# Math-123: Insolvability of the quintic

Sebastien Vasey

Harvard University

April 24, 2020

Today we study the following:

### Question

If $f(x) \in \mathbb{Q}[x]$, when is there a formula for the roots of $f(x)$ using just addition, multiplication, and extraction of roots?

# Simple radical extensions

We first study adjunctions of $n$th roots.

### Definition

An extension $K/F$ is a *simple radical extension* if it is obtained (for some $n$) by adjoining the $n$th root of an element $a$ of $F$:
$K = F(b)$, where $b^n = a$.

# Simple radical extensions

We first study adjunctions of $n$th roots.

### Definition

An extension $K/F$ is a *simple radical extension* if it is obtained (for some $n$) by adjoining the $n$th root of an element $a$ of $F$:
$K = F(b)$, where $b^n = a$.
Abuse of notation: we will also write $K = F(\sqrt[n]{a})$.

# Simple radical extensions

We first study adjunctions of $n$th roots.

### Definition

An extension $K/F$ is a *simple radical extension* if it is obtained (for some $n$) by adjoining the $n$th root of an element $a$ of $F$:
$K = F(b)$, where $b^n = a$.
Abuse of notation: we will also write $K = F(\sqrt[n]{a})$.

Note: such an extension $K/F$ will be Galois if and only if it contains *all* the roots of $x^n - a$ if and only if $F$ contains all the $n$th roots of unity.

# Simple radical extensions

We first study adjunctions of $n$th roots.

## Definition

An extension $K/F$ is a *simple radical extension* if it is obtained (for some $n$) by adjoining the $n$th root of an element $a$ of $F$:
$K = F(b)$, where $b^n = a$.
Abuse of notation: we will also write $K = F(\sqrt[n]{a})$.

Note: such an extension $K/F$ will be Galois if and only if it contains *all* the roots of $x^n - a$ if and only if $F$ contains all the $n$th roots of unity.

This explains why $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ is Galois, but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not: $-1, 1$ are the square roots of unity, but $\mathbb{Q}$ does not contain all cube roots of unity.

### Definition

An extension $K/F$ is *cyclic* if it is Galois with cyclic Galois group.

### Definition

An extension $K/F$ is *cyclic* if it is Galois with cyclic Galois group.

### Proposition

Let $F$ be a field of characteristic not dividing $n$, containing all the $n$th roots of unity. For any $a \in F$, $K = F(\sqrt[n]{a})$ is cyclic over $F$, of degree dividing $n$.

### Proof.

$x^n - a$ is separable because the characteristic does not divide $n$.

## Definition

An extension $K/F$ is *cyclic* if it is Galois with cyclic Galois group.

## Proposition

Let $F$ be a field of characteristic not dividing $n$, containing all the $n$th roots of unity. For any $a \in F$, $K = F(\sqrt[n]{a})$ is cyclic over $F$, of degree dividing $n$.

## Proof.

$x^n - a$ is separable because the characteristic does not divide $n$. $K/F$ is the splitting field, hence a Galois extension.

## Definition

An extension $K/F$ is *cyclic* if it is Galois with cyclic Galois group.

## Proposition

Let $F$ be a field of characteristic not dividing $n$, containing all the $n$th roots of unity. For any $a \in F$, $K = F(\sqrt[n]{a})$ is cyclic over $F$, of degree dividing $n$.

## Proof.

$x^n - a$ is separable because the characteristic does not divide $n$.
$K/F$ is the splitting field, hence a Galois extension.
If $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(\sqrt[n]{a})$ is also a root of $x^n - a$, so $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$, for some $n$th root of unity $\zeta_\sigma$.

### Definition

An extension $K/F$ is *cyclic* if it is Galois with cyclic Galois group.

### Proposition

Let $F$ be a field of characteristic not dividing $n$, containing all the $n$th roots of unity. For any $a \in F$, $K = F(\sqrt[n]{a})$ is cyclic over $F$, of degree dividing $n$.

### Proof.

$x^n - a$ is separable because the characteristic does not divide $n$.
$K/F$ is the splitting field, hence a Galois extension.
If $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(\sqrt[n]{a})$ is also a root of $x^n - a$, so $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$, for some $n$th root of unity $\zeta_\sigma$.
Thus $\sigma \mapsto \zeta_\sigma$ gives a map $\mathrm{Aut}(K/F) \to \mu_n$, where $\mu_n$ is the group of $n$th root of unity. This map is an injective homomorphism, and $\mu_n$ is cyclic of order $n$. □

**Definition**

An extension $K/F$ is *cyclic* if it is Galois with cyclic Galois group.

**Proposition**

Let $F$ be a field of characteristic not dividing $n$, containing all the $n$th roots of unity. For any $a \in F$, $K = F(\sqrt[n]{a})$ is cyclic over $F$, of degree dividing $n$.

**Proof.**

$x^n - a$ is separable because the characteristic does not divide $n$.
$K/F$ is the splitting field, hence a Galois extension.
If $\sigma \in \mathrm{Aut}(K/F)$, then $\sigma(\sqrt[n]{a})$ is also a root of $x^n - a$, so $\sigma(\sqrt[n]{a}) = \zeta_\sigma \sqrt[n]{a}$, for some $n$th root of unity $\zeta_\sigma$.
Thus $\sigma \mapsto \zeta_\sigma$ gives a map $\mathrm{Aut}(K/F) \to \mu_n$, where $\mu_n$ is the group of $n$th root of unity. This map is an injective homomorphism, and $\mu_n$ is cyclic of order $n$. □

**Question:** What about the converse?

### Theorem

Let $K/F$ be a cyclic extension of degree $n$. If the characteristic of $F$ does not divide $n$ and $F$ contains the $n$th roots of unity, then $K = F(\sqrt[n]{a})$ for some $a \in F$.

### Theorem

Let $K/F$ be a cyclic extension of degree $n$. If the characteristic of $F$ does not divide $n$ and $F$ contains the $n$th roots of unity, then $K = F(\sqrt[n]{a})$ for some $a \in F$.

**Proof:** Fix a generator $\sigma \in \mathrm{Aut}(K/F)$.

### Theorem

Let $K/F$ be a cyclic extension of degree $n$. If the characteristic of $F$ does not divide $n$ and $F$ contains the $n$th roots of unity, then $K = F(\sqrt[n]{a})$ for some $a \in F$.

**Proof:** Fix a generator $\sigma \in \mathrm{Aut}(K/F)$.

### Definition

For $\alpha \in K$ and any $n$th roof of unity $\zeta$, the *Lagrange resolvent of* $\alpha$ *and* $\zeta$ is:

$$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

## Theorem

Let $K/F$ be a cyclic extension of degree $n$. If the characteristic of $F$ does not divide $n$ and $F$ contains the $n$th roots of unity, then $K = F(\sqrt[n]{a})$ for some $a \in F$.

**Proof:** Fix a generator $\sigma \in \mathrm{Aut}(K/F)$.

## Definition

For $\alpha \in K$ and any $n$th roof of unity $\zeta$, the *Lagrange resolvent of $\alpha$ and $\zeta$* is:

$$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

Since $\zeta \in F$, it is fixed by $\sigma$, so:

$$\sigma((\alpha, \zeta)) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \ldots + +\zeta^{n-2}\sigma^{n-1}(\alpha) + \zeta^{n-1}\alpha$$

### Theorem

Let $K/F$ be a cyclic extension of degree $n$. If the characteristic of $F$ does not divide $n$ and $F$ contains the $n$th roots of unity, then $K = F(\sqrt[n]{a})$ for some $a \in F$.

**Proof:** Fix a generator $\sigma \in \mathrm{Aut}(K/F)$.

### Definition

For $\alpha \in K$ and any $n$th roof of unity $\zeta$, the *Lagrange resolvent of* $\alpha$ *and* $\zeta$ is:

$$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$$

Since $\zeta \in F$, it is fixed by $\sigma$, so:

$$\sigma((\alpha, \zeta)) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \ldots + +\zeta^{n-2}\sigma^{n-1}(\alpha) + \zeta^{n-1}\alpha$$

Thus $\sigma((\alpha, \zeta)) = \zeta^{-1}(\alpha, \zeta)$.

**Setup:** $\sigma$ a generator of $\mathrm{Aut}(K/F)$,
$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$

**Setup:** $\sigma$ a generator of $\mathrm{Aut}(K/F)$,
$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$
$\sigma((\alpha, \zeta)) = \zeta^{-1}(\alpha, \zeta)$.

**Setup:** $\sigma$ a generator of $\mathrm{Aut}(K/F)$,
$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$
$\sigma((\alpha, \zeta)) = \zeta^{-1}(\alpha, \zeta)$.
So $\sigma((\alpha, \zeta)^n) = \zeta^{-n}(\alpha, \zeta)^n = (\alpha, \zeta)^n$. This shows $(\alpha, \zeta)^n \in F$.

**Setup:** $\sigma$ a generator of $\mathrm{Aut}(K/F)$,
$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$

$\sigma((\alpha, \zeta)) = \zeta^{-1}(\alpha, \zeta)$.

So $\sigma((\alpha, \zeta)^n) = \zeta^{-n}(\alpha, \zeta)^n = (\alpha, \zeta)^n$. This shows $(\alpha, \zeta)^n \in F$.

Let $\zeta$ be a *primitive* $n$th root of unity. We now want to see $K = F((\alpha, \zeta))$, for some $\alpha \in K$.

**Setup:** $\sigma$ a generator of $\mathrm{Aut}(K/F)$,
$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$

$\sigma((\alpha, \zeta)) = \zeta^{-1}(\alpha, \zeta)$.

So $\sigma((\alpha, \zeta)^n) = \zeta^{-n}(\alpha, \zeta)^n = (\alpha, \zeta)^n$. This shows $(\alpha, \zeta)^n \in F$.

Let $\zeta$ be a *primitive* $n$th root of unity. We now want to see $K = F((\alpha, \zeta))$, for some $\alpha \in K$.

Recall from the proof of the fundamental theorem of Galois theory that $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent characters. Thus there must exist $\alpha \in K$ so that $(\alpha, \zeta) \neq 0$.

**Setup:** $\sigma$ a generator of $\mathrm{Aut}(K/F)$,
$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$

$\sigma((\alpha, \zeta)) = \zeta^{-1}(\alpha, \zeta)$.

So $\sigma((\alpha, \zeta)^n) = \zeta^{-n}(\alpha, \zeta)^n = (\alpha, \zeta)^n$. This shows $(\alpha, \zeta)^n \in F$.

Let $\zeta$ be a *primitive* $n$th root of unity. We now want to see $K = F((\alpha, \zeta))$, for some $\alpha \in K$.

Recall from the proof of the fundamental theorem of Galois theory that $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent characters. Thus there must exist $\alpha \in K$ so that $(\alpha, \zeta) \neq 0$.

Since $\zeta$ is primitive, $\zeta^{-i}(\alpha, \zeta) \neq (\alpha, \zeta)$ for any $1 \leq i < n$. Thus $\sigma^i$ does not fix $(\alpha, \zeta)$ for $1 \leq i < n$.

**Setup:** $\sigma$ a generator of $\mathrm{Aut}(K/F)$,
$(\alpha, \zeta) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \ldots + \zeta^{n-1}\sigma^{n-1}(\alpha)$

$\sigma((\alpha, \zeta)) = \zeta^{-1}(\alpha, \zeta)$.

So $\sigma((\alpha, \zeta)^n) = \zeta^{-n}(\alpha, \zeta)^n = (\alpha, \zeta)^n$. This shows $(\alpha, \zeta)^n \in F$.

Let $\zeta$ be a *primitive* $n$th root of unity. We now want to see $K = F((\alpha, \zeta))$, for some $\alpha \in K$.

Recall from the proof of the fundamental theorem of Galois theory that $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are linearly independent characters. Thus there must exist $\alpha \in K$ so that $(\alpha, \zeta) \neq 0$.

Since $\zeta$ is primitive, $\zeta^{-i}(\alpha, \zeta) \neq (\alpha, \zeta)$ for any $1 \leq i < n$. Thus $\sigma^i$ does not fix $(\alpha, \zeta)$ for $1 \leq i < n$.

By the fundamental theorem of Galois theory, $F((\alpha, \zeta))$ is not a proper subfield of $K$: $F((\alpha, \zeta)) = K$. This completes the proof.

# Root extensions

From now on, let $F$ be a field of characteristic zero.

# Root extensions

From now on, let $F$ be a field of characteristic zero.

## Definition

An extension $K/F$ is a *root extension* if there exists a chain of subfields $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$, where for all $i < s$, $K_{i+1}$ is a simple radical extension of $K_i$ ($K_{i+1} = K_i(\sqrt[n]{a_i})$, for some $a_i \in K_i$).

# Root extensions

From now on, let $F$ be a field of characteristic zero.

## Definition

An extension $K/F$ is a *root extension* if there exists a chain of subfields $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$, where for all $i < s$, $K_{i+1}$ is a simple radical extension of $K_i$ ($K_{i+1} = K_i(\sqrt[n]{a_i})$, for some $a_i \in K_i$).

## Definition

An element $\alpha$ (in some extension of $F$) *can be expressed by radicals* if $\alpha$ is in a root extension of $F$.

# Root extensions

From now on, let $F$ be a field of characteristic zero.

## Definition

An extension $K/F$ is a *root extension* if there exists a chain of subfields $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$, where for all $i < s$, $K_{i+1}$ is a simple radical extension of $K_i$ ($K_{i+1} = K_i(\sqrt[n]{a_i})$, for some $a_i \in K_i$).

## Definition

An element $\alpha$ (in some extension of $F$) *can be expressed by radicals* if $\alpha$ is in a root extension of $F$.

## Definition

A polynomial $f(x) \in F[x]$ *can be solved by radicals* if all its roots can be expressed by radicals.

# Example

- $\sqrt[171]{\sqrt{2}+\sqrt{5}}$ can be expressed by radicals over $\mathbb{Q}$:

# Example

- $\sqrt[171]{\sqrt{2}+\sqrt{5}}$ can be expressed by radicals over $\mathbb{Q}$: take $K_0 = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = K_1(\sqrt{5})$, $K_3 = K_2(\sqrt[171]{\sqrt{2}+\sqrt{5}})$.
- Any constructible number can be expressed by radicals over $\mathbb{Q}$.

# Example

- $\sqrt[171]{\sqrt{2}+\sqrt{5}}$ can be expressed by radicals over $\mathbb{Q}$: take $K_0 = \mathbb{Q}$, $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = K_1(\sqrt{5})$, $K_3 = K_2(\sqrt[171]{\sqrt{2}+\sqrt{5}})$.
- Any constructible number can be expressed by radicals over $\mathbb{Q}$.
- $\sqrt[3]{2}$ can be expressed by radicals over $\mathbb{Q}$, but is not constructible.

# Composite of root extensions

## Lemma

The composite of a simple radical extension with a root extension is a root extension.

# Composite of root extensions

## Lemma

The composite of a simple radical extension with a root extension is a root extension.

## Proof.

Let $F = K_0 \subseteq K_1 \ldots \subseteq K_s = K$ be a root extension, and let $K'/F$ be a simple radical extension: $K' = F(\sqrt[n]{a})$.

# Composite of root extensions

## Lemma

The composite of a simple radical extension with a root extension is a root extension.

## Proof.

Let $F = K_0 \subseteq K_1 \ldots \subseteq K_s = K$ be a root extension, and let $K'/F$ be a simple radical extension: $K' = F(\sqrt[n]{a})$.
Say $K_{i+1} = K_i(\sqrt[n_i]{a_i})$. Then $K'K_{i+1} = (K'K_i)(\sqrt[n_i]{a_i})$.

# Composite of root extensions

## Lemma

The composite of a simple radical extension with a root extension is a root extension.

## Proof.

Let $F = K_0 \subseteq K_1 \ldots \subseteq K_s = K$ be a root extension, and let $K'/F$ be a simple radical extension: $K' = F(\sqrt[n]{a})$.
Say $K_{i+1} = K_i(\sqrt[n_i]{a_i})$. Then $K'K_{i+1} = (K'K_i)(\sqrt[n_i]{a_i})$.
So $F \subseteq K' = K_0K' \subseteq K_1K' \subseteq \ldots \subseteq K_sK' = KK'$ shows $KK'$ is a root extension. $\square$

# Composite of root extensions

## Lemma

The composite of a simple radical extension with a root extension is a root extension.

## Proof.

Let $F = K_0 \subseteq K_1 \ldots \subseteq K_s = K$ be a root extension, and let $K'/F$ be a simple radical extension: $K' = F(\sqrt[n]{a})$.
Say $K_{i+1} = K_i(\sqrt[n_i]{a_i})$. Then $K'K_{i+1} = (K'K_i)(\sqrt[n_i]{a_i})$.
So $F \subseteq K' = K_0K' \subseteq K_1K' \subseteq \ldots \subseteq K_sK' = KK'$ shows $KK'$ is a root extension. □

## Lemma

Composite of root extensions are root extensions.

# Composite of root extensions

## Lemma

The composite of a simple radical extension with a root extension is a root extension.

## Proof.

Let $F = K_0 \subseteq K_1 \ldots \subseteq K_s = K$ be a root extension, and let $K'/F$ be a simple radical extension: $K' = F(\sqrt[n]{a})$.
Say $K_{i+1} = K_i(\sqrt[n_i]{a_i})$. Then $K'K_{i+1} = (K'K_i)(\sqrt[n_i]{a_i})$.
So $F \subseteq K' = K_0K' \subseteq K_1K' \subseteq \ldots \subseteq K_sK' = KK'$ shows $KK'$ is a root extension. □

## Lemma

Composite of root extensions are root extensions.

## Proof.

Say $F = K_0 \subseteq \ldots \subseteq K_s = K$ is a root extension, $K'/F$ is another root extension. Then $F \subseteq K_0K' \subseteq \ldots \subseteq K_sK'$ is an iteration of root extensions, hence a root extension. □

# More lemmas on root extensions

**Lemma**

If $K/F$ is a root extension, then its Galois closure $L/F$ is a root extension.

# More lemmas on root extensions

## Lemma

If $K/F$ is a root extension, then its Galois closure $L/F$ is a root extension.

## Proof.

Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension.

# More lemmas on root extensions

## Lemma

If $K/F$ is a root extension, then its Galois closure $L/F$ is a root extension.

## Proof.

Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension.
If $\sigma \in \mathrm{Aut}(L/F)$, then we get a chain of subfields
$F = K_0 = \sigma[K_0] \subseteq \sigma[K_1] \subseteq \ldots \subseteq \sigma[K_s] = \sigma[K]$.

# More lemmas on root extensions

## Lemma

If $K/F$ is a root extension, then its Galois closure $L/F$ is a root extension.

## Proof.

Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension.
If $\sigma \in \mathrm{Aut}(L/F)$, then we get a chain of subfields
$F = K_0 = \sigma[K_0] \subseteq \sigma[K_1] \subseteq \ldots \subseteq \sigma[K_s] = \sigma[K]$.
Note $\sigma[K_{i+1}]/\sigma[K_i]$ is a simple radical extension. Thus $\sigma[K]/F$ is a root extension.

# More lemmas on root extensions

## Lemma

If $K/F$ is a root extension, then its Galois closure $L/F$ is a root extension.

## Proof.

Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension.
If $\sigma \in \mathrm{Aut}(L/F)$, then we get a chain of subfields
$F = K_0 = \sigma[K_0] \subseteq \sigma[K_1] \subseteq \ldots \subseteq \sigma[K_s] = \sigma[K]$.
Note $\sigma[K_{i+1}]/\sigma[K_i]$ is a simple radical extension. Thus $\sigma[K]/F$ is a root extension.
$L$ is the composite of all the $\sigma[K]/F$'s, for $\sigma \in \mathrm{Aut}(K/F)$, so is a root extension. □

# One more lemma

## Lemma

If $K/F$ is a Galois root extension. Then there exists subfields $F = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_s = K$ such that $K'_{i+1}/K'_i$ is cyclic.

# One more lemma

## Lemma

If $K/F$ is a Galois root extension. Then there exists subfields $F = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_s = K$ such that $K'_{i+1}/K'_i$ is cyclic.

**Proof:** Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension. Say $K_{i+1} = \sqrt[n_i]{a_i}$, $a_i \in K_i$.

# One more lemma

## Lemma

If $K/F$ is a Galois root extension. Then there exists subfields $F = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_s = K$ such that $K'_{i+1}/K'_i$ is cyclic.

**Proof:** Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension. Say $K_{i+1} = \sqrt[n_i]{a_i}$, $a_i \in K_i$.

Since $K/F$ is Galois, $K/K_i$ is Galois for all $i$, so all the $n_i$th roots of $a_i$ are in $K$, so the $n_i$th roots of unity are in $K$.

# One more lemma

## Lemma

If $K/F$ is a Galois root extension. Then there exists subfields $F = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_s = K$ such that $K'_{i+1}/K'_i$ is cyclic.

**Proof:** Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension. Say $K_{i+1} = \sqrt[n_i]{a_i}$, $a_i \in K_i$.

Since $K/F$ is Galois, $K/K_i$ is Galois for all $i$, so all the $n_i$th roots of $a_i$ are in $K$, so the $n_i$th roots of unity are in $K$.

Let $F'$ be the smallest extension of $F$ with all the $n_i$th roots of unity, for each $i$. This is a root extension.

# One more lemma

## Lemma

If $K/F$ is a Galois root extension. Then there exists subfields $F = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_s = K$ such that $K'_{i+1}/K'_i$ is cyclic.

**Proof:** Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension. Say $K_{i+1} = \sqrt[n_i]{a_i}$, $a_i \in K_i$.

Since $K/F$ is Galois, $K/K_i$ is Galois for all $i$, so all the $n_i$th roots of $a_i$ are in $K$, so the $n_i$th roots of unity are in $K$.

Let $F'$ be the smallest extension of $F$ with all the $n_i$th roots of unity, for each $i$. This is a root extension.

We get a chain $F \subseteq F' = F'K_0 \subseteq F'K_1 \ldots \subseteq F'K_s = K$.

# One more lemma

**Lemma**

If $K/F$ is a Galois root extension. Then there exists subfields $F = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_s = K$ such that $K'_{i+1}/K'_i$ is cyclic.

**Proof:** Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension. Say $K_{i+1} = \sqrt[n_i]{a_i}$, $a_i \in K_i$.

Since $K/F$ is Galois, $K/K_i$ is Galois for all $i$, so all the $n_i$th roots of $a_i$ are in $K$, so the $n_i$th roots of unity are in $K$.

Let $F'$ be the smallest extension of $F$ with all the $n_i$th roots of unity, for each $i$. This is a root extension.

We get a chain $F \subseteq F' = F'K_0 \subseteq F'K_1 \ldots \subseteq F'K_s = K$.

For each $i$, $F'K_{i+1}/F'K_i$ is a simple radical extension where the base contains the relevant roots of unity so it is a cyclic extension.

# One more lemma

## Lemma

If $K/F$ is a Galois root extension. Then there exists subfields $F = K'_0 \subseteq K'_1 \subseteq \ldots \subseteq K'_s = K$ such that $K'_{i+1}/K'_i$ is cyclic.

**Proof:** Let $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ witness that $K$ is a root extension. Say $K_{i+1} = \sqrt[n_i]{a_i}$, $a_i \in K_i$.

Since $K/F$ is Galois, $K/K_i$ is Galois for all $i$, so all the $n_i$th roots of $a_i$ are in $K$, so the $n_i$th roots of unity are in $K$.

Let $F'$ be the smallest extension of $F$ with all the $n_i$th roots of unity, for each $i$. This is a root extension.

We get a chain $F \subseteq F' = F'K_0 \subseteq F'K_1 \ldots \subseteq F'K_s = K$.

For each $i$, $F'K_{i+1}/F'K_i$ is a simple radical extension where the base contains the relevant roots of unity so it is a cyclic extension. $F'/F$ is a composite of cyclotomic extensions, hence abelian, so can be written as an iteration of cyclic extensions. Done!

In conclusion, we have shown:

### Theorem

If $K/F$ is a root extension, then there is an extension $L$ of $K$ such that:

1. $L/F$ is Galois.
2. There exists subfield $F = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_s = L$ such that $L_{i+1}/L_i$ is a cyclic extension.

# Some group theory

## Definition

A finite group $G$ is *solvable* if there exists a chain of subgroups $1 = G_s \subseteq G_{s-1} \subseteq \ldots \subseteq G_0 = G$ such that $G_i / G_{i+1}$ is cyclic for all $i$.

# Some group theory

## Definition

A finite group $G$ is *solvable* if there exists a chain of subgroups $1 = G_s \subseteq G_{s-1} \subseteq \ldots \subseteq G_0 = G$ such that $G_i/G_{i+1}$ is cyclic for all $i$.

**Exercise 1:** If $H$ is a normal subgroup of $G$, then $G$ is solvable if and only if $G/H$ and $H$ are both solvable.

# Some group theory

### Definition

A finite group $G$ is *solvable* if there exists a chain of subgroups $1 = G_s \subseteq G_{s-1} \subseteq \ldots \subseteq G_0 = G$ such that $G_i/G_{i+1}$ is cyclic for all $i$.

**Exercise 1:** If $H$ is a normal subgroup of $G$, then $G$ is solvable if and only if $G/H$ and $H$ are both solvable.

**Exercise 2:** Show that "cyclic" can be replaced by "abelian" in the definition.

# Some group theory

### Definition

A finite group $G$ is *solvable* if there exists a chain of subgroups $1 = G_s \subseteq G_{s-1} \subseteq \ldots \subseteq G_0 = G$ such that $G_i/G_{i+1}$ is cyclic for all $i$.

**Exercise 1:** If $H$ is a normal subgroup of $G$, then $G$ is solvable if and only if $G/H$ and $H$ are both solvable.

**Exercise 2:** Show that "cyclic" can be replaced by "abelian" in the definition.

**Exercise 3:** The alternating group $A_n$ and the symmetric group $S_n$ are solvable if and only if $n \leq 4$ (use that $A_n$ is simple for $n \geq 5$ — see DF).

We will show:

**Theorem**

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

We will show:

### Theorem

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

### Corollary

If a polynomial in $\mathbb{Q}[x]$ has Galois group $S_n$ for $n \geq 5$, then it cannot be solved by radicals.

We will show:

**Theorem**

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Corollary**

If a polynomial in $\mathbb{Q}[x]$ has Galois group $S_n$ for $n \geq 5$, then it cannot be solved by radicals.

We will also see that the polynomial $f(x) = x^5 - 6x + 3$ has Galois group $S_5$, so is a specific example that cannot be solved by radicals.

We will show:

### Theorem

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

### Corollary

If a polynomial in $\mathbb{Q}[x]$ has Galois group $S_n$ for $n \geq 5$, then it cannot be solved by radicals.

We will also see that the polynomial $f(x) = x^5 - 6x + 3$ has Galois group $S_5$, so is a specific example that cannot be solved by radicals.

On the other hand, any polynomial of degree 4 or less can be solved by radicals.

(recall that $F$ has characteristic zero)

### Theorem

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Rightarrow$:** Assume $f(x)$ can be solved by radicals. By definition each root of $f(x)$ is contained in a root extension.

(recall that $F$ has characteristic zero)

### Theorem

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Rightarrow$:** Assume $f(x)$ can be solved by radicals. By definition each root of $f(x)$ is contained in a root extension.

By previous lemmas, each root of $f(x)$ is contained in a *Galois* root extension. Let $L/F$ be the composite of these extensions. It is again a Galois root extension.

(recall that $F$ has characteristic zero)

**Theorem**

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Rightarrow$:** Assume $f(x)$ can be solved by radicals. By definition each root of $f(x)$ is contained in a root extension.

By previous lemmas, each root of $f(x)$ is contained in a *Galois* root extension. Let $L/F$ be the composite of these extensions. It is again a Galois root extension.

Let $L_0 = F \subseteq L_1 \subseteq \ldots \subseteq L_s = L$ be intermediate subfields such that $L_{i+1}/L_i$ is cyclic for each $i < s$.

(recall that $F$ has characteristic zero)

### Theorem

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Rightarrow$:** Assume $f(x)$ can be solved by radicals. By definition each root of $f(x)$ is contained in a root extension.

By previous lemmas, each root of $f(x)$ is contained in a *Galois* root extension. Let $L/F$ be the composite of these extensions. It is again a Galois root extension.

Let $L_0 = F \subseteq L_1 \subseteq \ldots \subseteq L_s = L$ be intermediate subfields such that $L_{i+1}/L_i$ is cyclic for each $i < s$.

Let $G_i$ be the subgroup of the Galois group corresponding to $L_i$. By the fundamental theorem of Galois theory, $G_i/G_{i+1}$ is cyclic. Thus the Galois group $G_0 = \mathrm{Aut}(L/F)$ is solvable.

(recall that $F$ has characteristic zero)

**Theorem**

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Rightarrow$:** Assume $f(x)$ can be solved by radicals. By definition each root of $f(x)$ is contained in a root extension.

By previous lemmas, each root of $f(x)$ is contained in a *Galois* root extension. Let $L/F$ be the composite of these extensions. It is again a Galois root extension.

Let $L_0 = F \subseteq L_1 \subseteq \ldots \subseteq L_s = L$ be intermediate subfields such that $L_{i+1}/L_i$ is cyclic for each $i < s$.

Let $G_i$ be the subgroup of the Galois group corresponding to $L_i$. By the fundamental theorem of Galois theory, $G_i/G_{i+1}$ is cyclic. Thus the Galois group $G_0 = \mathrm{Aut}(L/F)$ is solvable.

The splitting field of $f(x)$ is a subfield of $L$, hence its Galois group is a quotient of $G_0$, hence solvable.

### Theorem

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Leftarrow$:** Assume the Galois group $G$ of $f(x)$ is solvable. Let $K/F$ be the splitting field of $f(x)$. Let $1 = G_s \subseteq G_{s-1} \ldots \subseteq G_0 = G$ witness solvability, and let $K_i$ be the fixed field of $G_i$.

### Theorem

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Leftarrow$:** Assume the Galois group $G$ of $f(x)$ is solvable. Let $K/F$ be the splitting field of $f(x)$. Let $1 = G_s \subseteq G_{s-1} \ldots \subseteq G_0 = G$ witness solvability, and let $K_i$ be the fixed field of $G_i$.

We have that $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ are subfields so that $K_{i+1}/K_i$ is a cyclic extension for each $i < s$.

**Theorem**

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Leftarrow$:** Assume the Galois group $G$ of $f(x)$ is solvable. Let $K/F$ be the splitting field of $f(x)$. Let $1 = G_s \subseteq G_{s-1} \ldots \subseteq G_0 = G$ witness solvability, and let $K_i$ be the fixed field of $G_i$.

We have that $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ are subfields so that $K_{i+1}/K_i$ is a cyclic extension for each $i < s$.

Let $n_i := [K_{i+1} : K_i]$. As before, let $F' \subseteq K$ be the field obtaining by adjoining all the $n_i$th roots of unity, for each $i$.

### Theorem

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Leftarrow$:** Assume the Galois group $G$ of $f(x)$ is solvable. Let $K/F$ be the splitting field of $f(x)$. Let $1 = G_s \subseteq G_{s-1} \ldots \subseteq G_0 = G$ witness solvability, and let $K_i$ be the fixed field of $G_i$.

We have that $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ are subfields so that $K_{i+1}/K_i$ is a cyclic extension for each $i < s$.

Let $n_i := [K_{i+1} : K_i]$. As before, let $F' \subseteq K$ be the field obtaining by adjoining all the $n_i$th roots of unity, for each $i$.

Consider the chain $F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \ldots \subseteq F'K_s = K$.

**Theorem**

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Leftarrow$:** Assume the Galois group $G$ of $f(x)$ is solvable. Let $K/F$ be the splitting field of $f(x)$. Let $1 = G_s \subseteq G_{s-1} \ldots \subseteq G_0 = G$ witness solvability, and let $K_i$ be the fixed field of $G_i$.

We have that $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ are subfields so that $K_{i+1}/K_i$ is a cyclic extension for each $i < s$.

Let $n_i := [K_{i+1} : K_i]$. As before, let $F' \subseteq K$ be the field obtaining by adjoining all the $n_i$th roots of unity, for each $i$.

Consider the chain $F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \ldots \subseteq F'K_s = K$.

By previous work, $\mathrm{Aut}(F'K_{i+1}/F'K_i) \cong \mathrm{Aut}(K_{i+1}/K_{i+1} \cap F')$ is a subgroup of $\mathrm{Aut}(K_{i+1}/K_i)$, hence cyclic. So $F'K_{i+1}/F'K_i$ is a cyclic extension.

### Theorem

The polynomial $f(x) \in F[x]$ can be solved by radicals if and only if the Galois group of $f(x)$ is solvable.

**Proof of $\Leftarrow$:** Assume the Galois group $G$ of $f(x)$ is solvable. Let $K/F$ be the splitting field of $f(x)$. Let $1 = G_s \subseteq G_{s-1} \ldots \subseteq G_0 = G$ witness solvability, and let $K_i$ be the fixed field of $G_i$.

We have that $F = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_s = K$ are subfields so that $K_{i+1}/K_i$ is a cyclic extension for each $i < s$.

Let $n_i := [K_{i+1} : K_i]$. As before, let $F' \subseteq K$ be the field obtaining by adjoining all the $n_i$th roots of unity, for each $i$.

Consider the chain $F \subseteq F' = F'K_0 \subseteq F'K_1 \subseteq \ldots \subseteq F'K_s = K$.

By previous work, $\mathrm{Aut}(F'K_{i+1}/F'K_i) \cong \mathrm{Aut}(K_{i+1}/K_{i+1} \cap F')$ is a subgroup of $\mathrm{Aut}(K_{i+1}/K_i)$, hence cyclic. So $F'K_{i+1}/F'K_i$ is a cyclic extension.

As $F'$ contains the relevant roots of unity, $F'K_{i+1}/F'K_i$ is a simple radical extension. As before $F'/F$ is a root extension. We're done.

# Example: $f(x) = x^5 - 6x + 3x \in \mathbb{Q}[x]$

We want to understand the roots of $f(x)$.

# Example: $f(x) = x^5 - 6x + 3x \in \mathbb{Q}[x]$

We want to understand the roots of $f(x)$.

- $f(x)$ is irreducible (Eisenstein).

# Example: $f(x) = x^5 - 6x + 3x \in \mathbb{Q}[x]$

We want to understand the roots of $f(x)$.

- $f(x)$ is irreducible (Eisenstein).
- Where do the roots of $f(x)$ lie? Plug in some values, see $f(-2) = -17, f(0) = 3, f(1) = -2, f(2) = 23$. So $f(x)$ has at least three real roots.

# Example: $f(x) = x^5 - 6x + 3x \in \mathbb{Q}[x]$

We want to understand the roots of $f(x)$.

- $f(x)$ is irreducible (Eisenstein).
- Where do the roots of $f(x)$ lie? Plug in some values, see $f(-2) = -17, f(0) = 3, f(1) = -2, f(2) = 23$. So $f(x)$ has at least three real roots.
- The derivative is $f'(x) = 5x^4 - 6$. It has only two real roots. If $f(x)$ had more real roots, $f'(x)$ would have more real roots (draw a picture).

# Example: $f(x) = x^5 - 6x + 3x \in \mathbb{Q}[x]$

We want to understand the roots of $f(x)$.

- $f(x)$ is irreducible (Eisenstein).
- Where do the roots of $f(x)$ lie? Plug in some values, see $f(-2) = -17, f(0) = 3, f(1) = -2, f(2) = 23$. So $f(x)$ has at least three real roots.
- The derivative is $f'(x) = 5x^4 - 6$. It has only two real roots. If $f(x)$ had more real roots, $f'(x)$ would have more real roots (draw a picture).
- Thus $f(x)$ has three real roots, two complex roots. The two complex roots must be conjugate (not preserved by complex conjugation).

# Example: $f(x) = x^5 - 6x + 3x$, continued

**So far we know:** $f(x)$ is irreducible with three real roots and two complex roots, interchanged by complex conjugation.

# Example: $f(x) = x^5 - 6x + 3x$, continued

**So far we know:** $f(x)$ is irreducible with three real roots and two complex roots, interchanged by complex conjugation.

- Let $K$ be the splitting field. Adjoining *one* root of $f(x)$ gives an extension of degree 5, so $K$ has degree divisible by 5.

# Example: $f(x) = x^5 - 6x + 3x$, continued

**So far we know:** $f(x)$ is irreducible with three real roots and two complex roots, interchanged by complex conjugation.

- Let $K$ be the splitting field. Adjoining *one* root of $f(x)$ gives an extension of degree 5, so $K$ has degree divisible by 5.
- Thus the Galois group $G$ is a subgroup of $S_5$, with order divisible by 5. In particular, it contains an element of order 5.

# Example: $f(x) = x^5 - 6x + 3x$, continued

**So far we know:** $f(x)$ is irreducible with three real roots and two complex roots, interchanged by complex conjugation.

- Let $K$ be the splitting field. Adjoining *one* root of $f(x)$ gives an extension of degree 5, so $K$ has degree divisible by 5.
- Thus the Galois group $G$ is a subgroup of $S_5$, with order divisible by 5. In particular, it contains an element of order 5.
- This element of order 5 must be a 5-cycle.

# Example: $f(x) = x^5 - 6x + 3x$, continued

**So far we know:** $f(x)$ is irreducible with three real roots and two complex roots, interchanged by complex conjugation.

- Let $K$ be the splitting field. Adjoining *one* root of $f(x)$ gives an extension of degree 5, so $K$ has degree divisible by 5.
- Thus the Galois group $G$ is a subgroup of $S_5$, with order divisible by 5. In particular, it contains an element of order 5.
- This element of order 5 must be a 5-cycle.
- $G$ also contains a transposition: restricting complex conjugation to $K$ gives an automorphism which permute the two complex roots and fixes the three real roots.

# Example: $f(x) = x^5 - 6x + 3x$, continued

**So far we know:** $f(x)$ is irreducible with three real roots and two complex roots, interchanged by complex conjugation.

- Let $K$ be the splitting field. Adjoining *one* root of $f(x)$ gives an extension of degree 5, so $K$ has degree divisible by 5.
- Thus the Galois group $G$ is a subgroup of $S_5$, with order divisible by 5. In particular, it contains an element of order 5.
- This element of order 5 must be a 5-cycle.
- $G$ also contains a transposition: restricting complex conjugation to $K$ gives an automorphism which permute the two complex roots and fixes the three real roots.
- Exercise: $S_5$ is generated by any transposition together with any 5-cycle.

# Example: $f(x) = x^5 - 6x + 3x$, continued

**So far we know:** $f(x)$ is irreducible with three real roots and two complex roots, interchanged by complex conjugation.

- Let $K$ be the splitting field. Adjoining *one* root of $f(x)$ gives an extension of degree 5, so $K$ has degree divisible by 5.
- Thus the Galois group $G$ is a subgroup of $S_5$, with order divisible by 5. In particular, it contains an element of order 5.
- This element of order 5 must be a 5-cycle.
- $G$ also contains a transposition: restricting complex conjugation to $K$ gives an automorphism which permute the two complex roots and fixes the three real roots.
- Exercise: $S_5$ is generated by any transposition together with any 5-cycle.
- Therefore the Galois group of $f(x)$ is $S_5$.

# Summary

(In characteristic zero)

- Any simple radical extension over a field containing enough roots of unity is cyclic.

# Summary

(In characteristic zero)

- Any simple radical extension over a field containing enough roots of unity is cyclic.
- Conversely, any cyclic extension over a field containing enough roots of unity is a simple radical extension.

# Summary

(In characteristic zero)

- Any simple radical extension over a field containing enough roots of unity is cyclic.
- Conversely, any cyclic extension over a field containing enough roots of unity is a simple radical extension.
- An element can be expressed by radicals if and only if it is is in an iteration of simple radical extensions (called a *root extension*).

# Summary

(In characteristic zero)

- Any simple radical extension over a field containing enough roots of unity is cyclic.
- Conversely, any cyclic extension over a field containing enough roots of unity is a simple radical extension.
- An element can be expressed by radicals if and only if it is is in an iteration of simple radical extensions (called a *root extension*).
- Using the Galois correspondence, a polynomial can be solved by radicals if and only if its Galois group is solvable.

# Summary

(In characteristic zero)

- Any simple radical extension over a field containing enough roots of unity is cyclic.
- Conversely, any cyclic extension over a field containing enough roots of unity is a simple radical extension.
- An element can be expressed by radicals if and only if it is is in an iteration of simple radical extensions (called a *root extension*).
- Using the Galois correspondence, a polynomial can be solved by radicals if and only if its Galois group is solvable.
- In particular, any polynomial with Galois group $S_n$, $n \geq 5$, cannot be solved by radicals.

# Summary

(In characteristic zero)

- Any simple radical extension over a field containing enough roots of unity is cyclic.
- Conversely, any cyclic extension over a field containing enough roots of unity is a simple radical extension.
- An element can be expressed by radicals if and only if it is is in an iteration of simple radical extensions (called a *root extension*).
- Using the Galois correspondence, a polynomial can be solved by radicals if and only if its Galois group is solvable.
- In particular, any polynomial with Galois group $S_n$, $n \geq 5$, cannot be solved by radicals.
- In particular, any polynomial of degree 4 or less can be solved by radicals, but $x^5 - 6x + 3$ cannot be solved by radicals.