Finite p-groups, automorphisms, multiple holomorphs, and skew braces

Andrea Caranti

Omaha, 30 May 2023

Dipartimento di Matematica
Università degli Studi di Trento
Italy

Nilpotent groups

Let G be a group. The commutator of $x, y \in G$ is

$$[x, y] = x^{-1}y^{-1}xy = x^{-1}x^{y} = (yx)^{-1}xy.$$

Thus $xy = yx[x, y]$, so that $xy = yx$ iff $[x, y] = 1$.

The commutator of two subgroups $H, K \leq G$ is the subgroup

$$[H, K] = \langle\, [h, k] : h \in H, k \in K \,\rangle.$$

Thus G is abelian iff $G' = [G, G] = \{\, 1 \,\}$.

The lower central series of G is defined recursively as

$$\begin{aligned} \gamma_1(G) &= G, \\ \gamma_{i+1}(G) &= [\gamma_i(G), G], \quad \text{for } i \geq 1. \end{aligned}$$

A group G is nilpotent if $\gamma_{n+1}(G) = \{\, 1 \,\}$ for some n. The minimum such n is the (nilpotence) class of G. So the groups of class one are the non-trivial abelian groups.

Groups of class two

A group G has class (at most) two if for all $x, y, z \in G$ one has

$$[[x, y], z] = 1, \quad \text{or equivalently} \quad [x, y]^z = z^{-1}[x, y]z = [x, y],$$

that is, the derived group

$$G' = [G, G] = \langle\, [x, y] : x, y \in G \,\rangle$$

is contained in the centre

$$\begin{aligned} Z(G) &= \{\, z \in G : [z, x] = 1 \text{ for all } x \in G \,\} \\ &= \{\, z \in G : z^x = z \text{ for all } x \in G \,\}. \end{aligned}$$

Calculations in an individual group of class two are somewhat easy

$$(xy)^2 = xyxy = xxy[y, x]y = x^2y^2[y, x].$$

More generally, in a group of class two one has for all n

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

Finite p-groups

Let p be a prime. A finite p-group (that is, a group of order p^n for some integer n) is nilpotent.

Finite, abelian p-groups are easily classified in terms of partitions.

The standard commutator identity

$$[x, yz] = [x, z][x, y]^z$$

shows that in a group of class two commutators are bilinear functions.

In finite p-groups of class two p-th powers also behave well for $p > 2$. For instance, if x, y have order $p > 2$, then

$$(xy)^p = x^p y^p [y, x]^{\binom{p}{2}} = x^p y^p [y, x^{\binom{p}{2}}] = 1,$$

so their product xy has order (at most) p. If $p = 2$, this does not work ($(xy)^2 = x^2 y^2 [y, x]$), see the dihedral group of order 8.

Automorphisms

Let G be a (nilpotent) group. Its group of central automorphisms is

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

Here $\mathrm{Aut}(G)$ is the group of automorphisms of G, and $\mathrm{Inn}(G)$ is the group of inner automorphisms, that is, the image of the map

$$\begin{aligned} G &\to \mathrm{Aut}(G) \\ g &\mapsto (x \mapsto x^g = g^{-1}xg). \end{aligned}$$

The kernel of this map is $Z(G)$, so that $\mathrm{Inn}(G) \cong G/Z(G)$. It follows that

$$\begin{aligned} \mathrm{Aut}_c(G) &= \{\, \alpha \in \mathrm{Aut}(G) : \alpha \text{ acts trivially on } G/Z(G) \,\} \\ &= \ker(\text{restriction map } \mathrm{Aut}(G) \to \mathrm{Aut}(G/Z(G))). \end{aligned}$$

Too many groups

H. Heineken and H. Liebeck
The occurrence of finite groups in the automorphism group of nilpotent groups of class 2
Arch. Math. (Basel) **25** (1974), 8–16

Theorem (Heineken and Liebeck)

Let X be an arbitrary finite group, $p > 2$ a prime. Then there is a finite p-group G of class two such that $\mathrm{Aut}(G)/\mathrm{Aut}_c(G) \cong X$.

- The class of finite p-groups of class two is as complicated as the class of all finite groups.
- If G is a nonabelian finite p-group, then $\mathrm{Inn}(G)$ is a non-trivial normal p-subgroup of $\mathrm{Aut}(G)$.
- (Adney and Yen) If the finite p-group G has no non-trivial central factor, then $\mathrm{Aut}_c(G) \trianglelefteq \mathrm{Aut}(G)$ is a p-group.
- If G has class two, then $\mathrm{Inn}(G) \leq \mathrm{Aut}_c(G)$.

Coclass (a diversion) I

The coclass of a finite p-group of order p^n and class c is $n - c$.

When $n - c = 1$ one speaks of a group of maximal class, as $n - 1$ is the highest possible class for a group of order p^n.

For each p, there is only one infinite pro-p-group of maximal class.

1. When $p = 2$ this is the 2-adic dihedral group, the extension of the group $\mathbf{Z}_2$ of diadic integers by an element inducing the automorphism which takes an element to its opposite.
2. For an arbitrary p, this is the extension of $\mathbf{Z}_p[\omega]$, where ω is a primitive p-th root of unity, by an element of order p acting as multiplication by ω.

Coclass (a diversion) II

C.R. Leedham-Green and M.F. Newman
Space groups and groups of prime-power order. I
Arch. Math. (Basel) **35** (1980), no. 3, 193–202

It is a deep result that for every r and prime p, there are a finite number of infinite pro-p-group of coclass r, and these are soluble.

C.R. Leedham-Green
The structure of finite p-groups
J. London Math. Soc. (2) **50** (1994), no. 1, 49–67

Aner Shalev
The structure of finite p-groups: effective proof of the coclass conjectures
Invent. Math. **115** (1994), no. 2, 315–345

Possibly as close to a classification of finite p-groups as it gets.

A special class of finite p-groups of class two

Let p be an odd prime.

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

where $D = [d_{i,(j,k)}]$ is an $n \times \binom{n}{2}$ matrix of maximum rank.

We have

$$\begin{aligned}
[x_i, x_t]^p &= [x_i^p, x_t] \\
&= [\prod_{j<k} [x_j, x_k]^{d_{i,(j,k)}}, x_t] \\
&= \prod_{j<k} [[x_j, x_k], x_t]^{d_{i,(j,k)}} = 1,
\end{aligned}$$

that is, $[G, G]^p = 1$.

More details

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

Since $[G, G]^p = 1$, and $G^p \le [G, G]$, we have $G^{p^2} = 1$. Moreover,

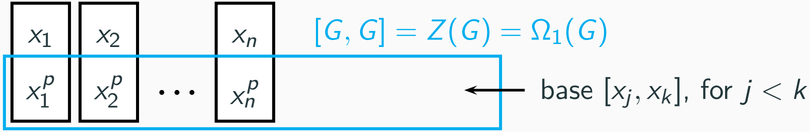
$$(yz)^p = y^p z^p [z, y]^{\binom{p}{2}} = y^p z^p,$$

that is, the map $y \mapsto y^p$ is a morphism $G \to [G, G]$. Thus

$$(\prod_i x_i^{e_i})^p = (\prod_i x_i^p)^{e_i} = \prod_i (\prod_{j<k} [x_j, x_k]^{d_{i,(j,k)}})^{e_i} =$$

$$= \prod_{j<k} (\prod_i [x_j, x_k]^{d_{i,(j,k)}})^{e_i} = \prod_{j<k} [x_j, x_k]^{\sum_i e_i d_{i,(j,k)}}$$

Thus $(\prod_i x_i^{e_i})^p = 1$ iff $\sum_i e_i d_{i,(j,k)} = 0$ in $\mathrm{GF}(p)$. Since $D = [d_{i,(j,k)}]$ is of maximum rank, this holds iff $(e_1, \ldots, e_n) = 0$ in $\mathrm{GF}(p)^n$, i.e., all exponents e_i are divisible by p, i.e. $\prod_i x_i^{e_i} \in G'$. Thus $\Omega_1(G) = \langle\, g \in G : g^p = 1 \,\rangle = [G, G]$.



$G' = [G,G]$ and $V = G/G'$ are elementary abelian p-groups, thus vector spaces over $\mathrm{GF}(p)$.

A construction via repeated cyclic extensions shows that the $[x_j, x_k]$, for $j < k$, are a base for the vector space G'.

Thus, there is an isomorphism of vector spaces

$$G' \to \bigwedge^2 V$$
$$[x_i, x_j] \mapsto (x_i G') \wedge (x_j G').$$

Some Linear Algebra II

$V = G/G'$ and $G' \cong \bigwedge^2 V$ are vector spaces over $\mathrm{GF}(p)$. Write $v_i = x_i G'$. Recall $x_i^p = \prod_{j<k} [x_j, x_k]^{d_{i,(j,k)}}$.

Then the p-th power map in G induces an injective linear map

$$\begin{aligned} \pi : V &\to \bigwedge^2 V \\ v_i &\mapsto \sum_{j<k} d_{i,(j,k)} v_j \wedge v_k, \end{aligned}$$

whose matrix is $D = [d_{i,(j,k)}]$.

Recall $\mathrm{Aut}(G)/\mathrm{Aut}_c(G)$ is the image of $\mathrm{Aut}(G)$ under

$$\mathrm{Aut}(G) \to \mathrm{Aut}(G/Z(G)) = \mathrm{GL}(V)$$

$\mathrm{Aut}(G)/\mathrm{Aut}_c(G)$ is the group of automorphisms induced on V, thus a subgroup of $\mathrm{GL}(V)$.

Some Linear Algebra III

Let $\widehat{\alpha}$ be the map induced on $\bigwedge^2 V$ by $\alpha \in \mathrm{GL}(V)$:

$$(v \wedge w)^{\widehat{\alpha}} = v^{\alpha} \wedge w^{\alpha}.$$

Then

$$\begin{aligned} \mathrm{GL}(V) &\geq \mathrm{Aut}(G)/\,\mathrm{Aut}_c(G) \\ &= \{\, \alpha \in \mathrm{GL}(V) : \alpha \circ \pi = \pi \circ \widehat{\alpha} \,\}, \end{aligned}$$

that is, the elements $\alpha \in \mathrm{GL}(V)$ that belong to $\mathrm{Aut}(G)/\,\mathrm{Aut}_c(G)$ are those for which the following diagram commutes

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

Some Linear Algebra IV

$$\mathrm{GL}(V) \geq \mathrm{Aut}(G)/\mathrm{Aut}_c(G) = \{ \alpha \in \mathrm{GL}(V) : \alpha \circ \pi = \pi \circ \widehat{\alpha} \},$$

or, in matrix terms $\alpha D = D\widehat{\alpha}$, since D is the matrix of the p-th power map $\pi : V \to \bigwedge^2 V$. This idea has been introduced for $\dim(V) = 3$ in

G. Daues and H. Heineken
Dualitäten und Gruppen der Ordnung p^6
Geometriae Dedicata **4** (1975), 215–220

and then used for $\dim(V) = 4$ in

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

Some linear algebra V

$$\begin{aligned}\mathrm{GL}(V) &\geq \mathrm{Aut}(G)/\,\mathrm{Aut}_c(G)\\ &= \{\, \alpha \in \mathrm{GL}(V) : \alpha \circ \pi = \pi \circ \widehat{\alpha} \,\},\end{aligned}$$

or, in matrix terms,

$$\alpha D = D\widehat{\alpha},$$

where D is the matrix of the p-th power map $\pi : V \to \bigwedge^2 V$.

A proof of this characterisation, and of an extension of it, is contained in

A.C and C. Tsang
Finite p-groups of class two with a large multiple holomorph
J. Algebra **617** (2023), 476–499

Modifying a group operation I

Reinhold Baer
Groups with abelian central quotient group
Trans. Amer. Math. Soc. **44** (1938), no. 3, 357–386

Let G be a group of nilpotence class two admitting unique square roots. For instance, G could be a finite p-group, for $p > 2$, and $\sqrt{g} = g^{(\exp(G)+1)/2}$. Define

$$g \circ h = g \cdot h \cdot [g, h]^{-1/2}.$$

Then $(G, \circ)$ is an abelian group.

$$\begin{aligned} h \circ g = h \cdot g \cdot [h, g]^{-1/2} &= g \cdot h \cdot [h, g] \cdot [h, g]^{-1/2} \\ &= g \cdot h \cdot [h, g]^{1/2} = g \cdot h \cdot [g, h]^{-1/2} = g \circ h. \end{aligned}$$

This is a very special case of the Lazard correspondence and the Baker–Campbell–Hausdorff formula.

Modifying a group operation II

$$g \circ h = g \cdot h \cdot [g, h]^{-1/2}.$$

In a group G of nilpotence class two, commutators are bilinear (and alternating) functions. If you take any bilinear function

$$\Delta : G \times G \to G'$$

then

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

defines another group operation on the set G. For instance, the inverse in $(G, \circ)$ is $x^{\ominus 1} = x^{-1} \cdot \Delta(x, x)$, as

$$x \circ (x^{-1} \cdot \Delta(x, x)) = x \cdot x^{-1} \cdot \Delta(x, x) \cdot \Delta(x, x^{-1} \cdot \Delta(x, x))$$

Now G' is in both kernels of Δ, as the codomain G' is abelian. Thus this equals $\Delta(x, x) \cdot \Delta(x, x^{-1}) = 1$.

The proof of associativity follows the same pattern.

Skew braces

A skew brace is a triple $(G, \cdot, \circ)$, where "$\cdot$" and "$\circ$" are two group operations on G, related by

$$((xy) \circ z) \cdot z^{-1} = (x \circ z) \cdot z^{-1} \cdot (y \circ z) \cdot z^{-1}.$$

In other words, for each $z \in G$ the map

$$\begin{aligned} \gamma(z) : G &\to G \\ x &\mapsto (x \circ z) \cdot z^{-1} \end{aligned}$$

is an endomorphism of $(G, \cdot)$. Actually,

$$\gamma : (G, \circ) \to \mathrm{Aut}(G)$$

is a morphism. Then

$$x^{\gamma(z)} = (x \circ z) \cdot z^{-1}$$

rephrases as

$$x \circ z = x^{\gamma(z)} \cdot z.$$

Central automorphisms I

The characterisation

$$\mathrm{GL}(V) \geq \mathrm{Aut}(G)/\,\mathrm{Aut}_c(G) = \{\, \alpha \in \mathrm{GL}(V) : \alpha \circ \pi = \pi \circ \widehat{\alpha} \,\},$$

has been used in

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

to exhibit explicit examples of groups of class two with all of their automorphisms central.

Cindy and I have been using these groups to construct examples where the multiple holomorph is big. (To be made more precise soon.)

Skew braces, regular subgroups and the multiple holomorph

Let $(G, \cdot)$ be a finite group, $\rho : (G, \cdot) \to \mathrm{Sym}(G)$ its right regular representation. A skew brace $(G, \cdot, \circ)$ corresponds to a regular subgroup $N \leq \mathrm{Hol}(G, \cdot) = N_{\mathrm{Sym}(G)}(\rho(G)) = \mathrm{Aut}(G)\rho(G)$ such that $N \cong (G, \circ)$.

The multiple holomorph of $(G, \cdot)$ is

$$N_{\mathrm{Sym}(G)}(\mathrm{Hol}(G)) = N_{\mathrm{Sym}(G)}(N_{\mathrm{Sym}(G)}(\rho(G))).$$

It acts transitively on the set of the regular subgroups N such that

1. $N \trianglelefteq \mathrm{Hol}(G)$, and
2. $(G, \cdot) \cong (G, \circ)$,

so that the group

$$T(G) = N_{\mathrm{Sym}(G)}(\mathrm{Hol}(G)) / \mathrm{Hol}(G)$$

acts regularly on the set of these regular subgroups.

Small is beautiful

$$T(G) = N_{\mathrm{Sym}(G)}(\mathrm{Hol}(G)) / \mathrm{Hol}(G)$$

acts regularly on the set of the regular subgroups N of $\mathrm{Sym}(G)$ such that

$$N \trianglelefteq \mathrm{Hol}(G), \quad \text{and} \quad (G, \cdot) \cong (G, \circ).$$

The first condition translates, in terms of gamma functions, to

$$\gamma(x^{\beta}) = \gamma(x)^{\beta} = \beta^{-1}\gamma(x)\beta, \quad \text{for all } \beta \in \mathrm{Aut}(G).$$

So if you want a big multiple holomorph (actually, a big $T(G)$), it is advisable to have $\mathrm{Aut}(G)$ as small as possibile.

Tim Kohl
Multiple holomorphs of dihedral and quaternionic groups
Comm. Algebra **43** (2015), no. 10, 4290–4304

J.E. Adney and Ti Yen
Automorphisms of a p-group.
Illinois J. Math. **9** (1965), 137–143

If G has no abelian direct factors, then the elements of $\mathrm{Aut}_c(G)$ correspond to the elements of $\mathrm{Hom}(G, Z(G))$, via

$$x \cdot x^f \mapsfrom f, \quad \text{and} \quad \beta \mapsto (x \mapsto x^{-1}x^\beta = [x, \beta]).$$

So if $\mathrm{Aut}(G) = \mathrm{Aut}_c(G)$ (i.e. $\mathrm{Aut}(G)$ is as small as possible), then $x^{\gamma(y)} = x \cdot [x, \gamma(y)]$, where $x \mapsto [x, \gamma(y)]$ is in $\mathrm{Hom}(G, Z(G))$, for a fixed y. Thus

$$x \circ y = x^{\gamma(y)} \cdot y = x \cdot [x, \gamma(y)] \cdot y = x \cdot y \cdot [x, \gamma(y)].$$

In fact, $\Delta : (x, y) \mapsto [x, \gamma(y)]$ is an arbitrary bilinear function with values in $Z(G)$.

From bilinear to linear

$$x \circ y = x \cdot y \cdot \Delta(x, y), \quad \text{with} \quad \Delta : V \times V \mapsto \bigwedge^2 V \quad \text{bilinear.}$$

In the class of groups described above $V = G/G'$ and $G' \cong \bigwedge^2 V$.

To determine the multiple holomorph, you want to determine those "$\circ$", and thus those Δ, for which $(G, \cdot) \cong (G, \circ)$.

Symmetric bilinear maps Δ always give that.

Now an alternating bilinear map

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

corresponds, by the universal property of the external square, to a linear map

$$\sigma : \bigwedge^2 V \to \bigwedge^2 V.$$

Commutators

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

with $\Delta : V \times V \mapsto \bigwedge^2 V$ bilinear and alternating, described by

$$\sigma : \bigwedge^2 V \to \bigwedge^2 V.$$

A straightforward computation yields

$$\begin{aligned} [x, y]_\circ &= [x, y] \cdot \Delta(x, y) \cdot \Delta(y, x)^{-1} \\ &= [x, y] \cdot \Delta(x, y)^2 \\ &= [x, y]^{1+2\sigma}. \end{aligned}$$

Thus $(G, \cdot)$ cannot be isomorphic to $(G, \circ)$ when $\sigma \in \mathrm{End}(\bigwedge^2 V)$ has $-1/2$ as an eigenvalue, because then the derived subgroup of $(G, \circ)$ is smaller than that of $(G, \cdot)$.

This happened with Baer's formula $x \circ y = x \cdot y \cdot [x, y]^{-1/2}$.

From automorphisms to isomorphisms I

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

The first diagram tells us that $\alpha \in \mathrm{Aut}(G)/\mathrm{Aut}_c(G) \leq \mathrm{GL}(V)$ iff

$$\alpha D = D\widehat{\alpha},$$

where D is the matrix of the p-th power map $\pi : V \to \bigwedge^2 V$ in $(G, \cdot)$. The second diagram tells us that $(G, \cdot) \cong (G, \circ)$ iff there is $\alpha \in \mathrm{GL}(V)$ s.t.

$$\alpha\pi_\circ = \pi\hat{\alpha},$$

where $\pi, \pi_\circ : V \to \bigwedge^2 V$ are induced from the p-th power maps on $(G, \cdot)$, resp. $(G, \circ)$.

From automorphisms to isomorphisms II

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

$(G, \cdot) \cong (G, \circ)$ iff there is $\alpha \in \mathrm{GL}(V)$ such that

$$\alpha\pi_\circ = \pi\hat{\alpha},$$

where $\pi, \pi_\circ : V \to \bigwedge^2 V$ are induced from the p-th power maps on $(G, \cdot)$, resp. $(G, \circ)$. When you put it in coordinates, you get

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

Heineken's characterization is the special case $\sigma = 0$, that is, when "$\cdot$" and "$\circ$" coincide, and we are talking automorphisms of $(G, \cdot)$.

That's All, Thanks!