

A new classification of the 2-generated p -groups of class 2

A. Ahmad¹ A. Magidin² R.F. Morse³

¹Universiti Teknologi Malaysia

²University of Louisiana at Lafayette

³University of Evansville

Special Session on Computational Group Theory,
Kalamazoo MI, Oct 2008

What Came Before

- Trebenko (1989) attempted a description of all 2-generated nilpotent groups of class two.
- For p -groups, this was picked up by Bacon and Kappe (1993) and Kappe-Visscher-Nor Haniza Sarmin (1999).
- The idea: pick $b \in G - \Phi(G)$ of minimal order, $a \in G$ of minimal order among those with $\langle a, b \rangle = G$, then consider the cases:
 - $\{1\} = \langle a \rangle \cap G' = \langle b \rangle \cap G'$;
 - $G' \subseteq \langle a \rangle$, $\{1\} = \langle b \rangle \cap G'$;
 - $\{1\} \neq \langle a \rangle \cap G' \neq G'$, $\{1\} = \langle b \rangle \cap G'$;
 - If $p = 2$, $\langle a \rangle \cap \langle b \rangle \neq \{1\}$.

A missing group

- Azhana binti Ahmad found (2008) a group of order 256 that did not appear in their list:

$$\left\langle a, b \mid \begin{array}{l} a^{2^4} = b^{2^5} = [a, b, a] = [a, b, b] = 1 \\ a^{2^2} = [a, b], \quad a^{2^3} = b^{2^4} = [a, b]^2 \end{array} \right\rangle.$$

- A similar group exists for any odd p .
- The group is not a split extension.

A different approach

Robert Morse suggested the following approach:

- 1 Let G be a 2-generator p -group of class 2, order p^n . Then G' is cyclic, and G^{ab} is a 2-generated noncyclic abelian group.
- 2 G can be realized as a central extension

$$1 \rightarrow C_{p^\gamma} \xrightarrow{\psi} G \xrightarrow{\eta} C_{p^\alpha} \times C_{p^\beta} \rightarrow 1$$

with $\alpha \geq \beta \geq \gamma$, $\alpha + \beta + \gamma = n$.

- 3 Let $\mathfrak{G}_p(\alpha, \beta, \gamma)$ be the collection of all p -groups of this type.
- 4 If $G \in \mathfrak{G}_p(\alpha, \beta, \gamma)$, $H \in \mathfrak{G}_p(\alpha', \beta', \gamma')$, and $G \cong H$, then $(\alpha, \beta, \gamma) = (\alpha', \beta', \gamma')$.

The parameters

Let $\alpha \geq \beta \geq \gamma \geq 1$, $G \in \mathfrak{G}_p(\alpha, \beta, \gamma)$.

Pick a generator $c \in G'$, and $a, b \in G$ that project onto a basis for $G^{\text{ab}} \cong C_{p^\alpha} \times C_{p^\beta}$, $|\bar{a}| = p^\alpha$, $|\bar{b}| = p^\beta$.

Then G is presented by specifying the relations

$$\begin{aligned}c^a &= 1, & c^b &= 1, \\ [a, b] &= c^t, & \gcd(t, p) &= 1 \\ a^{p^\alpha} &= c^r, & b^{p^\beta} &= c^s.\end{aligned}$$

Same group, different parameters?

Question

When is the group presented with parameters r, s, t isomorphic to the group with parameters r', s', t' ?

Isomorphisms

Proposition

Let $G, H \in \mathfrak{G}_p(\alpha, \beta, \gamma)$, $a, b, c \in G$ as above, with $[a, b] = c^t$, $a^{p^\alpha} = c^r$, $b^{p^\beta} = c^s$; and H generated by a', b', c' , $[a', b'] = c'^{t'}$, $a'^{p^\alpha} = c'^{r'}$, $b'^{p^\beta} = c'^{s'}$. Then H is isomorphic to G if and only if there exist $a_1, b_1, c_1 \in G$, with

$$\begin{aligned}a_1 &= a^k b^\ell, \\b_1 &= a^{mp^{\alpha-\beta}} b^n, \\c_1 &= c^q,\end{aligned}$$

that satisfy the same relations as a', b', c' , and

$$\gcd(p, kn - \ell mp^{\alpha-\beta}) = \gcd(p, q) = 1.$$

Sketch of proof

Sketch. If $\varphi: H \rightarrow G$ is an isomorphism, then

$$\begin{aligned}\varphi(a') &= a^k b^\ell c^u \\ \varphi(b') &= a^{mp^{\beta-\alpha}} b^n c^v.\end{aligned}$$

The values of u and v do not affect the relations we are interested in, so take a_1 and b_1 with $u = v = 0$, and $c_1 = \varphi(c')$.

If a_1, b_1, c_1 satisfy the relations of a', b', c' , this gives $\varphi: H \rightarrow G$. The conditions on $\gcd(kn - \ell mp^{\alpha-\beta})$ guarantees the map is onto, and $|G| = |H|$ yields that φ is an isomorphism. \square

Simplifying futher

Proposition

Let $G \in \mathfrak{G}_p(\alpha, \beta, \gamma)$, generated by a, b, c with parameters r, s, t . Write $r = up^\rho$, $s = vp^\sigma$, $\gcd(uv, p) = 1$, $0 \leq \rho, \sigma \leq \gamma$. Then G is isomorphic to the group in $\mathfrak{G}_p(\alpha, \beta, \gamma)$ with parameters $r' = p^\rho$, $s' = p^\sigma$, $t' = 1$.

Sketch. Since $G' = \langle c^t \rangle = \langle c \rangle$, we must have $\gcd(p, t) = 1$. Find integers w, x, y such that $\gcd(p, y) = 1$ and

$$wx t \equiv y p^0 \pmod{p^\gamma}$$

$$wr \equiv y p^\rho \pmod{p^\gamma}$$

$$xs \equiv y p^\sigma \pmod{p^\gamma}$$

Then set $a_1 = a^w$, $b_1 = b^x$, $c_1 = c^y$. \square

Preliminary Parametrization

Every 2-generated p -group of class 2 and order p^n can be described by 5 integers,

$$(\alpha, \beta, \gamma; \rho, \sigma)$$

where:

- $1 \leq \gamma \leq \beta \leq \alpha$ and $n = \alpha + \beta + \gamma$.
- $G^{\text{ab}} \cong C_{p^\alpha} \times C_{p^\beta}$.
- $[G, G] \cong C_{p^\gamma}$.
- $0 \leq \rho, \sigma \leq \gamma$.
- There exist a generator c of G' , and generators a, b of G with $[a, b] = c$, $a^{p^\alpha} = c^{p^\rho}$, $b^{p^\beta} = c^{p^\sigma}$.

Question

When is $(\alpha, \beta, \gamma; \rho, \sigma)$ isomorphic to $(\alpha, \beta, \gamma; r, s)$?

Computing the powers

Let $G \sim (\alpha, \beta, \gamma; \rho, \sigma)$. Set

$$\begin{aligned}a_1 &= a^k b^\ell \\ b_1 &= a^{mp^{\alpha-\beta}} b^n\end{aligned}$$

with $\gcd(p, kn - \ell mp^{\alpha-\beta}) = 1$. Then

$$\begin{aligned}a_1^{p^\alpha} &= a^{kp^\alpha} b^{\ell p^\alpha} [b, a]^{k\ell \binom{p^\alpha}{2}} \\ &= c^{kp^\rho + \ell p^{\alpha-\beta+\sigma} - k\ell \binom{p^\alpha}{2}}. \\ b_1^{p^\beta} &= a^{mp^\alpha} b^{np^\beta} [b, a]^{mnp^{\alpha-\beta} \binom{p^\beta}{2}} \\ &= c^{mp^\rho + np^\sigma - mnp^{\alpha-\beta} \binom{p^\beta}{2}}.\end{aligned}$$

We need to determine the highest power of p that divides the exponent of c in the given expressions.

Case 1: $\alpha > \beta$

If $\alpha > \beta$, we need $\gcd(p, kn) = 1$. The exponents simplify to:

$$\begin{aligned} a_1^{p^\alpha} &= c^{kp^\rho + lp^{\alpha-\beta+\sigma}}, \\ b_1^{p^\beta} &= c^{mp^\rho + np^\sigma}. \end{aligned}$$

Three cases:

- If $\rho \leq \sigma$, then $\mathbf{G} \sim (\alpha, \beta, \gamma; \rho, \gamma)$.
- If $\alpha - \beta + \sigma \leq \rho$, then $\mathbf{G} \sim (\alpha, \beta, \gamma; \gamma, \sigma)$.
- If $\sigma < \rho < \alpha - \beta + \sigma$, $\rho < \gamma$, then $\mathbf{G} \sim (\alpha, \beta, \gamma; \rho, \sigma)$.
(Missing family)

Case 2: $\alpha = \beta > \gamma$ or $\alpha = \beta = \gamma$ and $p > 2$

Here we need $\gcd(p, kn - \ell m) = 1$. The exponents simplify to

$$\begin{aligned} a_1^{p^\alpha} &= c^{kp^\rho + \ell p^\sigma}, \\ b_1^{p^\beta} &= c^{mp^\rho + np^\sigma}. \end{aligned}$$

We may exchange a and b .

Here, we have $G \sim (\alpha, \beta, \gamma; \min(\rho, \sigma), \gamma)$.

Case 3: $\alpha = \beta = \gamma$ and $p = 2$

Again we need $\gcd(p, kn - \ell m) = 1$ and the exponents of c become:

$$\begin{aligned} a_1^{p^\alpha} &= c^{kp^\rho + \ell p^\sigma + k\ell p^{\gamma-1}}, \\ b_1^{p^\beta} &= c^{mp^\rho + np^\sigma + mn p^{\gamma-1}}. \end{aligned}$$

- If $\min(\rho, \sigma) < \gamma - 1$ then $G \sim (\alpha, \beta, \gamma; \min(\rho, \sigma), \gamma)$.
- If $\min(\rho, \sigma) \geq \gamma - 1$ and $\max(\rho, \sigma) = \gamma$, then $G \sim (\alpha, \beta, \gamma; \gamma, \gamma)$.
- If $\rho = \sigma = \gamma - 1$, then $G \sim (\alpha, \beta, \gamma; \gamma - 1, \gamma - 1)$.

The classification

Theorem

Let $\alpha \geq \beta \geq \gamma > 0$, $G \in \mathfrak{G}_p(\alpha, \beta, \gamma)$. Let $a, b, c \in G$, with $\langle c \rangle = G'$, \bar{a}, \bar{b} a basis for G^{ab} , $[a, b] = c^i$, $a^{p^\alpha} = c^j$, $b^{p^\beta} = c^k$. Write $j = up^\rho$, $k = vp^\sigma$, with $\gcd(p, uv) = 1$. Then:

- If $\alpha > \beta$, then G is isomorphic to:
 - $(\alpha, \beta, \gamma; \rho, \gamma)$ if $\rho \leq \sigma$.
 - $(\alpha, \beta, \gamma; \gamma, \sigma)$ if $\alpha - \beta + \sigma \leq \rho$.
 - $(\alpha, \beta, \gamma; \rho, \sigma)$ if $\sigma < \rho < \alpha - \beta$, $\rho < \gamma$.
- If $\alpha = \beta > \gamma$, or $\alpha = \beta = \gamma$ and $p > 2$, then G is isomorphic to $(\alpha, \beta, \gamma; \min(\rho, \sigma), \gamma)$.
- If $\alpha = \beta = \gamma$ and $p = 2$, then G is isomorphic to:
 - $(\alpha, \beta, \gamma; \min(\rho, \sigma), \gamma)$ if $\min(\rho, \sigma) < \gamma - 1$.
 - $(\alpha, \beta, \gamma; \gamma - 1, \gamma - 1)$ if $\rho = \sigma = \gamma - 1$.
 - $(\alpha, \beta, \gamma; \gamma, \gamma)$ otherwise.

Counting the groups. Case 1: $\alpha = \beta$

We can use the classification to count the 2-generated p -groups of class exactly 2 and order p^n .

Fix $\alpha \geq \beta \geq \gamma > 0$, $\alpha + \beta + \gamma = n$. We only display the pair (ρ, σ) :

If $\alpha = \beta$, we have:

$$(0, \gamma), (1, \gamma), \dots, (\gamma, \gamma).$$

for a total of $\gamma + 1$ nonisomorphic groups. When $p = 2$,

$(\alpha, \beta, \gamma; \gamma - 1, \gamma) \cong (\alpha, \beta, \gamma; \gamma, \gamma)$, but then we also have $(\alpha, \beta, \gamma, \gamma - 1, \gamma - 1)$, so the total is the same.

Case 2: $\alpha - \beta > \gamma$

If $\alpha - \beta > \gamma$, then we have:

$$(0, \gamma), \dots, (\gamma, \gamma);$$

$$(1, 0), (2, 0), \dots, (\gamma, 0);$$

$$\vdots$$

$$(\gamma, \gamma - 1).$$

for a total of $1 + \dots + (\gamma + 1) = \frac{1}{2}(\gamma + 1)(\gamma + 2)$ nonisomorphic groups.

Case 3: $0 < \alpha - \beta \leq \gamma$

Here we have:

$$(0, \gamma), (1, \gamma), \dots, (\gamma, \gamma)$$

$$(1, 0), (2, 0), \dots, (\alpha - \beta, 0)$$

$$(2, 1), (3, 1), \dots, (\alpha - \beta + 1, 1)$$

$$\vdots$$

$$(\gamma - (\alpha - \beta) + 1, \gamma - (\alpha - \beta)), \dots, (\gamma, \gamma - (\alpha - \beta))$$

$$(\gamma - (\alpha - \beta) + 2, \gamma - (\alpha - \beta) + 1), \dots, (\gamma, \gamma - (\alpha - \beta) + 1)$$

$$(\gamma - (\alpha - \beta) + 3, \gamma - (\alpha - \beta + 2)), \dots, (\gamma, \gamma - (\alpha - \beta) + 2)$$

$$\vdots$$

$$(\gamma, \gamma - 1)$$

Total is:

$$(\gamma + 1) + \frac{1}{2}(\alpha - \beta)(2\gamma + 1 - (\alpha - \beta))$$

nonisomorphic groups.

Number of elements of $\mathfrak{G}(\alpha, \beta, \gamma)$

Theorem

Let $n > 0$, and let $\alpha \geq \beta \geq \gamma > 0$ be integers such that $\alpha + \beta + \gamma = n$. Then

$$|\mathfrak{G}_p(\alpha, \beta, \gamma)| = (\gamma + 1) + \frac{1}{2} \min(\alpha - \beta, \gamma) (2\gamma + 1 - \min(\alpha - \beta, \gamma)).$$

2-gen. groups of order p^n and class ≤ 2

n	Number of 2-gen. groups of class 2	Number of 2-gen. groups of class ≤ 2
1	0	1
2	0	2
3	2	4
4	3	6
5	5	8
6	9	13
7	13	17
8	18	23
9	26	31
10	34	40
11	44	50

Future directions

We have a “dictionary” between the old descriptions and the new ones.

Work in progress:

- Compute the nonabelian tensor square and other homological functors relative to the new description.
- Expand previous results to the new family.