Hopf-Galois Structures on Degree $mp$

Extensions

Timothy Kohl

May 2016
Hopf-Galois Theory

If $L/K$ is Galois with $\Gamma = Gal(L/K)$ then the elements of $\Gamma$ are an $L$-basis for $End_K(L)$ whence a natural map:

$$H = K[\Gamma] \xrightarrow{\mu} End_K(L)$$

which induces

$$I \otimes \mu : L \# H \xrightarrow{\sim} End_K(L)$$

For the group ring $K[\Gamma]$ the Hopf algebra structure is reflected in how $K[\Gamma]$ acts (via endomorphisms) on $L/K$ and in Hopf Galois theory, the idea is to consider actions by general Hopf algebras acting by endomorphisms on $L/K$.  

1
Hopf-Galois theory is a generalization of ordinary Galois theory in several ways.

- One can put Hopf Galois structure(s) on field extensions $L/K$ which aren’t Galois in the usual way because they are separable but non-normal e.g. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$

- Moreover, one can take an extension $L/K$ which is Galois with group $\Gamma$ (hence Hopf-Galois for $H = K[\Gamma]$) and also find other Hopf algebras which act besides $K[\Gamma]$.

Both cases are covered by the Greither-Pareigis enumeration and the formulation for the latter is as follows:
• $L/K$ finite Galois extension with $\Gamma = \text{Gal}(L/K)$.

$\Gamma$ acting on itself by left translation yields an embedding

$$\lambda : \Gamma \hookrightarrow B = \text{Perm}(\Gamma)$$

Definition: $N \leq B$ is regular if $N$ acts transitively and fixed point freely on $\Gamma$.

**Theorem 1:** [Greither-Pariegis - 1987]

The following are equivalent:

• There is a $K$-Hopf algebra $H$ such that $L/K$ is $H$-Galois

• There is a regular subgroup $N \leq B$ s.t. $\lambda(\Gamma) \leq \text{Norm}_B(N)$ where $N$ yields $H = (L[N])^\Gamma$. 
Definitions/Notation:

\[ B = \text{Perm}(\Gamma) \cong S_{|\Gamma|} \]

\[ R(\Gamma) = \{ N \leq B \mid N \text{ regular, } \lambda(\Gamma) \leq \text{Norm}_B(N) \} \]

\[ R(\Gamma, [M]) = \{ N \in R(\Gamma) \mid N \cong M \} \]

The goal then is to enumerate \( R(\Gamma) \) for a given \( \Gamma \) and this entails the enumeration of \( R(\Gamma, [M]) \) for each isomorphism class \( M \) of groups of order \( |\Gamma| \).
The problem in general is that one is searching for

\[ N \leq B \]

where \( B \) is very large!

We shall show in the case we study, that all \( N \) in ques-
tion are subgroups of a much smaller group.
Groups of Order $mp$

Consider those primes '$p$' and integers '$m$' such that

- $gcd(p, m) = 1$

- any group $\Gamma$ of order $mp$ has a unique (therefore characteristic) Sylow $p$-subgroup

- for any group $Q$ of order $m$, one has $p \nmid |Aut(Q)|$
One obvious class of \((p, m)\) for which the above holds are where \(p > m\), but others may be found.

For example, if \((p, m) = (5, 8)\) then Sylow theory easily shows that any group of order 40 will have a unique Sylow 5-subgroup.

Moreover for each group of order 8,

\[
\{C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_4, Q_2\}
\]

the respective automorphism groups have orders \(\{4, 8, 168, 8, 24\}\), none of which are divisible by 5.
For any such group $\Gamma$ of order $mp$ we have the following.

By Schur-Zassenhaus

$$\Gamma = PQ \cong P \times Q \text{ or } P \rtimes \tau Q$$

for $P$ the unique Sylow $p$-subgroup and $Q$ a subgroup of order $m$.

And since $p \nmid |Aut(Q)|$ then either $p \nmid |Aut(\Gamma)|$ or the Sylow $p$-subgroup of $Aut(\Gamma)$ is generated by inner automorphisms arising from $P$.

As such the Sylow $p$-subgroup of $Hol(\Gamma) = \Gamma \rtimes Aut(\Gamma)$ is isomorphic to either $C_p$ or $C_p \times C_p$. 
For $\lambda(\Gamma) \leq B$ we have $\lambda(\Gamma) = \mathcal{P} \mathcal{Q}$ where (by virtue of regularity) $\mathcal{P} = \langle \pi_1 \pi_2 \cdots \pi_m \rangle$ with

- $\pi_1, \ldots, \pi_m$ disjoint $p$ cycles

- $\mathcal{Q}$ is a regular permutation group on $\{\Pi_1, \ldots, \Pi_m\}$ where $\Pi_i = \text{Support}(\pi_i)$.

- In fact, the $\Pi_i$ are blocks with respect to the action of $\mathcal{Q}$. 
What we wish to prove is that for these $p$ and $m$ that if $N \in R(\Gamma)$ then $N \leq Norm_B(\mathcal{P})$.

This ultimately is due to the relationship between $\mathcal{P}$ and the Sylow $p$-subgroup of such a given $N$. 
As $N$ in $R(\Gamma)$ is also of order $mp$ then $N = P(N)Q(N)$ where $P(N) = \langle \theta \rangle$ has order $p$ where $\theta = \theta_1 \cdots \theta_m$, also a product of $m$ disjoint $p$-cycles.

**Proposition 2:** If $N \in R(\Gamma)$ with Sylow $p$-subgroup $P(N)$ then $P(N)$ is a semi-regular subgroup of $\mathcal{V} = \langle \pi_1, \ldots, \pi_m \rangle$.

Why?

Since $P(N) = \langle \theta \rangle$ is characteristic, it is normalized by $\lambda(\Gamma)$ and thus centralized by $\mathcal{P}$, and conversely that $P(N)$ centralizes $\mathcal{P}$.

If $p > m$ then $\theta\pi_i\theta^{-1} = \pi_i$ implies (after re-ordering if necessary) that $\theta_i \in \langle \pi_i \rangle$, so that $P(N) \leq \mathcal{V}$.
Recall that since $\mathcal{P}$ is semi-regular, its centralizer in $B$ is isomorphic to $C_p \wr S_m$, more specifically $\mathcal{V} \rtimes \mathcal{S}$ where $\mathcal{S}$ is the set of permutations of the 'blocks' consisting of the supports of the $\pi_i$. 
As it turns out, this is not automatically true that $P(N) \leq V$ if it’s merely assumed that $gcd(p, m) = 1$.

For example, if $p=5$ and $m=8$ then in $S_{40}$ let

$$\pi_i = (1+(i-1)5, 2+(i-1)5, 3+(i-1)5, 4+(i-1)5, 5+(i-1)5)$$
for $i = 1, \ldots, 8$ and let $\theta_j = (j, j+5, j+10, j+15, j+20)$
for $j = 1, \ldots, 5$ and $\theta_6 = \pi_6, \theta_7 = \pi_7, \theta_8 = \pi_8$.

One may verify that $\pi = \pi_1 \cdots \pi_8$ is centralized by $\theta = \theta_1 \cdots \theta_8$ but for $j = 1, \ldots, 5$ that $\theta_j$ is not a power of any $\pi_i$.

This example shows that the $P(N) \leq N$ being normalized, and thus centralized, by $\mathcal{P}$ is insufficient to guarantee that $P(N) \leq \langle \pi_1, \pi_2, \ldots, \pi_m \rangle$. 
However since $\Gamma$ normalizes $N$, then in fact we do have $P(N) \leq \mathcal{V}$. (even if $p < m$)

The reason is that with $\lambda(\Gamma) = \mathcal{P}\mathcal{Q}$ that $\mathcal{Q}$ must also normalizes $P(N)$ and *this* is what forces $P(N) \leq \mathcal{V}$. 
As $\lambda(\Gamma) = PQ$ normalizes $\mathcal{P}$ then for any $N \in R(\Gamma)$ we have $P(N)$ normalizes $\mathcal{P}$ so we need to look closely at the structure of $\text{Norm}_B(\mathcal{P})$. 
Proposition 3:

\[ \text{Norm}_B(\mathcal{P}) \cong C_p^m \times (U_p \times S_m) \]

- typical element \((\hat{a}, u, \alpha)\) where \(\hat{a} = [a_1, \ldots, a_m] \in \mathbb{F}_p^m\)

- \([a_1, \ldots, a_m]\) corresponds to \(\pi_1^{a_1} \cdots \pi_m^{a_m} \in \mathcal{V}\)

- \(u \in U_p = \mathbb{F}_p^*\) acts by scalar multiplication

- \(\alpha\) in \(S_m\) permutes the coordinates

- \((\hat{b}, v, \beta)(\hat{a}, u, \alpha) = (\hat{b} + v\beta(\hat{a}), vu, \beta\alpha)\)

- \(\text{Cent}_B(\mathcal{P})\) consists of those \((\hat{a}, u, \alpha)\) where \(u = 1\)
Since $P(N) \leq \mathcal{V} = \langle \pi_1, \ldots, \pi_m \rangle$ then its generator is of the form $\pi_1^{a_1} \cdots \pi_m^{a_m}$ for some set $\{a_i\}$ where all $a_i \neq 0$.

**Theorem 4:** Any semi-regular subgroup of $B$ of order $p$ that is normalized by $Q$, hence $\lambda(\Gamma)$, is generated by

$$\hat{p}_\chi = \sum_{\gamma \in Q} \chi(\gamma)\hat{v}_\gamma(1)$$

- $\chi : Q \to U_p = \mathbb{F}_p^\ast$ is a linear character of $Q$

- $\hat{v}_i = [0, \ldots, 1, \ldots, 0] \leftrightarrow \pi_i$.

- $Q$ acts regularly on $\{1, \ldots, m\}$. 

16
For example, if $m = 4$ and $Q \cong C_2 \times C_2 = \langle x, y \rangle$, we have

\[
\begin{array}{c|cccc}
  & 1 & x & y & xy \\
\hline
\chi_1 & 1 & 1 & 1 & 1 \\
\chi_2 & 1 & 1 & -1 & -1 \\
\chi_3 & 1 & -1 & 1 & -1 \\
\chi_4 & 1 & -1 & -1 & 1 \\
\end{array}
\]

whence subgroups

\[
P = P_1 = \langle [1, 1, 1, 1] \rangle = \langle \pi_1 \pi_2 \pi_3 \pi_4 \rangle
\]

\[
P_2 = \langle [1, 1, -1, -1] \rangle = \langle \pi_1 \pi_2 \pi_3^{-1} \pi_4^{-1} \rangle
\]

\[
P_3 = \langle [1, -1, 1, -1] \rangle = \langle \pi_1 \pi_2^{-1} \pi_3 \pi_4^{-1} \rangle
\]

\[
P_4 = \langle [1, -1, -1, 1] \rangle = \langle \pi_1 \pi_2^{-1} \pi_3^{-1} \pi_4 \rangle
\]
Now, to further organize the arrangement of $N$ in a given $R(\Gamma, [M])$ we consider the role of $N^{opp} = Cent_B(N)$.

For example, $\lambda(\Gamma)^{opp} = \rho(\Gamma)$ where $\rho : \Gamma \to Perm(\Gamma)$ is the right regular representation.
We have the following:

- $N$ regular if and only if $N^{opp}$ regular

- $N$ regular $\rightarrow (N^{opp})^{opp} = N$

- $Norm_B(N) = Norm_B(N^{opp})$

- $N \in R(\Gamma, [M])$ if and only if $N^{opp} \in R(\Gamma, [M])$
Theorem 5: If $\mathcal{P} = P_1, P_2, \ldots, P_k$ are the possible $P(N)$ then

(a) if $N$ is a direct product (with $P(N)$ as a factor) then

$$N \in R(\Gamma, [M]) \text{ implies } P(N) = \mathcal{P} = P(N^{opp})$$

(b) if $N$ is a semi-direct product then $P(N) \neq P(N^{opp})$

and

$$\left| \{N \in R(\Gamma, [M]) \mid P(N) = P_1 \} \right| = \sum_{i=2}^{k} \left| \{N \in R(\Gamma, [M]) \mid P(N) = P_i \} \right|$$

N.B. For a given isomorphism class $[M]$ it’s possible that $\{N \in R(\Gamma, [M]) \mid P(N) = P_i \}$ may be empty for some $i > 1$, or that $R(\Gamma, [M])$ might be empty altogether.
Orthogonality of characters, namely those giving rise to \( P(N) \) for \( N \in R(\Gamma) \), together with the assumption that \( p \nmid |\text{Aut}(Q)| \) ultimately yields the main theorem which allows us to 'contain' all of \( R(\Gamma) \) in a much smaller subgroup of \( B \).

**Theorem 6:** If \( N \in R(\Gamma) \) then \( N \leq \text{Norm}_B(\mathcal{P}) \).
To simplify the computations, one may observe that any two regular subgroups of $S_n$ that are isomorphic as abstract groups are in fact conjugate to each other.

The result of this is that instead of working in $B = Perm(\Gamma)$ and dealing with left regular representations, it is simpler to instead pick $\Gamma$ to be a regular subgroup of $B = S_{mp}$ and compute $N$ with respect to this choice of $\Gamma$. 
• Define $\mathcal{P} = \langle \pi_1 \cdots \pi_m \rangle$ where $\pi_i = (1 + p(i-1), \ldots, p^i)$

• For each (isomorphism class of) regular permutation group $Q$ of order $m$, embed $Q$ in $\text{Norm}_B(\mathcal{P})$

• For each character $\chi$ of $Q$ compute $\hat{p}_\chi$ and correspondingly $\Gamma = (\langle \hat{p}_\chi \rangle_Q)^{opp}$ which will be regular and contain $\mathcal{P}$.

• Let $\Gamma_1, \ldots, \Gamma_d$ be the distinct isomorphism classes resulting from this construction.

• Determine $N \in R(\Gamma_i, [\Gamma_j])$ for each $i, j$ where now all $\Gamma_i$ are regular subgroups of $B$ containing the same $\mathcal{P}$
Examples: Groups of Order $4p$

- $C_{4p}$
- $C_p \times V$
- $E_p = C_p \rtimes C_4$ if $p \equiv 1 \pmod{4}$
- $D_{2p}$
- $Q_p$
Theorem 7: Let $R(\Gamma, [M])$ be the set of regular subgroups $N$ isomorphic to $M$ in $Perm(\Gamma_i)$ that are normalized by $\lambda(\Gamma)$. Then the cardinality of $R(\Gamma, [M])$ is given by the following table:

<table>
<thead>
<tr>
<th>$\Gamma \setminus M$</th>
<th>$C_{4p}$</th>
<th>$C_p \times V$</th>
<th>$E_p$</th>
<th>$D_{2p}$</th>
<th>$Q_p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_{4p}$</td>
<td>1</td>
<td>1</td>
<td>4</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>$C_p \times V$</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>$E_p$</td>
<td>$p$</td>
<td>$p$</td>
<td>$2p + 2$</td>
<td>$2p$</td>
<td>$2p$</td>
</tr>
<tr>
<td>$D_{2p}$</td>
<td>$3p$</td>
<td>$p$</td>
<td>0</td>
<td>$4p + 2$</td>
<td>$4p + 2$</td>
</tr>
<tr>
<td>$Q_p$</td>
<td>$p$</td>
<td>$p$</td>
<td>$4p$</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>
Byott determined $|R(\Gamma_i, [\Gamma_j])|$ for groups of order $pq$ for $p$ and $q$ prime, where $p \equiv 1 \pmod{q}$, which can also be done via our method, the results being

<table>
<thead>
<tr>
<th>$\Gamma \setminus M$</th>
<th>$C_{pq}$</th>
<th>$C_p \rtimes C_q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_{pq}$</td>
<td>1</td>
<td>$2(q - 2)$</td>
</tr>
<tr>
<td>$C_p \rtimes C_q$</td>
<td>$p$</td>
<td>$2(p(q - 2) + 1)$</td>
</tr>
</tbody>
</table>
For $p = 2q + 1$ (where $q$ is prime, making $p$ a 'safe prime') and $m = p - 1 = 2q$

- $C_{mp}$
- $C_p \times D_q$
- $(C_p \rtimes C_q) \times C_2 = F \times C_2$
- $D_p \times C_q$
- $D_{pq}$
- $C_p \rtimes C_{2q} \cong Hol(C_p)$
**Theorem 8:** Let $R(\Gamma, [M])$ be the set of regular subgroups $N$ isomorphic to $M$ in $Perm(\Gamma_i)$ that are normalized by $\lambda(\Gamma)$. Then the cardinality of $R(\Gamma, [M])$ is given by the following table:

<table>
<thead>
<tr>
<th>$\Gamma \setminus M$</th>
<th>$C_{mp}$</th>
<th>$C_p \times D_q$</th>
<th>$F \times C_2$</th>
<th>$C_q \times D_p$</th>
<th>$D_{pq}$</th>
<th>$Hol(C_p)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_{mp}$</td>
<td>1</td>
<td>2</td>
<td>$2(q - 1)$</td>
<td>2</td>
<td>4</td>
<td>2$(q - 1)$</td>
</tr>
<tr>
<td>$C_p \times D_q$</td>
<td>$q$</td>
<td>2</td>
<td>0</td>
<td>2$q$</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>$F \times C_2$</td>
<td>$p$</td>
<td>2$p$</td>
<td>$2(p(q - 2) + 1)$</td>
<td>2$p$</td>
<td>4$p$</td>
<td>2$p(q - 1)$</td>
</tr>
<tr>
<td>$C_q \times D_p$</td>
<td>$p$</td>
<td>2$p$</td>
<td>$2p(q - 1)$</td>
<td>2</td>
<td>4</td>
<td>2$p(q - 1)$</td>
</tr>
<tr>
<td>$D_{pq}$</td>
<td>$qp$</td>
<td>2$p$</td>
<td>0</td>
<td>2$q$</td>
<td>4</td>
<td>0</td>
</tr>
</tbody>
</table>
| $Hol(C_p)$           | $p$     | 2$p$            | $2p(q - 1)$    | 2$p$            | 4$p$   | 2$(p(q - 2) + 1)$ (*)

(*) This case was enumerated by Childs using different techniques.
Groups of Square-Free Order

If we branch out from the $p > m$ case, we can consider groups of order $p_1 p_2 \cdots p_n$ for primes $p_1 < \ldots p_n$.

There is a classic formula due to Hölder (and utilized by Alonso) for the enumeration of groups of square-free order.

All such groups are iterated (semi)-direct products of cyclic groups, the number of which are dependent on whether $p_l \equiv 1 \ (mod \ p_k)$ for $l > k$, where the maximum number of groups occurs if each $p_l$ is congruent to 1 mod each $p_k$ for $l > k$. 
Consider groups of order $p_1p_2p_3$ for $p_1 < p_2 < p_3$.

If $|\Gamma| = p_1p_2p_3$ then the Sylow $p_3$-subgroup of $\Gamma$ is unique, and if $p = p_3$ and $m = p_1p_2$ then groups of order $m$ have automorphism groups of order relatively prime to $p_3$.

If $p_3 \equiv 1 (mod \, p_2)$ and $p_2 \equiv 1 (mod \, p_1)$ and $p_2 \equiv 1 (mod \, p_1)$ then $p_3 > p_1p_2$ (i.e. $p > m$) similar to the cases for the safe primes seen earlier.

However, if $p_3 \equiv 1 (mod \, p_1)$ and $p_2 \equiv 1 (mod \, p_1)$ and $p_3 \not\equiv 1 (mod \, p_2)$ then $p = p_3 < m = p_1p_2$. 
Proposition 9: [Alonso] If $p_1$, $p_2$ and $p_3$ are distinct odd primes where $p_1 < p_2 < p_3$ with $p_3 \equiv 1 \pmod{p_1}$, $p_2 \equiv 1 \pmod{p_1}$, but $p_3 \not\equiv 1 \pmod{p_2}$ then there are $p_1 + 2$ groups of order $p_1p_2p_3$:

$$C_{p_3p_2p_1} = \langle x, y, z | x^{p_3}, y^{p_2}, z^{p_1}, [y, x], [z, x], [z, y] \rangle$$

$$C_{p_2} \times (C_{p_3} \rtimes C_{p_1}) = \langle x, y, z | x^{p_3}, y^{p_2}, z^{p_1}, [y, x], [z, y], zxz^{-1}x^{-v_3} \rangle$$

$$C_{p_3} \times (C_{p_2} \rtimes C_{p_1}) = \langle x, y, z | x^{p_3}, y^{p_2}, z^{p_1}, [y, x], [z, x], zyz^{-1}y^{-v_2} \rangle$$

$$C_{p_3p_2} \rtimes_i C_{p_1} = \langle x, y, z | x^{p_3}, y^{p_2}, z^{p_1}, [y, x], zxz^{-1}x^{-v_3}, zyz^{-1}y^{-v_i} \rangle$$

$i = 1, \ldots, p_1 - 1$

where $v_3$ is the order $p_1$ element in $U_{p_3}$ and $v_2$ is the order $p_1$ element of $U_{p_2}$. 
Theorem 10: If we define

\[ f(a, b) = 2(a(b - 2) + 1) \]
\[ g(a, b) = 2a(b - 1) \]

then

<table>
<thead>
<tr>
<th>( \Gamma \setminus M )</th>
<th>( C_{p_3p_2p_1} )</th>
<th>( C_{p_3} \times (C_{p_2} \rtimes C_{p_1}) )</th>
<th>( C_{p_2} \times (C_{p_3} \rtimes C_{p_1}) )</th>
<th>( C_{p_3p_2} \rtimes_i C_{p_1} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( C_{p_3p_2p_1} )</td>
<td>1</td>
<td>( g(1, p_1) )</td>
<td>( g(1, p_1) )</td>
<td>( 2g(1, p_1) )</td>
</tr>
<tr>
<td>( C_{p_3} \times (C_{p_2} \rtimes C_{p_1}) )</td>
<td>( p_2 )</td>
<td>( f(p_2, p_1) )</td>
<td>( g(p_2, p_1) )</td>
<td>( 2f(p_2, p_1) )</td>
</tr>
<tr>
<td>( C_{p_2} \times (C_{p_3} \rtimes C_{p_1}) )</td>
<td>( p_3 )</td>
<td>( g(p_3, p_1) )</td>
<td>( f(p_3, p_1) )</td>
<td>( 2f(p_3, p_1) )</td>
</tr>
<tr>
<td>( C_{p_3p_2} \rtimes_j C_{p_1} )</td>
<td>( p_3p_2 )</td>
<td>( p_3f(p_2, p_1) )</td>
<td>( p_2f(p_3, p_1) )</td>
<td>-</td>
</tr>
</tbody>
</table>

| \( i, j \) | \( |R(C_{p_3p_2} \rtimes_j C_{p_1}, [C_{p_3p_2} \rtimes_i C_{p_1}])| \)
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>( j = i, -i )</td>
<td>( 2(p_3 + p_2 + (2p_1 - 5)p_2p_3 + 1) )</td>
</tr>
<tr>
<td>( j \neq i, -i )</td>
<td>( 2(2p_3 + 2p_2 + (2p_1 - 6)p_2p_3) )</td>
</tr>
</tbody>
</table>
Square Free Groups of Order $p_1 p_2 \cdots p_n$ in General

**Theorem 11:** [Birkhoff & Hall] If $|G| = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ then

(a) $|Aut(G)|$ divides $\theta(p_1^{n_1}) \cdots \theta(p_r^{n_r})|G|^{r-1}$.

(b) if $G$ is solvable, $|Aut(G)|$ divides $\theta(p_1^{n_1}) \cdots \theta(p_r^{n_r})|G|$.

(c) if $G$ is nilpotent, $|Aut(G)|$ divides $\theta(p_1^{n_1}) \cdots \theta(p_r^{n_r})$.

where $\theta(p^n) = (p^n - 1)((p^n - p)\cdots(p^n - p^{n-1})$. 

33
So if $|\Gamma| = p_1p_2\cdots p_r$ where $p_1 < \cdots < p_r$ then the Sylow $p_r$-subgroup is unique and $p = p_r \nmid |\text{Aut}(Q)|$ where $|Q| = p_1\cdots p_{r-1} = m$.

Thus this program may be applied to all groups of square-free order.
Thank you!