Finite p-groups of class two with a large/small multiple holomorph

Andrea Caranti and Cindy (Sin Yi) Tsang

Brussels, 20 January 2025, 9:30 CET

AC Dipartimento di Matematica
Università degli Studi di Trento
Trento
Italy
CT Department of Mathematics
Ochanomizu University
Tokyo
Japan

Isomorphic regular subgroups

Let $(G, 1)$ be a pointed set. A subgroup $N \leq \mathrm{S}(G)$ of the group $\mathrm{S}(G)$ of permutations on the set G is said to be regular if the map

$$N \to G, \qquad n \mapsto 1^n$$

is a bijection.

G.A. Miller
On the multiple holomorphs of a group
Math. Ann. **1** (1908), 133–142

Miller has shown that for two regular subgroups N, M of a symmetric group $\mathrm{S}(G)$, where G is a set, the following are equivalent:

- N and M are isomorphic, and
- N and M are conjugate in $\mathrm{S}(G)$.

The holomorph

Let now $G = (G, \cdot, 1)$ be a group. In $\mathsf{S}(G)$ we have the regular subgroup $\rho(G)$, the image of the right regular representation

$$\begin{aligned} \rho : G &\to \mathsf{S}(G) \\ g &\mapsto (x \mapsto x \cdot g). \end{aligned}$$

It is an easy fact that

$$N_{\mathsf{S}(G)}(\rho(G)) = \mathrm{Aut}(G)\rho(G) = \mathrm{Hol}(G) \cong \mathrm{Aut}(G) \ltimes G.$$

More generally, for every regular subgroup $N \leq \mathsf{S}(G)$ we have

$$N_{\mathsf{S}(G)}(N) \cong \mathrm{Hol}(N).$$

Regular subgroups of $\mathrm{Hol}(G)$ are in one-to-one correspondence with skew braces with additive group $(G, \cdot)$.

Skip details

Regular subgroups of the holomorph I

Regular subgroups $N \leq N_{S(G)}(\rho(G))$ occur in cryptography:

A. Caranti, F. Dalla Volta and M. Sala
Abelian *regular subgroups* of the affine group and radical rings.
Publ. Math. Debrecen 69 (2006), no. 3, 297–308.

In Hopf Galois theory:

C. Greither, B. Pareigis
Hopf Galois theory for separable field extensions
J. Algebra **106** (1987), 239–258

N. P. Byott
Uniqueness of Hopf Galois structure of separable field extensions
Comm. Algebra **24** (1996), 3217–3228

Regular subgroups of the holomorph II

More Hopf Galois:

S.C. Featherstonhaugh, A.C. and L. Childs
Abelian Hopf Galois structures on prime-power Galois field extensions.
Trans. Amer. Math. Soc. **364** (2012), no. 7, 3675–3684.

Regular subgroups $N \leq N_{S(G)}(\rho(G))$ are equivalent to skew braces on G, which determine solutions to the Yang-Baxter equation:

W. Rump
Braces, radical rings, and the quantum Y-B equation
J. Algebra **307** (2007), 153–170

L. Guarnieri and L. Vendramin
Skew braces and the Yang-Baxter equation
Math. Comp. **86** (2017), no. 307, 2519–2534

A converse to Cayley's theorem

Let $(G, \cdot)$ be a pointed set, and $N \leq \mathrm{S}(G)$ be a regular subgroup, so that the map

$$N \to G, \qquad n \mapsto 1^n$$

is a bijection, whose inverse

$$\nu : G \to N$$

maps $x \in G$ to the unique element $\nu(x) \in N$ such that $1^{\nu(x)} = x$.

One can use these maps to transport the group structure of N on the set G to get a group operation "$\circ$" on G such that

- $\nu : (G, \circ) \to N$ is an isomorphism.
- $x^{\nu(y)} = 1^{\nu(x)\nu(y)} = 1^{\nu(x \circ y)} = x \circ y$, so this is a converse to Cayley's theorem: every regular subgroup of $\mathrm{S}(G)$ is the image of the regular representation of a suitable group $(G, \circ)$.

Rephrasing isomorphism

$N = \{ \nu(x) : x \in G \} \leq \mathrm{S}(G)$ regular, where $\nu(x)$ is the unique element of N such that $1^{\nu(x)} = x$.

There are a group $(G, \circ)$, and a bijection $\nu : G \to N$ such that

- $\nu : (G, \circ) \to N$ is an isomorphism, and
- $x^{\nu(y)} = x \circ y$, that is, $\nu : (G, \circ) \to \mathrm{S}(G)$ is the right regular representation of $(G, \circ)$.

We can rephrase Miller's result as follows.

- Let $(G, \cdot, 1)$ be a group.
- Let $N \cong \rho(G) \cong G$ be a regular subgroup of $S(G)$.
- Then for $\vartheta \in \mathrm{S}(G)$ such that $1^\vartheta = 1$, the following are equivalent :
  - $\vartheta : (G, \cdot) \to (G, \circ)$ is an isomorphism, and
  - $\rho(G)^\vartheta = N$.

Regular subgroups of the holomorph III

Let

$$N \leq \mathrm{Hol}(G) = N_{\mathsf{S}(G)}(\rho(G)) = \mathrm{Aut}(G)\rho(G)$$

be a regular subgroup of $\mathsf{S}(G)$.

Then for the unique element $\nu(x) \in N$ such that $1^{\nu(x)} = x \in G$ we have

$$\nu(x) = \gamma(x)\rho(x),$$

where $\gamma : G \to \mathrm{Aut}(G)$ is a function, which is characterised by the functional equation

$$\gamma(x^{\gamma(y)}y) = \gamma(x)\gamma(y).$$

Groups having the same holomorph, and $T(G)$

G and N are said to have the same holomorph if $\rho(G), N$ are conjugate, and

$$\mathrm{Hol}(G) = N_{\mathsf{S}(G)}(\rho(G)) = N_{\mathsf{S}(G)}(N) \cong \mathrm{Hol}(N).$$

Let N be an element of

$\mathcal{H}(G) = \{\, N \leq \mathrm{Hol}(G) \text{ regular} : G \text{ and } N \text{ have the same holomorph} \,\}$.

Then $\rho(G)^{\vartheta} = N$ for a ϑ in the multiple holomorph

$$\mathrm{NHol}(G) = N_{\mathsf{S}(G)}(\mathrm{Hol}(G)) = N_{\mathsf{S}(G)}(N_{\mathsf{S}(G)}(\rho(G))).$$

According to Miller's result, $\mathcal{H}(G)$ is the orbit of $\rho(G)$ under the conjugation action of $\mathrm{NHol}(G)$.

The stabiliser of $\rho(G)$ is $\mathrm{Hol}(G) \trianglelefteq \mathrm{NHol}(G)$. Thus

$$T(G) = \mathrm{NHol}(G)/\mathrm{Hol}(G) \text{ acts regularly on } \mathcal{H}(G).$$

The structure of $T(G)$

It is conjectured that when G is centerless, $T(G)$ is an elementary abelian 2-group.

Cindy (Sin Yi) Tsang
The multiple holomorph of centerless groups
J. Pure Appl. Algebra **229** (2025), no. 1

When G is a finite p-group of class 2 (more generally, less than p), then $T(G)$ contains a cyclic subgroup of order $p - 1$.

A.C.
Multiple Holomorphs of Finite p-Groups of Class Two
J. Algebra **516** (2018), 352-372

Cindy (Sin Yi) Tsang
On the multiple holomorph of groups of squarefree or odd prime power order
J. Algebra **544** (2020), 1–28

Large and small

- A.C. and Cindy (Sin Yi) Tsang
  Finite p-groups of class two with a large multiple holomorph
  J. Algebra **617** (2023), 476–499
- A.C. and Cindy (Sin Yi) Tsang
  Finite p-groups of class two with a small multiple holomorph.
  J. Group Theory **27** (2024), no. 2, 345–381

Large

For finite p-groups of class two, $T(G)$ contains a cyclic subgroup of order $p-1$ (think of maps $x \mapsto x^d$, with $\gcd(x,p)=1$). Cindy and I wondered how big can $T(G)$ be. We found

Theorem

For any odd prime p, and $n \geq 4$, there exists a finite p-group G of class two and order $p^{n+\binom{n}{2}}$ such that $T(G)$ is isomorphic to

$$\mathbf{F}_p^{\binom{n}{2}\binom{n+1}{2}} \rtimes \left(\mathbf{F}_p^{\left(\binom{n}{2}-n\right)\times n} \rtimes \left(\mathrm{GL}(n, \mathbf{F}_p) \times \mathrm{GL}\left(\binom{n}{2} - n, \mathbf{F}_p \right) \right) \right).$$

The gist of it is that any finite group H occurs as a subgroup of $T(G)$, for some finite p-group G of class two, with p an odd prime.

I will only show how the part in colour occurs. We reduce the proof to elementary questions in linear algebra.

Normality is (somewhat) easy

Recall $N = \{ \gamma(x)\rho(x) : x \in G \}$, where $\gamma : G \to \mathrm{Aut}(G)$ satisfies $\gamma(x^{\gamma(y)}y) = \gamma(x)\gamma(y)$, and $N \cong (G, \circ)$, where $x \circ y = x^{\gamma(y)}y$.

$$\mathrm{Hol}(G) = N_{\mathrm{S}(G)}(\rho(G)) = N_{\mathrm{S}(G)}(N) \cong \mathrm{Hol}(N) \qquad (1)$$

implies $N \trianglelefteq \mathrm{Hol}(G)$. The latter condition can be conveniently stated in terms of gamma functions as

$$\gamma(xy) = \gamma(y)\gamma(x), \qquad \gamma(x^\beta) = \gamma(x)^\beta \qquad x, y \in G, \beta \in \mathrm{Aut}(G).$$

One cannot encode so neatly the fact that $G \cong N$, which when G is finite would give equality (1). Still it is clear that if we want a large $T(G)$, then (a) small (automorphism group) is beautiful.

In $\mathrm{Aut}(G)$ you have in any case the central automorphisms $\mathrm{Aut}_c(G)$ that act trivially on $G/Z(G)$, and thus on G', as for $\beta \in \mathrm{Aut}_c(G)$ we have $[x, y]^\beta = [x^\beta, y^\beta] = [xz_1, yz_2] = [x, y]$, for $z_1, z_2 \in Z(G)$.

Bilinear forms

Assume from now on $G' = Z(G)$ and $\mathrm{Aut}(G) = \mathrm{Aut}_c(G)$. We have

$$x^{\gamma(y)} = x \cdot x^{-1} x^{\gamma(y)} = x \cdot [x, \gamma(y)],$$

where

$$\begin{aligned} G \times G &\to Z(G) \\ (x, y) &\mapsto [x, \gamma(y)] \end{aligned}$$

turns out to be a morphism in both components, and thus yields a bilinear form

$$\Delta : G/G' \times G/G' \to Z(G). \tag{2}$$

The condition $\gamma(x^\beta) = \gamma(x)^\beta$, or $\Delta(x^\beta, y^\beta) = \Delta(x, y)^\beta$, is now empty on these forms, as $\mathrm{Aut}(G) = \mathrm{Aut}_c(G)$ acts trivially on both G/G' and $G' = Z(G)$. So you can describe the group operation $\circ$ associated to a regular subgroup $N \trianglelefteq \mathrm{Hol}(G)$ as

$$x \circ y = x^{\gamma(y)} y = xy\Delta(x, y),$$

for a bilinear form Δ as in (2).

Symmetric forms and isomorphic groups

If Δ is symmetric, then

$$\begin{aligned} \vartheta : (G, \cdot) &\to (G, \circ) \\ x &\mapsto x\Delta(x, x)^{1/2} \end{aligned}$$

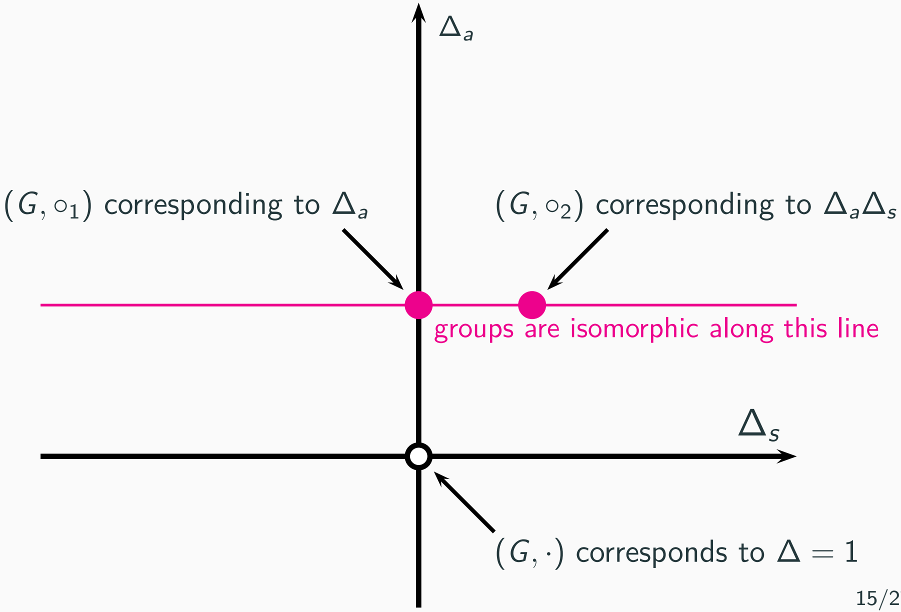
is an isomorphism, which means $\rho(G)$ and N are conjugate. Recall $x \circ y = xy\Delta(x, y)$.

More generally, if

$$\Delta = \Delta_a \Delta_s,$$

for a fixed antisymmetric form Δ_a, as the symmetric part Δ_s varies, all the corresponding groups $(G, \circ)$ are isomorphic, so we need only be concerned with antisymmetric forms.

$\Delta = \Delta_a \Delta_s$ and $x \circ y = xy\Delta(x, y)$



Computing automorphisms I

G. Daues and H. Heineken
Dualitäten und Gruppen der Ordnung p^6
Geometriae Dedicata **4** (1975), no. 2/3/4, 215–220

A.C.
Automorphism groups of p-groups of class 2 and exponent p^2: a classification on 4 generators
Ann. Mat. Pura Appl. **(4)** 134 (1983), 93–146

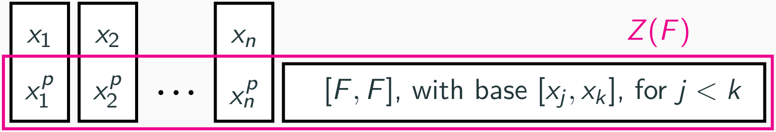
A.C.
A simple construction for a class of p-groups with all of their automorphisms central
Rend. Semin. Mat. Univ. Padova **135** (2016), 251–258

A special class

Let $\mathcal{F}$ be the free group on n generators. Consider the quotient group

$$F = \mathcal{F} / \langle\, [[\mathcal{F}, \mathcal{F}], \mathcal{F}], \mathcal{F}^{p^2}, [\mathcal{F}^p, \mathcal{F}] \,\rangle,$$

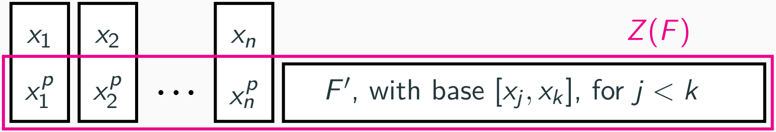
which is free in a suitable variety. F is defined by the equations $[[x, y], z] = x^{p^2} = [x^p, y] = 1$. Note $[F, F]^p = [F^p, F] = 1$.



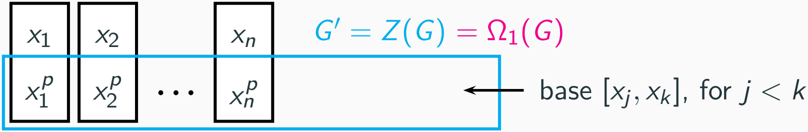
Consider, for $n \geq 4$,

$$G = G(D) = F / \langle\, x_i^p = \prod_{j<k} [x_j, x_k]^{d_{i,(j,k)}}, i = 1, \dots n \,\rangle.$$

$D = [d_{i,(j,k)}]$ is an $n \times \binom{n}{2}$ $\mathbf{F}_p$-matrix, which we take of full rank n.



$$G = G(D) = F/\langle\, x_i^p = \prod_{j<k} [x_j, x_k]^{d_{i,(j,k)}}, i = 1, \dots n \,\rangle,$$



The p-th power map

$$\pi : G/G' \to G', \qquad xG' \mapsto x^p$$

is a morphism, since p is odd: $(xy)^p = x^p y^p [y, x]^{\binom{p}{2}} = x^p y^p$.

π is injective, as its matrix $D = [d_{i,(j,k)}]$ has full rank n.

Computing automorphisms II

$V = G/G' = F/\operatorname{Frat}(F)$ is an $\mathbf{F}_p$-vector space of dimension n. Let $\alpha \in \mathrm{GL}(V) = \mathrm{GL}(n, \mathbf{F}_p)$.

$$\begin{tikzcd}
\ker(\psi) \arrow[r] & F \arrow[r, "\psi"] \arrow[d, "“\alpha”"'] \arrow[dr, "“\alpha”\psi"] & (G, \cdot) \arrow[d, dotted, "\vartheta"] \\
\ker(\psi) \arrow[r] & F \arrow[r, "\psi"'] & (G, \cdot)
\end{tikzcd}$$

“α” is the lift of $\alpha \in \mathrm{GL}(V) = \mathrm{GL}(F/\operatorname{Frat}(F))$ to $\mathrm{Aut}(F)$, which exists as F is free in a variety.

α lifts to an automorphism ϑ of $(G, \cdot)$ iff $\ker(\psi) \le \ker(“\alpha”\psi)$.

Since G' has a basis $[x_j, x_k]$, for $j < k$, we can identify

$$G' \xrightarrow{\simeq} \bigwedge^2 V$$

$$[x, y] \mapsto x \wedge y$$

Computing automorphisms III

$$\begin{tikzcd}
\ker(\psi) \arrow[r] & F \arrow[r, "\psi"] \arrow[d, "``\alpha"'] \arrow[dr, "``\alpha"\psi"] & (G,\cdot) \arrow[d, dotted, "\vartheta"] \\
\ker(\psi) \arrow[r] & F \arrow[r, "\psi"'] & (G,\cdot)
\end{tikzcd}$$

$\ker(\psi) \le \ker(``\alpha"\psi)$ translates to the commutativity of

$$\begin{tikzcd}
V \arrow[r, "\pi"] \arrow[d, "\alpha"'] & \bigwedge^2 V \arrow[d, "\widehat{\alpha}"] \\
V \arrow[r, "\pi"'] & \bigwedge^2 V
\end{tikzcd}$$

where $\pi : V \to \bigwedge^2 V$ is the p-th power map, and $\widehat{\alpha}$ is the map induced by α on $\bigwedge^2 V$. In matrix terms,

$$\alpha D = D\hat{\alpha}.$$

One can choose D so that $\alpha = 1$ is the only solution, that is,

$$\mathrm{Aut}(G) = \mathrm{Aut}_c(G).$$

Antisymmetric forms and commutators

Consider now two groups $G = G(D)$ and $(G, \circ)$, where

$$x \circ y = xy\Delta(x, y),$$

for an antisymmetric form

$$\Delta : V \times V \to \bigwedge^2 V.$$

By the universal property of the exterior square,

$$\Delta(x, y) = (x \wedge y)^\sigma = [x, y]^\sigma,$$

for some $\sigma \in \mathrm{End}(\bigwedge^2 V)$. Then

$[x, y]_\circ = [x, y]\Delta(x, y)\Delta(y, x)^{-1} = [x, y]\Delta(x, y)^2 = [x, y]^{1+2\sigma} \in G'$.

When $\sigma = 0$, that is, $\Delta = 1$, we have $(G, \circ) = (G, \cdot)$.

When $\sigma = -1/2$ is scalar, then $(G, \circ)$ is abelian. More generally, since we have $(G, \circ)' \subseteq G'$, for isomorphism we want $G' = (G, \circ)'$, so that σ cannot have $-1/2$ as an eigenvalue.

Computing isomorphisms I

If $\alpha \in \mathrm{GL}(V)$, we have

$$\begin{tikzcd}
\ker(\psi) \arrow[r] & F \arrow[r, "\psi"] \arrow[d, "``\alpha"'] \arrow[dr, "``\alpha"\psi_\circ"] & (G, \cdot) \arrow[d, dotted, "\vartheta"] \\
\ker(\psi_\circ) \arrow[r] & F \arrow[r, "\psi_\circ"'] & (G, \circ)
\end{tikzcd}$$

Since we have fixed the identification $G' \to \bigwedge^2 V$ given by $[x, y] \to x \wedge y$, and $[x, y]_\circ = [x, y]^{1+2\sigma}$, the diagram

$$\begin{tikzcd}
V \arrow[r, "\pi"] \arrow[d, "\alpha"'] & \bigwedge^2 V \arrow[d, "\widehat{\alpha}"] \\
V \arrow[r, "\pi_\circ"'] & \bigwedge^2 V
\end{tikzcd}$$

now yields

$$\alpha D (1 + 2\sigma)^{-1} = D\hat{\alpha}.$$

Computing Isomorphisms II

Recall that if $\vartheta : (G, \cdot) \to (G, \circ)$ is an isomorphism, α is the restriction of ϑ on $V = G/G'$, which is the same for both groups.

In the equation

$$\alpha^{-1} D \hat{\alpha} = D(1 + 2\sigma)^{-1}. \tag{3}$$

you can fix σ, that is, choose a group $(G, \circ)$, and solve for α, that is, look for an isomorphism $\vartheta : (G, \cdot) \to (G, \circ)$ which induces α on $V = G/G'$.

But what is of interest to us is that given an arbitrary $\alpha \in \mathrm{GL}(V)$, we can solve equation (3) for σ. It is a straightforward matter of linear algebra, whose details we will skip.

This will yield that the restriction $T(G) \to \mathrm{GL}(V)$ has for image the whole $\mathrm{GL}(V)$, as in the statement of the main theorem.

Skip to the small case

Computing Isomorphisms III

For a fixed, but arbitrary $\alpha \in \mathrm{GL}(V)$, consider the equation in $\sigma \in \mathrm{End}(\bigwedge^2 V)$

$$\alpha^{-1} D \hat{\alpha} = D(1 + 2\sigma)^{-1},$$

Here

$$\alpha^{-1} D \quad \text{and} \quad D$$

are two $n \times \binom{n}{2}$ matrices of full rank n. And now for a piece of elementary linear algebra, complete $\alpha^{-1} D, D$ to square invertibile matrices $\overline{\alpha^{-1} D}, \overline{D}$, and take $X = \overline{D}^{-1} \cdot \overline{\alpha^{-1} D}$. Then

$$\overline{\alpha^{-1} D} = \overline{D} \cdot X, \qquad \alpha^{-1} D = DX, \qquad \alpha^{-1} D \hat{\alpha} = D(X \hat{\alpha}).$$

Since $X, \hat{\alpha}$ are invertible, you may set $(1 + 2\sigma)^{-1} = X \hat{\alpha}$ to get

$$\sigma = \frac{1}{2}\left((X \hat{\alpha})^{-1} - 1\right),$$

as p is odd.

Computing Isomorphisms IV

We claimed that $T(G)$ is isomorphic to

$$\mathbf{F}_p^{\binom{n}{2}\binom{n+1}{2}} \rtimes \left(\mathbf{F}_p^{\left(\binom{n}{2}-n\right)\times n} \rtimes \left(\mathrm{GL}(n, \mathbf{F}_p) \times \mathrm{GL}\left(\binom{n}{2} - n, \mathbf{F}_p\right)\right)\right).$$

The $\mathbf{F}_p^{\binom{n}{2}\binom{n+1}{2}}$ part comes from the symmetric forms, the rest from the antisymmetric ones.

The $\mathrm{GL}(n, \mathbf{F}_p)$ part follows from the fact we have just proved: all $\alpha \in \mathrm{GL}(V)$ occur as restrictions of some $\vartheta \in T(G)$ to $G/G' = V$.

To get the rest of the statement, one would need the consider the restriction of $\vartheta \in T(G)$ to $G' = \bigwedge^2 V$, that is, fully exploit the degrees of freedom we had in solving in $X \in \mathrm{GL}(\bigwedge^2 V)$ the equation

$$\alpha^{-1} D = DX \qquad \text{via} \qquad X = \overline{D}^{-1} \cdot \overline{\alpha^{-1} D}.$$

Small

Let G be a finite p-group of class two, for $p > 2$. Then $T(G)$ contains a cyclic group of order $\varphi(p^r) = p^{r-1}(p-1)$, where p^r is the exponent of $G/Z(G)$.

The $p-1$ part is obtained by considering the power maps

$$\begin{aligned} \vartheta_d : G &\to G \\ x &\mapsto x^d, \end{aligned}$$

where $\gcd(d, p) = 1$. We have

$$(xy)^{\vartheta} = x^d y^d [y, x]^{\binom{d}{2}},$$

from which one can see that (ι is "conjugation by")

$$\rho(g)^{\vartheta_d} = \iota(g^{(1-d)/2})\rho(g^d) \in \mathrm{Aut}(G)\rho(G) = \mathrm{Hol}(G),$$

and since ϑ_d commutes elementwise with $\mathrm{Aut}(G)$, we have that $\vartheta_d \in \mathrm{NHol}(G) = N_{S(G)}(\mathrm{Hol}(G))$.

Small II

Let G be a finite p-group of class two, for $p > 2$. Then $T(G)$ contains a cyclic group of order $\varphi(p^r) = p^{r-1}(p-1)$, where p^r is the exponent of $G/Z(G)$.

So we may say that $T(G)$ is small, or minimal, when it reaches that lower bound.

We have considered various groups on $n = 3$ or 4 generators, of the previous form

$$\langle\, x_1, \dots, x_n : x_i^p = \prod_{j<k} [x_j, x_k]^{d_{i,(j,k)}}, i = 1, \dots n \,\rangle,$$

where the matrix $D = [d_{i,(j,k)}]$ has rank one, and found which cases yield a a small $T(G)$.

The case of rank zero (i.e. $D = 0$) yields easily a small $T(G)$, as G is free in the variety of groups of class two and exponent p there.

Thanks!

That's All, Thanks!