Hopf-Galois Structures and Hunting Through the Holomorph

Andrew Darlington

Thursday 1st June 2023

University of Exeter

Review of Galois Theory

L field containing $\mathbb{Q}$.

Review of Galois Theory

L field containing $\mathbb{Q}$. If L is the *splitting field* of some $p(x) \in \mathbb{Q}(x)$, we say $L/\mathbb{Q}$ is **Galois**. Otherwise it is non-normal.

Review of Galois Theory

L field containing $\mathbb{Q}$. If L is the *splitting field* of some $p(x) \in \mathbb{Q}(x)$, we say $L/\mathbb{Q}$ is **Galois**. Otherwise it is non-normal.

If $L/\mathbb{Q}$ is Galois, it has a group

$$\mathrm{Gal}(L/\mathbb{Q}) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \ \forall x \in \mathbb{Q}\}$$

and $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$.

Review of Galois Theory

L field containing $\mathbb{Q}$. If L is the *splitting field* of some $p(x) \in \mathbb{Q}(x)$, we say $L/\mathbb{Q}$ is **Galois**. Otherwise it is non-normal.

If $L/\mathbb{Q}$ is Galois, it has a group

$$\mathrm{Gal}(L/\mathbb{Q}) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma(x) = x \ \forall x \in \mathbb{Q}\}$$

and $|\mathrm{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}]$.

Theorem (Fundamental Theorem of Galois Theory)
If $L/\mathbb{Q}$ is Galois, then there is a bijective correspondence between

Fields $\mathbb{Q} < F < L$, and

Subgroups $H < \mathrm{Gal}(L/\mathbb{Q})$

given by $F = L^H$.

Replacing with a Hopf algebra

$L/\mathbb{Q}$ Galois, $G := \mathrm{Gal}(L/\mathbb{Q})$.

Replacing with a Hopf algebra

$L/\mathbb{Q}$ Galois, $G := \mathrm{Gal}(L/\mathbb{Q})$. Then

- L is a $\mathbb{Q}[G]$-module algebra

Replacing with a Hopf algebra

$L/\mathbb{Q}$ Galois, $G := \mathrm{Gal}(L/\mathbb{Q})$. Then

- L is a $\mathbb{Q}[G]$-module algebra
- The linear map induced by this action given by

$$\begin{aligned}\theta : L \otimes \mathbb{Q}[G] &\to \mathrm{End}_{\mathbb{Q}}(L) \\ x \otimes h &\mapsto \theta(x \otimes h)(y) = x(h \cdot y)\end{aligned}$$

  is an isomorphism.

Replacing with a Hopf algebra

$L/\mathbb{Q}$ Galois, $G := \mathrm{Gal}(L/\mathbb{Q})$. Then

- L is a $\mathbb{Q}[G]$-module algebra
- The linear map induced by this action given by

$$\begin{aligned} \theta : L \otimes \mathbb{Q}[G] &\to \mathrm{End}_{\mathbb{Q}}(L) \\ x \otimes h &\mapsto \theta(x \otimes h)(y) = x(h \cdot y) \end{aligned}$$

  is an isomorphism.
- $\mathbb{Q}[G]$ has the structure of a *Hopf algebra*.

Replacing with a Hopf algebra

$L/\mathbb{Q}$ Galois, $G := \mathrm{Gal}(L/\mathbb{Q})$. Then

- L is a $\mathbb{Q}[G]$-module algebra
- The linear map induced by this action given by

$$\begin{aligned} \theta : L \otimes \mathbb{Q}[G] &\to \mathrm{End}_{\mathbb{Q}}(L) \\ x \otimes h &\mapsto \theta(x \otimes h)(y) = x(h \cdot y) \end{aligned}$$

  is an isomorphism.
- $\mathbb{Q}[G]$ has the structure of a *Hopf algebra*.

This gives an example of a **Hopf-Galois Structure**

Some facts

Fact 1: $\mathbb{Q}[G]$ may not be the only Hopf algebra to act on L in such a way (unlike there being a unique Galois group)

Some facts

Fact 1: $\mathbb{Q}[G]$ may not be the only Hopf algebra to act on L in such a way (unlike there being a unique Galois group)

Fact 2: This also makes sense for non-normal extensions (it can actually be defined for certain rings as well)

Some facts

Fact 1: $\mathbb{Q}[G]$ may not be the only Hopf algebra to act on L in such a way (unlike there being a unique Galois group)

Fact 2: This also makes sense for non-normal extensions (it can actually be defined for certain rings as well)

Fact 3: There is an analogous "Hopf-Galois Correspondence". It is always injective, but not always surjective.

Some facts

Fact 1: $\mathbb{Q}[G]$ may not be the only Hopf algebra to act on L in such a way (unlike there being a unique Galois group)

Fact 2: This also makes sense for non-normal extensions (it can actually be defined for certain rings as well)

Fact 3: There is an analogous "Hopf-Galois Correspondence". It is always injective, but not always surjective.

My work focuses on studying, describing and counting Hopf-Galois structures for different field extensions.

Back to group theory

Define the *holomorph*, $\mathrm{Hol}(N)$ of a group N to be the semidirect product of N and $\mathrm{Aut}(N)$:

$$Hol(N) \cong N \rtimes \mathrm{Aut}(N).$$

Where

$$(\eta, \alpha)(\mu, \beta) = (\eta\alpha(\mu), \alpha\beta).$$

Note: $\mathrm{Hol}(N)$ has a natural action on N given by:

$$(\eta, \alpha) \cdot \mu = \eta\alpha(\mu)$$

Back to group theory

Define the *holomorph*, $\mathrm{Hol}(N)$ of a group N to be the semidirect product of N and $\mathrm{Aut}(N)$:

$$Hol(N) \cong N \rtimes \mathrm{Aut}(N).$$

Where

$$(\eta, \alpha)(\mu, \beta) = (\eta\alpha(\mu), \alpha\beta).$$

Note: $\mathrm{Hol}(N)$ has a natural action on N given by:

$$(\eta, \alpha) \cdot \mu = \eta\alpha(\mu)$$

$L/\mathbb{Q}$ (not necessarily Galois) extension, E Galois closure, and $G := \mathrm{Gal}(E/\mathbb{Q})$.

Back to group theory

Define the *holomorph*, $\mathrm{Hol}(N)$ of a group N to be the semidirect product of N and $\mathrm{Aut}(N)$:

$$Hol(N) \cong N \rtimes \mathrm{Aut}(N).$$

Where

$$(\eta, \alpha)(\mu, \beta) = (\eta\alpha(\mu), \alpha\beta).$$

Note: $\mathrm{Hol}(N)$ has a natural action on N given by:

$$(\eta, \alpha) \cdot \mu = \eta\alpha(\mu)$$

$L/\mathbb{Q}$ (not necessarily Galois) extension, E Galois closure, and $G := \mathrm{Gal}(E/\mathbb{Q})$. In 1996, Byott [Byo96] (building on [GP87]) showed that HGS on $L/\mathbb{Q}$ correspond with **transitive** subgroups of $\mathrm{Hol}(N)$ (where N cycles through the groups of order $[L : \mathbb{Q}]$) isomorphic to G.

Back to group theory

Define the *holomorph*, $\mathrm{Hol}(N)$ of a group N to be the semidirect product of N and $\mathrm{Aut}(N)$:

$$Hol(N) \cong N \rtimes \mathrm{Aut}(N).$$

Where

$$(\eta, \alpha)(\mu, \beta) = (\eta\alpha(\mu), \alpha\beta).$$

Note: $\mathrm{Hol}(N)$ has a natural action on N given by:

$$(\eta, \alpha) \cdot \mu = \eta\alpha(\mu)$$

$L/\mathbb{Q}$ (not necessarily Galois) extension, E Galois closure, and $G := \mathrm{Gal}(E/\mathbb{Q})$. In 1996, Byott [Byo96] (building on [GP87]) showed that HGS on $L/\mathbb{Q}$ correspond with **transitive** subgroups of $\mathrm{Hol}(N)$ (where N cycles through the groups of order $[L : \mathbb{Q}]$) isomorphic to G.

$$H = E[N]^G$$

Examples

- $\mathbb{Q}[G]$ is a HGS on $L/\mathbb{Q}$ of type G.

Examples

- $\mathbb{Q}[G]$ is a HGS on $L/\mathbb{Q}$ of type G.
- N is a transitive subgroup of $\mathrm{Hol}(N)$.

Examples

- $\mathbb{Q}[G]$ is a HGS on $L/\mathbb{Q}$ of type G.
- N is a transitive subgroup of $\mathrm{Hol}(N)$.
- $\mathrm{Hol}(N)$ is a transitive subgroup of $\mathrm{Hol}(N)$

Examples

- $\mathbb{Q}[G]$ is a HGS on $L/\mathbb{Q}$ of type G.
- N is a transitive subgroup of $\mathrm{Hol}(N)$.
- $\mathrm{Hol}(N)$ is a transitive subgroup of $\mathrm{Hol}(N)$
- If $G < \mathrm{Hol}(N)$ is transitive then $G < \mathrm{Hol}(N^{\mathrm{op}})$ is transitive.

Examples

- $\mathbb{Q}[G]$ is a HGS on $L/\mathbb{Q}$ of type G.
- N is a transitive subgroup of $\mathrm{Hol}(N)$.
- $\mathrm{Hol}(N)$ is a transitive subgroup of $\mathrm{Hol}(N)$
- If $G < \mathrm{Hol}(N)$ is transitive then $G < \mathrm{Hol}(N^{\mathrm{op}})$ is transitive.
- $L/\mathbb{Q}$ degree p^2, $2p$ [CS20], mp with $(m, p) = 1$ [Koh07] & [Koh16], squarefree Galois [AB20],...

$L/\mathbb{Q}$ degree pq

Idea: for each N of order pq, obtain a 'nice' presentation for $\mathrm{Hol}(N)$ to help find transitive subgroups.

$L/\mathbb{Q}$ degree pq

Idea: for each N of order pq, obtain a 'nice' presentation for $\mathrm{Hol}(N)$ to help find transitive subgroups.

There are two abstract groups of order pq for $q \mid (p-1)$: C_{pq} and $C_p \rtimes C_q$.

$L/\mathbb{Q}$ degree pq

Idea: for each N of order pq, obtain a 'nice' presentation for $\mathrm{Hol}(N)$ to help find transitive subgroups.

There are two abstract groups of order pq for $q \mid (p-1)$: C_{pq} and $C_p \rtimes C_q$. In each group, let σ, τ be the generators of orders p, q respectively.

$L/\mathbb{Q}$ degree pq

Idea: for each N of order pq, obtain a 'nice' presentation for $\mathrm{Hol}(N)$ to help find transitive subgroups.

There are two abstract groups of order pq for $q \mid (p-1)$: C_{pq} and $C_p \rtimes C_q$. In each group, let σ, τ be the generators of orders p, q respectively.

$$\mathrm{Hol}(C_{pq}) \cong C_{pq} \rtimes (C_{p-1} \times C_{q-1})$$
$$\mathrm{Hol}(C_p \rtimes C_q) \cong (C_p \rtimes C_q) \rtimes (C_p \rtimes C_{p-1})$$

$L/\mathbb{Q}$ degree pq

Idea: for each N of order pq, obtain a 'nice' presentation for $\mathrm{Hol}(N)$ to help find transitive subgroups.

There are two abstract groups of order pq for $q \mid (p-1)$: C_{pq} and $C_p \rtimes C_q$. In each group, let σ, τ be the generators of orders p, q respectively.

$$\mathrm{Hol}(C_{pq}) \cong C_{pq} \rtimes (C_{p-1} \times C_{q-1})$$
$$\mathrm{Hol}(C_p \rtimes C_q) \cong (C_p \rtimes C_q) \rtimes (C_p \rtimes C_{p-1})$$

In each case, we find the smallest subgroups of $\mathrm{Hol}(N)$ which are transitive on N and then build up.

For $N \cong C_{pq}$, these 'minimally transitive' subgroups are

$$N, \\ \langle \sigma, [\tau, \alpha^u] \rangle$$

for α generating the unique Sylow q-subgroup of $\mathrm{Aut}(N)$ and $u \neq 0$.

For $N \cong C_{pq}$, these 'minimally transitive' subgroups are

$$N,$$
$$\langle \sigma, [\tau, \alpha^u] \rangle$$

for α generating the unique Sylow q-subgroup of $\mathrm{Aut}(N)$ and $u \neq 0$.

To get ALL transitive subgroups of $\mathrm{Hol}(C_{pq})$ we may extend these groups by any subgroups of their normalisers in $\mathrm{Aut}(N)$ (that is $\mathrm{Aut}(N)$ and $\mathrm{Aut}(\langle \sigma \rangle)$ respectively).

For $N \cong C_{pq}$, these 'minimally transitive' subgroups are

$$N,$$
$$\langle \sigma, [\tau, \alpha^u] \rangle$$

for α generating the unique Sylow q-subgroup of $\mathrm{Aut}(N)$ and $u \neq 0$.

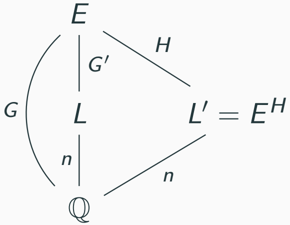
To get ALL transitive subgroups of $\mathrm{Hol}(C_{pq})$ we may extend these groups by any subgroups of their normalisers in $\mathrm{Aut}(N)$ (that is $\mathrm{Aut}(N)$ and $\mathrm{Aut}(\langle \sigma \rangle)$ respectively).

For $N \cong C_p \rtimes C_q$, it is possible to write $\mathrm{Hol}(N)$ as $P \rtimes R$ for P, R abelian groups of orders $p^2, q(p-1)$ respectively.

Questions

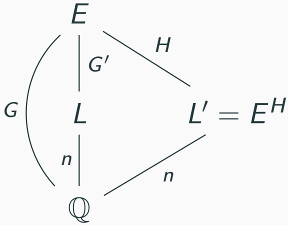
- How much can we extend the methods to all squarefree extensions?

Questions

- How much can we extend the methods to all squarefree extensions?
- 

  What can we say about $L'/\mathbb{Q}$?

Questions

- How much can we extend the methods to all squarefree extensions?
- 

  What can we say about $L'/\mathbb{Q}$?
- How much can we push these results to other related constructions?

Thank You!

- Ali A. Alabdali and Nigel P. Byott, *Hopf-Galois structures of squarefree degree*, J. Algebra **559** (2020), 58–86. MR 4093704
- N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228. MR 1402555
- Teresa Crespo and Marta Salguero, *Computation of Hopf Galois structures on low degree separable extensions and classification of those for degrees p^2 and $2p$*, Publ. Mat. **64** (2020), no. 1, 121–141. MR 4047559
- Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476
- Timothy Kohl, *Groups of order $4p$, twisted wreath products and Hopf-Galois theory*, J. Algebra **314** (2007), no. 1, 42–74. MR 2331752
- ———, *Hopf-Galois structures arising from groups with*