An assortment of associated orders in Hopf-Galois extensions

Paul Truman

Keele University, UK

Galois and Hopf-Galois study group
Thursday 22nd July, 2021

Context

I'll benefit greatly from the contributions of the previous speakers!

Daniel's talk introduced Hopf-Galois module theory.
Nigel's talk exploited the additional structure provided by Hopf algebras to create interesting examples.

This talk does things the other way around: suppose we're interested in a field, and study it via the various Hopf-Galois structures.
Typically, the associated order in not a Hopf order.
We will almost come full circle: conclude by returning to tamely ramified extensions of number fields.

Overview

- Generalized normal basis generators
- Opposite Hopf-Galois structures
- A subextension technique
- Tamely ramified extensions
- Extensions of number fields

Standing assumptions

L/K finite separable extension of fields, often p-adic or number fields.
E denotes Galois closure of L/K
$G = \mathrm{Gal}(E/K)$, $G_L = \mathrm{Gal}(E/L)$, $X = G/G_L$.

$\lambda : G \to \mathrm{Perm}(X)$ denotes left translation map.
This yields an action of G on $\mathrm{Perm}(X)$ by ${}^{g}\eta = \lambda(g)\eta\lambda(g)^{-1}$.
N denotes regular G-stable subgroup of $\mathrm{Perm}(X)$.
Hopf algebra giving corresponding Hopf-Galois structure is $E[N]^G$.
$\mathfrak{A}$ denotes associated order of $\mathfrak{O}_L$ in $E[N]^G$.

Many results remain valid if $\mathfrak{O}_L$ is replaced with a fractional ideal $\mathfrak{B}$ of L.

Generalized normal basis generators

Generalized normal basis generators

The Hopf-Galois analogue of the Normal Basis Theorem: if H gives a Hopf-Galois structure on L/K then L is a free H-module of rank 1.

Proposition

An element $x \in L$ is a free generator of L as an $E[N]^G$-module if and only if the matrix $T_N(x) = (\eta(\overline{g})[x])_{\eta \in N,\, \overline{g} \in X}$ is nonsingular.

Corollary

If M is a further G-stable regular subgroup of $\mathrm{Perm}(X)$ and $M \cong N$ then $E[M]^G$ and $E[N]^G$ have the same normal basis generators.

Proof.

We have $M = \pi N \pi^{-1}$ for some $\pi \in \mathrm{Perm}(X)$.

For $x \in L$ we have $T_M(x) = \left(\pi\eta\pi^{-1}(\overline{g})[x]\right)$, which differs from $T_N(x)$ by permutations of the rows and columns. □

Generalized normal basis generators

Example

Let L/K be a Galois extension with nonabelian Galois group G.

Consider the regular G-stable subgroups $\rho(G)$ and $\lambda(G)$.

The corresponding HGS are given by $L[\rho(G)]^G \cong K[G]$ and $L[\lambda(G)]^G$.

Let π be the permutation of G given by $\pi(g) = g^{-1}$.

Then for all $g, h \in G$ we have

$$\pi\lambda(g)\pi^{-1}[h] = \pi[gh^{-1}] = hg^{-1} = \rho(g)[h].$$

Thus $\rho(G) = \pi\lambda(G)\pi^{-1}$, and so the corresponding structures have the same generalized normal basis generators.

Opposite Hopf-Galois structures

Opposite Hopf-Galois structures

Greither and Pareigis observed that $N^{opp} = \mathrm{Cent}_{\mathsf{Perm}(X)}(N)$ is also a regular G-stable subgroup of Perm(X).

We always have $N \cong N^{opp}$, but $N = N^{opp}$ if and only if N is abelian.

Call the HGS corresponding to N, N^{opp} *opposites* of one another.

Example

If L/K is a Galois extension with group G then the regular subgroups $\lambda(G)$ and $\rho(G)$ are opposites of one another.

Hence the structures given by $K[G]$ and $L[\lambda(G)]^G$ are opposites of one another.

Proposition

If $h \in E[N]^G$ and $h' \in E[N^{opp}]^G$ then for all $x \in L$ we have

$$h \cdot (h' \cdot x) = h' \cdot (h \cdot x).$$

Opposite Hopf-Galois structures

Theorem (T. 2017)

Let L/K be a separable extension of local or global fields in any characteristic. Then $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module if and only if it is a free $\mathfrak{A}^{opp}$-module.

Proof.

Suppose that $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module, with generator x.

Then x is a free generator of L as an $E[N]^G$-module.

So x is a free generator of L as an $E[N^{opp}]^G$-module.

For each $a \in \mathfrak{A}$ define $z_a \in E[N^{opp}]^G$ by $z_a \cdot x = a \cdot x$.

Then $\mathfrak{A}^{opp} = \{z_a \mid a \in \mathfrak{A}\}$: given $y \in \mathfrak{O}_L$ write $y = b \cdot x$ with $b \in \mathfrak{A}$.

Then

$$z_a \cdot y = z_a \cdot (b \cdot x) = b \cdot (z_a \cdot x) \in \mathfrak{O}_L.$$

Hence $\mathfrak{O}_L = \mathfrak{A}^{opp} \cdot x$, and the action is free. □

Opposite Hopf-Galois structures

Corollary

Let L/K be a Galois extension of local fields which is at most weakly ramified. Then $\mathfrak{O}_L$ is free over its associated order in $L[\lambda(G)]^G$.

Corollary

Let $L/\mathbb{Q}$ be a Galois extension which is at most tamely ramified and such that $4 \nmid [L : \mathbb{Q}]$. Then $\mathfrak{O}_L$ is free over its associated order in $L[\lambda(G)]^G$.

It can be shown that if $\mathfrak{A}$ is a maximal order in $E[N]^G$ then $\mathfrak{A}^{opp}$ is a maximal order in $E[N^{opp}]^G$.
It is possible for $\mathfrak{A}$ to be a Hopf order in $E[N]^G$ without $\mathfrak{A}^{opp}$ being a Hopf order in $E[N^{opp}]^G$ (example later).

A subextension technique

A subextension technique

We need a couple of results concerning normality in Hopf-Galois extensions. We will suppose that L/K is Galois.

If P is a G-stable subgroup of N then $L[P]^G$ is a Hopf subalgebra of $L[N]^G$. We can form a corresponding "fixed field":

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

We have $[L : L^P] = \dim_K(L[P]^G) = |P|$.

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

If P is normal in N then $L[N/P]^G$ gives a Hopf-Galois structure on L^P/K.

The assumption that L/K is Galois can be relaxed to "separable": upcoming paper.

A subextension technique

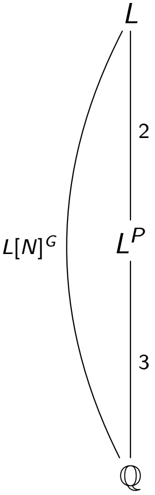
Example

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 $L[N/P]^G$.

Note that $L^P/\mathbb{Q}$ is not Galois.



A subextension technique

This is a slight generalization of a result of Gil-Muñoz and Rio.

Lemma

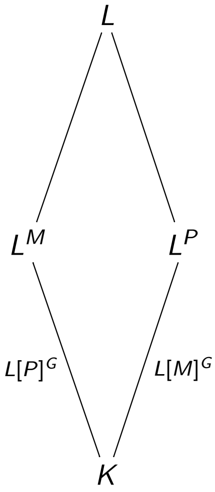
Suppose that $N = M \times P$ for G-stable subgroups M, P of N. Then

- *L^P/K is Hopf-Galois for $L[M]^G$;*
- *L^M/K is Hopf-Galois for $L[P]^G$.*

Suppose in addition that

- *L^P/K and L^M/K are arithmetically disjoint;*
- *$\mathfrak{O}_{L^M}$ is free over its associated order in $L[P]^G$;*
- *$\mathfrak{O}_{L^P}$ is free over its associated order in $L[M]^G$.*

Then $\mathfrak{O}_L$ is free over its associated order in $L[N]^G$.



Tamely ramified extensions

Tamely ramified extensions

Why study Hopf-Galois module structure of (at most) tamely ramified extensions L/K?

If L/K is Galois then $\mathfrak{O}_L$ is (locally) free $\mathfrak{O}_K[G]$-module.

Is $\mathfrak{O}_L$ (locally) free over its associated order in all Hopf-Galois structures?

What about non-normal extensions?

What about extensions of global fields?

Here there is the possibility of "better" descriptions.

Tamely ramified extensions

The order $\mathfrak{O}_E[N]^G$ within $E[N]^G$ is a formal analogue of $\mathfrak{O}_K[G]$ within $K[G]$. Regardless of whether L/K is tamely ramified, we have:

Proposition

$\mathfrak{O}_E[N]^G \subseteq \mathfrak{A}$.

Proof.

Let $z = \sum_{\eta \in N} c_\eta \eta \in \mathfrak{O}_E[N]^G$ and let $x \in \mathfrak{O}_L$.
Then $z \cdot x \in L$, but also

$$z \cdot x = \sum_{\eta \in N} c_\eta \eta^{-1}(\overline{1_G})[x] \in \mathfrak{O}_E.$$

Thus $z \cdot x \in \mathfrak{O}_E \cap L = \mathfrak{O}_L$. □

Tamely ramified extensions

We have just seen that $\mathfrak{O}_E[N]^G \subseteq \mathfrak{A}$.

If L/K is a wildly ramified extension of p-adic fields then $\mathfrak{O}_E[N]^G \subsetneq \mathfrak{A}$:

We have $\theta = \sum_{\eta \in N} \eta \in \mathfrak{O}_E[N]^G$, and $\theta \cdot x = \mathrm{Tr}_{L/K}(x)$ for all $x \in \mathfrak{O}_L$,

so $\pi_K^{-1}\theta \in \mathfrak{A}$.

However, if L/K is tamely ramified then we often have equality:

Theorem (T. 2018)

Suppose that L/K is a Galois extension of p-adic fields that is tamely ramified and that N is abelian. Then $\mathfrak{A} = \mathfrak{O}_L[N]^G$ and $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module.

The assumption that L/K is Galois can be removed, but need more machinery: upcoming paper.

Extreme cases: Unramified extensions

Proposition (T. 2011)

Suppose that L/K is an unramified extension of p-adic fields. Then $\mathfrak{A} = \mathfrak{O}_L[N]^G$, this is a Hopf order in $L[N]^G$, and $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module.

Proof.

In this case $\mathfrak{O}_L/\mathfrak{O}_K$ is a Galois extension of rings with group G.

Certainly $\mathfrak{O}_L[N]$ is an $\mathfrak{O}_L$-Hopf order in $L[N]$.

By Galois descent $\mathfrak{O}_L[N]^G$ is a Hopf order in $L[N]^G$.

The element $\theta = \sum_{\eta \in N} \eta$ is a left integral of $\mathfrak{O}_L[N]^G$.

We have $\theta \cdot x = \mathrm{Tr}_{L/K}(x)$ for all $x \in \mathfrak{O}_L$.

Since L/K is unramified, there exists $x \in \mathfrak{O}_L$ such that $\theta \cdot x = 1$.

Hence $\mathfrak{O}_L$ is an $\mathfrak{O}_L[N]^G$-tame extension of $\mathfrak{O}_K$.

It follows that $\mathfrak{O}_L$ is a free $\mathfrak{O}_L[N]^G$-module, and so $\mathfrak{A} = \mathfrak{O}_L[N]^G$. □

Extreme cases: Maximal associated orders

Proposition (T. 2011)

Suppose that L/K is an extension of p-adic fields, that $p \nmid [L:K]$, and that N is abelian. Then $\mathfrak{A} = \mathfrak{O}_E[N]^G$, this is the maximal order in $E[N]^G$, and $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module.

Proof.

Note that $|N| = [L:K]$.

Since $p \nmid |N|$ and N is abelian, $\mathfrak{O}_E[N]$ is the maximal order in $E[N]$.

Let $\mathcal{M}$ be the maximal order in $E[N]^G$.

If $z \in \mathcal{M}$ then $z \in \mathfrak{O}_E[N]$ and z is fixed by G, so $z \in \mathfrak{O}_E[N]^G$.

Hence $\mathfrak{O}_E[N]^G = \mathcal{M}$. But $\mathfrak{O}_E[N]^G \subseteq \mathfrak{A}$, so $\mathfrak{O}_E[N]^G = \mathfrak{A} = \mathcal{M}$.

Finally $\mathfrak{O}_L$ is a finitely generated torsionfree $\mathcal{M}$-module, hence free. □

Proving the main theorem

Theorem

Suppose that L/K is a Galois extension of p-adic fields that is tamely ramified and that N is abelian. Then $\mathfrak{A} = \mathfrak{O}_L[N]^G$ and $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module.

Proof.

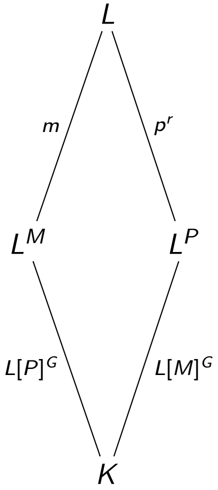
Write $N = M \times P$ with $|M| = m$, $|P| = p^r$, and $p \nmid m$.

Then M, P are normal and G-stable.

Thus L^P/K is Hopf-Galois for $L[M]^G$,

and L^M/K is Hopf-Galois for $L[P]^G$.

Continued . . .



Proving the main theorem

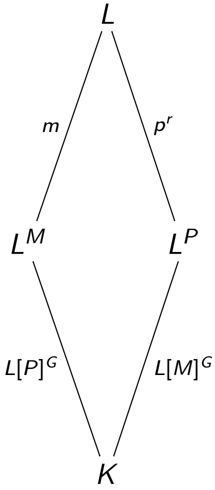
Proof Continued..

Since L/K is tamely ramified, L^M/K is unramified. Hence L^M/K and L^P/K are arithmetically disjoint.

Since L^M/K is unramified, $\mathfrak{O}_{L^M}$ is a free $\mathfrak{O}_L[P]^G$-module.

Since the degree of L^P/K is prime to p and M is abelian, $\mathfrak{O}_{L^P}$ is a free $\mathfrak{O}_L[M]^G$-module.

By the lemma, $\mathfrak{O}_L$ is a free $\mathfrak{O}_L[N]^G$-module. □



Tamely ramified extensions

Example

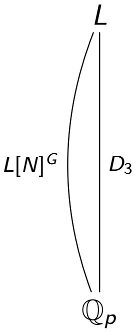
Let $p \equiv 2 \pmod 3$ be prime.

Let L be the splitting field of $x^3 - p$ over $\mathbb{Q}_p$.

$L/\mathbb{Q}_p$ is tamely ramified and Galois with group $G \cong D_3$.

Perm(G) contains G-stable regular subgroups that are isomorphic to C_6. Let N be one.

By the theorem the associated order of $\mathfrak{O}_L$ in $L[N]^G$ is $\mathfrak{O}_L[N]^G$, and $\mathfrak{O}_L$ is a free $\mathfrak{A}$-module.



Noncommutative Hopf-Galois structures

The assumption that N is abelian has been crucial.

The direct generalization to nonabelian N does not hold:

Example

Let $p \equiv 2 \pmod 3$ be prime.

Let L be the splitting field of $x^3 - p$ over $\mathbb{Q}_p$.

$L/\mathbb{Q}_p$ is tamely ramified and Galois with group $G \cong D_3$.

$\mathfrak{O}_L$ is free over its associated order in $\mathbb{Q}_p[G]$, which is $\mathbb{Z}_p[G]$.

Hence $\mathfrak{O}_L$ is free over its associated order in $L[\lambda(G)]^G$. But it can be shown that this associated order strictly contains $\mathfrak{O}_L[\lambda(G)]^G$.

Conjecture

If L/K is tamely ramified extension of p-adic fields then $\mathfrak{O}_L$ is free over its associated order in each Hopf-Galois structure on the extension.

Extensions of number fields

Galois Extensions of number fields

Suppose that L/K is Galois extension of number fields.

If K has class number one then can study $\mathfrak{O}_L$ directly:

Let $x_1, \ldots, x_n$ be $\mathfrak{O}_K$-basis of $\mathfrak{O}_L$.

Let $h_1, \ldots, h_n$ be K-basis of $L[N]^G$.

Study action of the h_i on the x_j: determine $\mathfrak{O}_K$-basis of $\mathfrak{A}$.

Let $x \in \mathfrak{O}_L$ be a candidate generator of $\mathfrak{O}_L$ as $\mathfrak{A}$-module.

Compute generalized module index $[\mathfrak{O}_L : \mathfrak{A} \cdot x]$, attempt to choose x such that this is trivial, or show that this is impossible.

Gil-Muñoz studies Galois extensions of $\mathbb{Q}$ of degree 4.

Obtains criteria for $\mathfrak{O}_L$ to be free over various associated orders in terms of solubility of generalized Pell equations.

In particular: the direct analogue of Leopoldt's theorem does not hold.

Another approach

First ask whether $\mathfrak{O}_L$ is *locally free* over $\mathfrak{A}$.

That is: for each prime $\mathfrak{p}$ of $\mathfrak{O}_K$ let

$$\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{O}_{K,\mathfrak{p}} \otimes_{\mathfrak{O}_K} \mathfrak{O}_L$$

and

$$\mathfrak{A}_\mathfrak{p} = \mathfrak{O}_{K,\mathfrak{p}} \otimes_{\mathfrak{O}_K} \mathfrak{A},$$

and ask whether $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_\mathfrak{p}$-module for all $\mathfrak{p}$.

Then employ some kind of local-to-global-machinery to study global freeness.

Earlier results on tamely ramified extensions can be generalized to this context.

Tamely ramified Galois extensions of number fields

Let L/K be a Galois extension of number fields.

Proposition

Suppose that $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$ that is unramified in L. Then $\mathfrak{A}_\mathfrak{p} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$, this is a Hopf order in $L_\mathfrak{p}[N]^G$, and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_\mathfrak{p}$-module.

Proposition

Suppose that $\mathfrak{p}$ is a prime ideal of $\mathfrak{O}_K$ that does not divide $[L:K]\mathfrak{O}_K$, and that N is abelian. Then $\mathfrak{A}_\mathfrak{p} = \mathfrak{O}_{L,\mathfrak{p}}[N]^G$, this is the maximal order in $L_\mathfrak{p}[N]^G$, and $\mathfrak{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_\mathfrak{p}$-module.

Theorem (T. 2011)

Suppose that no prime ideal of $\mathfrak{O}_K$ dividing $[L:K]\mathfrak{O}_K$ is ramified in L, and that N is abelian. Then $\mathfrak{A} = \mathfrak{O}_L[N]^G$ and $\mathfrak{O}_L$ is a locally free $\mathfrak{A}$-module.

Some local to global machinery

If $\mathfrak{O}_L$ is locally free over $\mathfrak{A}$ then it defines a class in the locally free class group $\mathrm{Cl}(\mathfrak{A})$.

We can describe this group via idèles.

Writing $H = L[N]^G$ let:

$$\mathbb{J}(H) = \left\{ (h_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} H_\mathfrak{p}^\times \mid h_\mathfrak{p} \in \mathfrak{A}_\mathfrak{p}^\times \text{ for almost all } \mathfrak{p} \right\}.$$

Then $\mathrm{Cl}(\mathfrak{A})$ is isomorphic to a quotient of $\mathbb{J}(H)$ by a certain subgroup arising from $\mathfrak{A}$.

To obtain the class of $\mathfrak{O}_L$ in $\mathrm{Cl}(\mathfrak{A})$:

Fix $x \in L$ such that $L = H \cdot x$;

For each $\mathfrak{p}$ let $x_\mathfrak{p}$ be such that $\mathfrak{O}_{L,\mathfrak{p}} = \mathfrak{A}_\mathfrak{p} \cdot x_\mathfrak{p}$;

Define $(h_\mathfrak{p})_\mathfrak{p}$ by $h_\mathfrak{p} \cdot x = x_\mathfrak{p}$;

study class of $(h_\mathfrak{p})_\mathfrak{p}$ in quotient.

Some local to global machinery

This approach is applied to give criteria for $\mathfrak{O}_L$ to be free over its associated orders in various Hopf-Galois structures for:

- tamely ramified $C_p \times C_p$ extensions
  (T. 2012, 2016);
- tamely ramified Q_8 extensions of $\mathbb{Q}$
  (S. Taylor, thesis, 2020);
- tamely ramified non-normal extensions of the form $L = K(\sqrt[p]{a})$ with $\zeta_p \notin K$
  (T. 2019);
- tamely ramified non-normal extensions of the form $L = K(\sqrt[p]{a_1}, \ldots \sqrt[p]{a_r})$ with $\zeta_p \notin K$.
  (Prestidge).

Thank you for your attention.