A Class of Profinite Hopf-Galois Extensions over Q

Timothy Kohl

Boston University

May 25, 2017

Hopf-Galois Theory

An extension K/k is Hopf-Galois if there is a k-Hopf algebra H and a k-algebra homomorphism $\mu : H \to End_k(K)$ such that

- $\mu(ab) = \sum_{(h)} \mu(h_{(1)}(a)\mu(h_{(2)})(b)$
- $K^H = \{a \in K \mid \mu(h)(a) = \epsilon(h)a \ \forall h \in H\} = k$
- μ induces $I \otimes \mu : K\#H \xrightarrow{\cong} End_k(K)$

If K/k is Galois with $\Gamma = Gal(K/k)$ then, by linear independence of characters, the elements of Γ are a K-basis for $End_k(K)$ whence there exists a natural map:

$$H = k[\Gamma] \xrightarrow{\mu} End_k(K)$$

which induces

$$I \otimes \mu : K\#H \xrightarrow{\cong} End_k(K)$$

For the group ring $k[\Gamma]$ the endomorphisms arise as linear combinations of the automorphisms given by the elements of Γ.

Hopf-Galois theory is a generalization of ordinary Galois theory in several ways.

- One can put Hopf Galois structure(s) on separable field extensions K/k which aren't classically Galois. e.g. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$
- Moreover, one can take an extension L/K which *is* Galois with group Γ (hence Hopf-Galois for $H = K[\Gamma]$) and also find *other* Hopf algebras which act besides $K[\Gamma]$.

In this talk we will be focusing on the case where K/k is not already a Galois extension.

- K/k is a finite separable extension
- $\Gamma = Gal(\tilde{K}/k)$ where $\tilde{K}$ is the normal closure
- $\Delta = Gal(\tilde{K}/K)$ and $B = Perm(\Gamma/\Delta)$

Γ acting on itself by left translation yields an embedding

$$\lambda : \Gamma \hookrightarrow B$$

Definition: $N \leq B$ is *regular* if N acts transitively and fixed point freely on Γ.

Theorem

[3, Greither-Pareigis] The following are equivalent:

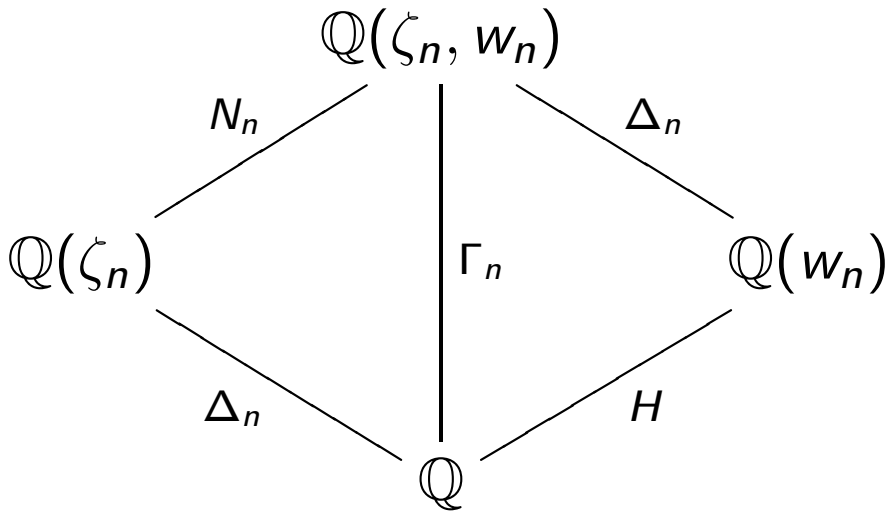
- *K/k is H-Galois for H a k-Hopf algebra*
- *There is a regular subgroup $N \leq B$ such that $\lambda(\Gamma) \leq Norm_B(N)$ where N yields $H = (\tilde{K}[N])^{\Gamma}$.*

where $\tilde{K} \otimes H \cong \tilde{K}[N]$. (i.e. H is $\tilde{K}$-form of $k[N]$)

Radical Extensions of $\mathbb{Q}$

The examples we consider are the radical extensions $\mathbb{Q}(w_n)/\mathbb{Q}$ where $w_n = \sqrt[p^n]{a}$ for $a \in \mathbb{Q}$, such that $[\mathbb{Q}(w_n) : \mathbb{Q}] = p^n$ where p is an odd prime, and ζ_n is a primitive p^{n-th} root of unity.

$$N_n = Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_n)) \cong C_{p^n}$$
$$\Delta_n = Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(w_n)) \cong Aut(C_{p^n})$$
$$\Gamma_n = Gal(\mathbb{Q}(w_n, \zeta_n)/\mathbb{Q}) = N_n\Delta_n$$



This case was enumerated by the presenter in 1998.

Theorem

[5, Theorem 3.3] For each n and each odd prime p, the extension $\mathbb{Q}(w_n)/\mathbb{Q}$ is Hopf-Galois with respect to the action of exactly one Hopf algebra, namely $H_n = (\mathbb{Q}(\zeta_n, w_n)[N_n])^{\Gamma_n}$, where, in fact, $H_n = (\mathbb{Q}(\zeta_n)[N_n])^{\Delta_n}$. That is, the extension is almost classical since $N_n \leq Gal(\mathbb{Q}(\zeta_n, w_n))$ and the equality of the two Hopf-algebras is due to the fact (from descent) that $N_n \leq \Gamma_n$ acts trivially on itself.

The $\mathbb{Q}$-Hopf algebra $H_n = (\mathbb{Q}(\zeta_n)[N_n])^{\Delta_n}$ can be described quite explicitly since $\Delta_n \cong Aut(N_n)$

Theorem

H_n is isomorphic to $(\mathbb{Q}[N_n])^*$ the linear dual of the group ring.

Specifically, H_n has a basis $\{e_{n,i}\}$ where

$$e_{n,i} = \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \sigma_n^j$$

which, if $\langle \chi_n \rangle$ is the generator of $\hat{N}_n$, can be identified with

$$\widehat{e}_{n,i} = \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \chi_n^j$$

where $\widehat{e}_{n,i}(\sigma_n^k) = \delta_{ik}$ and the isomorphism $\mathbb{Q}(\zeta_n)[N_n] \to \mathbb{Q}(\zeta_n)\widehat{N}_n$ is Δ_n-equivariant.

This isomorphism is mentioned in passing in [3] (actually quoting [1, p.39]) as being one of the Hopf algebras which act on this extension, but which by [5] is the only Hopf-Galois structure.

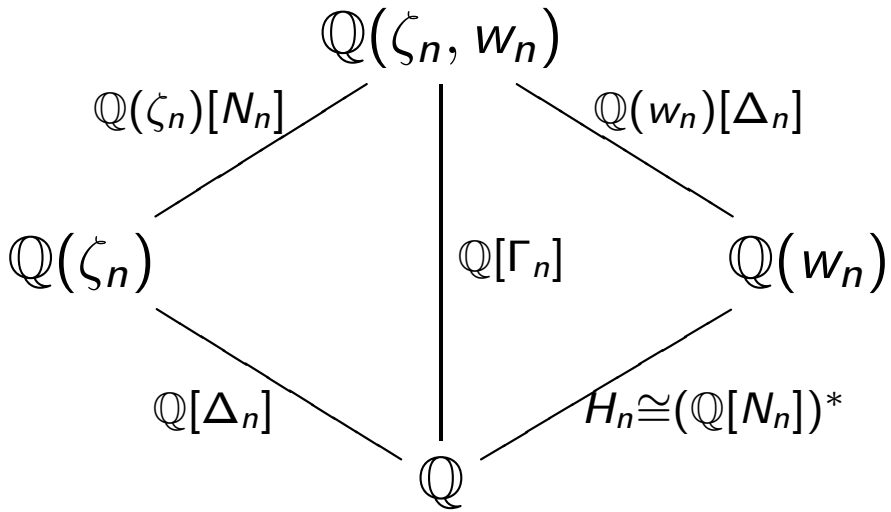
It's interesting to note how H_n acts on $\mathbb{Q}(w_n)$.

Proposition

The action of H_n on $\mathbb{Q}(w_n)$ is as follows. If $i = 0, \ldots, p^n - 1$ and $k = 0, \ldots p^n - 1$ then $e_{n,i}(w_n^k) = \delta_{ik} w_n^k$.

As such, the $e_{n,i}$ are almost a 'dual basis' to $\{1, w_n, \ldots, w_n^{p^n-1}\}$.

Extrapolating further, one could almost view this setup as a form of 'natural irrationality'.



Now we know that H_n will be a form of $\mathbb{Q}[N_n]$ in that $\mathbb{Q}(\zeta_n) \otimes H_n \cong \mathbb{Q}(\zeta_n)[N_n]$ but it will also be important in the sequel to have some insight into the structure of $\mathbb{Q}(\zeta_m) \otimes H_n$ for different m.

Lemma

Given H_n as defined above, if $m \geq n$ then $\mathbb{Q}(\zeta_m) \otimes H_n \cong \mathbb{Q}(\zeta_m)[N_n]$ and if $m < n$ then $\mathbb{Q}(\zeta_m) \otimes H_n$ contains $\sigma_n^{p^{n-m}}$.

So if one *partially* base changes H_n by throwing in p^{m-th} roots of unity for $m \leq n$ then the resulting Hopf algebra will contain a group ring over a sub-group of N_n.

We also consider the isomorphism

$$\mathbb{Q}(w_n)\#H_n \cong End_{\mathbb{Q}}(\mathbb{Q}(w_n))$$

which is a consequence of $\mathbb{Q}(w_n)/\mathbb{Q}$ being Hopf-Galois with respect to H_n. The underlying algebra of $\mathbb{Q}(w_n)\#H_n$ is $\mathbb{Q}(w_n) \otimes H_n$ but where the multiplication is 'twisted' by the action of H_n on $\mathbb{Q}(w_n)$. Specifically

$$(a\#h)(b\#h') = \sum_{(h)} ah_{(1)}(b)\#h_{(2)}h'$$

where in H_n we have

$$\Delta(e_{n,i}) = \sum_{\{s,t \mid s+t=i\}} e_{n,s} \otimes e_{n,t}$$

$\mathbb{Q}(w_n)$ is embedded in $End_{\mathbb{Q}}(\mathbb{Q}(w_n)$ via left multiplication and, of course, H_n is embedded as well.

Given the basis $\{w_n^j\}$ of $\mathbb{Q}(w_n)/\mathbb{Q}$ and the basis $\{e_{n,i}\}$ of H_n we have that $End_{\mathbb{Q}}(\mathbb{Q}(w_n))$ has basis $\{w_n^j \# e_{n,i}\}$ where

$$(w_n^j \# e_{n,i})(w_n^k) = \begin{cases} 0 & \text{if } i \neq k \\ w_n^{j+k} & \text{if } i = k \end{cases}$$

As such, the multiplication in $\mathbb{Q}(w_n)\#H_n$ is given by:

$$(w_n^j \# e_{n,i})(w_n^k \# e_{n,l}) = \begin{cases} w_n^{j+k} \# e_{n,l} \text{ if } k+l=i \\ 0 \qquad\qquad \text{otherwise} \end{cases}$$

Profinite Forms

In this section we shall construct a profinite Hopf algebra form that satisfies a generalization of the following due to Hagenmüller and Pareigis

Theorem

[4, Theorem 5] Let G be a finitely generated group with finite automorphism group $F = Aut(G)$. Then there is a bijection between $\mathbf{Gal}(k, F)$ *(extensions of k with Galois group F) and* $\mathbf{Hopf}(k[G])$ *(Hopf algebra forms of $k[G]$) which associates with each F-Galois extension K of k the Hopf algebra*

$$H = \{\sum c_g g \in KG | \sum f(c_g) f(g) = \sum c_g g \text{ for all } f \in F\}$$

Furthermore, H is a K-form of $k[G]$ by the isomorphism

$$\omega : H \otimes K \cong KG, \ \omega(h \otimes a) = ah$$

All the H_n are $\mathbb{Q}$-Hopf algebras which are $\mathbb{Q}(\zeta_n)$-forms of the group rings $\mathbb{Q}[N_n]$ and are examples of the above theorem in action.

The reason for this is that Δ_n is isomorphic to the automorphism group of the cyclic group N_n as well as to $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

What we would like to do now is to consider a profinite version of the above result where the usage of the term *profinite* is motivated by looking at the construction of the Galois group of a direct limit (union) of field extensions.

In particular, for a base field F, if $L = \varinjlim K$ where K is a chain of sub-fields of L containing F, then if each K is a Galois extension of F then $Gal(L/F) = \varprojlim Gal(K/F)$ the inverse limit of the Galois groups of each of the K/F.

Here we shall consider the fields $\mathbb{Q}(w_n)$. Even though these are not normal extensions of $\mathbb{Q}$, by what we have already shown each *is* Hopf-Galois over $\mathbb{Q}$ with respect to the Hopf algebras H_n.

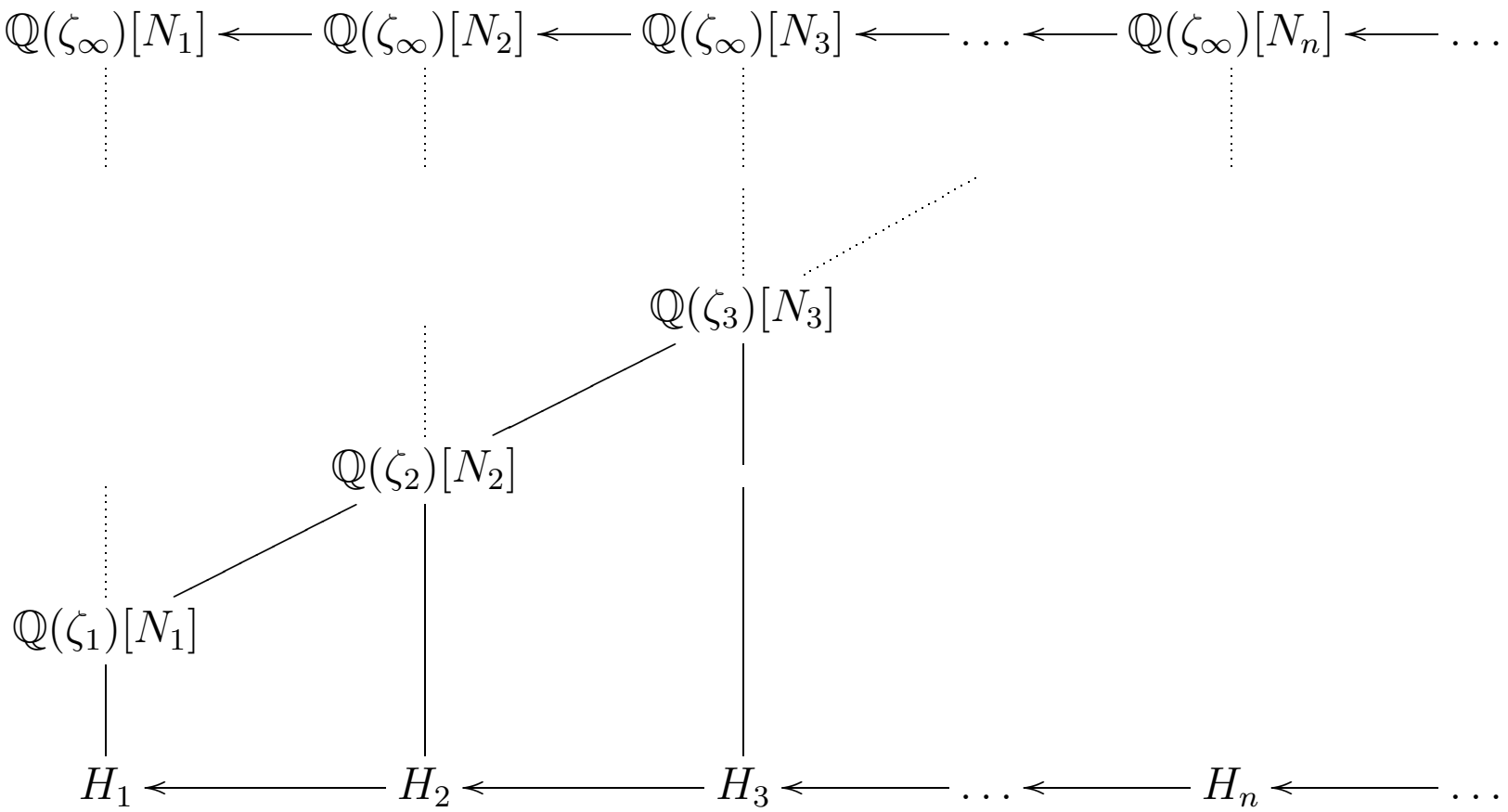
As such, we will start with an inverse system using the H_n. The resulting Hopf algebra will be a form of an infinite group whose automorphism group is not finite, but which satisfies the above theorem.

That the automorphism group is infinite contrasts with the setup in [4].

While the H_n are all $\mathbb{Q}$-Hopf algebras, the group rings $\mathbb{Q}(\zeta_n)[N_n]$ (which contain each H_n) are $\mathbb{Q}(\zeta_n)$-Hopf algebras for each n.

As such, one cannot start with a directed system involving these group rings, and then descend since these all lie in distinct categories of Hopf algebras, one for each ground field $\mathbb{Q}(\zeta_n)$.

Since each H_n is $\mathbb{Q}(\zeta_n)$-form of $\mathbb{Q}[N_n]$, we can base change all up to $\mathbb{Q}(\zeta_\infty)$ to yield $\mathbb{Q}(\zeta_\infty)$-Hopf algebras $\mathbb{Q}(\zeta_\infty)[N_n]$



Define $\nu_{j,i} : \mathbb{Q}(\zeta_\infty)[N_j] \longrightarrow \mathbb{Q}(\zeta_\infty)[N_i]$ for $j \geq i$ as follows:

$$\nu_{j,i}(q) = q \text{ for } q \in \mathbb{Q}(\zeta_\infty)$$
$$\nu_{j,i}(\sigma_j) = \sigma_i$$

Hence $\nu_{i,i}$ is the identity map on $\mathbb{Q}(\zeta_\infty)[N_i]$ and $\nu_{j,i} \circ \nu_{k,j} = \nu_{k,i}$ *for* $k \geq j \geq i$ and we have that $\nu_{j,i}$ is a surjective map of $\mathbb{Q}(\zeta_\infty)$-Hopf algebras.

Moreover, one can show that

$$\nu_{n,n-1}(e_{n,i}) = \begin{cases} e_{n-1,i/p} & \text{if } i \in p\mathbb{Z}_{p^{n-1}} \subseteq \mathbb{Z}_{p^n} \\ 0 & \text{otherwise} \end{cases}$$

One may note that, $\nu_{n,n-1} : H_n \to H_{n-1}$ where $H_n = (\mathbb{Q}[N_n])^*$ and $H_{n-1} = (\mathbb{Q}[N_{n-1}])^*$ can be viewed as the dual of the natural map $\alpha_{n-1,n} : \mathbb{Q}[N_{n-1}] \to \mathbb{Q}[N_n]$ given by $\alpha_{n-1,n}(\sigma_{n-1}) = \sigma_n^p$.

This would mean that $\alpha^*_{n-1,n}(e_{n,i})(\sigma^j_{n-1}) = e_{n,i}(\sigma_n^{pj}) = \delta_{i,pj}$.

As such $\alpha^*_{n-1,n}(e_{n,i}) = 0$ if i is not a multiple of p, and if i were a multiple of p then $\alpha^*_{n-1,n}(e_{n,i}) = e_{n-1,i/p}$ which is exactly what we get with $\nu_{n,n-1}$.

$H_n = (\mathbb{Q}(\zeta_n)[N_n])^{\Delta_n}$ where Δ_n acts diagonally on the scalars and group elements by virtue of it being $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and isomorphic to $Aut(N_n)$.

In a related way we will consider the action of $Gal(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})$ on each $\mathbb{Q}(\zeta_\infty)[N_n]$.

Define $\phi_{j,i} : \Delta_j \longrightarrow \Delta_i$ $(j \geq i)$ by $\phi_{j,i}(\delta_j) = \delta_i$.

It is easy to verify that $\{\Delta_i, \phi_{j,i}\}$ is also an inverse system and we shall define

$$\Delta_\infty = \varprojlim \Delta_i$$

which, amongst other things, is the Galois group of the profinite extension $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}$.

Restricting $\nu_{j,i}$ to the N_j yields an inverse system $\{N_j, \nu_{j,i}\}$ and we define $N_\infty = \varprojlim N_j$.

Each N_j is cyclic of order p^j and Δ_∞ is also the inverse limit of the automorphism groups of each N_j.

Since a given primitive root π mod p is also a primitive root mod p^n then we can choose the Galois group of $\mathbb{Q}(\zeta_j)$ to be generated by an element which acts to a raise ζ_n to π for all n.

Similarly, each automorphism group is generated by an element which acts to raise σ_n to the same power as well.

We have the following which is known, for example in Fuchs, [2, p.656], but we present here for use later.

Proposition

$$
\begin{aligned}
N_\infty &\cong \{\{\sigma_j^{a_j}\} \in \Pi_{j=1}^{\infty} N_j \mid \nu_{j,i}(\sigma_j^{a_j}) = \sigma_i^{a_i} \ (mod\ p^i))\} \\
&\cong \{\{\sigma_j^{a_j}\} \in \Pi_{j=1}^{\infty} N_j \mid a_j \equiv a_i \ (mod\ p^i))\} \\
&\cong J_p \text{ the p-adic integers} \\
\Delta_\infty &\cong \{\{\delta_i^{e_i}\} \in \Pi_{j=1} \Delta_j \mid \phi_{j,i}(\delta_j^{e_j}) = \delta_i^{e_i}\} \\
&\cong \{\{\delta_i^{e_i}\} \in \Pi_{j=1} \Delta_j \mid e_j \equiv e_i \ (mod\ p^i)\} \\
&\cong (J_p)^* \text{ the unit p-adic integers} \\
&\cong Aut(N_\infty) \\
&\cong Aut(\varinjlim N_n) \text{ (of interest later)}
\end{aligned}
$$

The following diagram commutes:

$$\begin{array}{ccc} \mathbb{Q}(\zeta_\infty)[N_j] & \xrightarrow{\nu_{j,i}} & \mathbb{Q}(\zeta_\infty)[N_i] \\ \Big\downarrow{\scriptstyle \delta_j} & & \Big\downarrow{\scriptstyle \delta_i} \\ \mathbb{Q}(\zeta_\infty)[N_j] & \xrightarrow[\nu_{j,i}]{} & \mathbb{Q}(\zeta_\infty)[N_i] \end{array}$$

i.e. The maps $\nu_{j,i}$ are compatible with the descent data coming from Δ_∞.

We have then that

$$\{\mathbb{Q}(\zeta_\infty)[N_j]\} \text{ and } \{(\mathbb{Q}(\zeta_\infty)[N_j])^{\Delta_\infty}\} \text{ and } \{H_j\}$$

are inverse systems with respect to $\nu_{j,i}$ where

$$\varprojlim \mathbb{Q}(\zeta_\infty)[N_j] = \mathbb{Q}(\zeta_\infty)[N_\infty]$$

and if we define

$$H_\infty = \varprojlim H_j$$

we ask what the relationship is between $\mathbb{Q}(\zeta_\infty)[N_\infty]$ and H_∞?

Theorem

Given $\mathbb{Q}(\zeta_\infty)$, N_∞, Δ_∞, *and* H_∞ *as defined above:*

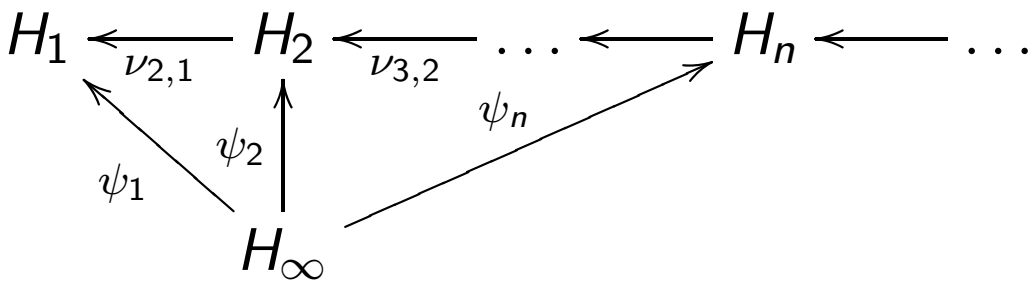
$$(a)\ \mathbb{Q}(\zeta_\infty) \otimes_{\mathbb{Q}} H_\infty \cong \mathbb{Q}(\zeta_\infty)[N_\infty]$$

$$(b)\ H_\infty = (\mathbb{Q}(\zeta_\infty)[N_\infty])^{\Delta_\infty}$$

Sketch of proof: That Δ_∞ acts on $\mathbb{Q}(\zeta_\infty)[N_\infty]$ is clear given that $\Delta_\infty \cong Gal(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})$ and $Aut(N_\infty)$.

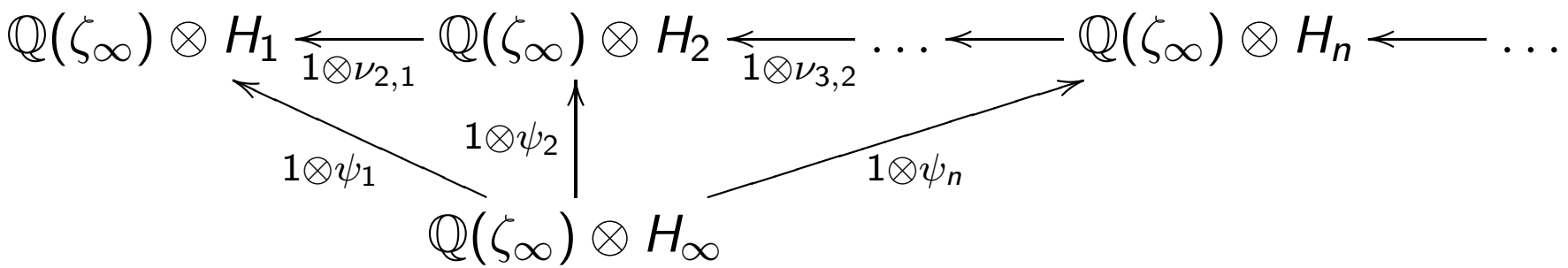
Moreover we know that $\delta_i(\nu_{j,i}(x)) = \nu_{j,i}(\delta_j(x)) = \nu_{j,i}(\phi_{j,i}(\delta_i)(x))$ for all $x \in \mathbb{Q}(\zeta_j)[N_j]$.
(i.e. we may think of the $\nu_{j,i}$'s as Δ_∞-maps)

Also, we have:

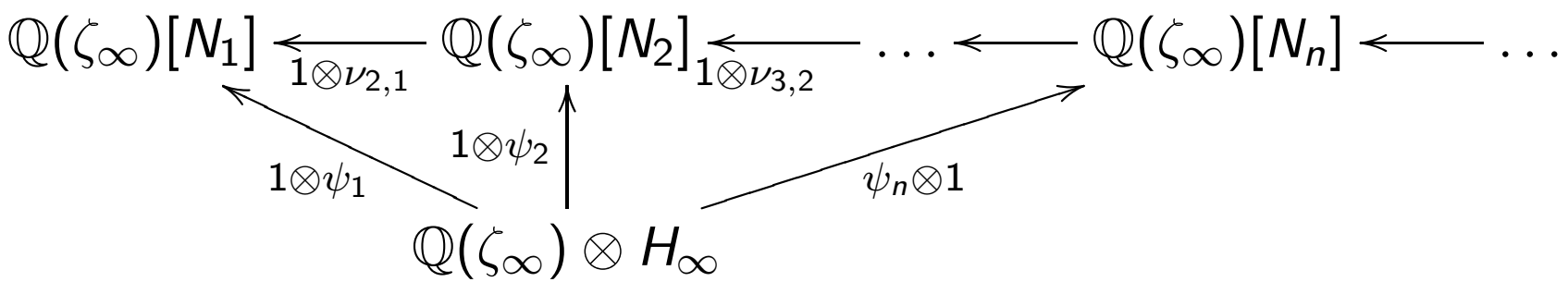


where the ψ_i are the canonical projections out of the direct limit.

If we base change the above up to $\mathbb{Q}(\zeta_\infty)$ then we have the following:



but since $\mathbb{Q}(\zeta_n) \otimes_{\mathbb{Q}} H_n \cong \mathbb{Q}(\zeta_n)[N_n]$ then we get



Direct limits can be interchanged with tensor products, but the same is not true generally for inverse limits, since tensor product does not usually commute with direct products.

However, we can 'build up' to $\mathbb{Q}(\zeta_\infty) \otimes H_\infty$ by first looking at $\mathbb{Q}(\zeta_m) \otimes \Pi_{n\geq 1} H_n$ where each $\mathbb{Q}(\zeta_m)$ is certainly finitely generated and projective as a $\mathbb{Q}$-module.

As such, by Webb [6, Prop. 1.1], the canonical map $\mathbb{Q}(\zeta_m) \otimes \Pi_{n\geq 1} H_n \to \Pi_{n\geq 1} \mathbb{Q}(\zeta_m) \otimes H_n$ is a bijection.

And as we saw earlier $\mathbb{Q}(\zeta_m) \otimes H_n$ contains $\mathbb{Q}(\zeta_m)[\langle \sigma_n^{p^{n-m}} \rangle]$.

Since tensor product *does* commute with direct limits, we have

$$\begin{aligned}\mathbb{Q}(\zeta_\infty) \otimes \Pi_{n\geq 1} H_n &\cong (\varinjlim_m \mathbb{Q}(\zeta_m)) \otimes \Pi_{n\geq 1} H_n \\ &\cong \varinjlim_m (\mathbb{Q}(\zeta_m) \otimes \Pi_{n\geq 1} H_n) \\ &\cong \varinjlim_m (\Pi_{n\geq 1} \mathbb{Q}(\zeta_m) \otimes H_n)\end{aligned}$$

where now, viewing the direct limit as union, each component in $\mathbb{Q}(\zeta_\infty) \otimes \Pi_{n\geq 1} H_n$ is exactly $\mathbb{Q}(\zeta_\infty)[N_n]$.

So, within this is the sub-algebra determined by the $\nu_{n,n-1}$, that is

$$\mathbb{Q}(\zeta_\infty) \otimes_{\mathbb{Q}} H_\infty = \mathbb{Q}(\zeta_\infty) \otimes_{\mathbb{Q}} (\varprojlim H_n) = \varprojlim (\mathbb{Q}(\zeta_\infty)[N_n]) = \mathbb{Q}(\zeta_\infty)[N_\infty]$$

which completes the proof of (a).

To show (b) we we shall use the following facts

$$\mathbb{Q}(\zeta_\infty)[N_\infty] \cong \{\{\gamma_j\} \in \Pi_{j=1}^{\infty}\mathbb{Q}(\zeta_\infty)[N_j] \mid \nu_{j,i}(\gamma_j) = \gamma_i)\}$$
$$H_\infty \cong \{\{\gamma_j\} \in \Pi_{j=1}^{\infty}H_j \mid \nu_{j,i}(\gamma_j) = \gamma_i)\}$$

Now if $\hat{\delta} = \{\delta_j^{e_j}\} \in \Delta_\infty$ and $\{\gamma_j\} \in \mathbb{Q}(\zeta_\infty)[N_\infty]$ then $\{\gamma_j\}^{\hat{\delta}} = \{\gamma_j\}$ implies that $\delta^{e_j}(\gamma_j) = \gamma_j$ for all j.

And we also have that $\gamma_j \in H_j$ for all $j \geq 1$ since Δ_∞ contains $\{\delta_j^{e_j}\}$ where $e_j = 1$ for any specified $j \geq 1$, so $\delta_j(\gamma_j) = \gamma_j$ for each $j \geq 1$ and therefore $\{\gamma_j\} \in \Pi_{j=1}^{\infty}H_j$.

But now, since $\{\gamma_j\} \in \mathbb{Q}(\zeta_\infty)[N_\infty]$ we have $\nu_{j,i}(\gamma_j) = \gamma_i$ so when restricted to $\gamma_j \in H_j$ we have $\{\gamma_j\} \in H_\infty$.

Thus $(\mathbb{Q}(\zeta_\infty)[N_\infty])^{\Delta_\infty} \subseteq H_\infty$.

The other inclusion is obvious since $H_\infty \subseteq \mathbb{Q}(\zeta_\infty)[N_\infty]$ and is fixed by *all* of $\Pi_{j=1}^{\infty}\Delta_j$, so therefore by Δ_∞.

One very interesting consequence of this is that since $\mathbb{Q}(\zeta_\infty) \otimes H_\infty$ is a group ring (and therefore a Hopf algebra) then by faithful flatness, so to is H_∞ itself and we have:

$$H_\infty \cong \varprojlim (\mathbb{Q}[N_n])^* \cong (\varinjlim \mathbb{Q}[N_n])^*$$

where $\varinjlim \mathbb{Q}[N_n] \cong \mathbb{Q}[\varinjlim N_n]$ is the group ring over the p-Prüfer group formed from the union of the $\{N_n\}$ since $N_n \cong C_{p^n}$.

This is a (rare?) example where the dual of an infinite dimensional Hopf algebra is also a Hopf algebra.

Aside from this descent theoretic proof of this fact, it is the author's conjecture that H_∞ is Hopf, even though it is the dual of an infinite group ring, since said infinite group is torsion.

$\mathbb{Q}(w_\infty)/\mathbb{Q}$ as an H_∞-Galois extension

The field $\mathbb{Q}(w_\infty)$ is certainly linearly disjoint to $\mathbb{Q}(\zeta_\infty)$ over $\mathbb{Q}$ and the normal closure of $\mathbb{Q}(w_\infty)$ is $\mathbb{Q}(\zeta_\infty)\mathbb{Q}(w_\infty)$. The question is, can we view $\mathbb{Q}(w_\infty)/\mathbb{Q}$ as a Hopf-Galois extension with respect to the action of H_∞?

Since $\mathbb{Q}(w_\infty)$ is the direct limit (union) over all $\mathbb{Q}(w^{p^n}) \subseteq \mathbb{Q}(w_\infty)$ then a given element lies in some particular $\mathbb{Q}(w_n)$ which is therefore acted on by H_n.

For each n we have that $\mathbb{Q}(w_n)\#H_n \cong End_{\mathbb{Q}}(\mathbb{Q}(w_n))$ and since $\mathbb{Q}(w_\infty) = \varinjlim \mathbb{Q}(w_n)$ then we wish to examine the relationships between $End_{\mathbb{Q}}(\mathbb{Q}(w_\infty))$ and $\mathbb{Q}(w_\infty)\#H_\infty$.

We begin by observing

$$\begin{aligned} End(\mathbb{Q}(w_\infty)) &= Hom(\varinjlim_n \mathbb{Q}(w_n), \varinjlim_m \mathbb{Q}(w_m)) \\ &\cong \varprojlim_n Hom(\mathbb{Q}(w_n), \varinjlim_m \mathbb{Q}(w_m)) \\ &\cong \varprojlim_n \left[\varinjlim_m Hom(\mathbb{Q}(w_n), \mathbb{Q}(w_m)) \right] \end{aligned}$$

where the direct limit (over n) in the first component becomes the inverse limit induced by the natural restriction map

$$Hom(\mathbb{Q}(w_n), \varinjlim_m \mathbb{Q}(w_m)) \longrightarrow Hom(\mathbb{Q}(w_{n-1}, \varinjlim_m \mathbb{Q}(w_m))$$

since $\mathbb{Q}(w_{n-1}) \subseteq \mathbb{Q}(w_n)$. The direct limit (over m) can be moved outside since $\mathbb{Q}(w_n)$ is finitely presented for each n.

The following technical fact is essential

Proposition

The algebra $Hom(\mathbb{Q}(w_n), \mathbb{Q}(w_m))$ *is isomorphic to*

(a) $\mathbb{Q}(w_m)\#\overline{H}_{m,n}$ *where* $\overline{H}_{m,n}$ *is the sub-algebra of* H_m *spanned by* $\{e_{m,i}\}$ *for* $i \in p^{m-n}\mathbb{Z}_{p^n} \subseteq \mathbb{Z}_{p^m}$ *if* $m \geq n$ *or*

(b) the sub-algebra of $\mathbb{Q}(w_n)\#H_n$ *spanned by* $\{w_n^j\#e_{n,i}\}$ *where* $i \in \mathbb{Z}_{p^n}$ *where* $p^{n-m}\big|(j+i)$ *if* $m < n$.

If one now considers the direct limit

$$\varinjlim_{m} Hom(\mathbb{Q}(w_n), \mathbb{Q}(w_m))$$

for a given n, then one is looking at homomorphisms into $\mathbb{Q}(w_m)$ given by the sub-algbebra of $\mathbb{Q}(w_n)\#H_n$ when $m < n$, or by the sub-algebra $\mathbb{Q}(w_m)\#\overline{H}_{m,n}$ where $\mathbb{Q}(w_n) \subseteq \mathbb{Q}(w_m)$ when $m \geq n$.

If for notational uniformity we define $\overline{H}_{m,n} = H_n$ when $m < n$ then we wish to first consider the direct limit $\varinjlim_{m} \overline{H}_{m,n}$.

Although we study the action on $\mathbb{Q}(w_\infty)$ by H_∞, which is the *inverse* limit of the H_m, there is a natural embedding of H_m into H_{m+1} via $e_{m,i} \mapsto e_{m+1,pi}$.

As such, for $m \geq n$ this restricts to an embedding $\overline{H}_{m,n} \hookrightarrow \overline{H}_{m+1,n}$ for each n. However, this embedding is, in fact, an isomorphism since $dim(\overline{H}_{m,n}) = p^n$ for each m!

Moreover, for each $m < n$, $\overline{H}_{m,n} = H_n$ so that, in fact:

$$\varinjlim_m \overline{H}_{m,n} \cong H_n$$

and since the union of the scalars $\mathbb{Q}(w_m)$ is $\mathbb{Q}(w_\infty)$ we have proved:

$$\varinjlim_m Hom(\mathbb{Q}(w_n), \mathbb{Q}(w_m)) \cong \mathbb{Q}(w_\infty)\#H_n$$

This leads us to the main result for this section.

Theorem

$$End_{\mathbb{Q}}(\mathbb{Q}(w_\infty)) \cong \mathbb{Q}(w_\infty)\#H_\infty$$

The principal observation needed is that the inverse limit

$$\varprojlim_n Hom(\mathbb{Q}(w_n), \mathbb{Q}(w_\infty))$$
$$\cong \varprojlim_n \mathbb{Q}(w_\infty)\#H_n$$

arises from the natural restriction maps, but these are exactly the $\nu_{n,n-1}$, which act as the identity on $\mathbb{Q}(w_\infty)$, that is:

$$\varprojlim_n \mathbb{Q}(w_\infty)\#\overline{H}_n \cong \mathbb{Q}(w_\infty)\#H_\infty$$

so that the endomorphism ring of $\mathbb{Q}(w_\infty)$ is the latter smash product, making $\mathbb{Q}(w_\infty)/\mathbb{Q}$ a Hopf-Galois extension with respect to the action of H_∞.

Can the action of H_∞ be viewed within the Greither-Pareigis theory?

We have that H_∞ is a $\mathbb{Q}(\zeta_\infty)$-form (and therefore a $\mathbb{Q}(w_\infty, \zeta_\infty)$-form) of the group ring $\mathbb{Q}[N_\infty]$. In terms of normal complements involving the Galois groups of the relevant intermediate extensions, namely

$$\begin{aligned} N_\infty &= Gal(\mathbb{Q}(w_\infty, \zeta_\infty)/\mathbb{Q}(\zeta_\infty)) \\ \Delta_\infty &= Gal(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \\ N_\infty \Delta_\infty &= Gal(\mathbb{Q}(w_\infty)\mathbb{Q}(\zeta_\infty)/\mathbb{Q} \end{aligned}$$

the extension $\mathbb{Q}(w_\infty)/\mathbb{Q}$ is almost classical. (i.e. 'N' is N_∞)

The delicate part is if N_∞ can be viewed as a regular subgroup, and moreover, of what ambient symmetric group?

The construction of H_∞ parallels that of a profinite Galois group acting on a direct limit (union) of field extensions, where the restriction to a given sub-field in the chain corresponds to the action of the Galois group acting on that field extension.

Here, H_∞ acts by restriction on $\mathbb{Q}(w_n)$ as H_n where, by Greither-Pareigis, there is a corresponding regular subgroup of $N_n \leq Perm(\Gamma_n/\Delta_n)$. Observe however that, as seen earlier, $\Gamma_n = N_n\Delta_n$ so that $\Gamma_n/\Delta_n = \{\sigma_n^i\Delta_n\}$ and where N_n acts naturally on the left, just as it would act on itself via the left regular representation.

(i.e. identify $Perm(\Gamma_n/\Delta_n) \cong Perm(N_n)$).

In the limit, the analogue would be N_∞ a regular subgroup of $\varinjlim_n Perm(N_\infty \Delta_\infty / \Delta_\infty) \cong \varinjlim_n Perm(N_\infty)$, via the left action, given that the left regular representation is the canonical example of a regular permutation group.

As such, in any related construction of an inverse limit of Hopf algebras acting on intermediate extensions, we should expect the restriction to any intermediate extension to also give rise to a regular subgroup embedded in the corresponding ambient symmetric group.
The resulting Hopf algebra is a form of a group ring over a profinite group, similarly embedded in the corresponding infinite ambient symmetric group.

i.e. We would likely need to replace $Perm(N_\infty)$ (which is uncountable!) with $\varinjlim_n Perm(N_n)$.

Thank you!

Appendix 1 - Other Radical Extensions

The pure radical extensions $\mathbb{Q}(w_n)/\mathbb{Q}$ had the property of being 'almost classical' in that the N which gives rise to the Hopf-Galois structure is contained in the Galois group of the normal closure over the base.

If one starts adding in p-power roots of unity then more Hopf-Galois structures arise:

Theorem

[5, Theorem 3.3 and Theorem 4.5] The radical extension $\mathbb{Q}(w_n, \zeta_r)/\mathbb{Q}(\zeta_r)$ has exactly p^r Hopf-Galois structures for $0 \leq r < n$ and p^{n-1} for $r = n$, of which $p^{min(r,n-r)}$ are almost classical and for all, the associated group N is cyclic of order p^n.

For example, $\mathbb{Q}(\zeta_1, w_n)/\mathbb{Q}(\zeta_1)$ has p Hopf-Galois structures, all $p^{min(1,n-1)} = p^1 = p$ of which are almost classical.

Moreover, the N's which arise are all cyclic of order p^n.

For the case of $\mathbb{Q}(\zeta_1, w_n)/\mathbb{Q}(\zeta_1)$ we have

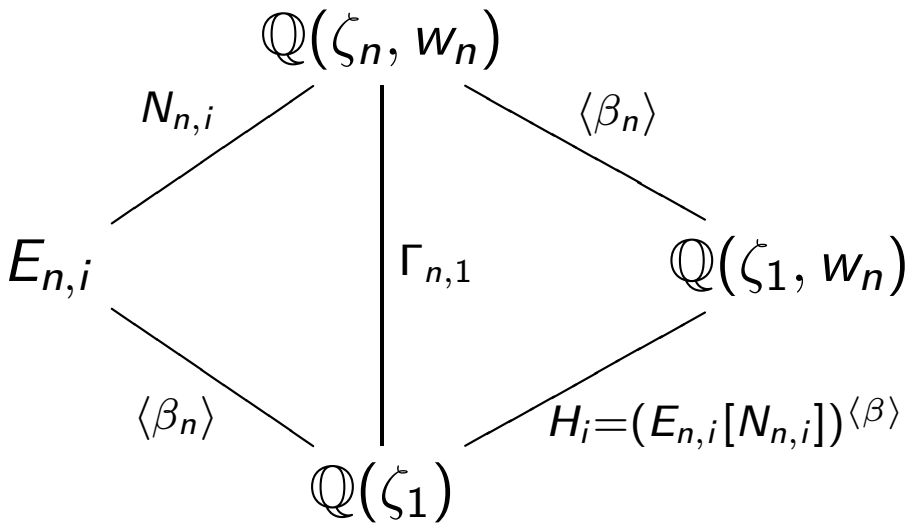
$$\Gamma_{n,1} = Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_1)) = \langle \sigma_n, \beta_n \rangle$$

where $\langle \sigma_n \rangle = Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_n))$ which we shall denote by $N_{n,0}$, which is cyclic of order p^n, of course, and $\langle \beta_n \rangle = Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_1, w_n))$, which is cyclic of order p^{n-1}

We note that $\Gamma_{n,1}$ is the Sylow p-subgroup of $Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q})$ since $\langle \beta_n \rangle$ is the Sylow p-subgroup of $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

One can show that $N_{n,0}$ and $N_{n,i} = \langle \sigma^i \beta^{p^{n-2}} \rangle$ for $i \in U_p$ are the p different normal complements to $\langle \beta_n \rangle$ in $\Gamma_{n,1}$, all of which are cyclic of order p^n of course.

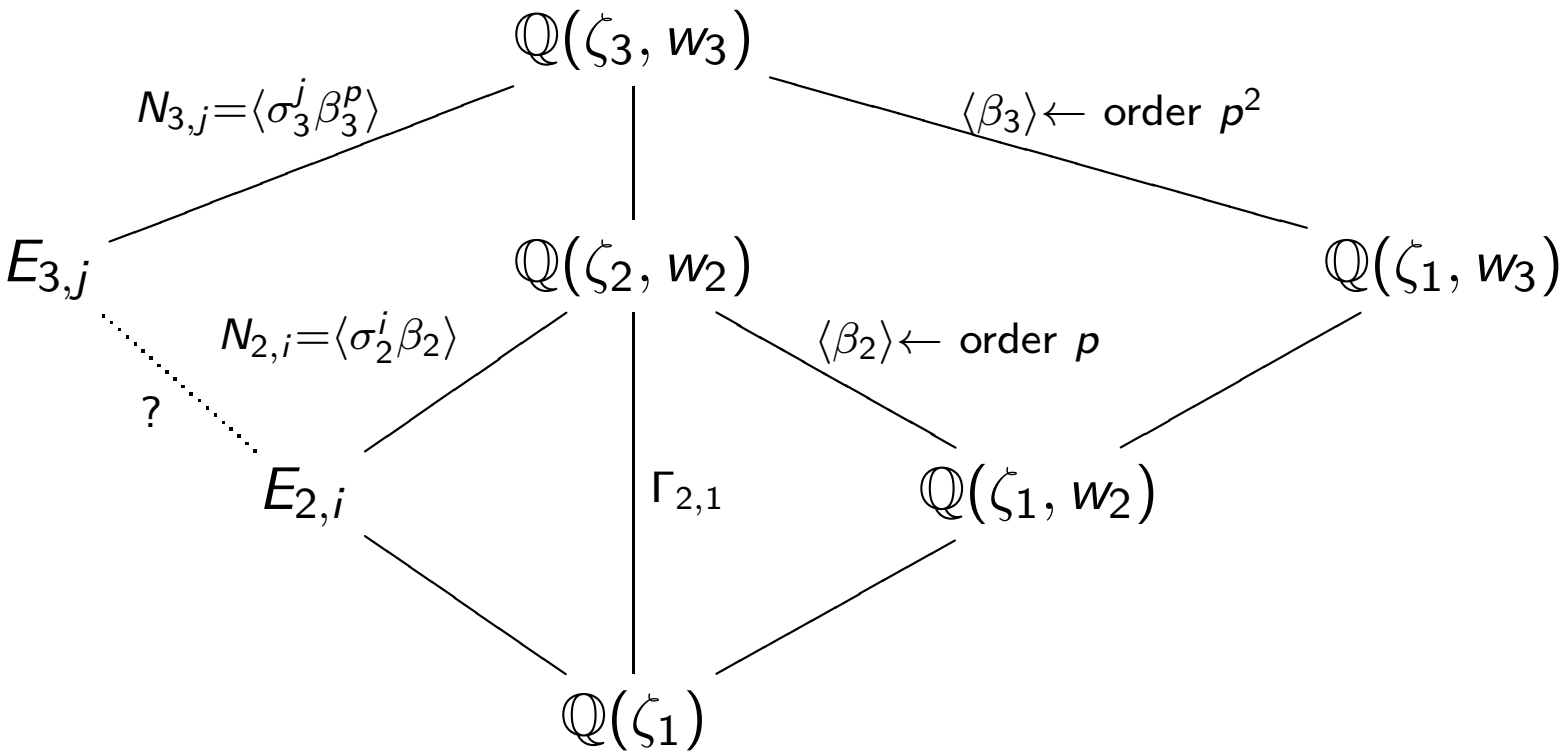
If we denote by $E_{n,i} = (\mathbb{Q}(\zeta_n, w_n))^{N_i}$ then $\mathbb{Q}(\zeta_1, w_n)/\mathbb{Q}(\zeta_1)$ is Hopf-Galois with respect to the action of $H_{n,i} = (E_i[N_{n,i}])^{\langle \beta_n \rangle}$



To see the relationship between the $N_{n,i}$ for different n, consider first the relationship between the $n = 2$ and $n = 3$ cases.

Observe that $N_{0,2} \subseteq N_{0,3}$ where, concordantly
$E_{2,0} = \mathbb{Q}(\zeta_2) = (\mathbb{Q}(\zeta_2, w_2))^{N_{2,0}} \subseteq (\mathbb{Q}(\zeta_3, w_3))^{N_{3,0}} = \mathbb{Q}(\zeta_3) = E_{3,0}$.

For the other $N_{2,i}$ and $N_{3,j}$ we have the following.



So the question is, when is $E_{2,i} \subseteq E_{3,j}$?

Proposition

For $Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_1)) = \langle \sigma_n, \beta_n \rangle$ *then for* $i \in \{0, \ldots, p-1\}$ *there is containment* $E_{n-1,i} \subseteq E_{n,i}$ *where* $E_{n,i}$ *is the fixed field of* $N_{n,i}$. *Moreover* $\{N_{n,i}, \nu_{n,n-1}\}$ *(for* $n \geq 3$*) forms an inverse system where for* $i = 0$ $\nu_{n,n-1}(\sigma_n) = \sigma_{n-1}$, *and for* $i \in U_p$ *that* $\nu_{n,n-1}(\sigma_n^i \beta_n^{p^{n-2}}) = \sigma_{n-1}^i \beta_{n-1}^{p^{n-3}}$.

For each n, $\langle \beta_n \rangle$ normalizes $N_{n,i}$ so that $N_{n,i}$ is a normal complement to $\langle \beta_n \rangle$ in $Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_1))$.

Also, since each $N_{n,i}$ is Abelian then $\mathbb{Q}(w_n)/\mathbb{Q}(\zeta_1)$ is Hopf-Galois with respect to the action of $H_{n,i} = (E_{n,i}[N_{n,i}])^{\langle \beta_n \rangle}$ where each is a $E_{n,i}$-form of the group ring $\mathbb{Q}(\zeta_1)[N_{n,i}]$.

If we define $\overline{\Delta}_n = \langle \beta_n \rangle$ then we may form the inverse limit $\overline{\Delta}_\infty$ of the system $\{\overline{\Delta}_n, \phi_{n,n-1}\}$ in the same fashion as we used to define Δ_∞.

Similarly, we may define $N_{\infty,i} = \underset{\longleftarrow}{lim} N_{n,i}$ and $E_{\infty,i} = \underset{\longrightarrow}{lim} E_{n,i}$, and $H_{\infty,i} = \underset{\longleftarrow}{\lim} H_{n,i}$.

In a manner identical to that developed earlier, we have therefore that $\mathbb{Q}(w_\infty, \zeta_1)/\mathbb{Q}(\zeta_1)$ is a Hopf-Galois extension with respect to the action of $H_{\infty,i}$, where $H_{\infty,i} \cong (E_{\infty,i}[N_{\infty,i}])^{\overline{\Delta}_\infty}$ and $E_{\infty,i} \otimes H_{\infty,i} \cong E_{\infty,i}[N_{\infty,i}]$.

This shows that the non-uniqueness of the Hopf-Galois structures which may act on a given extension holds for infinite extensions such as these.

Appendix 2 - Computational Sideline

We can associate/view the actions of $e_{n,i}$ and w_n^j within $End_{\mathbb{Q}}(\mathbb{Q}(w_n))$ as matrices and the $w_n^j \# e_{n,i}$ as products of these matrices. Consider the case $p = 3$ and $n = 1$.

With $\{1, w, w^2\}$ the basis for $\mathbb{Q}(w)$, view w^i as left multiplication l_{w^i} for $i = 0, 1, 2$ which act to cyclically rotate the basis vectors $\{1, w, w^2\}$.

Each e_i can be also be represented as a 3×3 matrix which is zero except for the $i + 1^{st}$ column which consists of the $i + 1^{st}$ elementary basis vector for $V = \mathbb{Q}^3$.

We're identifying $End_{\mathbb{Q}}(\mathbb{Q}(w)) \cong End_{\mathbb{Q}}(V) \cong M_3(\mathbb{Q})$ and we get the following 6 matrices:

$$l_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad e_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$l_w = \begin{bmatrix} 0 & 0 & a \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \qquad e_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$l_{w^2} = \begin{bmatrix} 0 & a & 0 \\ 0 & 0 & a \\ 1 & 0 & 0 \end{bmatrix} \qquad e_2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

which when multiplied in pairs $\{l_{w^j} e_i\}$ yield nine matrices

$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \right.$$
$$\begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},$$
$$\left. \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & a & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & a \\ 0 & 0 & 0 \end{bmatrix}, \right\}$$

corresponding to the $\{w_n^j \# e_i\}$.

Note also that this set is clearly a basis for the endomorphism ring since $\sum_{j,i} c_{j,i} l_{w^j} e_i$ equals

$$\begin{bmatrix} c_{0,0} & c_{2,1}a & c_{1,2}a \\ c_{1,0} & c_{0,1} & c_{2,2}a \\ c_{2,0} & c_{1,1} & c_{0,2} \end{bmatrix}$$

which, given that $a \in \mathbb{Q}$, gives every 3×3 matrix over $\mathbb{Q}$ for unique choices of $\{c_{j,i}\}$.

One sees the same motif for larger p and n, namely a $p^n \times p^n$ matrix where every entry above the main diagonal is multiplied by a.

S.U. Chase and M. Sweedler.
Hopf Algebras and Galois Theory.
Number 97 in Lecture Notes in Mathematics. Springer Verlag, Berlin, 1969.
10

L. Fuchs.
Abelian Groups.
Springer Monographs in Mathematics. Springer, 2015.
26

C. Greither and B. Pareigis.
Hopf galois theory for separable field extensions.
J. Algebra, 106:239–258, 1987.
6, 10

R. Haggenmüller and B. Pareigis.
Hopf algebra forms of the multiplicative group and other groups.
Manuscripta Math., 55:121–136, 1986.
16, 19


T. Kohl.
Classification of the hopf galois structures on prime power radical extensions.
J. Algebra, 207:525–546, 1998.
8, 10, 47


C. Webb.
Tensor and direct products.
Pacific Journal of Mathematics, 49:579–594, 1973.
32