QUASI-INVERSE ENDOMORPHISMS

A. CARANTI

Abstract. Greither and Pareigis have established a connection between Hopf Galois structures on a Galois extension $L/K$ with Galois group $G$, and the regular subgroups of the group of permutations on $G$, which are normalized by $G$. Byott has rephrased this connection in terms of certain equivalence classes of injective morphisms of $G$ into the holomorphs of the groups $N$ with the same cardinality of $G$.

Childs and Corradino have used this theory to construct such Hopf Galois structures, starting from fixed-point-free endomorphisms of $G$ that have abelian images. In this paper we show that a fixed-point-free endomorphism has an abelian image if and only if there is another endomorphism that is its inverse with respect to the circle operation in the near-ring of maps on $G$, and give a fairly explicit recipe for constructing all such endomorphisms.

1. Introduction

Our starting point is the paper [Chi12], in which Childs begins by reviewing the theory of Greither and Pareigis [GP87]. This theory establishes a bijection between Hopf Galois structures on a Galois extension $L/K$ of fields with Galois group $G$, and the regular subgroups of the group of permutations on $G$, which are normalized by $G$. Byott [By96a, By96b] has shown that the problem of determining these regular subgroups can be translated into that of finding certain equivalence classes of injective morphisms of $G$ into the holomorphs of the groups $N$ with the same cardinality of $G$. Childs and Corradino [CC07] and Childs [Chi07] have showed that abelian fixed-point-free endomorphisms of $G$ yield directly, via the above theory, such Hopf Galois structures. (Here we say with [Chi12] that an endomorphism is abelian if its image is abelian.) We refer to [Chi12] and [Chi00] for the details.

Childs studies in particular those Hopf Galois structures that arise from the abelian fixed-point-free endomorphism $\varphi$ of $G$ that admit an inverse endomorphism $\psi$ with respect to the circle operation $\varphi \circ \psi = \psi - \varphi \psi + \varphi$. (Childs calls $\psi$ the inverse of $\varphi$. Since he only considers fixed-point-free endomorphisms that are not automorphisms, the term is unambiguous in his context. In this paper we will have to deal also with fixed-point-free automorphisms, and with inverses with respect to map composition. We have thus preferred to use the classical term quasi-inverse for $\psi$ [Jac64, Chap. 1, Section. 5].)

Date: 14 December 2012, 11:29 CET — Version 5.01.
2010 Mathematics Subject Classification. 20D45 16N20 16Y30.
Key words and phrases. Hopf Galois structures, finite groups, fixed-point-free endomorphisms, quasi-inverse, near-ring.
In this paper we study the fixed-point-free endomorphisms of a finite group that have a quasi-inverse. We will show that for a fixed-point-free endomorphism of a finite group the properties of being abelian, and that of having a quasi-inverse, are equivalent (Theorem 3.4, which extends [Chi12, Remark 10], and shows that the condition of having a quasi-inverse is not restrictive in the context of [Chi12]). In Sections 4 and 7 we are able to give reasonably explicit recipes for constructing the groups that have such an endomorphism, and for determining all of their endomorphisms with this property. Our main tool is a version for groups of Fitting’s Lemma for modules (Section 4). We are then led to study fixed-point-free endomorphisms of finite abelian groups (Section 5), abelian nilpotent endomorphisms (Section 6), and how to put the two together (Section 7). In Section 8 we will be reviewing the examples of [Chi12] from our point of view, and provide some more.

2. Preliminaries

Let $G$ be a group, multiplicatively written. In our context, it is convenient to write maps on $G$ as exponents. Given two maps $\varphi, \psi$ on $G$, we define as usual their pointwise sum $\varphi + \psi$ by $x^{\varphi + \psi} = x^\varphi x^\psi$, for $x \in G$ and their product $\varphi \psi$ as their composition, $x^{\varphi \psi} = (x^\varphi)^\psi$. It is well known that these operations define a structure of a near-ring on the set $N(G)$ of maps on $G$. (See [Pil83].) The sum is not commutative in general, and only the distributive relation $\varphi (\psi + \vartheta) = \varphi \psi + \varphi \vartheta$ holds generally, while if $\varphi$ is an endomorphism of $G$, we also have $(\psi + \vartheta) \varphi = \psi \varphi + \vartheta \varphi$. Note also that for a map $\varphi$ on $G$, $-\varphi$ is defined by $\varphi + (-\varphi) = 0$ (where $x^0 = 1$ for all $x \in G$), so that $x^{-\varphi} = (x^\varphi)^{-1}$ for $x \in G$. Thus $-(\varphi + \psi) = -\psi - \varphi$ for maps $\varphi, \psi$ on $G$.

If $\varphi, \psi$ are endomorphisms of $G$, their sum $\varphi + \psi$ is not in general an endomorphism of $G$. We have

**Proposition 2.1.** Let $G$ be a group, $\varphi, \psi \in \text{End}(G)$. The following are equivalent

1. $\varphi + \psi \in \text{End}(G)$, and
2. $[G^\varphi, G^\psi] = 1$, that is, the images of $\varphi$ and $\psi$ commute elementwise.

Moreover, these conditions imply $\varphi + \psi = \psi + \varphi$.

**Proof.** $(ab)^{\varphi + \psi} = (ab)^\varphi (ab)^\psi = a^\varphi b^\varphi a^\psi b^\psi$ equals $a^{\varphi + \psi} b^{\varphi + \psi} = a^\varphi a^\psi b^\varphi b^\psi$ for all $a, b \in G$ if and only if $b^\varphi a^\psi = a^\psi b^\varphi$ for all $a, b \in G$. Setting $b = a$ in the last identity we obtain $\varphi + \psi = \psi + \varphi$. \qed

**Definition 2.2.** Let $\varphi$ be an endomorphism of the group $G$. A fixed point of $\varphi$ is an element $x \in G$ such that $x^\varphi = x$. We say that $\varphi$ is fixed-point-free if its only fixed point is 1.

The following is well-known [Gor68, Lemma 1.1., Chap. 10].

**Proposition 2.3.** Let $G$ be a finite group, $\varphi \in \text{End}(G)$. The following are equivalent:

1. the map $1 - \varphi$ is injective, and thus a bijection on $G$, and
2. $\varphi$ is fixed-point-free.
Proof. $x^{1-\varphi} = xx^{-\varphi} = yy^{-\varphi} = y^{1-\psi}$ if and only if $y^{-1}x = (y^{-1}x)^\varphi$, that is, $y^{-1}x$ is a fixed point of $\varphi$. □

3. QUASI-INVERSE ENDOMORPHISMS

Childs studies in [Chi12] the fixed-point-free endomorphisms $\varphi$ such that $1 - \varphi$ has an inverse of the same form $1 - \psi$, for some endomorphism $\psi$ of $G$.

Definition 3.1. Let $G$ be a finite group. A fixed-point-free endomorphisms $\varphi$ of $G$ is said to be quasi-invertible if there is an endomorphism $\psi$ of $G$ such that the map $1 - \psi$ is the inverse of the map $1 - \varphi$ with respect to map composition. $\psi$ is said to be the quasi-inverse of $\varphi$.

Clearly $\psi$ is also fixed-point-free by Proposition 2.3 and $\psi$ is uniquely determined by $\varphi$. A familiar argument shows that if $\psi$ is the quasi-inverse of $\varphi$, then $1 = (1 - \varphi)(1 - \psi) = 1 - \varphi + \varphi\psi - \psi$, so that $-\varphi + \varphi\psi - \psi = 0$, or

$$
\varphi + \psi = \varphi\psi.
$$

In other words, $\psi$ is the inverse of $\varphi$ with respect to the circle operation $\varphi \circ \psi = \psi - \varphi\psi + \varphi$ on the near-ring $N(G)$. Thus $\varphi$ is right quasi-regular in the classical radical theory of Jacobson [Jac64, Chap. 1, Section. 5], the catch here being that we require the (right) quasi-inverse $\psi$ of $\varphi$ to be another endomorphism of $G$.

Since $\varphi + \psi = \varphi\psi \in \text{End}(G)$, we have by Proposition 2.1 $\varphi + \psi = \psi + \varphi$, and thus $\varphi\psi = \psi\varphi$. Also, $[G^\varphi, G^\psi] = 1$. Now we can rewrite (3.1) as

$$
\varphi = -\psi + \varphi\psi = (-1 + \varphi)\psi,
$$

as $\psi \in \text{End}(G)$. This shows that $G^\varphi \subseteq G^\psi$ and then by symmetry (or because $-1 + \varphi$ is a bijection) $G^\varphi = G^\psi$. Also, if $x \in \ker(\varphi)$, then $1 = x^\varphi = x^{(-1+\varphi)\psi} = (x^{-1})^\psi$, so that $x \in \ker(\psi)$, and thus $\ker(\varphi) = \ker(\psi)$. We have obtained

Proposition 3.2. Let $G$ be a finite group, $\varphi, \psi$ two fixed-point-free endomorphisms of $G$ that are one the quasi-inverse of the other. Then

1. $\varphi + \psi = \psi + \varphi$ and $\varphi\psi = \psi\varphi$,
2. $G^\varphi = G^\psi$ is an abelian subgroup of $G$, and
3. $\ker(\varphi) = \ker(\psi)$.

We take, as in [Chi12, Definition 1], the following

Definition 3.3. An endomorphism $\varphi$ of the group $G$ is said to be abelian if its image $G^\varphi$ is abelian, or equivalently $G'' \leq \ker(\varphi)$.

Thus all quasi-invertible fixed-point-free endomorphisms $\varphi$ of the finite group $G$ are abelian. We have in fact

Theorem 3.4. Let $G$ be a finite group, $\varphi$ a fixed-point-free endomorphism of $G$. The following are equivalent:

1. $\varphi$ is quasi-invertible, and
2. $\varphi$ is abelian.

We defer the proof to Section 7.
4. **Fitting’s Lemma**

The following is a standard result in the theory of modules [Jac80, p. 113].

**Theorem 4.1** (Fitting’s Lemma). Let $A$ be a ring, and $M$ an $A$-module that is both artinian and noetherian.

Let $\varphi$ be an endomorphism of $M$. Then there is a a natural number $n$ such that $\ker(\varphi^n) = \ker(\varphi^{n+i})$ and $M^{\varphi^n} = M^{\varphi^{n+i}}$ for each $i \geq 0$. We have

$$M = \ker(\varphi^n) \oplus G^{\varphi^n}.$$ 

Moreover, the restriction of $\varphi$ to $\ker(\varphi^n)$ is nilpotent, and the restriction of $\varphi$ to $G^{\varphi^n}$ is an automorphism.

The following version for groups is folklore.

**Theorem 4.2** (Fitting’s Lemma for groups). Let $G$ be a group which satisfies the ascending chain condition on normal subgroups, and the descending chain condition on subgroups.

Let $\varphi$ be an endomorphism of $G$. Then there is a natural number $n$ such that $\ker(\varphi^n) = \ker(\varphi^{n+i})$ and $G^{\varphi^n} = G^{\varphi^{n+i}}$ for each $i \geq 0$. We have:

1. $G$ is the semidirect product of the normal subgroup $K = \ker(\varphi^n)$ by the subgroup $H = G^{\varphi^n}$,
2. the restriction of $\varphi$ to $K$ is nilpotent, and
3. the restriction of $\varphi$ to $H$ is an automorphism.

We give a proof that is basically the one recorded in [Car85] for finite groups.

**Proof.** An integer $n$ as in the statement exists because of the chain conditions. Set $H = G^{\varphi^n}$, $K = \ker(\varphi^n)$. We claim that $G$ is the semidirect product of $K$ by $H$.

In fact, $K = \ker(\varphi^n)$ is normal in $G$. For each $x \in G$, we have $x^{\varphi^n} \in G^{\varphi^n} = G^{\varphi^{n+i}}$.

Thus there is $y \in G$ such that $x^{\varphi^n} = y^{\varphi^{2n}}$. Then

$$(y^{\varphi^n} x)^{\varphi^n} = y^{\varphi^{2n}} x^{\varphi^n} = 1$$

that is, $y^{\varphi^n} x \in K$, so that $x = y^{\varphi^n} (y^{\varphi^n} x) \in HK$, and $G = HK$. Now $\varphi$ is surjective on $H = G^{\varphi^n} = G^{\varphi^{n+i}}$. If $x \in H \cap K$, then there is $y \in G$ such that $x = y^{\varphi^n}$, and $y^{\varphi^{2n}} = x^{\varphi^n} = 1$, so that $y \in \ker(\varphi^{2n}) = \ker(\varphi^n)$, and $x = 1$. It follows that $H \cap K = 1$, and since $\ker(\varphi) \leq K$, also that $\varphi$ is injective on $H$. □

**Proposition 3.2** yields readily

**Lemma 4.3.** If the fixed-point-free endomorphism $\varphi$ of the finite group $G$ has a quasi-inverse $\psi$, then $\psi$ acts on $K = \ker(\varphi^n)$ and $H = G^{\varphi^n}$.

**Theorem 4.2** and **Lemma 4.3** now yield two recipes,

1. one for constructing all finite groups that have a quasi-invertible fixed-point-free endomorphisms,
2. the other for constructing all such endomorphisms for a given finite group.

The first recipe is the following.

1. Take an arbitrary finite group $K$ and a finite abelian group $H$. 
(2) Take a fixed-point-free automorphism $\vartheta$ of $H$ (Section 5).
(3) Take a nilpotent endomorphism $\eta$ of $K$ which is abelian, that is, such that $K' \leq \ker(\eta)$ (Section 6).
(4) Construct a semidirect product $G$ of $K$ by $H$ such that $[K, H] \leq \ker(\eta)$ and $[H^0, K^\eta] = 1$, and define the quasi-invertible fixed-point-free endomorphism $\varphi$ of $G$ via its restrictions $\eta$ on $K$ and $\vartheta$ on $H$ (Theorem 7.2 of Section 7).

If we are already given a finite group $G$, this reads as follows.
(1) Write $G$ as the semidirect product of a normal subgroup $K$ by an abelian subgroup $H$.
(2) Take a fixed-point-free automorphism $\vartheta$ of $H$.
(3) Take a nilpotent endomorphism $\eta$ of $K$ such that $G' = K'[K, H] \leq \ker(\eta)$ and $[H^\vartheta, K^\eta] = 1$.
(4) Define the quasi-invertible fixed-point-free endomorphism $\varphi$ of $G$ via its restrictions $\eta$ on $K$ and $\vartheta$ on $H$.

5. The abelian case

If $\varphi$ is a fixed-point-free endomorphism of the abelian group $G$, then $\varphi$ clearly is quasi-invertible, as noted in [Chi12, Remark 10]. In fact, $1 - \varphi$ is an automorphism of $G$ here, so its inverse (with respect to map composition) is also an automorphism of $G$, and $\psi = -(1 - \varphi)^{-1} + 1 \in \text{End}(G)$ is the quasi-inverse of $\varphi$.

Since the Sylow $p$-subgroups of $G$ are fully invariant, we need only consider the case of finite abelian $p$-groups. We give a description of the fixed-point-free endomorphisms of a finite abelian $p$-group $G$, based on the approach of [HR07] to the automorphisms of a finite abelian $p$-group.

So let $G$ be a finite abelian $p$-group. Write $G$ as the direct product of homocyclic components
\begin{equation}
G = H_1 \times H_2 \times \ldots \times H_n,
\end{equation}
where each $H_i$ is homocyclic, of exponent $p^{e_i}$, with
\begin{equation}
0 < e_1 < e_2 < \cdots < e_n.
\end{equation}
(Clearly this decomposition is not unique in general.) If $u \in G$, we will write $u_i$ for the $i$-th component of $u$ with respect to the decomposition (5.1) that is, each $u_i \in H_i$ and $u = u_1 \cdot u_2 \cdot \ldots \cdot u_n$.

Let $\vartheta_i : H_i \to G$ and $\pi_i : G \to H_i$ be the injections and projections with respect to the decomposition (5.1). If $\alpha \in \text{End}(G)$, write
\begin{equation}
\alpha_{ij} = \vartheta_i \circ \alpha \circ \pi_j : H_i \to H_j
\end{equation}
for the $(i, j)$-th component of $\alpha$ and
\begin{equation}
\beta_i = \alpha_{ii} \big|_{\Omega_1(H_i)}
\end{equation}
for the restriction of $\alpha_{ii}$ to $\Omega_1(H_i) = \{ x \in H_i : x^p = 1 \}$. Then we have
\begin{equation}
u^\alpha = \prod_{i,j=1}^n u_i^{\alpha_{ij}} = \prod_{j=1}^n \left( \prod_{i=1}^n u_i^{\alpha_{ij}} \right),
\end{equation}
with $\prod_{i=1}^{n} u_{i}^{\alpha_{ij}} \in H_{j}$.

Our characterization of fixed-point-free endomorphisms of $G$ is the following:

**Proposition 5.1.** In the above notation, the following are equivalent:

1. $\alpha$ is a fixed-point-free endomorphism of $G$, and
2. each $\beta_{i}$ is a fixed-point-free endomorphism of $\Omega_{1}(H_{i})$.

Note that we can read off the action of $\beta_{i}$ also on $H_{i}/H_{i}^{p}$.

**Proof.** Clearly an endomorphism of $G$ has a nontrivial fixed point if and only if it has a fixed point of order $p$.

Suppose first that each $\beta_{i}$ is fixed-point-free on $\Omega_{1}(H_{i})$. Let $u \in \Omega_{1}(G)$ be a fixed point of $\alpha$. If $i > j$, then $p^{e_{i}} = \exp(H_{i}) > \exp(H_{j}) = p^{e_{j}}$, so that $\Omega_{1}(H_{i}) \leq \ker(\alpha_{ij})$. Therefore we have, according to (5.2),

$$
\begin{align*}
\left\{ \begin{array}{l}
u_{1}^{\beta_{1}} = u_{1} \\
u_{1}^{\alpha_{12}} \cdot u_{2}^{\beta_{2}} = u_{2} \\
\vdots \\
u_{1}^{\alpha_{1n}} \cdot u_{2}^{\alpha_{2n}} \cdot \ldots \cdot u_{n}^{\beta_{n}} = u_{n}
\end{array} \right.
\end{align*}
$$

so that we have $u_{1} = 0$ from the first identity, and then $u_{2} = 0$ from the second one, and so on, so that $u = 0$.

Conversely, suppose some of the $\beta_{i}$ have nontrivial fixed points, and let $k$ be the largest index $i$ for which this happens, so that $\beta_{k+1}, \ldots, \beta_{n}$ are fixed-point-free. We want to construct a fixed point $u$ of $\alpha$ of order $p$. We build $u$ as $u = u_{k} \cdot u_{k+1} \cdot \ldots \cdot u_{n}$, where the $u_{i} \in \Omega_{1}(H_{i})$ are determined as follows. Here (5.3) reads

$$
\begin{align*}
\left\{ \begin{array}{l}
u_{k}^{\beta_{k}} = u_{k} \\
u_{k}^{\alpha_{k,k+1}} \cdot u_{k+1}^{\beta_{k+1}} = u_{k+1} \\
\vdots \\
u_{k}^{\alpha_{k,n}} \cdot u_{k+1}^{\alpha_{k+1,n}} \cdot \ldots \cdot u_{n}^{\beta_{n}} = u_{n}
\end{array} \right.
\end{align*}
$$

Choose $1 \neq u_{k} \in \Omega_{1}(H_{k})$ as a nontrivial fixed point of $\beta_{k}$, so that the first equation is satisfied. Now the second equation reads

$$
\begin{align*}
u_{k}^{\alpha_{k,k+1}} = u_{k+1}^{1-\beta_{k+1}}.
\end{align*}
$$

Since $\beta_{k+1}$ is fixed-point-free on $\Omega_{1}(H_{k+1})$, the function $1 - \beta_{k+1}$ is bijective on $\Omega_{1}(H_{k+1})$ by Proposition 2.3, so that there is a $u_{k+1} \in \Omega_{1}(H_{k+1})$ which fulfills (5.5). Proceeding in the same fashion, we find values for $u_{k+1}, \ldots, u_{n}$ that satisfy all the equations of (5.4), so that the resulting $u$ is a nontrivial fixed point of $\varphi$ of order $p$. \qed

6. **Nilpotent endomorphisms**

We record a couple of immediate facts here.

**Proposition 6.1.** Let $G$ be a finite group, $\varphi$ a nilpotent endomorphism of $G$. Then $\varphi$ is fixed-point-free. Moreover, the following are equivalent

1. $\varphi$ is quasi-invertible, and
2. $\varphi$ is abelian.
Proof. If $\varphi^n = 0$, and $x = x^p$ for some $x \in G$, then $x = x^{p^n} = 1$.

If $\varphi$ is quasi-invertible, then $G^\varphi$ is abelian by Proposition 3.2.

Conversely, let $G^\varphi$ be abelian. The inverse (with respect to map composition) of the map $1 - \varphi$ is clearly $1 + \varphi + \varphi^2 + \cdots + \varphi^{n-1}$, so if $\varphi$ has a quasi-inverse $\psi$, then this is $\psi = -(1 + \varphi + \cdots + \varphi^{n-2})$. But $\psi$ is the composition of $\varphi$ with the restriction of $-(1 + \varphi + \cdots + \varphi^{n-2})$ to $G^\varphi$. Since the latter group is abelian, $-(1 + \varphi + \cdots + \varphi^{n-2})$ is an endomorphism of $G^\varphi$ by Proposition 2.1, so that $\psi$ is an endomorphism of $G$, and thus $\psi$ is indeed the quasi-inverse of $\varphi$. □

7. Piecing endomorphisms together

Let $G$ be the semidirect product of the normal subgroup $K$ by the subgroup $H$. Let $\vartheta \in \text{End}(H)$, $\eta \in \text{End}(K)$. We define a map $\varphi$ on $G$, the semidirect product of $K$ by $H$, by letting

$$ (hk)\varphi = h^\vartheta k^\eta, $$

for $h \in H$ and $k \in K$. This will be an endomorphism of $G$ and only if for all $h, h' \in H$ and $k, k' \in K$

$$(h'khk')^\varphi = (h'hk^h k')^\varphi = h'^\vartheta h^\vartheta (k^h)^\eta k'^\eta
$$

equals

$$(h'k)^\varphi(k'^\eta) = h'^\vartheta k^\eta h^\vartheta k'^\eta. $$

This means

$$ (k^h)^\eta = (k^\eta)^h^\vartheta, $$

for all $h \in H$ and $k \in K$, that is, $\eta : K \to K$ is a twisted morphism of $H$-modules, or equivalently, multiplying both sides of the previous equations on the left by $k^{-\eta}$,

$$ [k, h]^\eta = [k^\eta, h^\vartheta] $$

for all $h \in H$ and $k \in K$. Now we note

Lemma 7.1. If $\varphi$ is an abelian fixed-point-free endomorphism of the finite group $G$, then both terms of (7.2) vanish for all $h \in H$ and $k \in K$.

Proof. The right-hand term vanishes because $G^\varphi$ is abelian and contains $H^\vartheta$ and $K^\eta$, and the left one vanishes since $[K, H] \leq G' \cap K \leq \ker(\varphi) \cap K \leq \ker(\eta)$, again because $G^\varphi$ is abelian. □

We may state

Theorem 7.2. Let the finite group $G$ be the semidirect product of the group $K$ by the abelian group $H$. Let $\vartheta$ be a fixed-point-free endomorphism of $H$, and $\eta$ be a nilpotent endomorphism of $K$. Define a map $\varphi$ on $G$ by

$$ (hk)^\varphi = h^\vartheta k^\eta, $$

for $h \in H$ and $k \in K$.

Then the following are equivalent

(1) $\varphi$ is a quasi-invertible fixed-point-free endomorphism, and

(2) $G' = K'[K, H] \leq \ker(\eta)$, and $[K^\eta, H^\vartheta] = 1$. 

Note that the condition \( G' \leq \ker(\eta) \) contains both the condition \([K, H] \leq \ker(\eta)\), that we have seen to be necessary for \( \varphi \) to be an abelian endomorphism, and the condition \( K' \leq \ker(\eta) \) which states that \( \eta \) is an abelian endomorphism.

**Proof.** We are only left with proving that \( \varphi \) has a quasi-inverse under the hypotheses on \( \eta, \partial \), and the conditions of (2). Now by the results of Sections 3 and 9, the endomorphisms \( \eta \) and \( \vartheta \) have quasi-inverses \( \eta' \) and \( \vartheta' \). By the conditions of (2), and Proposition 8.2, we have \([K, H] \leq \ker(\eta) = \ker(\eta')\) and \([K^{\vartheta}, H^{\vartheta}] = [K^{\eta}, H^{\vartheta}] = 1\), so that the conditions for \( \eta' \) and \( \vartheta' \) to induce an endomorphism \( \psi \) of \( G \) are satisfied.

This will be the quasi-inverse of \( \varphi \), as for \( h \in H \) and \( k \in K \) we have

\[
(hk)^{-\varphi + \vartheta'} = (hk)^{-\varphi}(hk)^{\vartheta'} = k^{-\eta}h^{-\vartheta}h^{\vartheta'}k^{\eta'}h^{-\vartheta'} = k^{-\eta}h^{-\vartheta}h^{\vartheta'}k^{\eta'}h^{-\vartheta'}.
\]

Now all terms commute, as \( K^{\vartheta} = K^{\vartheta'} \), \( H^{\vartheta} = H^{\vartheta'} \) are abelian and \([K^{\vartheta}, H^{\vartheta}] = 1\). So we have

\[
(hk)^{-\varphi + \vartheta'} = h^{-\vartheta}k^{\eta'}h^{-\vartheta'}k^{\eta}k^{-\eta}h^{\vartheta}k^{-\eta}k^{\vartheta'}k^{-\eta}h^{\vartheta'} = h^{-\vartheta}k^{\eta'}k^{-\eta}k^{\vartheta'}k^{-\eta}k^{\vartheta'} = 1,
\]

that is, \( \psi \) is the quasi-inverse of \( \varphi \). \( \square \)

We are now in a position to give the

**Proof of Theorem 7.4.** Let \( \varphi \) be an abelian fixed-point-free endomorphism of the group \( G \). Decompose \( G \) as in Theorem 4.2 and let \( \eta \) be the restriction of \( \varphi \) to \( K \), and \( \vartheta \) the restriction of \( \varphi \) to \( H \). By Lemma 7.1, and the fact that \( \varphi \) is abelian, conditions (2) of Theorem 7.2 are satisfied, so that \( \varphi \) has a quasi-inverse. \( \square \)

### 8. Examples

We review first the examples of [Chi12, Section 5] from the point of view of this paper.

One of the examples is a Frobenius group (see [Gor68, 4.5], [Isa76, Chap. 7]) \( G \) with Frobenius kernel \( A \) and cyclic complement. (The kernel is taken to be abelian in the original example, but this is immaterial.)

So we have \( A = G' \), and \(|A|, |G : A| = 1\). Let \( \varphi \) be a nontrivial fixed-point-free endomorphism of \( G \). We have \( A = G' \leq \ker(\varphi) \) by Proposition 3.2. Choose a Frobenius complement \( \langle b \rangle \) such that \( G^{\varphi} \leq \langle b \rangle \), so that \( \langle b \rangle \) is \( \varphi \)-invariant. We are left with determining the fixed-point-free endomorphisms of \( \langle b \rangle \). These are, as noted in [Chi12], the maps \( b \mapsto b^s \), with \(|s - 1, |b|\) = 1. Proposition 5.1 yields the equivalent condition \( s \not\equiv 1 \pmod{p} \), for all primes dividing \(|b|\).

Clearly a group of order 2 has no nontrivial fixed-point-free automorphisms. Thus the subgroup \( K \) of Section 4 cannot have index 2 in the group \( G \).

This situation occurs in [Chi12] first when \( G = S_n \), the symmetric group on \( n \geq 3 \) letters. Here \( S_n' = A_n \leq K \), so we conclude as in [Chi12] that \( K = S_n \), and a nontrivial abelian fixed-point-free endomorphism must be nilpotent, and thus map \( G \) onto a subgroup generated by an even involution.

The case of dihedral groups is also described in [Chi12, Section 5]; we review it here according to our approach.
Let $G$ be a dihedral group, $\varphi$ be a nontrivial abelian fixed-point-free endomorphism of $G$, and $H$ and $K$ be the subgroups of Section 4. Fix an element $x$ such that $\langle x \rangle$ has index 2 in $G$, and an involution $y \notin \langle x \rangle$.

If $G$ has order twice an odd number, then $G' = \langle x \rangle$ has index 2. Since $K \geq \ker(\varphi) = G'$, by the above argument $\varphi$ should nilpotent, with $G^\varphi$ a subgroup of order 2 of $\ker(\varphi) = \langle x \rangle$. But the latter is a group of odd order, so there are no abelian fixed-point-free endomorphisms in this case.

If $G$ has order 4m, then $G' = \langle x^2 \rangle$ has order $m$. We first discuss what $K \geq G'$ can be.

If $K = G'$, then $G'$ must have a complement $H$. This occurs if and only if $m$ is odd, and then $H$ is one of the Klein four-groups $\langle x^m, x^i y \rangle$. We obtain $\varphi$ by extending the identity on $K$ by a (fixed-point-free) automorphism of order 3 of $H$. This covers case (5) with $i$ odd, and case (7) with $i$ even of [Chi12, Section 5].

If $K > G'$, then $K$ cannot have index 2, as noted above, so that $K = G$, and $\varphi$ is nilpotent. We discuss the possibilities for $\ker(\varphi) \geq G'$.

If $\ker(\varphi) = G'$, then $G^\varphi$ is one of the Klein four-groups $\langle x^m, x^i y \rangle$. These have to intersect $\ker(\varphi) = \langle x^2 \rangle$ in $\langle x^m \rangle$, and then $m$ must be even: this covers case (5) with $i$ even, and case (7) with $i$ odd.

If $\ker(\varphi) > G'$, there are three possibilities for the maximal subgroup $\ker(\varphi)$ of $G$. (Here $G^\varphi$ is a subgroup of order 2 of $\ker(\varphi)$.)

1. If $\ker(\varphi) = \langle x \rangle$, then $G^\varphi = \langle x^m \rangle$, and we get case (1).
2. If $\ker(\varphi) = \langle x^2, y \rangle$, then either $m$ is even and $G^\varphi = \langle x^m \rangle$ (case (3)), or $G^\varphi = \langle x^{2a} y \rangle$ for some $a$ (case (4)).
3. If $\ker(\varphi) = \langle x^2, xy \rangle$, then either $m$ is even and $G^\varphi = \langle x^m \rangle$ (case (2)), or $G^\varphi = \langle x^{2a+1} y \rangle$ for some $a$ (case (6)).

We now give a couple more examples.

Consider a semidirect product $G = HK$, with $K$ normal in $G$, and $H$ abelian. Clearly all fixed-point-free endomorphisms of $H$ induce abelian fixed-point-free endomorphisms $\varphi$ of $G$ with $K \leq \ker(\varphi)$. In all the examples so far, and in the notation of Theorem 4.2, we have had either $K = G$ (that is, $\varphi$ is nilpotent), or $\varphi$ trivial on $K$. We now give an example in which $K < G$, and $\varphi$ acts nontrivially on $K$.

Let $K$ be a (nonabelian) special $p$-group $[\text{Hup67}, \text{III.13}]$, that is, a group in which $K' = Z(K) = \text{Frat}(K)$ is elementary abelian. (Here $\text{Frat}(K) = K'K^p$ is the Frattini subgroup of $K$.) The endomorphisms in $\text{Hom}(K, Z(K)) \cong \text{Hom}(K/K', Z(K))$ are then all nilpotent. Consider the elementary abelian group $H$ of central automorphisms of $K$,

$$H = \{ 1 + f : f \in \text{Hom}(K, Z(K)) \},$$

and let $G$ be the natural extension of $K$ by $H$. Define $\eta$ on $K$ to be any element of $\text{Hom}(K, Z(K))$, and $\vartheta$ to be any fixed-point-free endomorphism of $H$. (We might for instance regard the elementary abelian group $H$ as the additive group of a finite field $E$, and take $\vartheta$ to be the multiplication by an element of $E$ different from 0,1.)
Clearly $[K, H] = Z(K) \leq \ker(\eta)$, and $K^n \leq Z(K)$ commutes with $H^\theta \leq H$. The recipe of Section 5 is thus satisfied, so that this defines a quasi-invertible fixed-point-free endomorphism of $G$.

However, Childs shows in [Chi12, Theorem 2] that two fixed-point-free endomorphisms $\varphi, \psi$ of the finite group $G$ induce the same regular subgroup of the group of permutations on $G$ (as in the Introduction) if and only if there is a fixed-point-free endomorphism $\zeta : G \to G$, with $G^\zeta \leq Z(G)$, such that $1 - \varphi = (1 - \zeta)(1 - \psi)$, or $\varphi = \psi - \zeta\psi + \zeta$. We say that two abelian endomorphisms fixed-point-free $\varphi, \psi$ are equivalent if they satisfy this condition.

Now it is not difficult to see that in the last example $\varphi$ is equivalent in this sense to another abelian fixed-point-free endomorphism which acts trivially on $K$.

To see an example where this does not happen, take $K$ to be the nonabelian $p$-group of order $p^3$ and exponent $p$, for $p$ odd. If $K = \langle a, b \rangle$, let $\eta$ be the nilpotent endomorphism of $K$ defined by $a \mapsto b \mapsto 1$, so $K^n = \langle b \rangle$ is abelian, but not central in $K$. We may then consider for instance the automorphism $\alpha$ of $K$ of order $p$ which acts as $a \mapsto ab, b \mapsto b$, and let $H = \langle \alpha \rangle$. For $\vartheta$ we may take any fixed-point-free endomorphism of $H$, that is, any map $\alpha \mapsto \alpha^s$, with $s \not\equiv 1 \pmod p$. If $G = HK$, then we have $G' = \langle b, z \rangle \leq \ker(\eta)$, and $[K^n, H^\theta] \leq [\langle b \rangle, H] = 1$, so that the recipe of Section 5 is satisfied.

References
[By96a] N. P. Byott, Uniqueness of Hopf Galois structure for separable field extensions, Comm. Algebra 24 (1996), no. 10, 3217–3228. MR 1402555 (97j:16051a)
[By96b] N. P. Byott, Corrigendum: “Uniqueness of Hopf Galois structure for separable field extensions”, Comm. Algebra 24 (1996), no. 11, 3705. MR 1405283 (97j:16051b)
[Car85] A. Caranti, Finite p-groups of exponent $p^2$ in which each element commutes with its endomorphic images, J. Algebra 97 (1985), no. 1, 1–13. MR 812164 (87b:20029)
[CC07] Lindsay N. Childs and Jesse Corradino, Cayley’s theorem and Hopf Galois structures for semidirect products of cyclic groups, J. Algebra 308 (2007), no. 1, 236–251. MR 2290920 (2007j:20026)
[Chi00] Lindsay N. Childs, Taming wild extensions: Hopf algebras and local Galois module theory, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000. MR 1767499 (2001e:11116)
[Chi07] Lindsay N. Childs, Some Hopf Galois structures arising from elementary abelian p-groups, Proc. Amer. Math. Soc. 135 (2007), no. 11, 3453–3460. MR 2336557 (2008j:16107)
[Chi12] Lindsay N. Childs, Fixed-point free endomorphisms and Hopf Galois structures, Proc. Amer. Math. Soc. (2012).
[Gor68] Daniel Gorenstein, Finite groups, Harper & Row Publishers, New York, 1968. MR 0231903 (38 #229)
[GP87] Cornelius Greither and Bodo Pareigis, Hopf Galois theory for separable field extensions, J. Algebra 106 (1987), no. 1, 239–258. MR 878476 (88i:12006)
[HR07] Christopher J. Hillar and Darren L. Rhea, Automorphisms of finite abelian groups, Amer. Math. Monthly 114 (2007), no. 10, 917–923. MR 2363058
[Hup67] B. Huppert, Endliche Gruppen. I, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967. MR 0224703 (37 #302)
[Isa76] I. Martin Isaacs, Character theory of finite groups, Academic Press [Harcourt Brace Jovanovich Publishers], New York, 1976, Pure and Applied Mathematics, No. 69. MR 0460423 (57 #417)
[Jac64] Nathan Jacobson, *Structure of rings*, American Mathematical Society Colloquium Publications, Vol. 37. Revised edition, American Mathematical Society, Providence, R.I., 1964. MR 0222106 (36 #5158)

[Jac80] ———, *Basic algebra. II*, W. H. Freeman and Co., San Francisco, Calif., 1980. MR 571884 (81g:00001)

[Pil83] Günther Pilz, *Near-rings*, second ed., North-Holland Mathematics Studies, vol. 23, North-Holland Publishing Co., Amsterdam, 1983, The theory and its applications. MR 721171 (85h:16046)

(A. Caranti) Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38123 Trento, Italy

*E-mail address: andrea.caranti@unitn.it*

*URL: http://science.unitn.it/~caranti/*