HOPF GALOIS STRUCTURES ON GALOIS EXTENSIONS OF FIELDS OF DEGREE mp

LINDSAY N. CHILDS

ABSTRACT. Let Γ be a group of order mp where p is prime and $m < p$. T. Kohl has shown that regular subgroups of $Perm(\Gamma)$ normalized by the image $\lambda(\Gamma)$ of the left regular representation λ lie in the normalizer in $Perm(\Gamma)$ of the p-Sylow subgroup $\mathcal{P}$ of $\lambda(\Gamma)$. These regular subgroups correspond by Galois descent to Hopf Galois structures on a Galois extension of fields with Galois group Γ. We describe Kohl's group and outline how to compute regular subgroups isomorphic to M when Γ and M are semidirect products $C_p \rtimes C_m$ of cyclic groups, and indicate connections with previous work on Hopf Galois structures obtained by other methods. Details are in a manuscript currently being revised.

1. Definitions and previous work

1969-1986. Chase and Sweedler [CS69] defined the concept of Hopf Galois extension. (Its scheme-theoretic translation is that of a principal homogeneous space for a group scheme.) For field extensions it generalizes the notion of a Galois extension of fields: let K be a field, L a finite field extension of K with $[L : K] = n$, H a cocommutative K-Hopf algebra, and suppose H acts on L making L an H-module algebra. Then L/K is an H-Galois extension if the dual $\gamma : L \to L \otimes_K H^*$ of the action $H \otimes_K L \to L$ yields an isomorphism $\alpha : L \otimes_K L \to L \otimes_K H^*$ by $\alpha(a \otimes b) = (a \otimes 1)\gamma(b)$.

It follows that $dim_K(H) = n = dim_K(L)$.

For a classical Galois extension L/K with Galois group Γ, $H = K\Gamma$ and α becomes the splitting isomorphism

$$L \otimes_K L \cong LG^*.$$

Chase and Sweedler [CS69] and Sweedler [Sw69] gave as an example a primitive purely inseparable exponent n field extension. But Chase, at least, was interested in doing purely inseparable Galois theory, and by the time of [Ch81], he had decided that a Hopf algebra H whose dimension over K is equal to $[L : K]$ was not large enough. Hence

Date: May 22, 2013.

his purely inseparable Galois theory of [Ch81], c.f. [Ch84], used a truncated automorphism scheme, represented by a K-Hopf algebra of dimension n^n.

The subject lay dormant for 18 years.

1987. Instead of looking at purely inseparable field extensions, Greither and Pareigis [GP87] looked at separable extensions, and showed thatthere exist non-trivial Hopf Galois structures for separable field extensions. In fact, every Galois extension with non-abelian Galois group has at least two Hopf Galois structures, one by the group ring of the Galois group, the other by the Hopf algebra $H_\lambda = L[\Gamma]^\Gamma$, where Γ acts on L via the Galois action and on Γ by conjugation (a non-trivial action if Γ is non-abelian). They showed that for finite Galois extensions of fields with Galois group Γ, Hopf Galois structures are bijective with regular subgroups M of $Perm(\Gamma)$ normalized by $\lambda(\Gamma)$, as follows:

If H acts on L making L/K a Hopf Galois extension, then $L \otimes_K H$ acts on $L \otimes_K L \cong L\Gamma^*$ making the right side an $L \otimes_K H$-Galois extension. It turns out that L-Hopf algebras that can make $L\Gamma^*$ a Hopf Galois extension of L must have the form LM where M is a regular group of permutations of the standard basis $\{e_\gamma\}$ of $L\Gamma^*$. Greither and Pareigis showed that Galois descent yields a bijection between Hopf Galois structures on L/K and regular subgroups M of $Perm(\Gamma)$ normalized by $\lambda(\Gamma)$.

For a set of groups $\{N\}$ representing isomorphism types of groups of order $|\Gamma|$, if $M \cong N$ we say H has *type* N.

1.1. **Byott's translation.** ([Ch89]), [By96]: Let $R(\Gamma, [N])$ = set of regular subgroups of $Perm(\Gamma)$ isomorphic to N and normalized by $\lambda(\Gamma)$. In [By96] Byott formalized the germ of an idea from [Ch89] to show that $R(\Gamma, [N])$ is bijective with the set of regular embeddings β of Γ into $Hol(N) \cong \rho(N) \rtimes Aut(N)$, modulo equivalence by conjugating $\beta(\Gamma)$ by automorphisms of N ("Byott's translation"). (Here λ, ρ are the left (right) regular representations of Γ in $Perm(\Gamma)$.)

This idea enabled one to seek Hopf Galois structures on L/K with Galois group Γ and of type N by translating the problem from the large, complicated group $Perm(\Gamma)$ to the usually much smaller and friendlier group $Hol(N)$. Thus most results counting Hopf Galois structures have used Byott's translation. For example:

$|R(\Gamma, [\Gamma])| = 1$ iff $|\Gamma| = g$ and $(g, \phi(g)) = 1$ [By96]

$|R(S_n, [S_n])| > (n!)^{1/2}$ for $n \geq 5$ [CaC99]

$|R(\Gamma, [N])| = 2$ or $= 0$ for Γ simple, nonabelian, $N = \Gamma$ [CaC99] or $\neq \Gamma$ [By04b]

Γ a finite abelian p-group [Ko98], [By96], [By13], [Ch05], [Ch07], [FCC12]:

for example, $|R(C_{p^n}, [N])| = p^{n-1}$ or $= 0$ if $N \cong C_{p^n}$ or not [Ko98];

$|R(G, [N])| = 0$ if G, N are abelian p-groups and N has p-rank m with $m + 1 < p$ [FCC12].

Γ a semidirect product of abelian groups [By04a], [BC12], [Ch03], [Ch13], [CCo07]:

for example, there are non-abelian groups Γ so that $|R(\Gamma, [N]) > 0$ for every isomorphism type $[N]$, e. g. [Ch03].

$Hol(N)$ is much easier to work in than $Perm(\Gamma)$. But....

Given $\beta : \Gamma \to Hol(N)$ a regular embedding, let $b : \Gamma \to N$ by

$$b(\gamma) = \beta(\gamma)(1_N)$$

(β regular implies b is bijective, but b is rarely a homomorphism). The corresponding subgroup M of $Perm(\Gamma)$ is

$$M = C(b^{-1})\lambda(N) = \{b^{-1}\pi b | \pi \in \lambda(N)\}$$

The corresponding K-Hopf algebra acting on L is

$$H = LM^\Gamma$$

where Γ acts on M via conjugation by $\lambda(\Gamma)$. The Hopf algebra H is not so difficult to identify: see [Ch00, (7.7)]. But the action of H is harder: an element

$$\xi = \sum_{\eta \in N} s_\eta \eta$$

in H acts on L by

$$\xi(a) = \sum s_\eta b^{-1}(\eta^{-1})(a).$$

(Note b^{-1}!) For Γ cyclic of prime power order, describing b^{-1} involves the p-adic logarithm function. For more complicated groups, b^{-1} is mostly unstudied.

2. Kohl's work

Kohl [Ko13] , extending [Ko07] for $m = 4$: $|\Gamma| = mp$, p prime, $p > m$, $\mathcal{P}$ the p-Sylow subgroup of $\lambda(\Gamma)$. Then

Theorem 2.1. *Every regular subgroup N of $B = Perm(\Gamma)$ normalized by $\lambda(\Gamma)$ is contained in $Norm_B(\mathcal{P})$, the normalizer in B of $\mathcal{P}$.*

Big cardinality reduction:
for $mp = 28$, $|Perm(\Gamma)| = 28! \sim 3 \times 10^{29}$, while $|Norm_B(\mathcal{P})| = 7^4 \cdot 6 \cdot 4! < 4 \times 10^5$.

Big structural improvement:

$$Norm_B(\mathcal{P}) \cong \mathbb{F}_p^m \rtimes (\mathbb{F}_p^\times \cdot S_m),$$

explicit enough to compute in.

3. A class of examples

Let $\mathbb{F}_p^\times = \langle b \rangle$, let $mh = p-1$ and let $b^h = u$. For e a divisor of m, let

$$\begin{aligned} F_e &= C_p \rtimes_e C_m \\ &= \langle x, y | x^p = y^m = 1, yx = x^{u^e} y \rangle. \end{aligned}$$

Then $F_m = C_p \times C_m = C_{pm}$, while
$F_1 \cong C_p \rtimes \langle u \rangle$;
if $m = p-1$ then $F_1 \cong Hol(C_p)$.

Special or related cases:
[Ch03]: $\Gamma = Hol(C_p)$ a safeprime;
[Ko13]: Γ of order $p(p-1)$ with p a safeprime (6 cases);
[By04]: Γ of order pq, primes.
[CCo07], [Ch13]: Hopf Galois structures arising from fixed point free endomorphisms.
[BC12]: Γ of order $p(p-1)$, p a safeprime, and Hopf Galois structures arising from fixed point free pairs of homomorphisms from Γ to N.

All of these except [Ch13] use only Byott's translation.

Kohl's approach, when available, avoids the issue of b^{-1}.

Recall:

$$F_e = C_p \rtimes_e C_m = \langle x, y \rangle, yx = x^{u^e} y.$$
$$F_m = C_{mp}.$$

Let Γ, M range through $\{F_e | e \text{ divides } m\}$. Then we find $R(\Gamma, [M])$, the regular subgroups N of $Perm(\Gamma)$ normalized by $\lambda(\Gamma)$ and $\cong M$. The counts are

Theorem 3.1. $|R(F_e, F_d)| =$

- $2p\phi(m/d)$ *for* $e \neq d$, $d \neq m$;
- p *for* $e < m, d = m$;
- $2p\phi(m/d) - 2(p-1)$ *for* $d = e$.

Also:

• We can see how the regular subgroups pair off as centralizers of each other in $Perm(\Gamma)$.

• We find which elements $\alpha(\Gamma)$ of $R(\Gamma, [\Gamma])$ correspond to abelian fixed point free endomorphisms ϕ, as described in [Ch12]: given such a ϕ, we obtain an embedding

$$\alpha : \Gamma \to Perm(\Gamma) \text{ by } \alpha(gm) = \lambda(gm)\rho(\phi(gm)).$$

• The regular subgroups N with $P(N) = \mathcal{P}$ yield a single $\lambda(\Gamma)$ isomorphism class: the corresponding K-Hopf algebra acting on L is

$$H_\lambda = L(\lambda(G))^{\lambda(G)}.$$

• For $d \neq e$, $d, e \neq m$, we find which elements of $R(\Gamma, M)$ arise from fixed point free pairs of homomorphisms from G_m to M: in particular:
–none of them if d does not divide e;
–all of them, if d divides e.

4. Kohl's group

To get these results, we work inside

$$Norm_{Perm(\Gamma)}(\mathcal{P}) = \mathbb{F}_p^m \cdot U \cdot S$$

where
$U = \langle u \rangle$ for u a fixed element of $\mathbb{F}_p^\times$ of order m, and
$S \cong S_m$.

Here

$$\mathcal{P} = P(\lambda(\Gamma)) = \langle \pi \rangle$$

is the p-Sylow subgroup of $\lambda(\Gamma)$.

We may describe how $Norm_{Perm(\Gamma)}(\mathcal{P})$ acts on Γ.

Regularity implies $\pi = \pi_1 \pi_2 \dots \pi_m$, a product of m p-cycles. Let $\mathbb{F}_p^m = \langle \pi_1, \pi_2, \dots, \pi_m \rangle$, and fix γ_j in the support of π_j. Then Γ is the disjoint union of the supports of the π_i, and we may lay out the elements of Γ by writing the π_j as p-cycles:

$$\begin{aligned}
\pi_1 =&(\gamma_1, \quad \pi_1(\gamma_1), \dots, \quad \pi_1^{p-1}(\gamma_1)) \\
\pi_2 =&(\gamma_2, \quad \pi_2(\gamma_2), \dots, \quad \pi_2^{p-1}(\gamma_2)) \\
&\vdots \\
\pi_j =&(\gamma_j, \quad \pi_j(\gamma_j), \dots, \quad \pi_j^{p-1}(\gamma_j)) \\
&\vdots \\
\pi_m =&(\gamma_m, \quad \pi_m(\gamma_m), \dots, \quad \pi_m^{p-1}(\gamma_m))
\end{aligned}$$

Then elements of $\mathbb{F}_p^m$ act on Γ in the obvious way, and U and S act on Γ by:

S permutes the rows $\{\pi_1, \dots, \pi_m\}$ and

u^r in U permutes the columns by sending $\pi_j^k(\gamma_j)$ to $\pi_j^{ku^r}(\gamma_j)$ for u in U.

Write elements of $Norm_{Perm(\Gamma)}(\mathcal{P})$ as $(\hat{a}, u^r, \alpha)$ for
$\hat{a} = \pi_1^{a_1} \cdots \pi_m^{a_m}$, α in S.

Let N be a regular subgroup of $Perm(\Gamma)$ contained in $Norm_{Perm(\Gamma)}(\mathcal{P})$. Assume $N \cong C_p \rtimes_d C_m$. Write $N = P(N)Q(N)$ where $P(N)$ is the p-Sylow subgroup of N and $Q(N)$ is a complementary subgroup of order m. Then $Q(N) = \langle(\hat{a}, u^r, \alpha)\rangle$ with α an m-cycle. Kohl showed that if $N = P(N) \times Q(N)$, then $P(N) = \mathcal{P}$; otherwise, let

$$N^{opp} = Cent_{Perm(\Gamma)}(N),$$

then $N^{opp} < Norm_{Perm(\Gamma)}(\mathcal{P})$, and:
exactly one of $\{N, N^{opp}\}$ has p-Sylow subgroup $= \mathcal{P}$.

(So we can count $R(F_e, F_d)$ by assuming $P(N) = \mathcal{P}$.)

We have $Norm_{Perm(\Gamma)}(\Gamma) = \mathbb{F}_p^m \cdot U \cdot S$.

For $\Gamma \cong F_e$, we have

$$\lambda(\Gamma) = \mathcal{P} \cdot \mathcal{Q} = \langle(\hat{1}, 1, I)\rangle \cdot \langle(\hat{0}, u^e, \sigma)\rangle$$

for fixed m-cycle σ.

If $P(N) = \mathcal{P}$, then N has the form

$$N = \langle((\hat{1}, 1, I), (\hat{a}, u^s, \alpha)\rangle.$$

If $P(N) \neq \mathcal{P}$, then the exponents on $\pi_1, \ldots \pi_m$ in $\mathbb{F}_p^m$ are given by the values of a linear character $\chi : \mathcal{Q} \to \mathbb{F}_p^\times$: the generator of $P(N)$ is $(\hat{p}_\chi, 1, I)$ where

$$\hat{p}_\chi = \sum_{\gamma \in \mathcal{Q}} \pi_{\gamma(1)}^{\chi(\gamma)}.$$

If $\mathcal{Q} = \langle q \rangle$, then the linear characters are $\chi_i : \mathcal{Q} \to \mathbb{F}_p^\times$, defined by $\chi_i(q^k) = u^{mk/i}$ for $i = 1, \ldots, m$.

Both when $P(N) = \mathcal{P}$ or $= \langle(\hat{p}_{\chi_i}, 1, I)\rangle$, the m-cycle $\alpha = \sigma^t$ for some t, so $Q(N) = \langle(\hat{a}, u^s, \sigma^t)\rangle$ for some $\hat{a}$ in $\mathbb{F}_p^m$, s and t mod m.

One obtains constraints on $i, \hat{a}, s$ and t by requiring that the generators of N satisfy the relations of F_d and that N is normalized by $\lambda(\Gamma)$. Then we can determine the range of possibilities for those parameters under those constraints.

What comes out is:

Theorem 4.1. *Let $e < m$ and $d \neq e$ be divisors of m. Let T be a transversal of $U_{m/d}$ in $U_m = \langle u \rangle$. Let $\lambda(\Gamma) \cong F_e$ and $M \cong F_d$. Write*

$$\lambda(\Gamma) = \mathcal{P} \cdot \langle(\hat{0}, u^e, \sigma)\rangle$$

where σ is a fixed m-cycle in S. Then every $N \cong F_d$ has the form

$$N = \mathcal{P} \cdot \langle(b_0 \hat{p}_{\chi_e}, u^d, \sigma^t)\rangle$$

for $b_0 \in \mathbb{F}_p$ and $t \in T$, or

$$N = \langle(\hat{p}_{\chi_i}, 1, I), (b_0 \hat{p}_{\chi_e}, 1, \sigma^t)\rangle$$

for $b_0 \in \mathbb{F}_p$, $t \in T$ *and* i *satisfying* $-it \equiv d \pmod{m}$.

There are analogous results for the other possibilities for e, d.

The bottom line: when applicable, Kohl's description is a useful bridge from previous work counting Hopf Galois structures towards an explicit description of those Hopf Galois structures.

References

[By96] N. P. Byott, Uniqueness of Hopf Galois structure of separable field extensions, Comm. Algebra **24** (1996), 3217–3228, Corrigendum, ibid., 3705.

[By97] N. Byott, Associated orders of certain extensions arising from Lubin-Tate formal groups, J. Theorie des Nombres de Bordeaux **9** (1997), 449–462.

[By99] N. Byott, Integral Galois module structure of some Lubin-Tate extensions, J. Number Theory **77** (1999), 252–273.

[By00] N. Byott, Galois module theory and Kummer theory for Lubin-Tate formal groups, pp. 55-67 in "Algebraic Number Theory and Diophantine Analysis" (F. Halter-Koch, R. Tichy, eds), (Proceedings of Conference in Graz, 1998), Walter de Gruyter, 2000.

[By02] N. P. Byott, Integral Hopf-Galois structures on degree p^2 extensions of p-adic fields. J. Algebra **248** (2002), 334–365.

[By04a] N. Byott, Hopf-Galois structures on Galois field extensions of degree pq, J. Pure Appl. Algebra **188** (2004), 45–57.

[By04b] N. Byott, Hopf-Galois structures on field extensions with simple Galois groups, Bull. London Math. Soc. **36** (2004), 23–29.

[By07] N. P. Byott, Hopf-Galois structures on almost cyclic field extensions of 2-power degree. J. Algebra **318** (2007), 351–371.

[By13] N. P. Byott, Nilpotent and abelian Hopf-Galois structures on field extensions, J. Algebra, **381**, 131–139.

[BC12] N. P. Byott, L. N. Childs, Fixed point free pairs of homomorphisms and nonabelian Hopf Galois structures, New York J. Math. 18 (2012), 707–731.

[Ca13] A. Caranti, Quasi-inverse endomorphisms, J. Group Theory (to appear, 2013)

[CaC99] S. Carnahan, L. N. Childs, Counting Hopf Galois structures on nonabelian Galois field extensions. J. Algebra **218** (1999), 81–92.

[CS69] S. U. Chase, M. E. Sweedler, Hopf Algebras and Galois Theory, Lecture Notes in Mathematics **97**, Springer Verlag, NY, 1969.

[Chs71] S. U. Chase, On inseparable Galois theory, Bull. Amer. Math. Soc. 77 (1971), 413–417.

[Chs72] S. U. Chase, On the automorphism scheme of a purely inseparable field extension, in Ring Theory (R. Gordon, ed.), Academic Press, 1972.

[Chs74] S. U. Chase, Infinitesimal group scheme actions on finite field extensions, Amer. J. Math. 98 (1974), 441–480.

[Ch89] L. N. Childs, On the Hopf Galois theory for separable field extensions. Comm. Algebra **17** (1989), 809–825.

[Ch96] L. N. Childs, Hopf Galois structures on degree p^2 cyclic extensions of local fields, New York J. Mathematics **2** (1996), 86–102.

[Ch00] L. N. Childs, Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory, American Mathematical Society, Mathematical Surveys and Monographs **80**, 2000.

[Ch03] L. N. Childs, On Hopf Galois structures and complete groups, New York J. Mathematics **9**, (2003), 99–116.

[Ch05] L. N. Childs, Elementary abelian Hopf Galois structures and polynomial formal groups. J. Algebra **283** (2005), 292–316.

[Ch07] L. N. Childs,Some Hopf Galois structures arising from elementary abelian p-groups. Proc. Amer. Math. Soc. **135** (2007), 3453–3460.

[Ch12] L. N. Childs, Fixed-point free endomorphisms of groups related to finite fields, Finite Fields and Their Applications 18 (2012), 661-673.

[Ch11] L. N. Childs, Hopf Galois structures on Kummer extensions of prime power degree, New York J. Math **17** (2011), 51–74.

[Ch13a] L. N. Childs, Fixed-point free endomorphisms and Hopf Galois structures, Proc. Amer. Math. Soc. 141 (2013), 1255-1265.

[CCo07] L. N. Childs, J. Corradino, Cayley's theorem and Hopf Galois structures for semidirect products of cyclic groups. J. Algebra **308** (2007), 236–251.

[CM94] L. N. Childs, D. Moss, Hopf algebras and local Galois module theory, in "Advances in Hopf Algebras" (J. Bergen, S. Montgomery, eds.) Marcel Dekker, 1994, 1–24.

[FE03] S. C. Featherstonhaugh, Abelian Hopf Galois structures on Galois field extensions of prime power order, Ph. D. thesis, University at Albany, 2003

[FCC12] S. C. Featherstonhaugh, A. Caranti, L. N. Childs, Abelian Hopf Galois structures on Galois field extensions of prime power order, Trans. Amer. Math. Soc. 364 (2012), 3675-3684.

[GC98] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, J. Algebra **106** (1987), 239–258.

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

[Ko07] Kohl, T., Groups of order $4p$, twisted wreath products and Hopf-Galois theory. J. Algebra **314** (2007), 42–74.

[Ko13] Kohl, T., Regular permutation groups of order mp and Hopf Galois structures, Algebra and Number Theory, to appear, 2013.

[Le59] H. W. Leopoldt, Uber die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. reine angew. Math. **201** (1959), 119–149.

[Mo96] D. J. Moss, Hopf Galois Kummer theory of formal groups, Amer. J. Math. **118** (1996), 301–318.

[Sw69] M. Sweedler, Hopf Algebras, Benjamin, 1969.

Department of Mathematics and Statistics, University at Albany, Albany, NY 12222

E-mail address: lchilds@albany.edu