Fields of Definition of G-Galois Branched Covers of the Projective Line

Hilaf Hasson

Jan 10, 2013

The Inverse Galois Problem

The Inverse Galois Problem

- Let K be a field.

The Inverse Galois Problem

- Let K be a field.
- IGP over K: Is every finite group a Galois group over K?

The Inverse Galois Problem

- Let K be a field.
- IGP over K: Is every finite group a Galois group over K?
- The IGP is conjectured to have a positive answer over all number fields.

Strategy

- How do you realize G over a number field K?

Strategy

- How do you realize G over a number field K?
- Realize G over $K(x)$.

Strategy

- How do you realize G over a number field K?
- Realize G over $K(x)$. Then specialize to some $\alpha \in K$.

Strategy

- How do you realize G over a number field K?
- Realize G over $K(x)$. Then specialize to some $\alpha \in K$.
- For example, for $G = \mathbb{Z}/2\mathbb{Z}$: adjoin y such that $y^2 = x$ to $\mathbb{Q}(x)$.

Strategy

- How do you realize G over a number field K?
- Realize G over $K(x)$. Then specialize to some $\alpha \in K$.
- For example, for $G = \mathbb{Z}/2\mathbb{Z}$: adjoin y such that $y^2 = x$ to $\mathbb{Q}(x)$. If you specialize $\mathbb{Q}(y)/\mathbb{Q}(x)$ to $x = 2$ you get $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

Strategy

- Can always specialize:
  Hilbert's Irreducibility Theorem: If $f(x, y) \in K[x, y]$ is irreducible, then for infinitely many $\alpha \in K$, $f(\alpha, y) \in K[y]$ is irreducible.

Translation to Algebraic Geometry

Translation to Algebraic Geometry

- Think of $K(x)$ as the function field of $\mathbb{P}^1_K$, and of its overfield as the function field of some curve.

Translation to Algebraic Geometry

- Think of $K(x)$ as the function field of $\mathbb{P}^1_K$, and of its overfield as the function field of some curve.
- Let G be a finite group, and K a field. A G-Galois branched cover of K-curves is a finite, connected map of smooth, projective K-curves whose extension of function fields is Galois with group G.

Translation to Algebraic Geometry

- Think of $K(x)$ as the function field of $\mathbb{P}^1_K$, and of its overfield as the function field of some curve.
- Let G be a finite group, and K a field. A G-Galois branched cover of K-curves is a finite, connected map of smooth, projective K-curves whose extension of function fields is Galois with group G.
- For example: $\mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ defined by $y^2 = x$ is a $\mathbb{Z}/2\mathbb{Z}$-Galois cover. (Induced extension of function fields: $\mathbb{Q}(y)/\mathbb{Q}(x)$.)

Translation to Algebraic Geometry

- Think of $K(x)$ as the function field of $\mathbb{P}^1_K$, and of its overfield as the function field of some curve.
- Let G be a finite group, and K a field. A G-Galois branched cover of K-curves is a finite, connected map of smooth, projective K-curves whose extension of function fields is Galois with group G.
- For example: $\mathbb{P}^1_{\mathbb{Q}} \to \mathbb{P}^1_{\mathbb{Q}}$ defined by $y^2 = x$ is a $\mathbb{Z}/2\mathbb{Z}$-Galois cover. (Induced extension of function fields: $\mathbb{Q}(y)/\mathbb{Q}(x)$.)
- The Regular Inverse Galois Problem over a field K: Does every finite group G satisfy that there exists a G-Galois branched cover of K-curves over $\mathbb{P}^1_K$?

Riemann's Existence Theorem

- Is there hope? Yes!

Riemann's Existence Theorem

- Is there hope? Yes!
- For every group G there is a G-Galois branched cover of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$. (Riemann's Existence Theorem)

Riemann's Existence Theorem

- Is there hope? Yes!
- For every group G there is a G-Galois branched cover of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$. (Riemann's Existence Theorem)
- RET: Every topological covering space of $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{a_1, ..., a_r\}$ with deck transformation group G is algebraic.

Riemann's Existence Theorem

- Is there hope? Yes!
- For every group G there is a G-Galois branched cover of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$. (Riemann's Existence Theorem)
- RET: Every topological covering space of $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{a_1, ..., a_r\}$ with deck transformation group G is algebraic. Furthermore, if $a_1, ..., a_r$ are $\bar{\mathbb{Q}}$-rational, then this cover descends to $\bar{\mathbb{Q}}$.

Riemann's Existence Theorem

- Is there hope? Yes!
- For every group G there is a G-Galois branched cover of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$. (Riemann's Existence Theorem)
- RET: Every topological covering space of $\mathbb{P}^1_{\mathbb{C}} \setminus \{a_1, ..., a_r\}$ with deck transformation group G is algebraic. Furthermore, if $a_1, ..., a_r$ are $\bar{\mathbb{Q}}$-rational, then this cover descends to $\bar{\mathbb{Q}}$.
- Classically, if G is generated by $r - 1$ elements, there's a covering space of $\mathbb{P}^1_{\mathbb{C}} \setminus \{a_1, ..., a_r\}$ with deck transformation group G.

Riemann's Existence Theorem

- Is there hope? Yes!
- For every group G there is a G-Galois branched cover of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$. (Riemann's Existence Theorem)
- RET: Every topological covering space of $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{a_1, \ldots, a_r\}$ with deck transformation group G is algebraic. Furthermore, if $a_1, \ldots, a_r$ are $\bar{\mathbb{Q}}$-rational, then this cover descends to $\bar{\mathbb{Q}}$.
- Classically, if G is generated by $r-1$ elements, there's a covering space of $\mathbb{P}^1_{\mathbb{C}} \smallsetminus \{a_1, \ldots, a_r\}$ with deck transformation group G.
- Since RET is not constructive, we don't know what number fields these covers descend to.

Fields of Definition

Fields of Definition

- K is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a *mere cover* if the map descends to K: $X_K \to \mathbb{P}^1_K$.

Fields of Definition

- K is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a *mere cover* if the map descends to K: $X_K \to \mathbb{P}^1_K$.
- K is a field of definition as a *G-Galois branched cover* if furthermore $X_K \to \mathbb{P}^1_K$ can be chosen to be G-Galois.

Fields of Definition

- K is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a *mere cover* if the map descends to K: $X_K \to \mathbb{P}^1_K$.
- K is a field of definition as a *G-Galois branched cover* if furthermore $X_K \to \mathbb{P}^1_K$ can be chosen to be G-Galois.
- For example for $\mathbb{P}^1_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ defined by $y^3 = x$: $\mathbb{Q}$ is a f.o.d. as a mere cover, but not as a $\mathbb{Z}/3\mathbb{Z}$-cover.

- Most attempts to understand the descent of these covers have focused on the "field of moduli".

- Most attempts to understand the descent of these covers have focused on the "field of moduli".
- Definition: The field of moduli of a G-Galois branched of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ is the subfield of $\bar{\mathbb{Q}}$ fixed by all those $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that take this cover to an isomorphic cover.

- Most attempts to understand the descent of these covers have focused on the "field of moduli".
- Definition: The field of moduli of a G-Galois branched of $\mathbb{P}^1_{\bar{\mathbb{Q}}}$ is the subfield of $\bar{\mathbb{Q}}$ fixed by all those $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ that take this cover to an isomorphic cover.
- The field of moduli of a G-Galois branched cover is the intersection of all fields of definition as a G-Galois branched cover. (Coombes and Harbater '85)

Previous Work

Previous Work

- Rigidity - Method of constructing covers with field of moduli $\mathbb{Q}$. (Matzat, Thompson, Belyi, Fried, Shih; Works only in certain cases.)

Previous Work

- Rigidity - Method of constructing covers with field of moduli $\mathbb{Q}$. (Matzat, Thompson, Belyi, Fried, Shih; Works only in certain cases.)
- Exploring the ramification of the field of moduli over $\mathbb{Q}$. (Beckmann, Obus, Wewers, Raynaud, Flon, H.)

Previous Work

- Rigidity - Method of constructing covers with field of moduli $\mathbb{Q}$. (Matzat, Thompson, Belyi, Fried, Shih; Works only in certain cases.)
- Exploring the ramification of the field of moduli over $\mathbb{Q}$. (Beckmann, Obus, Wewers, Raynaud, Flon, H.)
- When is the field of moduli a field of definition? (Belyi, Dèbes, Wewers)

The Structure of the Fields of Definition

- Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M.

The Structure of the Fields of Definition

- Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M.
- Harbater and Coombes have proven that M is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover.

The Structure of the Fields of Definition

- Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M.
- Harbater and Coombes have proven that M is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover.
- Theorem (H.): Let L be a field of definition as a mere cover, and let $X_L \to \mathbb{P}^1_L$ be an L-model as a mere cover.

The Structure of the Fields of Definition

- Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M.
- Harbater and Coombes have proven that M is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover.
- Theorem (H.): Let L be a field of definition as a mere cover, and let $X_L \to \mathbb{P}^1_L$ be an L-model as a mere cover. Then there exists a unique minimal field E containing L such that $E \times_L X_L \to \mathbb{P}^1_E$ is Galois.

The Structure of the Fields of Definition

- Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M.
- Harbater and Coombes have proven that M is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover.
- Theorem (H.): Let L be a field of definition as a mere cover, and let $X_L \to \mathbb{P}^1_L$ be an L-model as a mere cover. Then there exists a unique minimal field E containing L such that $E \times_L X_L \to \mathbb{P}^1_E$ is Galois.
- Furthermore, E/L is Galois with group a subgroup of $\mathrm{Aut}(G)$.

The Structure of the Fields of Definition

- Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M.
- Harbater and Coombes have proven that M is a field of definition of $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ as a mere cover.
- Theorem (H.): Let L be a field of definition as a mere cover, and let $X_L \to \mathbb{P}^1_L$ be an L-model as a mere cover. Then there exists a unique minimal field E containing L such that $E \times_L X_L \to \mathbb{P}^1_E$ is Galois.
- Furthermore, E/L is Galois with group a subgroup of $\mathrm{Aut}(G)$.
- In particular there is always a field of definition (as a G-Galois branched cover) that is Galois over the field of moduli with Galois group a subgroup of $\mathrm{Aut}(G)$.

Why is the field of moduli not a field of definition?

- Two reasons:

Why is the field of moduli not a field of definition?

- Two reasons:
  1. Every model $X_M \to \mathbb{P}^1_M$ yields a different field of definition.

Why is the field of moduli not a field of definition?

- Two reasons:
  1. Every model $X_M \to \mathbb{P}^1_M$ yields a different field of definition.
  2. It is not true that for every overfield L of M and mere cover model $X_L \to \mathbb{P}^1_L$, the model descends to M.

A Special Field of Definition

A Special Field of Definition

- Coombes and Harbater ('85): Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M. Then $M(\zeta_n)_n$ is a field of definition as a G-Galois branched cover.

A Special Field of Definition

- Coombes and Harbater ('85): Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M. Then $M(\zeta_n)_n$ is a field of definition as a G-Galois branched cover.
- H.: In fact $\cup_{\{n|\exists m: n \,\text{divides}\, |Z(G)|^m\}} M(\zeta_n)$ is a field of definition as a G-Galois branched cover.

A Special Field of Definition

- Coombes and Harbater ('85): Let $X_{\bar{\mathbb{Q}}} \to \mathbb{P}^1_{\bar{\mathbb{Q}}}$ be a G-Galois branched cover with field of moduli M. Then $M(\zeta_n)_n$ is a field of definition as a G-Galois branched cover.
- H.: In fact $\cup_{\{n \mid \exists m : n \text{ divides } |Z(G)|^m\}} M(\zeta_n)$ is a field of definition as a G-Galois branched cover.
- In particular there is a field of definition (as a G-Galois branched cover) that, as an extension of the field of moduli, ramifies only over primes that divide $|Z(G)|$.

Earlier Result

- H. (earlier result): For every G there is a G-Galois branched cover with field of moduli M, s.t. $M/\mathbb{Q}$ ramifies at most over the primes that divide $|G|$.

A Result Towards the IGP

- Corollary: For every G there is a G-Galois branched cover with a *field of definition* (as a G-Galois branched cover) L, s.t. $L/\mathbb{Q}$ ramified at most over the primes that divide $|G|$.

A Result Towards the IGP

- Corollary: For every G there is a G-Galois branched cover with a *field of definition* (as a G-Galois branched cover) L, s.t. $L/\mathbb{Q}$ ramified at most over the primes that divide $|G|$.
- Corollary: For every G there is a G-Galois field extension E/L, where $L/\mathbb{Q}$ is ramified at most over primes that divide $|G|$. (i.e., L is "almost" $\mathbb{Q}$.)