Hopf-Galois Theory for Fields

Objective: To generalize the notion of Galois extension by replacing the action of a group by a larger object, a Hopf algebra.

Background:
Let R be a commutative ring with unity.

An $R-Hopf\ algebra$ is an R-algebra H together with maps:

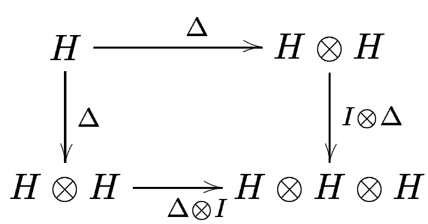
$$\Delta : H \to H \otimes_R H \text{ comultiplication}$$

$$\epsilon : H \to R \text{ counit}$$

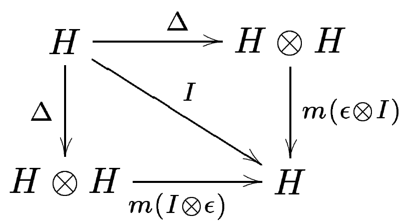
$$\lambda : H \to H \text{ antipode}$$

• Δ and ϵ are R-algebra maps
• λ is an R anti-homomorphism (ie. $\lambda(hh') = \lambda(h')\lambda(h)$)
such that the following diagrams commute

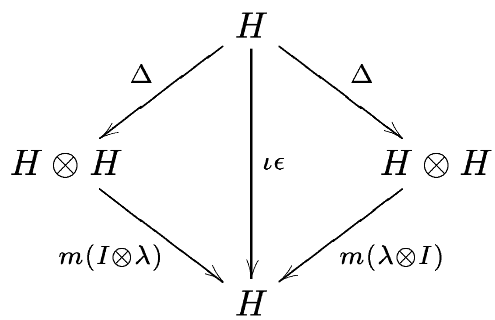
(1) Co-associativity



(2) Co-unitary property



(3) Antipode property



where

I (identity map on H)

$m : H \otimes H \longrightarrow H$ (multiplication on H)

$\iota : R \to H$ (R-algebra structure map for H)

Examples

The prototypical examples of Hopf algebras are group rings.

- G a (finite) group
- $H = RG$ is a Hopf algebra via the following definitions of Δ, ϵ and λ:

$$\Delta(g) = g \otimes g$$
$$\epsilon(g) = 1_R$$
$$\lambda(g) = g^{-1}$$

where $g \in G$ and extend by linearity to all of RG.

With this definition, properties (1)-(3) are easily verified.

e.g.

$$\begin{aligned} m(I \otimes \epsilon)\Delta(g) &= m(I \otimes \epsilon)(g \otimes g) \\ &= m(g \otimes 1) \\ &= g \end{aligned}$$

We say H is **cocommutative** if $\tau \circ \Delta = \Delta$ where τ is the 'switch' map, $\tau(x \otimes y) = y \otimes x$

So group rings are obviously cocommutative.

For general Hopf algebras, the comultiplication is given in 'Sweedler notation'

That is, if $h \in H$ then

$$\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$$

and can be extended to iterates of Δ unambigously by coassociativity.

eg.

$$\Delta_{(2)}(h) = (I \otimes \Delta)\Delta(h) = (\Delta \otimes I)\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)} \otimes h_{(3)}$$

- If H is a finitely generated, projective R-Hopf algebra then H^* is also via:

$$\Delta^*(f)(h \otimes k) = f(hk) \text{ for } f \in H^* \text{ and } h, k \in H$$
$$\epsilon^*(f) = f(1)$$
$$\lambda^*(f)(h) = f(\lambda(h))$$

Note(s):

- If H is f.g. proj. then $H \cong H^{**}$ as Hopf algebras
- H is comm (resp. cocomm) iff H^* is cocomm (resp. comm)

Alternate view

One which makes the definitions of Δ, ϵ and λ more 'natural' is follows.

G representable functor from $\mathbf{R-alg_c}$ to $\mathbf{Grp}$

That is,

$G(A) = Hom_{R-alg}(H, A)$ for some comm. R-alg. H for all comm. R-algebras A.

- representing algebra H is a Hopf algebra by virtue of the group structure on $G(A)$

I.E.

mult. on $G(A) \leftrightarrow$ comultiplcation on H

associativity $\leftrightarrow$ **co**associativity of Δ

inverse on $G(A) \leftrightarrow$ antipode on H

inverse for all group elements $\leftrightarrow$ antipode property

Example: the 'circle' functor

$$\mathcal{C} : \mathbf{R-alg_c} \to \mathbf{Grp}$$

$$C(A) = \{(a,b) \in R \times R | a^2 + b^2 = 1\}$$

group structure

$$(a,b)(c,d) = (ac - bd, ad + bc)$$

$$(a,b)^{-1} = (a, -b)$$

$$\text{identity} \to (1,0)$$

This is representable, that is $C(A) = Hom_{R-alg_c}(H, A)$ for

$$H = R[c,s]/(c^2 + s^2 - 1)$$

which is a Hopf algebra via the following definitions for Δ, ϵ and λ

$$\begin{array}{lll} \Delta(c) = c \otimes c - s \otimes s & \epsilon(c) = 1 & \lambda(c) = c \\ \Delta(s) = c \otimes s + s \otimes c & \epsilon(s) = 0 & \lambda(s) = -s \end{array}$$

This is called the **trigonometric algebra** due to the way the comultiplication resembles the formulæ:

$$cos(x+y) = cos(x)cos(y) - sin(x)sin(y)$$
$$sin(x+y) = cos(s)sin(y) + sin(x)cos(y)$$

Hopf Galois Extensions

- A a commutative R-algebra, finitely generated and projective as an R-module
- H a cocommutative $R-$Hopf algebra

Definition: A is an *H-module algebra* if there exists $\mu : H \to End_R(A)$, an $R-$algebra homomorphism such that for $h \in H$ and $x, y \in A$:

(i)
$$\mu(h)(xy) = \sum_{(h)} \mu(h_{(1)})(x)\mu(h_{(2)})(y)$$
$$\text{where } \Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$$

(ii)
$$\mu(h)(1) = \epsilon(h)1$$

We refer to condition (i) by saying that H *measures* A to A.

Condition (ii) is simply the statement that

$$R \subseteq A^H \text{ where}$$
$$A^H = \{x \in A | \mu(h)(x) = \epsilon(h)x \ \forall h \in H\}$$

which is the *fixed subalgebra* of A under the action of H.

A/R is an *H-Galois extension* if A is an H-module algebra such that

(1) $R = A^H$

(2) $A \otimes H \cong End_R(A)$ via $a \otimes h \mapsto (b \mapsto a\mu(h)(b))$

Equivalent to $\mu : H \to End_R(A)$ are maps

$$\mu' : H \otimes A \to A$$

an R-module map defining what's called an H-**co**module structure on A and

$$\mu'' : A \to A \otimes H^*$$

an R-algebra map making A into an $\mathbf{H^*}$ **object**

With this, the following are equivalent:

(1) A/R is $H - Galois$
(2) μ' yields an isomorphism $\mu' \otimes 1 : H \otimes A \to End_R(A)$
(3) μ'' yields an isomorphism $A \otimes A \to A \otimes H^*$

Note: We can view (3) in the following context:
Notation: $Spec(A) = Hom_{R-alg}(A, -)$ and $Spec(H^*) = Hom_{R-alg}(H^*, -)$

The map $\mu'' : A \to A \otimes H^*$ can be dualized into a map

$$Spec(H^*) \times Spec(A) \to Spec(A)$$

making $Spec(A)$ into a $Spec(H^*)$-set for the group scheme $Spec(H^*)$.

Recall H co-commutative implies H^* is commutative so this makes sense.

If $A \otimes A \cong A \otimes H^*$ then we call A a **Galois H^*-object** and at the level of schemes this translates into a bijection

$$Spec(H^*) \times Spec(A) \to Spec(A) \times Spec(A)$$

making $Spec(A)$ a principal homogeneous space under the action of $Spec(H^*)$.

i.e. The map $(g, x) \mapsto (gx, x)$ for $g \in Spec(H^*)$ and $x \in Spec(A)$ is bijective.

For those extensions which are H-Galois there is a Galois type correspondance between R-sub-Hopf algebras of H and subalgebras of A containing R.

Theorem [Chase, Sweedler Theorem 7.6]. *If we define for an R-sub-Hopf algebra W of H,*

$$Fix(W) = \{x \in A | \mu(w)(x) = \epsilon(w)x \ \forall w \in W\} = A^W$$

then the map

$$\{W \subseteq H \ sub-Hopf \ algebra\} \xrightarrow{Fix} \{E | R \subseteq E \subseteq A, \ E \ an \ R-subalgebra\}$$

is <u>injective</u> and inclusion reversing.

The case when Fix is also *surjective* is of importance and will be discussed.

Examples

- L/K Galois extension of fields with $G = Gal(L/K)$
- then L/K is also Hopf Galois with Hopf algebra $H = KG$.
- $\mu : H \to End_K(L)$ given as expected:

$$\begin{aligned} h &= \sum a_i g_i \in H,\ x, y \in L \\ \mu(h)(x) &= \sum a_i g_i(x) \\ \mu(h)(xy) &= \sum a_i g_i(xy) = \sum a_i g_i(x) g_i(y) = \sum_{(h)} \mu(h_1)(x)\mu(h_2)(y) \end{aligned}$$

which comes from $\Delta(h) = \sum a_i(g_i \otimes g_i)$
as well as

$$\begin{aligned} \mu(h)(1) &= \sum a_i g_i(1) \\ &= \sum a_i 1 \\ &= \epsilon(h)1 \end{aligned}$$

Since the elements of G are a K-basis for $End_K(L)$ then $L \otimes H \cong End_K(L)$

Hence, any extension which is Galois (in the usual sense) is Hopf Galois as well.

But what about field extensions which are not Galois in the usual sense?

Example

- $w = \sqrt[3]{2}$

- $\mathbb{Q}(w)$ - a separable but non-normal extension of $\mathbb{Q}$

- It is Hopf Galois for the $\mathbb{Q}$-Hopf algebra H exhibited below.

$N = \langle \sigma \rangle$ cyclic of order 3
ζ a primitive cube root of unity
Consider the group ring $\mathbb{Q}(\zeta, w)N$.

Define $\alpha_1 = \sigma + \sigma^2$ and $\alpha_2 = \zeta^2\sigma + \zeta\sigma^2$ and let $H = \mathbb{Q}[\alpha_1, \alpha_2]$

If we (for the moment) stipulate that

$$\begin{aligned} \sigma(w) &= \zeta w \\ \sigma^2(w) &= \zeta^2 w \\ \sigma(1) &= 1 \end{aligned}$$

the action of H on $\mathbb{Q}(w)$ is then:

$$\begin{aligned} \alpha_1(w) &= \zeta w + \zeta^2 w \\ &= (\zeta + \zeta^2) w \\ &= -w \end{aligned} \qquad \text{and} \qquad \begin{aligned} \alpha_2(w) &= \zeta^2(\zeta w) + \zeta(\zeta^2 w) \\ &= w + w \\ &= 2w \end{aligned}$$

Note also that $\alpha_1(1) = 2$ and $\alpha_2(1) = 2$.

If we treat $\mathbb{Q}(\zeta, w)N$ as a $\mathbb{Q}(\zeta, w)$-Hopf algebra then we can let the Hopf algebra structure on H be induced from that on $\mathbb{Q}(\zeta, w)N$, to wit:

$$\begin{aligned} \Delta(\sigma + \sigma^2) &= (\sigma \otimes \sigma + \sigma^2 \otimes \sigma^2) \\ \epsilon(\sigma + \sigma^2) &= 2 \\ \lambda(\sigma + \sigma^2) &= \sigma^2 + \sigma \end{aligned}$$

Here, H measures $\mathbb{Q}(w)$ to itself, for example

$$\begin{aligned}\alpha_1(w \cdot w) &= m(\sigma \otimes \sigma + \sigma^2 \otimes \sigma^2)(w \otimes w) \\ &= m(\zeta w \otimes \zeta w + \zeta^2 w \otimes \zeta^2 w) \\ &= \zeta^2 w^2 + \zeta w^2 \\ &= -w^2\end{aligned}$$

Note: The action of H seems to be connected to the (ordinary Galois) extensions $\mathbb{Q}(\zeta, w)/\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\zeta, w)/\mathbb{Q}$

Let's explore this a bit....

Behind the scenes in the above example (and in the theory as a whole) is some sort of faithfully flat descent.

Definition:

k a field

A a k-object of some sort (k-algebra, k-Hopf algebra etc.)

L an extension field of k.

Another such k-object B is called an <u>L-form</u> of A if $L \otimes B \cong L \otimes A$ as the corresponding L-objects.

Setup

L/k be a Galois extension with $\Gamma = Gal(L/k)$

S be a finite set

$L^S = Map(S, L)$ the L-algebra of set maps from S to L

generated by $\{u_s | s \in S\}$ where $u_s(t) = \delta_{s,t}$ and $u_s u_t = \delta_{s,t} u_s$.

A group N acts on L^S (by L-automorphisms) via permutations on S

This action is Galois (ala Galois theory of rings) or Hopf Galois (via the action of $H = LN$) iff N is a *regular* subgroup of $B = Perm(S)$.

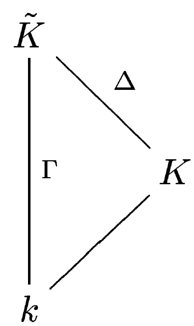
That is, N acts transitively and all point stabilizers are trivial.

Greither-Pareigis Theory

Greither and Pareigis give a characterization of Hopf Galois structures on separable field extensions which we outline here.

If K/k is a separable (but not necessarily normal) field extension where

- $\Gamma = Gal(\tilde{K}/k)$ and $\Delta = Gal(\tilde{K}/K)$ as diagrammed below:



Let

- $S = \Gamma/\Delta$ the set of left cosets of Δ in Γ
- $B = Perm(S)$ (observe $|S| = [K : k]$)

There is then an *embedding* $\Gamma \subseteq B$ where Γ acts on S by left translation.

Fact (1) There is a Γ equivariant, $\tilde{K}$-isomorphism, $\tilde{K} \otimes K \cong \tilde{K}^S$

Fact (2) If K/k is Hopf Galois for some k-Hopf algebra H then there is a unique regular subgroup $N \leq B = Perm(S)$ (arising due to H) for which $\tilde{K} \otimes H \cong \tilde{K}N$ (ie H is a $\tilde{K}$-form of kN)

For (2) the idea is this, if $\tilde{K}/k$ is H-Galois, this corresponds to a map

$$H \otimes_k K \to K$$

If we base change up to $\tilde{K}$ we get a map

$$(\tilde{K} \otimes_k H) \otimes_{\tilde{K}} (\tilde{K} \otimes_k K) \to (\tilde{K} \otimes_k K)$$

and by (1), $\tilde{K} \otimes K \cong \tilde{K}^S$ and so this is actually

$$(\tilde{K} \otimes H) \otimes \tilde{K}^S \to \tilde{K}^S$$

By faithful flatness, H is k-Hopf algebra iff $\tilde{K} \otimes H$ is a $\tilde{K}$-Hopf algbera.

Moreover, $\tilde{K} \otimes H$ is in fact $\tilde{K}N$ for some group N which acts regularly on S.

Why?

By Hopf Galois-ness, $K \otimes K \cong K \otimes H^*$ and so $\tilde{K}^S \cong \tilde{K} \otimes K \cong \tilde{K} \otimes H^*$ and so $\tilde{K} \otimes H^*$ has $\tilde{K}^S$ as its underlying algebra.

A Hopf algebra structure on $\tilde{K}^S$ *must* come from a group structure on S so $S = N$ and as such N must be regular.

Why?

$\Delta : \tilde{K}^S \to \tilde{K}^S \otimes \tilde{K}^S \cong \tilde{K}^{S \times S}$ corresponds to a map $m : S \times S \to S$ which is associative since Δ is co-associative, etc.

If N is a group then $(\tilde{K}^N)^*$ is $\tilde{K}N$.

As such the base changed action is actually:

$$\tilde{K}N \otimes \tilde{K}^S \to \tilde{K}^S$$

Given this, we have the following:

Theorem [Greither Pareigis 1987]. *Let $N \subseteq B$ be a subgroup. The following are equivalent:*

(a) There is a k-Hopf algebra H and an H-Galois structure on K/k which induces $N \subseteq B$ where H is a $\tilde{K}$-form of kN

(b) N is regular on $S = \Gamma/\Delta$ and the subgroup $\Gamma \subseteq B$ normalizes N.

Observations:

• This theorem allows us to enumerate and classify H-Galois structures by determining the regular subgroups N of $B = Perm(S)$ that are normalized by $\Gamma \subseteq B$.

• Unlike what occurs in ordinary Galois theory, a given extension can have several inequivalent Hopf Galois structures on it, where two H-Galois structures on K/k, corresponding to regular subgroups N and $N^{'}$ in B, are equivalent if there is a Γ isomorphism between them.

• In fact, one can have two Hopf algebras H and $H^{'}$ acting on K/k where H corresponds to N and $H^{'}$ to $N^{'}$ which give inequivalent Hopf Galois structures, even though N and $N^{'}$ may be isomorphic as abstract groups!

Almost Classical Extensions

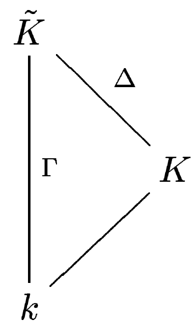
It is not necessary that a regular subgroup $N \subseteq B$ that is normalized by Γ be *contained* in Γ.

When $N \subseteq \Gamma$ the associated Hopf Galois structure on K/k satisfies a stronger version of the main theorem of Hopf Galois extensions.

Theorem - [Greither Pareigis 1987]. *If K/k is almost classically Galois, then there is a Hopf algebra H such that K/k is H-Galois and the main theorem holds in its strong form.*

That is, the map Fix is not only injective but is *surjective* as well.

Recall the setup,



where $S = \Gamma/\Delta$ and $B = Perm(S)$

In the almost classical case, a regular subgroup is N_*^{opp} where

N_* is a normal complement Δ in Γ
(equivalently $N = Gal(\tilde{K}/E)$ where $\tilde{K} = E \cdot K = E \otimes K$)

N_*^{opp} is the opposite subgroup to $N \leq B$

N_* is regular by virtue of being a normal complement to Δ

N_*^{opp} is regular iff N_* is regular.

In this case the Hopf algebra H is $(\tilde{K}N_*^{opp})^\Gamma$.

Observations

- Almost classical extensions very close to ordinary Galois extensions in terms of the one to one correspondence b/w sub Hopf-algebras and subfields of K.

- There is still the feature of the multiplicity of Hopf Galois structures that can be imposed on an extension

- For certain extensions, the only structures that arise *are* the almost classical ones.

- If L/K is Galois in the usual sense (with group G / Hopf algebra KG) one can sometimes find *additional* Hopf algebras which make L/K a Hopf Galois extension!.

The way that this theory is used is by rephrasing the condition

$$\Gamma \leq B \text{ normalizes } N \leq B$$

It is, of course, equivalent to $\Gamma \leq Norm_B(N)$ but we can be go further.

Any two of the following implies the third:

(1) $|N| = |S|$

(2) N acts transitively

(3) N acts fixed point freely

So if N acts regularly on S then it acts regularly on itself as well.

Hence we can identify

$$B = Perm(S) = Perm(N)$$

where N is embedded as $\lambda(N)$, the left regular representation of N.

So $Norm_B(N) = Norm_B(\lambda(N))$ which is an object known classically as $Hol(N)$ the holomorph of N.

Fact: $Aut(N)$ is (as a subgroup of $Hol(N)$) the set of all permutations in B which fix the identity of N and so there is a canonical isomorphism

$$Hol(N) \cong N \rtimes Aut(N)$$

So we handle the enumeration by looking at when (and if) the condition

$$\Gamma \leq Hol(N)$$

holds for *abstract* groups Γ and N.

Again, several N's can give distinct actions but be isomorphic as abstract groups.

For example,

[K] 1998

- p an odd prime and n a positive integer

- k a field of characteristic zero

- $K = k(w)$ with $w^{p^n} = a \in k$ where a is such that $[K : k] = p^n$

- $r =$ the largest integer between 0 and n such that $K \cap k(\zeta_{p^r}) = k(\zeta_{p^r})$ where ζ_{p^r} denotes a primitive $p^r th$ root of unity

- K/k is separable, but not always normal

- It is H-Galois with H a $\tilde{K}$-Hopf algebra form of group ring(s) kN where $\tilde{K}$ is the normal closure of K/k.

- If $r < n$ then there are p^r Hopf Galois structures on K/k for which the associated group N is cyclic of order p^n.

- Of these, $p^{min(r,n-r)}$ are almost classical and the rest are non almost classical.

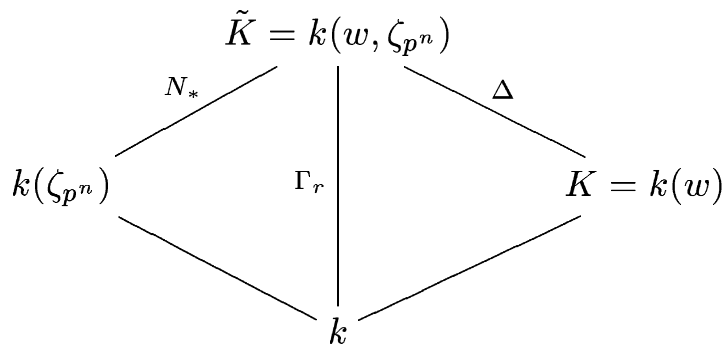
- When $r = n$, there are p^{n-1} H-Galois structures for which $N \cong C_{p^n}$ of which only one is almost classical.

- In fact, these are the only structures possible.

- For this class of extensions, N *must* be cyclic.

Rough Sketch of Proof.
key parameter r

The situation looks like this,



$N_* = \langle \sigma \rangle$ is cyclic of order p^n

$\sigma(w) = \zeta_{p^n} w$

$\Delta \cong Gal(k(\zeta_{p^n})/k)$

Δ isomorphic to a s.g. of $Aut(N_*) = \langle \delta \rangle$ where ${}^{\delta}\sigma = \sigma^{\pi}$ with $\langle \pi \rangle = (\mathbb{Z}/p^n\mathbb{Z})^*$

In particular

$$\begin{cases} \Delta \cong \langle \delta^{p^{r-1}(p-1)} \rangle \text{ if } 1 \leq r \leq n \\ \Delta \cong \langle \delta^{dp^e} \rangle \text{ for } d < p-1,\ 0 \leq e \leq n-1 \text{ if } r = 0 \end{cases}$$

Identify Δ as this subgroup since $\Gamma_r = N_*\Delta \cong N_* \rtimes \Delta$.

If $r = 0$, $d = 1$, and $e = 0$ then $\Delta \cong Aut(N_*)$ (and so $\Gamma \cong Hol(N_*)$)

If $r = n$ then $k = k(\zeta_{p^n})$ and K/k is already a Galois extension whereby $\tilde{K} = K$, $\Delta = \{1\}$ and so we define $\Gamma_n = N_* = Gal(K/k)$.

Any Hopf Galois structure on K/k will correspond to a regular subgroup N of $B = Perm(\Gamma_r/\Delta) \cong S_{p^n}$ normalized by Γ_r and by the earlier remarks about regularity, we must have $|N| = [K : k] = p^n$.

Cases

N cyclic of order p^n (hence regular) and moreover $N = N^{opp}$
Any such N has the form $(\sigma^i, \delta^{p^k(p-1)})$ for $i \in (\mathbb{Z}/p^{n-1-k}\mathbb{Z})^*$ for $k = 0 \ldots n-1$

Almost classical structures?

Look for those $N \triangleleft \Gamma_r$.

If $r = n$, the extension is already Galois and so $\Gamma = N_*$ and so $N = N_*$

For $0 \le r \le n$, $(\sigma^i, \delta^{p^k(p-1)}) \triangleleft \Gamma_r$ iff

$$
\begin{aligned}
n &\le k + (r+1) \\
k &\ge r - 1
\end{aligned}
$$

and the number of these is exactly $p^{min(r,n-r)}$.

For the general case one is looking for $N_\beta \leq B$ normalized by $\Gamma_r \leq B$.

For N cyclic of order p^n, if $Aut(N) = \langle \delta \rangle$ then we can look at the p-subgroups of $Aut(N)$, namely $\langle \delta^{p^{r-1}(p-1)} \rangle$ for $r = 0..n-1$.

As such we can define the *r-th lower holomorph* of N, $Hol_r(N)$ as

$$N \rtimes \langle \delta^{p^{r-1}(p-1)} \rangle$$

This makes it easy to view Γ_r as $Hol_r(N_*)$

So we want to look for those $N_\beta \leq B$ such that

$$Hol_r(N_*) \leq Hol(N_\beta)$$

Main idea is to realize that $N_\beta = \beta N_* \beta^{-1}$ for some $\beta \in B$ since both N_* are cyclic of order p^n, hence conjugate in B.

As such

$$Hol_r(N_*) \leq Hol(\beta N_* \beta^{-1})$$

and so

$$Hol_r(\beta^{-1} N_* \beta) \leq Hol(N_*)$$

So we may look for such $\beta^{-1} N_* \beta$ in the subgroup lattice of $Hol(N_*)$.

For $r < n$ there are precisely p^r such groups, for $r = n$ there are p^{n-1}.

The fact that there are no more arises due the examination of when

$$\Gamma \leq Hol(N)$$

where N has order p^n.

In particular, we show that unless N is cyclic, the p-Sylow subgroup of $Hol(N)$ has exponent *strictly less* than p^n.

As such, for $\Gamma = \Gamma_r$, each of which having the exponent of it's p-Sylow subgroup equalling p^n, rules out any N but cyclic of order p^n.

We can say something about uniqueness of Hopf Galois structures, in particular we have the following interesting result due to Byott.

Theorem - [Byott 1996]. *If L/K is Galois with group G where $|G| = n$ then L/K is Hopf Galois for a unique Hopf algebra if and only if n is Burnside number, that is $gcd(n, \phi(n)) = 1$ where ϕ is the Euler totient.*

Examples, $n = p, 2p, 3p, 5p, 17p, 257p$
$13p$ (for $p \not\equiv 1\ (mod\ 13)$ $p \geq 5$)
$3 \cdot 5 \cdot 17 \cdot 23 \cdot 53 \cdot 83 \cdot 257$