Sketch of the proof
Field Extensions

Def. \( \mathbb{Q} := \) the rational numbers, \( \mathbb{R} := \) the real numbers, and \( \mathbb{C} := \) the complex numbers.
Field Extensions

Def. \( \mathbb{Q} := \) the rational numbers, \( \mathbb{R} := \) the real numbers, and \( \mathbb{C} := \) the complex numbers.

• Field extensions:

\[ \mathbb{Q}(i) := \text{the smallest subfield of } \mathbb{C} \text{ containing } i. \]
Field Extensions

Def. \( \mathbb{Q} := \) the rational numbers, \( \mathbb{R} := \) the real numbers, and \( \mathbb{C} := \) the complex numbers.

• Field extensions:

\[ \mathbb{Q}(i) := \text{the smallest subfield of } \mathbb{C} \text{ containing } i. \]

\[ 1 + i, \quad (2 + 3i)/(4 - 5i) \]
Field Extensions

Def. $\mathbb{Q} :=$ the rational numbers, $\mathbb{R} :=$ the real numbers, and $\mathbb{C} :=$ the complex numbers.

Field extensions:

$\mathbb{Q}(i) :=$ the smallest subfield of $\mathbb{C}$ containing $i$.

$1 + i, \ (2 + 3i)/(4 - 5i)$

$a + bi$
Field Extensions

Def. \( \mathbb{Q} := \) the rational numbers, \( \mathbb{R} := \) the real numbers, and \( \mathbb{C} := \) the complex numbers.

• Field extensions:

\[ \mathbb{Q}(\sqrt[3]{2}) := \text{the smallest subfield of } \mathbb{C} \text{ containing } \sqrt[3]{2}. \]
Field Extensions

Def. \( \mathbb{Q} := \) the rational numbers, \( \mathbb{R} := \) the real numbers, and \( \mathbb{C} := \) the complex numbers.

• Field extensions:

\[ \mathbb{Q}(\sqrt[3]{2}) := \text{the smallest subfield of } \mathbb{C} \text{ containing } \sqrt[3]{2}. \]

\[ 1 + 3\sqrt[3]{2} + 4\sqrt[3]{2^2}, \frac{(1 + 3\sqrt[3]{2})}{(2 + 3\sqrt[3]{2^2})} \]
Field Extensions

Def. \( \mathbb{Q} := \) the rational numbers, \( \mathbb{R} := \) the real numbers, and \( \mathbb{C} := \) the complex numbers.

- Field extensions:

\[ \mathbb{Q}(\sqrt[3]{2}) := \text{the smallest subfield of } \mathbb{C} \text{ containing } \sqrt[3]{2}. \]

\[ 1 + 3\sqrt[3]{2} + 4\sqrt[3]{2}^2, \frac{(1 + 3\sqrt[3]{2})}{(2 + 3\sqrt[3]{2}^2)} \]

\[ a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2 \]
Field Extensions

Def. $\mathbb{Q} :=$ the rational numbers, $\mathbb{R} :=$ the real numbers, and $\mathbb{C} :=$ the complex numbers.

- Field extensions:

  $$\mathbb{Q}(\pi) :=$$ the smallest subfield of $\mathbb{C}$ containing $\pi$. 
Field Extensions

Def. \( \mathbb{Q} := \) the rational numbers, \( \mathbb{R} := \) the real numbers, and \( \mathbb{C} := \) the complex numbers.

- Field extensions:

\[ \mathbb{Q}(\pi) := \text{the smallest subfield of } \mathbb{C} \text{ containing } \pi. \]

\[ 1 + 3\pi + \pi^2, \frac{(1 + 3\pi^{2006})}{(2 + 3\pi^{2007})} \]
Field Extensions

Def. $\mathbb{Q} := \text{the rational numbers}, \mathbb{R} := \text{the real numbers, and} \mathbb{C} := \text{the complex numbers.}$

- Field extensions:

$$\mathbb{Q}(\pi) := \text{the smallest subfield of } \mathbb{C} \text{ containing } \pi.$$  

$$1 + 3\pi + \pi^2, \frac{(1 + 3\pi^{2006})}{(2 + 3\pi^{2007})}$$

$$\frac{a_0 + a_1\pi + \cdots + a_n\pi^n}{b_0 + b_1\pi + \cdots + b_m\pi^m}$$

where $n$ and $m$ are not fixed.
Field Extensions

Def. \( \mathbb{Q} := \) the rational numbers, \( \mathbb{R} := \) the real numbers, and \( \mathbb{C} := \) the complex numbers.

- Field extensions:

\[
\mathbb{Q}(\pi) := \text{the smallest subfield of } \mathbb{C} \text{ containing } \pi.
\]

\[
1 + 3\pi + \pi^2, \frac{1 + 3\pi^{2006}}{2 + 3\pi^{2007}}
\]

\[
\frac{a_0 + a_1\pi + \cdots + a_n\pi^n}{b_0 + b_1\pi + \cdots + b_m\pi^m}
\]

where \( n \) and \( m \) are not fixed.

\( \mathbb{Q}(\pi) \) is a \textit{transcendental} field ext.
Formal Field Extensions

$t$ is an *indeterminate*; it’s *not* a number in $\mathbb{C}$. 
Formal Field Extensions

$t$ is an indeterminate; it’s not a number in $\mathbb{C}$.

Def. $\mathbb{Q}(t) :=$ the set of formal expressions

$$\frac{a_0 + a_1 t + \cdots + a_n t^n}{b_0 + b_1 t + \cdots + b_m t^m}.$$
Formal Field Extensions

$t$ is an indeterminate; it’s not a number in $\mathbb{C}$.

**Def.** $\mathbb{Q}(t) := \text{the set of formal expressions}

\[ \frac{a_0 + a_1 t + \cdots + a_n t^n}{b_0 + b_1 t + \cdots + b_m t^m}. \]

$\mathbb{Q}(t) \approx \text{the set of rational functions.}$
Formal Field Extensions

\( t \) is an indeterminate; it’s not a number in \( \mathbb{C} \).

**Def.**  \( \mathbb{Q}(t) := \) the set of formal expressions

\[
\frac{a_0 + a_1 t + \cdots + a_n t^n}{b_0 + b_1 t + \cdots + b_m t^m}.
\]

\( \mathbb{Q}(t) \approx \) the set of rational functions.

\( \mathbb{Q}(t) \longrightarrow \mathbb{Q}(\pi) \) given by \( t \mapsto \pi \).

\[
\mathbb{Q}(t) \approx \mathbb{Q}(\pi)
\]
Field Isomorphisms

Isomorphic Fields:

• \( \mathbb{Q}(t) \approx \mathbb{Q}(\pi) \).
Field Isomorphisms

Isomorphic Fields:
• \( \mathbb{Q}(t) \approx \mathbb{Q}(\pi) \).

**Def.** \( \phi : K \rightarrow L \) is an *isomorphism* if
\( \phi : K \rightarrow L \) is a bijective map satisfying
Field Isomorphisms

Isomorphic Fields:

- $\mathbb{Q}(t) \approx \mathbb{Q}(\pi)$.

Def. $\phi : K \rightarrow L$ is an *isomorphism* if

$\phi : K \rightarrow L$ is a bijective map satisfying

1. $\phi(x + y) = \phi(x) + \phi(y)$;
2. $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$. 

Field Isomorphisms

Isomorphic Fields:

- \( \mathbb{Q}(t) \approx \mathbb{Q}(\pi) \).

**Def.** \( \phi : K \rightarrow L \) is an *isomorphism* if

\( \phi : K \rightarrow L \) is a bijective map satisfying

1. \( \phi(x + y) = \phi(x) + \phi(y) \);
2. \( \phi(x \cdot y) = \phi(x) \cdot \phi(y) \).

Two (distinct) isomorphic fields have the same arithmetic.
Field Isomorphisms

Isomorphic Fields:
- \( \mathbb{Q}(t) \approx \mathbb{Q}(\pi) \).

- \( \mathbb{Q}(\sqrt[3]{2}) \approx \mathbb{Q}(\alpha) \) where
  \( \alpha \in \mathbb{C} \) is another root of \( x^3 - 2 = 0 \).
Field Isomorphisms

Isomorphic Fields:

- $\mathbb{Q}(t) \approx \mathbb{Q}(\pi)$.

- $\mathbb{Q}(\sqrt[3]{2}) \approx \mathbb{Q}(\alpha)$ where
  \[ \alpha \in \mathbb{C} \text{ is another root of } x^3 - 2 = 0. \]

  Under the $\approx$,
  \[ a + b \sqrt[3]{2} + c \sqrt[3]{2}^2 \mapsto a + b \alpha + c \alpha^2. \]
Field Isomorphisms

Isomorphic Fields:

- \( \mathbb{Q}(t) \approx \mathbb{Q}(\pi) \).

- \( \mathbb{Q}(\sqrt[3]{2}) \approx \mathbb{Q}(\alpha) \) where
  \[ \alpha \in \mathbb{C} \] is another root of \( x^3 - 2 = 0 \).

Under the \( \approx \),
\[ a + b \sqrt[3]{2} + c \sqrt[3]{2^2} \mapsto a + b \alpha + c \alpha^2. \]

E.g.,
\[ (a + b \sqrt[3]{2} + c \sqrt[3]{2^2})^m = d + e \sqrt[3]{2} + f \sqrt[3]{2^2}; \]
Field Isomorphisms

Isomorphic Fields:

• $\mathbb{Q}(t) \approx \mathbb{Q}(\pi)$.

• $\mathbb{Q}(\sqrt[3]{2}) \approx \mathbb{Q}(\alpha)$ where
  $\alpha \in \mathbb{C}$ is another root of $x^3 - 2 = 0$.

  Under the $\approx$,
  \[ a + b \sqrt[3]{2} + c \sqrt[3]{2^2} \mapsto a + b \alpha + c \alpha^2. \]

  e.g.,
  \begin{align*}
  (a + b \sqrt[3]{2} + c \sqrt[3]{2^2})^m &= d + e \sqrt[3]{2} + f \sqrt[3]{2^2}; \\
  (a + b \alpha + c \alpha^2)^m &= d + e \alpha + f \alpha^2.
  \end{align*}
Field Automorphisms

Def. \( \phi : F \rightarrow F \) is an *automorphism* if

\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]
Field Automorphisms

Def. \( \phi : F \to F \) is an automorphism if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

\( \mathbb{C} = \mathbb{R}(i) \). Let \( j := -i \).
Field Automorphisms

Def. \( \phi : F \to F \) is an \textit{automorphism} if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

- \( \mathbb{C} = \mathbb{R}(i) \). Let \( j := -i \).

\[
X^2 + 1 = 0
\]
Field Automorphisms

Def. \( \phi : F \to F \) is an automorphism if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

- \( \mathbb{C} = \mathbb{R}(i) \). Let \( j := -i \).

\[
X^2 + 1 = 0
\]

\( \mathbb{C} \to \mathbb{C} \) given by \( a + bi \mapsto a + b j \).
Field Automorphisms

Def. \( \phi : F \rightarrow F \) is an automorphism if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

- \( \mathbb{C} = \mathbb{R}(i) \). Let \( j := -i \).

\[
X^2 + 1 = 0
\]

\( \mathbb{C} \longrightarrow \mathbb{C} \) given by \( a + bi \mapsto a + bj \).

e.g.,
\[
(a + bi)^m = c + di \\
(a + bj)^m = c + dj.
\]
Field Automorphisms

Def. $\phi : F \to F$ is an automorphism if
\[ \phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y). \]

• $\mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$?
Field Automorphisms

Def. \( \phi : F \to F \) is an \textit{automorphism} if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

- \( \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})? \)

\[
\sqrt[3]{2} \mapsto \sqrt[3]{2}.
\]
Field Automorphisms

Def. \( \phi : F \to F \) is an \textit{automorphism} if

\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

\begin{itemize}
  \item \( \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})? \)
  \item \( \sqrt[3]{2} \mapsto \sqrt[3]{2} \).
\end{itemize}

\( X^3 - 2 = 0 \) has one real

and two complex solutions.
Field Automorphisms

**Def.** $\phi : F \rightarrow F$ is an *automorphism* if

$$\phi(x + y) = \phi(x) + \phi(y); \ \phi(x \cdot y) = \phi(x) \cdot \phi(y).$$

- $\mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{Q}(\sqrt[3]{2})$?

$$\sqrt[3]{2} \mapsto \sqrt[3]{2}.$$ 

$X^3 - 2 = 0$ has one real and two complex solutions.

$id : \mathbb{Q}(\sqrt[3]{2}) \rightarrow \mathbb{Q}(\sqrt[3]{2})$ is the only automorphism.
Field Automorphisms

Def. \( \phi : F \rightarrow F \) is an automorphism if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

• Let \( \alpha \) and \( \beta \) be the two complex solutions of \( X^3 - 2 = 0 \). 
Field Automorphisms

Def. $\phi : F \to F$ is an automorphism if
$\phi(x + y) = \phi(x) + \phi(y); \phi(x \cdot y) = \phi(x) \cdot \phi(y)$.

- Let $\alpha$ and $\beta$ be the two complex solutions of $X^3 - 2 = 0$.
  Let $K := \mathbb{Q}(\sqrt[3]{2}, \alpha, \beta)$. 
Field Automorphisms

Def. \( \phi : F \to F \) is an **automorphism** if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

- Let \( \alpha \) and \( \beta \) be the two complex solutions of \( X^3 - 2 = 0 \).
  Let \( K := \mathbb{Q}(\sqrt[3]{2}, \alpha, \beta) \).
  An element of \( K \) is in the form of
  \[
a + (b\sqrt[3]{2} + c\alpha + d\beta) + (e\sqrt[6]{2^2} + f\sqrt[3]{2}\alpha + \cdots) + \cdots + g\sqrt[3]{2^2}\alpha^2\beta^2.
  \]
Field Automorphisms

Def. \( \phi : F \to F \) is an automorphism if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

- Let \( \alpha \) and \( \beta \) be the two complex solutions of \( X^3 - 2 = 0 \).
  Let \( K := \mathbb{Q}(3\sqrt{2}, \alpha, \beta) \).
  An element of \( K \) is in the form of
  \[
  a + (b3\sqrt{2} + c\alpha + d\beta) + (e3\sqrt{2}^2 + f3\sqrt{2}\alpha + \cdots) \\
  + \cdots + g3\sqrt{2}^2\alpha^2\beta^2.
  \]

- Can a function \( \phi : K \to K \) be defined by
  \( 3\sqrt{2} \leftrightarrow \alpha; \beta \leftrightarrow \beta \)?
Field Automorphisms

Def. \( \phi : F \rightarrow F \) is an **automorphism** if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

• Let \( \alpha \) and \( \beta \) be the two complex solutions of \( X^3 - 2 = 0 \).
  Let \( K := \mathbb{Q}(\sqrt[3]{2}, \alpha, \beta) \).
  An element of \( K \) is in the form of
\[
a + (b\sqrt[3]{2} + c\alpha + d\beta) + (e\sqrt[3]{2^2} + f\sqrt[3]{2}\alpha + \cdots) + \cdots + g\sqrt[3]{2^2}\alpha^2\beta^2.
\]

• Can a function \( \phi : K \rightarrow K \) be defined by
  \( \sqrt[3]{2} \leftrightarrow \alpha; \beta \leftrightarrow \beta \)?
  \( \star \alpha^2\beta = 2. \)
Field Automorphisms

**Def.** $\phi : F \to F$ is an *automorphism* if
\[ \phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y). \]

- Let $\alpha$ and $\beta$ be the two complex solutions of $X^3 - 2 = 0$.
  Let $K := \mathbb{Q}(\sqrt[3]{2}, \alpha, \beta)$.
  An element of $K$ is in the form of
  \[ a + (b\sqrt[3]{2} + c\alpha + d\beta) + (e\sqrt[3]{2}^2 + f\sqrt[3]{2}\alpha + \cdots) \]
  \[ + \cdots + g\sqrt[3]{2}^2 \alpha^2 \beta^2. \]

- Can a function $\phi : K \to K$ be defined by
  $\sqrt[3]{2} \leftrightarrow \alpha; \beta \leftrightarrow \beta$?
  \[ \star \alpha^2 \beta = 2. \]
  \[ \phi(\alpha^2 \beta) = \sqrt[3]{2}^2 \beta \text{ and } \phi(2) = 2. \]
Field Automorphisms

**Def.** $\phi : F \rightarrow F$ is an *automorphism* if

$\phi(x+y) = \phi(x) + \phi(y); \ \phi(x \cdot y) = \phi(x) \cdot \phi(y)$.

- Let $\alpha$ and $\beta$ be the two complex solutions of $X^3 - 2 = 0$.
  Let $K := \mathbb{Q}(\sqrt[3]{2}, \alpha, \beta)$.

  An element of $K$ is in the form of

  $a + (b\sqrt[3]{2} + c\alpha + d\beta) + (e\sqrt[2]{2} + f\sqrt[2]{\alpha} + \cdots) + \cdots + g\sqrt[3]{2} \alpha^2 \beta^2$.

- Can a function $\phi : K \rightarrow K$ be defined by

  $\sqrt[3]{2} \leftrightarrow \alpha; \ \beta \mapsto \beta$?

  $\star \ \alpha^2 \beta = 2$.

  $\phi(\alpha^2 \beta) = \sqrt[2]{2} \beta$ and $\phi(2) = 2$.

  $\sqrt[2]{2} \beta = 2$?
Field Automorphisms

Def. \( \phi : F \to F \) is an **automorphism** if
\[
\phi(x + y) = \phi(x) + \phi(y); \quad \phi(x \cdot y) = \phi(x) \cdot \phi(y).
\]

- Let \( \alpha \) and \( \beta \) be the two complex solutions of \( X^3 - 2 = 0 \).
  
  Let \( K := \mathbb{Q}(\sqrt[3]{2}, \alpha, \beta) \).
  
  An element of \( K \) is in the form of
  \[
a + (b \sqrt[3]{2} + c\alpha + d\beta) + (e \sqrt[3]{2}^2 + f \sqrt[3]{2} \alpha + \cdots) + \cdots + g \sqrt[3]{2}^2 \alpha^2 \beta^2.
  \]

- Can a function \( \phi : K \to K \) be defined by
  \[
  \sqrt[3]{2} \leftrightarrow \alpha; \quad \beta \leftrightarrow \beta?
  \]
  \* \( \alpha^2 \beta = 2 \).

  \[
  \phi(\alpha^2 \beta) = \sqrt[3]{2}^2 \beta \text{ and } \phi(2) = 2.
  \]
  \[
  \sqrt[3]{2}^2 \beta = 2?
  \]

The *group* of automorphisms
Radical Extensions

Examples:

Subfields of $\mathbb{C}$:

- $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$.
- $\mathbb{Q}(\sqrt[3]{2} + \sqrt[3]{3})$. 
Radical Extensions

Examples:

Subfields of \( \mathbb{C} \):

- \( \mathbb{Q}(\sqrt[3]{2}) \), \( \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) \).
- \( \mathbb{Q}(\sqrt[3]{\sqrt{2} + \sqrt[3]{3}}) \).

Formal radical extensions:

- \( \mathbb{Q}(\sqrt[3]{t}) \), \( \mathbb{Q}(\sqrt[3]{t_1}, \sqrt[3]{t_2}) \).
- \( \mathbb{Q}(\sqrt[3]{t_1 + t_2}) \).
Radical Extensions

Examples:

Subfields of \( \mathbb{C} \):
- \( \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) \).
- \( \mathbb{Q}(\sqrt[3]{2} + \sqrt[3]{3}) \).

Formal radical extensions:
- \( \mathbb{Q}(\sqrt[3]{t}), \mathbb{Q}(\sqrt[3]{t_1}, \sqrt[3]{t_2}) \).
- \( \mathbb{Q}(\sqrt[3]{t_1} + \sqrt[3]{t_2}) \).

The quadratic equation: \( x^2 + 2x + 3 = 0 \) has both solutions in \( \mathbb{Q}(\sqrt{2}i) = \mathbb{Q}(\sqrt{-2}) \).
Radical Extensions

Examples:

Subfields of $\mathbb{C}$:

- $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$.
- $\mathbb{Q}(\sqrt[3]{2} + \sqrt[3]{3})$.

Formal radical extensions:

- $\mathbb{Q}(\sqrt[3]{t})$, $\mathbb{Q}(\sqrt[3]{t_1}, \sqrt[3]{t_2})$.
- $\mathbb{Q}(\sqrt[3]{t_1 + t_2})$.

The quadratic equation: $x^2 + 2x + 3 = 0$

has both solutions in $\mathbb{Q}(\sqrt{2}i) = \mathbb{Q}(\sqrt{-2})$.

Quadratic Formula says, $x^2 + t_1x + t_2 = 0$

has both solutions in $\mathbb{Q}(t_1, t_2, \sqrt{t_1^2 - 4t_2})$. 
Radical Extensions

Def.  (1) A radical ext. of $\mathbb{Q}$ is $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where for each $k$,
$$\alpha^m_k \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{k-1})$$
for some $m$.

(2) A radical ext. of $K := \mathbb{Q}(t_1, \ldots, t_l)$ is $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where for each $k$,
$$\alpha^m_k \in K(\alpha_1, \ldots, \alpha_{k-1})$$
for some $m$. 
Radical Extensions

**Def.** (1) A radical ext. of $\mathbb{Q}$ is $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where for each $k$,
$$\alpha_k^m \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{k-1})$$
for some $m$.

(2) A radical ext. of $K := \mathbb{Q}(t_1, \ldots, t_l)$ is $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where for each $k$,
$$\alpha_k^m \in K(\alpha_1, \ldots, \alpha_{k-1})$$
for some $m$.

★ The cubic equation: $x^3 + t_2x^2 + t_1x + t_0 = 0$

has three solutions in a radical ext. of $\mathbb{Q}(t_0, t_1, t_2)$.

★ The quartic equation: $x^4 + t_3x^3 + t_2x^2 + t_1x + t_0 = 0$

has four solutions in a radical ext. of $\mathbb{Q}(t_0, t_1, t_2, t_3)$. 
Radical Extensions

Def. (1) A radical ext. of $\mathbb{Q}$ is $\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where for each $k$,
$$\alpha_k^m \in \mathbb{Q}(\alpha_1, \ldots, \alpha_{k-1})$$ for some $m$.

(2) A radical ext. of $K := \mathbb{Q}(t_1, \ldots, t_l)$ is $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ where for each $k$,
$$\alpha_k^m \in K(\alpha_1, \ldots, \alpha_{k-1})$$ for some $m$.

★ The equation: $x^n + t_{n-1}x^{n-1} + \cdots + t_1x + t_0 = 0$ for $n \geq 5$
does not have a solution
in a radical ext. of $\mathbb{Q}(t_0, \ldots, t_{n-1})$. 
Fields and Groups

Example of groups: a set of bijective functions on a set $V$. 
Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, \ a \neq 0 \}$. 
Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.

- $f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.
Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.

  - $f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.

- $S = \{ \sigma : V \to V \mid \sigma \text{ bijective} \}$ where $V$ is a set.
Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.  
  $f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.

- $S = \{ \sigma : V \to V \mid \sigma \text{ bijective} \}$ where $V$ is a set.  
  When $V = \{1, 2, \ldots, n\}$, this group is denoted by $S_n$.  

Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.
  - $f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.

- $S = \{ \sigma : V \to V \mid \sigma \text{ bijective} \}$ where $V$ is a set.
  - When $V = \{1, 2, \ldots, n\}$, this group is denoted by $S_n$.
  - $S_n$ is equivalent to the set of all permutations of $n$ letters.
Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.  
  $\clubsuit$ $f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.

- $S = \{ \sigma : V \to V \mid \sigma \text{ bijective} \}$ where $V$ is a set.

  When $V = \{1, 2, \ldots, n\}$, this group is denoted by $S_n$.

  $S_n$ is equivalent to

  the set of all permutations of $n$ letters.

  So, $S_n$ has $n!$ elements.
Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.
  - $f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.
- $S = \{ \sigma : V \to V \mid \sigma \text{ bijective} \}$ where $V$ is a set.
  - When $V = \{1, 2, \ldots, n\}$, this group is denoted by $S_n$.
  - $S_n$ is equivalent to the set of all permutations of $n$ letters.
  - So, $S_n$ has $n!$ elements.

Example: $S_3$ and $V = \{1, 2, 3\}$. 
**Fields and Groups**

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.
  
  $\clubsuit$ $f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.

- $S = \{ \sigma : V \rightarrow V \mid \sigma \text{ bijective} \}$ where $V$ is a set.

  When $V = \{1, 2, \ldots, n\}$, this group is denoted by $S_n$.

  $S_n$ is equivalent to

  the set of all permutations of $n$ letters.

  So, $S_n$ has $n!$ elements.

  **Example**: $S_3$ and $V = \{1, 2, 3\}$.

  If $\sigma = (1 \ 2)$ and $\tau = (1 \ 2 \ 3)$,
Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.  
  ♣ $f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.

- $S = \{ \sigma : V \to V \mid \sigma \text{ bijective} \}$ where $V$ is a set.
  When $V = \{1, 2, \ldots, n\}$, this group is denoted by $S_n$.
  $S_n$ is equivalent to the set of all permutations of $n$ letters.

So, $S_n$ has $n!$ elements.

Example: $S_3$ and $V = \{1, 2, 3\}$.

If $\sigma = (1\ 2)$ and $\tau = (1\ 2\ 3)$,

$$\sigma \circ \tau = (2\ 3).$$
Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.
  - $f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.
- $S = \{ \sigma : V \to V \mid \sigma \text{ bijective} \}$ where $V$ is a set.
  
  When $V = \{1, 2, \ldots, n\}$, this group is denoted by $S_n$.
  
  $S_n$ is equivalent to
  the set of all permutations of $n$ letters.
  
  So, $S_n$ has $n!$ elements.

The group of field automorphisms: $F = K(u_1, \ldots, u_n)$

$\text{Aut}_K(F) := \{ \sigma : F \xrightarrow{\sim} F \mid \sigma(a) = a, \forall a \in K \}$. 
Fields and Groups

Example of groups: a set of bijective functions on a set V.

• $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.
  ♣ $f \circ g$ is bijective, and $f \circ f^{-1} = id$.  

• $S = \{ \sigma : V \to V \mid \sigma \text{ bijective} \}$ where V is a set.
  When $V = \{1, 2, \ldots, n\}$, this group is denoted by $S_n$.
  $S_n$ is equivalent to
  the set of all permutations of n letters.
  So, $S_n$ has $n!$ elements.

The group of field automorphisms: $F = K(u_1, \ldots, u_n)$

$\text{Aut}_K(F) := \{ \sigma : F \sim F \mid \sigma(a) = a, \forall a \in K \}$.

e.g., $F = \mathbb{Q}(\sqrt[3]{2}, \alpha, \beta) \Rightarrow \text{Aut}_{\mathbb{Q}}(F) \approx S_3$. 
Fields and Groups

Example of groups: a set of bijective functions on a set $V$.

- $G = \{ f(x) = ax + b : a, b \in \mathbb{R}, a \neq 0 \}$.
  - $\blacklozenge f \circ g$ is bijective, and $f \circ f^{-1} = \text{id}$.

- $S = \{ \sigma : V \to V \mid \sigma \text{ bijective} \}$ where $V$ is a set.
  
  When $V = \{1, 2, \ldots, n\}$, this group is denoted by $S_n$.
  $S_n$ is equivalent to the set of all permutations of $n$ letters.
  
  So, $S_n$ has $n!$ elements.

The group of field automorphisms: $F = K(u_1, \ldots, u_n)$

$\text{Aut}_K(F) := \{ \sigma : F \sim F \mid \sigma(a) = a, \forall a \in K \}$.

The two groups: $S_n$ and $\text{Aut}_K(F)$
Fields and Groups

\[ x^n + t_{n-1}x^{n-1} + \cdots + t_1x + t_0 = 0 \text{ for } n \geq 5 \]

\[ K := \mathbb{Q}(t_0, \ldots, t_{n-1}) \]

Suppose, \( F = K(u_1, \ldots, u_n) \) is contained in a rad. ext. of \( K \) where \( u_1, \ldots, u_n \) are \( n \) solutions of the above pol. (written in terms of radicals of \( t_i \)'s).
Fields and Groups

\[ x^n + t_{n-1}x^{n-1} + \cdots + t_1x + t_0 = 0 \text{ for } n \geq 5 \]

\[ K := \mathbb{Q}(t_0, \ldots, t_{n-1}) \]

Suppose, \( F = K(u_1, \ldots, u_n) \) is contained in a rad. ext. of \( K \)

where \( u_1, \ldots, u_n \) are \( n \) solutions of the above pol.

(written in terms of radicals of \( t_i \)'s).

★ Field theory:

(1) radical ext. \( \Rightarrow \) the group \( \text{Aut}_K(F) \) is solvable.
Fields and Groups

\[ x^n + t_{n-1}x^{n-1} + \cdots + t_1x + t_0 = 0 \text{ for } n \geq 5 \]

\[ K := \mathbb{Q}(t_0, \ldots, t_{n-1}) \]

Suppose, \( F = K(u_1, \ldots, u_n) \) is contained in a rad. ext. of \( K \) where \( u_1, \ldots, u_n \) are \( n \) solutions of the above pol. (written in terms of radicals of \( t_i \)'s).

★ Field theory:

(1) radical ext. \( \Rightarrow \) the group \( \text{Aut}_K(F) \) is solvable.
(2) polynomial equation \( \Rightarrow \) \( \text{Aut}_K(F) \cong S_n \).
Fields and Groups

\[ x^n + t_{n-1}x^{n-1} + \cdots + t_1x + t_0 = 0 \text{ for } n \geq 5 \]

\[ K := \mathbb{Q}(t_0, \ldots, t_{n-1}) \]

Suppose, \( F = K(u_1, \ldots, u_n) \) is contained in a rad. ext. of \( K \) where \( u_1, \ldots, u_n \) are \( n \) solutions of the above pol.

(written in terms of radicals of \( t_i \)'s).

★ Field theory:

(1) radical ext. ⇒ the group \( \text{Aut}_K(F) \) is solvable.

(2) polynomial equation ⇒ \( \text{Aut}_K(F) \cong S_n \).

★ Group theory: \( S_n \) is not solvable if \( n \geq 5 \).
Fields and Groups

\[ x^n + t_{n-1}x^{n-1} + \cdots + t_1x + t_0 = 0 \text{ for } n \geq 5 \]

\[ K := \mathbb{Q}(t_0, \ldots, t_{n-1}) \]

Suppose, \( F = K(u_1, \ldots, u_n) \) is contained in a rad. ext. of \( K \) where \( u_1, \ldots, u_n \) are \( n \) solutions of the above pol. (written in terms of radicals of \( t_i \)'s).

★ Field theory:

(1) radical ext. \( \Rightarrow \) the group \( \text{Aut}_K(F) \) is solvable.

(2) polynomial equation \( \Rightarrow \) \( \text{Aut}_K(F) \approx S_n \).

★ Group theory: \( S_n \) is not solvable if \( n \geq 5 \).

(Abel, Galois, Jordan)
Solvable Groups

Def. A group $G$ is *solvable* if there are *normal* subgroups

$$1 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_m \triangleleft G$$

s.t. $H_{k+1}/H_k$ are *abelian*. 
Solvable Groups

Def. A group $G$ is solvable if there are normal subgroups

$$1 \triangleleft H_1 \triangleleft H_2 \triangleleft \cdots \triangleleft H_m \triangleleft G$$

s.t. $H_{k+1}/H_k$ are abelian.

Evariste Galois

Let $K$ be any field ext. of $\mathbb{Q}$, and $F$, an ext. of $K$. Then,

* $F$ is contained in a rad. ext. of $K$ if and only if
  * $\text{Aut}_K(F)$ is solvable,
  * provided that $F/K$ is Galois.
Proof of $\text{Aut}_K(F) \cong S_5$

$$f(x) = x^5 - t_4 x^4 + t_3 x^3 - t_2 x^2 + t_1 x - t_0 = 0$$

has solutions in a radical ext. of $K := \mathbb{Q}(t_0, \ldots, t_4)$. 
Proof of $\text{Aut}_K(F) \approx S_5$

$$f(x) = x^5 - t_4 x^4 + t_3 x^3 - t_2 x^2 + t_1 x - t_0 = 0$$

has solutions in a radical ext. of $K := \mathbb{Q}(t_0, \ldots, t_4)$.

Then, $f(x) = (x - u_1) \cdots (x - u_5)$, and

$$t_4 = u_1 + u_2 + u_3 + u_4 + u_5$$
$$t_3 = u_1 u_2 + u_1 u_3 + u_1 u_4 + \cdots + u_4 u_5$$
$$t_2 = u_1 u_2 u_3 + u_1 u_2 u_4 \cdots + u_3 u_4 u_5$$
$$t_1 = u_1 u_2 u_3 u_4 + u_1 u_2 u_3 u_5 + \cdots + u_2 u_3 u_4 u_5$$
$$t_0 = u_1 u_2 u_3 u_4 u_5$$
**Proof of** $\text{Aut}_K(F) \cong S_5$

$$f(x) = x^5 - t_4 x^4 + t_3 x^3 - t_2 x^2 + t_1 x - t_0 = 0$$

has solutions in a radical ext. of $K := \mathbb{Q}(t_0, \ldots, t_4)$.

Let $v_1, \ldots, v_5$ be indeterminates.

Define $M := \mathbb{Q}(v_1, \ldots, v_5)$ and

$$s_4 := v_1 + v_2 + v_3 + v_4 + v_5$$
$$s_3 := v_1 v_2 + v_1 v_3 + v_1 v_4 + \cdots + v_4 v_5$$
$$s_2 := v_1 v_2 v_3 + v_1 v_2 v_4 + \cdots + v_3 v_4 v_5$$
$$s_1 := v_1 v_2 v_3 v_4 + v_1 v_2 v_3 v_5 + \cdots + v_2 v_3 v_4 v_5$$
$$s_0 := v_1 v_2 v_3 v_4 v_5$$

Define $L := \mathbb{Q}(s_0, \ldots, s_4)$, which is a subfield of $M$. 
Proof of $\text{Aut}_K(F) \cong S_5$

$$f(x) = x^5 - t_4 x^4 + t_3 x^3 - t_2 x^2 + t_1 x - t_0 = 0$$

has solutions in a radical ext. of $K := \mathbb{Q}(t_0, \ldots, t_4)$.

Let $v_1, \ldots, v_5$ be indeterminates.

Define $M := \mathbb{Q}(v_1, \ldots, v_5)$ and

$$s_4 := v_1 + v_2 + v_3 + v_4 + v_5$$
$$s_3 := v_1 v_2 + v_1 v_3 + v_1 v_4 + \cdots + v_4 v_5$$
$$s_2 := v_1 v_2 v_3 + v_1 v_2 v_4 + \cdots + v_3 v_4 v_5$$
$$s_1 := v_1 v_2 v_3 v_4 + v_1 v_2 v_3 v_5 + \cdots + v_2 v_3 v_4 v_5$$
$$s_0 := v_1 v_2 v_3 v_4 v_5$$

Define $L := \mathbb{Q}(s_0, \ldots, s_4)$, which is a subfield of $M$.

$\exists$ field isomorphism $\phi : F \rightarrow M$ s.t. $u_k \mapsto v_k$
Proof of $\text{Aut}_K(F) \approx S_5$

$f(x) = x^5 - t_4 x^4 + t_3 x^3 - t_2 x^2 + t_1 x - t_0 = 0$
has solutions in a radical ext. of $K := \mathbb{Q}(t_0, \ldots, t_4)$.

Let $\nu_1, \ldots, \nu_5$ be indeterminates.

Define $M := \mathbb{Q}(\nu_1, \ldots, \nu_5)$ and

\[
\begin{align*}
s_4 & := \nu_1 + \nu_2 + \nu_3 + \nu_4 + \nu_5 \\
s_3 & := \nu_1 \nu_2 + \nu_1 \nu_3 + \nu_1 \nu_4 + \cdots + \nu_4 \nu_5 \\
s_2 & := \nu_1 \nu_2 \nu_3 + \nu_1 \nu_2 \nu_4 + \cdots + \nu_3 \nu_4 \nu_5 \\
s_1 & := \nu_1 \nu_2 \nu_3 \nu_4 + \nu_1 \nu_2 \nu_3 \nu_5 + \cdots + \nu_2 \nu_3 \nu_4 \nu_5 \\
s_0 & := \nu_1 \nu_2 \nu_3 \nu_4 \nu_5
\end{align*}
\]

Define $L := \mathbb{Q}(s_0, \ldots, s_4)$, which is a subfield of $M$.

$\exists$ field isomorphism $\phi : F \to M$ s.t. $u_k \mapsto \nu_k$

$\text{Aut}_K(F) \approx \text{Aut}_L(M)$
Proof of $\text{Aut}_K(F) \approx S_5$

Proof of $F \approx M$
Proof of $\text{Aut}_K(F') \approx S_5$

Proof of $F \approx M$

Enough to show $s_0, \ldots, s_4$ are "indeterminates," i.e.,

\[ K = \mathbb{Q}(t_0, \ldots, t_4) \approx \mathbb{Q}(s_0, \ldots, s_4) = L. \]
Proof of $\text{Aut}_K(F) \cong S_5$

Proof of $F \cong M$

Enough to show $s_0, \ldots, s_4$ are “indeterminates,” i.e.,
\[ K = \mathbb{Q}(t_0, \ldots, t_4) \cong \mathbb{Q}(s_0, \ldots, s_4) = L. \]

• $s_0, \ldots, s_4$ are “indeterminates”
  if and only if $f(s_0, \ldots, s_4) \neq 0$ for all polynomials $f \neq 0$
  in five variables.
Proof of $\text{Aut}_K(F) \approx S_5$

Proof of $F \approx M$

Enough to show $s_0, \ldots, s_4$ are “indeterminates,” i.e.,

$$K = \mathbb{Q}(t_0, \ldots, t_4) \approx \mathbb{Q}(s_0, \ldots, s_4) = L.$$  

• $s_0, \ldots, s_4$ are “indeterminates”
  if and only if $f(s_0, \ldots, s_4) \neq 0$ for all polynomials $f \neq 0$
  in five variables.

Suppose that $\exists f$ s.t. $f(s_0, \ldots, s_4) = 0$, i.e., $f(v_1 \cdots v_5, \ldots, v_1 + \cdots + v_5) = 0$. 

Proof of $\text{Aut}_K(F) \approx S_5$

Proof of $F \approx M$

Enough to show $s_0, \ldots, s_4$ are “indeterminates,” i.e.,
$$K = \mathbb{Q}(t_0, \ldots, t_4) \approx \mathbb{Q}(s_0, \ldots, s_4) = L.$$

- $s_0, \ldots, s_4$ are “indeterminates”
  if and only if $f(s_0, \ldots, s_4) \neq 0$ for all polynomials $f \neq 0$
in five variables.

Suppose that $\exists f$ s.t. $f(s_0, \ldots, s_4) = 0$, i.e., $f(v_1 \cdots v_5, \ldots, v_1 + \cdots + v_5) = 0$.

Then, $\exists y_0, \ldots, y_4 \in \mathbb{C}$ such that $f(y_0, \ldots, y_4) \neq 0$. 
Proof of Aut$_K(F) \approx S_5$

Proof of $F \approx M$

Enough to show $s_0, \ldots, s_4$ are “indeterminates,” i.e.,

$K = \mathbb{Q}(t_0, \ldots, t_4) \approx \mathbb{Q}(s_0, \ldots, s_4) = L.$

- $s_0, \ldots, s_4$ are “indeterminates”
  if and only if $f(s_0, \ldots, s_4) \neq 0$ for all polynomials $f \neq 0$
  in five variables.

Suppose that $\exists$ $f$ s.t. $f(s_0, \ldots, s_4) = 0$, i.e., $f(v_1 \cdots v_5, \ldots, v_1 + \cdots + v_5) = 0$.

Then, $\exists$ $y_0, \ldots, y_4 \in \mathbb{C}$ such that $f(y_0, \ldots, y_4) \neq 0$.

Hence, $\exists$ $z_1, \ldots, z_5 \in \mathbb{C}$ by F.T.A s.t.

$y_0 = z_1 \cdots z_5, \ldots, y_4 = z_1 + \cdots + z_5,$

$f(z_1 \cdots z_5, \ldots, z_1 + \cdots + z_5) \neq 0.$ QED
Proof of $\text{Aut}_K(F) \approx S_5$

Proof of $F \approx M$

Enough to show $s_0, \ldots, s_4$ are “indeterminates,” i.e.,

$$K = \mathbb{Q}(t_0, \ldots, t_4) \approx \mathbb{Q}(s_0, \ldots, s_4) = L.$$  

• $s_0, \ldots, s_4$ are “indeterminates”
  if and only if $f(s_0, \ldots, s_4) \neq 0$ for all polynomials $f \neq 0$
  in five variables.

Suppose that $\exists f$ s.t. $f(s_0, \ldots, s_4) = 0$, i.e., $f(v_1 \cdots v_5, \ldots, v_1 + \cdots + v_5) = 0$.

Then, $\exists y_0, \ldots, y_4 \in \mathbb{C}$ such that $f(y_0, \ldots, y_4) \neq 0$.

Hence, $\exists z_1, \ldots, z_5 \in \mathbb{C}$ by F.T.A s.t.

$$y_0 = z_1 \cdots z_5, \ldots, y_4 = z_1 + \cdots + z_5,$$

$$f(z_1 \cdots z_5, \ldots, z_1 + \cdots + z_5) \neq 0. \text{ QED}$$

$$\text{Aut}_K(F) \approx \text{Aut}_L(M)$$
Proof of $\text{Aut}_L(M) \approx S_5$

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

- $s_4 := v_1 + v_2 + v_3 + v_4 + v_5$
- $s_3 := v_1v_2 + v_1v_3 + v_1v_4 + \cdots + v_4v_5$
- $s_2 := v_1v_2v_3 + v_1v_2v_4 + \cdots + v_3v_4v_5$
- $s_1 := v_1v_2v_3v_4 + v_1v_2v_3v_5 + \cdots + v_2v_3v_4v_5$
- $s_0 := v_1v_2v_3v_4v_5$
Proof of $\text{Aut}_L(M) \cong S_5$

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

\begin{align*}
  s_4 &:= v_1 + v_2 + v_3 + v_4 + v_5 \\
  s_3 &:= v_1v_2 + v_1v_3 + v_1v_4 + \cdots + v_4v_5 \\
  s_2 &:= v_1v_2v_3 + v_1v_2v_4 + \cdots + v_3v_4v_5 \\
  s_1 &:= v_1v_2v_3v_4 + v_1v_2v_3v_5 + \cdots + v_2v_3v_4v_5 \\
  s_0 &:= v_1v_2v_3v_4v_5
\end{align*}

- $S_5 \hookrightarrow \text{Aut}_L(M)$, i.e., $S_5$ fixes $L$.  

Proof of $\text{Aut}_L(M) \approx S_5$

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

\begin{align*}
s_4 &:= v_1 + v_2 + v_3 + v_4 + v_5 \\
s_3 &:= v_1 v_2 + v_1 v_3 + v_1 v_4 + \cdots + v_4 v_5 \\
s_2 &:= v_1 v_2 v_3 + v_1 v_2 v_4 + \cdots + v_3 v_4 v_5 \\
s_1 &:= v_1 v_2 v_3 v_4 + v_1 v_2 v_3 v_5 + \cdots + v_2 v_3 v_4 v_5 \\
s_0 &:= v_1 v_2 v_3 v_4 v_5
\end{align*}

- $S_5 \hookrightarrow \text{Aut}_L(M)$, i.e., $S_5$ fixes $L$.

- **Galois Theory:** $\forall H \leq \text{Aut}_L(M)$, a subgroup.

\[
M^H := \left\{ x \in M : \sigma(x) = x, \ \forall \sigma \in H \right\},
\]
called the fixed subfield of $H$. 
Proof of $\text{Aut}_L(M) \approx S_5$

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

\begin{align*}
s_4 &:= v_1 + v_2 + v_3 + v_4 + v_5 \\
s_3 &:= v_1v_2 + v_1v_3 + v_1v_4 + \cdots + v_4v_5 \\
s_2 &:= v_1v_2v_3 + v_1v_2v_4 \cdots + v_3v_4v_5 \\
s_1 &:= v_1v_2v_3v_4 + v_1v_2v_3v_5 + \cdots + v_2v_3v_4v_5 \\
s_0 &:= v_1v_2v_3v_4v_5
\end{align*}

- $S_5 \hookrightarrow \text{Aut}_L(M)$, i.e., $S_5$ fixes $L$.

- **Galois Theory:**

\[ \{H \leq \text{Aut}_L(M)\} \rightarrow \{N : L \leq N \leq M\} \text{ given by } H \mapsto M^H \]
Proof of $\text{Aut}_L(M) \cong S_5$

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

$$
s_4 := v_1 + v_2 + v_3 + v_4 + v_5
$$
$$
s_3 := v_1 v_2 + v_1 v_3 + v_1 v_4 + \cdots + v_4 v_5
$$
$$
s_2 := v_1 v_2 v_3 + v_1 v_2 v_4 + \cdots + v_3 v_4 v_5
$$
$$
s_1 := v_1 v_2 v_3 v_4 + v_1 v_2 v_3 v_5 + \cdots + v_2 v_3 v_4 v_5
$$
$$
s_0 := v_1 v_2 v_3 v_4 v_5
$$

- $S_5 \hookrightarrow \text{Aut}_L(M)$, i.e., $S_5$ fixes $L$.

- **Galois Theory:**

  \[
  \{H \leq \text{Aut}_L(M)\} \rightarrow \{N : L \leq N \leq M\} \text{ given by } H \mapsto M^H \]

  is a one-to-one correspondence.
Proof of $\text{Aut}_L(M) \approx S_5$

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

\[
\begin{align*}
    s_4 &:= v_1 + v_2 + v_3 + v_4 + v_5 \\
    s_3 &:= v_1 v_2 + v_1 v_3 + v_1 v_4 + \cdots + v_4 v_5 \\
    s_2 &:= v_1 v_2 v_3 + v_1 v_2 v_4 + \cdots + v_3 v_4 v_5 \\
    s_1 &:= v_1 v_2 v_3 v_4 + v_1 v_2 v_3 v_5 + \cdots + v_2 v_3 v_4 v_5 \\
    s_0 &:= v_1 v_2 v_3 v_4 v_5
\end{align*}
\]

• $S_5 \hookrightarrow \text{Aut}_L(M)$, i.e., $S_5$ fixes $L$.

• Galois Theory:

\[
\{ H \leq \text{Aut}_L(M) \} \rightarrow \{ N : L \leq N \leq M \}
\]

given by $H \mapsto M^H$

is a one-to-one correspondence.

e.g., $\text{Aut}_L(M) \hookrightarrow L$, i.e., $M^{\text{Aut}_L(M)} = L$
Proof of $\text{Aut}_L(M) \cong S_5$

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

\begin{align*}
s_4 &:= v_1 + v_2 + v_3 + v_4 + v_5 \\
s_3 &:= v_1v_2 + v_1v_3 + v_1v_4 + \cdots + v_4v_5 \\
s_2 &:= v_1v_2v_3 + v_1v_2v_4 + \cdots + v_3v_4v_5 \\
s_1 &:= v_1v_2v_3v_4 + v_1v_2v_3v_5 + \cdots + v_2v_3v_4v_5 \\
s_0 &:= v_1v_2v_3v_4v_5
\end{align*}

- $S_5 \hookrightarrow \text{Aut}_L(M)$, i.e., $S_5$ fixes $L$.

- **Galois Theory:** $M^{S_5} := \{ x \in M : \sigma(x) = x, \ \forall \sigma \in S_5 \}$. 
Proof of $\text{Aut}_L(M) \cong S_5$

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

\begin{align*}
s_4 & := v_1 + v_2 + v_3 + v_4 + v_5 \\
ss_3 & := v_1v_2 + v_1v_3 + v_1v_4 + \cdots + v_4v_5 \\
ss_2 & := v_1v_2v_3 + v_1v_2v_4 + \cdots + v_3v_4v_5 \\
ss_1 & := v_1v_2v_3v_4 + v_1v_2v_3v_5 + \cdots + v_2v_3v_4v_5 \\
ss_0 & := v_1v_2v_3v_4v_5
\end{align*}

- $S_5 \hookrightarrow \text{Aut}_L(M)$, i.e., $S_5$ fixes $L$.

- **Galois Theory:** $M^{S_5} := \{x \in M : \sigma(x) = x, \ \forall \sigma \in S_5\}$. $L = M^{S_5}$ and Galois Theory $\Rightarrow S_5 \cong \text{Aut}_L(M)$. 
Proof of $\text{Aut}_L(M) \cong S_5$

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

\[
\begin{align*}
s_4 &:= v_1 + v_2 + v_3 + v_4 + v_5 \\
s_3 &:= v_1 v_2 + v_1 v_3 + v_1 v_4 + \cdots + v_4 v_5 \\
s_2 &:= v_1 v_2 v_3 + v_1 v_2 v_4 + \cdots + v_3 v_4 v_5 \\
s_1 &:= v_1 v_2 v_3 v_4 + v_1 v_2 v_3 v_5 + \cdots + v_2 v_3 v_4 v_5 \\
s_0 &:= v_1 v_2 v_3 v_4 v_5
\end{align*}
\]

- $S_5 \hookrightarrow \text{Aut}_L(M)$, i.e., $S_5$ fixes $L$.

- **Galois Theory**: $M^{S_5} := \{x \in M : \sigma(x) = x, \ \forall \sigma \in S_5\}$. $L = M^{S_5}$ and Galois Theory $\Rightarrow$ $S_5 \cong \text{Aut}_L(M)$.

Why $L = M^{S_5}$?
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \text{ and } L = \mathbb{Q}(s_0, \ldots, s_4) \text{ where} \]

\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5 \]
\[ s_3 := v_1v_2 + v_1v_3 + v_1v_4 + \cdots + v_4v_5 \]
\[ s_2 := v_1v_2v_3 + v_1v_2v_4 + \cdots + v_3v_4v_5 \]
\[ s_1 := v_1v_2v_3v_4 + v_1v_2v_3v_5 + \cdots + v_2v_3v_4v_5 \]
\[ s_0 := v_1v_2v_3v_4v_5 \]

\[ \bullet s_0, \ldots, s_4 \text{ are} \]

\textit{elementary symmetric polynomials} \textit{for} \( n = 5 \).
Symmetric Functions

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

$$s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, s_0 := v_1v_2v_3v_4v_5.$$

Prop. $M^{S_5} = L$; that is, all rational functions fixed under the action of $S_5$ are rational functions in $s_0, \ldots, s_4$.

proof:
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \] and \[ L = \mathbb{Q}(s_0, \ldots, s_4) \] where

\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, s_0 := v_1 v_2 v_3 v_4 v_5. \]

Prop. \[ M^{S_5} = L; \] that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4 \).

proof:
Define an order:

(1) \[ v_1 v_2^2 v_3 v_5 > v_1 v_2 v_3 v_5; \deg(v_1 v_2^2 v_3 v_5) = 5 > 4 = \deg(v_1 v_2 v_3 v_5). \]
Symmetric Functions

\( M := \mathbb{Q}(v_1, \ldots, v_5) \) and \( L = \mathbb{Q}(s_0, \ldots, s_4) \) where
\[
s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, \quad s_0 := v_1 v_2 v_3 v_4 v_5.
\]

Prop. \( M^{S_5} = L \); that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4 \).

proof:
Define an order:

1. \( v_1 v_2^2 v_3 v_5 > v_1 v_2 v_3 v_5 \); \( \deg(v_1 v_2^2 v_3 v_5) = 5 > 4 = \deg(v_1 v_2 v_3 v_5) \).
2. \( v_1 v_2^2 v_3 v_4 > v_1 v_2 v_3^2 v_4 \); \( \deg(v_1 v_2^2 v_3 v_4) = \deg(v_1 v_2 v_3^2 v_4) \).
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \text{ and } L = \mathbb{Q}(s_0, \ldots, s_4) \text{ where} \]
\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, s_0 := v_1v_2v_3v_4v_5. \]

**Prop.** \( M^{S_5} = L; \) that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4. \)

**proof:** Suppose, \( f(v_1, \ldots, v_5) \) is a pol. fixed under the action of \( S_5. \)
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \]  and \[ L = \mathbb{Q}(s_0, \ldots, s_4) \]  where
\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, \]
\[ s_0 := v_1v_2v_3v_4v_5. \]

**Prop.**  \( M^{S_5} = L; \)  that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4. \)

**proof:** Suppose, \( f(v_1, \ldots, v_5) \) is a pol. fixed under the action of \( S_5. \)

\[ f(v_1, \ldots, v_5) = a(v_1^{r_1} \cdots v_5^{r_5} + \cdots + v_5^{r_1} \cdots v_1^{r_5}) \]
\[ + \text{lower-order terms} \]

where \( r_1 \geq r_2 \geq \cdots \geq r_5. \)
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \] and \[ L = \mathbb{Q}(s_0, \ldots, s_4) \] where
\[
    s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, s_0 := v_1v_2v_3v_4v_5.
\]

**Prop.** \( M^{S_5} = L \); that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4 \).

**proof:** Suppose, \( f(v_1, \ldots, v_5) \) is a pol. fixed under the action of \( S_5 \).

\[
    f(v_1, \ldots, v_5) = a(v_1^{r_1} \cdots v_5^{r_5} + \cdots + v_5^{r_1} \cdots v_1^{r_5})
    + \text{lower-order terms}
\]

where \( r_1 \geq r_2 \geq \cdots \geq r_5 \).

E.g., \( v_1^2v_2v_3^3v_4v_5^4 \longrightarrow v_1^4v_2v_3^3v_4v_5 \).
Symmetric Functions

\( M := \mathbb{Q}(v_1, \ldots, v_5) \) and \( L = \mathbb{Q}(s_0, \ldots, s_4) \) where

\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, \]
\[ s_0 := v_1 v_2 v_3 v_4 v_5. \]

Prop. \( M^{S_5} = L \); that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4 \).

proof:

\[ s_4^{d_4} = (v_1 + \cdots + v_5)^{d_4} = v_1^{d_4} + \cdots \]
\[ s_3^{d_3} = (v_1 v_2 + \cdots + v_4 v_5)^{d_3} = v_1^{d_3} v_2^{d_3} + \cdots \]
\[ \cdots \]
\[ s_0^{d_0} = v_1^{d_0} v_2^{d_0} v_3^{d_0} v_4^{d_0} v_5^{d_0} \]
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \text{ and } L = \mathbb{Q}(s_0, \ldots, s_4) \text{ where} \]
\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, \ s_0 := v_1 v_2 v_3 v_4 v_5. \]

Prop. \[ M^{S_5} = L; \] that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4 \).

proof:
\[ s_4^d = (v_1 + \cdots + v_5)^d = v_1^d + \cdots \]
\[ s_3^d = (v_1 v_2 + \cdots + v_4 v_5)^d = v_1^d v_2^d + \cdots \]
\[ \ldots \]
\[ s_0^d = v_1^d v_2^d v_3^d v_4^d v_5^d \]
\[ s_4^d \cdots s_0^d = v_1^{d_4 + \cdots + d_0} v_2^{d_3 + \cdots + d_0} v_3^{d_2 + d_1 + d_0} v_4^{d_1 + d_0} v_5^{d_0} + \cdots \]
Symmetric Functions

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

$s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, s_0 := v_1v_2v_3v_4v_5.$

Prop. $M^{S_5} = L$; that is, all rational functions fixed under the action of $S_5$ are rational functions in $s_0, \ldots, s_4.$

proof:

• $f(v_1, \ldots, v_5) = a(v_1^{r_1} \cdots v_5^{r_5} + \cdots + v_5^{r_1} \cdots v_1^{r_5})$
  + lower-order terms

• $s_4^{d_4} \cdots s_0^{d_0} = v_1^{d_4+\cdots+d_0}v_2^{d_3+\cdots+d_0}v_3^{d_2+d_1+d_0}v_4^{d_1+d_0}v_5^{d_0}$
  + lower-order terms
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \] and \[ L = \mathbb{Q}(s_0, \ldots, s_4) \] where
\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, s_0 := v_1 v_2 v_3 v_4 v_5. \]

**Prop.** \( M^{S_5} = L \); that is, all rational functions fixed under the *action* of \( S_5 \) are rational functions in \( s_0, \ldots, s_4 \).

**proof:**
- \( f(v_1, \ldots, v_5) = a(v_1^{r_1} \cdots v_5^{r_5} + \cdots + v_5^{r_1} \cdots v_1^{r_5}) \) + lower-order terms
- \( s_4^{d_4} \cdots s_0^{d_0} = v_1^{d_4 + \cdots + d_0} v_2^{d_3 + \cdots + d_0} v_3^{d_2 + d_1 + d_0} v_4^{d_1 + d_0} v_5^{d_0} \) + lower-order terms

\[ d_0 := r_5, \ d_1 + d_0 := r_4, \ldots, d_4 + \cdots + d_0 := r_1 \]
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \text{ and } L = \mathbb{Q}(s_0, \ldots, s_4) \text{ where} \]
\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, \ s_0 := v_1 v_2 v_3 v_4 v_5. \]

**Prop.** \( M^{S_5} = L; \) that is, all rational functions fixed under the *action* of \( S_5 \) are rational functions in \( s_0, \ldots, s_4. \)

**proof:**

\[ f(v_1, \ldots, v_5) - a s_4^{d_4} \cdots s_0^{d_0} \] has its highest-order term lower than that of \( f(v_1, \ldots, v_5), \)
and is still symmetric.
Symmetric Functions

\( M := \mathbb{Q}(v_1, \ldots, v_5) \) and \( L = \mathbb{Q}(s_0, \ldots, s_4) \) where

\[
s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, \quad s_0 := v_1v_2v_3v_4v_5.
\]

Prop. \( M^{S_5} = L \); that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4 \).

proof:

\[
f(v_1, \ldots, v_5) - a s_4^{d_4} \cdots s_0^{d_0} \text{ has its highest-order term lower than that of } f(v_1, \ldots, v_5),
\]

and is still symmetric.

By induction, \( f(v_1, \ldots, v_5) \) is a polynomial in \( s_0, \ldots, s_4 \).
Symmetric Functions

$M := \mathbb{Q}(v_1, \ldots, v_5)$ and $L = \mathbb{Q}(s_0, \ldots, s_4)$ where

$$s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, s_0 := v_1 v_2 v_3 v_4 v_5.$$

**Prop.** $M^{S_5} = L$; that is, all rational functions fixed under the action of $S_5$ are rational functions in $s_0, \ldots, s_4$.

**proof:** Let $f = g/h$ be a rational function fixed under the action of $S_5$. 

Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \] and \[ L = \mathbb{Q}(s_0, \ldots, s_4) \] where
\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, s_0 := v_1v_2v_3v_4v_5. \]

Prop. \[ M^{S_5} = L; \] that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4 \).

proof: Let \( f = g/h \) be a rational function fixed under the action of \( S_5 \).

Let \( H := \prod_{\sigma \in S_5} \sigma(h) \), which is a polynomial \( h \cdot \text{(stuff)} \) and fixed under \( S_5 \).
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \text{ and } L = \mathbb{Q}(s_0, \ldots, s_4) \text{ where} \]
\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, \]
\[ s_0 := v_1v_2v_3v_4v_5. \]

Prop. \( M^{S_5} = L; \) that is, all rational functions fixed under the action of \( S_5 \) are rational functions in \( s_0, \ldots, s_4. \)

proof: Let \( f = g/h \) be a rational function fixed under the action of \( S_5. \)

Let \( H := \prod_{\sigma \in S_5} \sigma(h), \) which is a polynomial \( h \cdot \text{(stuff)} \)

and fixed under \( S_5. \)

Thus, \( H \cdot f = g \cdot (H/h) \) is a polynomial fixed under \( S_5, \) and written in terms of \( s_i \)'s.
Symmetric Functions

\[ M := \mathbb{Q}(v_1, \ldots, v_5) \text{ and } L = \mathbb{Q}(s_0, \ldots, s_4) \text{ where } \]
\[ s_4 := v_1 + v_2 + v_3 + v_4 + v_5, \ldots, s_0 := v_1v_2v_3v_4v_5. \]

Prop. \[ M^{S_5} = L; \text{ that is, all rational functions fixed under the action of } S_5 \text{ are rational functions in } s_0, \ldots, s_4. \]

proof: Let \( f = g/h \) be a rational function fixed under the action of \( S_5 \).

Let \( H := \prod_{\sigma \in S_5} \sigma(h), \) which is a polynomial \( h \cdot (\text{stuff}) \) and fixed under \( S_5 \).

Thus, \( H \cdot f = g \cdot (H/h) \) is a polynomial fixed under \( S_5 \), and written in terms of \( s_i \)'s.

\[ f = (H \cdot f)/H \text{ is a rat'l function in } s_i \text{'s.} \]
Fields and Groups

\[ x^n + t_{n-1}x^{n-1} + \cdots + t_1x + t_0 = 0 \text{ for } n \geq 5 \]

\[ K := \mathbb{Q}(t_0, \ldots, t_{n-1}) \]

Suppose, \( F = K(u_1, \ldots, u_n) \) is contained in a rad. ext. of \( K \) where \( u_1, \ldots, u_n \) are \( n \) solutions of the above pol. (written in terms of radicals of \( t_i \)'s).

★ Field theory:

1. radical ext. ⇒ the group \( \text{Aut}_K(F) \) is solvable.
2. polynomial equation ⇒ \( \text{Aut}_K(F) \approx S_n. \)

★ Group theory: \( S_n \) is not solvable if \( n \geq 5. \)

(Abel, Galois, Jordan)
Proof of rad. $\Rightarrow$ solvable group

Example: $X^5 - 7 = 0$.

$K = \mathbb{Q}(\zeta_5)$ and $F = \mathbb{Q}(\zeta_5, \sqrt[5]{7})$ where $\zeta_5$ is a primitive fifth root of 1.
Proof of rad. ⇒ solvable group

Example: $X^5 - 7 = 0$.

$K = \mathbb{Q}(\zeta_5)$ and $F = \mathbb{Q}(\zeta_5, \sqrt[5]{7})$ where $\zeta_5$ is a primitive fifth root of 1.

- $\text{Aut}_K(F) \cong \mathbb{Z}/5\mathbb{Z}$; abelian.

$$\sigma \in \text{Aut}_K(F) \Rightarrow \sigma(\sqrt[5]{7}) = \sqrt[5]{7}\zeta^a_5.$$
Proof of rad. $\Rightarrow$ solvable group

Example: $X^5 - 7 = 0$.

$K = \mathbb{Q}(\zeta_5)$ and $F = \mathbb{Q}(\zeta_5, \sqrt[5]{7})$ where $\zeta_5$ is a primitive fifth root of 1.

- $\text{Aut}_K(F) \approx \mathbb{Z}/5\mathbb{Z}$; abelian.
  
  $\sigma \in \text{Aut}_K(F) \Rightarrow \sigma(\sqrt[5]{7}) = \sqrt[5]{7} \zeta_5^a$.

- $\text{Aut}_\mathbb{Q}(F)/\text{Aut}_K(F) \approx \text{Aut}_\mathbb{Q}(K) \approx \mathbb{Z}/4\mathbb{Z}$; abelian.
Proof of rad. ⇒ solvable group

Example: \(X^5 - 7 = 0\).

\[K = \mathbb{Q}(\zeta_5)\text{ and } F = \mathbb{Q}(\zeta_5, \sqrt[5]{7})\text{ where }\zeta_5\text{ is a primitive fifth root of }1.\]

- \(\text{Aut}_K(F) \approx \mathbb{Z}/5\mathbb{Z};\text{ abelian.}\)
  \[\sigma \in \text{Aut}_K(F) \Rightarrow \sigma(\sqrt[5]{7}) = \sqrt[5]{7} \zeta_5^a.\]

- \(\text{Aut}_Q(F)/\text{Aut}_K(F) \approx \text{Aut}_Q(K) \approx \mathbb{Z}/4\mathbb{Z};\text{ abelian.}\)

\[1 \triangleleft \text{Aut}_K(F) \triangleleft \text{Aut}_Q(F).\]
Proof of $S_n$ being not solvable

Def. The alternating group $A_n$ is the subgroup of $S_n$ consisting of permutations obtained by an even-number of transpositions.
Proof of $S_n$ being not solvable

Def.  The alternating group $A_n$ is
the subgroup of $S_n$ consisting of
permutations obtained by
an even-number of transpositions.

★ $A_n$ is simple if $n \geq 5$, i.e.,
it does not contain a nontriv. normal subgroup.
Proof of $S_n$ being not solvable

Def. The alternating group $A_n$ is the subgroup of $S_n$ consisting of permutations obtained by an even-number of transpositions.

★ $A_n$ is simple if $n \geq 5$, i.e., it does not contain a nontriv. normal subgroup.

$$1 \lhd A_n \lhd S_n$$

$A_n$ is not abelian.
Fields and Groups

\[ x^n + t_{n-1}x^{n-1} + \cdots + t_1x + t_0 = 0 \text{ for } n \geq 5 \]

\[ K := \mathbb{Q}(t_0, \ldots, t_{n-1}) \]

Suppose, \( F = K(u_1, \ldots, u_n) \) is contained in a rad. ext. of \( K \) where \( u_1, \ldots, u_n \) are \( n \) solutions of the above pol. (written in terms of radicals of \( t_i \)'s).

★ Field theory:
  
  (1) radical ext. ⇒ the group \( \text{Aut}_K(F) \) is solvable.
  (2) polynomial equation ⇒ \( \text{Aut}_K(F) \approx S_n \).

★ Group theory: \( S_n \) is not solvable if \( n \geq 5 \).

(Abel, Galois, Jordan)