Enumerating Hopf-Galois Structures on Dihedral Extensions

Timothy Kohl

Boston University

May 27, 2019

Hopf-Galois Theory

An extension K/k is Hopf-Galois if there is a k-Hopf algebra H and a k-algebra homomorphism $\mu : H \to End_k(K)$ such that

- $\mu(ab) = \sum_{(h)} \mu(h_{(1)}(a)\mu(h_{(2)})(b)$
- $K^H = \{a \in K \mid \mu(h)(a) = \epsilon(h)a \ \forall h \in H\} = k$
- μ induces $I \otimes \mu : K\#H \xrightarrow{\cong} End_k(K)$

By the Greither-Pareigis theorem, for K/k a Galois extension of fields with $G = Gal(K/k)$ the Hopf algebras which act are of the form $(K[N])^G$ where $N \leq B = Perm(G)$ is a regular subgroup normalized by $\lambda(G) \leq B$.

The enumeration therefore is of those regular $N \leq B$, where N must have the same cardinality as G but need not be isomorphic.

To organize any such enumeration we define:

$$R(G) = \{N \leq B \mid N \text{ regular and } \lambda(G) \leq Norm_B(N)\}$$
$$R(G,[M]) = \{N \in R(G) | N \cong M\}$$

where $[M]$ denotes an isomorphism class of a group of order $|G|$.

We will be considering $R(G,[G])$ for G a dihedral group.

The general setup will be as follows. We assume that L/K is Galois with group $G = D_n$ and so $B = Perm(G)$ where D_n may be presented as

$$\begin{aligned} D_n &= \{x, t \mid x^n = 1, t^2 = 1, xt = tx^{-1}\} \\ &= \{1, x, x^2, \ldots, x^{n-1}, t, tx, tx^2, \ldots, tx^{n-1}\} \end{aligned}$$

where $|D_n| = 2n$, for $n \geq 3$.

Note, for N a regular subgroup of B one has

$$Norm_B(N) \cong Hol(N) \cong N \rtimes Aut(N)$$

and since $N \in R(D_n, [D_n])$ we begin with a number of observations about D_n and its holomorph.

Proposition

For $n \geq 3$ *with* $D_n = \{t^a x^b | a \in \mathbb{Z}_2; b \in \mathbb{Z}_n\}$ *and letting* $U_n = \mathbb{Z}_n^*$

(a) $C = \langle x \rangle$ *is a characteristic subgroup of* D_n

(b) $Aut(D_n) = \{\phi_{i,j} | i \in \mathbb{Z}_n; j \in U_n\}$ *where*

$$\phi_{i,j}(t^a x^b) = t^a x^{ia+jb}$$

$$\phi_{i_2,j_2} \circ \phi_{i_1,j_1} = \phi_{i_2+j_2 i_1, j_2 j_1}$$

(c) $Aut(D_n) \cong Hol(\mathbb{Z}_n)$

In order to organize the enumeration of the $N \in R(G, [G])$ we consider some global structural information about how a regular subgroup isomorphic to D_n acts on the elements of D_n viewed as a set.

Wreath Products and Blocks

Definition

If G is a permutation group acting on a set Z then a *block* for G is a subset $X \subseteq Z$ such that for $g \in G$, $X^g = X$ or $X^g \cap X = \emptyset$.

In our example, we shall consider Z as the underlying set of $G = D_n$ and look at blocks arising from subgroups of $B = Perm(G)$ and in particular how regularity ties in with these block structures. Recalling our presentation of D_n define :

$$X = \{1, x, x^2, \ldots, x^{n-1}\}$$
$$Y = \{t, tx, tx^2, \ldots, tx^{n-1}\}$$
$$Z = X \cup Y$$

where $Z = G$ (as sets) and $B \cong Perm(Z)$.

Next, define $\tau_* : X \to Y$ by $\tau_*(x^j) = tx^j$ which induces an isomorphism $Perm(X) \to Perm(Y)$

From here on, we set $B_X = Perm(X)$ and $B_Y = Perm(Y)$ and consider

$$W(X, Y) = (B_X \times B_Y) \rtimes \langle \tau \rangle$$

where τ has order 2 and is defined as follows:

$$\tau(\beta)(x) = \tau_*^{-1}(\beta(\tau_*(x))) \text{ for } x \in X \text{ and } \beta \in B_Y$$
$$\tau(\alpha)(y) = \tau_*(\alpha(\tau_*^{-1}(y))) \text{ for } y \in Y \text{ and } \alpha \in B_X$$

As $B_X \cong B_Y \cong S_n$ and $\langle \tau \rangle \cong S_2$ we find that

$$W(X, Y) \cong S_n \wr S_2$$

the wreath product of S_n and S_2.

Note: As an element of B,

$$\tau = (1,t)(x,tx)\dots(x^{n-1},tx^{n-1}) \\ = \lambda(t)$$

Define a map $\delta : W(X,Y) \to B = Perm(Z)$ by

$$\delta(\alpha,\beta,\tau^k)(z) = \begin{cases} \beta(\tau_*(z)), \ k=1, \ z \in X \\ \alpha(z), \ k=0, \ z \in X \\ \alpha(\tau_*^{-1}(z)), \ k=1, \ z \in Y \\ \beta(z), \ k=0, \ z \in Y \end{cases}$$

It is readily verified that δ is an embedding of $W(X,Y)$ as a subgroup of B.

We need to make a number of observations about wreath products such as $W(X, Y)$ which are probably known but for which no convenient reference could be found.

Lemma

If $w \in W(X, Y)$ then either $w(X) = X$ and $w(Y) = Y$ or $w(X) = Y$ and $w(Y) = X$.

As such, we may regard $W(X, Y)$ as the maximal subgroup of B for which X is a block.

Although we shall use the above indicated choice of τ_*, it is useful to observe the following.

Proposition

For any two bijections τ_* and τ'_* of X to Y, the induced wreath products W and W' are equal as subgroups of B.

Definition

For Z such that $|Z| = 2n$, a *splitting* $\{X, Y\}$ of Z is a partition of Z into two equal size subsets.

We note that for a given splitting $\{X, Y\}$ of Z every bijection $\tau_* : X \to Y$ yields the same subgroup of B which we may denote $W(X, Y; \tau_*)$ or simply $W(X, Y)$.

Also, for later use, we note the following:

Proposition

For a given splitting $\{X, Y\}$ and $\sigma \in B$, we have $\sigma W(X, Y)\sigma^{-1} = W(X^\sigma, Y^\sigma)$ where $X^\sigma = \sigma(X)$ and $Y^\sigma = \sigma(Y)$.

Corollary

$Norm_B(W(X,Y)) = W(X,Y)$

As a small aside, we can consider, for a given $\{X, Y\}$ the subgroup $S(X,Y) = B_X \times B_Y$ of B.

Proposition

$S(X,Y) \triangleleft W(X,Y)$ and, in fact, $Norm_B(S(X,Y)) = W(X,Y)$.

Note, $W(X,Y) = S(X,Y) \cup S(X,Y)\tau$ for any τ induced by $\tau_* : X \to Y$.

Before considering the enumeration of $R(G)$ we shall first consider how regularity and block structure are connected.

Proposition

If $N \leq B$ is regular then $N \leq W(X, Y)$ if and only if N contains an index 2 subgroup K with $X = Ke_G$. (assuming $e_G \in X$)

The K's which arise are of course normal, but we need the following fact about the normalizers of regular subgroups N.

Proposition

If $N \leq B$ is regular and $N \leq W(X, Y)$ corresponding to $K \leq N$ as above, then $Norm_B(N) \leq W(X, Y)$ if and only if K is a characteristic subgroup of N.

Corollary

If $N \leq B$ is regular and $N \leq W(X, Y)$ corresponding to $K \leq N$ as above, and K is unique, then $Norm_B(N) \leq W(X, Y)$ for the splitting $\{X, Y\}$ corresponding to K only.

Proof.

The bijection $b : N \to G$ (given by $b(n) = ne_G$) induces an isomorphism $\phi : Perm(G) \to Perm(N)$ and if $X = Ke_G$, then $b(X) = Ke_N = K = \tilde{X}$, and similarly $\tilde{Z} = N$ and $\tilde{Y} = \tilde{Z} - \tilde{X}$. In $Perm(N)$ we have $\phi(K) = \lambda(K) \leq \lambda(N) = \phi(N)$ corresponding to $\tilde{X} = K$. Now, $Hol(N) = Norm_{Perm(N)}(N) = \rho(N)Aut(N)$ and so for $\eta \in Hol(N)$ we have $\eta = \rho(m)\alpha$ for $m \in N$ and $\alpha \in Aut(N)$ and so if K is characteristic then

$$\begin{aligned}\eta(\tilde{X}) &= \rho(m)\alpha(K)\\ &= Km^{-1}\\ &= K \text{ or } N - K \ (i.e.\ \tilde{X} \text{ or } \tilde{Y})\end{aligned}$$

For the converse observe that $N = K \cup nK$ (for some $n \notin K$) and so for $\alpha \in Aut(N) \leq Norm_B(N)$ we have $\alpha(K) = K$ or nK which, of course, means $\alpha(K) = K$, so, in fact, $Norm_B(N) \leq W(X, Y)$ implies $Aut(N) \leq S(X, Y) = B_X \times B_Y$. □

The block/splitting structure of $\lambda(G)$ for $G = D_n$ is as follows.

Proposition

Given $G = D_n$ as presented above, then:

(a) If n is odd, then $\lambda(G) \leq W(X_0, Y_0)$ for exactly one $\{X_0, Y_0\}$.

(b) If n is even then $\lambda(G) \leq W(X_i, Y_i)$ for exactly three $\{X_i, Y_i\}$

Proof

The underlying set is $\{1, x, \ldots, x^{n-1}, t, tx, \ldots, tx^{n-1}\}$ and

$$\lambda(x) = (1\ x\ \cdots x^{n-1})(t\ tx^{n-1}\ \ldots tx)$$

and

$$\lambda(t) = (1\ t)(x\ tx)\cdots(x^{n-1}\ tx^{n-1})$$

For n odd, the claim is that there is exactly one block of size n (equivalently only one splitting yielding a wreath product containing G), namely

$$X_0 = \{1, x, \ldots, x^{n-1}\} \text{ and } Y_0 = \{t, tx, \ldots, tx^{n-1}\}$$

which corresponds to the unique index 2 subgroup $K_0 = \langle\lambda(x)\rangle$ where $X_0 = Orb_{\langle\lambda(x)\rangle}(1)$.

For n even, we have the following two additional splittings:

$$X_1 = \{1, x^2, \ldots, x^{n-2}, t, tx^2, \ldots, tx^{n-2}\}$$
$$Y_1 = \{x, x^3, \ldots, x^{n-1}, tx, tx^3, \ldots, tx^{n-1}\}$$

and

$$X_2 = \{1, x^2, \ldots, x^{n-2}, tx, tx^3, \ldots, tx^{n-1}\}$$
$$Y_2 = \{x, x^3, \ldots, x^{n-1}, t, tx^2, \ldots, tx^{n-2}\}$$

which correspond to the additional index 2 subgroups $K_1 = \langle \lambda(x^2), \lambda(t) \rangle$ and $K_2 = \langle \lambda(x^2), \lambda(tx^{n-1}) \rangle$

However, only K_0 is ever characteristic.

Corollary

For all n, if $G = D_n$ *then* $Hol(G) \leq W(X_0, Y_0)$ *for a unique* $\{X_0, Y_0\}$.

i.e. For n even, $\lambda(G)$ is contained in $W(X_i, Y_i)$ for $i = 0, 1, 2$, but the holomorph is only contained in $W(X_0, Y_0)$.

Now, as far as the membership of $R(D_n, [D_n])$ is concerned, we have the following.

Theorem

Let $N \in R(D_n, [D_n])$ *with* K *the characteristic index 2 subgroup of* N *and* $X = K \cdot 1$ *(with* $Y = Z - X$*).*

(a) If n *is odd then* $X = X_0$*.*

(b) If n *is even then* $X = X_i$ *for either* $i = 0$*, 1, or 2.*

Part (a) is a consequence of the fact that $\lambda(G) \leq W(X_0, Y_0)$ uniquely so that $\lambda(G) \leq Norm_B(N) \leq W(X, Y)$ implies $X = X_0$.

Part (b) is a consequence of the fact that $Norm_B(N) \leq W(X, Y)$ and $\lambda(G) \leq W(X_i, Y_i)$ for $i = 0, 1, 2$ so that X must be X_i for *exactly one* such i.

The splitting corresponding to the index 2 characteristic subgroup K of any $N \in R(D_n, [D_n])$ is sufficient to actually determine N itself.

To see this, we start by considering the subgroup $K_0 = \langle \lambda(x) \rangle \leq \lambda(D_n)$

Proposition

[1, Prop. 2.6] Given $G = D_n$ *as presented above, with* $K_0 = \lambda(\langle x \rangle) \leq \lambda(G)$, $Norm_B(K_0) = Norm_B(\lambda(G)) = Hol(G)$.

What we have in general is that if $N \cong D_n$ is regular and K its index 2 characteristic subgroup then $Norm_B(N) = Norm_B(K)$.

Theorem

For $G = D_n$, if $G \cong N \leq B$ is regular with $K \leq N$ the index 2 characteristic subgroup then $\lambda(G)$ normalizes N iff and only if $\lambda(G)$ normalizes K.

The advantage of this is that, if K is generated by $k_X k_Y$ (a product of two disjoint n-cycles) where $1 \in Supp(k_X)$ we can focus on how it is acted on by $\lambda(x)$ and $\lambda(t)$, starting with the fact that $Orb_{\langle k_X \rangle}(1) = X_i$ for $i = 0$, 1, or 2 as indicated above.

Moreover, we need not worry about the order 2 generator of N.

Why?

Proposition

If $k_X k_Y$ is product of two disjoint n-cycles, then $K = \langle k_X k_Y \rangle$ is the index 2 characteristic subgroup of exactly one regular subgroup $N \leq B$ where $N \cong D_n$.

(Why?) Since τ has order 2, it must be a product of n disjoint transpositions by regularity.

We claim that $\tau(X) = Y$ and $\tau(Y) = X$.

If n is odd then $\tau(X) = X$ and $\tau(Y) = Y$ is clearly impossible since one of the transpositions would have to contain an element of X and one from Y which would contradict $\tau(X) = X$.

If n is even then one *could* have $n/2$ transpositions with elements from X and $n/2$ transpositions with elements from Y, but what would happen is that the resulting group $\langle k_x k_y, \tau \rangle$ would have fixed points.

For example, if $k_X = (1,2,3,4)$ and $k_Y = (5,6,7,8)$ and $\tau = (1,4)(2,3)(5,8)(6,7)$ then $\tau k_X \tau^{-1} = k_X^{-1}$ and $\tau k_Y \tau^{-1} = k_Y^{-1}$ so that $\langle k_x k_y, \tau \rangle \cong D_4$ but this group is not fixed point free, e.g.

$$(1,2,3,4)(5,6,7,8)(1,4)(2,3)(5,8)(6,7) = (2,4)(6,8)$$

In contrast $\langle (1,2,3,4)(5,6,7,8), (1,8)(2,7)(3,6)(4,5) \rangle$ is also isomorphic to D_4 but is regular too.

As such τ is a product of disjoint transpositions where each transposition contains one element from X and one from Y.

Specifically if $k_X = (z_1, z_2, \ldots, z_n)$ and $k_Y = (z'_1, z'_2, \ldots z'_n)$ (whence $k_Y^{-1} = (z'_n, z'_{n-1}, \ldots, z'_2, z'_1)$) then the only possibilities for τ are

$$
\begin{aligned}
&(z_1, z'_n)(z_2, z'_{n-1})(z_3, z'_{n-2}) \cdots (z_n, z'_1) \\
&(z_1, z'_{n-1})(z_2, z'_{n-2})(z_3, z'_{n-3}) \cdots (z_n, z'_n) \\
&(z_1, z'_{n-2})(z_2, z'_{n-3})(z_3, z'_{n-4}) \cdots (z_n, z'_{n-1}) \\
&\vdots \\
&(z_1, z'_1)(z_2, z'_n)(z_3, z'_{n-1}) \cdots (z_n, z'_2)
\end{aligned}
$$

where each (together with $k_X k_y$) generate the same group.

As such, the enumeration of $N \in R(D_n, [D_n])$ is equivalent to the characterization of $K \leq N$ the (cyclic) characteristic subgroup of index 2.

We divide the analysis between the case where n is odd, versus when n is even.

Also integral to the determination of $|R(G,[G])|$ is the notion of the multiple holomorph of a group.

Briefly, the collection

$$\mathcal{H}(G) = \{ \text{ regular } N \leq Hol(G) \mid N \cong G \text{ and } Hol(N) = Hol(G)\}$$

is exactly parameterized by $\tau \in T(G) = Norm_B(Hol(G))/Hol(G)$ the multiple holmorph of G.
i.e.

$$\mathcal{H}(G) = \{\tau\lambda(G)\tau^{-1} \mid \tau \in T(G)\}$$

And since $\lambda(G) \leq Hol(G) = Hol(N)$ it is quite clear that $\mathcal{H}(G) \subseteq R(G,[G])$.

And for D_n we have the following

Theorem

[1, Thm. 2.11] For $G = D_n$ we have:

$$|\mathcal{H}(D_n)| = |T(D_n)| = |\Upsilon_n|$$

where $\Upsilon_n = \{u \in U_n \mid u^2 = 1\}$ the units of exponent 2 mod n.

What we wish to show is the following:

Theorem

For $G = D_n$ we have that $|R(G, [G])|$ equals

(a) $|\Upsilon_n|$ if n is odd, where all $Norm_B(N) \leq W(X_0, Y_0)$

(b) $\mu_n|\Upsilon_n|$ for n even, for $Norm_B(N) \leq W(X_0, Y_0)$ where

$$\mu_n = |\{v \in \Upsilon_n \mid gcd(v+1, n) = 2\}|$$

(c) $\frac{\frac{n}{2} \cdot |\Upsilon_n| \cdot \phi(\frac{n}{2})}{\phi(n)}$ for n even, for $Norm_B(N) \leq W(X_i, Y_i)$ for $i = 1, 2$

[Note: If $8|n$ then $\mu_n = 2$ otherwise $\mu_n = 1$.]

We start by considering those $N \in R(G, [G])$ for which $Norm_B(N) \leq W(X_0, Y_0)$ where

$$X_0 = \{1, x, \ldots, x^{n-1}\}$$
$$Y_0 = \{t, tx, \ldots, tx^{n-1}\}$$

and we recall that this is true automatically if n is odd.

In this case, if $K \leq N$ is the (unique) subgroup of index 2, we have $K = \langle k \rangle = \langle k_X k_Y \rangle$ where $Supp(k_X) = X_0$ and $Supp(k_Y) = Y_0$.

Since $Supp(k_X) = X_0$ and $Supp(k_Y) = Y_0$ then $k_X(x^i) = x^{k_X(i)}$ and $k_Y(tx^j) = tx^{k_Y(j)}$ so we may, for convenience, identify

$$k_X = (x^{i_0}, x^{i_1}, \ldots, x^{i_{n-1}}) = (i_0, i_1, \ldots, i_{n-1})$$
$$k_Y = (tx^{j_0}, tx^{j_1}, \ldots, tx^{j_{n-1}}) = (j_0, j_1, \ldots, j_{n-1})$$

The question is, what are the possibilities for these two n-cycles?

We begin by using the fact that N (whence K) is normalized by $\lambda(D_n)$ so in particular by $\lambda(t)$ and $\lambda(x)$.

We have

$$\begin{aligned}\lambda(x)k\lambda(x)^{-1}(x^i) &= \lambda(x)k(x^{i-1}) \\ &= \lambda(x)(x^{k_X(i-1)}) \\ &= x^{k_X(i-1)+1}\end{aligned}$$

and

$$\begin{aligned}\lambda(x)k\lambda(x)^{-1}(tx^j) &= \lambda(x)k(x^{j+1}) \\ &= \lambda(x)(tx^{k_Y(j+1)}) \\ &= tx^{k_Y(j+1)-1}\end{aligned}$$

where $\lambda(x)k\lambda(x)^{-1} = k^v = k_X^v k_Y^v$ for some $v \in U_n$ where $v^n = 1$.

So under the identification

$$
\begin{aligned}
k_X &= (i_0, i_1, \ldots, i_{n-1}) \\
k_Y &= (j_0, j_1, \ldots, j_{n-1}) \\
i_0 &= 0 \quad j_0 = 0
\end{aligned}
$$

we have $k_X^v = (i_0, i_v, \ldots, i_{(n-1)v})$ and $k_Y^v = (j_0, j_v, \ldots, j_{(n-1)v})$ and therefore:

$$
\begin{aligned}
k_X(i_a - 1) &= i_{a+v} - 1 \\
k_Y(j_b + 1) &= j_{b+v} + 1
\end{aligned}
$$

If we assume $i_{rv} = 1$ for some r then we have

$$k_X(i_{rv} - 1) = k_X(0) = k_X(i_0) = i_{(r+1)v} - 1 = i_1$$

but then

$$k_X(i_1) = k_X(i_{(r+1)v} - 1) = i_{(r+2)v} - 1 = i_2$$
$$k_X(i_2) = k_X(i_{(r+2)v} - 1) = i_{(r+3)v} - 1 = i_3$$
$$\cdots$$

which implies that $i_{(r+e)v} - i_e = 1$ for each $e \in \mathbb{Z}_n$.

Similarly, for some s, we have $j_{sv} + 1 = j_0 = 0$ (i.e. $j_{sv} = -1$) and so a similar inductive argument shows that

$$j_{(s+e)v} - j_e = -1 = n - 1$$

for each $e \in \mathbb{Z}_n$.

Normalization by $\lambda(t)$ yields

$$\begin{aligned}\lambda(t)k\lambda(t)^{-1}(x^i) &= \lambda(t)k(tx^i)\\ &= \lambda(t)(tx^{k_Y(i)})\\ &= x^{k_Y(i)}\end{aligned}$$

and

$$\begin{aligned}\lambda(t)k\lambda(t)^{-1}(tx^j) &= \lambda(t)k(x^j)\\ &= \lambda(t)(x^{k_X(j)})\\ &= tx^{k_X(j)}\end{aligned}$$

where $\lambda(t)k\lambda(t)^{-1} = k^u = k_X^u k_Y^u$ for some $u \in U_n$ where $u^2 = 1$.

What this implies is that $x^{i_{e+u}} = k_X^u(x^{i_e}) = x^{k_Y(i_e)}$, and if we again focus on the exponents we get

$$i_{e+u} = k_X^u(i_e) = k_Y(i_e)$$

so we can consider what happens with $e = 0, 1, \dots$ (recalling that $i_0 = j_0 = 0$ and that $k_Y(j_f) = j_{f+1}$) then we get

$$\begin{aligned} i_u &= k_Y(i_0) = k_Y(j_0) = j_1 \\ i_{2u} &= k_Y(i_u) = k_Y(j_1) = j_2 \\ i_{3u} &= k_Y(i_{2u}) = k_Y(j_2) = j_3 \\ &\vdots \end{aligned}$$

namely $j_f = i_{uf}$ for each $f \in \mathbb{Z}_n$, and since $u^2 = 1$ we can write this as $j_{uf} = i_f$ too.

So to summarize so far, we have n-cycles $(i_0, \ldots, i_{n-1})$ and $(j_0, \ldots, j_{n-1})$ where the $i's$ and $j's$ satisfy the following relations

$$\begin{aligned} i_0 &= 0 \\ j_0 &= 0 \\ i_{rv} &= 1 \text{ for some } r \\ j_{sv} &= -1 \text{ for some } s \\ i_{(r+e)v} - i_e &= 1 \text{ for each } e \in \mathbb{Z}_n \\ j_{(s+e)v} - j_e &= -1 \text{ for each } e \in \mathbb{Z}_n \\ j_g &= i_{ug} \text{ for each } g \in \mathbb{Z}_n \end{aligned}$$

where $u^2 = 1$ and $v^n = 1$.

So the question is what are the solutions of this system of equations, as these determine the possibilities for $k = k_X k_Y$.

Simplification (1): The relation $i_{ug} = j_g$ implies that the values of j_g are completely determined by i_g for $g \in \mathbb{Z}_n$ since u is a unit.

Simplification (2): We can show that, in fact, $r, s \in U_n$.

Why are $r, s \in U_n$?

If $r \notin U_n$ then for some $m < n$ we have $mr \equiv 0(\ mod \ n)$.

From the relation $i_{(r+e)v} - i_e = 1$ we have

$$\begin{aligned} i_{rv} - i_0 &= 1 \ [e = 0] \\ i_{2rv} - i_{rv} &= 1 \ [e = r] \\ i_{3rv} - i_{2rv} &= 1 \ [e = 2r] \\ &\vdots \\ i_{mrv} - i_{(m-1)rv} &= 1 \ [e = (m-1)r] \end{aligned}$$

Looking at the left and right hand sides, we see that the indices $\{0, rv, \ldots, (m-1)rv\}$ and $\{0, r, \ldots, (m-1)r\}$ are equal since $v \in U_n$.

As such, if we add these m equations we get

$$0 = (\sum_{e=0}^{m-1} i_{erv}) - (\sum_{f=0}^{m-1} i_{fr}) = m$$

in $\mathbb{Z}_n$ which is impossible since $m < n$.

So we conlude that in fact $r \in U_n$ and similarly $s \in U_n$ as well.

The next task is to determine $v \in U_n$, which (at the very least) must satisfy the equation $v^n = 1$.

From $i_{(r+e)v} - i_e = 1$, $i_0 = 0$, $i_{rv} = 1$ we obtain

$$
\begin{aligned}
i_{rv+rv^2} - i_{rv} &= 1 \text{ [i.e. } i_{rv+rv^2} = 2] \\
i_{rv+rv^2+rv^3} - i_{rv+rv^2} &= 1 \text{ [i.e. } i_{rv+rv^2+rv^3} = 3] \\
&\vdots \\
i_{rv+rv^2+\cdots+rv^e} &= e
\end{aligned}
$$

We can now use this relation as follows:

$$rv = u(sv + \cdots + sv^{n-1}) \text{ i.e. } [e = 1]$$
$$rv + rv^2 = u(sv + \cdots + sv^{n-2}) \text{ i.e. } [e = 2]$$

which implies $r = -usv^{n-3}$, and for $e = 3$ we have

$$rv + rv^2 + rv^3 = u(sv + \cdots + sv^{n-3})$$

which paired with the $e = 2$ case yields $r = -usv^{n-5}$ which ultimately implies $v^2 = 1$.

Now, if n is odd then $v^n = 1$ together with $v^2 = 1$ immediately implies that $v = 1$.

If n is even then we can use the $v^2 = 1$ relation as follows.

If in $i_{rv+rv^2+\cdots+rv^e} = e$ we look at the index $rv + rv^2 + \cdots + rv^e$ we have

$$rv + rv^2 + \cdots + rv^e = \begin{cases} fr(v+1) & \text{if } e = 2f \\ fr(v+1) + rv & \text{if } e = 2f+1 \end{cases}$$

For the system

$$\begin{aligned} i_0 &= 0 \\ i_{rv} &= 1 \text{ for some } r \\ i_{(r+e)v} - i_e &= 1 \text{ for each } e \in \mathbb{Z}_n \end{aligned}$$

the solutions we seek are those for which all i_g are distinct.

As we just saw $i_{rv+rv^2+\cdots+rv^e} = e$ for each $e \in \mathbb{Z}_n$ which can be simplified to

$$\begin{aligned} i_{fr(v+1)} &= 2f \qquad \text{if } e = 2f \\ i_{fr(v+1)+rv} &= 2f + 1 \text{ if } e = 2f + 1 \end{aligned}$$

for $f \in \{0, \ldots, \frac{n}{2} - 1\}$.

So in order that each i_g is distinct we consider whether

$$f_1 r(v+1) = f_2 r(v+1)$$
$$f_1 r(v+1) + rv = f_2 r(v+1) + rv$$

which is equivalent to $fr(v+1) = 0$.

Since r is a unit then this is equivalent to $f(v+1) = 0 \pmod{n}$.

In $\mathbb{Z}_n$ one has $|v+1| = \frac{n}{gcd(v+1,n)}$ which means $|v+1| = n/2$ if and only if $gcd(v+1,n) = 2$ and therefore that $fr(v+1) = 0$ only when $f = 0$.

We note a technical fact:

Lemma

Let n be even and $v \in \Upsilon_n$:

(a) if $8 \nmid n$ then $gcd(v+1, n) = 2$ only if $v = 1$
(b) if $8|n$ then $gcd(v+1, n) = 2$ only if $v = 1, \frac{n}{2}+1$

So $\mu_n = 2$ if $8|n$ or $\mu_n = 1$ if $8 \nmid n$.

So for the solutions of

$$
\begin{aligned}
i_0 &= 0 \\
i_{rv} &= 1 \text{ for some } r \in U_n \\
j_{sv} &= -1 \text{ for some } s \in U_n \\
i_{(r+e)v} - i_e &= 1 \text{ for each } e \in \mathbb{Z}_n \\
j_{(s+e)v} - j_e &= -1 \text{ for each } e \in \mathbb{Z}_n \\
j_g &= i_{ug} \text{ for each } g \in \mathbb{Z}_n
\end{aligned}
$$

for a given $u \in \Upsilon_n$, and pair $(r, s) \in U_n \times U_n$, we must have $s = -ur$ since $j_g = i_{ug}$. If $8 \nmid n$ then $v = 1$ only, and if $8|n$ $v = 1, \frac{n}{2} + 1$ and so we have overall

$$|\Upsilon_n| \cdot \phi(n) \cdot \mu_n$$

distinct $k_X k_Y$, which yields $|\Upsilon_n| \cdot \mu_n$ distinct $K = \langle k_X k_Y \rangle$, and so that many $N \in R(G, [G])$ where $Norm_B(N) \leq W(X_0, Y_0)$.

This completes the analysis for the case where $Norm_B(N) \leq W(X_0, Y_0)$.

We have shown that if $8 \nmid n$ and N has block structure $\{X_0, Y_0\}$ then $N \in \mathcal{H}(G)$.

Note, this corresponds to $v = 1$ only, and for $8|n$ the $v = \frac{n}{2} + 1$ possibility yields the other $|\Upsilon_n|$ different $N \in R(G, [G])$ which do *not* lie in $\mathcal{H}(G)$.

For n even, the situation is a bit more complicated, but can be understood in terms of the other block structures $\{X_1, Y_1\}$ and $\{X_2, Y_2\}$.

If n is even then a given $N \in R(G, [G])$ is such that $Norm_B(N) \leq W(X_i, Y_i)$ for exactly one $i \in \{0, 1, 2\}$.

The case where $Norm_B(N) \leq W(X_0, Y_0)$ has just been covered.

Let's consider $Norm_B(N) \leq W(X_1, Y_1)$ where

$$X_1 = \{1, x^2, \ldots, x^{n-2}, t, tx^2, \ldots, tx^{n-2}\}$$
$$Y_1 = \{x, x^3, \ldots, x^{n-1}, tx, tx^3, \ldots, tx^{n-1}\}$$

which means N's characteristic two subgroup K is of the form $\langle k_x k_Y \rangle$ where $Supp(k_x) = X_1$ and $Supp(k_Y) = Y_1$.

As such we have

$$k_X = (t^{a_0}x^{b_0}, t^{a_1}x^{b_1}, \ldots, t^{a_{n-1}}x^{b_{n-1}})$$
$$k_Y = (t^{c_0}x^{d_0}, t^{c_1}x^{d_1}, \ldots, t^{c_{n-1}}x^{d_{n-1}})$$

where $a_e, c_e \in \{0, 1\}$ and $b_e \in \{0, 2, \ldots, n-2\}$ and $d_e \in \{1, 3, \ldots, n-1\}$.

Moreover, each even number b_e appears twice, and each odd number d_e appears twice, and similarly, half of the a_e are 0 and half are 1 and similarly for c_e.

Now, for

$$k_X = (t^{a_0}x^{b_0}, t^{a_1}x^{b_1}, \ldots, t^{a_{n-1}}x^{b_{n-1}})$$
$$k_Y = (t^{c_0}x^{d_0}, t^{c_1}x^{d_1}, \ldots, t^{c_{n-1}}x^{d_{n-1}})$$

we can assume that $(a_0, b_0) = (0, 0)$ and $(c_0, d_0) = (0, 1)$.

Moreover, we will assume that $(a_r, b_r) = (1, 0)$ and $(c_s, d_s) = (1, 1)$ for some r, s since $1, t \in Supp(k_x)$ and $x, tx \in Supp(k_Y)$.

The idea then will be to again determine equations amongst the a_e, b_e, c_e, d_e whose solutions govern the potential generators of any such $K \leq N$ characteristic (of index 2) for $N \in R(G, [G])$.

We have that $\lambda(x)$ and $\lambda(t)$ must normalize K since K is characteristic in N.

Since

$$\lambda(t) = (1, t)(x, tx) \dots (x^{n-1}, tx^{n-1})$$
$$\lambda(x) = (1, x, \dots, x^{n-1})(t, tx^{n-1}, \dots, tx)$$

we have that $\lambda(t)(X_1) = X_1$ and $\lambda(t)(Y_1) = Y_1$ while $\lambda(x)(X_1) = Y_1$ and $\lambda(x)(Y_1) = X_1$ and so

$$\lambda(t) k_X \lambda(t) = k_X^u$$
$$\lambda(t) k_Y \lambda(t) = k_Y^u \text{ for some } u \in \Upsilon_n$$

$$\lambda(x) k_X \lambda(x)^{-1} = k_Y^v$$
$$\lambda(x) k_Y \lambda(x)^{-1} = k_X^v \text{ for some } v \in U_n \text{ where } v^n = 1$$

As such, conjugation by $\lambda(t)$ yields

$$(t^{a_0+1}x^{b_0}, t^{a_1+1}x^{b_1}, \ldots, t^{a_{n-1}+1}x^{b_{n-1}}) = (t^{a_0}x^{b_0}, t^{a_u}x^{b_u}, \ldots, t^{a_{(n-1)u}}x^{b_{(n-1)u}})$$
$$(t^{c_0+1}x^{d_0}, t^{c_1+1}x^{d_1}, \ldots, t^{c_{n-1}+1}x^{d_{n-1}}) = (t^{c_0}x^{d_0}, t^{d_u}x^{d_u}, \ldots, t^{c_{(n-1)u}}x^{d_{(n-1)u}})$$

And since $(a_0, b_0) = (0, 0)$ then $(a_0 + 1, b_0) = (1, 0) = (a_r, b_r)$ and $(c_0 + 1, d_0) = (c_s, d_s)$ which implies that

$$(t^{a_0+1}x^{b_0}, t^{a_1+1}x^{b_1}, \ldots, t^{a_{n-1}+1}x^{b_{n-1}}) = (t^{a_r}x^{b_r}, t^{a_{r+u}}x^{b_{r+u}}, \ldots, t^{a_{r+(n-1)u}}x^{b_{r+(n-1)u}})$$
$$(t^{c_0+1}x^{d_0}, t^{c_1+1}x^{d_1}, \ldots, t^{c_{n-1}+1}x^{d_{n-1}}) = (t^{c_s}x^{d_s}, t^{d_{s+u}}x^{d_{s+u}}, \ldots, t^{c_{s+(n-1)u}}x^{d_{s+(n-1)u}})$$

and so

$$\begin{aligned} b_e &= b_{r+eu} \\ d_e &= d_{s+eu} \\ a_e + 1 &= a_{r+eu} \\ c_e + 1 &= c_{s+eu} \end{aligned}$$

for each $e \in \mathbb{Z}_n$.

Similarly, conjugation by $\lambda(x)$ yields

$$(t^{a_0}x^{b_0+(-1)^{a_0}}, t^{a_1}x^{b_1+(-1)^{a_1}}, \ldots, t^{a_{n-1}}x^{b_{n-1}+(-1)^{a_{n-1}}}) = (t^{c_0}x^{d_0}, t^{c_v}x^{d_v}, \ldots, t^{c_{(n-1)v}}x^{d_{(n-1)v}})$$
$$(t^{c_0}x^{d_0+(-1)^{c_0}}, t^{c_1}x^{d_1+(-1)^{c_1}}, \ldots, t^{c_{n-1}}x^{d_{n-1}+(-1)^{c_{n-1}}}) = (t^{a_0}x^{b_0}, t^{a_v}x^{b_v}, \ldots, t^{a_{(n-1)v}}x^{b_{(n-1)v}})$$

Here, $(a_0, b_0) = (0, 0)$ yields $(a_0, b_0 + (-1)^{a_0}) = (0, 1) = (c_0, d_0)$ so the first equation directly yields that

$$c_{ev} = a_e$$
$$d_{ev} = b_e + (-1)^{a_e}$$

for each $e \in \mathbb{Z}_n$.

And since $(c_s, d_s) = (1, 1)$ then $(c_s, d_s + (-1)^{c_s}) = (1, 0) = (a_r, b_r)$ which means that

$$
\begin{aligned}
(t^{c_0}x^{d_0+(-1)^{c_0}}, t^{c_1}x^{d_1+(-1)^{c_1}}, \ldots, t^{c_{n-1}}x^{d_{n-1}+(-1)^{c_{n-1}}}) &= (t^{a_0}x^{b_0}, t^{a_1}x^{b_1}, \ldots, t^{a_{(n-1)}}x^{b_{(n-1)}})^v \\
&= (t^{a_r}x^{b_r}, t^{a_{r+1}}x^{b_{r+1}}, \ldots, t^{a_{r+(n-1)}}x^{b_{r+(n-1)}})^v \\
&\downarrow \\
(t^{c_s}x^{d_s+(-1)^{c_s}}, t^{c_{s+1}}x^{d_{s+1}+(-1)^{c_{s+1}}}, \ldots, t^{c_{s+n-1}}x^{d_{s+n-1}+(-1)^{c_{s+n-1}}}) &= \\
&(t^{a_r}x^{b_r}, t^{a_{r+v}}x^{b_{r+v}}, \ldots, t^{a_{r+(n-1)v}}x^{b_{r+(n-1)v}})
\end{aligned}
$$

which yields

$$
\begin{aligned}
c_{s+e} &= a_{r+ev} \\
d_{s+e} + (-1)^{c_{s+e}} &= b_{r+ev}
\end{aligned}
$$

So a given

$$
\begin{aligned}
K &= \langle k_x k_Y \rangle \\
&= \langle (t^{a_0}x^{b_0}, t^{a_1}x^{b_1}, \ldots, t^{a_{n-1}}x^{b_{n-1}})(t^{c_0}x^{d_0}, t^{c_1}x^{d_1}, \ldots, t^{c_{n-1}}x^{d_{n-1}}) \rangle
\end{aligned}
$$

being normalized by $\lambda(G)$ implies that the following system of equations must be satisfied for each $e \in \mathbb{Z}_n$

$$
\begin{aligned}
a_e + 1 &= a_{r+eu} & b_e &= b_{r+eu} \\
c_e + 1 &= c_{s+eu} & d_e &= d_{s+eu} \\
c_{ev} &= a_e & d_{ev} &= b_e + (-1)^{a_e} \\
c_{s+e} &= a_{r+ev} & b_{r+ev} &= d_{s+e} + (-1)^{c_{s+e}}
\end{aligned}
$$

where $a_e, c_e \in \mathbb{Z}_2$, $b_e \in \{0, 2, \ldots, n-2\}$, $d_e \in \{1, 3, \ldots, n-1\}$ and

$$
\begin{aligned}
(a_o, b_0) &= (0, 0) \\
(a_r, b_r) &= (1, 0) \\
(c_0, d_0) &= (0, 1) \\
(c_s, d_s) &= (1, 1)
\end{aligned}
$$

Two immediate consequences:

Since $b_e = b_{r+eu}$ then we must have $b_{r+eu} = b_{r+(r+eu)u} = b_e$ since the b's must consist of *two* copies of every even integer between 0 and $n-2$.

As such (since $u^2 = 1$) we have $r(u+1) = 0$, and similarly $d_e = d_{s+eu}$ implies that $s(u+1) = 0$.

Additionally, the equations $a_e + 1 = a_{r+eu}$ and $c_e + 1 = c_{s+eu}$ imply that $r + eu \neq e$ and $s + eu \neq e$ which means that $r \notin \langle 1-u \rangle$ and $s \notin \langle 1-u \rangle$.

It turns out that, in fact, $u = -1$ so that $r(u+1) = 0$ and $s(u+1) = 0$ automatically and $r \notin \langle 1-u \rangle = \langle 2 \rangle$ and $s \notin \langle 1-u \rangle = \langle 2 \rangle$.

Furthermore, we must have that, in fact, $v^2 = 1$. (i.e. $v \in \Upsilon_n$)

And while r, s need not be units, they must satisfy $(s - rv)/2 \in U_{n/2}$ which yields δ_n possible $k_X k_Y$ where

$$\begin{aligned}
\delta_n &= |\{(v, r, s) \in \Upsilon_n \times \mathbb{Z}_n \times \mathbb{Z}_n \mid ((s - rv)/2) \in U_{n/2} \text{ and } s, r \notin \langle 2 \rangle\}| \\
&= \frac{n}{2} \cdot |\Upsilon_n| \cdot \phi(\frac{n}{2}) \\
&= \begin{cases} \frac{n}{2} \cdot |\Upsilon_n| \cdot \phi(n) & 4 \nmid n \\ \frac{n}{2} \cdot |\Upsilon_n| \cdot \frac{\phi(n)}{2} & 4|n \end{cases}
\end{aligned}$$

and so $\frac{\delta_n}{\phi(n)}$ possible K which therefore enumerates the $N \in R(G, [G])$ where $Norm_B(N) \leq W(X_1, Y_1)$.

For those $N \in R(G,[G])$ where $Norm_B(N) \leq W(X_2, Y_2)$ we can utilize the following:

Lemma

The automorphism $\phi_{(1,1)} \in Aut(D_n)$, where $\phi(x^b) = x^b$ and $\phi(tx^b) = tx^{b+1}$ has the property that $\phi(X_1) = X_2$, $\phi(X_2) = X_1$ and that $\phi(Y_1) = Y_2$ and $\phi(Y_2) = Y_1$, and also $\phi(X_0) = Y_0$ and $\phi(Y_0) = X_0$.

And since $\phi_{(1,1)} W(X_i, Y_i) \phi_{(1,1)}^{-1} = W(\phi_{(1,1)}(X_i), \phi_{(1,1)}(Y_i))$ and for a given $N \in R(G,[G])$ one has that $Norm_B(N)$ is contained in $W(X_i, Y_i)$ for exactly one $\{X_i, Y_i\}$ we have the following:

Theorem

If $R(G,[G];\{X_i,Y_i\})$ *is the set of those* $N \in R(G,[G])$ *such that* $Norm_B(N) \leq W(X_i,Y_i)$ *then* $|R(G,[G];\{X_1,Y_1\})| = |R(G,[G];\{X_2,Y_2\})|$.

In summary

$$|R(D_n,[D_n])| = \begin{cases} (\frac{n}{2}+2)|\Upsilon_n| & \text{if } 8|n \\ (\frac{n}{2}+1)|\Upsilon_n| & \text{if } 4|n \text{ but } 8 \nmid n \\ (n+1)|\Upsilon_n| & \text{if } 2|n \text{ but } 4 \nmid n \\ |\Upsilon_n| & \text{if } n \text{ odd} \end{cases}$$

Thank you!

T. Kohl.
Multiple holomorphs of dihedral and quaternionic groups.
Comm. Alg., 43:4290–4304, 2015.