Local Galois module theory: An overview

Lorenzo Stefanello

YRANT 2021

August 19, 2021

Outline

1. Classical Galois module theory
2. Hopf–Galois module theory

Classical Galois module theory

Normal basis

Let L/K be a finite Galois extension with Galois group G.
If R is any commutative ring with unity, we write $R[G]$ for the *group algebra*:

$$R[G] = \left\{ \sum_{\sigma \in G} r_\sigma \sigma \mid r_\sigma \in R \right\}.$$

Then L is a $K[G]$-module in a natural way. (All modules are assumed to be left.)

Theorem (Normal basis theorem)

L is a free $K[G]$-module of rank one. Equivalently, there is an element $x \in L$ such that $\{\sigma(x)\}_{\sigma \in G}$ is a K-basis of L.

Normal integral basis

Now suppose that L and K are p-adic fields, where p is a rational prime, and let $\mathcal{O}_L$ and $\mathcal{O}_K$ be the valuation rings. Since $\mathcal{O}_L$ is a $\mathcal{O}_K[G]$-module, the following question is natural.

Question (Normal integral basis)

Is $\mathcal{O}_L$ a free $\mathcal{O}_K[G]$-module of rank one? Equivalently, is there an element $x \in \mathcal{O}_L$ such that $\{\sigma(x)\}_{\sigma \in G}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$?

Not in general!

A ramification answer

Definition

L/K is *tamely ramified* if p does not divide the ramification index $e_{L/K}$.

Theorem (Noether's theorem, [Noether, 1932], [Ullom, 1970])

$\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module of rank one if and only if L/K is tamely ramified.

Question

What can we do when the extension is not tamely ramified?

Associated order

Definition (Associated order, [Leopoldt, 1959])

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

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

The following facts hold:

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

This means that $\mathfrak{A}_{L/K}$ is the right object to study.

Some known results

$\mathcal{O}_L$ is a free $\mathfrak{A}_{L/K}$-module of rank one if

- L/K is absolutely abelian [Leopoldt, 1959], [Lettl, 1990];
- $K = \mathbb{Q}_p$ and $G \cong D_{2p}$ [Bergé, 1972];
- $K = \mathbb{Q}_p$ and $G \cong Q_8$ [Martinet, 1972];
- $K = \mathbb{Q}_p$ and G is metacyclic of a certain type [Jaulent, 1981];
- L/K satisfies a technical ramification condition [Johnston, 2015].

Question

What can we say about the structure of $\mathcal{O}_L$ in the negative situations?

Hopf–Galois module theory

Hopf algebras

Definition (Informal definition)

A K*-Hopf algebra* is a K-algebra H with additional K-linear maps $\Delta\colon H \to H \otimes_K H$, $\varepsilon\colon H \to K$, and $S\colon H \to H$ which satisfy certain technical conditions.

Example

$K[G]$ is the prototypical example of K-Hopf algebra, where, for all $\sigma \in G$, $\Delta(\sigma) = \sigma \otimes \sigma$, $\varepsilon(\sigma) = 1$, and $S(\sigma) = \sigma^{-1}$.

Note that we can replace K with any commutative ring with unity, for example $\mathcal{O}_K$.

Hopf–Galois theory

The "classical" Galois structure on L/K consists of a K-Hopf algebra $K[G]$, together with an action of $K[G]$ on L satisfying certain properties. This yields the following generalisation.

Definition (Informal definition)

A *Hopf–Galois structure* on L/K consists of a suitable K-Hopf algebra H, together with an action of H on L which mimics the action of $K[G]$ on L. We say that L/K is *H-Galois*.

Example

L/K is $K[G]$-Galois, and this is the *classical Hopf–Galois structure*.

Associated order in Hopf–Galois extensions

Let H be a K-Hopf algebra, and suppose that L/K is H-Galois. We can define the *associated order* of $\mathcal{O}_L$ in H by

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

It behaves the classical associated order $\mathfrak{A}_{L/K}$ in $K[G]$, and we can ask whether $\mathcal{O}_L$ is a free $\mathfrak{A}_H$-module of rank one.
There are two main advantages:

1. We can study Galois theory with a more general approach.
2. While there is (at most) one Galois structure, there may be more Hopf–Galois structures.

Theorem ([Childs, 1987], [Childs and Moss, 1994])

If $\mathfrak{A}_H$ is an $\mathcal{O}_K$-Hopf algebra with operations induced by H, then $\mathcal{O}_L$ is a free $\mathfrak{A}_H$-module of rank one.

Corollary

If $\mathfrak{A}_{L/K}$ is an $\mathcal{O}_K$-Hopf algebra with operations induced by $K[G]$, then $\mathcal{O}_L$ is a free $\mathfrak{A}_{L/K}$-module of rank one.

2. There may be more Hopf–Galois structures

In [Byott, 1997], the use of Kummer theory of formal groups yields 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 a free $\mathfrak{A}_{L/K}$-module;
- L/K is H-Galois and $\mathcal{O}_L$ is a free $\mathfrak{A}_H$-module of rank one.

Question

Which is the correct Hopf–Galois structure?

A bridge to group theory

Theorem ([Greither and Pareigis, 1987])

The Hopf–Galois structures on L/K correspond bijectively to certain "special" subgroups of $\mathrm{Perm}(G)$.

This yields connections with the study of regular subgroups, skew braces, radical rings, and the Yang–Baxter equation, and it motivates even more the task of finding all the Hopf–Galois structures on a given Galois extension.

In [Caranti and Stefanello, 2021], we studied some ways to find explicitly Hopf–Galois structures starting from suitable endomorphisms of the Galois group.

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 Stefanello, L. (2021).
From endomorphisms to bi-skew braces, regular subgroups, the Yang-Baxter equation, and Hopf-Galois structures.
J. Algebra, 587:462–487.

Bibliography II

Childs, L. and Moss, D. J. (1994).
Hopf algebras and local Galois module theory.
In *Advances in Hopf algebras (Chicago, IL, 1992)*, volume 158 of *Lecture Notes in Pure and Appl. Math.*, pages 1–24. Dekker, New York.

Childs, L. N. (1987).
Taming wild extensions with Hopf algebras.
Trans. Amer. Math. Soc., 304(1):111–140.

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

Bibliography III

Jaulent, J.-F. (1981).
Sur la l-structure galoisienne des idéaux ambiges dans une extension métacyclique de degré nl sur le corps des rationnels.
In *Number theory, 1979–1980 and 1980–1981*, Publ. Math. Fac. Sci. Besançon, pages Exp. No. 3, 20. Univ. Franche-Comté, Besançon.

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 IV

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.

Noether, E. (1932).
Normalbasis bei Körpern ohne höhere Verzweigung.
J. Reine Angew. Math., 167:147–152.

Ullom, S. (1970).
Integral normal bases in Galois extensions of local fields.
Nagoya Math. J., 39:141–148.