Hopf algebras, Galois modules, and skew braces

Lorenzo Stefanello

Insalate di Matematica, 10 March 2022

Outline

- Skew braces
- Hopf algebras
- Galois modules

Skew braces

Main definition and examples

Definition ([Guarnieri and Vendramin, 2017])

A *skew brace* is a triple $(G, \cdot, \circ)$, where $(G, \cdot)$ and $(G, \circ)$ are groups and for all $g, h, k \in G$,

$$g \circ (h \cdot k) = (g \circ h) \cdot g^{-1} \cdot (g \circ k).$$

(Here $^{-1}$ denotes the inverse with respect to $\cdot$.)

Example

Let $(G, \cdot)$ be a group.

- $(G, \cdot, \cdot)$ is a skew brace.
- $(G, \circ, \cdot)$ is a skew brace, where $g \circ h = h \cdot g$.

Example

$(\mathbb{Z}, +, \circ)$ is a skew brace, where $m \circ n = m + (-1)^m n$.

Definition ([Drinfel'd, 1992])

A *solution* of the Yang–Baxter equation is a pair (X, r), where X is a nonempty set and

$$r\colon X \times X \to X \times X$$

is a bijective map such that

$$(r \times \mathrm{id}_X)(\mathrm{id}_X \times r)(r \times \mathrm{id}_X) = (\mathrm{id}_X \times r)(r \times \mathrm{id}_X)(\mathrm{id}_X \times r)$$

on $X \times X \times X$.

Problem

Find all the solutions of the Yang–Baxter equation.

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot, \circ)$ be a skew brace. Then (G, r) is a solution, where

$$r(g, h) = (g^{-1} \cdot (g \circ h), \overline{g^{-1} \cdot (g \circ h)} \circ g \circ h).$$

(Here an overline denotes the inverse with respect to $\circ$.)

Example

Consider $(G, \cdot, \cdot)$. Then (G, r) is a solution, where

$$r(g, h) = (h, h^{-1} \cdot g \cdot h).$$

Problem

Find explicit ways to construct skew braces.

Regular subgroups

Let $(G, \cdot)$ be a finite group, and write $\mathrm{Perm}(G)$ for the group of permutations on G. A subgroup $N \leq \mathrm{Perm}(G)$ is *regular* if $|N| = |G|$ and N acts transitively on G.

Example

Define λ and ρ as follows:

$$\begin{aligned} \lambda\colon G &\to \mathrm{Perm}(G) \\ \sigma &\mapsto (\tau \mapsto \sigma \cdot \tau) \\ \rho\colon G &\to \mathrm{Perm}(G) \\ \sigma &\mapsto (\tau \mapsto \tau \cdot \sigma^{-1}). \end{aligned}$$

Then $\lambda(G)$ and $\rho(G)$ are regular.

Skew braces and regular subgroups

Theorem ([Guarnieri and Vendramin, 2017])

Let $(G, \cdot)$ be a group. Then there is a bijective correspondence between skew braces $(G, \circ, \cdot)$ and regular subgroups N of $\mathrm{Perm}(G)$ normalised by $\lambda(G)$.

Explicitly, $N = \{\nu(g) \mid g \in G\}$, where $\nu(g)\colon h \mapsto g \circ h$.

Example

- $\lambda(G)$ corresponds to $(G, \cdot, \cdot)$.
- $\rho(G)$ corresponds to $(G, \circ, \cdot)$ with $g \circ h = h \cdot g$.

In [Caranti and LS, 2021], we constructed skew braces starting from suitable maps of a given group $(G, \cdot)$.

Corollary

Let $(G, \cdot)$ *be a group of nilpotency class two, and for all* $\psi \in \mathrm{End}(G)$, *define*

$$g \circ_\psi h = g \cdot \psi(g) \cdot h \cdot \psi(g)^{-1}.$$

Then for all $\psi, \varphi \in \mathrm{End}(G)$,

$$(G, \circ_\psi, \circ_\varphi)$$

is a skew brace.

Hopf algebras

The main definition

Let K be a field.

Definition

A *K-Hopf algebra* is a K-algebra H together with K-linear maps $\Delta\colon H \to H \otimes_K H$, $\varepsilon\colon H \to K$, and $S\colon H \to H$ such that certain technical conditions are satisfied.

Example

Let G be a finite group, and consider the *group algebra*

$$K[G] = \left\{ \sum_{\sigma \in G} k_\sigma \sigma \mid k_\sigma \in K \right\}.$$

Then $K[G]$ is a K-Hopf algebra: $\Delta(\sigma) = \sigma \otimes \sigma$, $\varepsilon(\sigma) = 1$, and $S(\sigma) = \sigma^{-1}$ for all $\sigma \in G$.

Let L/K be a finite Galois extension with Galois group G.
Then L is a left $K[G]$-module, with action

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

Moreover, the K-linear map

$$\begin{aligned} L \otimes_K K[G] &\to \mathrm{End}_K(L) \\ x \otimes h &\mapsto (y \mapsto x(h\cdot y)) \end{aligned}$$

is bijective.

Generalising Galois theory: Hopf–Galois theory

Let L/K be a finite extension, let H be a K-Hopf algebra, and suppose that L is a left H-module such that the H-action on L "mimics" that of $K[G]$.

Definition

We say that L/K is an *H-Galois extension*, or that H gives a *Hopf–Galois structure* on L/K, if the K-linear map

$$\begin{aligned} L \otimes_K H &\to \mathrm{End}_K(L) \\ x \otimes h &\mapsto (y \mapsto x(h \cdot y)) \end{aligned}$$

is bijective.

Example

L/K is a Galois extension with Galois group G if and only if L/K is an $K[G]$-Galois extension.
This structure is called the *classical* Hopf–Galois structure.

Motivations and an example

There are two main advantages:

- A finite Galois extension L/K has only one classical Hopf–Galois structure, but may have more nonclassical Hopf–Galois structures.
- Separable non-Galois finite extensions may admit Hopf–Galois structures!

Example ([Greither and Pareigis, 1987])

Take $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$, a separable non-Galois finite extension. Then there exists a $\mathbb{Q}$-Hopf algebra H such that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is H-Galois.

The Hopf–Galois correspondence

Let L/K be an H-Galois extension, and let H' be a K-sub Hopf algebra (in the obvious sense). Then

$$L^{H'} = \{x \in L \mid h \cdot x = \varepsilon(h)x \text{ for all } h \in H'\}$$

is a field, called the *fixed field* of H'.
Here $L^H = K$, and we obtain a correspondence inclusion-reversing and injective, not necessarily surjective.

Problem

Find in which cases the correspondence is also surjective.

Example

If $H = K[G]$, then we recover the usual Galois correspondence, because the K-sub Hopf algebra of $K[G]$ are all of the form $K[G']$ for $G' \leq G$.

Hopf–Galois structures and skew braces

Let L/K be a finite Galois extension with Galois group $(G, \cdot)$.

Theorem ([Greither and Pareigis, 1987])

There is a bijective correspondence between Hopf–Galois structures on L/K *and regular subgroups* N *of* $\mathrm{Perm}(G)$ *normalised by* $\lambda(G)$.

Corollary

There is a bijective correspondence between Hopf–Galois structures on L/K *and skew braces* $(G, \circ, \cdot)$.

Problem

Classify Hopf–Galois structures and skew braces, given the isomorphism class of $(G, \cdot)$.

Galois modules

The setting

Let L/K be a finite Galois extension with Galois group G.
Assume that we are in one of the following cases:

- L and K are number fields, that is, finite extensions of $\mathbb{Q}$. Write $\mathcal{O}_L$ and $\mathcal{O}_K$ for the integral closures of $\mathbb{Z}$ in L and K, respectively.
- L and K are p-adic fields, that is, finite extensions of $\mathbb{Q}_p$. Write $\mathcal{O}_L$ and $\mathcal{O}_K$ for the integral closures of $\mathbb{Z}_p$ in L and K, respectively.

The motivating question

By the normal basis theorem, L is free of rank one over $K[G]$. Similarly, $\mathcal{O}_L$ is a left $\mathcal{O}_K[G]$-module.

Question

Is $\mathcal{O}_L$ free of rank one over $\mathcal{O}_K[G]$?

Definition

L/K is *tamely ramified* if for all maximal ideals $\mathfrak{p}$ of $\mathcal{O}_K$, the characteristic of the residue field $\mathcal{O}_K/\mathfrak{p}$ does not divide the ramification index $e_{\mathfrak{p}}$ of $\mathfrak{p}$.

Theorem (Noether's theorem)

- *If $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$, then L/K is tamely ramified.*
- *If L and K are p-adic fields and L/K is tamely ramified, then $\mathcal{O}_L$ is free of rank one over $\mathcal{O}_K$.*

Associated order in $K[G]$

Question

What if L/K is not tamely ramified?

Definition ([Leopoldt, 1959])

The *associated order* of $\mathcal{O}_L$ in $K[G]$ is

$$\mathfrak{A}_{L/K} = \{h \in K[G] \mid h \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

Clearly $\mathcal{O}_L$ is a left $\mathfrak{A}_{L/K}$-module, and if $\mathcal{O}_L$ is free of rank one over an $\mathcal{O}_K$-subalgebra A of $K[G]$, then $A = \mathfrak{A}_{L/K}$.

Problem

Find in which cases $\mathcal{O}_L$ is free of rank one over $\mathfrak{A}_{L/K}$.

Some known results

$\mathcal{O}_L$ is free of rank one over $\mathfrak{A}_{L/K}$ in the following cases:

- $K = \mathbb{Q}$ and G is abelian ([Leopoldt, 1959]).
- $K = \mathbb{Q}$ and G is dihedral of order $2p$ ([Bergé, 1972]).
- $K = \mathbb{Q}$ and G is the quaternion group ([Martinet, 1972]).
- L and K are p-adic fields and $\mathrm{Gal}(L/\mathbb{Q}_p)$ is abelian ([Lettl, 1990]).
- L and K are p-adic fields and L/K satisfies a technical ramification condition ([Johnston, 2015]).

Question

What if $\mathcal{O}_L$ is not free over $\mathfrak{A}_{L/K}$?

Suppose that L/K is an H-Galois extension.

Definition

The *associated order* of $\mathcal{O}_L$ in H is

$$\mathfrak{A}_H = \{h \in H \mid h \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

Clearly $\mathcal{O}_L$ is a left $\mathfrak{A}_H$-module, and if $\mathcal{O}_L$ is free of rank one over an $\mathcal{O}_K$-subalgebra A of H, then $A = \mathfrak{A}_H$.

Problem

Find in which cases $\mathcal{O}_L$ is free of rank one over $\mathfrak{A}_H$.

A motivating result

In [Byott, 1997], it was built an extension of p-adic fields L/K and a K-Hopf algebra H such that

- L/K is Galois, but $\mathcal{O}_L$ is not free over $\mathfrak{A}_{L/K}$;
- L/K is H-Galois, and $\mathcal{O}_L$ is free of rank one over $\mathfrak{A}_H$.

Question

Which is the correct Hopf–Galois structure?

Bibliography I

Bergé, A.-M. (1972).
Sur l'arithmétique d'une extension diédrale.
Ann. Inst. Fourier (Grenoble), 22(2):31–59.

Byott, N. P. (1997).
Galois structure of ideals in wildly ramified abelian *p*-extensions of a *p*-adic field, and some applications.
J. Théor. Nombres Bordeaux, 9(1):201–219.

Caranti, A. and LS (2021).
Brace blocks from bilinear maps and liftings of endomorphisms.
arXiv:2110.11028.

Drinfel'd, V. G. (1992).
On some unsolved problems in quantum group theory.
In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin.

Greither, C. and Pareigis, B. (1987).
Hopf Galois theory for separable field extensions.
J. Algebra, 106(1):239–258.

Guarnieri, L. and Vendramin, L. (2017).
Skew braces and the Yang-Baxter equation.
Math. Comp., 86(307):2519–2534.

Johnston, H. (2015).
Explicit integral Galois module structure of weakly ramified extensions of local fields.
Proc. Amer. Math. Soc., 143(12):5059–5071.

Leopoldt, H.-W. (1959).
Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers.
J. Reine Angew. Math., 201:119–149.

Bibliography III

Lettl, G. (1990).
The ring of integers of an abelian number field.
J. Reine Angew. Math., 404:162–170.

Martinet, J. (1972).
Sur les extensions à groupe de Galois quaternionien.
C. R. Acad. Sci. Paris Sér. A-B, 274:A933–A935.