathbb{R}$ since it is the splitting field for the polynomial $x^2 + 1$ over $\mathbb{R}$.

# Normal Extensions

### Definition

An extension $L/K$ is **normal** if, for all irreducible polynomials $p \in K[x]$, if $p$ has one root in $L$, then $p$ has all its roots in $L$.

### Theorem

*An extension $L/K$ is normal if and only if there exists some polynomial $p \in K[x]$ such that $L$ is the splitting field for $p$ over $K$.*

### Example

1. $\mathbb{C}$ is a normal extension of $\mathbb{R}$ since it is the splitting field for the polynomial $x^2 + 1$ over $\mathbb{R}$.
2. $\mathbb{Q}(\sqrt[3]{2})$ is not a normal extension of $\mathbb{Q}$ since the polynomial $x^3 - 2$ does not have all its roots in $\mathbb{Q}(\sqrt[3]{2})$.

# The Galois Group

We care about all this because, for normal field extensions containing $\mathbb{Q}$, we can associate a useful group known as the **Galois group**.

# The Galois Group

We care about all this because, for normal field extensions containing $\mathbb{Q}$, we can associate a useful group known as the **Galois group**.

### Definition

Given a normal field extension $L/K$, define the group $\mathrm{Gal}(L/K)$ to be the set of automorphisms $\phi : L \to L$ such that $\phi(k) = k$ for all $k \in K$ under the operation of composition.

# The Galois Group

We care about all this because, for normal field extensions containing $\mathbb{Q}$, we can associate a useful group known as the **Galois group**.

### Definition

Given a normal field extension $L/K$, define the group $\mathrm{Gal}(L/K)$ to be the set of automorphisms $\phi : L \to L$ such that $\phi(k) = k$ for all $k \in K$ under the operation of composition.

### Example

The Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = C_2$ since the only automorphisms of $\mathbb{C}$ that fix $\mathbb{R}$ are the identity and complex conjugation.

# Fundamental Theorem of Galois Theory

**Theorem**

*Let $L/K$ be finite and Galois and $G = Gal(L/K)$. Let $\mathcal{F} = \{K \subseteq M \subseteq L \text{ subfields}\}$, $\mathcal{G} = \{H \subseteq G \text{ subgroups}\}$. Consider two maps $\Phi : \mathcal{G} \to \mathcal{F}$, $\Gamma : \mathcal{F} \to \mathcal{G}$.*

$$\Phi(H) = \{\lambda \in L : h(\lambda) = \lambda \text{ for all } h \in H\}$$

$$\Gamma(M) = \{g \in G : g(m) = m \text{ for all } m \in M\}$$

- $|G| = [L : K]$
- $\Phi$ *and* $\Gamma$ *are order-reversing bijections.*

The Fundamental Theorem of Galois Theory outlines a correspondence between the subfields of $L$ containing $K$ and the subgroups of $G$.

# Galois Correspondence Example

Let $K = \mathbb{Q}$ and $L$ be the splitting field of $f(x) = x^3 - 2$, which has roots $\alpha, \omega\alpha, \omega^2\alpha$ for $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. Then, $L = \mathbb{Q}(\alpha, \omega)$ and $[L : \mathbb{Q}] = 6$. The Fundamental Theorem of Galois Theory tells us that $|\mathrm{Gal}(L/\mathbb{Q})| = 6$.

# Galois Correspondence Example

Let $K = \mathbb{Q}$ and $L$ be the splitting field of $f(x) = x^3 - 2$, which has roots $\alpha, \omega\alpha, \omega^2\alpha$ for $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. Then, $L = \mathbb{Q}(\alpha, \omega)$ and $[L : \mathbb{Q}] = 6$. The Fundamental Theorem of Galois Theory tells us that $|\mathrm{Gal}(L/\mathbb{Q})| = 6$.

It is known that the every automorphism in $\mathrm{Gal}(L/\mathbb{Q})$ maintains a bijection from the roots of $f(x)$ to itself. All of the 6 permutations of the roots must be valid since $|\mathrm{Gal}(L/\mathbb{Q})| = 6$. It then follows that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. Each automorphism corresponds with a permutation of the roots.

# Galois Correspondence Example

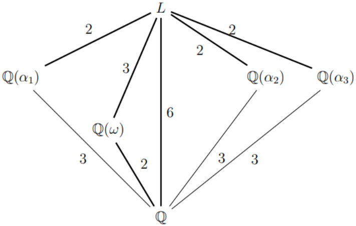
Let $K = \mathbb{Q}$ and $L$ be the splitting field of $f(x) = x^3 - 2$, which has roots $\alpha, \omega\alpha, \omega^2\alpha$ for $\alpha = \sqrt[3]{2}$ and $\omega = e^{2\pi i/3}$. Then, $L = \mathbb{Q}(\alpha, \omega)$ and $[L : \mathbb{Q}] = 6$. The Fundamental Theorem of Galois Theory tells us that $|\mathrm{Gal}(L/\mathbb{Q})| = 6$.

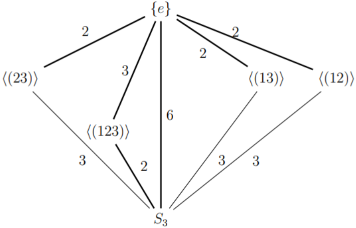
It is known that the every automorphism in $\mathrm{Gal}(L/\mathbb{Q})$ maintains a bijection from the roots of $f(x)$ to itself. All of the 6 permutations of the roots must be valid since $|\mathrm{Gal}(L/\mathbb{Q})| = 6$. It then follows that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. Each automorphism corresponds with a permutation of the roots.

For example, permutation (231) corresponds to the automorphism defined by $\alpha \to \omega\alpha, \omega\alpha \to \omega^2\alpha, \omega^2\alpha \to \alpha$, which gives $\omega \to \omega$.

# Galois Correspondence Example

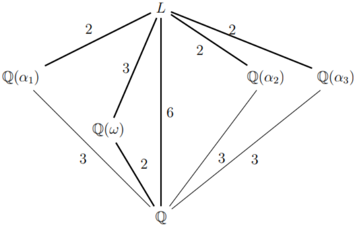
This gives the following correspondence, where $\alpha_1, \alpha_2, \alpha_3$ are the roots of $f(x)$.

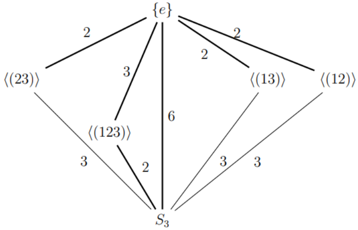


# Galois Correspondence Example

This gives the following correspondence, where $\alpha_1, \alpha_2, \alpha_3$ are the roots of $f(x)$.




For example, let us look at the correspondence between $\langle\langle 123\rangle\rangle$ and $\mathbb{Q}(\omega)$. $\langle\langle 123\rangle\rangle$ contains permutations $e, (123), (132)$. Clearly, permutation $e$ fixes all $\lambda \in L$. Permutation $(123)$ has $\alpha \to \omega\alpha, \omega\alpha \to \omega^2\alpha, \omega^2\alpha \to \alpha$, which gives $\omega \to \omega$. We can then see that $\mathbb{Q}(\omega)$ is the set of elements that are fixed. Similar for $(132)$.

# Fundamental Theorem of Galois Theory (cont.)

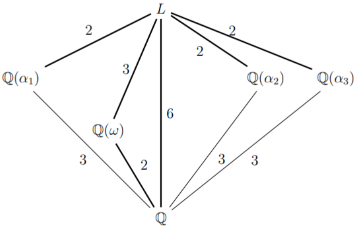
**Theorem**

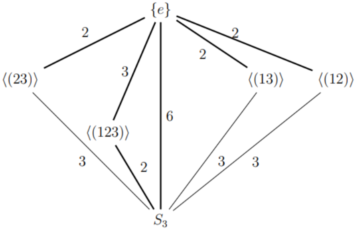
- *If* $M \in \mathcal{F}$ *corresponds to* $H \in \mathcal{G}$*, then* $H = Gal(L/M)$
- $H \in \mathcal{G}$ *is normal if and only if for the corresponding* $M \in \mathcal{F}$*,* $M/K$ *is normal, and in this case* $Gal(M/K) = G/H$

# Fundamental Theorem of Galois Theory (cont.)

**Theorem**

- *If $M \in \mathcal{F}$ corresponds to $H \in \mathcal{G}$, then $H = Gal(L/M)$*
- *$H \in \mathcal{G}$ is normal if and only if for the corresponding $M \in \mathcal{F}$, $M/K$ is normal, and in this case $Gal(M/K) = G/H$*



# Proof outline

- Field extensions by radicals
- Solvable Galois groups
- The splitting field of $X^5 - 6X + 3$

# Field extensions by radicals

### Definition

We say that the field extension $F/E$ is an *extension by radicals* if there is a series of fields

$$E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

such that, for each $i$, $F_{i+1} = F_i(\alpha_i)$, where $\alpha_i$ is an element of $F_{i+1}$ such that $\alpha_i^{n_i} \in F_i$ for some positive integer $n_i$.

# Field extensions by radicals

### Definition

We say that the field extension $F/E$ is an *extension by radicals* if there is a series of fields

$$E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

such that, for each $i$, $F_{i+1} = F_i(\alpha_i)$, where $\alpha_i$ is an element of $F_{i+1}$ such that $\alpha_i^{n_i} \in F_i$ for some positive integer $n_i$.

Clearly, an algebraic number $r$ is expressible by radicals iff $\mathbb{Q}(r)/\mathbb{Q}$ is an extension by radicals.

# Solvable Galois groups

### Definition

We say that a group $G$ is *solvable* iff there is a sequence of groups

$$\{e\} \subseteq H_n \subseteq H_{n-1} \subseteq \cdots \subseteq H_1 = G$$

such that, for all $i$, $H_{i+1} \triangleleft H_i$ and $H_i/H_{i+1}$ is abelian.

# Solvable Galois groups

**Definition**

We say that a group $G$ is *solvable* iff there is a sequence of groups

$$\{e\} \subseteq H_n \subseteq H_{n-1} \subseteq \cdots \subseteq H_1 = G$$

such that, for all $i$, $H_{i+1} \triangleleft H_i$ and $H_i/H_{i+1}$ is abelian.

We can relate this concept to field extensions by radicals as follows:

**Lemma**

Suppose $F/E$ is a finite and Galois field extension which is also an extension by radicals. Then $\mathrm{Gal}(F/E)$ is solvable.

Now we only need to study $\mathrm{Gal}(\mathbb{Q}(r)/\mathbb{Q})$ - another improvement!

# Proof of the lemma

Let

$$E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

be some series of fields that show that $F/E$ is an extension by radicals. WLOG assume all the $n_i$ are prime.

# Proof of the lemma

Let

$$E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

be some series of fields that show that $F/E$ is an extension by radicals. WLOG assume all the $n_i$ are prime. Letting $N := \prod_i n_i$, we can consider the tower of fields

$$K = F_0(\zeta_N) \subseteq F_1(\zeta_N) \subseteq \cdots \subseteq F_n(\zeta_N) = L$$

where $K := E(\zeta_N), L := F(\zeta_N)$.

# Proof of the lemma

Let

$$E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

be some series of fields that show that $F/E$ is an extension by radicals. WLOG assume all the $n_i$ are prime. Letting $N := \prod_i n_i$, we can consider the tower of fields

$$K = F_0(\zeta_N) \subseteq F_1(\zeta_N) \subseteq \cdots \subseteq F_n(\zeta_N) = L$$

where $K := E(\zeta_N), L := F(\zeta_N)$. Letting $G := \mathrm{Gal}(F(\zeta_N)/E(\zeta_N))$ and $G_i := \mathrm{Gal}(F(\zeta_N)/F_i(\zeta_N))$, we have

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G,$$

so $G$ is solvable.

# Proof of the lemma

Let

$$E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

be some series of fields that show that $F/E$ is an extension by radicals. WLOG assume all the $n_i$ are prime. Letting $N := \prod_i n_i$, we can consider the tower of fields

$$K = F_0(\zeta_N) \subseteq F_1(\zeta_N) \subseteq \cdots \subseteq F_n(\zeta_N) = L$$

where $K := E(\zeta_N), L := F(\zeta_N)$. Letting $G := \mathrm{Gal}(F(\zeta_N)/E(\zeta_N))$ and $G_i := \mathrm{Gal}(F(\zeta_N)/F_i(\zeta_N))$, we have

$$\{e\} = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_0 = G,$$

so $G$ is solvable. Since $\mathrm{Gal}(L/E)/\mathrm{Gal}(L/K) = \mathrm{Gal}(K/E)$ is abelian, we find that $\mathrm{Gal}(L/E)$ is also solvable.

# Proof of the lemma

Let

$$E = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

be some series of fields that show that $F/E$ is an extension by radicals. WLOG assume all the $n_i$ are prime. Letting $N := \prod_i n_i$, we can consider the tower of fields

$$K = F_0(\zeta_N) \subseteq F_1(\zeta_N) \subseteq \cdots \subseteq F_n(\zeta_N) = L$$

where $K := E(\zeta_N), L := F(\zeta_N)$. Letting $G := \mathrm{Gal}(F(\zeta_N)/E(\zeta_N))$ and $G_i := \mathrm{Gal}(F(\zeta_N)/F_i(\zeta_N))$, we have

$$\{e\} = G_n \lhd G_{n-1} \lhd \cdots \lhd G_0 = G,$$

so $G$ is solvable. Since $\mathrm{Gal}(L/E)/\mathrm{Gal}(L/K) = \mathrm{Gal}(K/E)$ is abelian, we find that $\mathrm{Gal}(L/E)$ is also solvable. Finally, since $\mathrm{Gal}(L/E)/\mathrm{Gal}(L/F) = \mathrm{Gal}(F/E)$, so $\mathrm{Gal}(F/E)$ is solvable and we are done.

# The splitting field of $X^5 - 6X + 3$ has Galois group $S_5$...

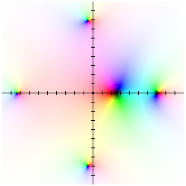
Now we give an example of a quintic equation whose roots are not expressible by radicals: $X^5 - 6X + 3 = 0$. Let $p(X) := X^5 - 6X + 3$ and $L$ the splitting field of $p(X)$ over $\mathbb{Q}$.

# The splitting field of $X^5 - 6X + 3$ has Galois group $S_5$...

Now we give an example of a quintic equation whose roots are not expressible by radicals: $X^5 - 6X + 3 = 0$. Let $p(X) := X^5 - 6X + 3$ and $L$ the splitting field of $p(X)$ over $\mathbb{Q}$.

What do we know about $\mathrm{Gal}(L/\mathbb{Q})$?

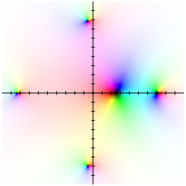
- It's a subgroup of $S_5$



# The splitting field of $X^5 - 6X + 3$ has Galois group $S_5$...

Now we give an example of a quintic equation whose roots are not expressible by radicals: $X^5 - 6X + 3 = 0$. Let $p(X) := X^5 - 6X + 3$ and $L$ the splitting field of $p(X)$ over $\mathbb{Q}$.
What do we know about $\mathrm{Gal}(L/\mathbb{Q})$?

- It's a subgroup of $S_5$
- It contains a 5-cycle

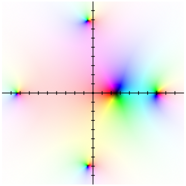


# The splitting field of $X^5 - 6X + 3$ has Galois group $S_5$...

Now we give an example of a quintic equation whose roots are not expressible by radicals: $X^5 - 6X + 3 = 0$. Let $p(X) := X^5 - 6X + 3$ and $L$ the splitting field of $p(X)$ over $\mathbb{Q}$.

What do we know about $\mathrm{Gal}(L/\mathbb{Q})$?

- It's a subgroup of $S_5$
- It contains a 5-cycle
- It contains complex conjugation, a transposition



This is actually enough to deduce $\mathrm{Gal}(L/\mathbb{Q}) = S_5$.

# … and $S_5$ is not solvable!

Notice that $S_1, S_2, S_3, S_4$ are solvable, but $S_5$ and so on are not solvable.

# … and $S_5$ is not solvable!

Notice that $S_1, S_2, S_3, S_4$ are solvable, but $S_5$ and so on are not solvable. We conclude:

- $S_5$ is not solvable

# … and $S_5$ is not solvable!

Notice that $S_1, S_2, S_3, S_4$ are solvable, but $S_5$ and so on are not solvable. We conclude:

- $S_5$ is not solvable
- … so $\mathrm{Gal}(L/\mathbb{Q})$ is not solvable

# ... and $S_5$ is not solvable!

Notice that $S_1, S_2, S_3, S_4$ are solvable, but $S_5$ and so on are not solvable. We conclude:

- $S_5$ is not solvable
- ... so $\mathrm{Gal}(L/\mathbb{Q})$ is not solvable
- ... so $L/\mathbb{Q}$ is not an extension by radicals

# … and $S_5$ is not solvable!

Notice that $S_1, S_2, S_3, S_4$ are solvable, but $S_5$ and so on are not solvable. We conclude:

- $S_5$ is not solvable
- … so $\mathrm{Gal}(L/\mathbb{Q})$ is not solvable
- … so $L/\mathbb{Q}$ is not an extension by radicals
- … so the roots of $p(X)$ are not expressible by radicals.

QED.

# Acknowledgements

We thank

- Our mentor Chun Hong Lo for his valuable guidance.
- Professor Pavel Etingof, Dr. Slava Gerovitch, Dr. Tanya Khovanova, the MIT Math Department, and the MIT PRIMES program, for providing us with this opportunity.
- You for listening.