Quotient Hopf-Galois structures and associated orders in Hopf-Galois extensions

Paul Truman

Keele University, UK

Hopf algebras and Galois module structure
University of Nebraska at Omaha
Tuesday 28th May, 2019

Overview

It is sometimes possible to relate questions about integral module structure in a Galois extension of local or global fields to analogous questions about subextensions.

In this talk we generalize these ideas to Hopf-Galois extensions.

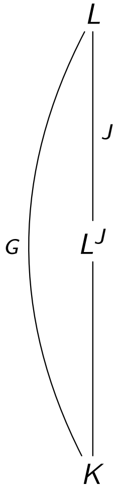
- Normality in Galois extensions via group algebras.
- Normality in separable Hopf-Galois extensions of fields.
- Two useful lemmas in Galois module theory.
- Hopf-Galois generalizations of these, and applications.

Normality in Galois extensions via group algebras

Let L/K be a Galois extension of fields with group G.
L/K is Hopf-Galois for $K[G]$.
We can characterize fixed fields via Hopf subalgebras:
The Hopf subalgebras of $K[G]$ are $K[J]$, with J a subgroup of G, and

$$\begin{aligned} L^J &= \{x \in L \mid \gamma(x) = x \text{ for all } \gamma \in J\} \\ &= \{x \in L \mid z \cdot x = \varepsilon(z)x \text{ for all } z \in K[J]\} \\ &= L^{K[J]}, \text{say.} \end{aligned}$$

L/L^J is Hopf-Galois for $L^J \otimes_K K[J]$.

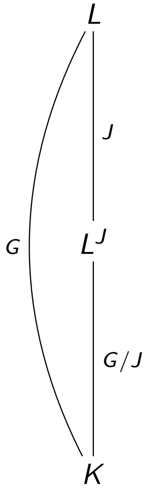


Normality in Galois extensions via group algebras

If J is a normal subgroup of G then L^J/K is a Galois extension with Galois group G/J.
In this case L^J/K is Hopf-Galois for $K[G/J]$.

Idea

Investigate analogous questions for Hopf-Galois structures on separable extensions of fields.



The Greither-Pareigis classification

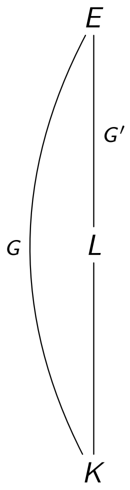
Theorem (Greither and Pareigis, 1987)

Let L/K be a separable extension of fields with Galois closure E.

- *Let $G = Gal(E/K)$, $G' = Gal(E/L)$, $X = G/G'$.*
- *Define $\lambda : G \to Perm(X)$ by $\lambda(\sigma)[\tau G'] = \sigma\tau G'$.*
- *Let G act on $Perm(X)$ by ${}^{\sigma}\eta = \lambda(\sigma)\eta\lambda(\sigma)^{-1}$.*

Then

- *There is a bijection between G-stable regular subgroups of $Perm(X)$ and Hopf-Galois structures on L/K;*
- *the Hopf algebra giving the Hopf-Galois structure corresponding to N is $E[N]^G$.*



Hopf subalgebras and fixed fields

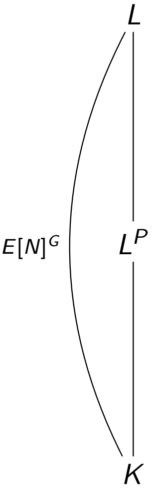
Let L/K be separable and Hopf-Galois for $E[N]^G$.

The Hopf subalgebras of $E[N]^G$ are $E[P]^G$ with P a G-stable subgroup of N.

Each Hopf subalgebra has a corresponding fixed field:

$$L^P = \{x \in L \mid z \cdot x = \varepsilon(z)x \text{ for all } z \in E[P]^G\}.$$

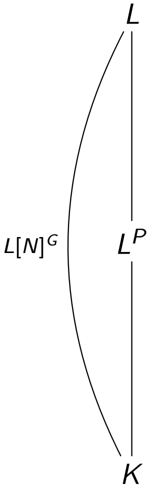
L/L^P is Hopf-Galois for $L^P \otimes_K E[P]^G$.



Example

If L/K is Galois with group G then $K[G]$ corresponds to $\rho(G) \subset \text{Perm}(G)$. The action of G on $\rho(G)$ is trivial, so every subgroup of $\rho(G)$ is G-stable. We recover the situation considered earlier.

Normality and quotient Hopf-Galois structures



Theorem (Koch, Kohl, T, Underwood, 2019)

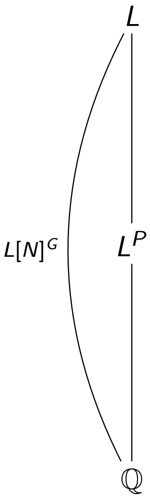
Suppose that L/K is a Galois extension of fields that is Hopf-Galois for $L[N]^G$, and that P is a normal G-stable subgroup of N.
Then L^P/K is Hopf-Galois for $L[N/P]^G$.

Important to note that L^P/K might not be Galois.

Normality and quotient Hopf-Galois structures

Example

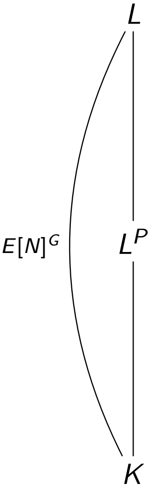
- Let L be the splitting field of $x^3 - 2$ over $\mathbb{Q}$.
- $L/\mathbb{Q}$ is Galois with Galois group $G \cong D_3$.
- $\mathrm{Perm}(G)$ contains G-stable regular subgroups that are isomorphic to C_6. Let N be one.
- $L/\mathbb{Q}$ is Hopf-Galois for $L[N]^G$.
- N has a unique subgroup P of order 2.
- P is normal and G-stable.
- By the theorem, $L^P/\mathbb{Q}$ is Hopf-Galois for $L[N/P]^G$.
- But $L^P/\mathbb{Q}$ is not Galois.



A slight generalization

Theorem

Suppose that L/K is a separable extension of fields that is Hopf-Galois for $E[N]^G$, and that P is a normal G-stable subgroup of N.
Then L^P/K is Hopf-Galois for $E[N/P]^G$.



Remainder of the talk is about the application of these ideas to questions of integral module structure.

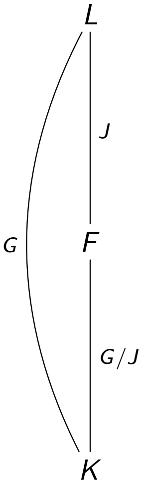
Henceforth, suppose that L/K is an extension of number fields or p-adic fields.

A useful lemma in Galois module theory

Suppose that L/K is Galois with group G, and $J \lhd G$.

Write $F = L^J$, and let

- $\pi : K[G] \twoheadrightarrow K[G/J]$ be the algebra homomorphism induced by the natural map $G \twoheadrightarrow G/J$;
- $\mathfrak{A}_{L/K}$ be the associated order of $\mathfrak{O}_L$ in $K[G]$;
- $\mathfrak{A}_{F/K}$ be the associated order of $\mathfrak{O}_F$ in $K[G/J]$.



Lemma (Byott and Lettl, 1996)

Suppose that $\mathfrak{O}_L = \mathfrak{A}_{L/K} \cdot \alpha$ and that L/F is (at most) tamely ramified. Then

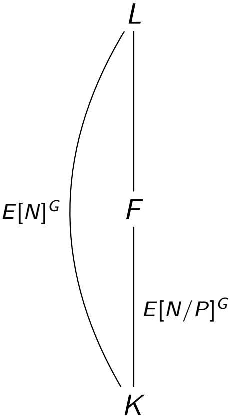
- $\mathfrak{A}_{F/K} = \pi(\mathfrak{A}_{L/K})$;
- $\mathfrak{O}_F = \mathfrak{A}_{F/K} \cdot \mathrm{Tr}_{L/F}(\alpha)$.

A Hopf-Galois version

Suppose that L/K is separable and Hopf-Galois for $E[N]^G$, and that $P \triangleleft N$ is G-stable.

Write $F = L^P$, and let

- $\mathfrak{A}_{L/K}$ be the associated order of $\mathfrak{O}_L$ in $E[N]^G$;
- $\mathfrak{A}_{F/K}$ be the associated order of $\mathfrak{O}_F$ in $E[N/P]^G$.



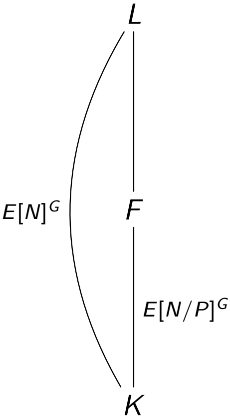
Lemma

The E-algebra homomorphism $\pi : E[N] \twoheadrightarrow E[N/P]$ induced by the natural map $N \twoheadrightarrow N/P$ descends to a K-algebra homomorphism $\pi : E[N]^G \twoheadrightarrow E[N/P]^G$

A Hopf-Galois version

Recall

- $F = L^P$;
- $\mathfrak{A}_{L/K}$ is the associated order of $\mathfrak{O}_L$ in $E[N]^G$;
- $\mathfrak{A}_{F/K}$ is the associated order of $\mathfrak{O}_F$ in $E[N/P]^G$.



Lemma

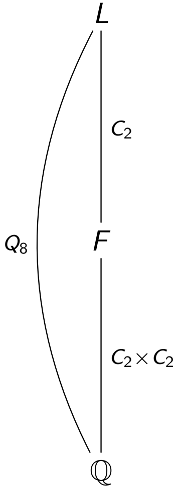
Suppose that $\mathfrak{O}_L = \mathfrak{A}_{L/K} \cdot \alpha$ and that L/F is tamely ramified. Then

- $\mathfrak{A}_{F/K} = \pi(\mathfrak{A}_{L/K})$;
- $\mathfrak{O}_F = \mathfrak{A}_{F/K} \cdot \mathrm{Tr}_{L/F}(\alpha)$.

An application

Theorem (Taylor)

Let $L/\mathbb{Q}$ be a tamely ramified Galois extension with group $G \cong Q_8$, and suppose that $L/\mathbb{Q}$ is Hopf-Galois for $L[N]^G$ with N cyclic.
Then $\mathfrak{O}_L$ is locally free, but not free, over $\mathfrak{A}_{L/\mathbb{Q}}$.



Proof.

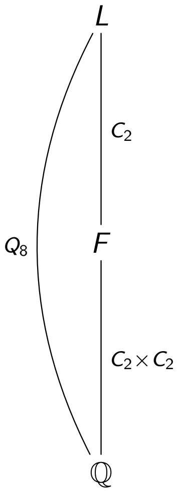
- Local freeness is already known.
- N has a unique subgroup P of order 2.
- P is normal and G-stable.
- $F = L^P$ is a real biquadratic extension of $\mathbb{Q}$.
- N/P is cyclic, and $K/\mathbb{Q}$ is Hopf-Galois for $L[N/P]^G$.

An application

Proof Continued...

- There are three HGS on $F/\mathbb{Q}$ for which the underlying N is cyclic.
- They correspond to the three quadratic subfields.
- $\mathfrak{O}_F$ is free over its associated order in a HGS only if the corresponding quadratic subfield is imaginary.
- Therefore $\mathfrak{O}_F$ is not free over its associated order in $L[N/P]^G$.
- By the lemma, $\mathfrak{O}_L$ is not free over $\mathfrak{A}_{L/\mathbb{Q}}$.

□



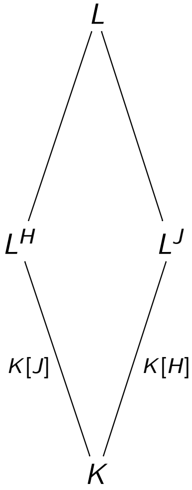
Another useful lemma in Galois module theory

Lemma (Byott and Lettl, 1996)

Suppose that L/K is Galois with group $G = H \times J$. Then L^H/K and L^J/K are linearly disjoint, and $L = L^H L^J$. Suppose in addition that

- $\mathfrak{d}(L^H/K)$ *and* $\mathfrak{d}(L^J/K)$ *are coprime;*
- $\mathfrak{O}_{L^H} = \mathfrak{A}_{L^H/K} \cdot \alpha$;
- $\mathfrak{O}_{L^J} = \mathfrak{A}_{L^J/K} \cdot \beta$.

Then $\mathfrak{O}_L = \mathfrak{A}_{L/K} \cdot \alpha\beta$.



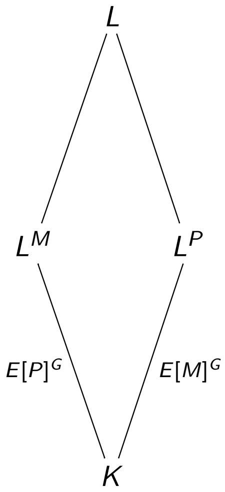
A Hopf-Galois version

Lemma

Suppose that L/K is separable and Hopf-Galois for $E[N]^G$, and that $N = M \times P$ for G-stable subgroups M, P of N. Then

- L^M/K *and* L^P/K *are linearly disjoint;*
- L^P/K *is Hopf-Galois for* $E[M]^G$*;*
- L^M/K *is Hopf-Galois for* $E[P]^G$*.*

Continued...



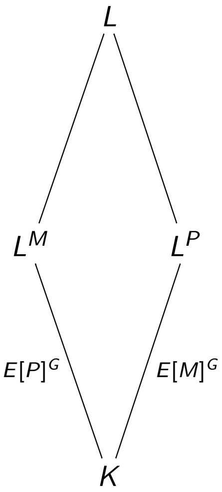
A Hopf-Galois version

Lemma (Continued)

Suppose in addition that

- $\mathfrak{d}(L^M/K)$ *and* $\mathfrak{d}(L^P/K)$ *are coprime;*
- $\mathfrak{O}_{L^M} = \mathfrak{A}_{L^M/K} \cdot \alpha$;
- $\mathfrak{O}_{L^P} = \mathfrak{A}_{L^P/K} \cdot \beta$.

Then $\mathfrak{O}_L = \mathfrak{A}_{L/K} \cdot \alpha\beta$.



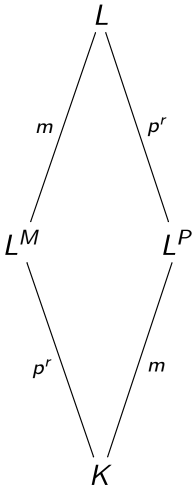
An application

Theorem

Let L/K be a tame separable extension of p-adic fields which is Hopf-Galois for $E[N]^G$, with N abelian. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}_{L/K}$-module.

Proof.

- Write $N = M \times P$ with $|M| = m$, $|P| = p^r$, and $p \nmid m$.
- M, P are normal and G-stable.
- L^P/K is Hopf-Galois for $E[M]^G$.
- L^M/K is Hopf-Galois for $E[P]^G$.

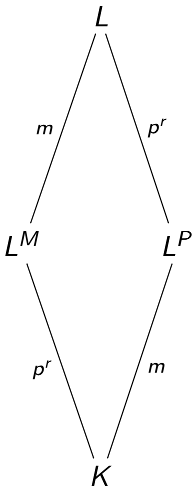


An application

Proof Continued..

- L^M/K is unramified, so $\mathfrak{O}_{L^M}$ is free over $\mathfrak{A}_{L^M/K}$.
- The degree of L^P/K is prime to p, so $\mathfrak{O}_{L^P}$ is free over $\mathfrak{A}_{L^P/K}$.
- $\mathfrak{d}(L^M/K)$ and $\mathfrak{d}(L^P/K)$ are coprime.
- By the lemma, $\mathfrak{O}_L$ is free over $\mathfrak{A}_{L/K}$.

□



Thank you for your attention.