Multiple Holomorphs and Isomorphism Classes Of Hopf-Galois Structures on Dihedral Extensions

Timothy Kohl

Boston University

May 30, 2019

This is joint work with

Robert Underwood - Auburn University Montgomery

Hopf-Galois Theory

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

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

As is known, the Hopf-Galois structures on a Galois extension L/K with $G = Gal(L/K)$ are in 1-1 correspondence with the regular subgroups $N \leq B = Perm(G)$ such that $\lambda(G) \leq Norm_B(N)$, where the Hopf algebra which acts is $H_N = (L[N])^{\lambda(G)}$ the fixed ring under the simultaneous action of G on scalars and on N.

This implies that $|N| = |G|$ but does not necessarily force N to be isomorphic to G, and indeed we may define

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

where $[M]$ represents any group of cardinality $|G|$.

Here however, we will, in fact, consider $R(G, [G])$ as this includes some primordial examples of the N which may arise.

For all G, we have $N = \rho(G) \in R(G, [G])$ since $\lambda(G)$ centralizes $\rho(G)$ and thus certainly normalizes it, where $H_{\rho(G)} \cong K[G]$ the group ring, i.e. the canonical action by virtue of G being the Galois group of L/K.

If G is non-abelian then $\lambda(G) \neq \rho(G)$ and since $\lambda(G)$ obviously normalizes itself we have $\lambda(G) \in R(G, [G])$ where $H_{\lambda(G)} = H_\lambda$ is the so-called *canonical non-classical* structure.

The relationship we focus on, as exemplified by $\lambda(G)$ and $\rho(G)$, is that

$$Norm_B(\rho(G)) = Norm_B(\lambda(G)) = Hol(G)$$

which leads to the discussion of the *multiple holomorph* of G.

For $\lambda(G) \leq B = Perm(G)$, one can ask for what other regular subgroups $N \leq B$ have the same normalizer, (holomorph) as G , namely $Hol(N) = Hol(G)$.

The equality implies that $N \leq Hol(G)$ and $\lambda(G) \leq Hol(N)$.

If we restrict our attention to those N which are isomorphic to G then N is a conjugate of $\lambda(G)$ by regularity.

So for such an N, where $\tau \in B$ is such that $\tau\lambda(G)\tau^{-1} = N$ then

$$\begin{aligned}
\tau Norm_B(\lambda(G))\tau^{-1} &= Norm_B(\tau\lambda(G)\tau^{-1}) \\
&= Norm_B(N) \\
&= Norm_B(\lambda(G))
\end{aligned}$$

which means $\tau \in Norm_B(Hol(G))$, and the converse is true as well.

Let us make a few definitions:

$$NHol(G) = Norm_B(Hol(G)) = Norm_B(Norm_B(\lambda(G)))$$

the multiple holomorph of G

$$T(G) = NHol(G)/Hol(G)$$

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

We observe that $\mathcal{H}(G) \subseteq R(G, [G])$, and the virtue of this is that $\mathcal{H}(G)$ (for many different G) may be readily enumerated.

We have the following basic fact(s) about $T(G)$ and $\mathcal{H}(G)$.

Proposition

Given the above definitions:

$$\begin{aligned} Orb_{T(G)}(\lambda(G)) &= \mathcal{H}(G) \\ &= \{N \text{ regular} \mid N \cong G \text{ and } N \lhd Hol(G)\} \\ &= Orb_{T(G)}(N) \text{ for any } N \in \mathcal{H}(G) \end{aligned}$$

and in particular $|T(G)| = |\mathcal{H}(G)|$.

The multiple holomorph of finite abelian groups was determined by G.A. Miller [4] in the early 1900's and what was utlimately discovered was that $|T(G)|$ is trivial if G has odd order, and $|T(G)| \leq 4$ in general.

Indeed, for many groups $|T(G)| = 2$, i.e. $\mathcal{H}(G) = \{\lambda(G), \rho(G)\}$, for example, if G is a non-abelian simple group, or complete.

Since then $T(G)$ has been computed for other classes of groups, by Caranti for perfect groups [1], and p-groups of class two [2], and the presenter [3] for the case of dihedral groups.

And indeed, for our discussion, we shall focus on the case where $G \cong D_n$.

We examine the case where $G \cong D_n$ for $n \geq 3$ since both $\mathcal{H}(G)$ and $T(G)$ are worked out in detail in [3].

We present the n-th dihedral group as follows:

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

and we also have a presentation of $Aut(D_n)$.

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

$$\phi_{i,j}(t^a x^b) = t^a x^{ia+jb}$$
$$\phi_{i_2,j_2} \circ \phi_{i_1,j_1} = \phi_{i_2+j_2 i_1, j_2 j_1}$$
$$\phi_{(0,1)} = I \quad \text{the identity}$$

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

The groups in $\mathcal{H}(D_n)$ are subgroups of $Hol(D_n)$ where typical elements have the form

$$(t^a x^b, \phi_{i,j})$$

and if we make the identification $\rho(t^i x^j) = (t^i x^j, I) \in Hol(D_n)$ then since $\lambda(D_n)$ is the centralizer of $\rho(D_n)$ we have

$$\lambda(t^i x^j) = (t, \phi_{(0,-1)})^i (x, \phi_{(2,1)})^j$$

.

The description of $\mathcal{H}(D_n)$ is given in [3, Theorem 2.11]

Theorem

$$\mathcal{H}(D_n) = \{\langle (x, \phi_{(u+1,1)}), (t, \phi_{(0,-u)}) \rangle \mid u \in \Upsilon_n\}$$

where

$$\Upsilon_n = \{u \in U_n \mid u^2 = 1\}$$

the group of exponent 2 units mod n.

The size and structure of the group Υ_n is basically determined by the number of quadratic residues of n, which in turn is keyed to the number of prime divisors of n vis-a-vis the Chinese Remainder Theorem, and is given below.

Lemma

For $n = 2^e p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$, $\Upsilon_n \cong \begin{cases} (\mathbb{Z}_2)^r & e <= 1 \\ (\mathbb{Z}_2)^{r+1} & e = 2 \\ (\mathbb{Z}_2)^{r+2} & e \geq 3 \end{cases}$

For $u \in \Upsilon_n$ let

$$\begin{aligned} N_u &= \langle (x, \phi_{(u+1,1)}), (t, \phi_{(0,-u)}) \rangle \\ &= \langle x_u, t_u \rangle \end{aligned}$$

and we note that $N_{-1} = \rho(D_n)$ and $N_1 = \lambda(D_n)$.

More generally, by [3, Corollary 1.13] we have, for any $N_u \in \mathcal{H}(D_n)$, that $N_u^{opp} = Cent_B(N_u) = N_{-u}$.

As we wish to consider the fixed rings $H_N = (L[N])^G$ where the G acting on N is $\lambda(G)$ of course, we have the following, which also comes from [3]. If we let $r = x_1 = \lambda(x)$ and $f = t_1 = \lambda(t)$ then

Proposition

$\lambda(D_n) = \langle r, f \rangle$ acts on $N_u = \langle x_u, t_u \rangle$ as follows:

$$
\begin{aligned}
r x_u r^{-1} &= x_u \\
r t_u r^{-1} &= t_u x_u^{-(u+1)} \\
f x_u f^{-1} &= x_u^{-u} \\
f t_u f^{-1} &= t_u
\end{aligned}
$$

With this we can establish the following.

Theorem

For each $N_u \in \mathcal{H}(D_n)$, none of the $H_{N_u} = (L[N_u])^{D_n}$ are isomorphic as Hopf algebras.

Proof.

Let $u, v \in \Upsilon_n$ with $N_u = \langle x_u, t_u \rangle$ and $N_v = \langle x_v, t_v \rangle$.

If there were a $\lambda(D_n)$-invariant isomorphism $\psi : N_u \to N_v$ then $\psi(x_u) = x_v^w$ for some unit w.

But for ψ to be $\lambda(D_n)$-invariant, then looking at how $f = t_1$ acts one would need that $-uw \equiv -vw \ (mod\ n)$ which is impossible since $u \neq v$. $\square$

[Note: We utilize the fact that $H_N \cong H_{N'}$ as Hopf-algebras iff there is a $\lambda(G)$-invariant isomorphism from N to N'.]

Our next question is, what about the potential isomorphisms that may exist between the H_{N_u} as K-algebras?

For this, we begin by constructing a basis for H_{N_u} which will allow us to analyze the basic structure of them as rings.

For $u \in \Upsilon_n$ let

$$\begin{aligned} N_u &= \langle (x, \phi_{(u+1,1)}), (t, \phi_{(0,-u)}) \rangle \\ &= \langle x_u, t_u \rangle \end{aligned}$$

and we note that $N_{-1} = \rho(D_n)$ and $N_1 = \lambda(D_n)$.

More generally, by [3, Corollary 1.13] we have, for any $N_u \in \mathcal{H}(D_n)$, that $N_u^{opp} = Cent_B(N_u) = N_{-u}$.

As to the case where n is even. We can utilize the enumeration discussed earlier this week.

Those N where $Norm_B(N) \leq W(X_0, Y_0)$, can be parameterized as $N_{u,v}$ where $u \in \Upsilon_n$ and $v = 1$, and, if $8|n$ also for $v = \frac{n}{2} + 1$ where $N_{u,1} = N_u \in \mathcal{H}(D_n)$.

For our purposes, the we can focus on how $\lambda(D_n)$ acts on the characteristic index 2 subgroup which we can denote $K_{u,v} = \langle k_{u,v} \rangle$.

For $r = \lambda(x)$ and $f = \lambda(t)$ we have

Proposition

$\lambda(D_n) = \langle r, f \rangle$ acts on $K_{u,v} = \langle k_{u,v} \rangle$ as follows:

$$r k_{u,v} r^{-1} = k_{u,v}^{v}$$
$$f k_{u,v} f^{-1} = k_{u,v}^{u}$$

With this in mind, we can establish the following:

Theorem

If n even, and $Norm_B(N) \leq W(X_0, Y_0)$ where $N = N_{u,v}$ for $u \in \Upsilon_n$ and $v = 1$ or $v = \frac{n}{2} + 1$ one has that there is no $\lambda(D_n)$ invariant isomorphism $\psi : N_{u_1,v_1} \to N_{u_2,v_2}$ unless $u_1 = u_2$ and $v_1 = v_2$.

Proof.

If $K_{u_i,v_i} = \langle k_{u_i,v_i} \rangle$ are the index 2 characteristic subgroups then any such $\psi : N_{u_1,v_1} \to N_{u_2,v_2}$ must map $k_{u_1,v_2} \mapsto k^w_{u_2,v_2}$ for some $w \in U_n$. However, by virtue of how $\lambda(D_n)$ acts, this would require

$$v_1 w \equiv v_2 w$$

$$u_1 w \equiv u_2 w$$

which, since $w \in U_n$ implies $u_1 = u_2$ and $v_1 = v_2$. $\square$

Corollary

For n even, and N such that $Norm_B(N) \leq W(X_0, Y_0)$ *no two of the resulting fixed rings* $(L[N])^{D_n}$ *are isomorphic as Hopf-algebrs.*

For those N where $Norm_B(N) \leq W(X_1, Y_1)$, we have that $N = N_{v,r}$ where $v \in \Upsilon_n$ and $r \in \mathbb{Z}_n - \langle 2 \rangle$.

Again we can focus on how $\lambda(D_n)$ acts on the characteristic index 2 subgroup which we can denote $K_{v,r} = \langle k_{v,r} \rangle$, specifically
For $r = \lambda(x)$ and $f = \lambda(t)$ we have

Proposition

$\lambda(D_n) = \langle r, f \rangle$ acts on $K_{v,r} = \langle k_{v,r} \rangle$ as follows:

$$r k_{v,r} r^{-1} = k_{v,r}^{v}$$
$$f k_{v,r} f^{-1} = k_{v,r}^{-1}$$

And in a similar fashion to the previous example, we can conclude that

Theorem

For $N_{v,r}$ as above, if $v_1 \neq v_2$ then N_{v_1,r_1} is not $\lambda(D_n)$-isomorphic to N_{v_2,r_2} and therefore the resulting fixed rings are not isomorphic as Hopf algebras.

For later reference, we can determine $N_u \cap \rho(D_n)$ as this determines $G(H_{N_u})$.

Proposition

For $N_u = \langle x_u, t_u \rangle \in \mathcal{H}(D_n)$ we have

$$N_u \cap \rho(D_n) = \langle x_u^{\frac{n}{gcd(u+1,n)}} \rangle$$

which equals $\langle x_{-1}^{\frac{n}{gcd(u+1,n)}} \rangle$ a cyclic group of order $gcd(u+1, n)$.

Notation: *As we will use it throughout the subsequent discussion we set $d_u = gcd(u+1, n)$ for $u \in \Upsilon_n$, and also define $m_u = \frac{n}{d_u}$.*

Basis for H_{N_u}

For a given regular N normalized by $\lambda(G)$, a basis for $H_N = (L[N])^G$ can be given that is universal in that it is defined for any L/K and N.

Proposition

Let $\alpha \in L$ be a normal basis generator for L/K with the property that $tr(\alpha) = 1$. Let N be a regular subgroup of $B = Perm(G)$ which is normalized by $\lambda(G)$. If for each $n \in N$ we define

$$v_n = \sum_{g \in G} g(\alpha)\lambda(g)n\lambda(g)^{-1}$$

then the set $\{v_n\}$ is a basis for $H_N = (L[N])^G$.

Proof:

We begin by verifying that each v_n lies in H.

Let $t \in G$ and observe

$$\begin{aligned} t(v_n) &= \sum_{g \in G} t(g(\alpha))\lambda(t)\lambda(g)n\lambda(g)^{-1}\lambda(t)^{-1} \\ &= \sum_{g \in G} (tg)(\alpha)\lambda(tg)n\lambda(tg)^{-1} \\ &= v_n \end{aligned}$$

so that $v_n \in H$.

Note that $v_{e_N} = e_N$ where e_N is the identity of N.

As there are $|N| = |G| = dim_k(H)$ different v_n we prove that they are a basis for H by proving linear independence. For computational convenience let

$$\pi^{-1}(m) = \{(g, n) \in G \times N \mid \lambda(g)n\lambda(g)^{-1} = m\}$$

and suppose now that $\sum_{n\in N} c_n v_n = 0$ for $c_n \in k$, that is

$$\begin{aligned} 0 &= \sum_{n\in N}\sum_{g\in G} c_n g(\alpha)\lambda(g)n\lambda(g)^{-1} \\ &= \sum_{m\in N}\left(\sum_{(g,n)\in\pi^{-1}(m)} c_n g(\alpha)\right) m \end{aligned}$$

which means that for each $m \in N$ we have

$$\sum_{(g,n)\in\pi^{-1}(m)} c_n g(\alpha) = 0 \tag{1}$$

but does this imply that each c_n in this sum is zero?

Since $\lambda(G)$ normalizes N then each $\lambda(g)$ acts as an automorphism of N.

As such, if $(g, n_1), (g, n_2) \in \pi^{-1}(m)$ then one must have $n_1 = n_2$ and therefore, for all the $(g, n) \in \pi^{-1}(m)$, the g's are all distinct.

As such the left hand side of (1) is a linear combination of *distinct* $g(\alpha)$ which means that for each $(g, n) \in \pi^{-1}(m)$ one has $c_n = 0$.

And since this holds true for all $m \in N$ then all $c_n = 0$.

$\square$

We have complete information on how $\lambda(D_n) = N_1$ conjugates elements of N_u and thus may start constructing the v_n bases for each $n = t_u^i x_u^j \in N_u$.

We define $F = L^{\langle r \rangle}$ and for α a normal basis generator of L/K, we define $\beta = tr_{L/F}(\alpha) = \sum_{b=0}^{n-1} r^b(\alpha)$.

We also observe that $1 = tr_{L/K}(\alpha) = tr_{F/K}(tr_{L/F}(\alpha)) = \beta + f(\beta)$ which we will use below.

Notation: As we will use it throughout the subsequent discussion we set $d_u = gcd(u+1, n)$ for $u \in \Upsilon_n$, and also define $m_u = \frac{n}{d_u}$.

For $x_u^j \in N_u$ we have

$$\begin{aligned} v_{x_u^j} &= \sum_{a=0}^{1} \sum_{b=0}^{n-1} (f^a r^b(\alpha))(f^a r^b) x_u^j (f^a r^b)^{-1} \\ &= \sum_{b=0}^{n-1} (r^b(\alpha)) x_u^j + (fr^b(\alpha)) x_u^{-uj} \\ &= tr_{L/F}(\alpha) x_u^j + f(tr_{L/F}(\alpha)) x_u^{-uj} \\ &= \beta x_u^j + f(\beta) x_u^{-uj} \\ &= \beta x_u^j + (1-\beta) x_u^{-uj} \end{aligned}$$

and we observe that, $v_{x_u^j} = x_u^j$ if and only if $j = -uj$ which is equivalent to $j(u+1) \equiv 0 \ (mod \ \ n)$, namely $j \in \langle m_u \rangle$. i.e. $N_u \cap \rho(D_n)$.

For $t_u x_u^j \in N_u$ we have

$$\begin{aligned}
v_{t_u x_u^j} &= \sum_{a=0}^{1} \sum_{b=0}^{n-1} (f^a r^b(\alpha))(f^a r^b) t_u x_u^j (f^a r^b)^{-1} \\
&= \sum_{b=0}^{n-1} r^b(\alpha) r^b(t_u x_u^j) r^{-b} + (fr^b(\alpha))(fr^b) t_u x_u^j (fr^b)^{-1} \\
&= \sum_{b=0}^{n-1} r^b(\alpha) t_u x_u^{j-b(u+1)} + fr^b(\alpha) t_u x_u^{b(u+1)-uj}
\end{aligned}$$

Looking at the coefficients and group element exponents in the above sum, we see the appearance of $j - b(u+1)$ and $b(u+1) - uj$ as b varies over $\mathbb{Z}_n$.

Proposition

For $m_u = \frac{n}{d_u}$ as defined earlier, if $b \equiv b' \pmod{m_u}$ then $j - b(u+1) \equiv j - b'(u+1) \pmod{n}$, and $b(u+1) - uj \equiv b'(u+1) - uj \pmod{n}$.

As such, if we define $W_e = \{t \in \mathbb{Z}_n \mid t \equiv e \pmod{m_u}\}$ for $e = 0..m_u - 1$ then $\mathbb{Z}_n = W_0 \cup W_1 \cdots \cup W_{m_u - 1}$, where, in fact, $W_0 = \langle m_u \rangle$ and $W_e = W_0 + e$.

For $\langle r^{m_u} \rangle \leq Gal(L/K)$ and $F_{d_u} = L^{\langle r^{m_u} \rangle}$ let $\gamma = tr_{L/F_{d_u}}(\alpha) = \sum_{l \in W_0} r^l(\alpha)$.

We have then:

$$
\begin{tikzcd}
\alpha \in L \arrow[d, dash] \arrow[d, bend left=60, "\langle r^{m_u} \rangle"] \arrow[dd, bend right=60, "\langle r \rangle"'] \\
\gamma \in F_{d_u} \arrow[d, dash] \arrow[d, bend left=60, "\langle r \rangle / \langle r^{m_u} \rangle = \{r^0, \dots, r^{m_u-1}\}"] \\
\beta \in F \arrow[d, dash] \arrow[d, bend right=60, "\langle f \rangle"'] \\
K
\end{tikzcd}
$$

and ultimately

$$
\begin{aligned}
v_{t_u x_u^j} &= \sum_{b=0}^{n-1} r^b(\alpha) t_u x_u^{j-b(u+1)} + f r^b(\alpha) t_u x_u^{b(u+1)-uj} \\
&= \sum_{e=0}^{m_u-1} r^e(\gamma) t_u x_u^{j-e(u+1)} + \sum_{e=0}^{m_u-1} f(r^e(\gamma)) t_u x_u^{-uj+e(u+1)}
\end{aligned}
$$

Another worthwhile point to consider is that since $\beta = tr_{L/F}(\alpha)$, then $F = K(\beta)$ and β is actually a normal basis generator of F/K where $f(\beta) = 1 - \beta$.

As such $irr_K(\beta) = x^2 + ax + s$, and since $f(\beta) = 1 - \beta$ then we must have $a = -1$ so that $\beta = \frac{1 \pm \sqrt{1-4s}}{2}$.

Similarly, since $\langle r^{m_u} \rangle$ is characteristic in $\langle r \rangle$ then $\langle r^{m_u} \rangle \triangleleft Gal(L/K)$.

As such, since $\gamma = tr_{L/F_d}(\alpha)$ then γ is a normal basis generator of F_{d_u}/F and $F_{d_u} = F(\gamma)$.

If $n = p$ a prime, then a bit of simplification takes place in that $\Upsilon_p = \{\pm 1\}$ where $u = -1$ still corresponds to the group ring $H_{\rho(D_p)}$ and $u = 1$ corresponds to the canonical non-classical structure $H_{\lambda(D_p)}$.

And in particular, for $u = 1$ we have $d_1 = gcd(2, p) = 1$ and $m_1 = p/1 = p$ so that $F_{d_1} = L$, i.e. $\gamma = \alpha$ and

$$
\begin{aligned}
v_{x_1^j} &= \beta x_1^j + (1-\beta) x_1^{-j} \\
v_{t_1 x_1^j} &= \sum_{e=0}^{p-1} r^e(\alpha) t_1 x_1^{j-2e} + \sum_{e=0}^{p-1} f(r^e(\alpha)) t_1 x_1^{2e-j}
\end{aligned}
$$

Multiplying Basis Vectors of H_{N_u}

Let us consider how these basis elements multiply with each other. For example

$$\begin{aligned} v_{x_u^j} \cdot v_{x_u^k} &= (\beta x_u^j + (1-\beta)x_u^{-uj})(\beta x_u^k + (1-\beta)x_u^{-uk}) \\ &= \beta^2 x_u^{j+k} + \beta(1-\beta)x_u^{j-uk} + \beta(1-\beta)x_u^{k-uj} + (1-\beta)^2 x_u^{-u(j+k)} \end{aligned}$$

which we can write as a linear combination of the other basis elements, specifically

$$v_{x_u^j} \cdot v_{x_u^k} = (1-s)v_{x_u^{j+k}} - s v_{x_u^{-u(j+k)}} + s v_{x_u^{j-uk}} + s v_{x_u^{k-uj}}$$

an immediate consequence of which is that $v_{x_u^j}$, and $v_{x_u^k}$ commute with each other, which isn't terribly surprising of course.

A subtle point to observe is that some of the 'n' in the v_n above may be duplicates.

For example, if $u = -1$ then

$$\begin{aligned} v_{x_u^j} \cdot v_{x_u^k} &= (1-s)v_{x_u^{j+k}} - sv_{x_u^{-u(j+k)}} + sv_{x_u^{j-uk}} + sv_{x_u^{k-uj}} \\ &= (1-s)v_{x_u^{j+k}} - sv_{x_u^{(j+k)}} + sv_{x_u^{j+k}} + sv_{x_u^{k+j}} \\ &= v_{x_u^{j+k}} \end{aligned}$$

which is basically reflecting the fact that $v_{x_{-1}^j} = x_{-1}^j$ and so $x_{-1}^j x_{-1}^k = x_{-1}^{j+k}$ of course.

More generally, $v_n = n$ if and only if $n \in N \cap \rho(G)$.

In particular, we recall that $v_{x_u^j} = \beta x_u^j + (1-\beta) x_u^{-uj} = x_u^j$ if and only if $j \equiv -uj \ (mod \ n)$ which is equivalent to $j \equiv 0 \ (mod \ m_u)$.

And applied to $\{j+k, -u(j+k), j-uk, k-uj\}$ we have

$$
\begin{gathered}
j+k \equiv -u(j+k) \ (mod \ n) \leftrightarrow j+k \equiv 0 \ (mod \ m_u) \\
j+k \equiv j-uk \ (mod \ n) \leftrightarrow k \equiv 0 \ (mod \ m_u) \\
j+k \equiv k-uj \ (mod \ n) \leftrightarrow j \equiv 0 \ (mod \ m_u) \\
-u(j+k) \equiv j-uk \ (mod \ n) \leftrightarrow j \equiv 0 \ (mod \ m_u) \\
-u(j+k) \equiv k-uj \ (mod \ n) \leftrightarrow k \equiv 0 \ (mod \ m_u) \\
j-uk \equiv k-uj \ (mod \ n) \leftrightarrow j \equiv k \ (mod \ m_u)
\end{gathered}
$$

which determines how the expression of $v_{x_u^j} \cdot v_{x_u^k}$ above condenses.

The next product for H_{N_u} to consider is this

$$v_{t_u x_u^j} \cdot v_{t_u x_u^k} = \Big(\sum_{c=0}^{m_u-1} r^c(\gamma) t_u x_u^{j-c(u+1)} + \sum_{c=0}^{m_u-1} f(r^c(\gamma)) t_u x_u^{-uj+c(u+1)}\Big)$$

$$\cdot \Big(\sum_{e=0}^{m_u-1} r^e(\gamma) t_u x_u^{k-e(u+1)} + \sum_{e=0}^{m_u-1} f(r^e(\gamma)) t_u x_u^{-uk+e(u+1)}\Big)$$

$$= \sum_{c=0}^{m_u-1} \sum_{e=0}^{m_u-1} r^c(\gamma) r^e(\gamma) x_u^{k-j+(c-e)(u+1)}$$

$$+ \sum_{c=0}^{m_u-1} \sum_{e=0}^{m_u-1} r^c(\gamma) f(r^e(\gamma)) x_u^{-uk-j+(c+e)(u+1))}$$

$$+ \sum_{c=0}^{m_u-1} \sum_{e=0}^{m_u-1} f(r^c(\gamma)) r^e(\gamma) x_u^{k+uj-(c+e)(u+1)}$$

$$+ \sum_{c=0}^{m_u-1} \sum_{e=0}^{m_u-1} f(r^c(\gamma)) f(r^e(\gamma)) x_u^{uj-uk-(c-e)(u+1)}$$

which can also be condensed a bit, and written as a linear combination of the other v_n.

We have

$$v_{t_u x_u^j} \cdot v_{t_u x_u^k} = \sum_{h=0}^{m_u-1} (a_h + b_h) v_{x_u^{k-j+h(u+1)}} + a_h v_{x_u^{uj-uk-h(u+1)}}$$
$$+ \sum_{h=0}^{m_u-1} p_h v_{x_u^{k+uj-h(u+1)}} + p_h v_{x_u^{-uk-j+h(u+1)}}$$

where

$$tr_{F_d/F}(r^h(\gamma)\gamma) = a_h + b_h\beta$$
$$tr_{F_d/F}(f(r^h(\gamma)\gamma)) = f(tr_{F_d/F}(r^h(\gamma)\gamma)) = (a_h + b_h) - b_h\beta$$
$$tr_{F_d/F}(r^h(\gamma)f(\gamma)) = p_h$$

The issue is that the values of a_h, b_h and p_h are dependent on the extension $L/F/K$, although one can show that:

$$\sum_{h=0}^{m_u-1} tr_{F_d/F}(r^h(\gamma)\gamma) = \beta^2 = -s + \beta$$

$$\sum_{h=0}^{m_u-1} tr_{F_d/F}(f(r^h(\gamma)\gamma)) = (1-\beta)^2 = (1-s) - \beta$$

$$\sum_{h=0}^{m_u-1} tr_{F_d/F}(r^h(\gamma)f(\gamma)) = \beta(1-\beta) = s$$

and so

$$\sum_{h=0}^{m_u-1} a_h = -s$$

$$\sum_{h=0}^{m_u-1} b_h = 1$$

$$\sum_{h=0}^{m_u-1} p_h = s$$

The other products, and their representation as (fairly simple!) linear combinations of the v_n are

$$v_{t_u x_u^k} \cdot v_{x_u^j} = (1-s)v_{tx_u^{k+j}} + (-s)v_{tx_u^{-u(k+j)}} + sv_{tx_u^{j-uk}} + sv_{tx_u^{k-uj}}$$
$$v_{x_u^j} \cdot v_{t_u x_u^k} = (1-s)v_{tx_u^{k-j}} + (-s)v_{tx_u^{-u(k-j)}} + sv_{tx_u^{-j-uk}} + sv_{tx_u^{k+uj}}$$

and the symmetry of the above expressions in j and k leads to a number of identities

$$v_{t_u x_u^k} \cdot v_{x_u^j} = v_{t_u x_u^j} \cdot v_{x_u^k}$$
$$v_{x_u^j} \cdot v_{t_u x_u^k} = v_{t_u x_u^{-j}} \cdot v_{x_u^k}$$
$$v_{t_u} \cdot v_{x_u^j} = v_{t_u x_u^j}$$
$$v_{x_u^j} \cdot v_{t_u} = v_{t_u x_u^{-j}}$$

In summary:

$$\begin{aligned}
v_{x_u^j} \cdot v_{x_u^k} &= (1-s)v_{x_u^{j+k}} - sv_{x_u^{-u(j+k)}} + sv_{x_u^{j-uk}} + sv_{x_u^{k-uj}} \\
v_{t_u x_u^j} \cdot v_{t_u x_u^k} &= \sum_{h=0}^{m_u-1} (a_h + b_h) v_{x_u^{k-j+h(u+1)}} + a_h v_{x_u^{uj-uk-h(u+1)}} \\
&\quad + \sum_{h=0}^{m_u-1} p_h v_{x_u^{k+uj-h(u+1)}} + p_h v_{x_u^{-uk-j+h(u+1)}} \\
v_{t_u x_u^k} \cdot v_{x_u^j} &= (1-s)v_{tx_u^{k+j}} + (-s)v_{tx_u^{-u(k+j)}} + sv_{tx_u^{j-uk}} + sv_{tx_u^{k-uj}} \\
v_{x_u^j} \cdot v_{t_u x_u^k} &= (1-s)v_{tx_u^{k-j}} + (-s)v_{tx_u^{-u(k-j)}} + sv_{tx_u^{-j-uk}} + sv_{tx_u^{k+uj}}
\end{aligned}$$

This leads to one immediately interesting (to me at least) consequence about the structure of H_{N_u}.

Theorem

If we define $H^0_{N_u} = Span(\{v_{x^i_u}\})$ and $H^1_{N_u} = Span(\{v_{t_u x^i_u}\})$ then the above facts about how the basis elements multiply implies that H_{N_u} can be decomposed as a $\mathbb{Z}_2$ graded ring $H_{N_u} = H^0_{N_u} \oplus H^1_{N_u}$.

Proof.

By the above product table for the v_n, one sees that $H^i_{N_u} H^j_{N_u} \subseteq H^{i+j}_{N_u}$. Indeed, one has that $v_{t_u} v_{x^j_u} = v_{t_u x^j_u}$ so that $v_{t_u} H^0_{N_u} \subseteq H^1_{N_u}$ and therefore $v_{t_u} H^0_{N_u} = H^1_{N_u}$. □

A Worked Out Example in Degree 6

For $K = \mathbb{Q}$ we construct a Galois extension L/K with $Gal(L/K) \cong D_3$. First, define $p(x) = x^3 - 2 \in K[x]$ which has roots w, ζw, $\zeta^2 w$ where $w = \sqrt[3]{2}$ and $\zeta = e^{\frac{2\pi i}{3}}$. We have that $Gal(L/K) = \langle r, f \rangle$ where

$$
\begin{aligned}
r(w) &= \zeta w \\
r(\zeta) &= \zeta \\
f(w) &= w \\
f(\zeta) &= \zeta^2
\end{aligned}
$$

so that $|r| = 3$ and $|f| = 2$ and $Gal(L/K) \cong D_3$. One may verify that

$$\alpha = \frac{1}{3} \sum_{i=0}^{1} \sum_{j=0}^{2} \zeta^i w^j$$

is a normal basis generator for L/K where $tr_{L/K}(\alpha) = 1$.

As $F = L^{\langle r \rangle}$ then $\beta = tr_{L/F}(\alpha) = \zeta + 1$ is a normal basis generator for F/K where $tr_{F/K}(\beta) = \beta + f(\beta) = 1$ and $irr_{F/K}(\beta) = x^2 - x - 1$ which means $F = \mathbb{Q}(\sqrt{-3})$.

Now, since $\Upsilon_3 = \{1, -1\}$ then $R(D_3, [D_3]) = \{\lambda(D_3), \rho(D_3)\}$ so the 'interesting' Hopf algebra action is by $N_1 = \lambda(D_3)$ corresponding to $u = 1 \in \Upsilon_3$ so that $d_1 = gcd(u+1, 3) = 1$ and $m_1 = 3$ and so, as observed earlier, $F_{d_1} = L$ and $\gamma = \alpha$.

The 'v_n' basis for H_{N_1} is

$$
\begin{aligned}
v_{x_1^0} = v_1 &= 1 \\
v_{x_1} &= \beta x_1 + (1-\beta) x_1^2 \\
v_{x_1^2} &= \beta x_1^2 + (1-\beta) x_1 \\
v_{t_1} &= \left(-\frac{1}{3}\,w^2\beta + \frac{1}{3} + \frac{1}{3}\,w\beta - w/3\right) t_1 x_1 + \left(-\frac{1}{3}\,w\beta + \frac{1}{3} + \frac{1}{3}\,w^2\beta - \frac{1}{3}\,w^2\right) t_1 {x_1}^2 \\
&\quad + \left(\frac{1}{3}\,w^2 + w/3 + \frac{1}{3}\right) t_1 \\
v_{t_1 x_1} &= \left(\frac{2}{3}\,w^2\beta + \frac{1}{3}\,w\beta - w/3 + \frac{1}{3}\right) t_1 x_1 + \left(-\frac{1}{3}\,w\beta - \frac{2}{3}\,w^2\beta + \frac{2}{3}\,w^2 + \frac{1}{3}\right) t_1 {x_1}^2 \\
&\quad + \left(w/3 - \frac{2}{3}\,w^2 + \frac{1}{3}\right) t_1 \\
v_{t_1 x_1^2} &= \left(-\frac{1}{3}\,w^2\beta - \frac{2}{3}\,w\beta + \frac{2}{3}\,w + \frac{1}{3}\right) t_1 x_1 + \left(\frac{2}{3}\,w\beta + \frac{1}{3}\,w^2\beta - \frac{1}{3}\,w^2 + \frac{1}{3}\right) t_1 {x_1}^2 \\
&\quad + \left(-\frac{2}{3}\,w + \frac{1}{3}\,w^2 + \frac{1}{3}\right) t_1
\end{aligned}
$$

Using MAPLE we can compute the different 'trace pairings' for the coefficients in the different products.

$$tr_{L/F}(r^0(\alpha)\alpha) = a_0 + b_0\beta = \frac{-5}{3} + \frac{5}{3}\beta$$
$$tr_{L/F}(r^1(\alpha)\alpha) = a_1 + b_1\beta = \frac{1}{3} + \frac{-1}{3}\beta$$
$$tr_{L/F}(r^2(\alpha)\alpha) = a_2 + b_2\beta = \frac{1}{3} + \frac{-1}{3}\beta$$

$$tr_{L/F}(f(r^0(\alpha)\alpha)) = (a_0 + b_0) - b_0\beta = -\frac{5}{3}\beta$$
$$tr_{L/F}(f(r^1(\alpha)\alpha)) = (a_1 + b_1) - b_1\beta = \frac{1}{3}\beta$$
$$tr_{L/F}(f(r^0(\alpha)\alpha)) = (a_2 + b_2) - b_2\beta = \frac{1}{3}\beta$$

$$tr_{L/F}(r^0(\alpha)f(\alpha)) = p_0 = \frac{5}{3}$$
$$tr_{L/F}(r^1(\alpha)f(\alpha)) = p_1 = -\frac{1}{3}$$
$$tr_{L/F}(r^2(\alpha)f(\alpha)) = p_2 = -\frac{1}{3}$$

So for example, we have the simplest product, namely the commuting basis elements v_{x_1} and $v_{x_1^2}$.

$$v_{x_1} \cdot v_{x_1^2} = v_{x_1^2} \cdot v_{x_1} = -v_{x_1^0} + v_{x_1^2} + v_{x_1}$$

and the others can be 'clustered' given the similarities one sees:

$$\begin{aligned}
v_{x_1} \cdot v_{x_1} &= -v_{x_1} + 2v_{x_1^0} \\
v_{x_1^2} \cdot v_{x_1^2} &= -v_{x_1^2} + 2v_{x_1^0} \\
v_{x_1^2} \cdot v_{t_1 x_1} &= -v_{t_1 x_1} + 2v_{t_1} \\
v_{t_1 x_1} \cdot v_{x_1} &= -v_{t_1 x_1} + 2v_{t_1} \\
v_{x_1} \cdot v_{t_1 x_1^2} &= -v_{t_1 x_1^2} + 2v_{t_1} \\
v_{t_1 x_1^2} \cdot v_{x_1^2} &= -v_{t_1 x_1^2} + 2v_{t_1}
\end{aligned}$$

and

$$\begin{aligned}
v_{t_1} \cdot v_t &= 5/3 v_{x_1^0} - 1/3 v_{x_1^2} - 1/3 v_{x_1} \\
v_{t_1} \cdot v_{t_1 x_1} &= 5/3 v_{x_1} - 1/3 v_{x_1^0} - 1/3 v_{x_1^2} \\
v_{t_1 x_1^2} \cdot v_{t_1} &= 5/3 v_{x_1} - 1/3 v_{x_1^0} - 1/3 v_{x_1^2} \\
v_{t_1} \cdot v_{t_1 x_1^2} &= 5/3 v_{x_1^2} - 1/3 v_{x_1^0} - 1/3 v_{x_1} \\
v_{t_1 x_1} \cdot v_{t_1} &= 5/3 v_{x_1^2} - 1/3 v_{x_1^0} - 1/3 v_{x_1}
\end{aligned}$$

and

$$
\begin{aligned}
v_{t_1x_1} \cdot v_{t_1x_1} &= -7/3v_{x_1^0} + 5/3v_{x_1^2} + 5/3v_{x_1} \\
v_{t_1x_1^2} \cdot v_{t_1x_1^2} &= -7/3v_{x_1^0} + 5/3v_{x_1^2} + 5/3v_{x_1} \\
v_{t_1x_1^2} \cdot v_{t_1x_1} &= -7/3v_{x_1} + 11/3v_{x_1^0} - 1/3v_{x_1^2} \\
v_{t_1x_1} \cdot v_{t_1x_1^2} &= -7/3v_{x_1^2} + 11/3v_{x_1^0} - 1/3v_{x_1}
\end{aligned}
$$

and

$$
\begin{aligned}
v_{x_1^2} \cdot v_{t_1} &= v_{t_1x_1} \\
v_{t_1} \cdot v_{x_1} &= v_{t_1x_1} \\
v_{x_1} \cdot v_{t_1} &= v_{t_1x_1^2} \\
v_{t_1} \cdot v_{x_1^2} &= v_{t_1x_1^2}
\end{aligned}
$$

and

$$
\begin{aligned}
v_{x_1^2} \cdot v_{t_1x_1^2} &= -v_{t_1} + v_{t_1x_1^2} + v_{t_1x_1} \\
v_{t_1x_1} \cdot v_{x_1^2} &= -v_{t_1} + v_{t_1x_1^2} + v_{t_1x_1} \\
v_{t_1x_1^2} \cdot v_{x_1} &= -v_{t_1} + v_{t_1x_1^2} + v_{t_1x_1} \\
v_{x_1} \cdot v_{t_1x_1} &= -v_{t_1} + v_{t_1x_1^2} + v_{t_1x_1}
\end{aligned}
$$

The goal is to show that even though none of the H_{N_u} are isomorphic as Hopf-algebras, they are isomorphic as K-algebras.

An ad-hoc approach/example in the D_3 case is to utilize the v_n basis to construct matrix units, and therefore an explicit isomorphism $(K[\lambda(D_3)])^{D_3} = H_{N_1} \to H_{N_{-1}} = K[\rho(D_3)]$.

This is made easier by the knowledge of the multiplication table for the $\{v_n\}$ we just explored.

We know that $K[D_3] \cong K \times K \times M_2(K)$ is the Wedderburn decomposition so the difficulty is in finding a 'copy' of $M_2(K)$ inside H_{N_1}, namely a set of matrix units.

Consider

$$\begin{aligned} h_{1,1} &= \frac{1}{3}(v_{x_1^0} - v_{x_1^2}) \\ h_{1,2} &= \frac{1}{6}(v_{t_1} - v_{t_1 x_1}) \\ h_{2,1} &= \frac{1}{3}(v_{t_1} - v_{t_1 x_1^2}) \\ h_{2,2} &= \frac{1}{3}(v_{x_1^0} - v_{x_1}) \end{aligned}$$

which we assert correspond to the elementary 2×2 matrices $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$.

If the character values of D_3 lie in K then the orthogonal idempotents

$$e_{\chi_i} = \frac{\chi_i(1)}{|D_3|} \sum_{g \in D_3} \chi_i(g^{-1})g$$

lie in $K[D_3]$.

There are two 1-d characters χ_1 and χ_2, where $\chi_1(g) = 1$ for all $g \in D_3$, $\chi_2(x_1^i) = (-1)^i$, $\chi_2(t_1 x_1^i) = 0$, as well as the 2-d character χ_3 where $\chi_3(1) = 2$, $\chi_3(x_1) = -1$,$\chi_3(x_1^2) = -1$, $\chi_3(t_1 x_1^j) = 0$

In particular we obtain

$$
\begin{aligned}
e_{\chi_1} &= \frac{1}{6}(t_1 x_1^2 + t_1 x_1 + t_1 + x_1^2 + x_1 + 1) \\
e_{\chi_2} &= \frac{1}{6}(-t_1 x_1^2 - t_1 x_1 - t_1 + x_1^2 + x_1 + 1) \\
e_{\chi_3} &= \frac{1}{3}(2 - x_1 - x_1^2)
\end{aligned}
$$

but what is quite extraordinary is how these may be represented in terms of the v-basis, namely that they actually reside in $H_{N_1} = (K[\lambda(D_3)])^{D_3}$.

Specifically

$$
\begin{aligned}
e_{\chi_1} &= \frac{1}{6}(t_1x_1^2 + t_1x_1 + t_1 + x_1^2 + x_1 + 1)\\
&= \frac{1}{6}(v_{t_1x_1^2} + v_{t_1x_1} + v_{t_1} + v_{x_1^2} + v_{x_1} + v_{x_1^0})
\end{aligned}
$$

$$
\begin{aligned}
e_{\chi_2} &= \frac{1}{6}(-t_1x_1^2 - t_1x_1 - t_1 + x_1^2 + x_1 + 1)\\
&= \frac{1}{6}(-v_{t_1x_1^2} - v_{t_1x_1} - v_{t_1} + v_{x_1^2} + v_{x_1} + v_{x_1^0})
\end{aligned}
$$

$$
\begin{aligned}
e_{\chi_3} &= \frac{1}{3}(2 - x_1 - x_1^2)\\
&= \frac{1}{3}(2v_{x_1^0} - v_{x_1} - v_{x_1^2})
\end{aligned}
$$

and the idempotent e_{χ_3} is used to obtain the $h_{i,j}$.

What we have then is that $H_{N_1} = H_\lambda$ (expressed in its Wedderburn form as $K \times K \times Mat_2(K)$) has basis $\{e_{\chi_1}, e_{\chi_2}, h_{1,1}, h_{1,2}, h_{2,1}, h_{2,2}\}$, which are all expressed in terms of the $v_{t_1^i x_1^j}$ basis vectors, explicitly

$$\left(a, b, \begin{bmatrix} c & d \\ e & f \end{bmatrix}\right) \mapsto ae_{\chi_1} + be_{\chi_2} + ch_{1,1} + dh_{1,2} + eh_{2,1} + fh_{2,2}$$

where, for example, we can see where the identity element of the direct product gets mapped

$$\left(1, 1, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) \mapsto e_{\chi_1} + e_{\chi_2} + h_{1,1} + h_{2,2} = v_{x_1^0}$$

which is congruous with the observation earlier that $v_{x_1^0}$ is the identity element of H_{N_u}.

As an interesting computational aside, the sub-algebra $H^0_{N_1} = Span(\{v_{x_1^j}\})$ can also be written as $Span(\{e_{\chi_1} + e_{\chi_2}, h_{1,1}, h_{2,2}\})$, namely as those elements of the form

$$\left(a, a, \begin{bmatrix} b & 0 \\ 0 & f \end{bmatrix}\right)$$

and similarly $H^1_{N_1} = Span(\{v_{t_1 x_1^j}\}) = Span(\{(e_{\chi_1} - e_{\chi_2}), h_{1,2}, h_{2,1}\})$ which equals

$$\left(a, -a, \begin{bmatrix} 0 & c \\ d & 0 \end{bmatrix}\right)$$

Going further, we can view $H_{N_1} = H_\lambda$ as a group ring in a kind of natural way. One may show that in $M_2(K)$ one has matrices

$$X = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$$

$$T = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

which can be shown satisfy the equations $X^3 = I$, $T^2 = I$ and $XT = TX^2$ so that $\langle X, T \rangle \cong D_3$ and therefore have elements (units) of the Wedderburn decomposition of H_{N_1} which also satisfy these relations, namely $h_X = (1, 1, X)$ and $h_T = (1, 1, T)$.

What we would like is to show that

$$\{1, h_X, (h_X)^2, h_T, h_T h_X, h_T(h_x)^2\} = \\ \{(1,1,I),(1,1,X),(1,1,X^2),(1,1,T),(1,1,TX),(1,1,TX^2)\}$$

are yet a different basis for H_{N_1}.

As it turns out, one must adjust h_T, and set it to be $(1,-1,T)$ in order to achieve linear independence, which yields the set

$$\{(1,1,I),(1,1,X),(1,1,X^2),(1,-1,T),(1,-1,TX),(1,-1,TX^2)\}$$

which *is* linearly independent.

The *five* 2×2 matrices X, X^2, T, TX, TX^2 cannot be a linearly independent subset of $M_2(K)$. And in terms of the basis $\{e_{\chi_1}, e_{\chi_2}, h_{1,1}, h_{1,2}, h_{2,1}, h_{2,2}\}$ one has

$$\begin{aligned}
1 &= 1e_{\chi_1} + 1e_{\chi_2} + 1h_{1,1} + 0h_{1,2} + 0h_{2,1} + 1h_{2,2} \\
h_X &= 1e_{\chi_1} + 1e_{\chi_2} + 0h_{1,1} + 1h_{1,2} + (-1)h_{2,1} + (-1)h_{2,2} \\
(h_X)^2 &= 1e_{\chi_1} + 1e_{\chi_2} + (-1)h_{1,1} + (-1)h_{1,2} + 1h_{2,1} + 0h_{2,2} \\
h_T &= 1e_{\chi_1} + (-1)e_{\chi_2} + 0h_{1,1} + 1h_{1,2} + 0h_{2,1} + 1h_{2,2} \\
h_T h_X &= 1e_{\chi_1} + (-1)e_{\chi_2} + (-1)h_{1,1} + (-1)h_{1,2} + 0h_{2,1} + 1h_{2,2} \\
h_T(h_X)^2 &= 1e_{\chi_1} + (-1)e_{\chi_2} + 1h_{1,1} + 0h_{1,2} + (-1)h_{2,1} + (-1)h_{2,2}
\end{aligned}$$

and, for reference, we can represent h_X and h_T in terms of the v basis.

$$
\begin{aligned}
h_X &= \frac{2}{3} v_{x_1} + \frac{1}{3} v_{x_1^2} - \frac{1}{6} v_{t_1} - \frac{1}{6} v_{t_1 x_1} + \frac{1}{3} v_{t_1 x_1^2} \\
h_T &= \frac{5}{6} v_{t_1} + \frac{1}{6} v_{t_1 x_1}
\end{aligned}
$$

So we have (in a kind of bare-handed way) demonstrated the following:

Theorem

If $D_3 = \langle x, t \mid x^3 = t^2 = 1, xt = tx^2 \rangle$ *then there is a* K*-algebra isomorphism* $\psi : K[D_3] \to H_{N_1}$ *given by* $\psi(x) = h_X$ *and* $\psi(t) = h_T$*.*

Idempotents in H_N

The similarity of the expression of the idempotents expressed in terms of the group elements and the v basis, e.g.

$$\begin{aligned} e_{\chi_1} &= \frac{1}{6}(t_1x_1^2 + t_1x_1 + t_1 + x_1^2 + x_1 + 1) \\ &= \frac{1}{6}(v_{t_1x_1^2} + v_{t_1x_1} + v_{t_1} + v_{x_1^2} + v_{x_1} + v_{x_1^0}) \end{aligned}$$

makes one wonder if there is, more generally, a direct analogue of the e_{χ_i} framed in terms of the v_n?

Conjecture/Question: If H_λ contains all the central idempotents as the group ring H_ρ does that imply that $H_\lambda \cong H_\rho$?

Consider the following.

Definition

For $N \in R(G)$ and $\{v_n\}$ the basis for $H_N = (L[N])^{\lambda(G)}$ let

$$v_\chi = \frac{\chi(e_N)}{|N|} \sum_{n \in N} \chi(n^{-1}) v_n$$

for each irreducible character $\chi : N \to K$ of N.

We model this on the usual idempotent defintion $e_\chi = \frac{\chi(e_N)}{|N|} \sum_{n \in N} \chi(n^{-1}) n \in K[N]$.

The first question is whether these v_χ are similarly orthogonal idempotents. Under some assumptions on χ we can show more in fact.

Theorem

For $N \in R(G)$ and v_χ as defined above, if χ is real valued and all character values lie in K, and $\chi(\lambda(g)n\lambda(g)^{-1}) = \chi(n)$ for all $n \in N$ and $g \in G$ then $v_\chi = e_\chi$.

Proof:

By assumption $\chi(n^{-1}) = \overline{\chi(n)} = \chi(n)$ and so:

$$
\begin{aligned}
v_\chi &= \frac{\chi(e_N)}{|N|} \sum_{n \in N} \chi(n^{-1}) v_n \\
&= \frac{\chi(e_N)}{|N|} \sum_{n \in N} \sum_{g \in G} \chi(n^{-1}) g(\alpha) \lambda(g) n \lambda(g)^{-1} \\
&= \frac{\chi(e_N)}{|N|} \sum_{g \in G} g(\alpha) \sum_{n \in N} \chi(n^{-1}) \lambda(g) n \lambda(g)^{-1} \\
&= \frac{\chi(e_N)}{|N|} \sum_{g \in G} g(\alpha) \sum_{n \in N} \chi(n) \lambda(g) n \lambda(g)^{-1} \\
&= \frac{\chi(e_N)}{|N|} \sum_{g \in G} g(\alpha) \sum_{n \in N} \chi(\lambda(g) n \lambda(g)^{-1}) \lambda(g) n \lambda(g)^{-1}
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{\chi(e_N)}{|N|} \sum_{g \in G} g(\alpha) \sum_{m \in N} \chi(m)m \\
&= \frac{\chi(e_N)}{|N|} \sum_{g \in G} g(\alpha) \sum_{m \in N} \chi(m^{-1})m \\
&= \frac{\chi(e_N)}{|N|} \sum_{m \in N} \chi(m^{-1})m \\
&= e_\chi
\end{aligned}
$$

where the second to last line is due to the assumption that $tr_{L/K}(\alpha) = 1$, which completes the proof. $\square$

As a corollary, we have the following.

Corollary

For $N \in R(G)$ and v_χ as defined above, if χ is real valued and all character values lie in K and the action of $\lambda(G)$ on N is by inner automorphisms, then $v_\chi = e_\chi$

Proof.

If conjugation by every $\lambda(g)$ induces an inner automorphism of N then all conjugacy classes are preserved and therefore all character values are preserved. $\square$

As a result, we have some immediate examples.

If G is such that all its irreducible character values are real and lie in K then for $N = \lambda(G), \rho(G)$ one has $v_\chi = e_\chi$.

Of course, the upshot of this is that for these N the Hopf algebras H_N contain the same orthogonal idempotents as does $K[N]$ itself (and therefore has identical Wedderburn decomposition to that of $K[N]$?)

Corollary

If $N \in R(G)$ *and* χ *is a real valued irreducible character of* N *such that all values of* χ *lie in* K *and* $\chi(\lambda(g)n\lambda(g)^{-1}) = \chi(n)$ *for all* $n \in N$ *and* $g \in G$ *then* $e_\chi \in H_N$*.*

For D_n, the question is, for what irreducible character(s) χ do we have $\chi(\lambda(g)n\lambda(g)^{-1}) = \chi(n)$ for every $n \in N$ where $N \in \mathcal{H}(D_n)$?

Given $N_u \in \mathcal{H}(D_n)$ where $N_u = \langle x_u, t_u \rangle$ and where $\lambda(G) = \langle r, f \rangle$ acts by

$$\begin{aligned} r x_u r^{-1} &= x_u \\ r t_u r^{-1} &= t_u {x_u}^{-(u+1)} \\ f x_u f^{-1} &= x_u^{-u} \\ f t_u f^{-1} &= t_u \end{aligned}$$

we look at whether each χ is $\lambda(G)$-invariant.

If n is even then the 1-d irreps are χ_1, χ_2, χ_3, and χ_4 where

	x_u^j	$t_u x_u^j$
χ_1	1	1
χ_2	1	-1
χ_3	$(-1)^j$	$(-1)^j$
χ_4	$(-1)^j$	$(-1)^{j+1}$

and for n odd, χ_3 and χ_4 aren't defined.

Clearly χ_1 and χ_2 are $\lambda(G)$-invariant, and for n even, $u \in \Upsilon_n$ must be odd, and so $u+1$ must be even and so $j-(u+1) \equiv j \ (mod\ 2)$ and $j \equiv -ju \ (mod\ 2)$ and so χ_3 and χ_4 are as well.

For the two dimensional irreps χ^h where $\chi^h(t_u x_u^j) = 0$ and $\chi^h(x_u^j) = 2cos(\frac{2hj\pi}{n})$ for $0 < h < \frac{n}{2}$ the question is whether

$$cos\left(\frac{2hj\pi}{n}\right) = cos\left(\frac{-2huj\pi}{n}\right)$$

for $u \in \Upsilon_n$?

And here is where a problem arises, namely the above equality holds (for all $h \in (0, \frac{n}{2})$) only if $u = \pm 1$, i.e. for $N_1 = \lambda(D_n)$ and $N_{-1} = \rho(D_n)$.

But at least we can conclude that $H_\lambda = H_{N_1} \cong H_{N_{-1}} = H_\rho$ for all n, not just $n = 3$, or even n a prime necessarily.

Questions:

(1) Does the fact that $e_\chi \in H_{N_1} = H_\lambda$ for each irreducible character χ imply that H_{N_1} has the same Wedderburn decomposition as $H_{N_{-1}} = H_\rho = K[\rho(D_n)]$?

(2) For those irreducible characters χ which are not $\lambda(G)$-invariant, are the v_χ idempotent? central?
(even if they don't lie in $K[\rho(D_n)]$?)

Thank you!

F. Dalla Volta A. Caranti.
Groups that have the same holomorph as a finite perfect group.
Arxiv preprint GR, 2017.

A. Caranti.
The multiple holomorphs of finite p-groups of class two.
Arxiv preprint GR, 2018.

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

G.A. Miller.
On the multiple holomorphs of a group.
Math. Ann., 66:133–142, 1908.