Hyperelliptic Curves with Points over Cyclotomic Extensions

Quincy Alston

Department of Mathematics

December 13, 2022

Penn
University of Pennsylvania

Outline

Galois Theory

Our Problem

Methodology

Results

Galois Theory

Definition (Field Extension/Adjoinment)

A field K is a **field extension** of $\mathbb{Q}$ if $\mathbb{Q}$. A **field extension** K of $\mathbb{Q}$ is denoted $K/\mathbb{Q}$. If $\alpha \notin \mathbb{Q}$, the smallest field extension of $\mathbb{Q}$ containing α, denoted $\mathbb{Q}(\alpha)$, is a **field adjoinment**.

Penn
UNIVERSITY *of* PENNSYLVANIA

Galois Theory

Definition (Field Extension/Adjoinment)

A field K is a **field extension** of $\mathbb{Q}$ if $\mathbb{Q}$. A **field extension** K of $\mathbb{Q}$ is denoted $K/\mathbb{Q}$. If $\alpha \notin \mathbb{Q}$, the smallest field extension of $\mathbb{Q}$ containing α, denoted $\mathbb{Q}(\alpha)$, is a **field adjoinment**.

Example: *Define* $\mathbb{Q}(i) := \{a + ib \,|, a, b \in \mathbb{Q}\}$.

Galois Theory

Definition (Field Extension/Adjoinment)

A field K is a **field extension** of $\mathbb{Q}$ if $\mathbb{Q}$. A **field extension** K of $\mathbb{Q}$ is denoted $K/\mathbb{Q}$. If $\alpha \notin \mathbb{Q}$, the smallest field extension of $\mathbb{Q}$ containing α, denoted $\mathbb{Q}(\alpha)$, is a **field adjoinment**.

> ***Example:*** *Define* $\mathbb{Q}(i) := \{a + ib \,|, a, b \in \mathbb{Q}\}$.
> $\mathbb{Q}(i)$ *is a field extension of* $\mathbb{Q}$ *because* $\mathbb{Q} \subset \mathbb{Q}(i)$. *We construct* $\mathbb{Q}(i)$ *by adjoining i to* $\mathbb{Q}$.

Galois Theory

Definition (Field Extension/Adjoinment)

A field K is a **field extension** of $\mathbb{Q}$ if $\mathbb{Q}$. A **field extension** K of $\mathbb{Q}$ is denoted $K/\mathbb{Q}$. If $\alpha \notin \mathbb{Q}$, the smallest field extension of $\mathbb{Q}$ containing α, denoted $\mathbb{Q}(\alpha)$, is a **field adjoinment**.

> ***Example:*** *Define* $\mathbb{Q}(i) := \{a + ib \,|, a, b \in \mathbb{Q}\}$.
> $\mathbb{Q}(i)$ *is a field extension of* $\mathbb{Q}$ *because* $\mathbb{Q} \subset \mathbb{Q}(i)$. *We construct* $\mathbb{Q}(i)$ *by adjoining i to* $\mathbb{Q}$.

Definition (Splitting Field)

Let $h(x)$ be a polynomial with coefficients in the field F. A field K is the **splitting field** of $h(x)$ if $K/\mathbb{Q}$ is the smallest field extension over which $h(x)$ can be factored into linear factors.

Galois Theory

Definition (Field Extension/Adjoinment)

A field K is a **field extension** of $\mathbb{Q}$ if $\mathbb{Q}$. A **field extension** K of $\mathbb{Q}$ is denoted $K/\mathbb{Q}$. If $\alpha \notin \mathbb{Q}$, the smallest field extension of $\mathbb{Q}$ containing α, denoted $\mathbb{Q}(\alpha)$, is a **field adjoinment**.

> ***Example:*** *Define* $\mathbb{Q}(i) := \{a + ib \,|, a, b \in \mathbb{Q}\}$.
> $\mathbb{Q}(i)$ *is a field extension of* $\mathbb{Q}$ *because* $\mathbb{Q} \subset \mathbb{Q}(i)$. *We construct* $\mathbb{Q}(i)$ *by adjoining i to* $\mathbb{Q}$.

Definition (Splitting Field)

Let $h(x)$ be a polynomial with coefficients in the field F. A field K is the **splitting field** of $h(x)$ if $K/\mathbb{Q}$ is the smallest field extension over which $h(x)$ can be factored into linear factors.

> ***Example:*** $\mathbb{Q}(i)$ *is the splitting field of* $h(x) = x^2 - 1 = (x + i)(x - i)$.

Galois Theory

Definition (Galois Extension)

A field extension K/F is a **Galois Extension** if K is the splitting field of a set of polynomials over F that have distinct roots.

Galois Theory

Definition (Galois Extension)

A field extension K/F is a **Galois Extension** if K is the splitting field of a set of polynomials over F that have distinct roots.

Example: *Let* $K := \mathbb{Q}(i)$. *Define* $F := \mathbb{Q}$.

Galois Theory

Definition (Galois Extension)

A field extension K/F is a **Galois Extension** if K is the splitting field of a set of polynomials over F that have distinct roots.

Example: *Let* $K := \mathbb{Q}(i)$*. Define* $F := \mathbb{Q}$*.*
Then $\mathbb{Q}(i)/\mathbb{Q}$ *is a Galois Extension because* $\mathbb{Q}(i)$ *is the splitting field of the polynomials* $f(x) = x^2 + 1$ *and* f *has distinct roots* $i, -i$*.*

Galois Theory

Definition (Automorphism)

Let $K/\mathbb{Q}$ be a field extension of $\mathbb{Q}$. A homomorphism $f : K \to K$ is an **automorphism** over $\mathbb{Q}$ if f is an isomorphism and f fixes $\mathbb{Q}$.

Galois Theory

Definition (Automorphism)

Let $K/\mathbb{Q}$ be a field extension of $\mathbb{Q}$. A homomorphism $f : K \to K$ is an **automorphism** over $\mathbb{Q}$ if f is an isomorphism and f fixes $\mathbb{Q}$.

Definition (Galois Group)

Consider the Galois extension $K/\mathbb{Q}$. The **Galois Group** G of $K/\mathbb{Q}$, denoted $\text{Gal}(K/\mathbb{Q})$, is the group under function composition of K-automorphisms that fix $\mathbb{Q}$.

Galois Theory

Definition (Automorphism)

Let $K/\mathbb{Q}$ be a field extension of $\mathbb{Q}$. A homomorphism $f : K \to K$ is an **automorphism** over $\mathbb{Q}$ if f is an isomorphism and f fixes $\mathbb{Q}$.

Definition (Galois Group)

Consider the Galois extension $K/\mathbb{Q}$. The **Galois Group** G of $K/\mathbb{Q}$, denoted $\mathrm{Gal}(K/\mathbb{Q})$, is the group under function composition of K-automorphisms that fix $\mathbb{Q}$.

Proposition: Let $K = \mathbb{Q}(i)$. Then

Galois Theory

Definition (Automorphism)

Let $K/\mathbb{Q}$ be a field extension of $\mathbb{Q}$. A homomorphism $f : K \to K$ is an **automorphism** over $\mathbb{Q}$ if f is an isomorphism and f fixes $\mathbb{Q}$.

Definition (Galois Group)

Consider the Galois extension $K/\mathbb{Q}$. The **Galois Group** G of $K/\mathbb{Q}$, denoted $\mathrm{Gal}(K/\mathbb{Q})$, is the group under function composition of K-automorphisms that fix $\mathbb{Q}$.

Proposition: Let $K = \mathbb{Q}(i)$. Then

$$Gal(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}.$$

Galois Theory

Definition (Automorphism)

Let $K/\mathbb{Q}$ be a field extension of $\mathbb{Q}$. A homomorphism $f : K \to K$ is an **automorphism** over $\mathbb{Q}$ if f is an isomorphism and f fixes $\mathbb{Q}$.

Definition (Galois Group)

Consider the Galois extension $K/\mathbb{Q}$. The **Galois Group** G of $K/\mathbb{Q}$, denoted $\mathrm{Gal}(K/\mathbb{Q})$, is the group under function composition of K-automorphisms that fix $\mathbb{Q}$.

Proposition: Let $K = \mathbb{Q}(i)$. Then

$Gal(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof: There are two automorphisms that map $\mathbb{Q}(i) \to \mathbb{Q}(i)$ and fix $\mathbb{Q}$: $f(a + bi) = a + bi$ and $f(a + bi) = a - bi$.

Galois Theory

Definition (Automorphism)

Let $K/\mathbb{Q}$ be a field extension of $\mathbb{Q}$. A homomorphism $f : K \to K$ is an **automorphism** over $\mathbb{Q}$ if f is an isomorphism and f fixes $\mathbb{Q}$.

Definition (Galois Group)

Consider the Galois extension $K/\mathbb{Q}$. The **Galois Group** G of $K/\mathbb{Q}$, denoted $\mathrm{Gal}(K/\mathbb{Q})$, is the group under function composition of K-automorphisms that fix $\mathbb{Q}$.

Proposition: Let $K = \mathbb{Q}(i)$. Then

$Gal(\mathbb{Q}(i)/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$.

Proof: There are two automorphisms that map $\mathbb{Q}(i) \to \mathbb{Q}(i)$ and fix $\mathbb{Q}$: $f(a + bi) = a + bi$ and $f(a + bi) = a - bi$. The automorphisms of $\mathbb{Q}(i)$ form the group $\mathbb{Z}/2\mathbb{Z}$ because $g^2 = f = id$.

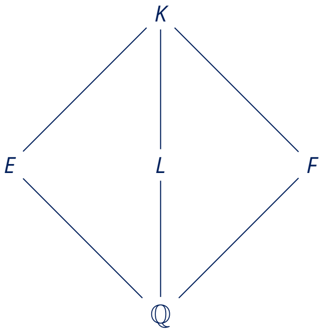
Penn
UNIVERSITY of PENNSYLVANIA

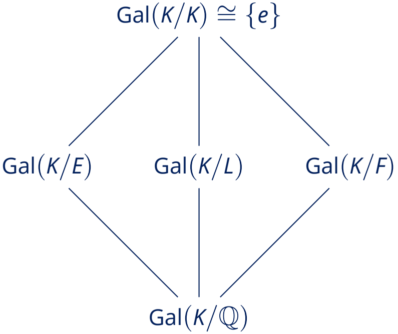
Galois Correspondence

There is a 1-1 correspondence between subfield extensions of a Galois extension and subgroups of the Galois group.

Galois Correspondence

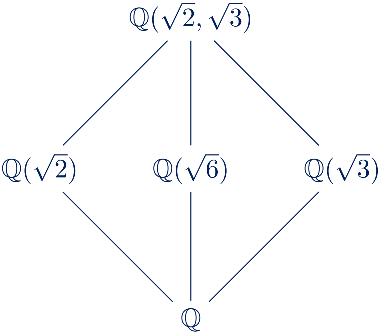
There is a 1-1 correspondence between subfield extensions of a Galois extension and subgroups of the Galois group.

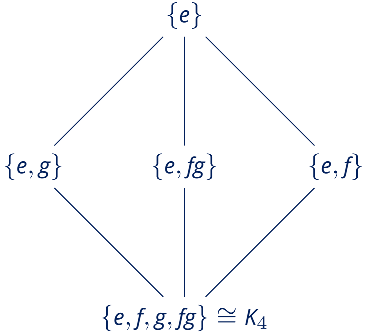




Galois Correspondence

- $e = id$
- $f : \sqrt{2} \to -\sqrt{2}$
- $g : \sqrt{3} \to -\sqrt{3}$





Algebraic Curves

Definition (Plane Curve)

A **plane curve** is the set of points $(\alpha, \beta) \in \mathbb{C}^2$ such that $F(\alpha, \beta) = 0$ for some polynomial $F(x, y)$ with coefficients in $\mathbb{Q}$.

Algebraic Curves

Definition (Plane Curve)

A **plane curve** is the set of points $(\alpha, \beta) \in \mathbb{C}^2$ such that $F(\alpha, \beta) = 0$ for some polynomial $F(x, y)$ with coefficients in $\mathbb{Q}$.

Example (Hyperelliptic Curves)

A plane curve E is **hyperelliptic** if it is of the form $y^2 = f(x)$ where $f(x) \in \mathbb{Q}[x]$. E is **elliptic** if $\deg(f(x)) = 3$.

Algebraic Curves

Definition (Plane Curve)

A **plane curve** is the set of points $(\alpha, \beta) \in \mathbb{C}^2$ such that $F(\alpha, \beta) = 0$ for some polynomial $F(x, y)$ with coefficients in $\mathbb{Q}$.

Example (Hyperelliptic Curves)

A plane curve E is **hyperelliptic** if it is of the form $y^2 = f(x)$ where $f(x) \in \mathbb{Q}[x]$. E is **elliptic** if $\deg(f(x)) = 3$.

Example: *The curve* $E : y^2 = x^3 - x + 1$ *is an elliptic curve.*

Bringing it all Together

Definition (Field Adjoining a Point on a Curve)

Let $P = (\alpha, \beta), \alpha, \beta \in \overline{\mathbb{Q}}$ be a point on $E : F(x, y) = 0$ over $\mathbb{Q}$.

Bringing it all Together

Definition (Field Adjoining a Point on a Curve)

Let $P = (\alpha, \beta), \alpha, \beta \in \overline{\mathbb{Q}}$ be a point on $E : F(x, y) = 0$ over $\mathbb{Q}$. By adjoining each coordinate of P to $\mathbb{Q}$, we **adjoin the point P to $\mathbb{Q}$** to get $\mathbb{Q}(P) := \mathbb{Q}(\alpha, \beta)$.

Bringing it all Together

Definition (Field Adjoining a Point on a Curve)

Let $P = (\alpha, \beta), \alpha, \beta \in \overline{\mathbb{Q}}$ be a point on $E : F(x, y) = 0$ over $\mathbb{Q}$. By adjoining each coordinate of P to $\mathbb{Q}$, we **adjoin the point** P **to** $\mathbb{Q}$ to get $\mathbb{Q}(P) := \mathbb{Q}(\alpha, \beta)$.

Example: *Let* $E : y^2 = x^3 - x + 1$ *and* $P = (2, \sqrt{7})$.

Bringing it all Together

Definition (Field Adjoining a Point on a Curve)

Let $P = (\alpha, \beta), \alpha, \beta \in \overline{\mathbb{Q}}$ be a point on $E : F(x, y) = 0$ over $\mathbb{Q}$. By adjoining each coordinate of P to $\mathbb{Q}$, we **adjoin the point** P **to** $\mathbb{Q}$ to get $\mathbb{Q}(P) := \mathbb{Q}(\alpha, \beta)$.

Example: *Let* $E : y^2 = x^3 - x + 1$ *and* $P = (2, \sqrt{7})$*. Since* P *is a point on* E*, we define* $\mathbb{Q}(P) = \mathbb{Q}(2, \sqrt{7}) = \mathbb{Q}(\sqrt{7})$.

Bringing it all Together

Definition (Field Adjoining a Point on a Curve)

Let $P = (\alpha, \beta), \alpha, \beta \in \overline{\mathbb{Q}}$ be a point on $E : F(x, y) = 0$ over $\mathbb{Q}$. By adjoining each coordinate of P to $\mathbb{Q}$, we **adjoin the point** P **to** $\mathbb{Q}$ to get $\mathbb{Q}(P) := \mathbb{Q}(\alpha, \beta)$.

Example: *Let $E : y^2 = x^3 - x + 1$ and $P = (2, \sqrt{7})$. Since P is a point on E, we define $\mathbb{Q}(P) = \mathbb{Q}(2, \sqrt{7}) = \mathbb{Q}(\sqrt{7})$.*

Definition (Parameterization)

Consider a plane curve $E : F(x, y) = 0$. Let $x(t), y(t)$ be polynomials with coefficients in $\mathbb{Q}$. Then the polynomial $F(x(t), y(t)) = 0$ is a **parameterization** of $F(x, y)$. The roots of $F(x(t), y(t))$ give us points on E.

Penn
UNIVERSITY *of* PENNSYLVANIA

Bringing it all Together

Definition (Field Adjoining a Point on a Curve)

Let $P = (\alpha, \beta), \alpha, \beta \in \overline{\mathbb{Q}}$ be a point on $E : F(x, y) = 0$ over $\mathbb{Q}$. By adjoining each coordinate of P to $\mathbb{Q}$, we **adjoin the point** P **to** $\mathbb{Q}$ to get $\mathbb{Q}(P) := \mathbb{Q}(\alpha, \beta)$.

Example: *Let* $E : y^2 = x^3 - x + 1$ *and* $P = (2, \sqrt{7})$*. Since P is a point on E, we define* $\mathbb{Q}(P) = \mathbb{Q}(2, \sqrt{7}) = \mathbb{Q}(\sqrt{7})$.

Definition (Parameterization)

Consider a plane curve $E : F(x, y) = 0$. Let $x(t), y(t)$ be polynomials with coefficients in $\mathbb{Q}$. Then the polynomial $F(x(t), y(t)) = 0$ is a **parameterization** of $F(x, y)$. The roots of $F(x(t), y(t))$ give us points on E.

Example: *Consider* $F(x, y) = x^2 + y^2 - 1 = 0$*. Let* $x(t) = 2t$ *and* $y(t) = t - 1$*. Then* $F(x(t), y(t)) = 5t^2 - 2t = 0$ *is a parameterization of* $F(x, y)$.

Inverse Galois Problem

Which finite groups can be realized as Galois groups over $\mathbb{Q}$?

- This is an open number theory problem known as the Inverse Galois Problem

Inverse Galois Problem

Which finite groups can be realized as Galois groups over $\mathbb{Q}$?

- This is an open number theory problem known as the Inverse Galois Problem

Inverse Galois Problem for Plane Curves

Let C be a plane curve over $\mathbb{Q}$. If we consider $\mathbb{Q}(P)$ such that P is a point on C, which groups can arise as $G = \text{Gal}(\mathbb{Q}(P)/\mathbb{Q})$?

Inverse Galois Problem

Which finite groups can be realized as Galois groups over $\mathbb{Q}$?

- This is an open number theory problem known as the Inverse Galois Problem

Inverse Galois Problem for Plane Curves

Let C be a plane curve over $\mathbb{Q}$. If we consider $\mathbb{Q}(P)$ such that P is a point on C, which groups can arise as $G = \text{Gal}(\mathbb{Q}(P)/\mathbb{Q})$?

Our Question

Fix a plane curve $C : F(x, y) = 0$. What parameterizations $x(t), y(t) \in \mathbb{Q}[t]$ give us polynomials with Galois group $G \ncong S_n$?

Inverse Galois Problem

Which finite groups can be realized as Galois groups over $\mathbb{Q}$?

- This is an open number theory problem known as the Inverse Galois Problem

Inverse Galois Problem for Plane Curves

Let C be a plane curve over $\mathbb{Q}$. If we consider $\mathbb{Q}(P)$ such that P is a point on C, which groups can arise as $G = \text{Gal}(\mathbb{Q}(P)/\mathbb{Q})$?

Our Question

Fix a plane curve $C : F(x, y) = 0$. What parameterizations $x(t), y(t) \in \mathbb{Q}[t]$ give us polynomials with Galois group $G \ncong S_n$?

- Particularly, we are searching for curves and parameterizations that give us cyclotomic polynomials, whose Galois groups are always abelian (i.e. not S_n).

Penn
University *of* Pennsylvania

Inverse Galois Problem

Which finite groups can be realized as Galois groups over $\mathbb{Q}$?

- This is an open number theory problem known as the Inverse Galois Problem

Inverse Galois Problem for Plane Curves

Let C be a plane curve over $\mathbb{Q}$. If we consider $\mathbb{Q}(P)$ such that P is a point on C, which groups can arise as $G = \text{Gal}(\mathbb{Q}(P)/\mathbb{Q})$?

Our Question

Fix a plane curve $C : F(x, y) = 0$. What parameterizations $x(t), y(t) \in \mathbb{Q}[t]$ give us polynomials with Galois group $G \not\cong S_n$?

- Particularly, we are searching for curves and parameterizations that give us cyclotomic polynomials, whose Galois groups are always abelian (i.e. not S_n).
- Can we get a Galois group of the form $(\mathbb{Z}/n\mathbb{Z})^\times$ from an elliptic curve?

Penn
University *of* Pennsylvania

Our Method

Claim [Keyes]

The parameterization $x(t) = t$, $y(t) = \frac{g(t)}{h(t)}$ on the hyperelliptic curve $F : y^2 = f(x)$ gives the following:

Penn
University of Pennsylvania

Our Method

Claim [Keyes]

The parameterization $x(t) = t$, $y(t) = \frac{g(t)}{h(t)}$ on the hyperelliptic curve $F : y^2 = f(x)$ gives the following:

$$\frac{g(t)^2}{h(t)^2} - f(t) = 0$$

$$\Theta(t) = g(t)^2 - h(t)^2 f(t) = 0$$

Our Method

Claim [Keyes]

The parameterization $x(t) = t$, $y(t) = \frac{g(t)}{h(t)}$ on the hyperelliptic curve $F : y^2 = f(x)$ gives the following:

$$\frac{g(t)^2}{h(t)^2} - f(t) = 0$$

$$\Theta(t) = g(t)^2 - h(t)^2 f(t) = 0$$

For each root α such that $\Theta(\alpha) = 0$, we adjoin $\mathbb{Q}(\alpha, \frac{g(\alpha)}{h(\alpha)})$ to get a Galois extension.

The field $\mathbb{Q}(\alpha, \frac{g(\alpha)}{h(\alpha)})$ is equal to $\mathbb{Q}(\alpha)$. [1]

Cyclotomic Polynomials

Definition (Cyclotomic Polynomial)

The nth **cyclotomic polynomial** denoted $\Phi_n(x)$ is the monic polynomial of minimal degree with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Example: *The 4th cyclotomic polynomial is* $\Phi_4(x) = x^2 + 1$

- Alternatively: $\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a)$
- Let p be prime. Then $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}})$.
- The degree of $\Phi_n(x)$ is given by the Euler-Totient function

Penn
UNIVERSITY *of* PENNSYLVANIA

Cyclotomic Polynomials

Definition (Cyclotomic Polynomial)

The nth **cyclotomic polynomial** denoted $\Phi_n(x)$ is the monic polynomial of minimal degree with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Example: *The 4th cyclotomic polynomial is* $\Phi_4(x) = x^2 + 1$

- Alternatively: $\Phi_n(x) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^a)$
- Let p be prime. Then $\Phi_{p^n}(x) = \Phi_p(x^{p^{n-1}})$.
- The degree of $\Phi_n(x)$ is given by the Euler-Totient function

Remark

Set $\Theta(t) := \Phi_n(t)$, the nth cyclotomic polynomial. If $\Theta(\alpha) = 0$ for some $\alpha \in \bar{\mathbb{Q}}$, then $\mathbb{Q}(x(\alpha), y(\alpha))/\mathbb{Q}$ gives a cyclotomic field extension of $\mathbb{Q}$.

Results

We computed examples using SageMath and generated a conjecture on how Cyclotomics factor. This conjecture implies results about our factoring method. We proved the following:

- **Theorem:** Let $n = p^m$ where $p \equiv 1 \mod 4$. Then $R(x) = x^{\frac{d}{2}} - \Phi_n(x)$ is reducible with a square factor.
- **Theorem:** Let $n = 3^m \cdot 2^\ell$. Then $R(x) = x^{\frac{d}{2}} - \Phi_n(x)$ is a perfect square.
- Recall our parametrization: $\Theta(t) = g(t)^2 - h(t)^2 f(t) = 0$. Then $\Phi_n(x) = \Theta(x)$, $g(x)^2 = x^{\frac{d}{2}}$, and $h(x)^2 f(x) = R(x)$.
- Thus $y^2 = f(x)$ is a hyperelliptic curve with a point over the *nth* cyclotomic field.

References

C. D. Keyes, *Growth of points on hyperelliptic curves over number fields*, (2019).