

# FIXED-POINT FREE ENDOMORPHISMS OF GROUPS RELATED TO FINITE FIELDS

LINDSAY N. CHILDS

ABSTRACT. Let  $G = \mathbb{F}_q \rtimes \langle \beta \rangle$  be the semidirect product of the additive group of the field of  $q = p^n$  elements and the cyclic group of order  $d$  generated by the invertible linear transformation  $\beta$  defined by multiplication by a power of a primitive root of  $\mathbb{F}_q$ . We study endomorphisms of  $G$ . We find an arithmetic condition on  $d$  so that every endomorphism is determined by its values on  $(1, 1)$  and  $(0, \beta)$ . When that is the case, we determine the fixed point free endomorphisms that are abelian (i.e. factor through an abelian quotient of  $G$ ) and the fixed point free automorphisms of  $G$ . If  $d$  equals the odd part of  $q - 1$  then we count the fixed point free automorphisms of  $G$ —such exist if and only if  $p$  is a Fermat prime.

## INTRODUCTION

Let  $p$  be an odd prime,  $q = p^n$ ,  $\mathbb{F}_p$  the field of  $p$  elements,  $A = \mathbb{F}_q$  the field of  $q = p^n$  elements. Then under addition,  $A = \mathbb{F}_p^n$  is an elementary abelian  $p$ -group of rank  $n$ .

Let  $x$  be a primitive root of  $\mathbb{F}_q$ . Let  $\beta$  be the automorphism of  $A$  given by  $\beta(f) = x^b f$ , multiplication by  $x^b$ , for all  $f$  in  $A$ , where  $b \not\equiv 0 \pmod{q-1}$ . Then  $\beta$  generates a cyclic subgroup of  $GL_n(\mathbb{F}_p)$  of order  $d$  where  $d = (q-1)/(q-1, b)$ . Let  $G = A \rtimes \langle \beta \rangle$ , the semidirect product of  $A$  and the cyclic group generated by  $\beta$ , where  $\beta$  acts on  $A$  as above. We will denote elements of  $G$  by  $(f, \beta^t)$ . Then the operation is

$$(f, \beta^t)(g, \beta^k) = (f + x^{bt}g, \beta^{t+k}).$$

One sees easily that  $G$  has trivial center.

We are interested in determining the fixed point free endomorphisms of  $G$ .

In addition to the intrinsic interest in finding endomorphisms of  $G$ , such endomorphisms are of interest in Galois theory. In 1968, Chase and Sweedler [CS68] introduced the notion of Hopf Galois extension, and in 1987 Greither and Pareigis [GP87] observed that a given Galois

---

*Date:* November 25, 2009.

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

extension of fields may have many Hopf Galois structures, and showed that the number of Hopf Galois structures on a Galois extension with Galois group  $G$  depends only on the group  $G$ . Since that time, a number of papers have studied Hopf Galois structures—see [Ch00], Chapter 2 for a survey of results from the last century. In [CCo06] we showed that each fixed point free endomorphism of  $G$  gives rise to one or two Hopf Galois structures on  $L|K$ , depending on whether the endomorphism is or is not an automorphism. In [Ch09] we obtained abelian fixed point free endomorphisms of a group that is the semidirect product of an elementary abelian  $p$ -group  $A$ ,  $p$  odd, and a cyclic group of automorphisms of  $A$  of order prime to  $p$ . The groups  $G$  of this paper are special cases of those groups.

The main focus in this paper is to determine the fixed point free automorphisms of  $G$ . As examples, we show that if  $(p^n - 1)/b$  is even, then  $G$  has no fixed point free automorphisms. If  $b = 2^e$ , the highest power of 2 dividing  $p^n - 1$ , then there are no fixed point free automorphisms unless  $p = 2^{2^f} - 1$  is a Fermat prime, in which case we determine all such automorphisms.

To simplify the analysis of endomorphisms of the groups  $G$  of interest, we first observe:

**Proposition 1.** *Let  $G = \mathbb{F}_q \rtimes \langle \beta \rangle$  where  $x$  is a primitive element of  $\mathbb{F}_q$  and  $\beta(f) = x^b f$  for all  $f$  in  $\mathbb{F}_q$ . Let  $e$  be the greatest common divisor of  $b$  and  $q - 1$ . Let  $H = \mathbb{F}_q \rtimes \langle \gamma \rangle$  where  $y$  is a primitive element of  $\mathbb{F}_q$  and  $\gamma(f) = y^e f$  for all  $f$  in  $\mathbb{F}_q$ . Then  $G$  and  $H$  are isomorphic as groups.*

*Proof.* Let  $\mathbb{F}_q = \mathbb{F}_p[x] = \mathbb{F}_p[y]$  where  $x, y$  are primitive roots.

Since  $e$  is the greatest common divisor of  $b$  and  $q - 1$ , we have  $b = k'e$  and  $e = bl' + (q - 1)v$  for some integers  $k', l', v$ . Then  $k'l' \equiv 1 \pmod{q - 1/e}$ . Lift  $k'$  to a unit  $k$  modulo  $q - 1$  and let  $l$  be the inverse of  $k$  modulo  $q - 1$ . Define a map  $\alpha$  from  $G$  to  $H$  by

$$\alpha(x^i, 1) = (y^{li}, 1), \alpha(0, \beta) = (0, \gamma).$$

Then, since  $x, y$  have order  $q - 1$ ,  $\alpha$  is a bijection with inverse  $\alpha^{-1}$  given by

$$\alpha^{-1}(y^j, 1) = (x^{jk}, 1), \alpha^{-1}(0, \gamma) = (0, \beta).$$

We check that  $\alpha$  is a homomorphism:

$$\begin{aligned} \alpha(x^g, \beta^h) &= (y^{lg}, \gamma^h) \\ \alpha(x^i, \beta^j) &= (y^{li}, \gamma^j) \\ \text{and } \alpha(x^g, \beta^h)\alpha(x^i, \beta^j) &= (x^g + x^{bh+i}, \beta^{h+j}). \end{aligned}$$

Then

$$\begin{aligned}\alpha((x^g, \beta^h)(x^i, \beta^j)) &= \alpha(x^g + x^{bh+i}, \beta^{h+j}) \\ &= (y^{lg} + y^{l(bh+i)}, \gamma^{h+j})\end{aligned}$$

while

$$\begin{aligned}\alpha((x^g, \beta^h)\alpha(x^i, \beta^j)) &= (y^{lg}, \gamma^h)(y^{li}, \gamma^j) \\ &= (y^{lg} + y^{he+li}, \gamma^{h+j}).\end{aligned}$$

Since  $k = k' + \frac{q-1}{e}j$  is a unit modulo  $q-1$  with inverse  $l$  modulo  $q-1$ , we have

$$ke \equiv k'e \equiv b \pmod{q-1},$$

hence

$$lb \equiv e \pmod{q-1}.$$

Thus

$$y^{he} = y^{lbh}$$

and so  $\alpha$  is an isomorphism of groups.  $\square$

Thus we shall assume throughout the rest of the paper that

$G = (\mathbb{F}_q, +) \rtimes \langle \beta \rangle$ , the semidirect product of the additive group of  $\mathbb{F}_q$  and the cyclic group generated by  $\beta$ , where  $\beta$  acts on  $\mathbb{F}_q$  by  $\beta(f) = x^b f$  and  $b < q-1$  divides  $q-1$ . Let  $bd = q-1$ . Then  $\beta$  has order  $d > 1$  and  $G$  has order  $dp^n$  where  $d$  and  $p^n$  are coprime.

### ENDOMORPHISMS OF $G$

In order to determine the endomorphisms of  $G$  we need the orders of the elements of  $G$ . Since  $x$  is a primitive element of  $\mathbb{F}_q = A$ , that is, a cyclic generator of the multiplicative group of  $\mathbb{F}_q$ , we may write the elements of  $A$  as  $0, 1, x, x^2, \dots, x^{q-2}$ .

The element  $(0, 1)$  has order 1;

The elements  $(f, 1)$  have order  $p$  for every  $f \neq 0$  in  $A$ ;

The elements  $(f, \beta^k)$  for  $\beta^k \neq 1$ :

$$\begin{aligned}(f, \beta^k)^m &= (h(1 + x^{bk} + x^{2bk} + \dots + x^{(m-1)bk}), \beta^{km}) \\ &= (f(\frac{x^{bkm} - 1}{x^{bk} - 1}), \beta^{km})\end{aligned}$$

For  $(f, \beta^k)^m = (0, 1)$ , we must have  $\beta^{km} = 1$ , hence  $km$  is a multiple of  $d$ . Thus  $bkm$  is a multiple of  $q-1$ , so  $x^{bkm} - 1 = 0$ . But since  $\beta^k \neq 1$ , we have  $x^{bk} - 1 \neq 0$ , hence is a unit of  $\mathbb{F}_q$ , and so

$$f(\frac{x^{bkm} - 1}{x^{bk} - 1}) = 0$$

for every  $f$ . Thus for every  $f$  the order of  $(f, \beta^k)$  is the order of  $\beta^k$ , namely,  $d/(d, k)$ , which is coprime to  $p$ .

Since  $A = \mathbb{F}_p[x] \cong \mathbb{F}_p^n$ ,  $G$  has a set of generators

$$(1, 1), (x, 1), \dots, (x^{n-1}, 1), (0, \beta),$$

and so any endomorphism  $\psi$  of  $G$  is determined by its values on those generators. Thus we may describe  $\psi$  by:

$$\psi(0, \beta) = (h, \beta^s)$$

and

$$\psi(1, 1) = (y_0, 1),$$

$$\psi(x, 1) = (y_1, 1),$$

⋮

for some elements  $y_0, y_1, \dots$  in  $\mathbb{F}_q$ , and by  $h$  in  $\mathbb{F}_q$  and  $s \not\equiv 0 \pmod{d}$ . In particular,  $\psi$  restricts to an endomorphism ( $\mathbb{F}_p$ -linear transformation) of  $A$  which we can also denote by  $\psi$ .

In this section we find conditions so that  $\psi$  is determined on  $A$  by the single parameter  $y_0$ .

For a start, we have:

**Proposition 2.** *Let  $\psi : G \rightarrow G$  be the endomorphism defined by the parameters  $y_0, y_1, \dots, y_{n-1}, h, s$ . Then for all  $k$ ,  $y_{r+bk} = y_r x^{bsk}$ .*

*Proof.* We have

$$(0, \beta)(x^r, 1) = (\beta(x^r), \beta) = (x^{r+b}, 1)(0, \beta).$$

Applying  $\psi$  gives

$$(h, \beta^s)(y_r, 1) = (y_{r+b}, 1)(h, \beta^s),$$

hence

$$(h + x^{bs}y_r, \beta^s) = (h + y_{r+b}, \beta^s).$$

Thus, for all  $r$ ,  $y_{r+b} = y_r x^{bs}$ . Hence for all  $k$ ,

$$y_{r+bk} = y_r x^{bsk}.$$

□

**Proposition 3.** *If  $\psi$  is non-trivial on  $\mathbb{F}_q$ , then  $\psi(0, \beta) = (h, \beta^s)$  where  $s$  is a power of  $p$ .*

*Proof.* Let  $m_b(X)$  be the irreducible polynomial over  $\mathbb{F}_p$  of minimal degree with  $x^b$  as a root. Write

$$m_b(X) = \sum_{i=0}^n g_i X^i.$$

Set  $X = x^b$  and apply  $\psi$  to  $(0, 1) = (x^r m_b(x^b), 1)$ :

$$\begin{aligned} (0, 1) &= (x^r m_b(x^b), 1) \\ &= \psi(x^r m_b(x^b), 1) \\ &= \psi\left(\sum g_i x^{r+bi}, 1\right) \\ &= \left(\sum g_i y_{r+bi}, 1\right). \end{aligned}$$

Thus

$$\begin{aligned} 0 &= \sum g_i y_{r+bi} \\ &= \sum g_i y_r x^{bsi} \\ &= y_r \sum g_i (x^{bs})^i \\ &= y_r g(x^{bs}). \end{aligned}$$

So either  $y_r = 0$  for all  $r$ , or  $g(x^{bs}) = 0$ . But since  $g(X)$  is an irreducible polynomial in  $\mathbb{F}_p[x]$  and has  $x^b$  as a root, the other roots of  $g(X)$  are  $(x^b)^{p^i}$  for  $i \geq 1$ . Thus either all  $y_r = 0$ , or  $s$  is a power of  $p$ .  $\square$

**Corollary 4.** *Let  $\psi : G \rightarrow G$  be the endomorphism defined by the parameters  $y_0, y_1, \dots, y_{n-1}, h, s$ . If  $\psi$  is one-to-one on  $\mathbb{F}_q \times 1$ , then  $\psi$  is one-to-one on  $G$ , hence an automorphism of  $G$ .*

*Proof.* If  $\psi$  is one-to-one on  $\mathbb{F}_q \times 1$ , then  $s$  is a power of  $p$ , so  $s$  and  $d$  are coprime. Suppose  $\psi(f, \beta^t) = (0, 1)$ . Then  $(*, \beta^{st}) = (0, 1)$ , hence, since  $s$  and  $d$  are coprime, we must have  $\beta^t = 1$ . So  $(f, \beta^t) = (f, 1)$ , and by assumption, if  $\psi(f, 1) = (0, 1)$  then  $f = 0$ .  $\square$

We can sharpen Proposition 2:

**Proposition 5.** *Let  $\beta(f) = x^b f$  with  $b = 2^c b'$ . Let  $\psi : G \rightarrow G$  be the endomorphism defined by the parameters  $y_0, y_1, \dots, y_{n-1}, h, s$ . If some  $y_k \neq 0$ , then for all  $r$ ,  $y_{r+b'k} = y_r x^{b'ks}$ .*

*Proof.* The assumption on  $y_k$  implies that  $s$  is a power of  $p$ , by Proposition 3.

We prove that for each  $j \geq 0$ , if  $y_{r+2^{j+1}b'k} = y_r x^{2^{j+1}b'sk}$  for all  $r, k$ , then  $y_{r+2^j b'k} = y_r x^{2^j b'sk}$  for all  $r, k$ .

Denote the minimal polynomial of  $x^{2^j b'}$  over  $\mathbb{F}_p$  by

$$n(X) = \sum_{k \geq 0} c_k X^k.$$

Split it up into even and odd powers of  $X$ ,

$$n(X) = \sum_{i \geq 0} c_{2i} X^{2i} + \sum_{i \geq 0} c_{2i+1} X^{2i+1},$$

and evaluate  $n(X)$  at  $x^{2^j b'}$ :

$$\begin{aligned} 0 &= x^{2^j b'} n_j(x^{2^j b'}) \\ &= \sum_{i \geq 0} c_{2i} (x^{2^j b'})^{2i} + \sum_{i \geq 0} c_{2i+1} (x^{2^j b'})^{2i+1} \end{aligned}$$

Set

$$E = \sum_{i \geq 0} c_{2i} (x^{2^j b'})^{2i} = - \sum_{i \geq 0} c_{2i+1} (x^{2^j b'})^{2i+1}.$$

Applying  $\psi$  to

$$\begin{aligned} 0 &= x^r \left( \sum_{i \geq 0} c_{2i} (x^{2^j b'})^{2i} + \sum_{i \geq 0} c_{2i+1} (x^{2^j b'})^{2i+1} \right) \\ &= \sum_{i \geq 0} c_{2i} x^{r+2^{j+1} b' i} + \sum_{i \geq 0} c_{2i+1} x^{r+2^{j+1} b' i+2^j} \end{aligned}$$

yields

$$0 = \sum_{i \geq 0} c_{2i} y_{r+2^{j+1} b' i} + \sum_{i \geq 0} c_{2i+1} y_{r+2^{j+1} b' i+2^j}.$$

We assume that  $y_{r+2^{j+1} b' k} = y_r x^{2^{j+1} b' ks}$ . Since  $s$  is a power of  $p$ , the first sum becomes

$$\begin{aligned} \sum_{i \geq 0} c_{2i} y_{r+2^{j+1} b' i} &= \sum_{i \geq 0} c_{2i} y_r x^{2^{j+1} b' si} \\ &= y_r \sum_{i \geq 0} c_{2i} x^{2^{j+1} b' is} \\ &= y_r \sum_{i \geq 0} c_{2i} x^{2^j b' 2is} \\ &= y_r \left( \sum_{i \geq 0} c_{2i} x^{2^j b' (2i)} \right)^s \\ &= y_r E^s. \end{aligned}$$

Similarly, the second sum becomes

$$\begin{aligned}
 \sum_{i \geq 0} c_{2i+1} y_{r+2^{j+1}b'i+2^j} &= \sum_{i \geq 0} c_{2i+1} y_{r+2^j b' i} x^{2^{j+1} i s} \\
 &= y_{r+2^j b'} \sum_{i \geq 0} c_{2i+1} x^{2^{j+1} b' i s} \\
 &= y_{r+2^j b'} \sum_{i \geq 0} c_{2i+1} x^{2^j (b' 2i+1) s} x^{-2^j b' s} \\
 &= y_{r+2^j b'} x^{-2^j b' s} \sum_{i \geq 0} c_{2i+1} (x^{b' 2^j})^{(2i+1) s} \\
 &= y_{r+2^j b'} x^{-2^j b' s} (-E)^s.
 \end{aligned}$$

since  $s$  is a power of  $p$ . Thus,

$$0 = y_r E^s + y_{r+2^j b'} x^{-2^j b' s} (-E)^s$$

and so

$$y_{r+2^j b'} = y_r x^{2^j b' s}.$$

Repeating this  $j$  times yields  $y_{r+b'} = y_r x^{b' s}$ . Hence  $y_{r+b'k} = y_r x^{kb' s}$  for all  $k \geq 1$ .  $\square$

When  $b' = 1$  this result tells us immediately that an endomorphism  $\psi$  is determined on  $A$  by a single parameter:

**Corollary 6.** *Suppose  $b = 2^r$  with  $r \leq e$ . Let  $\psi : G \rightarrow G$  be the endomorphism defined by the parameters  $y_0, y_1, \dots, y_{n-1}, h, s$ . Then  $y_k = y_0 x^{sk}$  for all  $k$ , hence  $\psi$  on  $A$  is uniquely determined by  $\psi(1, 1) = (y_0, 1)$ .*

More generally, whether or not  $\psi$  is determined on  $A$  by  $y_0$  is dependent on :

**Proposition 7.** *If  $a = (q-1)/b'$  does not divide  $p^m - 1$  for all  $m < n$ ,  $m$  dividing  $n$ , then for each  $k$ ,  $\psi(x^k) = y_k = y_0 x^{sk}$ .*

*Proof.* Since  $x$  is a primitive element of  $\mathbb{F}_q$ ,  $a$  is the order of  $x^{b'}$ . Let  $h(x)$  be the minimal polynomial of  $x^{b'}$ . If  $a$  does not divide  $p^m - 1$  for  $m < n$ , then  $h(x)$  does not divide  $x^{p^m - 1} - 1$  in  $\mathbb{F}_p[x]$ , and so, since  $h(x)$  divides  $x^{p^n} - x$  but not  $x^{p^m} - x$  for  $m < n$ , the degree of  $h(x)$  must be  $n$ .

Thus  $1, x^{b'}, x^{2b'}, \dots, x^{(n-1)b'}$  are linearly independent over  $\mathbb{F}_p$ , hence an  $\mathbb{F}_p$ -basis of  $\mathbb{F}_q$ . Thus for each  $k$  we may write

$$x^k = \sum_{i=0}^{n-1} c_i x^{ib'}.$$

Then

$$\begin{aligned}
y_k = \psi(x^k) &= \sum_{i=0}^{n-1} c_i \psi(x^{ib'}) \\
&= \sum_{i=0}^{n-1} c_i y_{ib'} \\
&= \sum_{i=0}^{n-1} c_i y_0 x^{ib's} \\
&= y_0 \left( \sum_{i=0}^{n-1} c_i x^{ib'} \right)^s \\
&= y_0 x^{ks}.
\end{aligned}$$

□

*Example 8.* We illustrate the arithmetic condition of Proposition 7. For all  $m$ , write  $p^m - 1 = 2^{e_m} q_m$  with  $q_m$  odd.

First, looking at powers of 2 limits the possibilities for the  $m$  for which  $p^m - 1$  can be divisible by  $a$ . Since  $b'$  divides  $q_n$ , the exponent of 2 in  $a = (p^n - 1)/b'$  is  $e_n$ . For  $m$  dividing  $n$ , if  $n/m$  is even then  $e_n > e_m$ . Thus  $a$  cannot divide  $p^m - 1$  for  $m < n$  unless  $n/m$  is odd.

Let  $p^m = 3^{12}$ . Then  $a$  cannot divide  $3^m - 1$  for  $m$  dividing 12 except possibly  $m = 4$ . Now  $3^{12} - 1 = 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 73$ , and so  $a = (3^{12} - 1)/b'$  divides  $3^4 - 1 = 2^4 \cdot 5$  only for  $b' = 7 \cdot 13 \cdot 73$  and  $b' = 5 \cdot 7 \cdot 13 \cdot 73$ , two of the sixteen possible choices for  $b'$ .

Let  $p^m = 7^{15}$ . Then  $a$  can possibly divide only  $7^m - 1$  for  $m = 1, 3, 5$ . Now

$$7^{15} - 1 = 2 \cdot 3^2 \cdot 19 \cdot 31 \cdot 2801 \cdot 159871,$$

so there are 48 possible choices for  $b'$ . Then  $a = (7^{15} - 1)/b'$  divides  $7^5 - 1 = 2 \cdot 3 \cdot 2801$  for six choices of  $b'$ , divides  $7^3 - 1 = 2 \cdot 3^2 \cdot 19$  for four choices of  $b'$ , and divides  $7 - 1 = 2 \cdot 3$  (hence both  $7^5 - 1$  and  $7^3 - 1$ ) for two choices of  $b'$ . Thus  $a$  divides  $7^m - 1$  for  $m < 15$  for eight of the 48 possible  $b'$ .

#### ABELIAN FIXED POINT FREE ENDOMORPHISMS

An endomorphism  $\psi$  of a group  $G$  is *abelian* if for all  $\sigma, \tau$  in  $G$ ,  $\psi(\sigma\tau) = \psi(\tau\sigma)$ , and *fixed point free* if the identity element of  $G$  is the only  $\sigma$  in  $G$  for which  $\psi(\sigma) = \sigma$ . An endomorphism is abelian

iff it is trivial on the commutator subgroup, hence factors through an abelian quotient group.

Assume as before that  $G = (\mathbb{F}_q, +) \rtimes \langle \beta \rangle$  where  $\beta$  acts on  $\mathbb{F}_q$  by  $\beta(f) = x^b f$  and  $bd = q - 1$  with  $d > 1$ . Write  $b = 2^c b'$  with  $b'$  odd, and assume that  $a = (q - 1)/b'$  does not divide  $p^m - 1$  for all  $m < n$ , following Proposition 7.

We determine the abelian fixed point free endomorphisms of  $G$ .

Let  $\psi$  be an endomorphism of  $G$ . The assumption on  $a$  implies that  $\psi$  on  $\mathbb{F}_q$  is uniquely determined by  $y_0$ , where  $\psi(1, 1) = (y_0, 1)$ . If  $y_0 \neq 0$ , then  $\psi$  is one-to-one on  $\mathbb{F}_q$ , hence by Proposition 4 is an automorphism of  $G$ , hence cannot be abelian. If  $y_0 = 0$ , then  $\psi$  is trivial on  $\mathbb{F}_q$ , hence factors through  $G/\mathbb{F}_q$ , a cyclic quotient group, and so  $\psi$  is abelian.

Suppose  $\psi$  is a non-trivial abelian endomorphism of  $G$ . Then  $\psi$  is determined by

$$\psi(0, \beta) = (h, \beta^s)$$

for some  $h$  in  $\mathbb{F}_q$  and some  $s \not\equiv 0 \pmod{q - 1}$ .

**Proposition 9.** *With  $G$ ,  $\psi$  as just described,  $\psi$  has no fixed point iff  $(s - 1, d) = 1$ .*

*Proof.* Since  $\psi(f, 1) = (0, 1)$  for all  $f$  in  $\mathbb{F}_q$ , there is no fixed point for  $\psi$  with  $t = 0$ . For  $t > 0$  we have

$$\psi(f, \beta^t) = \psi(0, \beta)^t = (h(1 + x^{bs} + x^{2bs} + \dots + x^{(t-1)bs}), \beta^{st}).$$

Suppose  $\psi(f, \beta^t) = (f, \beta^t)$  with  $t < d$ . If  $t > 0$ , we need

$$(s - 1)t \equiv 0 \pmod{d} \text{ and}$$

$$f = h(1 + x^{bs} + x^{2bs} + \dots + x^{(t-1)bs}).$$

If  $s - 1$  is coprime to  $d$ , then  $t = 0$ , so  $\psi$  has no fixed points.

If  $s - 1$  is not coprime to  $d$ , then there is some  $t \not\equiv 0 \pmod{d}$  satisfying  $t(s - 1) \equiv 0 \pmod{d}$ , and so there is some  $f$  so that  $\psi(f, \beta^t) = (f, \beta^t)$ , hence  $\psi$  has a fixed point.  $\square$

We can count the number of abelian fixed point free endomorphisms on  $G$ :

**Corollary 10.** *Let  $G = \mathbb{F}_{p^n} \rtimes \langle \beta \rangle$  where  $\beta(f) = x^b f$ ,  $b = 2^r b'$  divides  $p^n - 1$ , and  $d = (p^n - 1)/b$ . Assume that  $a = (q - 1)/b'$  does not divide  $p^m - 1$  for all  $m < n$ . There are  $p^n(\phi(d) - 1)$  non-trivial fixed point free abelian endomorphisms of  $G$*

*Proof.* The non-trivial abelian fixed-point free endomorphisms of  $G$  are endomorphisms  $\psi$  so that  $\psi(f, 1) = (0, 1)$  for all  $f$  in  $\mathbb{F}_q$  and  $\psi(0, \beta) = (h, \beta^s)$  with  $s \not\equiv 0$  and  $(s - 1, d) = 1$ . There are  $p^n$  choices for  $h$ , and  $\phi(d) - 1$  choices for  $s$ .  $\square$

By [Ch09], each abelian fixed point free endomorphism yields a distinct Hopf Galois structure on a Galois extension  $L|K$  with Galois group  $G$ .

*Example 11.* Let  $G = \mathbb{F}_{27} \rtimes \langle \beta \rangle$ , where  $x$  is a primitive root of  $\mathbb{F}_{27}$  and  $\beta(f) = x^2 f$  for  $f$  in  $\mathbb{F}_{27}$ . Then  $b' = 1$  and so the hypothesis that  $a = 27$  does not divide  $3^m - 1$  for  $m < 3$  is satisfied. So there are  $1 + 27 \cdot 12 = 325$  abelian fixed point free endomorphisms of  $G$ .

### AUTOMORPHISMS

As before, let  $G = \mathbb{F}_q \rtimes \langle \beta \rangle$ , where  $x$  is a primitive root of  $\mathbb{F}_q$ ,  $\beta(f) = x^b f$  with  $b = 2^r b'$  and  $bd = q - 1 = p^n - 1$ . Again assume that  $a = (q - 1)/b'$  does not divide  $p^m - 1$  for all  $m < n$ , so that every endomorphism of  $G$  is uniquely determined on  $\mathbb{F}_q$  by the image of  $(1, 1)$ .

We want to determine which automorphisms  $\psi$  are fixed point free.

**Theorem 12.** *Let  $\psi$  be an automorphism of  $G = \mathbb{F}_q \rtimes \langle \beta \rangle$  with  $q = p^n$ ,  $n$  odd, with  $\psi(0, \beta) = (h, \beta^s)$ . Suppose  $(s - 1, d) > 1$ . Then  $\psi$  has a fixed point: that is, there exists some  $(f, \beta^k) \neq (0, 1)$  so that  $\psi(f, \beta^k) = (f, \beta^k)$ .*

*Proof.* First we seek a fixed point of the form

$$\left( \sum_{i=0}^{n-1} c_i x^i, 1 \right)$$

for  $c_0, \dots, c_{n-1}$  in  $\mathbb{F}_p$ .

Since for every  $k$ ,  $\psi(x^k, 1) \neq (0, 1)$ , there is some exponent  $a(k)$  so that

$$\psi(x^k, 1) = (x^{a(k)}, 1).$$

We seek  $c_0, \dots, c_{n-1}$  in  $\mathbb{F}_p$  so that

$$\left( \sum_{i=0}^{n-1} c_i x^i, 1 \right) = \left( \sum_{i=0}^{n-1} c_i x^{a(i)}, 1 \right).$$

This is equivalent to

$$\sum_{i=0}^{n-1} c_i (x^i - x^{a(i)}) = 0,$$

which has a non-zero solution  $(c_0, \dots, c_{n-1})$  iff

$$\{x^i - x^{a(i)} : i = 0, \dots, n - 1\}$$

is a linearly dependent set over  $\mathbb{F}_p$ .

Now we seek a fixed point of the form  $(\sum_{i=0}^{n-1} c_i x^i, \beta^t)$  for some  $t$  with  $0 < t < d$ .

Since  $((s-1, d) > 0)$ , there exists some  $t$  with  $0 < t < d$  so that  $(s-1)t \equiv 0 \pmod{d}$ . Then

$$st \equiv t \pmod{d},$$

and so  $\beta^{st} = \beta^t$ , and  $x^{bst} = x^{bt} \neq 1$  since  $bt < bd = q-1$ , the order of  $x$ . Then

$$\psi(0, \beta^t) = \psi(0, \beta)^t = (h, b^s)^t = \left(h \left(\frac{x^{bts} - 1}{x^{bs} - 1}\right), \beta^{st}\right),$$

so we have

$$\psi\left(\sum_{i=0}^{n-1} c_i x^i, \beta^t\right) = \left(\sum_{i=0}^{n-1} c_i x^{a(i)} + h \left(\frac{x^{bts} - 1}{x^{bs} - 1}\right), \beta^{st}\right).$$

Thus the equation

$$\left(\sum_{i=0}^{n-1} c_i x^i, \beta^t\right) = \psi\left(\sum_{i=0}^{n-1} c_i x^i, \beta^t\right)$$

reduces to

$$\sum_{i=0}^{n-1} c_i (x^i - x^{a(i)}) = w$$

where

$$w = h \left(\frac{x^{bt} - 1}{x^{bs} - 1}\right) \neq 0.$$

This is solvable if

$$\{x^i - x^{a(i)} : i = 0, \dots, n-1\}$$

is a linearly independent set, hence a basis of  $\mathbb{F}_q = \mathbb{F}_p^n$ .

Combining the two cases shows that under the hypotheses,  $\psi$  has a fixed point.  $\square$

**Corollary 13.** *Let  $q = p^n$ ,  $p^n - 1 = 2^e q'$  with  $q'$  odd, and  $G = \mathbb{F}_q \rtimes \langle \beta \rangle$  with  $\beta(f) = x^b f$ , and suppose  $d$  is even. Then  $G$  has no fixed point free automorphisms.*

*Proof.* Since  $s$  is a power of  $p$ , we have  $(s-1, d) = (p^r - 1, d)$  is a multiple of 2, and so every automorphism of  $G$  has a fixed point by the last theorem.  $\square$

If  $s = p^r$  satisfies  $(s-1, d) = 1$ , then any possible fixed point  $(f, \beta^t)$  must have  $t = 0$ , so the first case of the previous proof applies and we have

**Proposition 14.** *If  $\psi : G \rightarrow G$  is an automorphism with  $\psi(1, 1) = (x^a, 1)$ ,  $\psi(0, \beta) = (h, \beta^s)$  where  $(s - 1, d) = 1$ , then  $\psi$  has a non-zero fixed point if and only if  $\{x^i - x^{a(i)} : i = 0, \dots, n - 1\}$  is a linearly dependent set.*

The only case where  $(s - 1, d) = 1$  can occur is when  $d$ , the order of  $\beta$ , is odd. Consider the following example:

*Example 15.* Let  $G = \mathbb{F}_{27} \rtimes \langle \beta \rangle$  and let  $x$  be a primitive element. Let  $\beta(f) = x^2 f$  for  $f$  in  $\mathbb{F}_{27}$ . Then  $b = 2$ ,  $d = 13$  and  $a = 27/b' = 27$ , so every endomorphism is determined on  $\mathbb{F}_{27}$  by its value on  $(1, 1)$ . An automorphism  $\psi : G \rightarrow G$  is defined by  $\psi(x^i, 1) = (x^a x^{is}, 1)$ ,  $\psi(0, \beta) = (h, \beta^s)$ . Thus  $\psi$  is determined by  $a, h$  and  $s = 3^r$ , and  $s - 1$  and  $d$  are coprime.

We find  $a$  so that  $x^a - 1, x^a x^s - x, x^a x^{2s} - x^2$  are linearly dependent. So we seek elements  $c_0, c_1, c_2$  in  $\mathbb{F}_3$  so that

$$c_0(x^a - 1) + c_1(x^a x^s - x) + c_2(x^a x^{2s} - x^2) = 0.$$

From this equation we have

$$\begin{aligned} x^a(c_0 + c_1 x^3 + c_2 x^6) &= (c_0 + c_1 x + c_2 x^2) \\ x^a(c_0 + c_1 x + c_2 x^2)^s &= (c_0 + c_1 x + c_2 x^2), \\ x^a &= (c_0 + c_1 x + c_2 x^2)^{1-s}. \end{aligned}$$

We have  $s = 3$  or  $9$ , so since  $x$  has order  $26$ , there is a solution iff  $a$  is a multiple of  $(1 - s, 26) = 2$ . Hence  $\psi$  has a fixed point iff  $a$  is even.

Thus for each choice of  $s$ ,  $\psi$  has a fixed point for  $13$  choices of  $a$ . Thus there are  $13$  fixed point free automorphisms  $\psi$  with  $\psi(0, \beta) = (h, \beta^s)$  for each  $s$  and each  $h$  in  $\mathbb{F}_{27}$ .

We generalize this example.

Let  $p$  be an odd prime, and let  $p^n - 1 = 2^{e_n} q_n$  with  $q_n$  odd.

**Theorem 16.** *Let  $q = p^n$ ,  $G = \mathbb{F}_q \rtimes \langle \beta \rangle$  where  $\beta(f) = x^b f$  for  $f$  in  $\mathbb{F}_q$ . Let  $b'$  be the odd part of  $b$ , and assume that  $(p^n - 1)/b'$  does not divide  $p^m - 1$  for  $m < n$ .*

(i) *If  $d = (p^n - 1)/b$  is even, then  $G$  has no fixed point free automorphisms.*

(ii) *If  $d = (p^n - 1)/b$  is odd, let  $\psi : G \rightarrow G$  be an automorphism, defined by  $\psi(1, 1) = (x^{a_0}, 1)$ ,  $\psi(0, \beta) = (h, \beta^s)$  where  $s = p^r$  and  $\beta^s \neq 1$ . Then  $\psi$  is fixed point free iff*

$$(p^r - 1, d) = 1$$

and

$$p^{(n,r)} - 1 = (p^n - 1, p^r - 1) \text{ does not divide } a_0.$$

Note: for every  $s = p^r$  for which  $(s - 1, d) = 1$ , there are  $(p^n - 1) - \frac{p^n - 1}{p^{(n,r)} - 1}$  choices of  $a_0$  for which  $\psi$  is fixed point free.

*Proof.* There are no fixed point free automorphisms for which  $(s - 1, d) > 1$ , in particular if  $d$  is even, since  $s - 1 = p^r - 1$  is even. So assume  $(s - 1, d) = 1$ . Then every fixed point of  $\psi$  has the form  $(y, 1)$ , that is, is a fixed point of  $\psi$  restricted to  $\mathbb{F}_q$ .

We look for  $x^f$  in  $\mathbb{F}_q$  so that  $\psi(x^f) = x^f$ .

On  $\mathbb{F}_q$ ,

$$\psi(x^f) = x^{a_0 + fs} = x^{a_0} x^{fs}.$$

So  $\psi(x^f) = x^f$  iff

$$x^f = x^{a_0} x^{fs}$$

iff

$$x^{f(1-s)} = x^{a_0},$$

that is,

$$a_0 \equiv f(1 - s) \pmod{p^n - 1}.$$

There exists an  $f$  satisfying this congruence iff  $(s - 1, p^n - 1) = (p^r - 1, p^n - 1) = p^{(n,r)} - 1$  divides  $a_0$ .

Thus every  $\psi$  such that  $(p^r - 1, d) = 1$  and  $a_0$  is not divisible by  $p^{(n,r)} - 1$  is fixed point free.  $\square$

With this last result one can easily determine the fixed point free automorphisms of a group  $G$  satisfying the arithmetic hypothesis of Proposition 7.

*Example 17.* Let  $q = 7^{15}$ ,  $b = 2b'$  where  $b' = 159871 \cdot 31$ . Then  $(7^{15} - 1)/b'$  does not divide  $7^5 - 1 = 2 \cdot 3 \cdot 2801$  or  $7^3 - 1 = 2 \cdot 9 \cdot 19$  or  $7 - 1 = 6$ , so every automorphism  $\psi$  of  $G$  is determined by  $\psi(1, 1) = (x^{a_0}, 1)$  and  $\psi(0, \beta) = (h, \beta^s)$  with  $s = 7^r$ . Since  $G$  has order  $7^{15} \cdot d$  where  $d = 9 \cdot 19 \cdot 2801$  and  $(d, 7 - 1) > 1$ , we have  $(d, 7^r - 1) > 1$  for all  $r$ . Thus  $G$  has no fixed point free automorphisms.

Now let  $q = 7^{15}$ ,  $b = 2b'$  where  $b' = 9 \cdot 159871$ . Then  $d = 19 \cdot 31 \cdot 2801$ , and  $a = (7^{15} - 1)/b' = 2d$  does not divide  $7^t - 1$  for every  $t < 15$  (we need only check  $t = 1, 3, 5$  by Example 8). Thus every automorphism  $\psi$  of  $G$  is determined by  $\psi(1, 1) = (x^{a_0}, 1)$  and  $\psi(0, \beta) = (h, \beta^s)$  with  $s = 7^r$ . Then  $(7^r - 1, d) = 1$  iff  $r$  is coprime to 15, so  $\psi$  is fixed point free for every triple  $(r, h, a_0)$  where  $r$  is coprime to 15,  $h$  is unrestricted, and  $a_0$  is not divisible by  $6 = 7^{(r,15)} - 1$ .

The case  $b' = 1$  is particularly straightforward. Write  $p^m - 1 = 2^{e_m} q_m$  with  $q_m$  odd, as before.

**Corollary 18.** *With  $G$  as in Theorem 16, let  $d = q_n$ , so that  $b = 2^{e_n}$  and  $b' = 1$ .*

- (1) *If  $p$  is not a Fermat prime, then  $G$  has no fixed point free automorphisms.*
- (2) *If  $p > 3$  is a Fermat prime, then an automorphism  $\psi$  is fixed point free for all  $h$ , all  $s = p^r$  with  $(r, n) = 1$  and all  $a_0$  not divisible by  $p - 1$ .*
- (3) *If  $p = 3$ , then an automorphism  $\psi$  is fixed point free for all  $h$ , all  $s = p^r$  with  $(r, n) = 1$  or  $2$ , and all  $a_0$  not divisible by  $p^{(n,r)} - 1$ .*

*Proof.* When  $b' = 1$  then  $a = p^n - 1$ , so the arithmetic condition of Theorem 7 holds trivially. Also,  $d = q_n$ , so  $d$  is divisible by  $q_m$  for all  $m$  dividing  $n$ . Thus if  $(r, n) = s$ , then  $(p^r - 1, d) = q_s$ .

If  $p$  is not a Fermat prime, then  $q_1 > 1$  and divides  $(p^r - 1, d)$  for all  $r > 0$ . So  $G$  has no fixed point free automorphisms.

If  $p = 2^c + 1 > 3$  is a Fermat prime, then for all  $r$  with  $(r, n) = 1$ ,  $(p^r - 1, d) = q_1 = 1$ , so an automorphism  $\psi$  is fixed point free for all  $h$ , all  $s = p^r$  with  $(r, n) = 1$  and all  $a_0$  not divisible by  $p - 1$ . On the other hand,  $q_k > 1$  for all  $k > 1$ . To see this it suffices, since  $(q_m, q_n) = q_{(m,n)}$ , to show that  $q_k > 1$  for  $k = 2$  or  $k$  odd. For  $k = 2$ ,  $p^2 - 1 = (1 + 2^c)^2 - 1 = 2^{c+1} + 2^{2c}$  is not a power of 2 if  $c + 1 < 2c$ , i. e. if  $c > 1$ . For  $k \geq 3$  odd,

$$p^k - 1 = (1 + 2^c)^k - 1 \equiv k2^c \pmod{2^{2c}},$$

and  $p^k - 1 > 2^c k$ , so  $p^k - 1$  is not a power of 2, hence  $q_k > 1$ . Thus for all  $r$  with  $(r, n) > 1$ ,  $(p^r - 1, d) = (q_r, q_n) > 1$ . Thus there are no fixed point free automorphisms with  $s = p^r$  with  $(r, n) > 1$ .

If  $p = 3$ , a similar argument holds except that  $e_2 = 1$  but  $e_4 = 5 > 1$ .  $\square$

When  $b = 2^e$  and  $p$  is a Fermat prime we count the number of fixed point free automorphisms:

**Corollary 19.** *Let  $G = \mathbb{F}_q \rtimes \langle \beta \rangle$  with  $q = p^n$  and  $\beta(z) = x^b z$  with  $b = 2^{e_n}$ .*

- (1) *For  $p = 2^{2^f} + 1$  a Fermat prime  $> 3$ , the number of fixed point free automorphisms of  $G$  is*

$$p^n(p^n - 1)\phi(n)\left(1 - \frac{1}{2^{2^f}}\right).$$

- (2) For  $p = 3$ , the number of fixed point free automorphisms of  $G$  is

$$3^n(3^n - 1)\frac{\phi(n)}{2}$$

if  $n$  is odd, and

$$3^n(3^n - 1)\frac{\phi(n)}{2} + 3^n(3^n - 1)\frac{7\phi(n/2)}{8}$$

if  $n$  is even.

*Proof.* Recall that  $\psi(0, \beta) = (h, \beta^s)$  and  $\psi(1, 1) = (x^{a_0}, 1)$ . The first factor  $p^n$  counts the number of choices for  $h$ . For  $s = p^r$  we obtain a fixed point free automorphism when  $(r, n) = 1$  or, if  $p = 3$ , when  $(r, n) = 2$ .

For  $p > 3$ ,  $\psi$  is then fixed point free when  $a_0$  is not a multiple of  $(p^r - 1, p^n - 1) = p - 1 = 2^{2^f}$ . Thus for each  $r$  coprime to  $n$ , the number of  $a_0$  is  $p^n - 1$  minus multiples of  $2^{e_1} = 2^{2^f}$ , namely

$$(p^n - 1) - \frac{p^n - 1}{2^{2^f}}.$$

For  $p = 3$ , given  $r$  with  $(n, r) = 1$  and  $h$ , the number of  $a_0$  for which  $\psi$  is fixed point free is

$$3^n - 1 - \frac{3^n - 1}{2} = \frac{3^n - 1}{2}.$$

If  $n$  is even, then we must also consider  $r$  such that  $(r, n) = 2$ . In that case,  $(3^r - 1, 3^n - 1) = 8$ , and so the possible  $a_0$  are those not a multiple of 8. Thus the number of fixed point free automorphisms for each  $h$  and  $r$  with  $(r, n) = 2$  is

$$(3^n - 1 - \frac{3^n - 1}{8}).$$

Finally,  $s = p^r$  is defined modulo the order of  $\beta$ , namely,  $d = (p^n - 1)/b$ . We will show immediately below that all  $p^r$  for  $r = 1, \dots, n$  are incongruent modulo  $d = (p^n - 1)/b$ . Given that, then for  $p > 3$  the number of fixed point free automorphisms is  $(\#h)(\#r)(\#a) =$

$$p^n \phi(n) \left( (p^n - 1) - \frac{(p^n - 1)}{2^{2^f}} \right),$$

where  $\phi(n)$  is Euler's function. For  $p = 3$  and  $n$  odd, the number of fixed point free automorphisms is

$$p^n \phi(n) \left( (p^n - 1) - \frac{(p^n - 1)}{2} \right),$$

while for  $p = 3$  and  $n$  even, the number of fixed point free automorphisms with  $(n, r) = 1$  is

$$p^n \phi(n) \left( (p^n - 1) - \frac{(p^n - 1)}{2} \right).$$

Since the number of  $r$  with  $(n, r) = 2$  is  $\phi(n/2)$ , the number of fixed point free automorphisms with  $(n, r) = 2$  is

$$p^n \phi\left(\frac{n}{2}\right) \left( (p^n - 1) - \frac{(p^n - 1)}{8} \right).$$

Modulo the next lemma, the proof is complete.  $\square$

To insure the accuracy of the count of the last corollary, we need to know that if  $b$  is a power of 2 dividing  $p^n - 1$  where  $p$  is a Fermat prime, then all  $p^r$  for  $r = 1, \dots, n$  are incongruent modulo  $d = (p^n - 1)/b$ . But if  $p^{r'} \equiv p^{r''} \pmod{d}$  with  $r'' > r'$ , then setting  $r = r'' - r'$ , we have  $p^r \equiv 1 \pmod{d}$ . We show:

**Lemma 20.** *Let  $p$  be a Fermat prime and  $n \geq 3$ . For  $b$  a divisor of  $2^{e_n}$ ,*

$$p^r \equiv 1 \pmod{\frac{p^n - 1}{b}}$$

*iff  $n$  divides  $r$ .*

*Proof.* Let  $p^m - 1 = 2^{e_m} q_m$  for all  $m \geq 1$ , where  $q_m$  is odd. We show that if  $p^s \equiv 1 \pmod{q_n}$ , then  $s \geq n$ . We have

$$(x^n - 1, x^s - 1) = x^r - 1$$

where  $r = (n, s)$ . Setting  $x = p$  and restricting to odd parts,

$$(q_n, q_s) = q_r.$$

Since

$$p^s - 1 \equiv 0 \pmod{\frac{p^n - 1}{b}}$$

and  $b$  is a power of 2,  $q_n$  divides  $q_s$ , and so  $q_n = q_r$ . Hence

$$\frac{p^n - 1}{p^r - 1}$$

is a power of 2. If  $r < t < n$  with  $r$  dividing  $t$  and  $t$  dividing  $n$ , then

$$\frac{p^n - 1}{p^t - 1} \text{ and } \frac{p^t - 1}{p^r - 1}$$

are also powers of 2.

Suppose  $f$  is odd and  $rf$  divides  $n$ . Then

$$p^{rf} - 1 = (p^r - 1)(1 + p^r + \dots + p^{r(f-1)}),$$

and the second factor is odd. Thus  $q_{rf} > q_r$ , and so

$$\frac{p^n - 1}{p^r - 1}$$

cannot be a power of 2. So we may assume that  $n = r2^c$  for some  $c > 0$ , let  $n = 2m$  and show that

$$\frac{p^{2m} - 1}{p^m - 1} = p^m + 1$$

is not a power of 2.

First assume that  $p = 2^c + 1$  with  $c > 1$  and  $m \geq 2$ . Then

$$\begin{aligned} p^m + 1 &= (2^c + 1)^m + 1 = 1 + t2^c + \binom{t}{2}2^{2c} + \dots + 1 \\ &\equiv 2 \pmod{4}. \end{aligned}$$

So for  $p$  a Fermat prime  $> 3$ ,  $p^m + 1$  is not a power of 2.

Now let  $p = 3$  and  $m \geq 2$ : we show that  $3^m + 1$  is not a power of 2. For if  $3^m + 1 = 2^s$  for some  $s$ , then since 2 is a primitive element modulo  $3^m$ , the least exponent  $s > 0$  so that  $2^s \equiv 1 \pmod{3^m}$  is  $s = 2 \cdot 3^{m-1}$ . But one sees easily that for all  $m \geq 2$ ,

$$2^{2 \cdot 3^{m-1}} = 4^{3^{m-1}} > 3^m + 1.$$

Hence  $3^m + 1$  is not a power of 2 for  $m \geq 2$ . That completes the proof.  $\square$

*Example 21.* Let  $p^n = 5^6$ , then  $5^6 - 1 = 2^3 \cdot 31 \cdot 63$  so  $b = 8$ . For a fixed point free automorphism,  $r$  can be 1 or 5. The number of fixed point free automorphisms of  $G$  is

$$5^6 \cdot \left(2 \frac{3 \cdot (5^6 - 1)}{4}\right).$$

Let  $p^n = 3^9$ , then  $b = 2$  and  $r$  can be  $= 1, 2, 4, 5, 7, 8$ . The number of fixed point free automorphisms of  $G$  is

$$3^9 \cdot \left(6 \frac{3^9 - 1}{2}\right).$$

Let  $p^n = 3^{10}$ . Then  $b = 8$ . For  $r = 1, 3, 7, 9$ ,  $(2^3, 3^r - 1) = 2$ , while for  $r = 2, 4, 6, 8$ ,  $(2^3, 3^r - 1) = 8$ . Thus the number of fixed point free endomorphisms of  $G$  is

$$\begin{aligned} &3^{10} \left[ \left(4(3^{10} - 1) - \left(\frac{3^{10} - 1}{8}\right)\right) + 4 \left( (3^{10} - 1) - \left(\frac{3^{10} - 1}{2}\right) \right) \right] \\ &= 3^{10} \frac{11}{2} (3^{10} - 1). \end{aligned}$$

Each fixed point free automorphism of  $G$  yields a distinct Hopf Galois structure on a Galois extension  $L|K$  with Galois group  $G$ , by [CCo06], Theorem 4.6.

## REFERENCES

- [CS69] S. U. Chase, M. E. Sweedler, Hopf algebras and Galois theory, Lecture Notes in Mathematics, Vol. 97 Springer-Verlag, Berlin-New York, 1969.
- [Ch00] L. N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Theory*, American Mathematical Society, Mathematical Surveys and Monographs **80**, 2000.
- [Ch09] L. N. Childs, Fixed-point free endomorphisms and Hopf Galois structures, preprint, November, 2009.
- [CCo06] L. N. Childs, J. Corradino, Cayley's Theorem and Hopf Galois structures for semidirect products of cyclic groups, *J. Algebra* (2006), 236-251.
- [GP87] C. Greither, B. Parieigis, Hopf Galois theory for separable field extensions, *J. Algebra* 106 (1987), 239-258.

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

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