New York Journal of Mathematics

New York J. Math. **9** (2003) 99–115.

On Hopf Galois structures and complete groups

Lindsay N. Childs

Abstract. Let L be a Galois extension of K, fields, with Galois group Γ. We obtain two results. First, if $\Gamma = \mathrm{Hol}(Z_{p^e})$, we determine the number of Hopf Galois structures on L/K where the associated group of the Hopf algebra H is Γ (i.e. $L \otimes_K H \cong L[\Gamma]$). Now let p be a safeprime, that is, p is a prime such that $q = (p-1)/2 > 2$ is also prime. If L/K is Galois with group $\Gamma = \mathrm{Hol}(Z_p)$, p a safeprime, then for every group G of cardinality $p(p-1)$ there is an H-Hopf Galois structure on L/K where the associated group of H is G, and we count the structures.

Contents

Let L be a Galois extension of K, fields, with finite Galois group Γ. Then L is an H-Hopf Galois extension of K for $H = K\Gamma$, where $K\Gamma$ acts on L via the natural action of the Galois group Γ on L. Greither and Pareigis [GP87] showed that for many Galois groups Γ, L is also an H-Hopf Galois extension of K for H a cocommutative K-Hopf algebra other than $K\Gamma$. The Hopf algebras H that arise have the property that $L \otimes_K H \equiv LG$, the group ring over L of a group G of the same cardinality as Γ. We call G the associated group of H.

From [By96] we know that for H a cocommutative K-Hopf algebra, H-Hopf Galois structures on L correspond bijectively to equivalence classes of regular embeddings $\beta : \Gamma \to \mathrm{Hol}(G) \subset \mathrm{Perm}(G)$. Here $\mathrm{Perm}(G)$ is the group of permutations of the set G, and $\mathrm{Hol}(G)$ is the normalizer of the left regular representation of G in $\mathrm{Perm}(G)$. One sees easily that $\mathrm{Hol}(G)$ contains the image of the right regular representation $\rho : G \to \mathrm{Perm}(G)$ and also $\mathrm{Aut}(G)$; then $\mathrm{Hol}(G) = \rho(G) \cdot \mathrm{Aut}(G)$ and is isomorphic to the semidirect product $G \rtimes \mathrm{Aut}(G)$. The equivalence relation on

Received July 22, 2003.

Mathematics Subject Classification. 12F, 16W.

Key words and phrases. Hopf Galois structure, complete group, holomorph.

I wish to thank Union College and Auburn University Montgomery for their hospitality.

ISSN 1076-9803/03

regular embeddings is by conjugation by elements of $\mathrm{Aut}(G)$ inside $\mathrm{Hol}(G)$: $\beta \sim \beta'$ if there exists γ in $\mathrm{Aut}(G)$ so that for all g in G, $\gamma\beta(g)\gamma^{-1} = \beta'(g)$.

Thus the number $e(\Gamma, G)$ of H-Hopf Galois structures on L/K where the associated group of H is G depends only on G and the Galois group Γ, and reduces to a purely group-theoretic problem.

If L is a Galois extension of K with Galois group Γ non-abelian simple or $\cong S_n$, then in [CC99] we counted the number of Hopf Galois structures on L/K with associated group $G = \Gamma$ by "unwinding" regular embeddings. The unwinding idea applies more generally when G is a complete group, i. e. has trivial center and trivial outer automorphism group. In this paper we apply this unwinding idea to determine $e(G, G)$ when G is the complete group $\mathrm{Hol}(Z_{p^e})$, p an odd prime.

One theme of research on Hopf Galois structures on Galois extensions of fields is to determine to what extent it is true that if L/K is Galois with Galois group Γ and is H-Hopf Galois where H has associated group G, then $G \cong \Gamma$. Positive results in this direction include Byott's original uniqueness theorem [By96]; Kohl's Theorem [Ko98] that if $\Gamma = Z_{p^e}$ then $G \cong \Gamma$; Byott's recent result [By03a], complementing [CC99], that if Γ is non-abelian simple then $G = \Gamma$; and Featherstonhaugh's recent result [Fe03] that if G and Γ are abelian p-groups with p sufficiently large compared to the p-rank of G and $\log_p$ of the exponent of G, then $G \cong \Gamma$. (A survey of results before 2000 in this area may be found in Chapter 2 of [C00]; Chapter 0 of [C00] describes how Hopf Galois structures on Galois extensions of local fields relate to local Galois module theory of wildly ramified extensions.)

In the last two sections of this paper we consider this uniqueness question for $\Gamma = \mathrm{Hol}(Z_p)$ when p is a safeprime, that is, $p = 2q + 1$ where p and q are odd primes. (The terminology "safeprime" arises in connection with factoring large numbers related to cryptography—see [C95, pp. 411-413].) Then there are exactly six isomorphism classes of groups of cardinality $p(p-1)$. We show that if L/K is a Galois extension with Galois group $\Gamma = \mathrm{Hol}(Z_p)$, then for each of the six groups G of cardinality $p(p-1)$ up to isomorphism, there is an H-Hopf Galois structure on L/K with associated group G, and we count their number. Thus $\Gamma = \mathrm{Hol}(Z_p)$ yields an example of the opposite extreme to the uniqueness results listed above.

1. Regular embeddings

Given a Galois extension L/K with Galois group Γ, and a group G of cardinality that of Γ, the number $e(\Gamma, G)$ of Hopf Galois structures on L/K whose Hopf algebra H has assocated group G is equal to the number of equivalence classes of regular embeddings of Γ into $\mathrm{Hol}(G)$, the semidirect product of G and $\mathrm{Aut}(G)$. Here an embedding $\beta : \Gamma \to \mathrm{Hol}(G)$ is regular if, when viewing $\mathrm{Hol}(G)$ inside $\mathrm{Perm}(G)$ via $(g, \alpha)(x) = \alpha(x)g^{-1}$, the orbit of the identity element 1 of G under $\beta(\Gamma)$ is all of G.

Obtaining $e(\Gamma, G)$ in any particular case involves a number of steps:

(a) determining $\mathrm{Aut}(G)$, hence $\mathrm{Hol}(G)$;
(b) finding monomorphisms β from Γ to $\mathrm{Hol}(G)$ by defining β on generators of Γ and checking β on the relations among those generators: in particular, it is helpful to know the orders of elements of $\mathrm{Hol}(G)$ in order to choose where to send the generators of Γ;
(c) checking for regularity of β;

(d) simplifying β under the equivalence relation of conjugation by elements of $\mathrm{Aut}(G)$ inside $\mathrm{Hol}(G)$—that is, finding a complete set of representatives for the equivalence classes of regular embeddings β;
(e) counting the representatives.

Of these tasks, checking regularity is the least natural. If we view $\mathrm{Hol}(G)$, the semidirect product of G and $\mathrm{Aut}(G)$, as $G \times \mathrm{Aut}(G)$ as sets, the operation is

$$(g, \alpha) \cdot (g', \alpha') = (g\alpha(g'), \alpha\alpha')$$

for $g, g' \in G, \alpha, \alpha' \in \mathrm{Aut}(G)$. Then $G \cong \{(g, 1)\}$ is a normal subgroup of $\mathrm{Hol}(G)$, and the projection π_2 onto $\mathrm{Aut}(G)$ by $\pi_2(g, \alpha) = \alpha$ is a homomorphism; however the projection π_1 onto G, $\pi_1(g, \alpha) = g$, is not. But since an element (g, α) viewed in $\mathrm{Perm}(G)$ acts on the identity element 1 of the set G by $(g, \alpha)(1) = \alpha(1)g^{-1} = g^{-1}$, checking regularity of a 1-1 homomorphism $\beta : \Gamma \to \mathrm{Hol}(G)$ is the same as determining whether the function (non-homomorphism) $\pi_1\beta : \Gamma \to G$ is bijective.

Let $\mathrm{Inn}(G)$ be the group of inner automorphisms of G, then $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$ and $\mathrm{Aut}(G)/\mathrm{Inn}(G) = O(G)$, the outer automorphism group, fits in the exact sequence

$$1 \to Z(G) \to G \to \mathrm{Aut}(G) \to O(G) \to 1$$

where the map $C : G \to \mathrm{Aut}(G)$ is conjugation: $C(g)(x) = gxg^{-1}$ for $g, x \in G$, and $Z(G)$ is the center of G.

Suppose $Z(G) = (1)$ and the composition of the 1-1 homomorphism $\beta : \Gamma \to \mathrm{Hol}(G)$ with the homomorphism $\mathrm{Hol}(G) \to O(G)$ yields a trivial homomorphism from Γ to $O(G)$. Then β maps into $G \rtimes \mathrm{Inn}(G)$, and, following [CC99], we may decompose β as follows: we have a homomorphism

$$j : G \rtimes \mathrm{Inn}(G) \to G \times G$$

by $j(g, C(h)) = (gh, h)$ for $g, h \in G$, with inverse sending (g, h) to $(gh^{-1}, C(h))$. Letting $p_i : G \times G \to G$ be projection onto the ith factor, $i = 1, 2$, the homomorphism β yields homomorphisms $\beta_1 = p_1 j \beta$ and $\beta_2 = p_2 j \beta : \Gamma \to G$ such that

$$\beta(\gamma) = (\beta_1(\gamma)\beta_2(\gamma)^{-1}, C(\beta_2)).$$

Then β is regular iff

$$\{\pi_1\beta(\gamma) | \gamma \in \Gamma\} = \{\beta_1(\gamma)\beta_2(\gamma)^{-1} | \gamma \in \Gamma\} = G.$$

Thus whenever $Z(G) = (1)$ and $\beta(\Gamma) \subset G \rtimes \mathrm{Inn}(G)$, we may describe β, and in particular the function $\pi_1\beta : \Gamma \to G$, in terms of the homomorphisms $\beta_1, \beta_2 : \Gamma \to G$, namely,

$$\pi_1\beta(\gamma) = \beta_1(\gamma)\beta_2(\gamma)^{-1}.$$

A class of groups G where $Z(G) = (1)$ and $\beta(\Gamma) \subset G \rtimes \mathrm{Inn}(G)$ is the class of complete groups, that is, finite groups G with $Z(G) = (1)$ and $O(G) = (1)$. The best-known examples of finite complete groups are $\mathrm{Aut}(A)$ where A is simple and non-abelian, S_n for $n \geq 3, n \neq 6$, and $\mathrm{Hol}(Z_m)$ where m is odd. (See [Sch65, III.4.u-w] .) Another class is the class of simple groups, for if G is simple, then $O(G)$ is solvable, so any $\beta : G \to \mathrm{Hol}(G)$ has image in $G \rtimes \mathrm{Inn}(G)$.

In [CC99] we let $\Gamma = G$ and determined $e(G, G)$, the number of regular embeddings of G to $\mathrm{Hol}(G)$, when G is simple non-abelian or $S_n, n \geq 4$. In the next

section we examine the case where $\Gamma = G = \mathrm{Hol}(Z_q)$ where $q = p^e$ and p is an odd prime.

2. $\mathrm{Hol}(Z_{p^e})$

Let $G = Z_{p^e} \rtimes Z_{p^e}^*$, the holomorph of Z_{p^e}. Let b be a number $< p^e$ that generates $Z_{p^e}^*$. Let $\Gamma = G$. In this section we prove:

Theorem 2.1. *If $G = \mathrm{Hol}(Z_{p^e})$, p odd, then up to equivalence there are*

$$e(G,G) = 2p^{e-1}\phi(p^{e-1}) + 2p^e\phi(p^{e-1})(\phi(p-1)-1)$$

regular embeddings of G into $\mathrm{Hol}(G)$. Thus $e(G,G)$ is the number of H-Hopf Galois structures on a Galois extension L/K with Galois group G where the associated group of H is G.

Proof. We wish to find equivalence classes of regular embeddings of G in $\mathrm{Hol}(G)$. Since G is complete, we know from the last section that any homomorphism $\beta : G \to \mathrm{Hol}(G)$ may be decomposed as

$$\beta(g) = \beta_1(g)\beta_2(g)^{-1}C(\beta_2(g))$$

for homomorphisms $\beta_1, \beta_2 : G \to G$. So we begin by describing the homomorphisms from G to G.

Let $\alpha : G \to G$ be a homomorphism. Then α is determined by

$$\alpha(1,1) = (m,c) \text{ of order dividing } p^e, \text{ and}$$
$$\alpha(0,b) = (n,d) \text{ of order dividing } p^{e-1}(p-1).$$

If $\alpha(1,1)$ has order dividing p^e, then $c = 1$. To see this, first note that for any $s > 0$,

$$(m,c)^s = (m(1 + c + c^2 + \ldots c^{s-1}), c^s)$$

so c must have order dividing p^e, which implies that $c \equiv 1 \pmod{p}$. Also, for $\alpha(0,b)$ to have order dividing $p^{e-1}(p-1)$ we require that $d \not\equiv 1 \pmod{p}$ or p divides n. For if $d \equiv 1 \pmod{p}$ one sees by induction that $(n,d)^{p^{e-1}} = (p^{e-1}n', 1)$ where p divides n' iff p divides n. Thus if p does not divide n, then (n,d) has order p^e. On the other hand, if $d \not\equiv 1 \pmod{p}$, then

$$(n,d)^{p-1} = \left(n\left(\frac{d^{p-1}-1}{d-1}\right), d^{p-1}\right)$$

and p divides $d^{p-1} - 1$ but not $d - 1$, so the order of (n,d) divides $p^{e-1}(p-1)$.

Now we check the relation

$$(b,1)(0,b) = (b,b) = (0,b)(1,1).$$

Applying α yields:

$$(m(1 + c + \ldots c^{b-1}), c^b)(n,d) = (n,d)(m,c),$$

hence

$$(m(1 + c + \ldots c^{b-1}) + c^b n, c^b d) = (n + dm, dc).$$

Thus $c^b d = cd$. Since d is a unit modulo p^e it follows that $c^b = c$, hence $c^{b-1} = 1$. But since $c = 1 + pf$ for some f,

$$1 = (1 + pf)^{b-1}.$$

Since $b-1$ is relatively prime to p and $(1+pf)^{p^{e-1}}=1$, it follows that $1+pf=1$, hence $f=0$ and $c=1$.

Thus for any homomorphism $\alpha: G \to G$,

$$\alpha(1,1)=(m,1)$$

for some m.

Since $c=1$, the requirement

$$(m(1+c+\ldots c^{b-1})+c^b n, c^b d)=(n+dm, dc)$$

becomes

$$(mb+n,d)=(n+dm,d)$$

which implies that $bm=dm$. Thus if $m\neq 0$, then $b\equiv d \pmod p$, and if m is a unit (i.e. relatively prime to p), then $b=d$. In the latter case, $\alpha(1,1)=(m,1)$ has order p^e and $\alpha(0,b)=(n,b)$ has order $p^{e-1}(p-1)$.

Clearly if α is an automorphism then m is relatively prime to p and so $b=d$. Conversely, if $\alpha(1,1)=(m,1)$ with m relatively prime to p, then $\alpha(0,b)=(n,b)$ for some n. Conjugating α by (h,c) in G yields

$$\begin{aligned}(h,c)\alpha(1,1)(h,c)^{-1} &= (h,c)(m,1)(-c^{-1}h,c^{-1})\\ &= (h+cm-h,1)\\ &= (cm,1).\end{aligned}$$

We choose c so that $cm=1$. Then we choose h so that

$$\begin{aligned}(0,b)=(h,c)\alpha(0,b)(h,c)^{-1} &= (h,c)(n,b)(-c^{-1}h,c^{-1})\\ &= (h+cn,bc)(-c^{-1}h,c^{-1})\\ &= (h+cn-bh,b)\\ &= ((1-b)h+cn,b):\end{aligned}$$

we set $h=-(1-b)^{-1}cn$, possible because b has order $p^{e-1}(p-1) \pmod{p^e}$ and hence $b\not\equiv 1 \pmod p$. With these choices of h and c, the homomorphism $C(h,c)\alpha: G\to G$ is the identity on the generators $(1,1)$ and $(0,b)$ of G, and so $\alpha=C(h,c)^{-1}$ is an automorphism of G.

Now we ask about regularity: for which pairs of endomorphisms (β_1,β_2) is

$$\{\beta_1(g)\beta_2(g)^{-1}|g\in G\}=G,$$

or equivalently, $\pi_1\beta=\beta_1\cdot\beta_2^{-1}$ is a 1-1 function from G to G? Let $\beta_i(1,1)=(m_i,1), \beta_i(0,b)=(n_i,d_i)$ for $i=1,2$.

If neither β_1 nor β_2 is an automorphism, then p divides m_1 and m_2, so

$$\begin{aligned}\beta_1(p^{e-1}l,1)\beta_2(p^{e-1}l,1)^{-1} &= (p^{e-1}lm_1,1)(-p^{e-1}lm_2,1)\\ &= (0,1)(0,1)=(0,1)\end{aligned}$$

for all l, and so $\beta_1\cdot\beta_2^{-1}$ is not 1-1.

Suppose both β_1 and β_2 are automorphisms. If $m_1\equiv m_2 \pmod p$ then

$$\begin{aligned}\beta_1\cdot\beta_2^{-1}(p^{e-1},1) &= (p^{e-1}m_1-p^{e-1}m_2,1)\\ &= (0,1)\\ &= \beta_1\cdot\beta_2^{-1}(0,1)\end{aligned}$$

so $\beta_1 \cdot \beta_2^{-1}$ is not 1-1. If $m_1 \not\equiv m_2 \pmod{p}$, then let $s(m_1 - m_2) = n_1 - n_2$. Then

$$\begin{aligned}\beta_1 \cdot \beta_2^{-1}(0,b) &= (n_1 - n_2, 1)\\ &= ((m_1 - m_2)s, 1)\\ &= \beta_1 \cdot \beta_2^{-1}(s,1),\end{aligned}$$

so again, $\beta_1 \cdot \beta_2^{-1}$ is not 1-1.

Thus for β to be regular, exactly one of β_1 and β_2 is an automorphism.

We return to looking at regularity after we look at equivalence by $\mathrm{Aut}(G) = \mathrm{Inn}(G)$ inside $\mathrm{Hol}(G)$.

For $g, h, k \in G$ we have

$$\begin{aligned}(1, C(g))(h, C(k))(1, C(g)^{-1}) &= (C(g)(h), C(g)C(k)C(g)^{-1})\\ &= (ghg^{-1}, C(gkg^{-1}).\end{aligned}$$

Thus if $\beta(x) = (\beta_1(x)\beta_2(x)^{-1}, C(\beta_2(x)))$ for $x \in G$, then $\beta \sim \beta'$ with

$$\begin{aligned}\beta'(x) &= (g\beta_1(x)\beta_2(x)^{-1}g^{-1}, C(g\beta_2(x)g^{-1}))\\ &= (g\beta_1(x)g^{-1} \cdot (g\beta_2(x)g^{-1})^{-1}, C(g\beta_2(x)g^{-1})) :\end{aligned}$$

we get from β to β' by simultaneously conjugating β_1 and β_2 by $g \in G$.

Assume β_2 is an automorphism, then, up to equivalence, we may assume that β_2 is the identity automorphism on G and β_1 is not an automorphism. Then $e(G,G)$ will be twice the number of possible β_1, since the case where β_1 is an automorphism and β_2 is not is the same.

Returning to the regularity question, we ask, for which β_1 is $\{\beta_1(g)g^{-1}\} = G$?

Assume

$$\begin{aligned}\beta_1(1,1) &= (m,1)\\ \beta_1(0,b) &= (n,d)\end{aligned}$$

for some m divisible by p, some $d \neq 1$ and some n. Then

$$\begin{aligned}\beta_1(l,b^k) &= \beta_1(l,1)\beta_1(0,b^k)\\ &= (lm,1)\left(n\left(\frac{d^k-1}{d-1}\right), d^k\right)\\ &= \left(lm + n\left(\frac{d^k-1}{d-1}\right), d^k\right).\end{aligned}$$

For any h, r we want to find l, k so that

$$(*)\qquad \begin{aligned}\beta_1(l,b^k)(l,b^k)^{-1} &= \left(lm + n\left(\frac{d^k-1}{d-1}\right), d^k\right)(-b^{-k}l, b^{-k})\\ &= \left(lm + n\left(\frac{d^k-1}{d-1}\right) - d^k b^{-k} l, d^k b^{-k}\right)\\ &= (h, b^r).\end{aligned}$$

In order that for any r, there is a k so that $b^r = (db^{-1})^k$, we require that db^{-1} generates $Z_{p^e}^*$. Now for β_1 to be a homomorphism, we need $bm = dm$, and this is possible only if $m = 0$ or $b \equiv d \pmod{p}$. But in the latter case, $db^{-1} \equiv 1 \pmod{p}$, so cannot generate $Z_{p^e}^*$. Thus if $\{\beta_1(g)g^{-1}\} = G$, then $m = 0$, and $d = b^{f+1}$ such that b^f generates $Z_{p^e}^*$.

Thus β_1 is defined by

$$\beta_1(1,1) = (0,1)$$
$$\beta_1(0,b) = (n,d),$$

and $(*)$ becomes

$$(n(1+d+\cdots+d^{k-1}) - b^{fk}l, b^{fk}) = (h, b^r),$$

which is solvable for all n and for all f such that b^f generates $Z_{p^e}^*$. We have two cases:

If $d = b^{f+1} \equiv 1 \pmod{p}$, then $p-1$ divides $f+1$ and p divides n (or else β is not a homomorphism).

If $d = b^{f+1} \not\equiv 1 \pmod{p}$, then n is arbitrary.

The first case gives p^{e-1} choices for n and $\phi(p^{e-1})$ choices for f.

The second case gives p^e choices for n and

$$\phi(p^{e-1}(p-1)) - \phi(p^{e-1}) = \phi(p^{e-1})(\phi(p-1)-1)$$

choices for f. The theorem follows. □

Corollary 2.2. *If $G = Hol(Z_p)$, then $e(G,G) = 2(1+p(\phi(p-1)-1))$.*

Example 2.3. For $p=5$ there are, up to equivalence, $2(1+5(2-1)) = 12$ regular embeddings of $G = Z_5 \rtimes Z_5^*$ into $\mathrm{Hol}(G)$. If we choose $b=2$ then b and b^3 generate Z_5^*, so $d = b^0 = 1$ or $d = b^2 = 4$. Thus if we let β_2 be the identity automorphism, then $\beta_1(1,1) = (0,1)$ and $\beta_1(0,2) = (n,4)$, $n = 0,1,2,3,4$, or $(0,1)$.

3. Groups of order $p(p-1)$

Let $\Gamma = \mathrm{Hol}(Z_p)$ with p an odd prime, as above, and let $p-1 = 2q$. Then there are at least five non-isomorphic groups G of order $2qp$ other than Γ, namely, $Z_{2qp}, D_{qp}, D_p \times Z_q, D_q \times Z_p$, and $(Z_p \rtimes Z_q) \times Z_2$ (where Z_q is identified as the subgroup of $\mathrm{Aut}(Z_p)$ of index 2, and D_n is the dihedral group of order $2n$). The five groups are non-isomorphic because their centers have orders $2pq, 1, q, p$ and 2 respectively.

If q is also an odd prime, then q is called a Sophie Germain prime, resp. p is called a safeprime, and in that case, these five groups, together with $\Gamma = \mathrm{Hol}(Z_p)$, are the only groups of order $2pq$, up to isomorphism. To see this, we first obtain the following lemma, needed also in the next section:

Lemma 3.1. *Let p be prime, $p = 2q+1$. Then*

$$\mathrm{Aut}(D_p) = \mathrm{Aut}(Z_p \rtimes Z_q) = \mathrm{Aut}(\mathrm{Hol}(Z_p)) = \mathrm{Inn}(\mathrm{Hol}(Z_p)).$$

Proof. Let $G = Z_p \rtimes Z_a$ with $a = 2, q$ or $2q = p-1$. Write Z_p additively and view Z_a as the cyclic subgroup of order a inside $Z_p^* = \mathrm{Aut}(Z_p)$ and $G \subset Hol(Z_p)$. Let b generate Z_a. If α is an automorphism of G, then:

1. $\alpha(1,1) = (m,1)$ for p not dividing m, and
2. $\alpha(0,b) = (n,b)$ for any n (as one sees by applying α to the relation $(b,1)(0,b) = (b,b) = (0,b)(1,1)$.)

So there are $p(p-1) = |\mathrm{Hol}(Z_p)|$ automorphisms of G. Now if (l,d) is any element of $\mathrm{Hol}(Z_p)$, then conjugation by (l,d) is an automorphism of G, since

$$(l,d)(m,b^r)(l,d)^{-1} = (l+dm-b^rl, b^r) \in G.$$

Hence the conjugation map $C : \mathrm{Hol}(Z_p) \to \mathrm{Aut}(G)$,

$$C(l,d)(m,b^r) = (l,d)(m,b^r)(l,d)^{-1} = (l + dm - b^r l, b^r),$$

is defined. Then C is 1-1. For if $C(l_1,d_1) = C(l_2,d_2)$ on G, then

$$l_1 + d_1 m - b^r l_1 = l_2 + d_2 m - b^r l_2$$

for all m, r: in particular for $m = 1, r = 0$ we get $d_1 = d_2$ and for $m = 0, r = 1$ we get $l_1 = l_2$. Thus C is an isomorphism. □

Proposition 3.2. *If q and $p = 2q + 1$ are odd primes, then, up to isomorphism, there are exactly six groups of order $p(p-1)$.*

This is probably well-known, but we sketch a proof for the reader's convenience.

Proof. If G has order $p(p-1)$ then by the first Sylow Theorem, G has a unique normal subgroup G_p of order p. By Schur's Theorem, G_p has a complementary subgroup of order $2q$, and hence a subgroup K of order q. Then $G_pK = J$ is a subgroup of G of order pq, hence normal in G. By Schur's Theorem again, J has a complementary subgroup of order 2 in G, so G is isomorphic to a semidirect product $J \rtimes_\alpha Z_2$.

If $J \cong Z_{pq}$ then $G \cong Z_{pq} \rtimes_\alpha Z_2$ where

$$\alpha : Z_2 \to \mathrm{Aut}(Z_{pq}) \cong Z_{p-1} \times Z_{q-1}$$

has four possibilities, $\alpha(-1) = (\pm 1, \pm 1)$. These yield $G \cong D_{pq}, D_p \times Z_q, D_q \times Z_p$ and Z_{2pq}.

If $J \cong Z_p \rtimes Z_q \subset \mathrm{Hol}(Z_p)$, then $G \cong J \rtimes_\alpha Z_2$ where $\alpha : Z_2 \to \mathrm{Aut}(Z_p \rtimes Z_q) \cong \mathrm{Inn}(\mathrm{Hol}(Z_p))$. If α is trivial, we obtain $(Z_p \rtimes Z_q) \times Z_2$. Otherwise, the elements of order 2 in $\mathrm{Inn}(\mathrm{Hol}(Z_p)_)$ are of the form $C(l,-1)$ for any $l \in Z_p$. Define

$$\alpha_l : Z_2 \to \mathrm{Inn}(\mathrm{Hol}(Z_p))$$

by $\alpha_l(-1) = C(l,-1)$. One checks easily that

$$(Z_p \rtimes Z_q) \rtimes_{\alpha_0} Z_2 \cong Z_p \rtimes Z_{2q} = \mathrm{Hol}(Z_p)$$

by the map sending $((a,b),\epsilon)$ to $(a, \epsilon b)$ for $a \in Z_p$, $b \in Z_q \subset Z_{p-1}$, $\epsilon \in Z_2 \subset Z_{p-1}$. Now $\langle \alpha_0 \rangle = \langle C(0,-1) \rangle$ and $\langle \alpha_l \rangle = \langle C(l,-1) \rangle$ are conjugate in $\mathrm{Inn}(\mathrm{Hol}(Z_p))$ for $l \neq 0$ by $C(m,1)$ where $2m \equiv l \pmod p$: $C(m,1)C(0,-1)C(-m,1) = C(2m,-1)$. It follows from [DF99], p. 186, Exercise 6 that

$$(Z_p \rtimes Z_q) \rtimes_{\alpha_l} Z_2 \cong (Z_p \rtimes Z_q) \rtimes_{\alpha_0} Z_2$$

for all l. Thus $J = Z_p \rtimes Z_q$ yields only two possible groups, up to isomorphism. □

4. Nonuniqueness

If we begin with the Galois group Γ of a Galois extension L/K of fields, then to determine the K-Hopf Galois structures on L, we need to count equivalence classes of regular embeddings of Γ into $\mathrm{Hol}(G)$, where G varies over isomorphism classes of groups of the same cardinality as Γ. This can be a formidable task for certain cardinalities!

In this section, we let $\Gamma = \mathrm{Hol}(Z_p)$, $p = 2q + 1$ a safeprime > 5, and determine $e(\Gamma, G)$, the number of regular embeddings of Γ into $\mathrm{Hol}(G)$, for all six groups G of order $p(p-1) = 2pq$. We did the case $G = \Gamma$ in Theorem 2.1 and found that $e(G,G) = 2 + 2p(q-2)$. Here is the result for $G \ncong \Gamma$:

Theorem 4.1. *Let $\Gamma = \mathrm{Hol}(Z_p)$, with p and $q = (p-1)/2$ odd primes. Then:*

(1) $e(\Gamma, Z_p \rtimes Z_q \times Z_2) = 2p(q-1)$;
(2) $e(\Gamma, D_q \times Z_p) = 2p$;
(3) $e(\Gamma, D_p \times Z_q) = 2p$;
(4) $e(\Gamma, Z_{2qp}) = p$;
(5) $e(\Gamma, D_{pq}) = 4p$.

Proof. We do each case in turn, following the steps outlined in Section 1.

(1): Proof that $e(\Gamma, Z_p \rtimes Z_q \times Z_2) = 2p(q-1)$. Using Lemma 3.1 we have

$$\begin{aligned}\mathrm{Hol}(Z_p \rtimes Z_q \times Z_2) &= \mathrm{Hol}(Z_p \rtimes Z_q) \times \mathrm{Hol}(Z_2)\\ &= ((Z_p \rtimes Z_q) \rtimes \mathrm{Inn}(\mathrm{Hol}(Z_p)) \times Z_2\\ &\subset (\mathrm{Hol}(Z_p) \rtimes \mathrm{Inn}(\mathrm{Hol}(Z_p)) \times Z_2\\ &\cong \mathrm{Hol}(Z_p) \times \mathrm{Hol}(Z_p) \times Z_2;\end{aligned}$$

thus we may unwind any homomorphism $\beta : \Gamma \to ((Z_p \rtimes Z_q) \rtimes \mathrm{Inn}(\mathrm{Hol}(Z_p)) \times Z_2$ as in Section 1. If

$$\beta(\gamma) = ((m, b^{2r}), C(l, b^s)) \times \epsilon$$

with $\epsilon = \pm 1, Z_p^* = \langle b \rangle$ and m, l are modulo p, then $\beta(\gamma)$ maps to $(m, b^{2r})(l, b^s) \times (l, b^s) \times \epsilon$ under the map to $\mathrm{Hol}(Z_p) \times \mathrm{Hol}(Z_p) \times Z_2$. So β induces homomorphisms $\beta_1 : \Gamma \to \mathrm{Hol}(Z_p)$, defined by $\beta_1(\gamma) = (m, b^{2r})(l, b^s)$, and $\beta_2 : \Gamma \to \mathrm{Hol}(Z_p)$, defined by $\beta_2(\gamma) = (l, b^s)$. If we define $\beta_0 : \Gamma \to Z_2$ by $\beta_0(\gamma) = \epsilon$, then

$$\beta(\gamma) = (\beta_1(\gamma)\beta_2(\gamma)^{-1}, C(\beta_2(\gamma)) \times \beta_0(\gamma).$$

Let $\gamma \in \mathrm{Hol}(Z_p), \gamma = (m, b^t)$. Then the only non-trivial homomorphism β_0 is given by $\beta_0(\gamma) = -1$ if t is odd, and $= 1$ if t is even. (If $\beta_0(\gamma) = 1$ for all γ, then β will not be regular.) As for the possibilities for the homomorphisms β_1 and β_2, we determined these in the proof of Theorem 2.1, namely:

1. If β_i is an automorphism, then $\beta_i(1,1) = (m, 1)$, $m \neq 0$ and $\beta_i(0, b) = (n, b)$ for any n.
2. If β_i is not an automorphism, then $\beta_i(1,1) = (0,1)$ and $\beta_i(0, b) = (n, d)$ for $d = b^r$, $r \neq 0$, and any n, or $\beta_i(0, b) = (0, 1)$.

As in the proof of Theorem 2.1, if both β_1 and β_2 are not automorphisms, or if both β_1 and β_2 are automorphisms, then $\beta_1 \cdot \beta_2^{-1}$ is not 1-1, so β is not regular. Thus we can assume one is an automorphism and the other not. Assuming β_2 is an automorphism, we can conjugate it by an automorphism of $\mathrm{Hol}(Z_p)$ to transform it to the identity map. Then

$$\begin{aligned}\beta_1(0, b)\beta_2(0, b)^{-1} &= (n, d)(0, b)^{-1}\\ &= (n, db^{-1}) :\end{aligned}$$

this must lie in $Z_p \rtimes Z_q$, which means that $d = b^r$ must be an odd power of b. Then

$$\begin{aligned}\beta_1 \cdot \beta_2^{-1}(l, b^s) &= (n, d)^s (l, b^s)^{-1}\\ &= \left(n \left(\frac{d^s - 1}{d - 1} \right) - l(db^{-1})^s, (db^{-1})^s \right).\end{aligned}$$

For β to be regular, $\beta_1 \cdot \beta_2^{-1}$ must map onto $Z_p \rtimes Z_q$, so we need that $db^{-1} = b^{r-1}$ generates Z_q. Thus $r - 1$ must be coprime to q. There are $q - 1$ odd numbers $r < p$ with $r - 1$ coprime to q.

For any such r, $(db^{-1})^s$ is a unit of Z_p, so given any n, h in Z_p there is some l in Z_p so that $n\left(\frac{d^s-1}{d-1}\right) - l(db^{-1})^s = h$. Hence for any suitable r and any n, $\beta_1 \cdot \beta_2^{-1}$ maps $\mathrm{Hol}(Z_p)$ onto $Z_p \rtimes Z_q$.

Thus we have determined all regular β: we have p choices for n, and $q-1$ choices for d. Interchanging the roles of β_1 and β_2 yields the same result. Thus there are $2p(q-1)$ regular embeddings of $\mathrm{Hol}(Z_p)$ into $\mathrm{Hol}(Z_p \rtimes Z_q \times Z_2)$, as claimed.

(2): Proof that $e(\Gamma, D_q \times Z_p) = 2p$. We seek regular embeddings

$$\beta : \Gamma \to \mathrm{Hol}(D_q \times Z_p).$$

We have

$$\mathrm{Hol}(D_q \times Z_p) \cong \mathrm{Hol}(D_q) \times \mathrm{Hol}(Z_p)$$

and by Lemma 3.1, the map

$$\mathrm{Hol}(D_q) \cong D_q \rtimes \mathrm{Inn}(\mathrm{Hol}(Z_q)) \to \mathrm{Hol}(Z_q) \times \mathrm{Hol}(Z_q)$$

is 1-1 and maps $(m,\epsilon)C(n,d)$ to $(m,\epsilon)(n,d) \times (n,d)$. Suppose

$$\beta(1,1) = (q,\epsilon)C(n,d) \times (m,c).$$

Now $\beta(1,1)$ must have order p (or else β is not 1-1), so $(n,d) = (q,\epsilon) = (0,1)$, $c = 1$ and $m \neq 0$, hence

$$\beta(1,1) = (0,1)C(0,1) \times (m,1)$$

with $m \neq 0$.

Suppose $\beta(0,b) = (l,\epsilon)C(k,d) \times (s,c)$ in $D_q \rtimes \mathrm{Inn}(\mathrm{Hol}(Z_q)) \times \mathrm{Hol}(Z_p)$ for l, ϵ, k, d mod q and s, c mod p. If $\epsilon = 1$, then no element of D_q of the form $(*, -1)$ is hit by $\pi_1(\beta)$, and so β is not regular. Thus $\epsilon = -1$.

Applying β to the condition $(b,1)(0,b) = (0,b)(1,1)$ yields $c \equiv b \pmod{p}$. Hence (k,b) has order $p-1$. We require that $(n,-1)C(l,d)$ have order dividing $2q$ in $D_q \rtimes \mathrm{Inn}(\mathrm{Hol}(Z_q)$, which maps 1-1 to $\mathrm{Hol}(Z_q) \times \mathrm{Hol}(Z_q)$ as noted above. Thus $(n-l,-d)$ and (l,d) must have order 1, 2 or q in $\mathrm{Hol}(Z_q)$. But then $d = 1$ or -1.

Thus any regular embedding β satisfies:

1. $\beta(1,1) = (0,1)C(0,1) \times (m,1)$ with $m \neq 0$ in Z_p, and
2. $\beta(0,b) = (n,-1)C(l,d) \times (k,b)$ with $d = \pm 1$.

Now modify β by conjugating by

$$(0,1)C(h,c) \times (0,b^r) \in \mathrm{Aut}(D_q \times Z_p) \subset D_q \rtimes \mathrm{Inn}(\mathrm{Hol}(Z_q)) \times Hol(Z_p).$$

First, looking at $\beta(1,1)$:

$$\begin{aligned}((0,1)C(h,c) \times (0,b^r)))&((0,1)C(0,1) \times (m,1))((0,1)C(h,c) \times (0,b^r))^{-1}) \\ &= ((0,1)C(0,1) \times (b^r m, 1).\end{aligned}$$

Now, looking at $\beta(0,b)$:

$$\begin{aligned}((0,1)C(h,c) \times (0,b^r)))&((n,-1)C(l,d) \times (k,b))((0,1)C(h,c) \times (0,b^r))^{-1}) \\ &= (2h+cn,-1)C(cl+h-dh,d) \times (b^r k, b).\end{aligned}$$

Let β henceforth denote the conjugated embedding. Choose r so that $b^r m = 1$. Then

$$\beta(1,1) = (0,1)C(0,1) \times (1,1).$$

We choose h, c in

$$\beta(0,b) = (2h + cn, -1)C(cl + h(1-d), d) + (b^r k, b).$$

We have four possibilities.

If $d = 1$ and $l = 0$ we can choose $c \neq 0$ and h so that

$$\beta(0,b) = (0,-1)C(0,1) + (b^r k, b).$$

But then β is not regular, for $\pi_1\beta$ does not map onto D_q.

If $d = -1$ and $l = n$, then we can choose $c = 2, h = -n$, but then

$$\beta(0,b) = (0,-1)C(0,-1) + (b^r k, b),$$

so β is not regular.

If $d = 1$ and $l \neq 0$, choose $c \equiv l^{-1} \pmod q$ and h so that $2h + cn \equiv 0$, then

$$\beta(0,b) = (0,-1)C(1,1) + (b^r k, b).$$

If $d = -1$ and $l \neq n$, then we can choose $c, h \neq 0$ with

$$\begin{aligned} 2h + cn &= 0 \\ cl + 2h &= 1, \end{aligned}$$

giving

$$\beta(0,b) = (0,-1)C(1,-1) + (b^r k, b).$$

One verifies that

$$\begin{aligned} \beta(1,1) &= ((0,1)C(0,1) \times (1,1) \\ \beta(0,b) &= ((0,-1)C(1,\pm 1) \times (b^r k, b) \end{aligned}$$

is regular, for any k. There are p choices for k, and hence, up to equivalence, there are $2p$ regular embeddings of $\mathrm{Hol}(Z_p)$ into $\mathrm{Hol}(D_q \times Z_p)$: $e(\mathrm{Hol}(Z_p), D_q \times Z_p) = 2p$.

(3): Proof that $e(\Gamma, D_p \times Z_q) = 2p$. This argument is similar to the last case. We seek regular embeddings

$$\beta : \mathrm{Hol}(Z_p) \to \mathrm{Hol}(D_p \times Z_q) \cong \mathrm{Hol}(D_p) \times \mathrm{Hol}(Z_q).$$

We have

$$\mathrm{Hol}(D_p \times Z_q) \cong \mathrm{Hol}(D_p) \times \mathrm{Hol}(Z_q)$$

and by Lemma 3.1, the map

$$\mathrm{Hol}(D_p) \cong D_p \rtimes \mathrm{Inn}(\mathrm{Hol}(Z_p) \to \mathrm{Hol}(Z_p) \times \mathrm{Hol}(Z_p)$$

is 1-1 and maps $(m,\epsilon)C(n,d)$ to $(m,\epsilon)(n,d) \times (n,d)$.

Suppose $\beta(1,1) = (m,\epsilon)C(n,d) \times (l,c)$. Then $\beta(1,1)$ must have order p, so (n,d) and $(m + \epsilon n, \epsilon d)$ have order dividing p. This implies $d = \epsilon = 1$. Also (l,c) has order dividing p in $\mathrm{Hol}(Z_q)$, so $(l,c) = (0,1)$. Thus

$$\beta(1,1) = (m,1)C(n,1) \times (0,1)$$

with m or $n \not\equiv 0 \pmod p$.

Suppose $\beta(0,b) = (l,\epsilon)C(k,d) \times (s,c)$, of order $2q$. Then $\epsilon = -1$ or else β is not regular. Also, (s,c) must have order dividing $2q$ in $\mathrm{Hol}(Z_q)$. But since β is regular, we must have $(t,*)$ in the image of β for all t in Z_q, so $c = 1$ and $s \neq 0$.

Applying β to the relation $(b,1)(0,b) = (0,b)(1,1)$ yields

$$((bm,1)C(bn,1) \times (0,1))((l,-1)C(k,d) \times (s,1)) \\ = ((l,-1)C(k,d) \times (s,1))((m,1)C(n,1) \times (0,1)).$$

This yields no condition on s, but on the left components we obtain

$$(bm + 2bn + l, -1)C(bn + k, d) = (l - dm, -1)C(dn + k, d).$$

Thus

$$2bn + bm = -dm$$
$$bn = dn.$$

If $n \neq 0$, then $b = d$ and $n = -m$. If $n = 0$, then $d = -b$. Thus

$$\beta(1,1) = (m,1)C(-m,1) \times (0,1)$$
$$\beta(0,b) = (l,-1)C(k,b) \times (s,1),$$

or

$$\beta(1,1) = (m,1)C(0,1) \times (0,1)$$
$$\beta(0,b) = (l,-1)C(k,-b) \times (s,1).$$

One then sees easily that $\beta(0,b)$ has order dividing $2q$.

Now we modify β by an automorphism of $D_p \times Z_q$.

If we conjugate the right factors by $(0,s^{-1})$ in $\mathrm{Aut}(Z_q)$, then $(s,1)$ is transformed into $(1,1)$.

If we conjugate the left factors by $(0,1)C(g,c)$ in $\mathrm{Aut}(D_p)$, then

$$(m,1)C(n,1) \text{ becomes } (cm,1)C(cn,1)$$

and

$$(l,-1)C(k,\pm b) \text{ becomes } (2g + cl, -1)C(g + ck \mp bg, \pm b).$$

Choose c so that $cm = 1$. Then $cn = 0$ or -1.

Choose g so that $2g + cl = 0$. Then we have the following representatives of equivalence classes of β:

$$\beta(1,1) = (1,1)C(-1,1) \times (0,1)$$
$$\beta(0,b) = (0,-1)C(k,b) \times (1,1),$$

and

$$\beta(1,1) = (1,1)C(0,1) \times (0,1)$$
$$\beta(0,b) = (0,-1)C(k,-b) \times (1,1).$$

It is a routine check that for any k modulo p, both β are regular Thus we have $2p$ equivalence classes of regular embeddings of $\mathrm{Hol}(Z_p)$ into $\mathrm{Hol}(D_p \times Z_q)$.

(4): Proof that $e(\Gamma, Z_{2qp}) = p$. Let

$$\beta : \mathrm{Hol}(Z_p) \to \mathrm{Hol}(Z_{2pq}) \cong \mathrm{Hol}(Z_p) \times \mathrm{Hol}(Z_q) \times Z_2$$

be a regular embedding. Then $\beta(1,1)$ has order p, so

$$\beta(1,1) = (m,1) \times (0,1) \times 0$$

for some $m \not\equiv 0 \pmod{p}$. Also, $\beta(0,b)$ has order $p - 1 = 2q$, so

$$\beta(0,b) = (n,d) \times (l,1) \times e$$

with $d \not\equiv 1 \pmod{p}$. If $e \equiv 0 \pmod{2}$ or $l \equiv 0 \pmod{q}$ then β is not regular, hence we have $e \equiv 1 \pmod{2}$ and $l \not\equiv 0 \pmod{q}$.

The condition $(b,1)(0,b) = (0,b)(1,1)$ implies that $d \equiv b \pmod p$. Thus in $\mathrm{Hol}(Z_{2pq})$,

$$\begin{aligned}\beta(1,1) &= (2qm, 1)\\ \beta(0,b) &= (n,c)\end{aligned}$$

with p not dividing m, $2q$ not dividing n, and $c \equiv b \pmod p, c \equiv 1 \pmod{2q}$.

Now we consider β under equivalence by automorphisms of Z_{2pq}. We conjugate β by $(0,d)$ with d coprime to $2pq$:

$$\begin{aligned}(0,d)(2qm,1)(0,d^{-1}) &= (2dqm,1)\\ (0,d)(n,c)(0,d^{-1}) &= (dn,c).\end{aligned}$$

Choose d so that

$$\begin{aligned}dm &\equiv 1 \pmod p\\ dn &\equiv 1 \pmod{2q}.\end{aligned}$$

Then after conjugating, β becomes:

$$\begin{aligned}\beta(1,1) &= (2q,1)\\ \beta(0,b) &= (1+2ql,c).\end{aligned}$$

We check that β is regular for any l modulo p. We have

$$\begin{aligned}\beta(n,b^k) &= \beta(n,1)\beta(0,b)^k\\ &= (2qn,1)((1+2ql)(1+c+\cdots+c^{k-1}),c^k)\\ &= (2qn+(1+2ql)(1+c+\cdots+c^{k-1}),c^k).\end{aligned}$$

Let a be any element of Z_{2pq}. To solve

$$a \equiv 2qn + (1+2ql)(1+c+\cdots+c^{k-1}) \pmod{2pq}$$

for n and k it suffices to solve

$$\begin{aligned}a &\equiv 2qn + (1+2ql)(1+c+\cdots+c^{k-1}) \pmod p\\ a &\equiv 1+c+\cdots+c^{k-1} \equiv k \pmod{2q}.\end{aligned}$$

Clearly for each a modulo $2pq$ there are unique values for k,n that solve these congruences. Thus for any l, β is 1-1 and regular, and so $e(\mathrm{Hol}(Z_p), Z_{2pq}) = p$.

(5): Proof that $e(\Gamma, D_{pq}) = 4p$. Let $\beta : \mathrm{Hol}(Z_p) \to \mathrm{Hol}(D_{pq})$ be a regular embedding. We have

$$\mathrm{Hol}(D_{pq}) = D_{pq} \rtimes \mathrm{Inn}(\mathrm{Hol}(Z_{pq})) \to \mathrm{Hol}(Z_{pq}) \times \mathrm{Hol}(Z_{pq})$$

by $(m,\epsilon)C(n,d) \mapsto (m,\epsilon)(n,d) \times (n,d)$. Also,

$$\mathrm{Hol}(Z_{pq}) \cong \mathrm{Hol}(Z_p) \times \mathrm{Hol}(Z_q)$$

by $(l,c) \mapsto ((l,c)mod(p),(l,c)mod(q))$. Under this map, D_{pq} maps into $D_p \times D_q$.

Let $\beta(1,1) = (m,\epsilon)C(n,d)$, of order p. Then $\beta(1,1)$ maps to

$$(m+\epsilon d, \epsilon d) \times (n,d) \mod p, (m+\epsilon d, \epsilon d) \times (n,d) \mod q,$$

which must have order p. Hence

$$\begin{aligned}(m+\epsilon d, \epsilon d) &\equiv (0,1) \pmod q\\ (n,d) &\equiv (0,1) \pmod q\end{aligned}$$

and

$$\epsilon d \equiv d \equiv 1 \pmod{p}$$
$$n \text{ or } m + \epsilon n \not\equiv 0 \pmod{p}.$$

Let $\beta(0,b) = (l,\epsilon)C(k,c)$. By regularity we must have $\epsilon = -1$, or else $\pi_1(\beta)$ maps into $\{(*,1)\} \subset D_{pq}$. Then $\beta(0,b)$ maps to

$$(l-k,-c) \times (k,c) \mod p, (l-k,-c) \times (k,c) \mod q.$$

This has order $2q = p-1$, so we must have

$$c \equiv \pm 1 \pmod{q}.$$

From $(b,1)(0,b) = (0,b)(1,1)$ we obtain

$$(bqm,1)C(bqn,1)(l,-1)C(k,c) = (l,-1)C(k,c)(qm,1)C(qn,1),$$

hence

$$(bqm + 2bqn + l, C(k + bqn, c) = (l - cqm, -1)C(k + cqn, c)$$

and so

$$bqn = cqn$$
$$cqm = bqm + 2bqn.$$

This yields no conditions modulo q, but modulo p, we have:

1. If $n \not\equiv 0$, then $c = b$ and $m = -n$.
2. If $n \equiv 0$, then $c = -b$ and $m \not\equiv 0$.

Now we look for a nice representative for β modulo conjugation by elements of $\mathrm{Inn}(\mathrm{Hol}(Z_{pq}))$. For $(g,d) \in \mathrm{Hol}(Z_{pq})$,

$$\begin{aligned} C(g,d)\beta(1,1)C(g,d)^{-1} &= (g,d)(qm,1)(g,d)^{-1}C((g,d)(qn,1)(g,d)^{-1}) \\ &= (dqm,1)C(dqn,1), \\ C(g,d)\beta(0,b)C(g,d)^{-1} &= (g,d)(l,-1)(g,d)^{-1}C((g,d)(k,c)(g,d)^{-1}) \\ &= (2g+dl,-1)C(g+dk-cg,c). \end{aligned}$$

We may choose d and g modulo pq by choosing them modulo p and modulo q separately.

Modulo p:

1. If $n \not\equiv 0$, choose d so that $dqn \equiv -1$, then $dqm \equiv -dqn \equiv 1$ and $c \equiv b$.
2. If $n \equiv 0$, choose d so that $dqm \equiv 1$ and $c \equiv -b$.

Choose g so that $2g + dl \equiv 0$. Then, since $d \not\equiv 0$, $g - cg + dk$ is arbitrary, so (letting β now denote the conjugated embedding) we have, modulo p:

$$\beta(1,1) = (1,1)C(-1,1), \beta(0,b) = (0,-1)C(k,b)$$

or

$$\beta(1,1) = (1,1)C(0,1), \beta(0,b) = (0,-1)C(k,-b).$$

Modulo q:

$$\beta(1,1) = (0,1)C(0,1)$$
$$\beta(0,b) = (2g+dl,-1)C((1-c)g+dk,c)$$

where $c \equiv \pm 1$.

If $c \equiv 1$ and $k \not\equiv 0$, set $dk \equiv 1$ and

$$2g + dl \equiv 0.$$

Then

$$\beta(1,1) = (0,1)C(0,1)$$

and

$$\beta(0,b) = (0,-1)C(1,1)$$

or (if $k \equiv 0$)

$$\beta(0,b) = (0,-1)C(0,1).$$

However, in this last case, β is not regular: $\pi_1\beta$ maps to $\{(0,\pm 1)\} \subset \mathrm{Hol}(Z_q)$.

If $c \equiv -1$, we have

$$\beta(0,b) = (2g + dl, -1)C((2g + dk, -1).$$

If $l \equiv k$ we can choose g so that $2g + dk = 2g + dl \equiv 0$, but then β is not regular. Thus we must have $l \not\equiv k$, and then we may choose $d \neq 0$ and g so that

$$2g + dl \equiv 0$$
$$2g + dk \equiv 1$$

and so

$$\beta(1,1) = (0,1)C(0,1)$$

and

$$\beta(0,b) = (0,-1)C(-1,1).$$

To summarize, any regular embedding is equivalent to

$$\beta(1,1) = (1,1)C(-1,1), \quad \beta(0,b) = (0,-1)C(k,b)$$

or

$$\beta(1,1) = (1,1)C(0,1), \quad \beta(0,b) = (0,-1)C(k,-b)$$

modulo p and to

$$\beta(1,1) = (0,1)C(0,1), \quad \beta(0,b) = (0,-1)C(1,1)$$

or

$$\beta(1,1) = (0,1)C(0,1), \quad \beta(0,b) = (0,-1)C(-1,1)$$

modulo q.

We show that all four combinations give regular embeddings of $\mathrm{Hol}(Z_p)$ to $\mathrm{Hol}(D_{pq})$, and so, since k is arbitrary in Z_p, we have $4p$ equivalence classes of regular embeddings.

Note that in every combination,

$$\beta_1(l,b^r)\beta_2(l,b^r)^{-1} = (*,(-1)^r)$$

both modulo p and modulo q, and so $\beta_1 \cdot \beta_2^{-1}$ maps to $D_{pq} \subset \mathrm{Hol}(Z_p)$. To show regularity, we need only show that modulo p every element of D_p is in the image of $\beta_1 \cdot \beta_2^{-1}$, and similarly modulo q.

Mod p: If

$$\beta(1,1) = (1,1)C(-1,1), \quad \beta(0,b) = (0,-1)C(k,b)$$

modulo p, then

$$\beta_1(l,b^r)\beta_2(l,b^r)^{-1} = \left(-k\left(\frac{1-(-b)^r}{1+b}\right) + (-1)^r\left(-l + k\left(\frac{1-b^r}{1-b}\right)\right), (-1)^r\right)$$

and for r and l arbitrary we can obtain all elements $(m, \pm 1)$ of D_p.

If

$$\beta(1,1) = (1,1)C(0,1), \quad \beta(0,b) = (0,-1)C(k,-b)$$

modulo p then

$$\beta_1(l,b^r)\beta_2(l,b^r)^{-1} = \left(\left(l + (-k)\frac{1-b^r}{1-b}\right) + (-1)^r k\left(\frac{1-(-b)^r}{1+b}\right), (-1)^r\right)$$

and again for r and l arbitrary we can obtain all elements $(m, \pm 1)$ of D_p.

Mod q: If

$$\beta(1,1) = (0,1)C(0,1), \quad \beta(0,b) = (0,-1)C(1,1)$$

modulo q, then

$$\beta_1(l,b^r)\beta_2(l,b^r)^{-1} = \begin{cases} (-r,1) & \text{if } r \text{ is even,} \\ (-1+r,-1) & \text{if } r \text{ is odd.} \end{cases}$$

Since $0 \le r < 2q$ and we're working modulo q, we can obtain all elements $(m, \pm 1)$ of D_q.

If

$$\beta(1,1) = (0,1)C(0,1), \quad \beta(0,b) = (0,-1)C(-1,1)$$

modulo q, then

$$\beta_1(l,b^r)\beta_2(l,b^r)^{-1} = \begin{cases} (-r,1) & \text{if } r \text{ is even,} \\ (1-r,-1) & \text{if } r \text{ is odd.} \end{cases}$$

Again, since $0 \le r < 2q$ and we're working modulo q, we can obtain all elements $(m, \pm 1)$ of D_q.

Thus

$$\{\beta_1(l,b^r)\beta_2(l,b^r)^{-1}\} = \begin{cases} D_p & \text{modulo } p \\ D_q & \text{modulo } q, \end{cases}$$

and so all four combinations of β modulo p and modulo q are regular. This completes the proof that $e(\mathrm{Hol}(Z_p), D_{pq}) = 4p$. □

Combining Theorems 2.1 and 4.1 yields:

Corollary 4.2. a) *If L is a Galois extension of K, fields, with Galois group $\Gamma = \mathrm{Hol}(Z_p)$, $p > 5$ a safeprime, then for every group G of cardinality that of Γ, there is a H-Hopf Galois structure on L/K where the associated group of H is G.*

b) *The number of Hopf Galois structures on L/K is $2 + 3p + 4pq$.*

Remark 4.3. N. Byott [By03b] has obtained the analogous result to Corollary 4.2a) for both the cyclic group and the non-abelian group of order pq, p and q primes with q dividing $p-1$. His approach is not to determine regular embeddings of Γ into $\mathrm{Hol}(G)$ up to equivalence, but rather to determine the set of regular subgroups of $\mathrm{Hol}(G)$ whose intersection with $\mathrm{Aut}(G)$ is a given cardinality.

References

[By96] N. P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra 24 (1996), 3217–3228, MR 97j:16051a, Zbl 0878.12001; Corrigendum: Comm. Algebra 24 (1996), 3705, MR 97j:16051b.

[By03a] N. P. Byott, *Hopf-Galois structures on field extensions with simple Galois groups*, Bull. London Math. Soc. (to appear).

[By03b] N. P. Byott, *Hopf-Galois structures on Galois field extensions of degree pq*, preprint, 2003.

[CC99] S. Carnahan, L. Childs, *Counting Hopf Galois structures on non-abelian Galois field extensions*, J. Algebra 218 (1999), 81–92, MR 2000e:12010, Zbl 0988.12003.

[C95] L. Childs, *A Concrete Introduction to Higher Algebra*, 2nd edition, Springer Verlag, 1995, MR 96h:00002, Zbl 0841.00001.

[C00] L. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, Amer. Math. Soc. Math. Surveys and Monographs, vol. 80, 2000, MR 2001e:11116, Zbl 0944.11038.

[DF99] D. Dummit, R. Foote, *Abstract Algebra, Second Edition*, John Wiley & Sons, New York, 1999, MR 92k:00007, Zbl 0943.00001.

[Fe03] S. Featherstonhaugh, *Abelian Hopf Galois structures on Galois field extensions of prime power order*, Ph. D. thesis, University at Albany, August, 2003.

[GP87] C. Greither, B. Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra 106 (1987), 239–258, MR 88i:12006, Zbl 0615.12026.

[Ko98] T. Kohl, *Classification of the Hopf Galois structures on prime power radical extensions*, J. Algebra 207 (1998), 525–546, MR 99g:16049, Zbl 0953.12003.

[Sch65] E. Schenkman, *Group Theory*, Princeton, Van Nostrand, 1965, MR 57 #416, Zbl 0133.27302.

Department of Mathematics and Statistics, University at Albany, Albany, NY 12222
lc802@math.albany.edu http://math.albany.edu:8000/~lc802/

This paper is available via http://nyjm.albany.edu:8000/j/2003/9-8.html.