PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 141, Number 4, April 2013, Pages 1255–1265
S 0002-9939(2012)11418-2
Article electronically published on September 21, 2012

FIXED-POINT FREE ENDOMORPHISMS AND HOPF GALOIS STRUCTURES

LINDSAY N. CHILDS

(Communicated by Ted Chinburg)

Abstract. Let $L|K$ be a Galois extension of fields with finite Galois group G. Greither and Pareigis showed that there is a bijection between Hopf Galois structures on $L|K$ and regular subgroups of $Perm(G)$ normalized by G, and Byott 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 2007 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.

1. 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.

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

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

for a in L, η in N. This action makes GL into an LN-Hopf Galois extension of L. Conversely, if H is an L-Hopf algebra making $GL|L$ into a Hopf Galois extension, then $H = LN$ for some regular subgroup N of $Perm(G)$ with the action as just described.

Received by the editors November 18, 2009 and, in revised form, November 14, 2010; July 21, 2011; and August 25, 2011.

2000 *Mathematics Subject Classification.* Primary 12F10.

The author thanks the mathematics department at Virginia Commonwealth University for its hospitality while this research was conducted and the referee for numerous helpful suggestions.

If the regular subgroup N of $Perm(G)$ 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 $LN \otimes_L GL \to GL$ 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 in this way every Hopf Galois structure on $L|K$ corresponds 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:

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

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

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

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 nonabelian 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 nonabelian 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 [CCo07], 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.

2. Fixed point free endomorphisms

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

$$\alpha_\psi : G \to Perm(G)$$

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 $Perm(G)$, and so $\alpha_\psi(G)$ is a subgroup of $Perm(G)$.

The subgroup $\alpha_\psi(G)$ is a regular subgroup of $Perm(G)$ provided that $G = \alpha_\psi(G)(e)$, where e is the identity element of the set G on which $Perm(G)$ 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 $\sigma \mapsto \sigma\psi(\sigma^{-1})$ 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 $\alpha_\psi = \lambda$.

We want to know when two fixed point free endomorphisms yield the same regular subgroup of $Perm(G)$.

Theorem 2. *Let ψ, ψ' be fixed point free endomorphisms of a finite group G. Then $\alpha_\psi(G) = \alpha_{\psi'}(G)$ if and only if there exists a fixed point free endomorphism $\zeta : G \to G$ with image in $Z(G)$, the center of G, so that for all σ in G,*

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

Given ψ, ψ', the endomorphism ζ is unique. If ψ is abelian and $\alpha_\psi(G) = \alpha_{\psi'}(G)$, then ψ' is abelian.

Proof. Let ψ be a fixed point free endomorphism of G and let $\zeta : G \to G$ be a fixed point free endomorphism of G with image in $Z(G)$. (Then ζ is abelian.) Let $\pi : G \to G$ by $\pi(\sigma) = \sigma\zeta(\sigma^{-1})$. Then π is a homomorphism of G because ζ is a homomorphism with image in $Z(G)$. Also, π is one-to-one, hence an automorphism of G, because ζ is fixed point free. Define $\psi' : G \to G$ by

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

Then ψ' is an endomorphism of G, since $\zeta(\sigma)$ is in $Z(G)$, and is easily seen to be fixed point free and abelian if ψ is abelian. Now for η in G we have

$$\begin{aligned}\alpha_{\psi'}(\sigma)(\eta) &= \sigma\eta\psi'(\sigma^{-1}) \\ &= \sigma\eta\zeta(\sigma^{-1})\psi(\pi(\sigma^{-1})) \\ &= \sigma\zeta(\sigma^{-1})\eta\psi(\pi(\sigma^{-1})) \\ &= \pi(\sigma)\eta\psi(\pi(\sigma^{-1})) \\ &= \alpha_\psi(\pi(\sigma))(\eta).\end{aligned}$$

So

$$\alpha_{\psi'}(G) = \alpha_\psi(G).$$

Conversely, let ψ, ψ' be fixed point free endomorphisms of G with $\alpha_\psi(G) = \alpha_{\psi'}(G)$. Then there is a unique permutation π of G so that

$$\alpha_{\psi'}(\sigma) = \alpha_\psi(\pi(\sigma))$$

for all σ in G. Since α_ψ and $\alpha_{\psi'}$ are injective endomorphisms from G to $Perm(G)$, it follows that π is a homomorphism, hence an automorphism of G.

Applying the permutation $\alpha_{\psi'}(\sigma)$ to the identity element e of the set G yields

$$\alpha_{\psi'}(\sigma)(e) = \alpha_\psi(\pi(\sigma))(e),$$

which yields

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

Then for all η in G, the identity

$$\alpha_{\psi'}(\sigma)(\eta) = \alpha_\psi(\pi(\sigma))(\eta)$$

yields

$$\begin{aligned}\sigma\eta\psi'(\sigma^{-1}) &= \pi(\sigma)\eta\psi(\pi(\sigma^{-1})) \\ &= \pi(\sigma)\eta\pi(\sigma^{-1})\sigma\psi'(\sigma^{-1}),\end{aligned}$$

which implies that

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

Thus $\pi(\sigma^{-1})\sigma$ is in the center $Z(G)$ of G. If we define $\zeta : G \to G$ by $\zeta(\sigma) = \pi(\sigma^{-1})\sigma$, then ζ is an abelian endomorphism of G with image in $Z(G)$, ζ is fixed point free since π is an automorphism of G, and we have

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

Since ψ is fixed point free, it follows easily that ζ is unique. If ψ is abelian, then one sees easily that ψ' is abelian. □

Let $\mathcal{F} \supseteq \mathcal{F}_{ab} \supseteq \mathcal{Z}$ be the set of fixed point free endomorphisms of G, resp. abelian fixed point free endomorphisms, resp. fixed point free endomorphisms with image contained in the center $Z(G)$ of G.

Corollary 3. *The number of Hopf Galois structures on $GL|L$ induced by fixed point free endomorphisms of G is $\#\mathcal{F}/\#\mathcal{Z}$. If G has trivial center, then every fixed point free endomorphism of G yields a distinct Hopf Galois structure of LG on GL induced by the regular subgroup $\alpha_\psi(G)$ of $Perm(G)$.*

Proof. The Hopf Galois structures on $GL|L$ are in one-to-one correspondence with regular subgroups of $Perm(G)$, by [GP87]. For ψ, ψ' in $\mathcal{F}$, if we write $\psi \sim \psi'$ if $\alpha_\psi(G) = \alpha_{\psi'}(G)$, then $\sim$ is an equivalence relation on $\mathcal{F}$, and by Theorem 2, the equivalence class of each ψ in $\mathcal{F}$ has the same cardinality as $\mathcal{Z}$. So $\#\mathcal{F}/\#\mathcal{Z}$ is the number of equivalence classes. The last sentence of the corollary corresponds to $\#\mathcal{Z} = 1$. □

The action of $\alpha_\psi(G)$ on GL is given by

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

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.

3. K-Hopf Galois structures

For ψ a fixed point free endomorphism of G, we have the regular embedding $\alpha_\psi : G \to Perm(G)$ 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 an 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 $f : L\lambda(G) \to L\alpha_\psi(G)$ 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 $H_\psi = L\alpha_\psi(G)^G$. □

Corollary 6. *The number of H_λ-Hopf Galois structures on $L|K$ induced from abelian fixed point free endomorphisms of G is $\#\mathcal{F}_{ab}/\#\mathcal{Z}$. In particular, if the center of G is trivial, then the H_λ-Hopf Galois structures arising from endomorphisms in $\mathcal{F}_{ab}$ are all distinct.*

Remark 7. Given an endomorphism ψ of G, [CaC99] and [CCo07] also considered the embedding $\beta_\psi : G \to Perm(G)$ given by $\beta_\psi(g) = \lambda(\psi(g))\rho(g)$. One may verify easily that if the center of G is trivial, then $\beta_\psi(G)$ is normalized by $\lambda(G)$ iff $\psi(G)$ is trivial, in which case $\beta_\psi(G) = \rho(G)$, which descends to the classical Galois structure on $L|K$.

4. 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. Given a finite group G, let N be a group of the same cardinality as G. Byott's translation shows that 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], [CCo07], [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) $b : G \to N$ 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 yields 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 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 (not necessarily abelian) fixed point free endomorphism of G. Set $\beta : G \to Hol(G)$ by

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

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

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

Then the corresponding embedding $\alpha : G \to Perm(G)$ 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 8. *Let ψ, θ be fixed point free endomorphisms of G. Let $b : G \to G$ by $b(\sigma) = \sigma\psi(\sigma^{-1})$, and $c : G \to G$ by $c(\tau) = \tau\theta(\tau^{-1})$. Then b and c are inverse bijections if and only if for all σ in G,*

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

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

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

Given ψ, if there is an endomorphism θ so that $\theta(\psi(\sigma)) = \psi(\sigma)\theta(\sigma)$, then we call θ the *inverse* of ψ. The endomorphism θ is unique, since it is uniquely determined by $c = b^{-1}$. It is easy to see that if ψ is abelian and θ is the inverse of ψ, then θ is abelian. (Since abelian endomorphisms of nonabelian groups are never automorphisms, the use of "inverse" in this context is perhaps not too perverse.)

Corollary 9. *Let ψ be a fixed point free endomorphism of G, and define the regular embedding $\beta : G \to Hol(G)$ by $\beta(\tau) = \lambda(\tau)\rho(\psi(\tau))$. If ψ has an inverse θ, then the corresponding regular embedding α of G into $Perm(G)$ is defined by $\alpha(\sigma) = \lambda(\sigma)\rho(\theta(\sigma))$.*

Proof. The maps $b, c : G \to G$ corresponding to ψ, θ are

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

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 Theorem 5 shows that the Hopf Galois action on a field extension $L|K$ corresponding to θ in Corollary 9 is via the Hopf algebra H_λ.

Remark 10. Fixed point free endomorphisms of abelian groups do not yield nontrivial Hopf Galois structures. But we note that if G is abelian, written additively, and ψ is a fixed point free endomorphism of G, then ψ always has an inverse. For $b = I - \psi$ is an automorphism of G. Let $\theta = I - b^{-1}$. Then θ is a fixed point free endomorphism of G, and $I = bb^{-1}$ implies that $\theta\psi = \theta + \psi$. Thus if G is abelian, then every fixed point free endomorphism of G has an inverse.

5. 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 nonabelian simple group there are no nontrivial fixed point free endomorphisms; cf. [Go82, p. 55].) Hence every nontrivial fixed point free endomorphism induces a homomorphism from S_n/A_n into S_n, so is abelian. For the endomorphism to be fixed point free, the nontrivial coset must map to an even permutation of order 2. Each such nontrivial fixed point free endomorphism of S_n yields a distinct action of H_λ on a Galois extension $L|K$ with Galois group S_n.

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

Examples involving abelian by cyclic semi-direct products. Let A be a finite abelian group of order n, written additively, and let $G = A \rtimes \langle\beta\rangle$, where β in $Aut(A)$ has order d with $(n, d) = 1$. We assume that the center of G is trivial. It is routine to see that the center of G is $\{z \in A : (\beta - 1)(z) = 0\}$. So the assumption on the center is equivalent to the condition that $\beta - 1$ is injective on A.

We wish to define ψ, an endomorphism of G.

Since β has order prime to n, then for each $f \neq 0$ in A, $\psi(f, 1) = (g, 1)$ for some g in A. Thus ψ restricts to an endomorphism of A that we also denote by ψ. Thus $\psi(f, 1) = (\psi(f), 1)$. Let $\psi(0, \beta) = (h, \beta^s)$.

Since $(0, \beta)(f, 1) = (\beta(f), 1)(0, \beta)$ in G and ψ is an endomorphism,

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

that is,

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

If $s = 0$, then $h = 0$ and $\psi(f) = \psi(\beta(f))$. Since $\beta - 1$ is injective on A, it follows that $\psi(A) = 0$, and so ψ is trivial.

If $s \neq 0$, then for ψ to be an endomorphism of G we must have

$$\psi(0, \beta^d) = ((1 + \beta^s + \ldots + \beta^{s(d-1)})(h), \beta^{sd}) = (0, 1).$$

This condition holds if and only if $(1 + \beta^s + \ldots + \beta^{s(d-1)})(h) = 0$. To insure that condition holding, we restrict s so that $\beta^s - 1$ is injective on A. Then

$$(\beta^s - 1)(1 + \beta^s + \ldots + \beta^{s(d-1)})(h) = (\beta^{sd} - 1)(h) = 0,$$

so $\psi(0, \beta^d) = (0, 1)$.

For ψ to be an abelian endomorphism, for all f in A,

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

that is,

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

hence $\beta^s(\psi(f)) = \psi(f)$. Since $\beta^s\psi = \psi\beta$, the abelian condition on ψ thus implies that $\psi\beta = \psi$ on A. Since $\beta - 1$ is injective on A, ψ must be trivial on A. Conversely, if ψ is trivial on A, then ψ is abelian.

So henceforth we assume that ψ is an abelian endomorphism of G as described in the next proposition.

Proposition 11. *Let $G = A \rtimes \langle \beta \rangle$ as above, and let ψ be an abelian endomorphism of G such that $\psi(f, 1) = (0, 1)$ for all f in A and $\psi(0, \beta) = (h, \beta^s)$ for some h in A, where $s \neq 0$ and $\beta^s - 1$ is injective on A. Then ψ is fixed point free on G iff $(s - 1, d) = 1$.*

Proof. We try to solve $\psi(g, \beta^t) = (g, \beta^t)$. Since $\psi(g) = 0$, this is equivalent to

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

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

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

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, we let

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

Then (g, β^t) is a fixed point of ψ.

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 $g = 0$. Thus ψ is fixed point free. □

For these endomorphisms, we can find the inverse of ψ:

Proposition 12. *Let $G = A \rtimes \langle \beta \rangle$, where β is an element of $Aut(A)$ with $\beta^d = 1$, where $(d, n) = 1$. Let $\psi : G \to G$ be the abelian fixed point free endomorphism with $\psi(f, 1) = (0, 1)$ for f in A and $\psi(0, \beta) = (h, \beta^s)$ with $\beta^s - 1$ injective on A, and $(s - 1, d) = 1$. Define t by $(s - 1)(t - 1) \equiv 1 \pmod{d}$, and g in A by $(\beta^s - 1)(g) = (\beta^t - 1)(h)$. Then $\theta : G \to G$, defined by $\theta(f, 1) = (0, 1)$ and $\theta(0, \beta) = (g, \beta^t)$, is an abelian fixed point free endomorphism of G and is the inverse of ψ.*

Proof. We first observe that $\beta^t - 1$ is injective. Since $(s-1)(t-1) \equiv 1 \pmod{d}$, $\beta^{t(s-1)} = \beta^s$, so if $\beta^t(g) = g$ for some nonzero g in A, then $\beta^s(g) = g$. Thus if $\beta^s - 1$ is injective on A, so is $\beta^t - 1$.

The argument that θ is an abelian, fixed point free endomorphism of G then follows that for ψ, above.

The condition $(\beta^s - 1)(g) = (\beta^t - 1)(h)$ implies easily that $\psi(0, \beta)$ and $\theta(0, \beta)$ commute.

To show that θ is the inverse of ψ, it suffices (since θ and ψ are both trivial on A) to show that for all n,

$$\theta(\psi(0, \beta^n)) = \psi(0, \beta^n)\theta(0, \beta^n).$$

Since θ and ψ are both endomorphisms and $\psi(0, \beta)$ and $\theta(0, \beta)$ commute, it suffices to show that

$$\theta\psi(0, \beta) = \psi(0, \beta)\theta(0, \beta).$$

This becomes

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

or

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

or

$$(g + \beta^t g + \ldots + \beta^{t(s-1)}g, \beta^{ts}) = (h + \beta^s(g), \beta^{s+t}).$$

Since $(s-1)(t-1) \equiv 1 \pmod{d}$, we have $\beta^{s+t} = \beta^{st}$, so it suffices to check that

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

Applying the injective map $(\beta^t - 1)$ to both sides yields

$$(\beta^{ts} - 1)(g) = (\beta^t - 1)(h) + (\beta^t - 1)\beta^s(g)$$

or

$$((\beta^{ts} - 1) - (\beta^{s+t} - \beta^s))(g) = (\beta^t - 1)(h),$$

which follows from the assumptions $\beta^{s+t} = \beta^{st}$ and $(\beta^s - 1)(g) = (\beta^t - 1)(h)$. Thus θ is the inverse of ψ, as claimed. □

In case A is cyclic, the examples above specialize to those in [CCo07].

Dihedral groups. Let $G = D_m$, the dihedral group of order $2m$. If m is odd, then by Proposition 11 and the discussion preceding Proposition 11, G has no nontrivial abelian fixed point free endomorphisms.

On the other hand, 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 nontrivial abelian fixed point free endomorphisms $\psi : G \to G$:

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

Examples (1)-(3) are in $\mathcal{Z}$, i.e. have image in the center of G.

There are $4m$ endomorphisms of types (4)-(7). If m is even, there are four endomorphisms in $\mathcal{Z}$; hence by Corollary 6 the number of Hopf Galois structures on a Galois extension $L|K$ with Galois group $G = D_{2m}$ induced by abelian fixed point free endomorphisms of G is $m + 1$. If m is odd, $\#\mathcal{Z} = 2$, so the number of Hopf Galois structures is $2m + 1$.

All of these endomorphisms are their own inverses except for the endomorphisms of types (5) and (7). If m is even, then the inverse of ψ_i of type (5) (resp. of type (7)) is ψ_{m+i} of type (5) (resp. of type (7)); if m is odd, then the inverse of ψ_i of type (5) is ψ_{m+i} of type (7).

References

[By96] N. P. Byott, Uniqueness of Hopf Galois structure of separable field extensions, Comm. Algebra 24 (1996), 3217-3228. MR1402555 (97j:16051a)

[By02] N. P. Byott, Integral Hopf-Galois structures on degree p^2 extensions of p-adic fields, J. Algebra 248 (2002), 334-365. MR1879021 (2002j:11142)

[By04] N. P. Byott, Hopf-Galois structures on field extensions with simple Galois groups, Bulletin of the London Mathematical Society 36 (2004), 23-29. MR2011974 (2004i:16049)

[CaC99] S. Carnahan, L. N. Childs, Counting Hopf Galois structures on non-abelian Galois field extensions, J. Algebra 218 (1999), 81-92. MR1704676 (2000e:12010)

[Ch00] L. N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, Mathematical Surveys and Monographs **80**, American Mathematical Society, 2000. MR1767499 (2001e:11116)

[Ch03] L. N. Childs, On Hopf Galois structures and complete groups, New York J. Math. 9 (2003), 99-115. MR2016184 (2004k:16097)

[Ch05] L. N. Childs, Elementary abelian Hopf Galois structures and polynomial formal groups, J. Algebra 283 (2005), 292-316. MR2102084 (2005g:16073)

[Ch07] L. N. Childs, Some Hopf Galois structures arising from elementary abelian p-groups, Proc. Amer. Math. Soc. 135 (2007), 3453-3460. MR2336557 (2008j:16107)

[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. MR2290920 (2007j:20026)

[Go82] D. Gorenstein, *Finite Simple Groups, An Introduction to Their Classification*, Plenum, New York/London, 1982. MR698782 (84j:20002)

[GP87] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions, J. Algebra 106 (1987), 239-258. MR878476 (88i:12006)

[Ko07] T. Kohl, Groups of order $4p$, twisted wreath products and Hopf-Galois theory, J. Algebra 314 (2007), 42-74. MR2331752 (2008e:12001)

Department of Mathematics and Statistics, University at Albany, Albany, New York 12222

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