Enumeration of Hopf-Galois structures on cyclic field extensions

George Samways

University of Exeter

Supervised by Nigel Byott

gs348@exeter.ac.uk

Hopf-Galois extensions I

Let L/K be a Galois extension of degree n, with Galois group $\mathrm{Gal}(L/K) = \Gamma$, and let H be a K-Hopf algebra. The field L is an H-module algebra if it satisfies the following, $\forall h \in H$ and $\forall x, y \in L$:

$$h(xy) = \sum h_{(1)}(x)h_{(2)}(y),$$
$$h(1) = \varepsilon(h)1.$$

If L is a H-module algebra, and the map:

$$j : L \otimes H \to \mathrm{End}_K(L)$$
$$j(x \otimes h)(y) = xh(y)$$

is an isomorphism, then H together with its action on elements of L is called a Hopf-Galois structure on L/K.

Hopf-Galois extensions II

Greither and Pareigis showed that this is equivalent to a question based entirely in group theory.

Theorem ([Greither and Pareigis, 1987])

Let L/K be a Galois extension, with $Gal(L/K) = \Gamma$. There is a bijection between regular subgroups G of $Perm(\Gamma)$ normalised by $\lambda(\Gamma)$, and Hopf-Galois structures on L/K.

This theorem gives us a method for finding Hopf-Galois structures, but it is in general difficult due to the size of $\mathrm{Perm}(\Gamma)$. Byott [Byott, 1996] reversed the relationship between G and Γ: to find Hopf-Galois structures, we can consider regular embeddings of Γ into the holomorph $\mathrm{Hol}(G)$.

Previous Work I

We make use of the following results from earlier work on enumerating Hopf-Galois structures.

Theorem ([Byott, 2007])

Let L/K be a cyclic Galois extension of degree 2^n, $n \geq 3$. Then L/K admits $3 \cdot 2^{n-2}$ Hopf-Galois structures: 2^{n-2} each of cyclic, dihedral, and generalised quaternion type.

Theorem ([Kohl, 1997])

Let L/K be a cyclic Galois extension of degree p^n, where p is an odd prime. Then there are p^{n-1} Hopf-Galois structures, all of cyclic type.

Previous Work II

Theorem ([Alabdali and Byott, 2017])

Let L/K be a cyclic Galois extension of squarefree degree n, and let G be any group of order n. Let $z = |Z(G)|$, $g = |[G,G]|$ and $d = n/(gz)$. Then there are $2^{\omega(g)}\varphi(d)$ Hopf-Galois structures of type G, where $\omega(g)$ is the number of distinct prime factors of g.

We wish to generalise these results to cyclic Galois extensions of arbitrary degree. In particular, if $4 \nmid n$ then for a given type G we can find the number of structures in terms of G.

Characteristic subgroups

Let G be some abstract group. We call a subgroup $H \subseteq G$ *characteristic* if, for all $\theta \in \mathrm{Aut}(G)$, $\theta(H) = H$, and write H char G.

Theorem

Let G be the type of a Hopf-Galois structure on L/K, and let H char G. Then H, respectively G/H, is the type of a Hopf-Galois structure on some Galois extension with Galois group Δ, respectively Γ/Δ, where Δ is the subgroup of Γ of order $|H|$.

Creating a subgroup series for G I

Throughout, given a prime divisor $p|n$, we write n_p to denote the highest power of p dividing n.

Let G be the type of a Hopf-Galois structure on L/K. Let G_1 be a *minimal characteristic subgroup* - a characteristic subgroup which is characteristically simple. Since G_1 char G, G_1 is the type of a Hopf-Galois structure. By Byott [Byott, 2015], G_1 must be an abelian simple group, so it is of the form C_p^m where p is a prime - that is, G_1 has elementary abelian type, and the associated extension is cyclic of prime power degree. Then, due to previous results, p^m is prime (i.e. $m = 1$) or $p^m = 4$ and $G_1 \cong C_2 \times C_2$.

Creating a subgroup series for G II

G/G_1 is also the type of a Hopf-Galois structure on some cyclic extension. As before, let $\bar{G}_2$ be a minimal characteristic subgroup of G/G_1: by the above, $\bar{G}_2$ is either C_p or $C_2 \times C_2$.
Additionally, $\bar{G}_2 \cong G_2/G_1$ for some subgroup $G_1 \lhd G_2 \lhd G$, and $\bar{G}_2$ char G/G_1 implies that G_2 char G.
We continue this to find further subgroups $G_3, \ldots, G_r$, until G/G_r is characteristically simple.
Then we have a normal series:

$$1 \lhd G_1 \lhd \cdots \lhd G_r \lhd G,$$

in which each G_i char G, and each *subquotient* G_i/G_{i-1} is isomorphic to either C_{p_j} for some prime p_j, or $C_2 \times C_2$.

Creating a subgroup series for G III

Let $n = \prod p_i^{n_{p_i}}$ where the distinct primes p_i are labelled so that $p_i > p_{i+1}$. We may choose the series such that the subquotients are 'ordered', in the sense that if $G_i/G_{i-1} \cong C_p$ and $G_{i+1}/G_i \cong C_q$, then $p \geq q$, and all cyclic subquotients appear before any $C_2 \times C_2$ terms appear. Additionally, at most one subquotient (G/G_r) is isomorphic to $C_2 \times C_2$. Then we may add the term G_{r+1}:

$$1 \lhd G_1 \lhd \cdots \lhd G_r \lhd G_{r+1} \lhd G,$$

where $G_{r+1}/G_r \cong C_2$ is a normal subgroup of $C_2 \times C_2$, to get a normal series with all subquotients cyclic. Hence G is supersolvable.

Sylow subgroups of G I

$$1 \lhd G_0 \lhd \cdots \lhd G_r \lhd G$$

Assume that p_1 is odd, and consider the term $G_{n_{p_1}}$ in this series. $G_{n_{p_1}}$ is a characteristic subgroup of G of order $p_1^{n_{p_1}}$, so is the unique p_1-Sylow subgroup of G. It is also the type of a Hopf-Galois structure on a cyclic extension of prime power degree, so by previous results it is cyclic.

Now we consider $G/G_{n_{p_1}}$. This is the type of a Hopf-Galois structure on a cyclic field extension, so by the above we can form a similar series for $G/G_{n_{p_1}}$. Then, again assuming that p_2 is odd, $G/G_{n_{p_1}}$ has a unique cyclic p_2-Sylow subgroup H.

Sylow subgroups of G II

The p_2-Sylow subgroup H of $G/G_{n_{p_1}}$ is isomorphic to $SG_{n_{p_1}}/G_{n_{p_1}}$, where S is some p_2-Sylow subgroup of G. We have:

$$H \cong SG_{n_{p_1}}/G_{n_{p_1}} \cong S/(S \cap G_{n_{p_1}}) \cong S,$$

so the p_2-Sylow subgroup of G is also cyclic (although not necessarily unique). Similarly we can find the p_k-Sylow subgroup for an odd prime p_k by performing the above steps with the quotient $G/G_{n_{p_1}+\cdots+n_{p_{k-1}}}$.

Hence every p-Sylow subgroup of G for an odd prime p is cyclic, and by quotienting out at the appropriate term in the series we find that the 2-Sylow subgroup appears as the type of a Hopf-Galois structure on a cyclic extension. Then by previous results the 2-Sylow subgroup must be one of three types: cyclic, dihedral, or of generalised quaternion type.

Presentations of G I

If the 2-Sylow subgroup is cyclic, G is a C-group (i.e. all of its Sylow subgroups are cyclic). Then G has the following presentation, due to Murty and Murty [Murty and Murty, 1984]:

$$G = \langle \sigma, \tau | \sigma^e = \tau^d = 1, \tau\sigma\tau^{-1} = \sigma^r \rangle.$$

Here $\gcd(d, e) = 1$ and $de = n$. Further, $\mathrm{ord}_e(r) = d'$, where $\gamma(d)|d'|d$. Here $\gamma(d) = \prod_{p|d} p$ is the radical of d. In particular, if n is squarefree then $\gamma(d) = d' = d$ and we retrieve the setting in Alabdali's paper.

Presentations of G II

On the other hand, if the 2-Sylow subgroup is not cyclic, it contains a normal cyclic subgroup of index 2, and we have the following presentation due to Zassenhaus [Zassenhaus, 1936]:

$$G = \langle \sigma, \tau, \eta | \sigma^e = 1, \tau^d = \sigma^t, \tau\sigma\tau^{-1} = \sigma^r, \eta\sigma\eta^{-1} = \sigma^\ell, \eta\tau\eta^{-1} = \tau^\ell \rangle.$$

Here $\mathrm{ord}_e(r) = d$, $\gcd(e, r-1) = z$, $zt = m$, $\ell \equiv 1 \pmod d$ and $\ell^2 \equiv 1 \pmod e$. Further, either $\eta^2 = 1$ or $d \equiv 0 \pmod 2$ and $\eta^2 = \tau^{zt/2}$. Note that this case can only occur if $4|n$, as otherwise the 2-Sylow subgroup must be cyclic.

For now we work in the first presentation where G is a C-group, and the 2-Sylow subgroup is cyclic.

Holomorph of G I

We first find the form of $\mathrm{Hol}(G) = G \rtimes \mathrm{Aut}(G)$. Any element of G has the form $\sigma^\alpha \tau^\beta$. To simplify notation, we introduce:

$$S(x,k) = 1 + x + x^2 + \cdots + x^{k-1}, \quad z = \gcd(e, r-1).$$

Let $\theta \in \mathrm{Aut}(G)$. We have:

$$\theta(\sigma) = \sigma^s, \quad \theta(\tau) = \sigma^a \tau^b,$$

where $\gcd(e,s) = 1$, $a \equiv 0 \pmod{z}$, and $b \equiv 1 \pmod{d'}$.

$$\begin{aligned} \theta(\tau\sigma\tau^{-1}) &= \sigma^a \tau^b \sigma^s \tau^{-b} \sigma^{-a} \\ &= \sigma^{sr^b} \\ &= \sigma^{sr} = \theta(\sigma^r). \end{aligned}$$

Holomorph of G II

We denote a given automorphism by $\theta_{a,b,s}$. Then an element of $\mathrm{Hol}(G)$ has the form $(\sigma^\alpha\tau^\beta, \theta_{a,b,s})$, with multiplication given by:

$$(\sigma^\alpha\tau^\beta, \theta_{a,b,s}) \cdot (\sigma^\gamma\tau^\delta, \theta_{c,d,t}) = (\sigma^{\alpha+\gamma sr^\beta + aS(r,\delta)}\tau^{\beta+\delta b}, \theta_{a+cs,bd,st}).$$

Regularity conditions I

Consider a regular cyclic subgroup of $\mathrm{Hol}(G)$, $C = \langle \hat{x} \rangle$, where $\hat{x} = (\sigma^{\alpha}\tau^{\beta}, \theta_{a,b,s})$. Powers of $\hat{x}$ have the form:

$$\hat{x}^k = (\sigma^{\alpha'}\tau^{\beta S(b,k)}, \theta_{a',b',s'}),$$

for some α', a', b', s'. Since C is regular, there is some k so that $\hat{x}^k \cdot 1_G = \tau$. This then implies that $\beta S(b,k) \equiv 1 \pmod{d} \implies \gcd(k,d) = 1$.

Regularity conditions II

Choosing k such that $\gcd(k, e) = 1$, we then have a k coprime to n (i.e. $C = \langle \hat{x}^k \rangle$) such that:

$$\hat{x}^k = (\sigma^{\alpha'}\tau, \theta_{a',b',s'}).$$

In fact, there are $\varphi(e)$ generators of C with this form. We may now assume that if $C = \langle x \rangle$ is a regular cyclic subgroup of $\mathrm{Hol}(G)$, x has the form of $\hat{x}^k$ above.

Theorem

Let $C = \langle x \rangle$ be a cyclic subgroup of $\mathrm{Hol}(G)$. Then C is regular if and only if $\langle x^d \rangle$ acts transitively on $\langle \sigma \rangle$.

Regularity conditions III

We now consider the simpler problem of when $\langle x^d \rangle$ is transitive on $\langle \sigma \rangle$.

$$x^{di} = (\sigma^{A(di)}, \theta_{aS(s,di),b^{di},s^{di}}),$$

where $A(di) = \alpha S(rs, di) + a \sum_{h=0}^{di-1} S(s,h) r^h$. In particular, $A(di)$ should take all residue classes modulo e as i varies in order for this to be transitive.

Our strategy is to find conditions so that $A(di)$ takes all residue classes modulo q^{n_q} for primes $q|e$. Defining $g = e/z$ we can divide the primes q into those dividing z and those dividing g.

Regularity conditions IV

If $q|z$ then $a \equiv 0 \pmod{q^{n_q}}$, so the expression simplifies to $A(di) \equiv \alpha S(rs, di) \pmod{q^{n_q}}$.

Theorem

If $A(di)$ takes all residue values $\pmod{q^{\gamma_q}}$ then $s \equiv 1 \pmod{q^{\delta}}$ for some $1 \leq \delta \leq \gamma$, and $q \nmid \alpha$.

Regularity conditions V

If $q|g$, a may now be non-zero. Note that $r \not\equiv 0, 1 \pmod{q}$ as it has order dividing d and $q \nmid \gcd(e, r-1)$, so in this case we cannot have $q = 2$.

Theorem

If $A(di)$ takes all residue values $\pmod{q^{\gamma_q}}$ then either:

1. $s \equiv 1 \pmod{q}$ *and* $q \nmid a$*, or*
2. $s \equiv r^{-1} \pmod{q}$ *and* $q \nmid \alpha(s-1) + a$.

We can then combine our results for all primes $q|e$ to obtain conditions on α, a, s for $\langle x^d \rangle$ to be transitive on $\langle \sigma \rangle$.

Enumeration of Hopf-Galois structures I

Counting the choices of α, a, s, we get $2^{\omega(g)} \frac{e}{\gamma(e)} \varphi(z) g \varphi(g)$ generators of regular cyclic subgroups in $\mathrm{Hol}(G)$ of the form where τ has a single exponent (here $\omega(g)$ denotes the number of distinct prime factors of g). Since each regular cyclic subgroup has $\varphi(e) = \varphi(z)\varphi(g)$ such generators, we get the total number of regular subgroups as:

$$2^{\omega(g)} \frac{e}{\gamma(e)} g.$$

Enumeration of Hopf-Galois structures II

We now find the total number of Hopf-Galois structures of type G, using the formula from [Byott, 1996]:

$$\frac{|\mathrm{Aut}(C_n)|}{|\mathrm{Aut}(G)|} 2^{\omega(g)} \frac{e}{\gamma(e)} g = 2^{\omega(g)} \frac{e}{\gamma(e)} \frac{d'}{d} \varphi(d).$$

Note that in the squarefree case, $e = \gamma(e)$, $d' = d$, and we retrieve the number of structures in the squarefree case: $2^{\omega(g)}\varphi(d)$. This is a complete result for groups when $4 \nmid n$ since in that case we can guarantee the 2-Sylow subgroup will be cyclic.

Groups without a cyclic 2-Sylow subgroup I

Work on the case where the 2-Sylow subgroup is not cyclic is ongoing. In this case, G has a normal subgroup G' of index 2 which is itself a C-group. We can split the group G' into primes q for which the q-Sylow subgroups are normal, and primes p for which the p-Sylow subgroups are not normal:

$$G' = \left(\prod_{q|e} C_{q^{n_q}} \rtimes \prod_{p|d} C_{p^{n_p}} \right)$$

Then we have that $G/G' \cong \langle \eta \rangle$ has order 2, and depending on the structure of the 2-Sylow subgroup of G the η may have order 2 or 4.

Currently we are trying to understand the shape of $\mathrm{Aut}(G)$ in this setting. For example, in the case where all p-Sylow subgroups of G' are normal (G' is cyclic) we should agree with results on dihedral extensions.

References I

A. Alabdali and N. Byott (2017)
Counting Hopf-Galois structures on cyclic field extensions of squarefree degree.
J. Algebra 493, 1-19

N. Byott (2015)
Solubility criteria for Hopf-Galois structures.
New York J. Math. 21, 883-903.

N. P. Byott (2007)
Hopf-Galois structures on almost cyclic field extensions of 2-power degree.
J. Algebra 318, 351-371.

N. P. Byott (1996)
Uniqueness of Hopf Galois Structure for Separable Field Extensions.
Commutative Algebra 24(10), 3217-3228.

References II

L. Childs (1989)
On the Hopf Galois theory for separable field extensions.
Commutative Algebra 17, 809-825.

C. Greither, B. Pareigis (1987)
Hopf Galois theory for separable field extensions.
J. Algebra 106 (1), 239-258.

T. Kohl (1997)
Classification of the Hopf Galois Structures on prime power radical extensions.
J. Algebra 207, 525-546.

Murty, M. R., Murty, V. K. (1984)
On groups of squarefree order.
Math. Ann, 267(3), 299-309.

References III

Zassenhaus, H. (1936)
Über endliche Fastkörper.
Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, 11(1), 187-220.