An introduction to Hopf-Galois theory

Daniel Gil Muñoz

Charles University in Prague
Department of Algebra

Debrecen, February 2023

Table of contents

Table of contents

Let L/K be a finite and separable extension of fields.

Let L/K be a finite and separable extension of fields.

L/K is Galois if and only if

$$\sigma\colon L \longrightarrow \overline{K} \quad K\text{-embedding} \quad \Longrightarrow \quad \sigma \in \mathrm{Aut}_K(L).$$

Let L/K be a finite and separable extension of fields.

L/K is Galois if and only if

$$\sigma\colon L \longrightarrow \overline{K} \quad K\text{-embedding} \quad \Longrightarrow \quad \sigma \in \mathrm{Aut}_K(L).$$

If so, $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ is the Galois group of L/K.

Let L/K be a finite and separable extension of fields.

L/K is Galois if and only if

$$\sigma \colon L \longrightarrow \overline{K} \quad K\text{-embedding} \quad \Longrightarrow \quad \sigma \in \mathrm{Aut}_K(L).$$

If so, $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ is the Galois group of L/K.

Let $G \leq \mathrm{Aut}_K(L)$. The K-group algebra of G is

$$K[G] = \Big\{ \sum_{\sigma \in G} a_\sigma \sigma \mid a_\sigma \in K \Big\}.$$

Let L/K be a finite and separable extension of fields.

L/K is Galois if and only if

$$\sigma\colon L \longrightarrow \overline{K} \quad K\text{-embedding} \quad \Longrightarrow \quad \sigma \in \mathrm{Aut}_K(L).$$

If so, $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ is the Galois group of L/K.

Let $G \leq \mathrm{Aut}_K(L)$. The K-group algebra of G is

$$K[G] = \Big\{ \sum_{\sigma\in G} a_\sigma \sigma \mid a_\sigma \in K \Big\}.$$

It acts on $x \in L$ by

$$\Big(\sum_{\sigma\in G} a_\sigma \sigma \Big) \cdot x = \sum_{\sigma\in G} a_\sigma \sigma(x).$$

Let L/K be a finite and separable extension of fields.

L/K is Galois if and only if

$$\sigma\colon L \longrightarrow \overline{K} \quad K\text{-embedding} \quad \Longrightarrow \quad \sigma \in \mathrm{Aut}_K(L).$$

If so, $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L)$ is the Galois group of L/K.

Let $G \leq \mathrm{Aut}_K(L)$. The K-group algebra of G is

$$K[G] = \Big\{ \sum_{\sigma \in G} a_\sigma \sigma \mid a_\sigma \in K \Big\}.$$

It acts on $x \in L$ by

$$\Big(\sum_{\sigma \in G} a_\sigma \sigma \Big) \cdot x = \sum_{\sigma \in G} a_\sigma \sigma(x).$$

This defines a K-linear map $K[G] \otimes_K L \longrightarrow L$.

$$\Big(\sum_{\sigma\in G} a_\sigma \sigma\Big)\cdot x = \sum_{\sigma\in G} a_\sigma \sigma(x).$$

This defines a K-linear map $K[G]\otimes_K L \longrightarrow L$.

$$\Big(\sum_{\sigma\in G} a_\sigma \sigma\Big)\cdot x = \sum_{\sigma\in G} a_\sigma \sigma(x).$$

This defines a K-linear map $K[G]\otimes_K L \longrightarrow L$.

At the same time, there is an embedding $K[G]\hookrightarrow \mathrm{End}_K(L)$.

$$\Big(\sum_{\sigma\in G} a_\sigma \sigma\Big)\cdot x = \sum_{\sigma\in G} a_\sigma \sigma(x).$$

This defines a K-linear map $K[G]\otimes_K L \longrightarrow L$.

At the same time, there is an embedding $K[G] \hookrightarrow \mathrm{End}_K(L)$.

If we adjoin scalars of L, this yields a canonical map $j\colon L\otimes_K K[G] \longrightarrow \mathrm{End}_K(L)$.

$$\Big(\sum_{\sigma\in G} a_\sigma \sigma\Big)\cdot x = \sum_{\sigma\in G} a_\sigma \sigma(x).$$

This defines a K-linear map $K[G]\otimes_K L \longrightarrow L$.

At the same time, there is an embedding $K[G]\hookrightarrow \mathrm{End}_K(L)$.

If we adjoin scalars of L, this yields a canonical map $j\colon L\otimes_K K[G]\longrightarrow \mathrm{End}_K(L)$.

Theorem

Let L/K be a finite and separable extension and let $G\leq \mathrm{Aut}_K(L)$. Then L/K is Galois with group G if and only if j is a K-linear isomorphism.

$$\left(\sum_{\sigma\in G} a_\sigma \sigma\right)\cdot x = \sum_{\sigma\in G} a_\sigma \sigma(x).$$

This defines a K-linear map $K[G]\otimes_K L \longrightarrow L$.

At the same time, there is an embedding $K[G]\hookrightarrow \mathrm{End}_K(L)$.

If we adjoin scalars of L, this yields a canonical map $j\colon L\otimes_K K[G]\longrightarrow \mathrm{End}_K(L)$.

Theorem

Let L/K be a finite and separable extension and let $G\leq \mathrm{Aut}_K(L)$. Then L/K is Galois with group G if and only if j is a K-linear isomorphism.

Now, $K[G]$ is a K-Hopf algebra (a K-vector space with some additional structure).

Let L/K be a finite extension of fields.

Let L/K be a finite extension of fields.

A **Hopf-Galois structure** on L/K is a finite cocommutative K-Hopf algebra H together with a K-linear map $\cdot\colon H \otimes L \longrightarrow L$ in such a way that:

Let L/K be a finite extension of fields.

A **Hopf-Galois structure** on L/K is a finite cocommutative K-Hopf algebra H together with a K-linear map $\cdot\colon H \otimes L \longrightarrow L$ in such a way that:

(i) The action of H on L is compatible with the Hopf algebra operations of H.

Let L/K be a finite extension of fields.

A **Hopf-Galois structure** on L/K is a finite cocommutative K-Hopf algebra H together with a K-linear map $\cdot\colon H \otimes L \longrightarrow L$ in such a way that:

(i) The action of H on L is compatible with the Hopf algebra operations of H.

(ii) The canonical map $j\colon L \otimes_K H \longrightarrow \mathrm{End}_K(L)$ induced by the assignation

$$\begin{array}{ccc} H & \longrightarrow & \mathrm{End}_K(L) \\ h & \longmapsto & x \mapsto h \cdot x \end{array}$$

is a K-linear isomorphism.

Let L/K be a finite extension of fields.

A **Hopf-Galois structure** on L/K is a finite cocommutative K-Hopf algebra H together with a K-linear map $\cdot\colon H \otimes L \longrightarrow L$ in such a way that:

(i) The action of H on L is compatible with the Hopf algebra operations of H.

(ii) The canonical map $j\colon L \otimes_K H \longrightarrow \mathrm{End}_K(L)$ induced by the assignation

$$\begin{array}{rcl} H & \longrightarrow & \mathrm{End}_K(L) \\ h & \longmapsto & x \mapsto h \cdot x \end{array}$$

is a K-linear isomorphism.

The extension L/K is said to be **Hopf-Galois** if it admits some Hopf-Galois structure.

Let L/K be a finite extension of fields.

A **Hopf-Galois structure** on L/K is a finite cocommutative K-Hopf algebra H together with a K-linear map $\cdot\colon H \otimes L \longrightarrow L$ in such a way that:

(i) The action of H on L is compatible with the Hopf algebra operations of H.

(ii) The canonical map $j\colon L \otimes_K H \longrightarrow \mathrm{End}_K(L)$ induced by the assignation

$$\begin{array}{rcl} H & \longrightarrow & \mathrm{End}_K(L) \\ h & \longmapsto & x \mapsto h \cdot x \end{array}$$

is a K-linear isomorphism.

The extension L/K is said to be **Hopf-Galois** if it admits some Hopf-Galois structure.

We also say that L/K is H-Galois.

- If L/K is Galois, then it is Hopf-Galois. Indeed, $K[G]$ together with the Galois action is a Hopf-Galois structure on L/K, called the **classical Galois structure**.

- If L/K is Galois, then it is Hopf-Galois. Indeed, $K[G]$ together with the Galois action is a Hopf-Galois structure on L/K, called the **classical Galois structure**.
- There are many Hopf-Galois extensions that are not Galois, such as $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Also, there are extensions that are not Hopf-Galois.

- If L/K is Galois, then it is Hopf-Galois. Indeed, $K[G]$ together with the Galois action is a Hopf-Galois structure on L/K, called the **classical Galois structure**.
- There are many Hopf-Galois extensions that are not Galois, such as $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Also, there are extensions that are not Hopf-Galois.
- A Hopf-Galois extension might have several Hopf-Galois structures. It is possible that the same Hopf algebra endowed with different actions give rise to different Hopf-Galois structures.

- If L/K is Galois, then it is Hopf-Galois. Indeed, $K[G]$ together with the Galois action is a Hopf-Galois structure on L/K, called the **classical Galois structure.**
- There are many Hopf-Galois extensions that are not Galois, such as $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Also, there are extensions that are not Hopf-Galois.
- A Hopf-Galois extension might have several Hopf-Galois structures. It is possible that the same Hopf algebra endowed with different actions give rise to different Hopf-Galois structures.
- 'Fundamental' theorem of Hopf-Galois theory: If L/K is H-Galois, there is an injective map from the Hopf subalgebras of H to the intermediate fields of L/K.

Table of contents

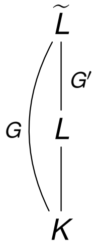
Most of the research in Hopf-Galois theory takes place in the world of (finite) separable extensions.

Most of the research in Hopf-Galois theory takes place in the world of (finite) separable extensions.

In this setting, there is a characterization of the Hopf-Galois structures on the extension.

Most of the research in Hopf-Galois theory takes place in the world of (finite) separable extensions.

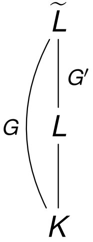
In this setting, there is a characterization of the Hopf-Galois structures on the extension.



L/K separable extension with normal closure $\widetilde{L}$.

Most of the research in Hopf-Galois theory takes place in the world of (finite) separable extensions.

In this setting, there is a characterization of the Hopf-Galois structures on the extension.

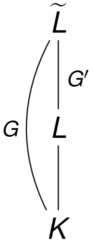


L/K separable extension with normal closure $\widetilde{L}$.

$G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$, $X = G/G'$.

Most of the research in Hopf-Galois theory takes place in the world of (finite) separable extensions.

In this setting, there is a characterization of the Hopf-Galois structures on the extension.



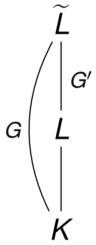
L/K separable extension with normal closure $\widetilde{L}$.

$G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$, $X = G/G'$.

There is an embedding $G \hookrightarrow \mathrm{Perm}(X)$ by left multiplication on cosets.

Most of the research in Hopf-Galois theory takes place in the world of (finite) separable extensions.

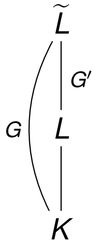
In this setting, there is a characterization of the Hopf-Galois structures on the extension.



L/K separable extension with normal closure $\widetilde{L}$.

$G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$, $X = G/G'$.

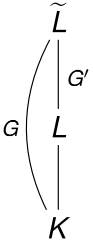
There is an embedding $G \hookrightarrow \mathrm{Perm}(X)$ by left multiplication on cosets.
In particular, G acts on $\mathrm{Perm}(X)$ by conjugation.



L/K separable extension with normal closure $\widetilde{L}$.

$G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$, $X = G/G'$.

There is an embedding $G \hookrightarrow \mathrm{Perm}(X)$ by left multiplication on cosets.
In particular, G acts on $\mathrm{Perm}(X)$ by conjugation.



L/K separable extension with normal closure $\widetilde{L}$.

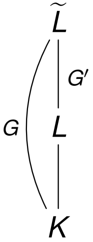
$G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$, $X = G/G'$.

There is an embedding $G \hookrightarrow \mathrm{Perm}(X)$ by left multiplication on cosets.
In particular, G acts on $\mathrm{Perm}(X)$ by conjugation.

Theorem (Greither-Pareigis theorem, 1986)

There is a bijective correspondence between the following:

- *Hopf-Galois structures on L/K.*
- *Regular G-stable subgroups of $\mathrm{Perm}(X)$.*



L/K separable extension with normal closure $\widetilde{L}$.

$G = \mathrm{Gal}(\widetilde{L}/K)$, $G' = \mathrm{Gal}(\widetilde{L}/L)$, $X = G/G'$.

There is an embedding $G \hookrightarrow \mathrm{Perm}(X)$ by left multiplication on cosets.
In particular, G acts on $\mathrm{Perm}(X)$ by conjugation.

Theorem (Greither-Pareigis theorem, 1986)

There is a bijective correspondence between the following:

- *Hopf-Galois structures on L/K.*
- *Regular G-stable subgroups of $\mathrm{Perm}(X)$.*

A subgroup $N \leq \mathrm{Perm}(X)$ is regular if

$$\forall x, y \in X \, \exists! \eta \in N : \; \eta(x) = y.$$

Some applications of Greither-Pareigis theorem (and its refinements):

Some applications of Greither-Pareigis theorem (and its refinements):

- Ennumeration of Hopf-Galois structures on an extension of fields within a class. For instance: Extensions of degree p, p^2, pq, $2p$, $4p$, square-free degree. . .

Some applications of Greither-Pareigis theorem (and its refinements):

- Ennumeration of Hopf-Galois structures on an extension of fields within a class. For instance: Extensions of degree p, p^2, pq, $2p$, $4p$, square-free degree...
- Isomorphisms problems for Hopf-Galois structures. If H is the Hopf algebra in a Hopf-Galois structure, is it isomorphic to some familiar object?

Some applications of Greither-Pareigis theorem (and its refinements):

- Ennumeration of Hopf-Galois structures on an extension of fields within a class. For instance: Extensions of degree p, p^2, pq, $2p$, $4p$, square-free degree...
- Isomorphisms problems for Hopf-Galois structures. If H is the Hopf algebra in a Hopf-Galois structure, is it isomorphic to some familiar object?
- Some general results.

Some applications of Greither-Pareigis theorem (and its refinements):

- Ennumeration of Hopf-Galois structures on an extension of fields within a class. For instance: Extensions of degree p, p^2, pq, $2p$, $4p$, square-free degree...
- Isomorphisms problems for Hopf-Galois structures. If H is the Hopf algebra in a Hopf-Galois structure, is it isomorphic to some familiar object?
- Some general results. For instance:

Some applications of Greither-Pareigis theorem (and its refinements):

- Ennumeration of Hopf-Galois structures on an extension of fields within a class. For instance: Extensions of degree p, p^2, pq, $2p$, $4p$, square-free degree...
- Isomorphisms problems for Hopf-Galois structures. If H is the Hopf algebra in a Hopf-Galois structure, is it isomorphic to some familiar object?
- Some general results. For instance:
    - A prime degree extension L/K is Hopf-Galois if and only if G is solvable.

Some applications of Greither-Pareigis theorem (and its refinements):

- Ennumeration of Hopf-Galois structures on an extension of fields within a class. For instance: Extensions of degree p, p^2, pq, $2p$, $4p$, square-free degree...
- Isomorphisms problems for Hopf-Galois structures. If H is the Hopf algebra in a Hopf-Galois structure, is it isomorphic to some familiar object?
- Some general results. For instance:
  - A prime degree extension L/K is Hopf-Galois if and only if G is solvable.
  - A separable extension with Burnside degree admits at most one Hopf-Galois structure.

Greither-Pareigis theory is also the vehicle to connect Hopf-Galois theory with skew braces.

Greither-Pareigis theory is also the vehicle to connect Hopf-Galois theory with skew braces.

Definition

A skew (left) brace is a tern $(B, \cdot, \circ)$ *where* B *is a non-empty set and* $\cdot, \circ$ *are binary operations on* B *such that:*

1. $(B, \cdot)$ *and* $(B, \circ)$ *are groups.*
2. *For each* $a, b, c \in B$, $a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c)$.

Greither-Pareigis theory is also the vehicle to connect Hopf-Galois theory with skew braces.

Definition

A skew (left) brace is a tern $(B, \cdot, \circ)$ *where* B *is a non-empty set and* $\cdot$, $\circ$ *are binary operations on* B *such that:*

1. $(B, \cdot)$ *and* $(B, \circ)$ *are groups.*
2. *For each* $a, b, c \in B$, $a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c)$.

The interest in the theory of skew braces relies in its applicability to the Yang-Baxter equation.

Greither-Pareigis theory is also the vehicle to connect Hopf-Galois theory with skew braces.

Definition

A skew (left) brace is a tern $(B, \cdot, \circ)$ where B is a non-empty set and $\cdot$, $\circ$ are binary operations on B such that:

1. *$(B, \cdot)$ and $(B, \circ)$ are groups.*
2. *For each $a, b, c \in B$, $a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c)$.*

The interest in the theory of skew braces relies in its applicability to the Yang-Baxter equation.

Bachiller (2016), Guarnieri-Vendramin (2017): There is a (non-bijective) correspondence between skew braces of size n and Hopf-Galois structures on a degree n Galois extension.

Greither-Pareigis theory is also the vehicle to connect Hopf-Galois theory with skew braces.

Definition

A skew (left) brace is a tern $(B, \cdot, \circ)$ *where* B *is a non-empty set and* $\cdot$, $\circ$ *are binary operations on* B *such that:*

1. $(B, \cdot)$ *and* $(B, \circ)$ *are groups.*
2. *For each* $a, b, c \in B$, $a \circ (b \cdot c) = (a \circ b) \cdot a^{-1} \cdot (a \circ c)$.

The interest in the theory of skew braces relies in its applicability to the Yang-Baxter equation.

Bachiller (2016), Guarnieri-Vendramin (2017): There is a (non-bijective) correspondence between skew braces of size n and Hopf-Galois structures on a degree n Galois extension.

This link led to new questions and answers in both areas and currently constitutes a very active research field.

There are Hopf-Galois extensions that are not Galois but are very similar to those.

There are Hopf-Galois extensions that are not Galois but are very similar to those.

Definition

Let L/K be a separable extension. We say that L/K is ***almost classically Galois*** *if it satisfies any of these equivalent conditions:*

There are Hopf-Galois extensions that are not Galois but are very similar to those.

Definition

Let L/K be a separable extension. We say that L/K is ***almost classically Galois*** *if it satisfies any of these equivalent conditions:*

- *G' has some normal complement J within G.*

There are Hopf-Galois extensions that are not Galois but are very similar to those.

Definition

Let L/K be a separable extension. We say that L/K is ***almost classically Galois*** *if it satisfies any of these equivalent conditions:*

- *G' has some normal complement J within G.*
- *There is some intermediate field $K \leq M \leq \widetilde{L}$ such that $\widetilde{L} \cong L \otimes_K M$ as K-algebras.*

There are Hopf-Galois extensions that are not Galois but are very similar to those.

Definition

Let L/K be a separable extension. We say that L/K is ***almost classically Galois*** *if it satisfies any of these equivalent conditions:*

- *G' has some normal complement J within G.*
- *There is some intermediate field $K \leq M \leq \widetilde{L}$ such that $\widetilde{L} \cong L \otimes_K M$ as K-algebras.*

In that case, L/K is Hopf-Galois and $J = \mathrm{Gal}(\widetilde{L}/M)$.

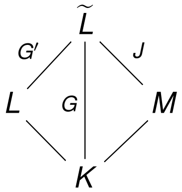
There are Hopf-Galois extensions that are not Galois but are very similar to those.

Definition

Let L/K be a separable extension. We say that L/K is ***almost classically Galois*** *if it satisfies any of these equivalent conditions:*

- *G' has some normal complement J within G.*
- *There is some intermediate field $K \leq M \leq \widetilde{L}$ such that $\widetilde{L} \cong L \otimes_K M$ as K-algebras.*

In that case, L/K is Hopf-Galois and $J = \mathrm{Gal}(\widetilde{L}/M)$.



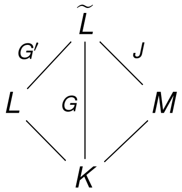
There are Hopf-Galois extensions that are not Galois but are very similar to those.

Definition

*Let L/K be a separable extension. We say that L/K is **almost classically Galois** if it satisfies any of these equivalent conditions:*

- *G' has some normal complement J within G.*
- *There is some intermediate field $K \leq M \leq \widetilde{L}$ such that $\widetilde{L} \cong L \otimes_K M$ as K-algebras.*

In that case, L/K is Hopf-Galois and $J = \mathrm{Gal}(\widetilde{L}/M)$.



$\widetilde{L}/M$ is a Galois extension with Galois group J and with the same degree as L/K.

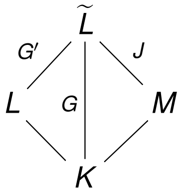
There are Hopf-Galois extensions that are not Galois but are very similar to those.

Definition

Let L/K be a separable extension. We say that L/K is ***almost classically Galois*** *if it satisfies any of these equivalent conditions:*

- *G' has some normal complement J within G.*
- *There is some intermediate field $K \leq M \leq \widetilde{L}$ such that $\widetilde{L} \cong L \otimes_K M$ as K-algebras.*

In that case, L/K is Hopf-Galois and $J = \mathrm{Gal}(\widetilde{L}/M)$.



$\widetilde{L}/M$ is a Galois extension with Galois group J and with the same degree as L/K.

Usual strategy: Translate properties from $\widetilde{L}/M$ to L/K.

Table of contents

Hopf-Galois theory can be used to broaden the domain of Galois module theory.

Hopf-Galois theory can be used to broaden the domain of Galois module theory.

Theorem (Normal basis theorem)

Let L/K be a finite Galois extension with group G. There is some $\alpha \in L$ such that

$$\{\sigma(\alpha)\}_{\sigma \in G}$$

is a K-basis of L. Equivalently, L is a free $K[G]$-module.

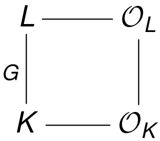
Hopf-Galois theory can be used to broaden the domain of Galois module theory.

Theorem (Normal basis theorem)

Let L/K be a finite Galois extension with group G. There is some $\alpha \in L$ such that

$$\{\sigma(\alpha)\}_{\sigma \in G}$$

is a K-basis of L. Equivalently, L is a free $K[G]$-module.



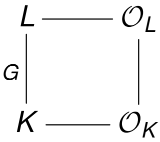
Hopf-Galois theory can be used to broaden the domain of Galois module theory.

Theorem (Normal basis theorem)

Let L/K be a finite Galois extension with group G. There is some $\alpha \in L$ such that

$$\{\sigma(\alpha)\}_{\sigma \in G}$$

is a K-basis of L. Equivalently, L is a free $K[G]$-module.



If L/K is a Galois extension of number or p-adic fields, a normal basis might be integral. In that case, $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-free.

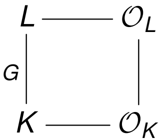
Hopf-Galois theory can be used to broaden the domain of Galois module theory.

Theorem (Normal basis theorem)

Let L/K be a finite Galois extension with group G. There is some $\alpha \in L$ such that

$$\{\sigma(\alpha)\}_{\sigma \in G}$$

is a K-basis of L. Equivalently, L is a free $K[G]$-module.



If L/K is a Galois extension of number or p-adic fields, a normal basis might be integral. In that case, $\mathcal{O}_L$ is $\mathcal{O}_K[G]$-free.

The issue is that $\mathcal{O}_L$ is not $\mathcal{O}_K[G]$-free for a bunch of extensions L/K.

Definition (Leopoldt, 1959)

Let L/K be a Galois extension of number or p-adic fields with group G. The associated order of $\mathcal{O}_L$ in $K[G]$ is defined as

$$\mathfrak{A}_{L/K} = \{\lambda \in K[G] \mid \lambda \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

Definition (Leopoldt, 1959)

Let L/K be a Galois extension of number or p-adic fields with group G. The associated order of $\mathcal{O}_L$ in $K[G]$ is defined as

$$\mathfrak{A}_{L/K} = \{\lambda \in K[G] \mid \lambda \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

Even if $\mathcal{O}_L$ is not $\mathcal{O}_K[G]$-free, it might still happen that $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.

Definition (Leopoldt, 1959)

Let L/K be a Galois extension of number or p-adic fields with group G. The associated order of $\mathcal{O}_L$ in $K[G]$ is defined as

$$\mathfrak{A}_{L/K} = \{\lambda \in K[G] \mid \lambda \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

Even if $\mathcal{O}_L$ is not $\mathcal{O}_K[G]$-free, it might still happen that $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.

Unfortunately, $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free in general.

Definition (Leopoldt, 1959)

Let L/K be a Galois extension of number or p-adic fields with group G. The associated order of $\mathcal{O}_L$ in $K[G]$ is defined as

$$\mathfrak{A}_{L/K} = \{\lambda \in K[G] \mid \lambda \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

Even if $\mathcal{O}_L$ is not $\mathcal{O}_K[G]$-free, it might still happen that $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-free.

Unfortunately, $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free in general.

Problem

Find a necessary and sufficient condition for the $\mathfrak{A}_{L/K}$-freeness of $\mathcal{O}_L$.

There is a natural generalization of this picture to Hopf-Galois theory.

There is a natural generalization of this picture to Hopf-Galois theory.

Definition

Let L/K be an H-Galois extension of number or p-adic fields. The associated order of $\mathcal{O}_L$ in H is defined as

$$\mathfrak{A}_H = \{h \in H \mid h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

There is a natural generalization of this picture to Hopf-Galois theory.

Definition

Let L/K be an H-Galois extension of number or p-adic fields. The associated order of $\mathcal{O}_L$ in H is defined as

$$\mathfrak{A}_H = \{h \in H \mid h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

Problem

Find a necessary and sufficient condition for the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$.

There is a natural generalization of this picture to Hopf-Galois theory.

Definition

Let L/K be an H-Galois extension of number or p-adic fields. The associated order of $\mathcal{O}_L$ in H is defined as

$$\mathfrak{A}_H = \{h \in H \mid h \cdot x \in \mathcal{O}_L \text{ for all } x \in \mathcal{O}_L\}.$$

Problem

Find a necessary and sufficient condition for the $\mathfrak{A}_H$-freeness of $\mathcal{O}_L$.

Byott (1997): There is a Galois extension L/K of p-adic fields such that $\mathcal{O}_L$ is not $\mathfrak{A}_{L/K}$-free but $\mathcal{O}_L$ is $\mathfrak{A}_H$-free in some other Hopf-Galois structure H on L/K.

There are still few results on Hopf-Galois module theory for extensions of number fields.

There are still few results on Hopf-Galois module theory for extensions of number fields.

G., Rio (2022): Quartic Galois number fields.

There are still few results on Hopf-Galois module theory for extensions of number fields.

G., Rio (2022): Quartic Galois number fields.

Let L be a quartic number field such that $L/\mathbb{Q}$ is Galois.

There are still few results on Hopf-Galois module theory for extensions of number fields.

G., Rio (2022): Quartic Galois number fields.

Let L be a quartic number field such that $L/\mathbb{Q}$ is Galois.

It was already known that $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free (in fact, for every abelian extension of $\mathbb{Q}$).

There are still few results on Hopf-Galois module theory for extensions of number fields.

G., Rio (2022): Quartic Galois number fields.

Let L be a quartic number field such that $L/\mathbb{Q}$ is Galois.

It was already known that $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free (in fact, for every abelian extension of $\mathbb{Q}$).

If $L/\mathbb{Q}$ is cyclic, there is a non-classical Hopf-Galois structure.

There are still few results on Hopf-Galois module theory for extensions of number fields.

G., Rio (2022): Quartic Galois number fields.

Let L be a quartic number field such that $L/\mathbb{Q}$ is Galois.

It was already known that $\mathcal{O}_L$ is $\mathfrak{A}_{L/\mathbb{Q}}$-free (in fact, for every abelian extension of $\mathbb{Q}$).

If $L/\mathbb{Q}$ is cyclic, there is a non-classical Hopf-Galois structure.

Proposition

$L = \mathbb{Q}(\sqrt{a(d+b\sqrt{d})})$, where:

- *$a \in \mathbb{Z}$ is odd square-free and $b \in \mathbb{Z}_{>0}$.*
- *$d = b^2 + c^2$ for some $c \in \mathbb{Z}_{>0}$ and d is square-free.*
- $\gcd(a, d) = 1$.

Proposition

$L = \mathbb{Q}(\sqrt{a(d + b\sqrt{d})})$, *where:*

- $a \in \mathbb{Z}$ *is odd square-free and* $b \in \mathbb{Z}_{>0}$.
- $d = b^2 + c^2$ *for some* $c \in \mathbb{Z}_{>0}$ *and* d *is square-free.*
- $\gcd(a, d) = 1$.

Proposition

$L = \mathbb{Q}(\sqrt{a(d+b\sqrt{d})})$, *where:*

- $a \in \mathbb{Z}$ *is odd square-free and* $b \in \mathbb{Z}_{>0}$.
- $d = b^2 + c^2$ *for some* $c \in \mathbb{Z}_{>0}$ *and* d *is square-free.*
- $\gcd(a, d) = 1$.

Theorem

Let $L/\mathbb{Q}$ *be a cyclic quartic extension defined by* $a, b, c, d \in \mathbb{Z}$ *as before. Let* H *be its non-classical Hopf-Galois structure. The following are equivalent:*

- $\mathcal{O}_L$ *is* $\mathfrak{A}_H$*-free.*
- *The quadratic form* $[b, 2c, -b]$ *represents* 1.
- *The Pell equation* $x^2 - dy^2 = b$ *has some solution* (x, y) *such that* b *divides* $x - cy$.

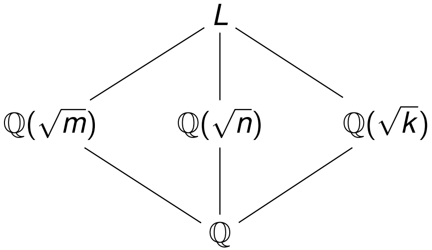
Let $L=\mathbb{Q}(\sqrt{m},\sqrt{n})$ be a biquadratic extension.

Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ be a biquadratic extension.

Let $d = \gcd(m, n)$ and $k = \frac{mn}{d^2}$.

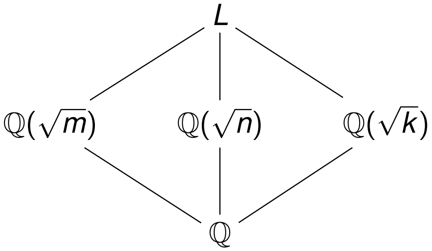
Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ be a biquadratic extension.

Let $d = \gcd(m, n)$ and $k = \frac{mn}{d^2}$.



Let $L = \mathbb{Q}(\sqrt{m}, \sqrt{n})$ be a biquadratic extension.

Let $d = \gcd(m, n)$ and $k = \frac{mn}{d^2}$.



There are three non-classical Hopf-Galois structures H_m, H_n, H_k on L/K, each one depending on an intermediate field.

Theorem (Truman (2012), G.-Rio (2022))

The freeness of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module is given by the following table.

Theorem (Truman (2012), G.-Rio (2022))

The freeness of $\mathcal{O}_L$ as $\mathfrak{A}_H$-module is given by the following table.

Mod 4		$\mathcal{O}_L$ as $\mathfrak{A}_{H_i}$-module		
m	n	H_m	H_n	H_k
1	1	Free $\iff$ $\exists x, y \in \mathbb{Z}$: $x^2 + my^2 = \pm 2d$	Free $\iff$ $\exists x, y \in \mathbb{Z}$: $x^2 + ny^2 = \pm 2d$	Free $\iff$ $\exists x, y \in \mathbb{Z}$: $x^2 + ky^2 = \pm 2\frac{n}{d}$
1	$\neq 1$	Free $\iff$ $\exists x, y \in \mathbb{Z}$: $x^2 + my^2 = \pm 2d$	Not free	Not free
3	2	Free $\iff$ $\exists x, y \in \mathbb{Z}$: $x^2 + my^2 = \pm 4d$	Free $\iff$ $\exists x, y \in \mathbb{Z}$: $x^2 + ny^2 = \pm 2d$	Free $\iff$ $\exists x, y \in \mathbb{Z}$: $x^2 + ky^2 = \pm 2\frac{n}{d}$

Work in progress: Kummer theory for Hopf-Galois extensions.

Work in progress: Kummer theory for Hopf-Galois extensions.

A Galois extension L/K is said to be Kummer if $\zeta_n \in K$ and L/K is abelian with exponent dividing n.

Work in progress: Kummer theory for Hopf-Galois extensions.

A Galois extension L/K is said to be Kummer if $\zeta_n \in K$ and L/K is abelian with exponent dividing n.

It is known that Kummer extensions of K are of the form

$$L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k}), \quad a_i \in K, \quad \zeta_n \in K$$

Work in progress: Kummer theory for Hopf-Galois extensions.

A Galois extension L/K is said to be Kummer if $\zeta_n \in K$ and L/K is abelian with exponent dividing n.

It is known that Kummer extensions of K are of the form

$$L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k}), \quad a_i \in K, \quad \zeta_n \in K$$

It is possible to generalize this notion to Hopf-Galois extensions L/K, for which it may happen that $\zeta_n \notin K$.

Work in progress: Kummer theory for Hopf-Galois extensions.

A Galois extension L/K is said to be Kummer if $\zeta_n \in K$ and L/K is abelian with exponent dividing n.

It is known that Kummer extensions of K are of the form

$$L = K(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_k}), \quad a_i \in K, \quad \zeta_n \in K$$

It is possible to generalize this notion to Hopf-Galois extensions L/K, for which it may happen that $\zeta_n \notin K$.

Theorem

Let $L = \mathbb{Q}(\sqrt[n]{a})$ with $a \in \mathbb{Q}$. Assume that $L \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ and that $\mathcal{O}_L = \mathbb{Z}[\sqrt[n]{a}]$. Then there is some Hopf-Galois structure H on $L/\mathbb{Q}$ such that $\mathcal{O}_L$ is $\mathfrak{A}_H$-free.

- S.U. Chase, M.E. Sweedler; *Hopf Algebras and Galois Theory*, Lecture Notes in Mathematics, Springer, 1969.
- L.N. Childs; *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory,* Mathematical Surveys and Monographs 80, American Mathematical Society, 2000.
- D. Gil-Muñoz, A. Rio; *Hopf-Galois module structure of quartic Galois extensions of* $\mathbb{Q}$*,* J. Pure Appl. Algebra 266 (2022), 107045.
- C. Greither, B. Pareigis; *Hopf-Galois theory for separable field extensions*, Journal of Algebra **106** (1987), 239-258.
- L. Guarnieri, L. Vendramin; *Skew braces and the Yang-Baxter equation* Mathematics of Computation **86** (2017), 2519-2534.

Thank you for your attention