

FIXED-POINT FREE ENDOMORPHISMS AND HOPF GALOIS STRUCTURES

LINDSAY N. CHILDS

ABSTRACT

Let $L|K$ be a Galois extension of fields with finite Galois group G . Greither and Pareigis [GP87] showed that there is a bijection between Hopf Galois structures on $L|K$ and regular subgroups of $Perm(G)$ normalized by G , and Byott [By96] translated the problem into that of finding equivalence classes of embeddings of G in the holomorph of groups N of the same cardinality as G . In [CCo06] we showed, using Byott's translation, that fixed point free endomorphisms of G yield Hopf Galois structures on $L|K$. Here we show how abelian fixed point free endomorphisms yield Hopf Galois structures directly, using the Greither-Pareigis approach, and, in some cases, also via the Byott translation. The Hopf Galois structures that arise are "twistings" of the Hopf Galois structure by H_λ , the K -Hopf algebra that arises from the left regular representation of G in $Perm(G)$. The paper concludes with various old and new examples of abelian fixed point free endomorphisms.

HOPF GALOIS STRUCTURES

We first review the Greither-Pareigis approach to Hopf Galois structures.

Let G be a finite group. The left (resp. right) regular representation λ (resp. ρ) of G in $Perm(G)$ is the map from G to $Perm(G)$ given by

$$\lambda(\sigma)(\tau) = \sigma\tau,$$

resp.

$$\rho(\sigma)(\tau) = \tau\sigma^{-1}$$

for σ, τ in G .

Date: November 18, 2009.

2000 Mathematics Subject Classification. 12F10.

My thanks to the Mathematics Department at Virginia Commonwealth University for its hospitality while this research was conducted.

Let the field L be a Galois extension of the field K with Galois group G . To find a Hopf Galois structure on $L|K$, we find a regular subgroup N of $Perm(G)$. Let $GL = Map(G, L) = \sum_{\sigma \in G} Lx_\sigma$, where $x_\sigma(\tau) = \delta_{\sigma, \tau}$. Then N acts on GL via

$$\eta(ax_\sigma) = ax_{\eta(\sigma)}$$

for a in L , η in N . This action makes GL into a LN -Hopf Galois extension of L . If N is normalized by $\lambda(G)$, then G acts on LN via

$$\sigma(a\eta) = \sigma(a)\lambda(\sigma)\eta\lambda(\sigma^{-1})$$

and on GL via

$$\sigma(ax_\tau) = \sigma(a)x_{\lambda(\sigma)(\tau)} = \sigma(a)x_{\sigma\tau}.$$

The fixed ring of GL under the action of G is isomorphic to L via the map

$$a \mapsto \sum_{\sigma \in G} \sigma(a)x_\sigma,$$

and the action $LN \otimes_L GL \rightarrow GL$ descends uniquely to a Hopf Galois action of the K -Hopf algebra $H = LN^G$ on $GL^G \cong L$. Greither and Pareigis [GP87] show that every Hopf algebra structure on $L|K$ corresponds in this way to a unique regular subgroup N of $Perm(G)$ normalized by $\lambda(G)$.

If $N = \rho(G)$, the image of the right regular representation of G in $Perm(G)$, then the action of $\rho(G)$ on GL is by

$$\rho(\tau)(ax_\sigma) = ax_{\rho(\tau)(\sigma)} = ax_{\sigma\tau^{-1}}$$

for a in L . Since $\lambda(G)$ commutes with $\rho(G)$ in $Perm(G)$, the action of $\lambda(G)$ on $\rho(G)$ is trivial, and so $LN^G = KG$ and the action of $\rho(G)$ on GL descends to the usual action of G on L :

$$\begin{aligned} \rho(\tau)\left(\sum_{\sigma} \sigma(a)x_\sigma\right) &= \sum_{\sigma} \sigma(a)x_{\rho(\tau)(\sigma)} \\ &= \sum_{\sigma} \sigma(a)x_{\sigma\tau^{-1}} \\ &= \sum_{\pi} \pi(\tau(a))x_\pi \end{aligned}$$

which corresponds to $\tau(a)$ in L . Thus we recover the action on L by the Galois group G of $L|K$. But if G is nonabelian and $N = \lambda(G)$, then the action of $\lambda(G)$ on GL is via

$$\lambda(\tau)(ax_\sigma) = ax_{\lambda(\tau)(\sigma)} = ax_{\tau\sigma},$$

which descends to an action on L of $LN^G = H_\lambda$ where

$$H_\lambda = \left\{ \sum_{\sigma \in G} a_\sigma \sigma : \sum_{\sigma \in G} a_\sigma \sigma = \sum_{\sigma \in G} \tau(a_\sigma) \tau \sigma \tau^{-1} \right\},$$

a K -Hopf algebra which has basis elements of the form

$$\sum_{\tau} \tau(a) \tau \sigma \tau^{-1}$$

where σ runs through representatives of the conjugacy classes of G , and for each σ , a is chosen from a K -basis of L^S where S is the centralizer of σ , and the sum is over elements τ in a transversal of S in G .

Every non-abelian Galois extension $L|K$ of fields has at least these two distinct Hopf Galois structures, the classical structure by the Galois group, corresponding to ρ , and the Hopf Galois structure by H_λ , corresponding to λ . The two actions coincide if G is abelian.

For G a non-abelian simple group, it was shown in [By04], extending [CaC99], that the Hopf Galois structures corresponding to λ and ρ are the only possible Hopf Galois structures on a Galois extension with Galois group G . For certain cyclic Galois groups G , the classical Galois structure is the only Hopf Galois structure, see [By96]. But for many groups G there are large numbers of Hopf Galois structures on Galois extensions of fields with Galois group G .

A number of papers have studied Hopf Galois structures, in part because of potential applications to Galois module theory. For a survey of results from the 20th century, see [Ch00], Chapter 2; for an interesting application to local Galois module theory, see [By02]. The Greither-Pareigis approach to finding Hopf Galois structures can be difficult in general, because of the size of $Perm(G)$. (See [Ko07] for the most extensive attempt to classify Hopf Galois structures using the Greither-Pareigis framework.) For that reason, a translation of the Greither-Pareigis classification, formally codified by Byott [By96], has been utilized in most subsequent work related to classifying Hopf Galois structures. This was the case in [CCo06], which first explicitly observed a connection between fixed point free endomorphisms and Hopf Galois structures. On the other hand, it has been relatively difficult to describe Hopf Galois structures that arise from Byott's translation.

We review Byott's translation below.

Definition 1. An endomorphism ψ of G is *abelian* if $\psi(\sigma\tau) = \psi(\tau\sigma)$ for all σ, τ in G .

The main point of the present paper is that abelian fixed point free endomorphisms yield Hopf Galois structures quite straightforwardly

using the Greither-Pareigis approach and can also yield structures easily via Byott's translation as well. We show in the second half of the paper that there are many examples.

FIXED POINT FREE ENDOMORPHISMS

Let ψ be an endomorphism of the Galois group G . Define a homomorphism

$$\alpha_\psi : G \rightarrow \text{Perm}(G)$$

by

$$\alpha_\psi(\sigma) = \lambda(\sigma)\rho(\psi(\sigma)).$$

Since $\lambda(G)$ and $\rho(G)$ commute and λ, ρ and ψ are homomorphisms, it is routine to check that α_ψ is a homomorphism from G into $\text{Perm}(G)$, and so $\alpha_\psi(G)$ is a subgroup of $\text{Perm}(G)$.

The subgroup $\alpha_\psi(G)$ is a regular subgroup of $\text{Perm}(G)$ provided that $G = \alpha_\psi(G)(e)$ where e is the identity element of the set G on which $\text{Perm}(G)$ acts. But this is so iff

$$\begin{aligned} G &= \{\lambda(\sigma)\rho(\psi(\sigma))(e) : \sigma \in G\} \\ &= \{\sigma e \psi(\sigma)^{-1} : \sigma \in G\} \\ &= \{\sigma \psi(\sigma)^{-1} : \sigma \in G\}. \end{aligned}$$

The function $\sigma \mapsto \sigma \psi(\sigma)$ is onto G iff it is one-to-one, iff for all σ, τ in G ,

$$\sigma \psi(\sigma^{-1}) = \tau \psi(\tau^{-1}) \text{ implies } \sigma = \tau.$$

But $\sigma \psi(\sigma^{-1}) = \tau \psi(\tau^{-1})$ iff $\tau^{-1}\sigma = \psi(\tau^{-1}\sigma)$. So $G = \alpha_\psi(G)(e)$ if and only if ψ is *fixed point free*, that is, the only element π of G for which $\psi(\pi) = \pi$ is the identity element of G .

If ψ is the trivial endomorphism, then ψ is abelian and fixed point free, and $\alpha_\psi = \lambda$.

If G is abelian, then $\alpha_\psi(G) = \lambda(G)$, because for every π in G ,

$$\alpha_\psi(\sigma)(\pi) = \sigma \pi \psi(\sigma^{-1}) = \sigma \psi(\sigma^{-1}) \pi = \lambda(\sigma \psi(\sigma^{-1}))(\pi).$$

On the other hand,

Proposition 2. *If $\psi : G \rightarrow G$ is an endomorphism and $\psi(G)$ is not contained in the center of G , then $\alpha_\psi(G) \neq \lambda(G)$.*

Proof. Suppose $\alpha_\psi(G) = \lambda(G)$. Then for each σ in G there exists an element $\theta(\sigma)$ in G so that

$$\lambda(\sigma)\rho(\psi(\sigma)) = \lambda(\theta(\sigma)).$$

Then

$$\lambda(\sigma)\rho(\psi(\sigma))(e) = \lambda(\theta(\sigma))(e),$$

so

$$\sigma\psi(\sigma)^{-1} = \theta(\sigma),$$

and so for all π in G ,

$$\lambda(\sigma)\rho(\psi(\sigma))(\pi) = \lambda(\sigma\psi(\sigma^{-1}))(\pi),$$

hence

$$\sigma\pi\psi(\sigma^{-1}) = \sigma\psi(\sigma^{-1})\pi.$$

Thus $\psi(\sigma)$ is in the center of G . □

In fact, we have

Proposition 3. *Let G be a finite group with trivial center. Let ψ, ψ' be fixed point free endomorphisms of G . If $\alpha_\psi(G) = \alpha_{\psi'}(G)$, then $\psi = \psi'$.*

Proof. Suppose $\alpha_\psi(G) = \alpha_{\psi'}(G)$. Then for each σ in G there exists some τ in G so that

$$\lambda(\sigma)\rho(\psi(\sigma)) = \lambda(\tau)\rho(\psi'(\tau)).$$

Then for all π in G ,

$$\lambda(\sigma)\rho(\psi(\sigma))(\pi) = \lambda(\tau)\rho(\psi'(\tau))(\pi),$$

so for all π ,

$$\sigma\pi\psi(\sigma^{-1}) = \tau\pi\psi'(\tau^{-1}),$$

hence for all π ,

$$\tau^{-1}\sigma\pi\psi(\sigma^{-1})\psi'(\tau) = \pi.$$

In particular, for $\pi = e$, the identity of G , we have

$$\psi'(\tau) = \psi(\sigma)\sigma^{-1}\tau.$$

Substituting this into the formula involving π gives

$$\tau^{-1}\sigma\pi\psi(\sigma^{-1})\psi(\sigma)\sigma^{-1}\tau = \pi,$$

or

$$\tau^{-1}\sigma\pi\sigma^{-1}\tau = \pi,$$

for all π in G . But that implies that $\tau^{-1}\sigma$ commutes with every element of G . Since G has trivial center, $\sigma = \tau$, and so for all σ in G , we have

$$\lambda(\sigma)\rho(\psi(\sigma)) = \lambda(\sigma)\rho(\psi'(\sigma)),$$

hence $\psi = \psi'$. □

Thus if G has trivial center, then every fixed point free endomorphism of G yields a distinct Hopf Galois structure by $\alpha_\psi(G)$ on GL . The action is

$$\alpha_\psi(\tau)(ax_\sigma) = ax_{\lambda(\tau)\rho(\psi(\tau)(\sigma))} = ax_{\tau\sigma\psi(\tau^{-1})}.$$

Thus the $\alpha_\psi(G)$ action on GL may be viewed as a twisting by the endomorphism ψ of the $\lambda(G)$ -action on GL .

K -HOPF GALOIS STRUCTURES

For ψ a fixed point free endomorphism of G , we have the regular embedding $\alpha_\psi : G \rightarrow \text{Perm}(G)$ by $\alpha_\psi(\sigma) = \lambda(\sigma)\rho(\psi(\sigma))$. For α_ψ to yield a K -Hopf algebra structure on L , $\alpha_\psi(G)$ must be normalized by $\lambda(G)$.

Proposition 4. *If ψ is abelian, then $\alpha_\psi(G)$ is normalized by $\lambda(G)$.*

Proof. If we conjugate $\alpha_\psi(\sigma)$ by $\lambda(\tau)$ for σ, τ in G , we obtain

$$\begin{aligned} \lambda(\tau)\alpha_\psi(\sigma)\lambda(\tau)^{-1} &= \lambda(\tau)\lambda(\sigma)\rho(\psi(\sigma))\lambda(\tau)^{-1} \\ &= \lambda(\tau)\lambda(\sigma)\lambda(\tau)^{-1}\rho(\psi(\sigma)) \\ &= \lambda(\tau\sigma\tau^{-1})\rho(\psi(\sigma)). \end{aligned}$$

This equals $\alpha_\psi(\tau\sigma\tau^{-1})$ if $\psi(\sigma) = \psi(\tau\sigma\tau^{-1})$. □

Theorem 5. *Each abelian fixed point free endomorphism of G yields a distinct H_λ -Hopf Galois structure on $L|K$.*

Proof. If ψ is an abelian fixed point free endomorphism of G , then $\alpha_\psi(G)$ yields a Hopf Galois structure on $L|K$ by the K -Hopf algebra $H_\psi = L\alpha_\psi(G)^{\lambda(G)}$. Recalling that $H_\lambda = L\lambda(G)^{\lambda(G)}$, we show that H_λ is isomorphic to H_ψ as K -Hopf algebras.

The map sending $\lambda(\sigma)$ to $\lambda(\sigma)\rho(\psi(\sigma))$ is an isomorphism of groups, and induces an L -Hopf algebra isomorphism $f : L\lambda(G) \rightarrow L\alpha_\psi(G)$ of the corresponding group rings. We need to see if f respects the action of G on H_λ and H_ψ . So we ask, is

$$f(\tau(a\lambda(\sigma))) = \tau f(a\lambda(\sigma))?$$

The left side is

$$\begin{aligned} f(\tau(a\lambda(\sigma))) &= f(\tau(a)\lambda(\tau)\lambda(\sigma)\lambda(\tau^{-1})) \\ &= f(\tau(a)\lambda(\tau\sigma\tau^{-1})) \\ &= \tau(a)\lambda(\tau\sigma\tau^{-1})\rho(\psi(\tau\sigma\tau^{-1})), \end{aligned}$$

while the right side is

$$\begin{aligned}\tau f(a\lambda(\sigma)) &= \tau(a\lambda(\sigma)\rho(\psi(\sigma))) \\ &= \tau(a)\lambda(\tau)\lambda(\sigma)\rho(\psi(\sigma))\lambda(\tau^{-1}) \\ &= \tau(a)\lambda(\tau)\lambda(\sigma)\lambda(\tau^{-1})\rho(\psi(\sigma)).\end{aligned}$$

Thus f respects the G -action iff for all σ, τ in G ,

$$\rho(\psi(\tau\sigma\tau^{-1})) = \rho(\psi(\sigma)),$$

which holds since ψ is abelian.

Thus f is a G -module homomorphism, hence induces an isomorphism from $H_\lambda = L\lambda(G)^G$ to $H_\psi = L\alpha_\psi(G)^G$. \square

This result may be viewed as saying that if ψ is an abelian and fixed point free endomorphism of G , then the action of $\lambda(G)$ on GL twisted by ψ descends to a twisting by ψ of the action of H_λ on L .

BYOTT'S TRANSLATION

As noted above, a useful way to count Hopf Galois structures on a Galois extension $L|K$ with Galois group G is via Byott's translation. This works as follows. Given a finite group G , let N be a group of the same cardinality as G . Then each regular embedding of G into $Hol(N) \subset Perm(N)$ yields a Hopf Galois structure on a Galois extension of fields with Galois group G . Since $Hol(G) \cong G \rtimes Aut(G)$ is often a much more well-understood group than $Perm(G)$, the Byott translation approach has been used successfully to count Hopf Galois structures, for example in [By96], [CaC99], [Ch03], [By04], [Ch05], [CCo06], [Ch07].

To get from a regular embedding β of G into $Hol(N) = \rho(N) \cdot Aut(N)$ to a regular subgroup $\alpha(N)$ of $Perm(G)$, we use β to define a function (usually not a homomorphism) $b : G \rightarrow N$ by $b(\sigma) = \beta(\sigma)(e_N)$ (where e_N is the identity element of N). Then b is necessarily a bijection by regularity of β , so gives a homomorphism from $Perm(G)$ to $Perm(N)$ by conjugation: π in $Perm(G)$ maps to $b\pi b^{-1}$. This then yields a regular embedding α of N in $Perm(G)$ whose image $\alpha(N)$ is normalized by $\lambda(G)$, namely,

$$\alpha(\eta) = b^{-1}\lambda(\eta)b.$$

Thus for σ in G ,

$$\alpha(\eta)(\sigma) = b^{-1}(\eta b(\sigma)).$$

The embedding α is the one that defines the action of the Hopf algebra LN on GL , and hence the action of the K -Hopf algebra LN^G on $GL^G \cong L$.

In practice, it can be difficult to identify the inverse of b . But for embeddings β arising from some endomorphisms, we can identify b^{-1} and the embedding α .

Let $N = G$ and let ψ be a fixed point free endomorphism of G . Set $\beta : G \rightarrow \text{Hol}(G)$ by

$$\beta(\sigma) = \lambda(\sigma)\rho(\psi(\sigma)).$$

The corresponding function $b : G \rightarrow G$ is defined by

$$b(\sigma) = \lambda(\sigma)\rho(\psi(\sigma))(e_G) = \sigma\psi(\sigma^{-1}).$$

Then the corresponding embedding $\alpha : G \rightarrow \text{Perm}(G)$ is

$$\begin{aligned} \alpha(\eta)(\tau) &= (b^{-1}(\lambda(\eta)b)(\tau)) \\ &= b^{-1}(\eta\tau\psi(\tau^{-1})). \end{aligned}$$

Thus to understand the regular embedding α , and hence the Hopf Galois action, we need b^{-1} .

Proposition 6. *Let ψ, θ be fixed point free endomorphisms of G . Let $b : G \rightarrow G$ by $b(\sigma) = \sigma\psi(\sigma^{-1})$, and $c : G \rightarrow G$ by $c(\tau) = \tau\theta(\tau^{-1})$. If for all σ in G ,*

$$\theta(\psi(\sigma)) = \psi(\sigma)\theta(\sigma),$$

then b and c are inverse bijections.

Proof.

$$\begin{aligned} cb(\sigma) &= c(\sigma\psi(\sigma^{-1})) \\ &= \sigma\psi(\sigma^{-1})\theta(\sigma\psi(\sigma^{-1}))^{-1} \\ &= \sigma\psi(\sigma^{-1})\theta(\psi(\sigma))\theta(\sigma^{-1}). \end{aligned}$$

Then $cb(\sigma) = \sigma$ iff

$$\sigma = \sigma\psi(\sigma^{-1})\theta(\psi(\sigma))\theta(\sigma^{-1}),$$

iff

$$\theta(\psi(\sigma)) = \psi(\sigma)\theta(\sigma).$$

□

Say that θ is the *inverse* of ψ if the corresponding bijections c and b are inverses of each other. (Since abelian endomorphisms are never invertible as functions, perhaps this use of “inverse” is not too perverse.)

Corollary 7. *Let ψ be a fixed point free endomorphism of G , and define the regular embedding $\beta : G \rightarrow \text{Hol}(G)$ by $\beta(\tau) = \lambda(\tau)\rho(\psi(\tau^{-1}))$. Then the corresponding regular embedding α of G into $\text{Perm}(G)$ is defined by $\alpha(\sigma) = \lambda(\sigma)\rho(\theta(\sigma))$ where θ is the inverse of ψ .*

Proof. The corresponding maps $b, c : G \rightarrow G$ are defined by

$$b(\sigma) = \sigma\psi(\sigma^{-1})$$

and

$$c(\tau) = \tau\theta(\tau^{-1}).$$

If b and c are inverse bijections, then

$$\begin{aligned} \alpha(\sigma)(\tau) &= c(\sigma b(\tau)) \\ &= c(\sigma\tau\psi(\tau)^{-1}) \\ &= \sigma\tau\psi(\tau)^{-1}\theta((\sigma\tau\psi(\tau)^{-1})^{-1}) \\ &= \sigma\tau\psi(\tau)^{-1}\theta(\psi(\tau))\theta(\tau^{-1})\theta(\sigma^{-1}). \end{aligned}$$

Since θ and ψ are inverses, we have

$$\theta(\psi(\tau)) = \psi(\tau)\theta(\tau),$$

so

$$\begin{aligned} \alpha(\sigma)(\tau) &= \sigma\tau\psi(\tau)^{-1}\psi(\tau)\theta(\tau)\theta(\tau^{-1})\theta(\sigma^{-1}) \\ &= \sigma\tau\theta(\sigma^{-1}) \\ &= (\lambda(\sigma)\rho(\theta(\sigma)))(\tau). \end{aligned}$$

□

If ψ is abelian, then so is θ . So if ψ is abelian, then Theorem 5 shows that the Hopf Galois action on a field extension $L|K$ corresponding to θ in Corollary 7 is via the Hopf algebra H_λ .

EXAMPLES

Symmetric groups. In [CaC99] it was observed that for $G = S_n$, $n \geq 5$, every fixed point free endomorphism of G is trivial on the alternating group $A_n \subset S_n$. (For a non-abelian simple group there are no non-trivial fixed point free endomorphisms, c.f. [Go82, p. 55].) Hence every non-trivial fixed point free endomorphism induces a homomorphism from S_n/A_n into S_n , hence is abelian. For the endomorphism to be fixed point free, the non-trivial coset must map to an even permutation of order 2. Each such non-trivial fixed point free endomorphism of S_n yields a distinct action of H_λ on any Galois extension $L|K$ with Galois group S_n .

It is easy to see that each such endomorphism is its own inverse.

Metacyclic groups. In [CCo06] we examined groups G of the form $G = Z_h \rtimes Z_k$ where h is odd. Write $G = \langle x, y \rangle$ with relations $yx = x^b y$, where b is coprime to h and has order k modulo h . Assume $(b-1, h) = 1$. Then by [CCo06, Proposition 2.1], G has trivial center.

The abelian fixed point free endomorphisms $\psi : G \rightarrow G$ are defined by

$$\psi(x) = 1, \psi(y) = x^r y^s,$$

where by [CCo06, Proposition 3.1],

$$\begin{aligned} r \frac{b^{sk} - 1}{b^s - 1} &\equiv 0 \pmod{h} \text{ if } s \not\equiv 0 \pmod{k}; \\ rk &\equiv 0 \pmod{h} \text{ if } s \equiv 0 \pmod{k}, \end{aligned}$$

and by [CCo06, Corollary 5.2], $(s-1, k) = 1$.

In particular, if $G = D_m$, the dihedral group of order $2m$ with m odd, then $h = m, k = 2, s$ must be 0, and then $r = 0$, so G has no non-trivial abelian fixed point free endomorphisms.

Returning to the general case $G = Z_h \rtimes Z_k$ where h is odd, and given the abelian fixed point free endomorphisms ψ of G with $\psi(x) = 1, \psi(y) = x^r y^s$ as above, and θ with

$$\theta(x) = 1, \theta(y) = x^t y^w,$$

we seek conditions for θ to be the inverse of ψ , that is,

$$\psi(\theta(\sigma)) = \theta(\sigma)\psi(\sigma)$$

for all σ in G .

Proposition 8. *Suppose s satisfies $(b^s - 1, h) = 1$. If w is defined by $(w-1)(s-1) \equiv 1 \pmod{k}$ and t by $t(b^s - 1) \equiv r(b^w - 1)$, then θ is the inverse of ψ .*

Proof. Since $\psi(x) = 1 = \theta(x)$, it suffices to show that

$$\psi(\theta(y^n)) = \theta(y^n)\psi(y^n)$$

for all $n \geq 1$. Substituting, this equation becomes

$$x^{t(\frac{b^{wsn}-1}{b^w-1})} y^{wsn} = x^{r(\frac{b^s-1}{b^s-1})+t(\frac{b^{wn}-1}{b^w-1})b^{sn}} y^{sn+wn}.$$

Simplifying the exponents yields:

$$wsn \equiv sn + wn \pmod{k}$$

and

$$t\left(\frac{b^{wsn} - b^{wn+sn} + b^{sn} - 1}{b^w - 1}\right) \equiv r\left(\frac{b^{sn} - 1}{b^s - 1}\right) \pmod{h}.$$

The first congruence for $n = 1$ is the same as any of the following four congruences:

$$\begin{aligned} ws &\equiv w + s \pmod{k} \\ (s - 1)(w - 1) &\equiv 1 \pmod{k}, \\ w &\equiv s(w - 1) \pmod{k} \\ s &\equiv w(s - 1) \pmod{k}. \end{aligned}$$

The last two imply that

$$b^w \equiv b^{s(w-1)} \pmod{h}$$

and

$$b^s \equiv b^{w(s-1)} \pmod{h}.$$

These last congruences imply that for each prime p dividing h , if $b^s - 1$ is a unit modulo h , then so is $b^w - 1$.

Given that the denominators are units modulo h , we may use the congruence

$$b^{ws} \equiv b^{w+s} \pmod{h}$$

to simplify the congruence modulo h to

$$t\left(\frac{b^{sn} - 1}{b^w - 1}\right) \equiv r\left(\frac{b^{sn} - 1}{b^s - 1}\right) \pmod{h},$$

which follows from

$$t(b^s - 1) \equiv r(b^w - 1) \pmod{h},$$

a congruence that uniquely defines t from r modulo h .

Thus if t and w are defined as in the statement of the theorem, then θ is the inverse of ψ . \square

Even dihedral groups. Let $G = D_{2m} = \langle x, y \rangle$, the dihedral group of order $4m$, with relations $x^{2m} = 1 = y^2, yx = x^{-1}y$. Then the center of G is $\langle x^m \rangle$, of order 2. One may verify that G has the following abelian fixed point free endomorphisms $\psi : G \rightarrow G$:

- (1) $\psi(x) = 1, \psi(y) = x^m$;
- (2) $\psi(x) = x^m, \psi(y) = x^m$ if $(m - 1, 2m) = 1$;
- (3) $\psi(x) = x^m, \psi(y) = 1$ if $(m - 1, 2m) = 1$;
- (4) $\psi(x) = x^i y, \psi(y) = 1$ with i even;
- (5) $\psi(x) = x^i y, \psi(y) = x^m$ with $i + m$ even;
- (6) $\psi(x) = x^i y, \psi(y) = x^i y$ with i odd;
- (7) $\psi(x) = x^i y, \psi(y) = x^{i+m} y$ with $i + m$ odd.

Examples (1)-(3) have image in the center of G ; the others, by Proposition 2, yield regular subgroups $\alpha_\psi(G) \neq \lambda(G)$ in $Perm(G)$ normalized by $\lambda(G)$.

Examples involving elementary abelian p -groups. Let p be an odd prime and let A be an elementary abelian p -group of rank n , which we can identify as the vector space \mathbb{F}_p^n . Let $G = \mathbb{F}_p^n \rtimes \langle \beta \rangle$ where β in $GL_n(\mathbb{F}_p)$ has order d with $(p, d) = 1$. Let ψ be an endomorphism of G . Since β has order prime to p , then for each $f \neq 0$ in \mathbb{F}_p^n , $\psi(f, 1) = (g, 1)$ for some g in \mathbb{F}_p^n . Thus ψ restricts to an endomorphism of \mathbb{F}_p^n . Denote $\psi(f, 1) = (\psi(f), 1)$.

Proposition 9. *If $(s - 1, d) > 1$, then ψ has a fixed point on G . If $(s - 1, d) = 1$, then ψ has a fixed point on G if and only if ψ has a fixed point on \mathbb{F}_p^n .*

Proof. If ψ has a fixed point $g \neq 0$ in \mathbb{F}_p^n , then $\psi(g, 1) = (g, 1)$, and so ψ has a fixed point on G .

Suppose ψ has no fixed point on \mathbb{F}_p^n . Then the map $g \mapsto g - \psi(g)$ for g in \mathbb{F}_p^n is one-to-one, so for every k in \mathbb{F}_p^n , there exists some g in \mathbb{F}_p^n so that $g - \psi(g) = k$.

We try to solve $\psi(g, \beta^t) = (g, \beta^t)$ for $t \neq 0$. This is equivalent to

$$(\psi(g), 1)(h, \beta^s)^t = (g, \beta^t),$$

which in turn is equivalent to $\beta^{st} = \beta^t$ and

$$g - \psi(g) = (1 + \beta^s + \beta^{2s} + \dots + \beta^{(t-1)s})(h).$$

Suppose $(s - 1, d) > 1$. Then there exists some $t \not\equiv 0 \pmod{d}$ so that $\beta^{st} = \beta^t$. For such a t , since ψ has no fixed point on \mathbb{F}_p^n , there exists some g in \mathbb{F}_p^n so that

$$g - \psi(g) = (1 + \beta^s + \beta^{2s} + \dots + \beta^{(t-1)s})(h).$$

Thus ψ has a fixed point on G .

Suppose, on the other hand, that $(s - 1, d) = 1$. Then the only solution of $\psi(g, \beta^t) = (g, \beta^t)$ has $t = 0$, in which case $\psi(g, 1) = (g, 1)$ iff ψ has a fixed point on \mathbb{F}_p^n . \square

Proposition 10. *Let G be as in the last proposition, and let ψ be an endomorphism of G such that $\psi(f, 1) = (\psi(f), 1)$ for all f in \mathbb{F}_p^n and $\psi(0, \beta) = (h, \beta^s)$ for some h in \mathbb{F}_p^n . Then ψ is abelian iff $\psi(f) = \beta^s(\psi(f))$, iff $\psi(f) = \psi(\beta(f))$ for all f in \mathbb{F}_p^n .*

Proof. We have

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

for all f in \mathbb{F}_q . Applying ψ gives

$$(h, \beta^s)(\psi(f), 1) = (\psi(\beta(f)), 1)(h, \beta^s)$$

and so, looking at the \mathbb{F}_p^n -components, we obtain

$$\beta^s(\psi(f)) = \psi(\beta(f)).$$

Then ψ is abelian iff $\psi(f, 1)\psi(0, \beta) = \psi(0, \beta)\psi(f, 1)$, iff

$$(\psi(f), 1)(h, \beta^s) = (\psi(\beta(f)), 1)(h, \beta^s),$$

iff $\psi(f) = \psi(\beta(f)) = \beta^s(\psi(f))$. \square

Thus ψ is abelian iff ψ is constant on orbits of \mathbb{F}_p^n under β , iff $\psi(\mathbb{F}_p^n)$ is contained in the fixed point set of β^s .

Example 11. Let ψ is an endomorphism of G that is trivial on \mathbb{F}_p^n . Then ψ is abelian. If $\psi(0, \beta) = (h, \beta^s)$ with $(s-1, d) = 1$, then also ψ has no fixed points.

For endomorphisms ψ trivial on \mathbb{F}_p^n as in these last examples, we can find the inverse of ψ :

Proposition 12. *Let $G = \mathbb{F}_p^n \rtimes \langle \beta \rangle$ where β is an element of $GL_n(\mathbb{F}_p)$ with $\beta^d = 1$, where $(d, p) = 1$. Let $\psi : G \rightarrow G$ be the endomorphism with $\psi(f, 1) = (0, 1)$ for f in \mathbb{F}_p^n and $\psi(0, \beta) = (h, \beta^s)$ with $s \not\equiv 0 \pmod{d}$ and $(s-1, d) = 1$. Let $\theta : G \rightarrow G$ be the endomorphism with $\theta(f, 1) = (0, 1)$ and $\theta(0, \beta) = (g, \beta^t)$ where $(s-1)(t-1) \equiv 1 \pmod{d}$. Then θ is the inverse of ψ if*

$$(\beta^s - 1)(g) = (\beta^t - 1)(h).$$

Proof. We show that for all n ,

$$\psi(\theta(\beta^n)) = \theta(\beta^n)\psi(\beta^n).$$

This becomes

$$(h, \beta^{tn})^s = (g, \beta^t)^n (h, \beta^s)^n$$

for all n , which simplifies to

$$\begin{aligned} (1) \quad & (1 + bt^s + \dots + \beta^{(tn-1)s})(h) \\ & = (1 + \beta^t + \dots + \beta^{(n-1)t})g + \beta^{tn}(1 + \beta^s + \dots + \beta^{s(n-1)})(h) \end{aligned}$$

and

$$(2) \quad \beta^{tsn} = \beta^{tn+sn}$$

The second equality follows from the assumption that $(s-1)(t-1) \equiv 1 \pmod{d}$.

To study equation (1) in \mathbb{F}_p^n , we need to justify some algebraic manipulations. Let $m(x)$ be the minimal polynomial of β in $\mathbb{F}_p[x]$. Then $\mathbb{F}_p[\beta] \cong \mathbb{F}_p[x]/m(x)$ is a field. Now $m(x)$ divides $x^d - 1$ but because

β has order d , $m(x)$ does not divide $x^r - 1$ for any r with $1 \leq r < d$. Since in $\mathbb{F}_p[x]$ the greatest common divisor of $x^d - 1$ and $x^e - 1$ is $x^r - 1$ where r is the greatest common divisor of d and e , it follows that for all $e > 0$, $x^e - 1$ is invertible modulo $m(x)$ unless d divides e .

Now the coefficient of h in equation (1) maps to the image in $\mathbb{F}_p[x]/(m(x))$ of

$$\begin{aligned} & 1 + x^s + \dots + x^{(tn-1)s} - x^{tn}(1 + x^s + \dots + x^{s(n-1)}) \\ &= \frac{x^{tns} - 1}{x^s - 1} - x^{tn} \left(\frac{x^{sn} - 1}{x^s - 1} \right), \end{aligned}$$

and since $x^{tns} \equiv x^{tn}x^{sn}$ modulo $m(x)$, the coefficient of h simplifies to

$$\frac{x^{tn} - 1}{x^s - 1}.$$

The coefficient of g maps to the image in $\mathbb{F}_p[x]/m(x)$ of

$$\frac{x^{nt} - 1}{x^t - 1}.$$

By assumption, $s \not\equiv 0 \pmod{d}$, hence also t , and so $x^s - 1$ and $x^t - 1$ are invertible modulo $m(x)$. Thus if g and h satisfy

$$(\beta^s - 1)g = (\beta^t - 1)h,$$

then g and h uniquely determine each other, and the equation (1) required for θ to be the inverse of ψ is satisfied. \square

REFERENCES

- [By96] N. P. Byott, Uniqueness of Hopf Galois structure of separable field extensions, *Comm. Algebra* 24 (1996), 3217-3228.
- [By02] N. P. Byott, Integral Hopf-Galois structures on degree p^2 extensions of p -adic fields, *J. Algebra* 248 (2002), 334-365.
- [By04] N. P. Byott, Hopf-Galois structures on field extensions with simple Galois groups, *Bulletin of the London Mathematical Society* 36 (2004), 23-29.
- [CaC99] S. Carnahan, L. N. Childs, Counting Hopf Galois structures on non-abelian Galois field extensions, *J. Algebra* 218 (1999), 81-92.
- [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. Math.* 9 (2003), 99-115.
- [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.

- [CCo06] L. N. Childs, J. Corradino, Cayley's Theorem and Hopf Galois structures for semidirect products of cyclic groups, *J. Algebra* (2006), 236-251.
- [Go82] D. Gorenstein, *Finite Simple Groups, An Introduction to Their Classification*, Plenum, New York/London, 1982.
- [GP87] C. Greither, B. Parieigis, Hopf Galois theory for separable field extensions, *J. Algebra* 106 (1987), 239-258.
- [Ko07] T. Kohl, Groups of order $4p$, twisted wreath products and Hopf-Galois theory, *J. Algebra*, 314 (2007), 42-74.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY AT ALBANY,
ALBANY, NY 12222

E-mail address: `childs@math.albany.edu`