SOME HOPF GALOIS STRUCTURES
ARISING FROM ELEMENTARY ABELIAN \( p \)-GROUPS

LINDSAY N. CHILDS

(Communicated by Martin Lorenz)

Abstract. Let \( p \) be an odd prime, \( G = \mathbb{Z}_p^m \), the elementary abelian \( p \)-group of rank \( m \), and let \( \Gamma \) be the group of principal units of the ring \( \mathbb{F}_p[x]/(x^{m+1}) \). If \( L/K \) is a Galois extension with Galois group \( \Gamma \), then we show that for \( p \geq 5 \), the number of Hopf Galois structures on \( L/K \) afforded by \( K \)-Hopf algebras with associated group \( G \) is greater than \( p^s \), where \( s = \frac{(m-1)^2}{3} - m \).

If \( L/K \) is a Galois extension of fields with Galois group \( \Gamma \), then the action of \( \Gamma \) as automorphisms of \( L \) makes \( L \) an \( H \)-Hopf Galois extension for \( H = K \Gamma \). But as first systematically observed by Greither and Pareigis [G-P87], there may be other \( K \)-Hopf algebras \( H \) that act on \( L \) making \( L \) a Hopf Galois extension. Any such \( H \) has the property that \( L \otimes_K H \cong LG \) for some group \( G \) of the same cardinality as \( \Gamma \): we say that \( H \) has associated group \( G \). Byott [By96] transformed the problem of determining Hopf Galois structures on a Galois extension with Galois group \( \Gamma \) by \( K \)-Hopf algebras with associated group \( G \), into the problem of finding equivalence classes of regular embeddings of \( \Gamma \) into the holomorph of \( G \), \( \text{Hol}(G) \cong G \rtimes \text{Aut}(G) \), the normalizer in \( \text{Perm}(G) \) of the image of \( G \) under the left regular representation of \( G \) in \( \text{Perm}(G) \). For \( \beta, \beta' \) one-to-one homomorphisms from \( \Gamma \) to \( \text{Hol}(G) \), the equivalence is: \( \beta \sim \beta' \) iff there exists an automorphism \( \delta \) of \( G \) so that (in \( \text{Hol}(G) \)), for all \( g \) in \( G \), \( \beta'(g) = \delta \beta(g) \delta^{-1} \).

Let \( \mathcal{E}(\Gamma, G) \) denote the set of equivalence classes of regular embeddings of \( \Gamma \) into \( \text{Hol}(G) \).

Let \( p \) be an odd prime number and \( G = \mathbb{Z}_p^m \), the elementary abelian \( p \)-group of rank \( m \). S. Featherstonhaugh showed [Fec00] that if \( p > m \), then \( \mathcal{E}(\Gamma, G) \) is nonempty iff \( G \cong \Gamma \). In [Ch05, 8.2] we showed that if \( p > m \), then there exist at least \((p^m - 1)(p^m - p)(p^m - p^2)\cdots(p^m - p^{m-2}) \) abelian Hopf algebra structures on Galois extensions \( L/K \) with Galois group \( \Gamma \cong G \). This paper complements this work. Here we let \( G = \mathbb{Z}_p^m \) and let \( \Gamma \) be the group of principal units of the ring \( \mathbb{F}_p[x]/(x^{m+1}) \). When \( p > m \), then \( \Gamma \cong G \). If \( L/K \) is a Galois extension with Galois group \( \Gamma \), then we obtain a lower bound on the cardinality of \( \mathcal{E}(\Gamma, G) \) and hence on the number of Hopf Galois structures on \( L/K \) with associated group \( G \). In particular, we show that for \( p \geq 5 \) (or if \( p = 3 \) and \( m \) is sufficiently large), the cardinality of \( \mathcal{E}(\Gamma, G) \) is greater than \( p^s \) where \( s = \frac{(m-1)^2}{3} - m \). This result more than confirms the necessity of the assumption \( p > m \) in Featherstonhaugh’s work.
and further reinforces the remark closing [GPS7] that “in the construction of Hopf Galois extensions there is a certain arbitrariness, in contrast to the classical case where the Galois group always comes with the field”.

For a survey of work on Hopf Galois extensions prior to 2000, see [Ch00].

1. The structure of $\Gamma$

As above and for the remainder of the paper, $\Gamma$ is the group $1 + M$ of principal units of the finite ring $R = \mathbb{F}_p[x]/(x^{m+1})$, a local ring with maximal ideal $M$ generated by the image in $R$ of the indeterminate $x$. We note that $\Gamma$ is isomorphic to the group $\mathbb{G}_m(R) = (M, +G_m)$ of $R$-points of the multiplicative formal group $\mathbb{G}_m$, via the isomorphism $\psi : \mathbb{G}_m(R) \to 1 + M$, given by $\psi(a) = 1 + a$.

We are interested in the structure of $\Gamma$ as a finite abelian group.

**Proposition 1.** $\Gamma$ is the direct sum of the cyclic groups generated by $\{1 + x^r \mid 1 \leq r \leq m, (r, p) = 1\}$.

**Proof.** Since $R$ has characteristic $p$, $(1 + x^s)^p = 1 + x^h$ is the same as that generated by $\{1 + x^r \mid 1 \leq r \leq m, (r, p) = 1\}$. Now for any $r$, if $e_r$ satisfies

$$p^{e_r-1}r \leq m < p^{e_r}r,$$

then $(1 + x^r)$ has order $p^{e_r}$. The product of the orders of $\{1 + x^r \mid 1 \leq r \leq m, (r, p) = 1\}$ is then $\prod_{1 \leq r \leq m, (r, m)=1} p^{e_r}$. But that product equals $p^m$. For when $(r, p) = 1$, then $e_r = |S_r|$ is the cardinality of the set

$$S_r = \{r, pr, p^2r, \ldots, p^{e_r-1}r\};$$

the sets $S_r$ are pairwise disjoint and the union of the $S_r$ for $(r, p) = 1$ and $1 \leq r \leq m$ is the set $\{1, 2, \ldots, m\}$. Thus

$$\sum_{1 \leq r \leq m, (r, p) = 1} |S_r| = \sum_{1 \leq r \leq m, (r, p) = 1} e_r = m,$$

and so

$$\prod_{1 \leq r \leq m, (r, p) = 1} p^{e_r} = p^m.$$

To show that $\Gamma$ is the direct sum of the cyclic groups generated by $1 + x^r$ for $(r, p) = 1$, it suffices to show that $\Delta = \Gamma$.

Let $f(x) = 1 + a_1x + a_2x^2 + \cdots + a_mx^m$ be an arbitrary element of $m$. We show that for $1 \leq r \leq m$ there is a product $h_r$ of elements of $\Delta$ so that

$$f(x) \equiv h_r \pmod{x^{r+1}}.$$

For $r = 1$ we have

$$(1 + x)^{a_1} \equiv 1 + a_1x \equiv f(x) \pmod{x^2}.$$

Suppose for $r \geq 1$ we have $h_{r-1}$ in $\Delta$ so that

$$h_{r-1} \equiv f(x) \equiv 1 + a_1x + \cdots + a_{r-1}x^{r-1} \pmod{x^r}.$$

Let

$$h_{r-1} = 1 + a_1x + \cdots + a_{r-1}x^{r-1} + b_rx^r \pmod{x^{r+1}}.$$
Then we set
\[ h_r = (1 + x^r)^{a_r-b_r}h_{r-1} \equiv (1 + (a_r - b_r)x^r)h_r \]
\[ \equiv 1 + a_1x + \cdots + a_{r-1}x^{r-1} + b_rx^r + (a_r - b_r)x^r \]
\[ \equiv f(x) \pmod{x^{r+1}}. \]

By induction, \( f(x) \) is in \( \Delta \); hence \( \Delta = \Gamma \). \( \square \)

Since \( e_r = 1 \) for all \( r \) iff \( m < p \), we have

**Corollary 2.** \( \Gamma \cong Z_p^n \) iff \( m < p \).

**Corollary 3.** As abelian groups,
\[ \Gamma \cong Z_p^{d_1} \times Z_p^{d_2} \times \cdots \times Z_p^{d_s}, \]
where
\[ d_k = \left\lfloor \frac{m}{p^k-1} \right\rfloor - 2 \left\lfloor \frac{m}{p^k} \right\rfloor + \left\lfloor \frac{m}{p^{k+1}} \right\rfloor. \]

**Proof.** From the proof of Proposition 1, the element \( 1 + x^r \) has order \( p^{s_r} \) if and only if \( p^{s_r-1}r \leq m < p^{s_r}r \). Thus \( d_k \), the number of subgroups \( \langle 1 + x^r \rangle \) of order \( p^k \), satisfies
\[ d_k = \left| \{ r | (r,p) = 1 \text{ and } p^{k-1}r \leq m < p^kr \} \right| \]
\[ = \left| \{ r | (r,p) = 1 \text{ and } \frac{m}{p^k} < r \leq \frac{m}{p^{k-1}} \} \right|. \]

Now
\[ \left| \{ r | \frac{m}{p^k} < r \leq \frac{m}{p^{k-1}} \} \right| = \left\lfloor \frac{m}{p^{k-1}} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor, \]
while
\[ \left| \{ ps | \frac{m}{p^k} < ps \leq \frac{m}{p^{k-1}} \} \right| = \left| \left\{ s | \frac{m}{p^{k+1}} < s \leq \frac{m}{p^k} \right\} \right| \]
\[ = \left\lfloor \frac{m}{p^{k+1}} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor. \]

Hence
\[ d_k = \left\lfloor \frac{m}{p^{k-1}} \right\rfloor - 2 \left\lfloor \frac{m}{p^k} \right\rfloor + \left\lfloor \frac{m}{p^{k+1}} \right\rfloor. \] \( \square \)

2. **Hopf Galois structures**

As noted in the introduction, to find Hopf Galois structures on a Galois extension \( L/K \) of fields with Galois group \( \Gamma \), we need to find regular embeddings
\[ \beta : \Gamma \to Hol(G) \cong G \rtimes Aut(G) \]
for \( G \) a group of the same cardinality as \( \Gamma \). For \( \sigma \) in \( \Gamma \), write \( \beta(\sigma) = (\beta_1(\sigma), \beta_2(\sigma)) \) in \( G \rtimes Aut(G) \). Then \( \beta \) is a regular embedding if \( \beta(\Gamma) \) is a regular subgroup of \( Hol(G) \), that is, \( |G| = |\Gamma| \) and \( \{ \beta_1(\sigma) | \sigma \in \Gamma \} = G \).

When \( G = Z_p^m \), we have a 1-1 homomorphism from \( Hol(G) \) to \( GL_{m+1}(\mathbb{F}_p) \) by identifying \( G \) with \( \mathbb{F}_p^m \) and \( Aut(G) \) with \( GL_m(\mathbb{F}_p) \), and mapping \((v,A)\) in \( Hol(G) \) (with \( v \) in \( G \cong \mathbb{F}_p^m \), \( A \) in \( GL_m(\mathbb{F}_p) \)) to the \( m+1 \times m+1 \) matrix \( \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \) in \( GL_{m+1}(\mathbb{F}_p) \). Then a subgroup \( H \) of \( Hol(G) \) is regular if \( |H| = |G| \) and \( \{ v | (v,A) \in H \} = G \).

**Proposition 4.** There is a regular subgroup of \( Hol(G) \subset GL_{m+1}(\mathbb{F}_p) \) isomorphic to \( \Gamma \).
Proof. Let $X$ be the $m+1 \times m+1$ Jordan block matrix

$$
\begin{pmatrix}
0 & 1 & \cdots & 0 & 0 \\
0 & 0 & \cdots & 0 & 0 \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & 1 \\
0 & 0 & \cdots & 0 & 0
\end{pmatrix}.
$$

Then the map

$$
\beta : \mathbb{F}_p[x]/(x^{m+1}) \to M_{m+1}(\mathbb{F}_p)
$$

by $\beta(\sum_{i=0}^{m} a_i x^i) = \sum_{i=0}^{m} a_i X^i$ is a 1-1 ring homomorphism that restricts to a 1-1 group homomorphism

$$
\beta : \Gamma = 1 + M \to GL_{m+1}(\mathbb{F}_p)
$$

by $\beta(1 + \sum_{i=1}^{m} a_i x^i) = I + \sum_{i=1}^{m} a_i X^i$. Then $\beta(\Gamma)$ is a regular subgroup of $Hol(G)$ since

$$
I + \sum_{i=1}^{m} a_i X^i = (A_v^n),
$$

where $v = \begin{pmatrix} a_m & \cdots & a_m-1 \\
0 & \cdots & 0 \\
a_2 & \cdots & a_1 \\
a_1 & \cdots & a_1 \\
\end{pmatrix}$ and

$$
A = \begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_{m-1} \\
0 & 1 & a_1 & \cdots & a_{m-2} \\
\vdots & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & \cdots & 1 & a_1 \\
0 & 0 & \cdots & 0 & 1
\end{pmatrix}.
$$

Evidently, the image of $\beta$ includes all $v$ in $F_p^m = G$, so $\beta(\Gamma)$ is a regular subgroup of $Hol(G)$. □

As observed in [Ch05, Section 5], given the regular subgroup $\beta(\Gamma) = J$ of $Hol(G)$, we obtain $|Aut(\Gamma)|$ regular embeddings, namely, embeddings of the form $\beta \alpha$, where $\alpha$ is an arbitrary element of $Aut(\Gamma)$. Two embeddings $\beta \alpha$ and $\beta \alpha'$ are equivalent if there exists an element $\gamma$ of $Aut(\Gamma) = GL_m(\mathbb{F}_p)$ in the stabilizer of $J$ so that conjugation by $\gamma$ takes $\beta \alpha$ to $\beta \alpha'$. More precisely, let

$$
Sta(\gamma) = \{ \gamma \in GL_m(\mathbb{F}_p) \mid \gamma \left( \begin{array}{cc} \gamma^{-1} & 0 \\ 0 & 1 \end{array} \right) \gamma^{-1} = J \}.
$$

If we denote by $C(\gamma)$ the inner automorphism of $Hol(G)$ given by conjugation by $\gamma$ in $Aut(G)$, then $\beta \alpha$ and $\beta \alpha'$ are equivalent if there exists an element $\gamma$ in $Sta(J)$ so that

$$
C(\gamma) \beta \alpha = \beta \alpha'.
$$

Now

$$
S = \{ \beta^{-1} C(\gamma) \beta | \gamma \in Sta(J) \}
$$

is a subgroup of $Aut(\Gamma)$, and the equivalence classes of regular embeddings of $\Gamma$ to $J$ are in 1-1 correspondence with the right cosets of $S$ in $Aut(\Gamma)$. So the number of equivalence classes of regular embeddings of $\Gamma$ to $J$ is

$$
|Aut(\Gamma)| / |Sta(J)|.
$$

In [Ch05 8.1] it was proved that

$$
|Sta(J)| = p^m - p^{m-1}.
$$

So we need to compute $|Aut(\Gamma)|$, where

$$
\Gamma = Z_{p^{d_1}} \times Z_{p^{d_2}} \times \ldots \times Z_{p^{d_e}}.
$$
If we write elements of $\Gamma$ as column vectors

$$
(a_{1,1} \cdots a_{1,d_1} \ a_{2,1} \cdots a_{2,d_2} \cdots a_{e,1} \cdots a_{e,d_e})^{tr}
$$

with $a_{j,k}$ in $Z_p^d$, then, abbreviating $Hom(M, N)$ by $(M, N)$, we have

$$
End(\Gamma) = \begin{pmatrix}
(Z_p^d, Z_p^d) & (Z_p^d, Z_p^d) & \cdots & (Z_p^d, Z_p^d) \\
(Z_p^d, Z_p^d) & (Z_p^d, Z_p^d) & \cdots & (Z_p^d, Z_p^d) \\
& & \ddots & \cdots \\
& & & (Z_p^d, Z_p^d)
\end{pmatrix}.
$$

Now $(Z_p^r, Z_p^r) \cong Z_p^r$ if $r \geq s$, and $\cong p^{s-r}Z_p$ if $r < s$, both isomorphisms given by sending $f$ to $f(1)$. Hence if $(Z_p^k)_{r,s}$ denotes $r \times s$ matrices with entries in $Z_p^k$, we have

$$
End(\Gamma) = \begin{pmatrix}
(Z_p^d, Z_p^d) & (Z_p^d, Z_p^d) & \cdots & (Z_p^d, Z_p^d) \\
p(Z_p^d, Z_p^d) & (Z_p^d, Z_p^d) & \cdots & (Z_p^d, Z_p^d) \\
& & \ddots & \cdots \\
p^{e-1}(Z_p^d) & p^{e-2}(Z_p^d) & \cdots & (Z_p^d)
\end{pmatrix}.
$$

Now an element $A$ of $End(\Gamma)$ is an automorphism iff its image in $End(\Gamma) = Z_p^{d_1} \times Z_p^{d_2} \times \cdots \times Z_p^{d_e}$ is an automorphism. But the image of $End(\Gamma)$ in $End(\Gamma)$ is the ring of block upper triangular matrices, and the invertible elements of the image of $End(\Gamma)$ consists of block upper triangular matrices where the blocks along the diagonal are invertible matrices. Thus

$$
Aut(\Gamma) = \begin{pmatrix}
GL_{d_1}(Z_p) & (Z_p)^{d_1,d_2} & \cdots & (Z_p)^{d_1,d_e} \\
p(Z_p^d, Z_p^d) & GL_{d_2}(Z_p^d) & \cdots & (Z_p)^{d_2,d_e} \\
& & \ddots & \cdots \\
p^{e-1}(Z_p^d) & p^{e-2}(Z_p^d) & \cdots & GL_{d_e}(Z_p^d)
\end{pmatrix}.
$$

Now for $l \geq k$,

$$
| (Z_p^k)_{d_k,d_l} | = (p^k)^{d_k}
$$

and for $l \leq k$,

$$
| (p^{k-l}Z_p^k)_{d_k,d_l} | = (p^l)^{d_k}
$$

Hence for $l < k$, the cardinality of the $(l, k)$ block, $(Z_p^k)_{d_l,d_k}$, is the same as the cardinality of the $(k, l)$ block, $(p^{k-l}Z_p^k)_{d_k,d_l}$, and the cardinality of the upper off-diagonal blocks of $Aut(\Gamma)$ is $p^h$, where

$$
h = d_1(d_2 + d_3 + \cdots + d_e) + 2d_2(d_3 + d_4 + \cdots + d_e) + \cdots + (e-1)d_{e-1}d_e.
$$

Thus if we let $g_k = |GL_{d_k}(Z_p^k)|$, then

$$
|Aut(\Gamma)| = g_1g_2 \cdots g_e \cdot p^{2h}.
$$

To determine $g_k$, we have the short exact sequence of groups:

$$
1 \rightarrow I + p(Z_p^k)_{d_k,d_k} \rightarrow GL_{d_k}(Z_p^k) \rightarrow GL_{d_k}(Z_p) \rightarrow 1,
$$

$...
and so
\[ g_k = |GL_{d_k}(Z_{p^k})| = |I + p(Z_{p^k})| \cdot |GL_{d_k}(Z_p)| = p^{(k-1)d_k^2} \cdot (p^{d_k} - 1)(p^{d_k} - p)(p^{d_k} - p^2) \cdots (p^{d_k} - p^{d_k-1}). \]
Thus we have
\[ \text{Proposition 5. } |\text{Aut}(\Gamma)| = p^c q, \text{ where } 
\[ c = 2h + \sum_{k=1}^{e} (k-1)d_k^2 + \frac{d_k(d_k - 1)}{2}, \]
and
\[ q = \prod_{k=1}^{e} \prod_{m=1}^{d_k} (p^m - 1). \]
Here is a lower bound on \(|\text{Aut}(\Gamma)|\):
\[ \text{Proposition 6. } \text{For } p \geq 5 \text{ or } m \geq 25, \ |\text{Aut}(\Gamma)| > p^s \text{ where } s \geq \frac{(m-1)^2}{4}. \]
\[ \text{Proof. } \text{Since } p^{d_k} - p^r \geq p^{d_k-1} \text{ for all } r < d_k, \text{ we have } 
\[ g_k \geq p^{(k-1)d_k^2 + d_k(d_k - 1)}. \]
So
\[ |\text{Aut}(G)| > p^s \]
with
\[ s = 2h + \sum_{k=1}^{e} (k-1)d_k^2 + \sum_{k=1}^{e} d_k(d_k - 1). \]
Now
\[ \frac{m}{p^k} - 1 < \left\lceil \frac{m}{p^k} \right\rceil \leq \frac{m}{p^k} \text{ for } k \geq 1. \]
Hence for \( k > 1, \)
\[ d_k = \left\lfloor \frac{m}{p^k} \right\rfloor - 2 \left\lfloor \frac{m}{p^k} \right\rfloor + \left\lfloor \frac{m}{p^{k+1}} \right\rfloor \geq \frac{m}{p^{k-1}} - 1 - 2 \frac{m}{p^k} + \frac{m}{p^{k+1}} - 1 = \frac{(p-1)^2}{p^{k+1}} m - 2 \]
and
\[ d_1 \geq m - 2 \frac{m}{p} + \frac{m}{p^2} - 1 = \frac{(p-1)^2}{p^2} m - 1. \]
Also, for \( k \geq 2, \)
\[ s_k = d_k + d_{k+1} + \cdots + d_e = \left\lfloor \frac{m}{p^{k-1}} \right\rfloor - \left\lfloor \frac{m}{p^k} \right\rfloor \geq \frac{m}{p^{k-1}} - 1 - \frac{m}{p^k} = \frac{(p-1)m}{p^k} - 1. \]
Thus, just focusing on the terms in $s$ involving $d_1$ and $d_2$, we have
\[ 2h \geq 2d_1s_2 + 4d_2s_3 \geq A, \]
where
\[ A := 2\left(\frac{(p-1)^2}{p^2} - m - 1\right)\left(\frac{(p-1)^2}{p^2} - m - 2\right) + 4\left(\frac{(p-1)^2}{p^3} - m - 2\right)\left(\frac{(p-1)^2}{p^3} - m - 1\right). \]
Also,
\[ \sum_{k=1}^{c} (k-1)d_k^2 \geq d_2^2 \geq B := \left(\frac{(p-1)^2}{p^2} - m - 2\right)^2, \]
and
\[ \sum_{k=1}^{c} d_k(d_k - 1) \geq (d_1 - 1)d_1 + (d_2 - 1)d_2 \]
\[ \geq C := \left(\frac{(p-1)^2}{p^2} - m - 2\right)\left(\frac{(p-1)^2}{p^2} - m - 1\right) + \left(\frac{(p-1)^2}{p^3} - m - 3\right)\left(\frac{(p-1)^2}{p^3} - m - 2\right). \]
Hence
\[ s \geq A + B + C = a(m-b)^2 + c, \]
where (with the aid of Maple 9.0.1),
\[ a = \frac{p^6 - 2p^5 + 2p^4 - 2p^3 - p^2 + 4p - 2}{p^6}, \]
\[ b = \frac{5p^3(p^2 + 2p - 1)}{2(p^5 - p^4 + p^3 - p^2 - 2p + 2)}, \]
\[ c = 22 - \frac{25(-2p^5 + 2p^4 - 2p^3 - p^2 + p^5 + 4p - 2)(p^4 + 4p^3 + 2p^2 - 4p + 1)}{4(p^5 - p^4 + p^3 - p^2 - 2p + 2)^2}. \]
For a simple lower bound for $s$, one can show (with Maple) that the minimum value of $(a(m-b)^2 + c) - \left(\frac{(m-1)^2}{3}\right)$ is
\[ c_0 = \frac{117p^6 - 650p^5 + 835p^4 - 200p^3 - 1085p^2 + 1490p - 595}{4(2p^6 - 6p^5 + 6p^4 - 6p^3 - 3p^2 + 12p - 6)}, \]
which is $> 0$ for $p \geq 5$, while if $p = 3$,
\[ (a(m-b)^2 + c) - \frac{(m-1)^2}{3} = \frac{109}{729} (m - \frac{1647}{109})^2 - \frac{4078}{327}, \]
which is $\geq 0$ for $m \geq 25$. \hfill \Box

Since $|\text{Sta}(J)| = p^m - p^{m-1} < p^m$, we obtain the lower bound stated in the Introduction:

**Theorem 7.** For $\Gamma$ the group of principal units of $\mathbb{F}_p[x]/(x^{m+1})$, the number of $H$-Hopf Galois structures on $L/K$ with Galois group $\Gamma$, where $H$ has associated group $G = \mathbb{Z}_p^n$, is $\geq p^s$ where $s \geq \frac{(m-1)^2}{3} - m$ if $p \geq 5$ or $m \geq 25$.

For specific examples we may of course compute explicitly: if $p = 3, m = 10$, we have $|\text{Sta}(J)| = 2 \cdot 3^3$ and $d_1 = 5, d_2 = 1, d_3 = 1$; hence
\[ |\text{Aut}(\Gamma)| = 3^{24} \cdot (3^5 - 1)(3^5 - 3)(3^5 - 2^2)(3^5 - 3^3)(3^5 - 3^4). \]
and the number of equivalence classes of Hopf Galois structures corresponding to the regular subgroup $J$ is

$$3^{28} \cdot 2^{11} \cdot 5 \cdot 11^2 \cdot 13 = 368, 488, 392, 004, 133, 406, 720.$$  

References


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