Hopf-Galois Structures on Galois Field Extensions of Squarefree Degree

Ali A. Alabdali[1]

University of Exeter, UK

08/09/2017

[1]aaab201@exeter.ac.uk

Hopf-Galois structure

- For normal separable field extension L/K, $\Gamma = Gal(L/K) =$ group of K-automorphisms of L.

- The group algebra $K[\Gamma] = \{\sum_{\gamma\in\Gamma} C_\gamma \gamma \ : C_\gamma \in K\}$ acts on L with the maps below is a Hopf algebra.

$$
\begin{array}{rrl}
\text{comultiplication} & \Delta : & \sum C_\gamma \gamma \longmapsto \sum C_\gamma \gamma \otimes \gamma \in K[\Gamma] \otimes K[\Gamma] \\
\text{counit} & \epsilon : & \sum C_\gamma \gamma \longmapsto \sum C_\gamma \\
\text{antipode} & S : & \sum C_\gamma \gamma \longmapsto \sum C_\gamma \gamma^{-1}
\end{array}
$$

- We can generalise this to look at other Hopf algebras H giving L a Hopf-Galois structure.

Greither and Pareigis theory

- Hopf-Galois theory for separable extensions.

- The key result of [Greither and Pareigis, 1987] : Hopf-Galois structures on L/K correspond to regular subgroups $G \leq Perm(\Gamma)$ normalised by left translations by Γ.

Regular subgroups

- $H \leq Perm(\Gamma)$ is said to be regular if it satisfies any two of the following conditions which imply to satisfy the other:
  1. $Stab_H(\gamma)$ is the trivial group, for any $\gamma \in \Gamma$
  2. H acts transitively on Γ
  3. $|H| = |\Gamma|$.

- By using the bijection between H and Γ, given G with $|G| = |\Gamma|$, the number of such H isomorphic to G

$$= \frac{|Aut(\Gamma)|}{|Aut(G)|} \sharp(\text{ regular subgroups in } Hol(G) \text{ isomorphic to } \Gamma),$$

where $Hol(G) = G \rtimes Aut(G) = \{[g, \alpha] \mid g \in G,\ \alpha \in Aut(G)\}$, with

$$[g, \alpha][g^{'}, \alpha^{'}] = [g\alpha(g^{'}), \alpha\alpha^{'}].$$

[Byott, 1996]

Groups of squarefree order

For n squarefree any group of order n has form

$$G(d,\, e,\, k) = \langle \rho, \pi : \rho^e = 1 = \pi^d : \pi\rho\pi^{-1} = \rho^k \rangle$$

where $n = de$, $gcd(k,\, e) = 1$ and $ord_e(k) = d$.
In this case $G(d,\, e,\, k)$ isomorphic to $G(d^{'},\, e^{'},\, k^{'})$ if and only if $d = d^{'}$, $e = e^{'}$, and $k, k^{'}$ generate the same cyclic subgroup of $U(e)$ the group of units in the ring $\mathbb{Z}/e\mathbb{Z}$ of integers modulo e. [Murty and Murty, 1984]
Centre of $G(d,\, e,\, k) \cong C_z$ where $z = gcd(e,\, k-1)$ with $e = zg$, in which g (respectively, z) is the order of the commutator subgroup $G^{'}$ (respectively, the centre $Z(G)$) of G.

Fix the group $G = G(d,\, e,\, k)$ and the numbers g, z. For each prime $q \mid e$, let $r_q = ord_q(k)$. Thus we have
$r_q = 1 \Leftrightarrow q \mid z$; $r_q \mid gcd(d,\, q-1)$; $lcm\{r_q : q \mid e\} = lcm\{r_q : q \mid g\} = d$.

Counting regular subgroups

We fix a group G of squarefree order $n = de$. Then $Aut(G)$ is generated by the automorphism θ and automorphism ϕ_s for each $s \in U(e)$, where

$$\theta(\rho) = \rho, \quad \theta(\pi) = \rho^z \pi, \quad \phi_s(\rho) = \rho^s, \quad \phi_s(\pi) = \pi, \quad \phi_s \theta \phi_s^{-1} = \theta^s.$$

Therefore, we have

$$Aut(G) \cong C_g \rtimes U(e) \text{ and } |Aut(G)| = g\phi(e).$$

We count regular subgroups of a given isomorphism type inside $Hol(G)$. Let Γ be another group of order n.

$$\Gamma = G(\delta, \epsilon, \kappa) = \langle S,\ T : S^\epsilon = T^\delta = 1,\ TST^{-1} = S^\kappa \rangle,$$

and set $\zeta = gcd(\kappa - 1, \epsilon)$, $\gamma = \epsilon/\zeta$ and $\rho_q = ord_q(\kappa)$ for primes $q \mid \epsilon$. Set $X = S^\zeta$ and $Y = TS^\gamma$. As S^γ generates the centre of Γ, we have

$$\Gamma = G(\delta, \epsilon, \kappa) = \langle X,\ Y : X^\gamma = Y^{\zeta\delta} = 1,\ YXY^{-1} = X^\kappa \rangle.$$

Some properties

Proposition 1

For $Hol(G)$ to contain any regular subgroups isomorphic to Γ, we must have $d \mid \zeta\delta$ and hence $\gamma \mid e$.

Lemma 2

Let X, Y be elements of $Hol(G)$ of the form $X = [\sigma^a, \theta^c]$, $Y = [\sigma^u\tau, \theta^v\phi_t]$. Suppose that X and Y satisfy the properties:

(i) The subgroup $\langle X \rangle$ of $Hol(G)$ acts regularly on $\{\sigma^{em/\gamma} : m \in \mathbb{Z}\}$;

(ii) $Y^{\zeta\delta} = 1$;

(iii) $YX = X^{\kappa}Y$, where $\kappa = \kappa_0^h$ for some $h \in \mathbb{Z}_\delta^\times$, κ_0 is a fixed value of κ;

(iv) The subgroup $\langle X, Y^d \rangle$ of $Hol(G)$ acts transitively on $\{\sigma^m : m \in \mathbb{Z}\}$.

Then X and Y generate a regular subgroup of $Hol(G)$ isomorphic to Γ. Conversely, every regular subgroup of $Hol(G)$ isomorphic to Γ contains exactly $\gamma\phi(e)$ such pairs of generators.

Main results

Definition 3

For each $h \in \mathbb{Z}_\delta^\times$, let $N(k, \kappa_0, h)$ be the number of quintuples $(a, c, u, v, t) \in \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e \times \mathbb{Z}_g \times \mathbb{Z}_e^\times$ such that the elements $X = [\sigma^a, \theta^c]$, $Y = [\sigma^u \tau, \theta^v \phi_t] \in Hol(G)$ satisfy conditions (i)-(iv) of Lemma 2, for which $YX = X^\kappa Y$ with $\kappa = \kappa_0^h$. Thus $N(k, \kappa_0) = \sum_{h \in \mathbb{Z}_\delta^\times} N(k, \kappa_0, h)$.

Theorem 4

The number of quintuples is

$$N(k, \kappa_0, h) = \frac{\phi(e)\gamma g 2^{\omega(g)}}{\phi(d)} \prod_{r_q \neq \rho_q} \phi(r_q) \prod_{r_q = \rho_q} \left[\phi(r_q) - 1 + \frac{1}{q} \right].$$

[For each $q \mid g$, there are $\phi(r_q)$ choices of k mod q of order r_q.]

Main results

So the number of Hopf-Galois structures of type G on a Galois extension with Galois group isomorphic to Γ is

$$\frac{|Aut(\Gamma)|}{|Aut(G)|} \times \frac{1}{\gamma\phi(e)} \sum_{h \in \mathbb{Z}_\delta^\times} N(k,\, \kappa_0,\, h) = \frac{\phi(\epsilon)}{g\phi(e)^2} \sum_{h \in \mathbb{Z}_\delta^\times} N(k,\, \kappa_0,\, h).$$

Hence we have:

Theorem 6

Let G, Γ be groups of squarefree order n. Then the total number of Hopf-Galois structures of type G on a Galois extension with Galois group Γ is 0 if $\gamma \nmid e$, and otherwise it is

$$2^{\omega(g)}\gamma \prod_{r_q \neq \rho_q} \phi(r_q) \prod_{r_q = \rho_q} \left[\phi(r_q) - 1 + \frac{1}{q}\right].$$

Sketch of proof of Theorem 6

This follows from

1. Proposition 1 which proves the regularity of the subgroup $\langle X,\, Y^d \rangle$.
2. Definition 3 which explains the number of quintuples $(a,\, c,\, u,\, v,\, t)$.
3. Theorem 4 by multiplying with the number of quintuples $N(k,\, \kappa_0) = \sum_{h \in \mathbb{Z}_\delta^\times} N(k,\, \kappa_0,\, h)$. Then, we have the total number of Hopf-Galois structures as

$$2^{\omega(g)}\gamma \prod_{r_q \neq \rho_q} \phi(r_q) \prod_{r_q = \rho_q} \left[\phi(r_q) - 1 + \frac{1}{q}\right].$$

Thank You