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

Timothy Kohl
Boston University

May 24, 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 Γ or Γ/Γ' where $\lambda(\Gamma) \leq Norm_B(N)$.

Preliminaries:

We begin with some definitions.

Definition: If X is a finite set, let $B = Perm(X)$, a subgroup $N \leq B$ is *regular* if any two of the following conditions hold:

- N acts transitively on X
- N acts without fixed points, i.e. $\nu(x) = x$ only if $\nu = e_N$
- $|N| = |X|$

The canonical example(s) are $\lambda(\Gamma)$ and $\rho(\Gamma)$, the left and right regular representations of Γ in $Perm(\Gamma)$.

Definition: A subgroup of B which acts without fixed points is *semi-regular*.

Thus any subgroup of a regular subgroup is semi-regular.

As such, a semi-regular subgroup of order $|X|$ is therefore automatically regular, and any semi-regular subgroup can have at most $|X|$ elements.

We also observe that any subgroup of B which is transitive must have *at least* $|X|$ elements.

It's relatively easy to show that a semi-regular subgroup $K \leq B$ is a subgroup of a regular subgroup. (Basically one can extend K by a group of complementary order which remains semi-regular and is therefore regular.)

Does M being transitive imply that it contains a regular subgroup?

As it turns out, the answer is no.

(ref. TRANSITIVE PERMUTATION GROUPS WITHOUT SEMIREGULAR SUBGROUPS (2002) by Peter Cameron et. al., Journal of the London Mathematical Society)

Regularity imposes a number of restrictions on the cycle structure of elements.

Lemma:

If $x \in X$ and $\nu \in N$ then $|Orb_{\langle\nu\rangle}(x)| = |\nu|$

What this means is that if $\nu \in N$ where $|\nu| = r$ and $n = rs = |X| = |N|$ then ν is a product of s disjoint r-cycles.

Why? Since $\nu \in N$ then ν has no fixed points, and neither does any non-trivial power of ν.

So if ν contained a cycle of length $t < r = |\nu|$ then ν^t would have fixed points where $\nu^t \neq e_N$.

Normalizers

The condition $\lambda(\Gamma) \leq Norm_B(N)$ prompts us to consider the structure of the normalizer of a regular permutation group.

For $B = Perm(\Gamma)$ and $N = \lambda(\Gamma)$, it is a standard fact (for example in Marshall Hall's book) that

$$Norm_B(\lambda(\Gamma)) = \rho(\Gamma)Aut(\Gamma)$$

where $\rho(\gamma)(\gamma') = \gamma'\gamma^{-1}$ is the right regular representation and $Aut(\Gamma) = \{h \in Norm_B(\lambda(\Gamma)) \mid h(e_\Gamma) = e_\Gamma\}$.

This is canonically isomorphic to $\Gamma \rtimes Aut(G)$ and actually the original definition of $Hol(\Gamma)$ the holomorph of Γ.

An interesting 'extremal' example is the case where Γ is a complete group, for then $Hol(\Gamma) = \lambda(\Gamma)\rho(\Gamma) \cong \Gamma \times \Gamma$.

This seems incorrect since there does not seem to be an $Aut(\Gamma)$ factor.

However, completeness includes the condition that $Aut(\Gamma) = Inn(\Gamma)$ which can be represented as $\{\lambda(g)\rho(g) \mid g \in \Gamma\}$ so that $\rho(\Gamma)Aut(\Gamma) = \lambda(\Gamma)\rho(\Gamma)$.

Since the left and right regular representations of Γ always commute then $Hol(G)$ is a direct product.

The significance of $\rho(\Gamma)$ in these examples is that $\rho(\Gamma) = Cent_B(\lambda(G))$.

Definition: For N a regular subgroup of B, the *opposite* group is $N^{opp} = Cent_B(N)$.

Note: In some old papers this is called the *conjoint*. (The opposite has a definition given in terms of the elements of N but it coincides with $Cent_B(N)$ anyway.)

So for N regular one has

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

where $Aut(N) = \{h \in Norm_B(N) \mid h(e_\Gamma) = e_\Gamma\}$.

In fact, there is nothing terribly special about the condition $h(e_\Gamma) = e_\Gamma$.

We may observe that for $N \leq B$ regular that

$$Norm_B(N) = N^{opp} A_{(\gamma,N)}$$

where $A_{(\gamma,N)} = \{h \in Norm_B(N) \mid h(\gamma) = \gamma\}$ for *any* $\gamma \in \Gamma$.

Indeed, all the $A_{(\gamma,N)}$ are conjugate, specifically $\pi A_{(\gamma,N)} \pi^{-1} = A_{(\pi(\gamma),N)}$ for any $\pi \in B$.

We observe the following symmetries of $(\ )^{opp}$:

- $N \cap N^{opp} = Z(N)$
- If N is semi-regular then N^{opp} is transitive.
- If N is transitive then N^{opp} is semi-regular.
- N is regular iff N^{opp} is regular
- $(N^{opp})^{opp} = N$ if N is (semi-)regular
- $Norm_B(N) = Norm_B(N^{opp})$

The last statement above is a consequence of the following:

Lemma:

Given a regular subgroup N of B, and its normalizer $Norm_B(N)$. If M is a normal regular subgroup of $Norm_B(N)$ then $Norm_B(N) \leq Norm_B(M)$.

If $|Aut(M)| = |Aut(N)|$ then $Norm_B(N) = Norm_B(M)$.

This leads to a different kind of symmetry between regular subgroups N normalized by $\lambda(\Gamma)$. In particular, in this theorem N and M need not be isomorphic as groups in order to have isomorphic holomorphs.

A classic example of this phenomenon is the relationship between the dihedral groups D_{2n} and quaternionic (dicyclic) groups Q_n of order $4n$ for $n \geq 3$:

$$D_{2n} = \{x, t |\ x^{2n} = 1, t^2 = 1, xt = tx^{-1}\}$$
$$Q_n = \{x, t |\ x^{2n} = 1, t^2 = x^n, xt = tx^{-1}\}$$

and viewed as subgroups of $Perm(\{x^i, tx^i\})$ they have a common automorphism group:

$$\begin{aligned} Aut(D_{2n}) &= \{\phi_{(i,j)} \mid i \in \mathbb{Z}_{2n}, j \in U(\mathbb{Z}_{2n})\} \\ &\cong \mathbb{Z}_{2n} \rtimes U(\mathbb{Z}_{2n}) \cong Hol(\mathbb{Z}_{2n}) \\ &\text{where } \phi_{(i,j)}(t^a x^b) = t^{ia} x^{ia+jb} \end{aligned}$$

It was known by Burnside that in fact $Hol(D_{2n}) \cong Hol(Q_n)$ and by viewing both as permutations on $\{x^i, tx^i\}$ we have that $Hol(D_{2n}) = Hol(Q_n)$ since one can show that:

$$\rho_Q(x^b)\phi_{(i,j)} = \rho_D(x^b)\phi_{(i,j)}$$
$$\rho_Q(tx^b)\phi_{(i,j)} = \rho_D(tx^{b+n})\phi_{(i+n,j)}$$

The upshot of this is that if $\lambda(\Gamma)$ normalizes a given copy of D_{2n} then it normalizes its opposite as seen above, and it also normalizes a copy of Q_n and *its* opposite.

Other examples:

$$n = 40$$

$$\{D_{20}, Q_{10}\}$$

$$\{C_{20} \rtimes C_2, C_4 \times D_5\}$$

$$n = 88$$

$$\{D_{44}, Q_{22}\}$$

$$\{C_{44} \rtimes C_2, C_4 \times D_{11}\}$$

$$n = 156$$

$$\{D_{78}, Q_{39}\}$$

$$\{C_3 \times Q_{13}, C_6 \times D_{13}\}$$

$$\{C_{26} \times D_3, C_{13} \times Q_3\}$$

$$\{C_2 \times ((C_{13} \rtimes C_3) \rtimes C_2), (C_{13} \rtimes C_4) \rtimes C_3\}$$

Decompositions

When $\Gamma = C_r \times C_s$ where $gcd(r,s) = 1$ then $Aut(\Gamma) \cong Aut(C_r) \times Aut(C_s)$ and concordantly

$$Hol(\Gamma) \cong Hol(C_r) \times Hol(C_s)$$

Similarly if Γ nilpotent, expressed as a product of its Sylow p-subgroups, then its holomorph is a direct product of the holomorphs of each of these (characteristic) subgroups.

Other decompositions are possible.

If G is centerless then Fitting (using the Krull-Remak-Schmidt theorem) showed that G is decomposable as a product of distinct indecomposable normal subgroups (up to order)

$$G \cong (G_{11} \times \cdots \times G_{1n_1}) \times \cdots \times (G_{s1} \times \cdots \times G_{sn_s})$$

where the $G_{i1}, \ldots G_{in_i}$ are all isomorphic, and $G_{ij} \not\cong G_{kl}$ unless $i = k$. Furthermore

$$Aut(G) \cong (Aut(G_{i1}) \wr S_{n_1}) \times \cdots \times (Aut(G_{s1}) \wr S_{n_s})$$

whence

$$Hol(G) \cong (Hol(G_{i1}) \wr S_{n_1}) \times \cdots \times (Hol(G_{s1}) \wr S_{n_s})$$

Bear in mind that in these examples the component groups are normal, semi-regular subgroups. So for a given $N \leq B$ regular with $K \triangleleft N$ then obviously $K \leq Norm_B(N)$.

In fact, K is characteristic in N if and only if $K \triangleleft Norm_B(N)$.

To see this, realize that what $Hol(N)$ represents is the largest subgroup of B wherein automorphisms of N are realized by conjugation.

(i.e. The distinction between Inner and Outer automorphisms goes away.)

Semi-Regular Subgroups and Wreath Products

The wreath products in the automorphisms (and holomorphs) seen earlier can be understood by looking at the centralizers/normalizers of semi-regular subgroups.

We start with a classic example due to Burnside.

Let $n = rs$ and consider the semi-regular cyclic subgroup $K = \langle (1, 2, \ldots, s) \cdots ((r-1)s+1, \ldots, rs) \rangle \leq S_n$.

We have

$$\begin{aligned} Cent_{S_n}(K) &\cong C_s \wr S_r \\ &= (C_s \times \cdots \times C_s) \rtimes S_r \end{aligned}$$

where S_r acts by coordinate shift on C_s^r.

and where each copy of C_s corresponds to a cycle

$$((j-1)s+1, \ldots, js)$$

in the generator of K and for $(j-1)s+k \in \{1, \ldots, n\}$ one applies an element $\sigma \in S_r$ to send it to $(j'-1)s+k$ where it is then acted on by a power of $((j'-1)s+1, \ldots, j's)$.

This wreath product is a subgroup of a larger one within S_n, namely the subgroup of S_n consisting of those permutations which preserve the supports (blocks)

$$\Pi_j = \{(j-1)s + 1, \ldots, js\}$$

that is

$$(Perm(\Pi_1) \times \cdots \times Perm(\Pi_r)) \rtimes S_r \cong S_s \wr S_r$$

For this same $K \leq S_n$ the normalizer is a 'twisted' wreath product:

$$Norm_{S_n}(K) \cong C_s^r \rtimes (\Delta \times S_r)$$

where Δ is isomorphic to $Aut(C_s)$ acting by exponentiating each s-cycle to the same unit, and S_r still acts by coordinate shift.

That is

$$(j-1)s+k \mapsto ((j'-1)s+1,\ldots,j'r))^u((j'-1)s+k)$$

for $u \in U_s$.

For $K \leq B$ a general semi-regular subgroup (not necessarily cyclic) one has

$$Cent_B(K) \cong K \wr S_r$$
$$Norm_B(K) \cong K^r \rtimes (Aut(K) \times S_r)$$

where $r = n/|K|$ and the analogues of the Π_i are the orbits under the action of K.

As such, if $K \triangleleft N$ for some regular N then $N \leq Norm_B(K)$ where the structure of this normalizer is as given above.

Moreover, $K|_{\Pi_i}$ is a regular subgroup of $Perm(\Pi_i)$.

On a somewhat related note, the appearance of wreath products in this discussion can be looked at as a consequence of the following.

Universal Embedding Theorem [Kaloujnine-Krasner]

Given an exact sequence of groups

$$1 \to K \to N \to Q \to 1$$

expressing N as an extension of K by Q (split or not) then one may find an isomorphic copy of N embedded in $K \wr Q$.

Now, if we view N as embedded as a regular subgroup of $B = Perm(X)$ with semi-regular subgroup K then $Cent_B(K) \cong K \wr S_m$ where $m = [N : K] = |Q|$.

And thus, this S_m will contain a reqular subgroup isomorphic to Q.

But this $K \wr Q$ centralizes K so any extension of K by Q contained herein would have to centralize K.

Well, if $K \leq N$ then $N^{opp} \leq Cent_B(K)$ and, of course $N \cong N^{opp}$.

An interesting curio appears when looking again at the dihedral groups D_n.

Recall that

$$D_n = \{x, t|\ x^n = 1, t^2 = 1, xt = tx^{-1}\}$$

and if $C_n = \langle x \rangle$ then $\lambda(C_n) \leq \lambda(D_n)$ is a semi-regular subgroup.

Since $\lambda(x)$ is a product of two disjoint n-cycles then by the above result:

$$Norm_B(\lambda(C_n)) \cong (C_n \times C_n) \rtimes (U_n \times S_2)$$

where $U_n = (\mathbb{Z}_n)^* \cong Aut(C_n)$ so that, in particular $|Norm_B(\lambda(C_n))| = 2n^2\phi(n)$

But now, since $\lambda(C_n)$ is characteristic in $\lambda(D_n)$ then $Norm_B(\lambda(D_n)) \leq Norm_B(\lambda(C_n))$.

And since

$$\begin{aligned} Norm_B(\lambda(D_n)) &= Hol(D_n) \\ &\cong D_n \rtimes Hol(C_n) \\ &\cong D_n \rtimes (C_n \rtimes U_n) \end{aligned}$$

then $|Norm_B(D_n)| = 2n{\cdot}n{\cdot}\phi(n)$ which is exactly $|Norm_B(\lambda(C_n))|$

As such, we have

$$Norm_B(\lambda(C_n)) = Norm_B(\lambda(D_n))$$

so that any question about groups normalizing $\lambda(D_n)$ can be examined by looking at whether they normalize $\lambda(C_n)$.

Thank you!