Regular and Semi-regular Permutation Groups and Their Centralizers and Normalizers II

Timothy Kohl

May 2016
Motivation:

Let $K/k$ be separable where $\Gamma = Gal(\tilde{K}/k)$ and $\Gamma' = Gal(\tilde{K}/K)$ where $\tilde{K}$ is the Galois closure of $K/k$.

Any Hopf-Galois structure on $K/k$ corresponds to a regular subgroup $N \leq B = Perm(X)$ where $X$ is either $\Gamma$ or $\Gamma/\Gamma'$ where $\lambda(\Gamma) \leq \text{Norm}_B(N)$.

For now we shall consider the case where $\tilde{K} = K$ and $X = \Gamma$. 
If $K/k$ is Hopf-Galois for $H = (K[N])^{\Gamma}$ then one has $n = |N| = |\Gamma| = [K : k]$.

As such, there may be $N$ from different isomorphism classes of groups of order $n$.

**Definition** For $\Gamma$ as above and $[M]$ an isomorphism class of group of order $n$, let

$$R(\Gamma) = \{N \leq B \mid N \text{ regular and } \lambda(\Gamma) \leq \text{Norm}_{B}(N)\}$$

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

And so $R(\Gamma)$ is the union of $R(\Gamma, [M])$ over all isomorphism classes of groups $M$ of order $n$. 
Of course, some $R(\Gamma, [M])$ may be empty.

One problem with enumerating these $N$ is that one is 'searching' within the ambient symmetric group $B = \text{Perm}(\Gamma)$ and the other is trying to work with the normalization by the left regular representation of $\Gamma$.

A more broader view of this problem can be achieved by mentioning the following important fact.

**Theorem:** If $N$ and $M$ are regular subgroups of $B = \text{Perm}(X)$ which are isomorphic as groups, then they are conjugate as subgroups of $B$. 
So if one’s goal is the simple enumeration of \( R(\Gamma) \) then there is actually nothing special about \( \lambda(\Gamma) \).

Specifically, for any \( \beta \in B \)

\[
\lambda(\Gamma) \leq \text{Norm}_B(N) \iff \beta\lambda(\Gamma)\beta^{-1} \leq \text{Norm}_B(\beta N\beta^{-1})
\]

That is, the number of regular \( N \) normalized by \( \lambda(\Gamma) \) is the same as the number normalized by any conjugate of \( \lambda(\Gamma) \).
Also, what if one wants to consider the problem of looking at all Hopf-Galois structures on all Galois extensions of degree $n$?
One can proceed as follows.

Let $X$ be a set such that $|X| = n$, for simplicity we can even say $X = \{1, \ldots, n\}$ so that $B = \text{Perm}(X) = S_n$.

In $\text{Perm}(X)$ pick $\Gamma_1, \ldots, \Gamma_t$ which are regular subgroups, one from each isomorphism class of groups of order $n$. 
Define $R(\Gamma_i, [\Gamma_j])$ to be the set of those $N \leq B$ normalized by $\Gamma_i$ which are isomorphic to (and therefore conjugates of) $\Gamma_j$.

So one would like to enumerate $R(\Gamma_i, [\Gamma_j])$ for all pairings $(\Gamma_i, [\Gamma_j])$.

These count the number of Hopf-Galois structures on Galois extensions $K/k$ where $Gal(K/k) \cong \Gamma_i$ where the associated regular subgroup is of isomorphism type $[\Gamma_j]$. 
The enumeration of $R(\Gamma_i, [\Gamma_j])$ is related to the enumeration of:

$$S(\Gamma_j, [\Gamma_i]) = \{N \leq \text{Norm}_B(\Gamma_j) \mid N = \beta \Gamma_i \beta^{-1} \text{ for some } \beta \in B\}$$

the set of regular subgroups of $\text{Norm}_B(\Gamma_j)$ which are isomorphic (hence conjugate) to $\Gamma_i$.

The relationship between $S(\Gamma_j, [\Gamma_i])$ and $R(\Gamma_i, [\Gamma_j])$ was given by Byott (in relating regular $N$ normalized by $\lambda(\Gamma)$ to regular embeddings of $\Gamma$ into $\text{Hol}(N)$) and the presenter in the enumeration of the Hopf-Galois structures on cyclic extensions of degree $p^n$.

The following is a synthesis of these ideas.
For $\Gamma$ a regular subgroup of $B$, define $Hol(\Gamma)$ to be $Norm_B(\Gamma)$.

**Proposition** If $B = Perm(X)$ and $\Gamma_i$ and $\Gamma_j$ are regular subgroups of $B$ then

$$|S(\Gamma_j, [\Gamma_i])| \cdot |Hol(\Gamma_i)| = |R(\Gamma_i, [\Gamma_j])| \cdot |Hol(\Gamma_j)|.$$
The proof of this is takes advantage of the 'isomorphic' equals 'conjugate' idea so that one views both sides of this equation as the count of elements in $B$ that conjugate one regular subgroup to another.

In particular, what we show is that

$$
|\{\beta \in B \mid \beta \Gamma_i \beta^{-1} \leq Hol(\Gamma_j)\}| = |\{\alpha \in B \mid \Gamma_i \leq Hol(\alpha \Gamma_j \alpha^{-1})\}|
$$
If $M \in S(\Gamma_j,[\Gamma_i])$ then $M \leq Hol(\Gamma_j)$ and $M \cong \Gamma_i$ which implies that there exists $\beta \in B$ such that $M = \beta \Gamma_i \beta^{-1}$.

And since the normalizer of the conjugate is the conjugate of the normalizer then

$$\beta \Gamma_i \beta^{-1} \leq Hol(\Gamma_j) \iff \Gamma_i \leq Hol(\beta^{-1} \Gamma_j \beta)$$

and so $\beta^{-1} \Gamma_j \beta \in R(\Gamma_i,[\Gamma_j])$.

Also, if we replace $\beta$ by $\beta h$ for any $h \in Hol(\Gamma_i)$ then $(\beta h) \Gamma_i (\beta h)^{-1} = \beta \Gamma_i \beta^{-1} = M$.

However, the $(\beta h)^{-1} \Gamma_i (\beta h)$ are all (not necessarily distinct) elements of $R(\Gamma_i,[\Gamma_j])$. 
In parallel, any \( N \in R(\Gamma_i, [\Gamma_j]) \) is equal to \( \alpha \Gamma_j \alpha^{-1} \) for some \( \alpha \) and that replacing \( \alpha \) by \( \alpha k \) for any \( k \in Hol(\Gamma_j) \) yields the same \( N \).

Moreover \( \alpha^{-1} \Gamma_i \alpha \) lies in \( S(\Gamma_j, [\Gamma_i]) \) and likewise \( (\alpha k)^{-1} \Gamma_i (\alpha k) \).

Note that

\[
\beta_1 \Gamma_i \beta_1^{-1} = \beta_2 \Gamma_i \beta_2^{-1}
\]

if and only if

\[
\beta_1 Hol(\Gamma_i) = \beta_2 Hol(\Gamma_i)
\]

..
As such we can parametrize the elements of \( S(\Gamma_j, [\Gamma_i]) \) by a set of distinct cosets

\[
\beta_1 \text{Hol}(\Gamma_i), \ldots, \beta_s \text{Hol}(\Gamma_i)
\]

and \( R(\Gamma_i, [\Gamma_j]) \) by distinct cosets

\[
\alpha_1 \text{Hol}(\Gamma_j), \ldots, \alpha_r \text{Hol}(\Gamma_j)
\]
The bijection we seek is:

\[ \Phi : \bigcup_{k=1}^{s} \beta_k Hol(\Gamma_i) \rightarrow \bigcup_{l=1}^{r} \alpha_l Hol(\Gamma_j) \]
defined by \( \Phi(\beta_k h) = (\beta_k h)^{-1} \).

That \( \Phi(\beta_k h) \) lies in the union on the right hand side is due to the analysis given above, and this map is clearly bijective.
Since $Hol(\Gamma) \cong \Gamma \times Aut(\Gamma)$ then we have:

**Corollary 1:**

$$|S(\Gamma_j, [\Gamma_i])| \cdot |Aut(\Gamma_i)| = |R(\Gamma_i, [\Gamma_j])| \cdot |Aut(\Gamma_j)|.$$ and of course:

**Corollary 2:** For $\Gamma$ a particular regular subgroup of $B$:

$$|S(\Gamma, [\Gamma])| = |R(\Gamma, [\Gamma])|$$
Lastly, one should note that $e_B$ ’paramaterizes’ $\Gamma$ in $S(\Gamma, [\Gamma])$ and $R(\Gamma, [\Gamma])$ since trivially $e_B \Gamma e_B^{-1} = \Gamma$.

Moreover, suppose $N \in S(\Gamma, [\Gamma]) \cap R(\Gamma, [\Gamma])$ then there is some $\beta \in B$ such that $\beta \Gamma \beta^{-1} = N$, but then $M = \beta^{-1} \Gamma \beta$ also lies in $S \cap R$.

As such, we have a set $T = \{\beta_1, \ldots, \beta_k\}$ (where we may assume $\beta_1 = e_B$) such that

$$S \cap R = \{\beta_1 \Gamma \beta_1^{-1}, \ldots, \beta_k \Gamma \beta_k^{-1}\}$$

where $T$ contains the identity and is closed under inverses.

Is this set ever a group?
The answer is, sometimes.

More specifically, since $\beta$ and $\beta h$ determine the same conjugate of $\Gamma$ for any $h \in Hol(\Gamma)$ then this set $T$ is not unique.

However, it turns out that $T$ can be chosen such that it does form a group.
What is needed minimally is that all the $N \in S \cap R$ normalize each other.

For example, if $\Gamma = C_{p^n}$ then $|S \cap R| = p^r$ where $r = \left\lceil \frac{n}{2} \right\rceil$ and there exists (many) $T \leq B$ (all isomorphic to $C_{p^{r'}}$) which parameterize $S \cap R$. 
Moreover, for some $\Gamma$ there may be different isomorphism classes of groups, $T$, which parameterize $S \cap R$. For example, if $\Gamma = D_4$ then $|S \cap R| = 6$ and there exist 32 groups isomorphic to $C_6$ and 32 groups isomorphic to $S_3$ that parameterize $S \cap R$. 
Note, the parameterization of $S \cap R$ by a group is related to the idea of parameterizing the set

$$\mathcal{H}(\Gamma) = \{ N \leq Hol(\Gamma) \mid N \cong \Gamma \text{ and } \text{Norm}_B(N) = Hol(\Gamma) \}$$

$$= \{ N \triangleleft Hol(\Gamma) \mid N \cong \Gamma \}$$

$$\subseteq S \cap R$$

which is in direct correspondence with $NHol(\Gamma)/Hol(\Gamma)$ where $NHol(\Gamma) = \text{Norm}_B(Hol(\Gamma))$, the so called multiple holomorph of $\Gamma$.

Indeed, the orbit of $\Gamma$ under this quotient is exactly $\mathcal{H}(\Gamma)$, so this quotient would be embedded in any such $T$ that parameterizes $S \cap R$. 

20
Thank you!